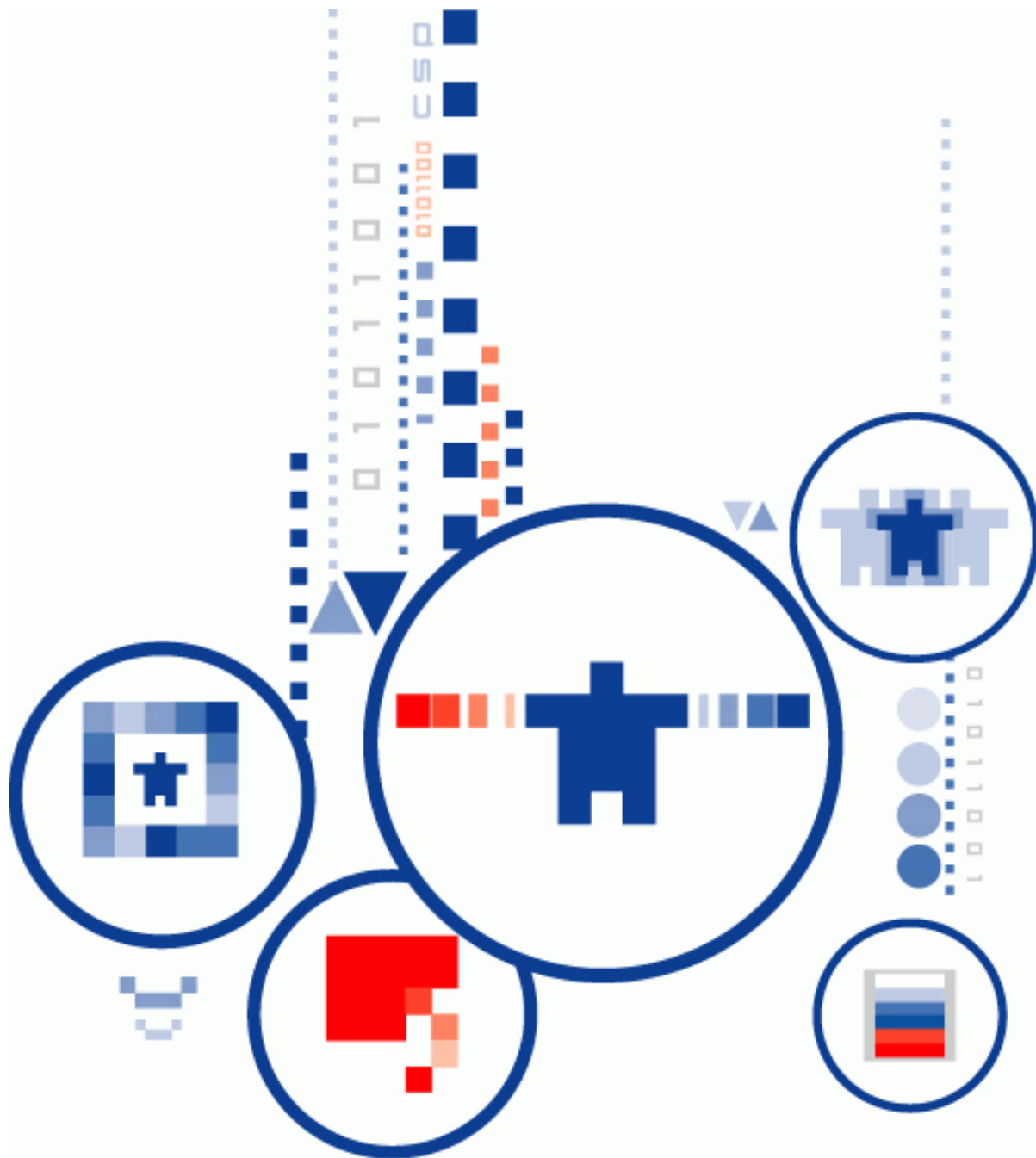




КриптоПро **Центр Мониторинга**

Руководство по установке и настройке

СОДЕРЖАНИЕ

1. Аннотация	3
2. Общее описание КriptoПро Центр Мониторинга	4
2.1. Сервер Мониторинга «КriptoПро Центр мониторинга»	5
2.2. Агенты «КriptoПро Центр Мониторинга»	5
2.3. Лицензирование КriptoПро Центр Мониторинга	5
2.4. Принцип работы КriptoПро Центр Мониторинга	9
2.4.1. Оснастка	10
2.4.2. Файл Конфигурации	11
2.4.3. Служба	12
2.4.4. Журнал событий КriptoПро Центр Мониторинга	13
3. Системные требования	18
4. Установка КriptoПро Центр Мониторинга	19
4.1. Установка КriptoПро Центр Мониторинга	19
4.2. Удаление КriptoПро Центр Мониторинга	21
4.3. Обновление КriptoПро Центр Мониторинга	21
4.3.1. Совместимость версий DSS и Центра Мониторинга	23
5. Настройка КriptoПро Центр Мониторинга	25
5.1. Настройка лицензии	25
5.2. Настройка экземпляров тестирования	27
5.2.1. Параметры экземпляра тестирования DSS	28
5.3. Настройка экземпляров тестов	30
5.3.1. Создание экземпляра теста из шаблона тестов	30
5.3.2. Перечень тестов и их параметров	31
5.3.3. Добавление теста к экземпляру тестирования	39
5.4. Конфигурация тестирования	41
5.4.1. Основные настройки	41
5.4.2. Настройка почтовой рассылки	43
5.4.3. Настройка мониторинга журналов	45
5.4.4. Настройка СМС-рассылки	47
5.4.5. Веб-служба	51
СВЕДЕНИЯ О РАЗРАБОТЧИКЕ	54

1. Аннотация

Настоящий документ содержит описание, а также руководство по установке, и настройке программного комплекса «КриптоПро Центр Мониторинга». Данный программный комплекс используется для мониторинга работоспособности и оперативного уведомления администраторов о выявленных сбоях, ошибках функционирования и прочих внештатных ситуациях.

Документ предназначен для системных администраторов и Администраторов СЭП «КриптоПро DSS», ПАК «КриптоПро УЦ», ПАК «Службы УЦ».

Данный документ, включая подбор и расположение иллюстраций и материалов в нём, является объектом авторских прав и охраняется в соответствии с законодательством Российской Федерации. Обладателем исключительных авторских и имущественных прав является ООО «КРИПТО-ПРО». Использование этих материалов любым способом без письменного разрешения правообладателя запрещено и может повлечь ответственность, предусмотренную законодательством РФ. Информация, приведённая в данном документе, предназначена исключительно для ознакомления и не является исчерпывающей. Состав продуктов, компонент, их функции, характеристики, версии, доступность и пр. могут быть изменены компанией ООО «КРИПТО-ПРО» без предварительного уведомления. Все указанные данные о характеристиках продуктов основаны на международных или российских стандартах и результатах тестирования, полученных в независимых тестовых или сертификационных лабораториях, либо на принятых в компании методиках. В данном документе компания ООО «КРИПТО-ПРО» не предоставляет никаких ни явных, ни подразумеваемых гарантий. Владелец товарных знаков КриптоПро, КРИПТО-ПРО, логотипов и правообладателем исключительных прав на их дизайн и использование, патентов на соответствующие продукты является ООО «КРИПТО-ПРО». Названия прочих технологий, продуктов, компаний, упоминающихся в данном документе, могут являться товарными знаками своих законных владельцев. Сведения, приведённые в данном документе, актуальны на дату его публикации. При перепечатке и использовании данных материалов либо любой их части ссылки на ООО «КРИПТО-ПРО» обязательны.

© 2000-2018, ООО «КРИПТО-ПРО» Все права защищены.

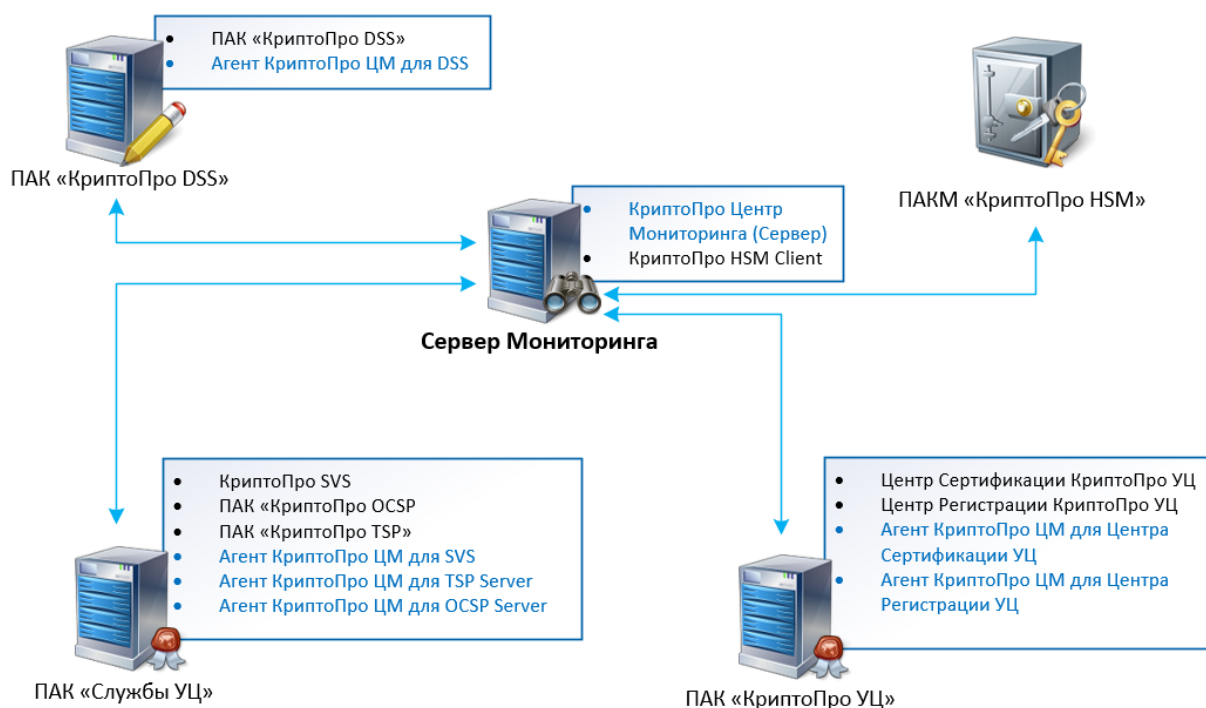
2. Общее описание КriptoПро Центр Мониторинга

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

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

- **Сервер Мониторинга** "КriptoПро Центр Мониторинга" (далее – Сервер Мониторинга)
- **Агенты** "КriptoПро Центр Мониторинга" (далее — Агенты). В настоящее время доступны следующие Агенты:
 - Агент КriptoПро Центр Мониторинга для **DSS**;
 - Агент КriptoПро Центр Мониторинга для **Центра Сертификации УЦ**;
 - Агент КriptoПро Центр Мониторинга для **Центра Регистрации УЦ**;
 - Агент КriptoПро Центр Мониторинга для **КriptoПро TSP Server**;
 - Агент КriptoПро Центр Мониторинга для **КriptoПро OCSP Server**;
 - Агент КriptoПро Центр Мониторинга для **КriptoПро SVS**.

На рисунке ниже представлена схема взаимодействия компонентов ПК «КriptoПро 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. Данная конфигурация не является единственным вариантом размещения компонентов ПК «КriptoПро Центр Мониторинга» и может быть изменена в соответствии с требованиями к inspected программно-аппаратным комплексам.



Каждый экземпляр КriptoПро 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.



Основным различием экземпляров (Сервера и Агентов) КriptoПро Центр Мониторинга является лицензия, определяющая роль экземпляра в программном комплексе. Принцип лицензирования описан в разделе 2.3.

2.1. Сервер Мониторинга «КriptoПро Центр мониторинга»

Сервер Мониторинга "КriptoПро Центр Мониторинга" выполняет следующие задачи:

- Мониторинг серверов с помощью удаленных тестов;
- Централизованный сбор информации об удаленных тестах и проверках, выполняемых Агентами «КriptoПро Центр Мониторинга»;
- Рассылка почтовых уведомлений и СМС-сообщений 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 КriptoПро Центр Мониторинга (см. раздел 2.3).

2.2. Агенты «КriptoПро Центр Мониторинга»

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

- Мониторинг серверов с помощью локальных и удаленных тестов в рамках действующей лицензии (см. раздел 2.3);
- Рассылка почтовых уведомлений и СМС-сообщений об ошибках и предупреждениях.

2.3. Лицензирование КriptoПро Центр Мониторинга



В данном разделе описаны типы лицензий для КriptoПро Центр Мониторинга, их особенности и влияние на работу программного комплекса. Процедура ввода лицензии описана в разделе 0 настоящего документа.

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 виды лицензий на КристоПро Центр Мониторинга:

Лицензия по умолчанию. Данная лицензия не имеет ограничений в работе с экземплярами тестирования и экземплярами тестов. Активируется автоматически при установке КристоПро Центр Мониторинга и действует 3 месяца с момента первого запуска оснастки. После ввода лицензии любого другого типа Лицензия по умолчанию отключается. После удаления из оснастки КристоПро Центр Мониторинга всех лицензий любого типа Лицензия по умолчанию возвращается.



Срок действия Лицензии по умолчанию отсчитывается с первого запуска оснастки 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 «КристоПро 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 КристоПро Центр Мониторинга». Данная лицензия имеет ограничения на работу с экземплярами тестирования и экземплярами тестов. При вводе заменяет Лицензию по умолчанию. В Таблица 1 указаны доступные для каждой лицензии экземпляры тестирования и тесты. Полное описание экземпляров тестирования находится в разделе 5.2, экземпляров тестов — в разделе 5.3.

Таблица 1 — Соответствие лицензий КристоПро Центр Мониторинга и доступных экземпляров тестов

Вид лицензии	Доступные экземпляры тестирования	Доступные экземпляры тестов
По умолчанию	Все	Все
КристоПро Центр Мониторинга	Все	Все
Агент КристоПро Центр Мониторинга для DSS	Нетипизированный экземпляр, DSS	Тест лицензии Сервиса Подписи DSS Тест лицензии Центра Идентификации DSS Тестовая аутентификация Тестовая подпись Тест криптопровайдеров DSS Тест конечных точек DSS Тест доступности обработчика УЦ Проверка сертификатов Веб-интерфейса DSS Проверка сертификатов Сервиса Подписи DSS

Вид лицензии	Доступные экземпляры тестирования	Доступные экземпляры тестов
		Тест подключения к базе данных Сервиса Подписи DSS Проверка сертификатов Центра Идентификации DSS Тест подключения к базе данных Центра Идентификации DSS Тест службы проверки подписи Тест TSP-службы Загрузка журналов HSM Тест указанного криптопровайдера Тест указанного сертификата Тест указанной базы данных Тест доступности указанной службы Тест доступности указанной веб-службы Тест CRL Тест срока действия CRL Тест OCSP-службы Проверка используемой оперативной памяти Проверка используемого места на диске Получение журналов Агента Мониторинга Тест состояния удаленного Агента Мониторинга Тест состояния HSM Выполнение указанного скрипта
Агент КриптоПро Центр Мониторинга для Центра Сертификации УЦ	Нетипизированный экземпляр	Тест CRL Тест срока действия CRL Тест указанного криптопровайдера Тест указанного сертификата Тест указанной базы данных Тест доступности указанной службы Тест доступности указанной веб-службы Проверка используемой оперативной памяти Проверка используемого места на диске Получение журналов Агента Мониторинга Тест состояния удаленного Агента Мониторинга Тест состояния HSM Выполнение указанного скрипта
Агент КриптоПро Центр Мониторинга	Нетипизированный экземпляр	Тест CRL Тест срока действия CRL Тест указанного криптопровайдера

Вид лицензии	Доступные экземпляры тестирования	Доступные экземпляры тестов
для Центра Регистрации УЦ		Тест указанного сертификата Тест указанной базы данных Тест доступности указанной службы Тест доступности указанной веб-службы Тестирование связи с Центром Сертификации УЦ Тест компонента ServiceBroker Центра Регистрации УЦ Проверка количества сообщений в системных очередях ЦР УЦ Тест состояния очередей Центра Регистрации УЦ Тест подключения к БД Центра Регистрации УЦ Проверка используемой оперативной памяти Проверка используемого места на диске Получение журналов Агента Мониторинга Тест состояния удаленного Агента Мониторинга Выполнение указанного скрипта
Агент КриптоПро Центр Мониторинга для OCSP Server	Нетипизированный экземпляр	Тест срока действия CRL Тест CRL Тест OCSP-службы Тест указанного сертификата Тест указанного криптопровайдера Тест указанной базы данных Тест доступности указанной службы Тест доступности указанной веб-службы Проверка используемой оперативной памяти Проверка используемого места на диске Получение журналов Агента Мониторинга Тест состояния удаленного Агента Мониторинга Выполнение указанного скрипта
Агент КриптоПро Центр Мониторинга для TSP Server	Нетипизированный экземпляр	Тест TSP-службы Тест указанного сертификата Тест указанного криптопровайдера Тест указанной базы данных Тест доступности указанной службы Тест доступности указанной веб-службы Тест CRL Проверка используемой оперативной памяти Проверка используемого места на диске Получение журналов Агента Мониторинга

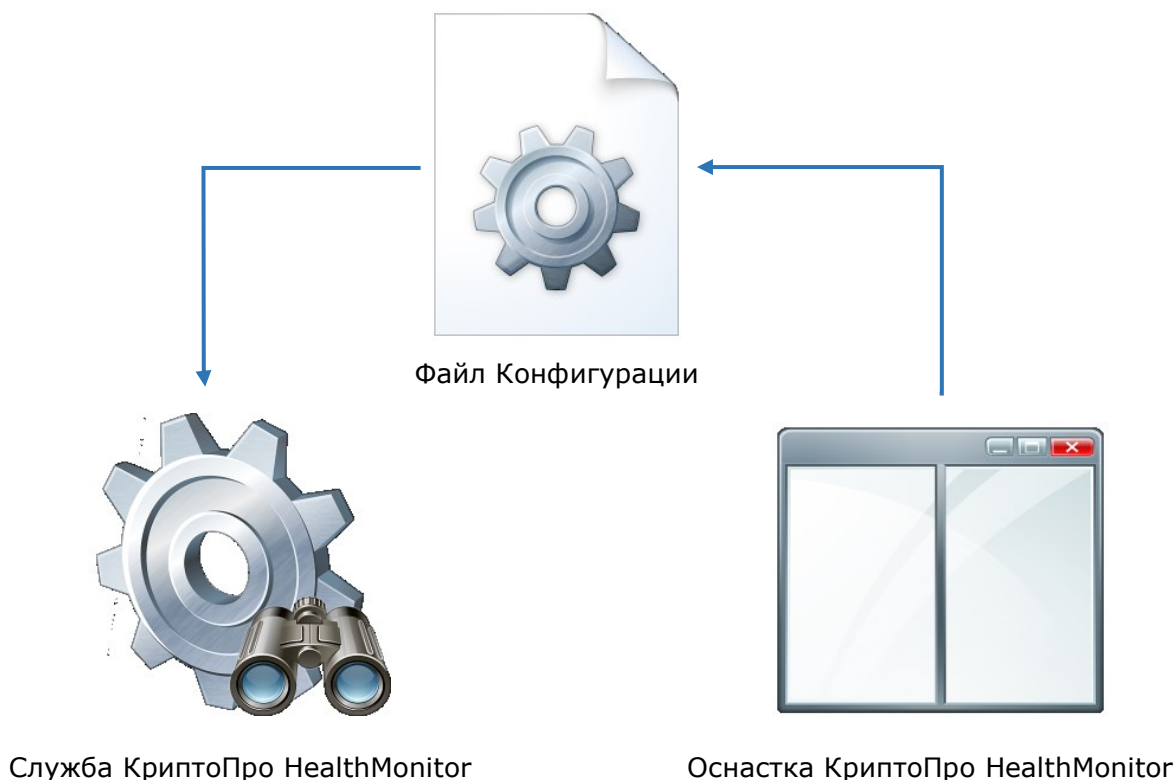
Вид лицензии	Доступные экземпляры тестирования	Доступные экземпляры тестов
		Тест состояния удаленного Агента Мониторинга Выполнение указанного скрипта
Агент КриптоПро Центр Мониторинга для SVS	Нетипизированный экземпляр	Тест CRL Тест OCSP-службы Тест указанного сертификата Тест указанного криптопровайдера Тест указанной базы данных Тест Сервиса Проверки Подписи Тест доступности указанной веб-службы Тест доступности указанной службы Проверка используемой оперативной памяти Проверка используемого места на диске Получение журналов Агента Мониторинга Тест состояния удаленного Агента Мониторинга Выполнение указанного скрипта
Агент КриптоПро Центр мониторинга для ОТА	Нетипизированный экземпляр	Тесты находятся в стадии разработки

2.4. Принцип работы КриптоПро Центр Мониторинга

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

- Оснастка КриптоПро HealthMonitor (см раздел 2.4.1);
- Файл Конфигурации (см. раздел 2.4.2);
- Служба КриптоПро HealthMonitor (см. раздел 2.4.3).

Эти компоненты связаны между собой следующим образом:



Из представленной схемы следует, что Оснастка явно не взаимодействует со Службой. Оснастка 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.



После внесения **ЛЮБЫХ** изменений внутри Оснастки необходимо перезапускать Службу, чтобы внесенные изменения отразились на последующем тестировании.

Перезапуск Службы может быть произведен при помощи системной консоли управления службами, либо через Оснастку (см. раздел 2.4.3.1).

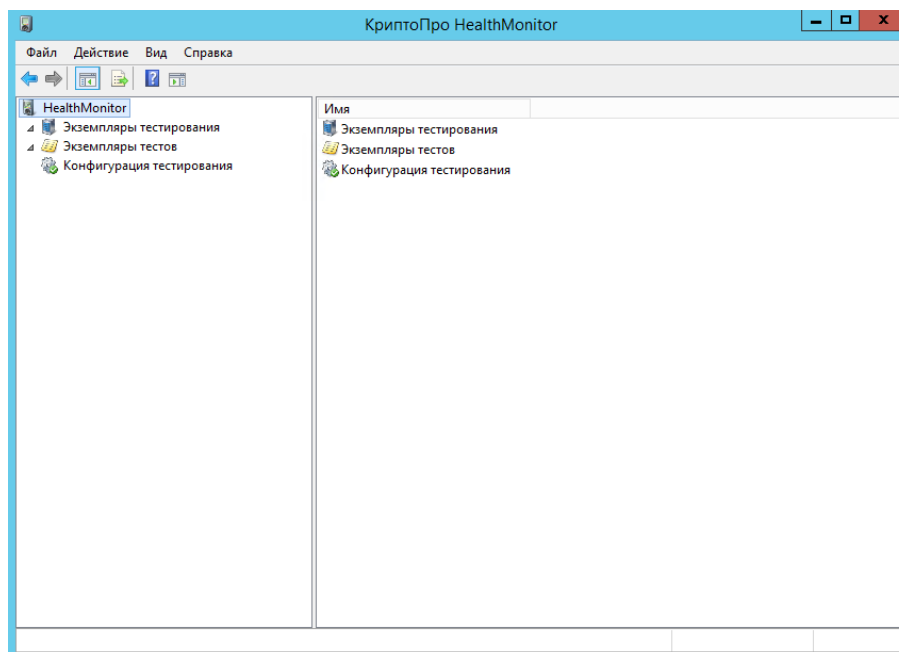
2.4.1. Оснастка

Оснастка КриптоПро Центр Мониторинга представляет собой консоль управления Microsoft (Microsoft Management Console, MMC) и позволяет управлять при помощи графического интерфейса настройками тестов и экземпляров тестирования, а также общими настройками Сервера/Агента Мониторинга.

Основное окно Оснастки состоит из следующих элементов:

- **Экземпляры тестирования** (раздел 5.2) — здесь настраиваются экземпляры систем, тестирование которых производится при помощи КриптоПро Центр Мониторинга.
- **Экземпляры тестов** (раздел 5.3) — здесь находятся тесты, созданные из шаблонов тестов (см. раздел 5.3.1) и настроенные под экземпляры тестирования.
- **Конфигурация тестирования** (раздел 5.4) — здесь располагаются общие настройки КриптоПро Центр Мониторинга.

КриптоПро Центр Мониторинга.



Для удобства настройки тестирования возможно вручную выполнить тесты (см. раздел 5.3.1) и получить результаты их выполнения непосредственно в Оснастке, однако информация о результате выполнения этих тестов не будет записана в журнал событий (см. раздел 2.4.4).

При работе с Оснасткой необходимо обращать внимание на следующее:

- При внесении ЛЮБЫХ изменений внутри Оснастки требуется сохранять их 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.
- При внесении некоторых изменений внутри Оснастки потребуется ее перезапуск. Без этого в некоторых случаях невозможно будет продолжить настройку. Предупреждение о перезапуске выводится Оснасткой автоматически в модальном окне.



Оснастка не может самостоятельно осуществлять полноценный мониторинг. Внесение изменений внутри Оснастки и их **сохранение** только производит запись в Файл Конфигурации (см. раздел 2.4.2).

2.4.2. Файл Конфигурации

Настройки экземпляра КриптоПро Центр Мониторинга сохраняются в следующие Файлы Конфигурации:

- **DefaultModeConfig.xml** — содержит сведения об экземплярах тестов и экземплярах тестирования для режима мониторинга **Default** (см. раздел 5.4.1);
- **MinModeConfig.xml** — содержит сведения об экземплярах тестов и экземплярах тестирования для режима мониторинга **Min** (см. раздел 5.4.1);
- **CryptoPro.DSS.MonitoringTool.exe.config** — содержит общие настройки экземпляра Центра Мониторинга, включая сведения о лицензии;
- **SmsConfig.xml** — содержит настройки, внесенные на этапе настройки СМС-рассылки (см. раздел 5.4.4).



Все перечисленные Файлы Конфигурации создаются и изменяются в автоматическом режиме (при внесении изменений через Оснастку) и не подлежат редактированию вручную.

Изменения, внесенные администратором КриптоПро Центр Мониторинга в Оснастке, записываются в Файл Конфигурации. Файлы Конфигурации используются при работе Службой КриптоПро HealthMonitor (см. раздел 2.4.3).



Файл Конфигурации **перезаписывается** при сохранении изменений, внесенных в настройки при работе с Оснасткой. При этом Служба мониторинга продолжает работать с версией файла, актуальной на момент ее запуска (см. раздел 2.4.3).

2.4.3. Служба

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



После того, как Файл Конфигурации был перезаписан, требуется перезапуск Службы (см. раздел 2.4.3.1), чтобы она использовала в дальнейшем тестировании новую версию Файла Конфигурации.

По умолчанию Служба запускается под пользователем «Система». Учетную запись, от которой запускается Служба, можно изменить в ее настройках в консоли управления службами **Services.msc**. В некоторых случаях Службе может не хватать прав (например, при тестировании БД какой-либо системы). Тогда в БД тестируемой системы необходимо выдать права учетной записи, под которой запускается Служба.

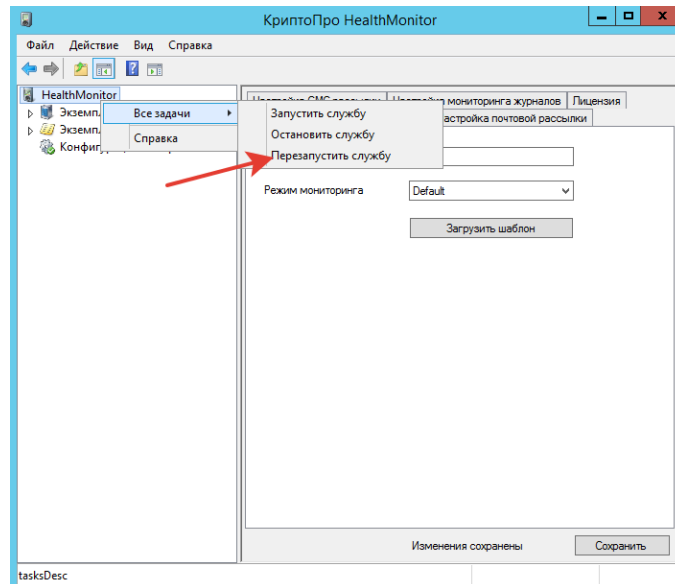
Сообщения о работе Службы «КриптоПро Health Monitor» записываются в автоматически создаваемый при установке ПК журнал событий (см. раздел 2.4.4).

2.4.3.1. Управление HealthMonitor

Службой

КриптоПро

После того, как Файл Конфигурации был перезаписан, требуется перезапуск Службы. Для перезапуска службы КриптоПро Health Monitor воспользуйтесь консолью управления службами **Services.msc**, либо нажмите правой кнопкой мыши на корневом элементе HealthMonitor в Оснастке и выберите пункты «Все задачи» - «Перезапустить службу».



Запуск Службы или ее остановка производятся также при помощи консоли управления службами **Services.msc**, либо в корневом элементе HealthMonitor в Оснастке: «Все задачи» - «Запустить службу/Остановить службу».

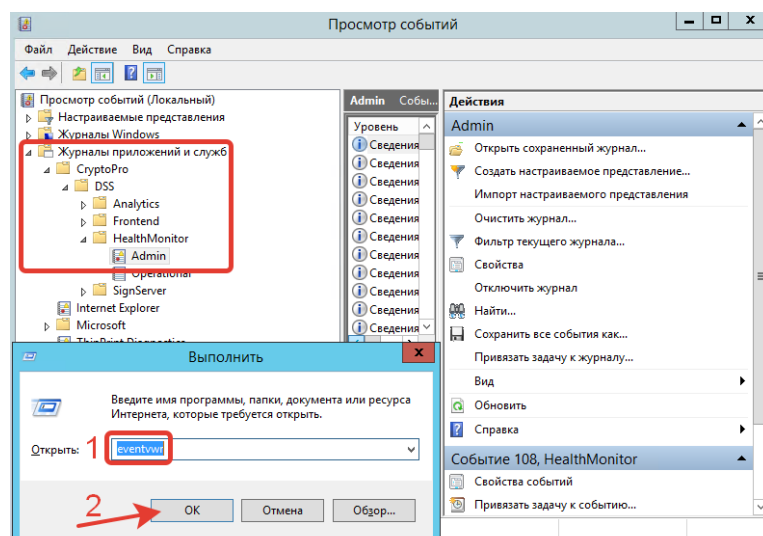
2.4.4. Журнал Мониторинга

событий

КриптоПро

Центр

Сообщения о работе Службы КриптоПро Центр Мониторинга записываются в автоматически создаваемый при установке ПК журнал событий **CryptoPro-DSS-HealthMonitor\Admin**. Запустить консоль просмотра событий можно с правами локального администратора, выполнив команду Win+R — eventvwr.



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

- группе;
- типу;
- кодам.

Каждое из событий может иметь один из трех типов, представленных в Таблица 2. Для событий типов **i** и **w** может быть настроено оповещение администратора программного комплекса по почте. Для событий всех типов (**i**, **w**, **e**) может быть настроено оповещение администратора посредством СМС-сообщений. Подробнее о настройке оповещения см. разделы 5.4.2—5.4.4.

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.
Ошибка (Error)	e	Сообщение об ошибке.

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

Таблица 3 — События журнала Центра Мониторинга

Код события	Тип события	Название
Информационные сообщения 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

Код события	Тип события	Название
109	i	Результат выполнения тестов (тесты без ошибок)
110	w	Результат выполнения тестов (одна или несколько ошибок в тестах)
111	i	Отправка отчётов успешно сконфигурирована
112	i	Веб-служба успешно сконфигурирована
113	i	Отправка отчётов по SMS успешно сконфигурирована
Ошибки работы сервиса (200-299)		
200	e	Нетипизированная ошибка
201	e	Ошибка при чтении конфигурации тестов
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
Ошибки тестов (500-599)		
500	e	Нетипизированная ошибка теста DSS 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 DSS)
504	e	Ошибка теста EndpointTest (Тест конечных точек DSS)
505	e	Ошибка теста EnrollsTest (Тест доступности обработчика УЦ)

Код события	Тип события	Название
506	e	Ошибка теста FeCertificateValidationTest (Проверка сертификатов Веб-интерфейса DSS)
507	e	Ошибка теста OcspTest (Тест доступности службы OCSP)
508	e	Ошибка теста SsCertificateValidationTest (Проверка сертификатов Сервиса Подписи DSS)
509	e	Ошибка теста SsDataBaseConnectionTest (Тест подключения к БД Сервиса Подписи DSS)
510	e	Ошибка теста StsCertificateValidationTest (Проверка сертификатов Центра Идентификации DSS)
511	e	Ошибка теста StsDataBaseConnectionTest (Тест подключения к БД сервиса Центра Идентификации DSS)
512	e	Ошибка теста SvsTest (Тест Сервиса Проверки Подписи)
513	e	Ошибка теста TspTest (Тест TSP-службы)
514	e	Ошибка теста CrITest (Тест CRL)
515	e	Ошибка теста HsmLogTest (Загрузка журналов HSM)
516	e	Ошибка теста SimpleCryptoProviderTest (Тест указанного криптопровайдера)
517	e	Ошибка теста SimpleCertificateTest (Тест указанного сертификата)
518	e	Ошибка теста SimpleDataBaseConnectionTest (Тест указанной базы данных)
519	e	Ошибка теста SimpleServiceTest (Тест указанной службы)
520	e	Ошибка теста SimpleHttpAvailabilityTest (Тест указанной веб службы)
521	e	Ошибка теста CrIVerificationTest (Тест срока действия CRL)
522	e	Ошибка теста PingCaTest (Тестирование связи с Центром Сертификации УЦ)
523	e	Ошибка теста RaServiceBrokerTest (Тест компонента Service Broker Центра Регистрации УЦ)
524	e	Ошибка теста RaQueuesOverflowTest (Проверка количества сообщений в системных очередях ЦР УЦ)
525	e	Ошибка теста RaQueuesStateTest (Тест состояния очередей Центра Регистрации УЦ)
526	e	Ошибка теста RaDataBaseConnectionTest (Тест подключения к БД Центра Регистрации УЦ)

Код события	Тип события	Название
527	e	Ошибка теста StsLicenseTest (Тест лицензий Центра Идентификации DSS)
528	e	Ошибка теста SsLicenseTest (Тест лицензий Сервиса Подписи DSS)
529	e	Ошибка теста UsedMemoryTest (Проверка используемой оперативной памяти)
530	e	Ошибка теста UsedDiskSpaceTest (Проверка используемого места на диске)
531	e	Ошибка теста GetLogsTest (Получение журналов Агента Мониторинга)
532	e	Ошибка теста HsmStatusTest (Тест состояния HSM)
533	e	Ошибка теста GetLastTestStatusTest (Тест состояния удаленного Агента Мониторинга)
534	e	Ошибка теста SimplePowershellTest (Выполнение указанного скрипта)
Предупреждения тестов (600-699)		
600	w	Нетипизированное предупреждение теста DSS (id события по умолчанию)
603	w	Предупреждение теста CryptoProviderTest (Тест криптопровайдеров DSS)
606	w	Предупреждение теста FeCertificateValidationTest (проверка сертификатов веб интерфейса DSS)
608	w	Предупреждение теста SsCertificateValidationTest (проверка сертификатов сервиса подписи DSS)
610	w	Предупреждение теста StsCertificateValidationTest (проверка сертификатов ЦИ DSS)
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 DSS)
628	w	Предупреждение теста SsLicenseTest (Тест лицензий Сервиса Подписи DSS)
631	w	Предупреждение теста GetLogsTest (Получение журналов Агента Мониторинга)
632	w	Предупреждение теста HsmStatusTest (Тест состояния HSM)

3. Системные требования

Системные требования к КriptoПро Центр Мониторинга основываются на системных требованиях, предъявляемых к СЭП «КriptoПро DSS». Полное описание системных требований к КriptoПро DSS содержится в разделе 2 документа ЖТЯИ.00096-02 92 02 КriptoПро DSS. Руководство администратора.

В случае, если Центр Мониторинга устанавливается на отдельной машине, предъявляются следующие основные требования:

- Windows Server 2008 R2/2012/2012R2 (x64)/2016;
- Microsoft .NET Framework;
- КriptoПро HSM Client (для подключения к КriptoПро HSM).



КriptoПро Центр Мониторинга не имеет собственной базы данных, хотя и может использовать тесты, которым требуется подключение к БД КriptoПро DSS или другой системы (см. разделы 2.4.3 и 0). В связи с этим, требования к СУБД в настоящем документе не предъявляются.

4. Установка КристоПро Центр Мониторинга

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

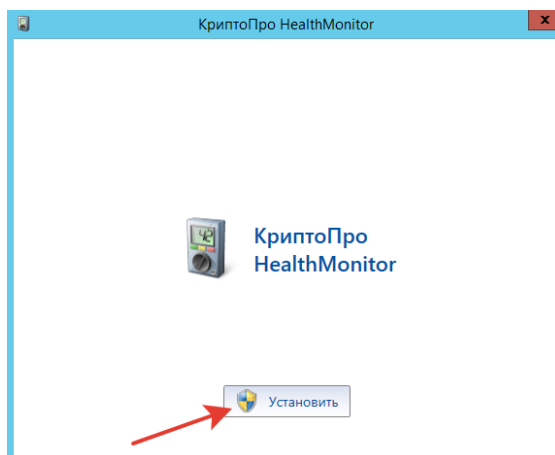
4.1. Установка КристоПро Центр Мониторинга

Для установки ПО «КристоПро Центр Мониторинга» необходимо запустить установочный файл **HealthMonitorInstall.exe**.

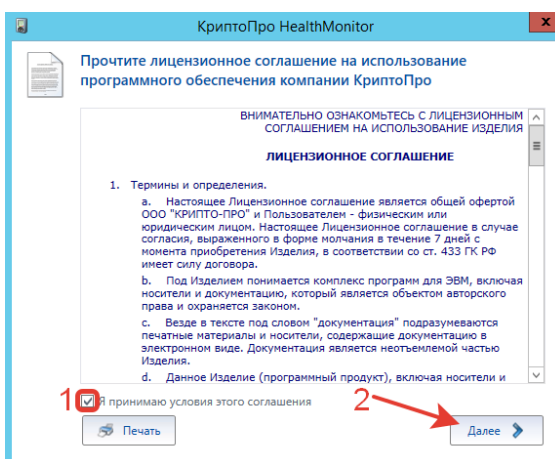


HealthMonitorInstall.exe

Откроется Мастер установки. Если запуск установочного файла производился не с правами локального администратора рабочей станции, нажмите кнопку «Установить» и подтвердите внесение изменений. В случае, если прав достаточно, после запуска Мастера установки произойдет автоматический переход к следующему этапу.



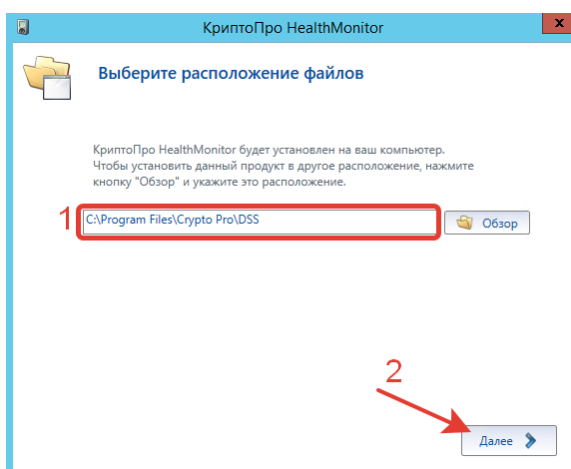
Ознакомьтесь с лицензионным соглашением. Для продолжения установки поставьте галочку «Я принимаю условия этого соглашения» и нажмите «Далее».



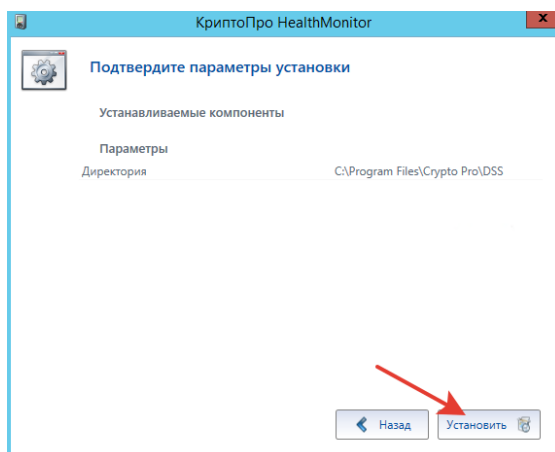
Укажите директорию, куда будет установлен КристоПро Центр Мониторинга, и нажмите «Далее».



Если данный экземпляр Центра Мониторинга разворачивается в целях мониторинга состояния СЭП «КриптоПро DSS», необходимо оставить расположение по умолчанию. В остальных случаях не имеет значения, в какую директорию будет установлен Центр Мониторинга.



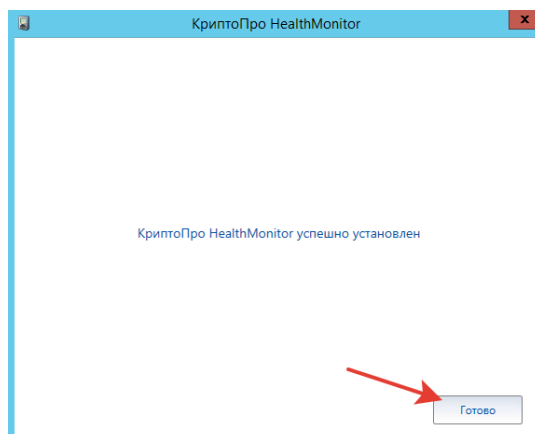
Убедитесь, что выбраны верные параметры установки и нажмите «Установить».



В случае успешной установки появится окно «КриптоПро Health Monitor успешно установлен». Для завершения работы с Мастером установки нажмите «Готово».



После установки КриптоПро Центр Мониторинга требуется перезагрузка рабочей станции.

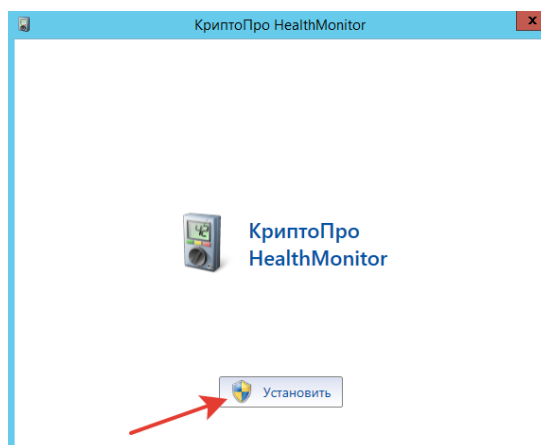


4.2. Удаление КристоПро Центр Мониторинга

Для удаления ПО «КристоПро Центр Мониторинга» необходимо запустить установочный файл **HealthMonitorInstall.exe**.



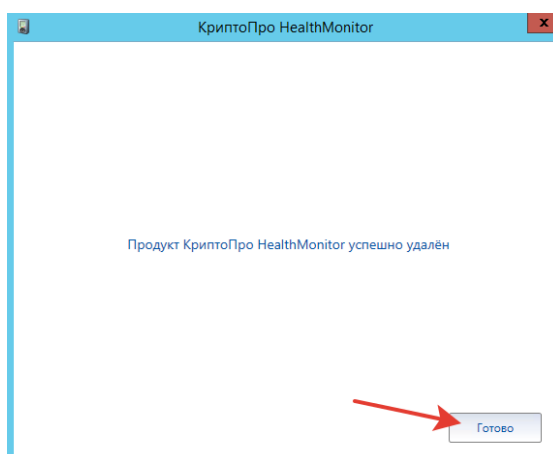
Откроется Мастер установки. Если запуск установочного файла производился не с правами локального администратора рабочей станции, нажмите кнопку «Установить» и подтвердите внесение изменений. В случае, если прав достаточно, после запуска Мастера установки произойдет автоматический переход к следующему этапу.



Удаление КристоПро Центр Мониторинга производится автоматически. В случае успешного удаления появится окно «КристоПро Health Monitor успешно удален». Для завершения работы с Мастером установки нажмите «Готово».



После удаления КристоПро Центр Мониторинга требуется перезагрузка рабочей станции.



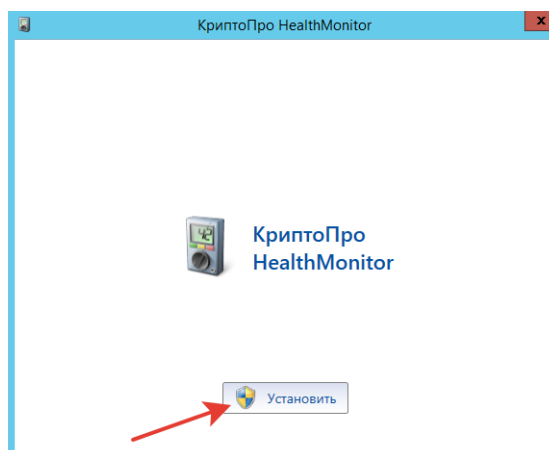
4.3. Обновление КристоПро Центр Мониторинга

Для обновления ПО «КристоПро Центр Мониторинга» необходимо запустить установочный файл **HealthMonitorInstall.exe**.

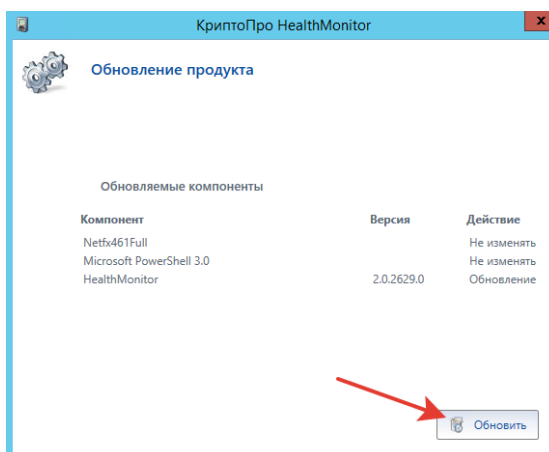


HealthMonitorInstall.exe

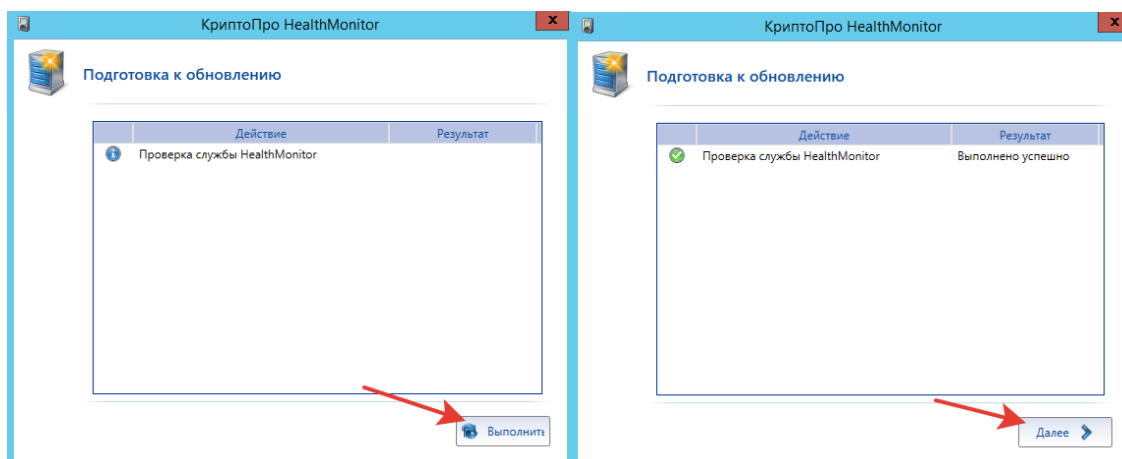
Откроется Мастер установки. Если запуск установочного файла производился не с правами локального администратора рабочей станции, нажмите кнопку «Установить» и подтвердите внесение изменений. В случае, если прав достаточно, после запуска Мастера установки произойдет автоматический переход к следующему этапу.



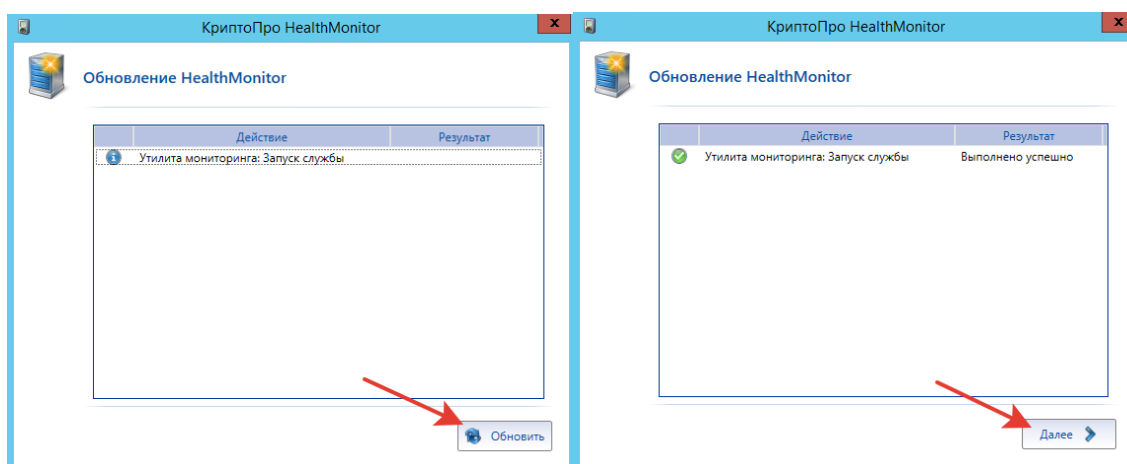
Ознакомьтесь со списком подлежащих обновлению компонентов и нажмите «Обновить».



Отобразится окно с действиями, необходимыми для подготовки к обновлению. Ознакомьтесь со списком этих действий и нажмите «Выполнить». После завершения действий по подготовке к обновлению нажмите «Далее».



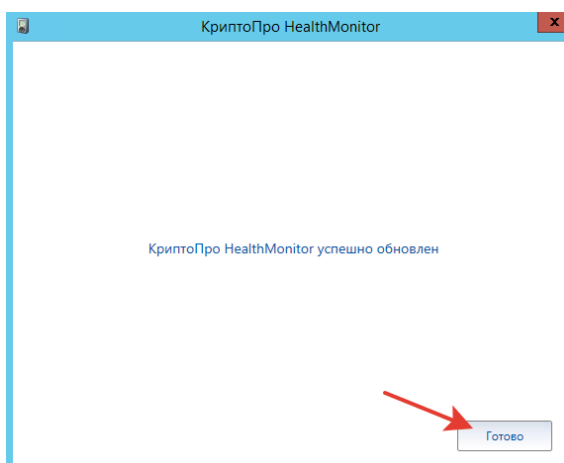
Обновление производится в автоматическом режиме. После его окончания будет предложено произвести запуск службы мониторинга. Для этого нажмите «Обновить». После запуска службы нажмите «Далее».



В случае успешного обновления появится окно «КриптоПро Health Monitor успешно обновлен». Для завершения работы с Мастером установки нажмите «Готово».



После обновления КриптоПро Центр Мониторинга требуется перезагрузка рабочей станции.



4.3.1. Совместимость версий DSS и Центра Мониторинга

При выполнении тестов, уникальных для КриптоПро DSS, Центр Мониторинга чувствителен к версии DSS. В связи с этим, при сильном расхождении версии экземпляра Центра Мониторинга и тестируемого им DSS могут оказаться неработоспособными следующие тесты:

- Тест криптопровайдеров Сервиса Подписи DSS;
- Тест доступности обработчика УЦ;
- Тест лицензии Сервиса Подписи DSS;
- Тест лицензии Центра Идентификации DSS;
- Проверка сертификатов Веб-интерфейса DSS;
- Проверка сертификатов Сервиса Подписи DSS;
- Проверка сертификатов Центра Идентификации DSS;
- Тест подключения к базе данных Сервиса Подписи DSS;

- Тест подключения к базе данных Центра Идентификации DSS.



Следующие настройки необходимо выполнять только в случае неработоспособности перечисленных тестов (при условии, что они работали корректно ранее).

При обновлении экземпляра КриптоПро Центр Мониторинга в директории **<Путь установки> \Crypto Pro\DSS\HealthMonitor** автоматически создается папка **Tests**, содержащая файл **CryptoPro.DSS.MonitoringTool.DssDependantTests.dll** и папки с бэкапом(-ми) этого файла из предыдущих версий Центра Мониторинга. Папки имеют названия, соответствующие старой версии Центра Мониторинга (и КриптоПро DSS).

Пример:

 2.0.2665.0

 CryptoPro.DSS.MonitoringTool.DssDependantTests.dll

Для восстановления работоспособности перечисленных выше тестов **СКОПИРУЙТЕ С ЗАМЕНОЙ** файл **CryptoPro.DSS.MonitoringTool.DssDependantTests.dll** из папки с именем, соответствующим Вашей версии КриптоПро DSS, в папку **<Путь установки> \Crypto Pro\DSS\HealthMonitor\Tests**.

5. Настройка КriptoПро Центр Мониторинга

Настройка КriptoПро Центр Мониторинга состоит из трех основных разделов:

- **Экземпляры тестирования** (раздел 5.2) — здесь настраиваются экземпляры систем, тестирование которых производится при помощи КriptoПро Центр Мониторинга.
- **Экземпляры тестов** (раздел 5.3) — здесь находятся тесты, полученные из шаблонов и специально настроенные под экземпляры тестирования.
- **Конфигурация тестирования** (раздел 5.4) — здесь располагаются общие настройки КriptoПро Центр Мониторинга.

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

1. Настройка лицензии (см. раздел 5.1).
2. Основные настройки (см. раздел 5.4.1).
3. Настройка экземпляров тестирования (см. раздел 5.2).
4. Настройка экземпляров тестов (см. раздел 5.3.1).
5. Добавление тестов к экземпляру тестирования (см. раздел 5.3.2.1).
6. Настройка оповещения (см. разделы 5.4.2—5.4.3).
7. Дополнительные настройки (см. разделы 5.4.3—0).

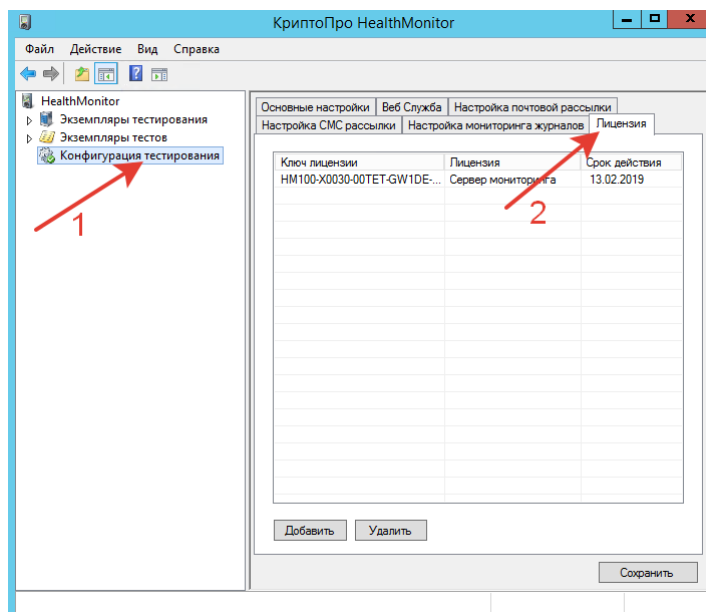


Все указанные настройки могут изменяться/дополняться вместе с новыми версиями КriptoПро Центр Мониторинга.

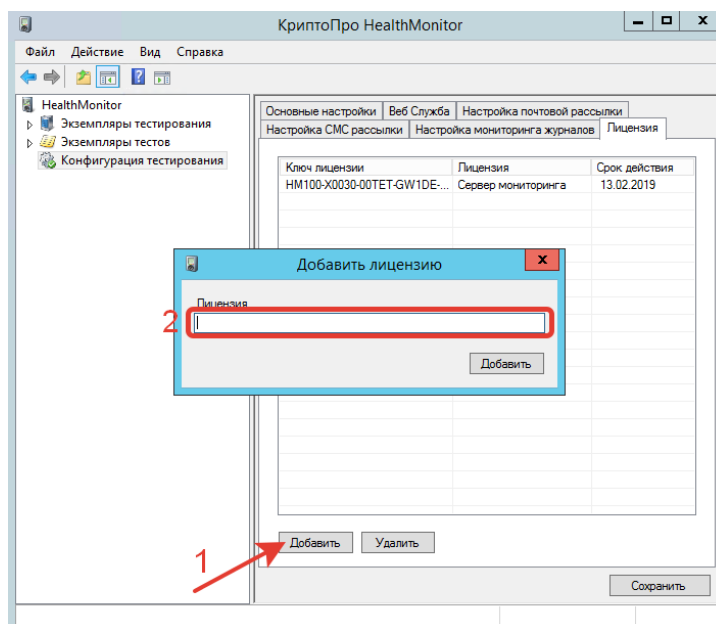
5.1. Настройка лицензии

Настройка лицензии для КriptoПро Центр Мониторинга относится к разделу «Конфигурация тестирования», но приводится в начале настройки, так как лицензия определенного типа необходима для дальнейшей работы с программным комплексом.

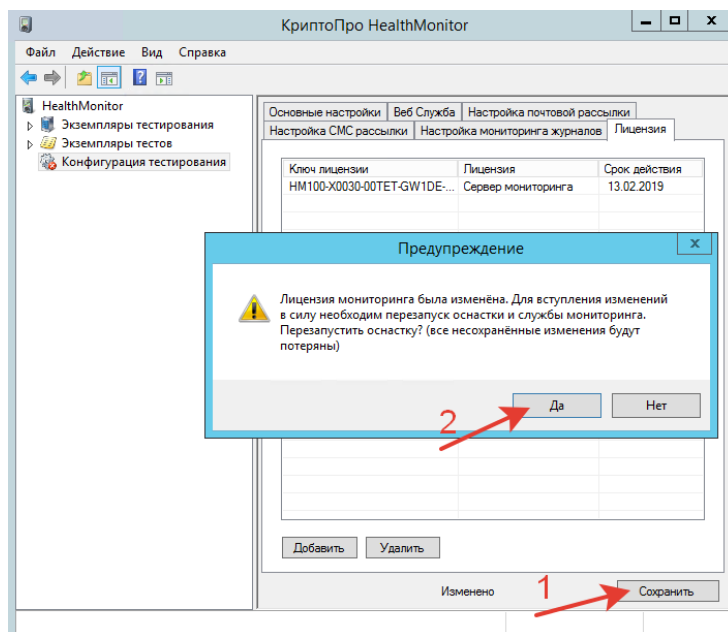
Ввод лицензии одинаков как для Сервера Мониторинга, так и для любого из Агентов Мониторинга. Для ввода лицензии запустите оснастку КriptoПро Центр Мониторинга (cp.dss.ru.msc), либо добавьте оснастку «Управление КriptoПро HealthMonitor» в консоли управления (ММС), и перейдите к разделу «Конфигурация тестирования». Перейдите на вкладку «Лицензия» в правой части оснастки.



Для добавления новой лицензии нажмите кнопку «Добавить» и введите лицензионный ключ в появившемся окне.



Обязательно сохраните конфигурацию путем нажатия кнопки «Сохранить». Потребуется перезапуск оснастки, для чего нажмите кнопку «Да» в появившемся окне с предупреждением. Оснастка автоматически перезапустится.



Обязательно перезапустите службу **КриптоПро Health Monitor** при помощи системной консоли управления службами, либо через оснастку (см. раздел 2.4.2). после чего можно начинать работу.

5.2. Настройка экземпляров тестирования

В настоящее время в КриптоПро Центр Мониторинга доступны для тестирования два типа экземпляров:

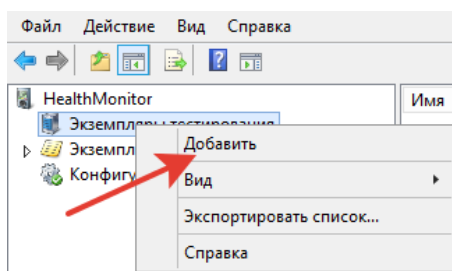
- DSS;
- Нетипизированный экземпляр.

Для экземпляра DSS в КриптоПро Центр Мониторинга доступны дополнительные настройки (см. раздел 5.2.1), в то время как для нетипизированного экземпляра какие-либо дополнительные настройки отсутствуют.

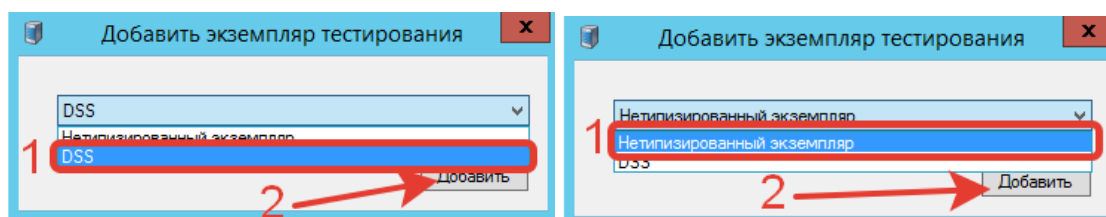


Экземпляр тестирования необязательно соответствует однозначно инспектируемой системе. Экземпляр тестирования означает определенный набор тестов и (в случае с экземпляром типа DSS) набор настроек.

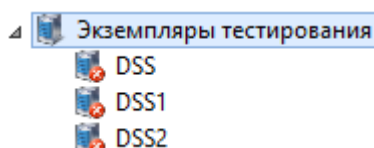
Перед созданием экземпляра тестирования убедитесь, что выбран правильный режим работы КриптоПро Центр Мониторинга (Default или Min, см. раздел 5.4.1). Для добавления нового экземпляра тестирования нажмите правой кнопкой мыши на раздел «Экземпляры тестирования» и выберите «Добавить».



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



Новый экземпляр будет отображаться в разделе «Экземпляры тестирования». Имя созданного экземпляра тестирования 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 **DSS** 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: DSS, DSS1, DSS2...).



После добавления экземпляра необходимо добавить тесты, которые для него будут выполняться (см. раздел 5.3.2.1). Для экземпляра тестирования типа DSS необходимо выполнить ряд настроек, описанных в разделе 5.2.1.

Для копирования экземпляра тестирования нажмите на него правой кнопкой мыши и выберите «Копировать». Будет добавлен новый экземпляр тестирования с идентичными настройками, однако к его имени в конце добавится номер по порядку (см. выше).

Для удаления экземпляра тестирования нажмите на него правой кнопкой мыши и выберите «Удалить». **Внимание:** удаление экземпляра тестирования не требует подтверждения.

5.2.1. Параметры экземпляра тестирования DSS

Для задания параметров экземпляра тестирования DSS в разделе «Экземпляры тестирования» выберите созданный ранее экземпляра типа DSS (1) и перейдите на вкладку «Параметры DSS» (2). Заполните предложенные поля на вкладке «Параметры DSS» и нажмите кнопку «Сохранить конфигурацию» (3). Описание параметров DSS представлено в Таблица 4.



Обратите внимание на значок около имени экземпляра тестирования. Когда в конфигурацию экземпляра вносятся изменения, около него появляется значок . Сохранение конфигурации приводит экземпляр в готовое к тестированию состояние, о чем свидетельствует значок .

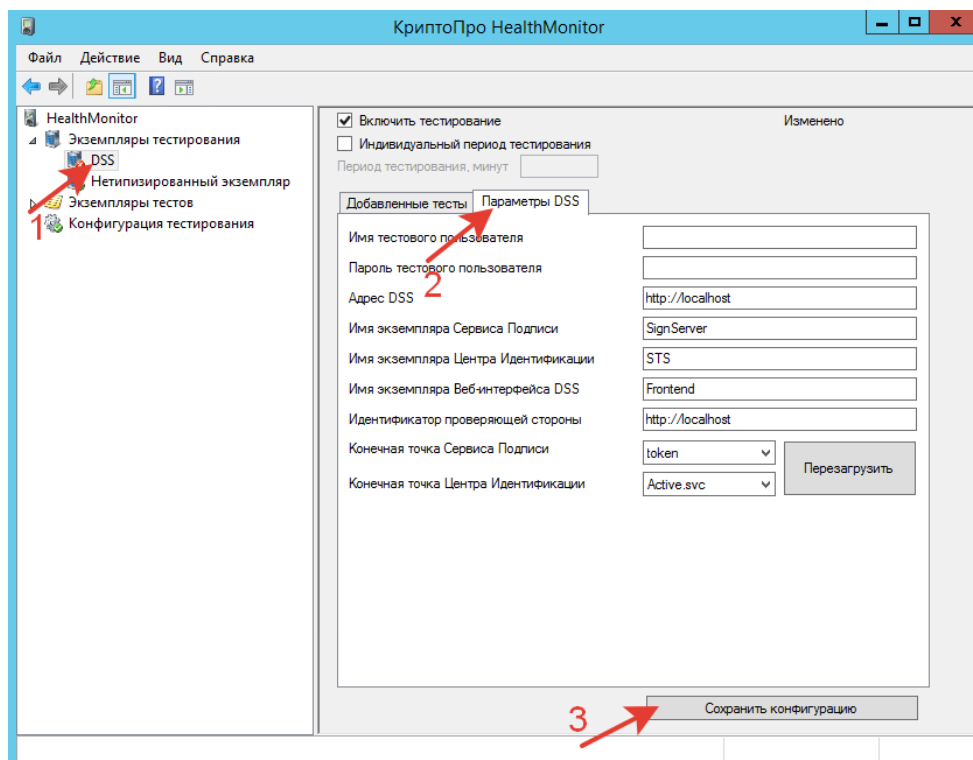


Таблица 4 — Параметры DSS

Параметр	Описание
Имя тестового пользователя	Логин Пользователя на Центре Идентификации DSS. Внимание: для данного Пользователя должна быть настроена аутентификация по логину и паролю или только идентификация.
Пароль тестового пользователя	Пароль Пользователя на Центре Идентификации DSS. Если для Пользователя назначен метод входа «Только идентификация», данное поле можно оставить пустым.
Адрес DSS	Адрес сервера, на котором расположен Сервис Подписи ПAK «КриптоПро DSS». Значение по умолчанию — http://localhost. Внимание: для тестирования все компоненты DSS должны быть развернуты на одном сервере.
Имя экземпляра Сервиса Подписи	Соответствует имени экземпляра Сервиса Подписи DSS, который нужно протестировать. Получить значение можно при помощи командлета Get-DssProperties.
Имя экземпляра ЦИ	Соответствует имени экземпляра Центра Идентификации DSS, который нужно протестировать. Получить значение можно при помощи командлета Get-DssStsProperties.
Имя экземпляра Веб-интерфейса DSS	Соответствует имени экземпляра Веб-интерфейса DSS, который нужно протестировать. Получить значение можно при помощи командлета Get-DssFeProperties.
Идентификатор проверяющей стороны	Идентификатор Сервиса Подписи как проверяющей стороны. Представляет собой URI формата urn:cryptopro:dss:signserver:<Имя приложения Сервиса

Параметр	Описание
	Подписи>. Получить значение можно при помощи командлета Get-DssRelyingPartyTrust.
Конечная точка Сервиса Подписи*	Нажмите кнопку «Перезагрузить», чтобы получить список доступных конечных точек. Поле используется для теста подписи. Для успешного тестирования необходимо выбрать конечную точку, соответствующую выбранному протоколу взаимодействия Центра Мониторинга и DSS (https или http)*.
Конечная точка Центра Идентификации**	Нажмите кнопку «Перезагрузить», чтобы получить список доступных конечных точек. Поле используется для теста аутентификации. Для успешного тестирования необходимо выбрать конечную точку, соответствующую выбранному протоколу взаимодействия Центра Мониторинга и DSS (https или http)**.

*Рекомендуется использовать конечную точку **Issuedtoken/transport/nosc**. Для этого в адресе DSS должно быть записано имя узла с DSS точно так же, как в сертификате его веб-сервера. Если нет возможности указать имя узла, используйте конечную точку **issuedtoken/nosc**.

Рекомендуется при аутентификации с использованием протокола TLS выбирать конечную точку **username/transport, без TLS — **active.svc**.



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

5.3. Настройка экземпляров тестов

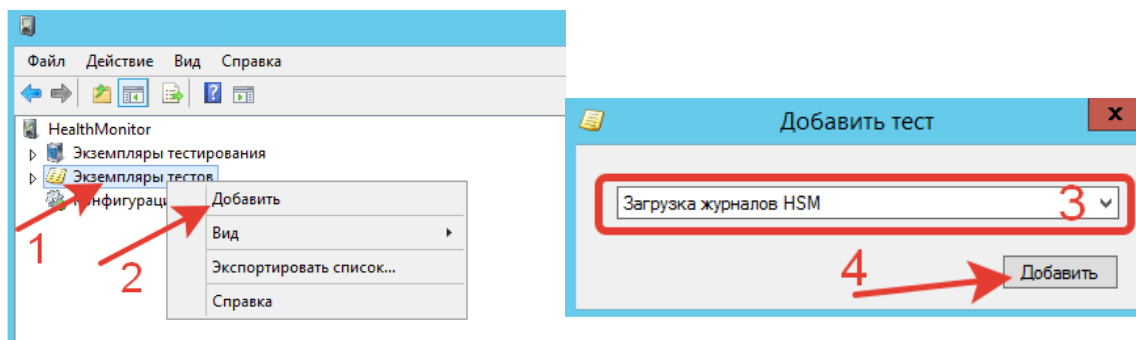
Экземпляром теста в КriptoПро Центр Мониторинга называется тест, созданный из шаблона теста, и настроенный (при наличии настроек).

- Создание тестов из шаблона описано в разделе 5.3.1.
- Описание всех тестов и их параметров дано в разделе 5.3.2.
- Добавление тестов к экземпляру тестирования описано в разделе 5.3.2.1.

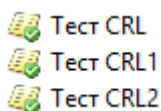
5.3.1. Создание экземпляра теста из шаблона тестов

Перед созданием экземпляра теста убедитесь, что лицензия на определенный экземпляр Центра Мониторинга введена (см. разделы 2.3, 5.1) и выбран правильный режим работы КriptoПро Центр Мониторинга (Default или Min, см. раздел 5.4.1).

Чтобы добавить экземпляр теста из шаблона, нажмите правой кнопкой мыши на раздел «Экземпляры тестов» (1) и выберите «Добавить» (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 CRL, Тест CRL1, Тест CRL2...).



Выполните настройку добавленных тестов. Параметры тестов описаны в разделе 5.3.2.



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



Обратите внимание на значок около имени экземпляра теста. Когда в параметры теста вносятся изменения, около него появляется значок . Сохранение конфигурации приводит тест в готовое к тестированию состояние, о чем свидетельствует значок .

Для копирования экземпляра теста нажмите на него правой кнопкой мыши и выберите «Копировать». Будет добавлен новый экземпляр теста с идентичными настройками, однако к его имени в конце добавится номер по порядку (см. выше).

Для удаления экземпляра теста нажмите на него правой кнопкой мыши и выберите «Удалить». **Внимание:** удаление экземпляра теста не требует подтверждения.

5.3.2. Перечень тестов и их параметров

В Таблица 5 приводится описание всех доступных в КриптоПро Центр Мониторинга тестов, а также их параметров.

Таблица 5 — Описание тестов

Тест	Описание	Параметры	Min режим
Выполнение указанного скрипта	Тест выполняет указанный powershell скрипт. При указании пути необходимо указать полный путь к скрипту. Тест завершается успешно,	➤ Путь к файлу скрипта	+

Тест	Описание	Параметры	Min режим
	если указанный скрипт завершился без исключения.		
Загрузка журналов HSM	При исполнении теста выполняется загрузка журнала аудита и журнала событий HSM. 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. Подробнее особенности теста см. раздел 5.3.2.1.	➤ Адрес HSM; ➤ Версия HSM (HSM 1.0/ HSM 2.0) ➤ Отпечаток сертификата аудитора HSM ➤ Период тестирования <количество> 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 настройке мониторинга журналов в разделе 5.4.3)	+
Проверка используемой оперативной памяти	Тест выполняет проверку доли используемой оперативной памяти и выдаёт ошибку при превышении заданного порога. Порог предупреждения задаётся в процентах.	➤ Предупреждать при превышении – доля используемой оперативной памяти в процентах	+
Проверка используемого места на диске	Тест выполняет проверку доли используемого места на указанном диске и выдаёт ошибку при превышении заданного порога. Порог предупреждения задаётся в процентах.	➤ Выбор диска – выбор локального диска, на котором производится мониторинг ➤ Предупреждать при превышении – доля используемого места в процентах	+
Проверка количества сообщений в системных очередях ЦР УЦ	Тест проверяет количество сообщений в очередях Центра Регистрации УЦ. Если количество сообщений в какой либо очереди превышает заданное значение, тест завершается с ошибкой.	➤ Максимально допустимое количество сообщений в очереди	-
Проверка сертификатов Веб-интерфейса DSS	Тест выполняет проверку сертификатов Веб-интерфейса DSS. В список проверяемых сертификатов входит: сертификат Веб-интерфейса Пользователя, TLS-сертификат сервера приложений (IIS), сертификаты доверенных издателей маркеров безопасности. 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.	TLS-сертификат ➤ Проверка срока действия (чекбокс) ➤ Проверка периода действия закрытого ключа (чекбокс) ➤ Проверять отзывы сертификата (чекбокс) Сервисный сертификат ➤ Проверка срока действия (чекбокс) ➤ Проверка периода действия закрытого ключа (чекбокс) ➤ Проверять отзывы сертификата (чекбокс) Проверка сертификатов доверенных издателей ➤ Проверка срока действия (чекбокс)	-

Тест	Описание	Параметры	Min режим
		➤Проверка периода действия закрытого ключа (чекбокс) ➤Проверять отзыв сертификата (чекбокс) ➤Сообщать об истечении за <количество> часов/дней/месяцев/лет	
Проверка сертификатов Сервиса Подписи DSS	Тест выполняет проверку сертификатов Сервиса Подписи DSS. В список проверяемых сертификатов входит: сертификат Сервиса Подписи, TLS-сертификат сервера приложений (IIS), сертификаты обработчиков УЦ, сертификат ключа доступа к ПАКМ «КриптоПро HSM», сертификаты доверенных издателей маркеров безопасности. 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.	TLS-сертификат ➤Проверка срока действия (чекбокс) ➤Проверка периода действия закрытого ключа (чекбокс) ➤Проверять отзыв сертификата (чекбокс) Сервисный сертификат ➤Проверка срока действия (чекбокс) ➤Проверка периода действия закрытого ключа (чекбокс) ➤Проверять отзыв сертификата (чекбокс) Проверка сертификатов доверенных издателей ➤Проверка срока действия (чекбокс) ➤Проверка периода действия закрытого ключа (чекбокс) ➤Проверять отзыв сертификата (чекбокс) Проверка сертификатов операторов УЦ ➤Проверка срока действия (чекбокс) ➤Проверка периода действия закрытого ключа (чекбокс) ➤Проверять отзыв сертификата (чекбокс) ➤Сообщать об истечении за <количество> часов/дней/месяцев/лет	
Проверка сертификатов Центра Идентификации DSS	Тест выполняет проверку сертификатов Центра Идентификации DSS. В список проверяемых сертификатов входит: сертификат Центра Идентификации, TLS-сертификат сервера приложений (IIS), сертификаты проверяющих сторон, сертификаты доверенных издателей маркеров безопасности. 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.	TLS-сертификат ➤Проверка срока действия (чекбокс) ➤Проверка периода действия закрытого ключа (чекбокс) ➤Проверять отзыв сертификата (чекбокс) Сервисный сертификат ➤Проверка срока действия (чекбокс) ➤Проверка периода действия закрытого ключа (чекбокс)	

Тест	Описание	Параметры	Min режим
		➤Проверять отзыв сертификата (чекбокс) Проверка сертификатов доверенных издателей ➤Проверка срока действия (чекбокс) ➤Проверка периода действия закрытого ключа (чекбокс) ➤Проверять отзыв сертификата (чекбокс) Проверка сертификатов проверяющих сторон ➤Проверка срока действия (чекбокс) ➤Проверка периода действия закрытого ключа (чекбокс) ➤Проверять отзыв сертификата (чекбокс) ➤Сообщать об истечении за <количество> часов/дней/месяцев/лет	
Тест CRL	Тест проверяет доступность точки распространения списков отзыва сертификатов (COC). Проверяется только сетевая доступность точки. Если требуется проверять доступность нескольких COC, то необходимо создать несколько экземпляров данного теста.	➤Адрес точки распространения COC	+
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.	➤Имя хранилища сертификатов (Подгружается автоматически) ➤Расположение хранилища сертификатов (Current User/Local Machine) ➤Отпечаток сертификата (подгружается автоматически в зависимости от выбранного хранилища) ➤Адрес OCSP-службы	+
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.	➤Адрес TSP-службы ➤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)	+
Тест доступности обработчика УЦ	Тест проверяет доступность обработчика Удостоверяющего Центра. Идентификатор обработчика УЦ можно получить при помощи командлета Get-DssEnrollment. Если требуется проверить доступность нескольких	➤ID обработчика УЦ (в БД Сервиса Подписи DSS)	-

Тест	Описание	Параметры	Min режим
	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. Внимание: У Пользователя DSS должен быть хотя бы один действительный сертификат и настроена аутентификация в DSS по логину/паролю или только идентификация.		
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 удаленных проверок Агентов Мониторинга (см. раздел 0).	➤Адрес службы	+
Тест компонента ServiceBroker Центра Регистрации УЦ	Тест проверяет состояние компонента Service Broker Центра Регистрации УЦ. Если компонент активирован, тест завершается успешно.	-	-
Тест конечных точек DSS	Тест проверяет доступность служб некоторых экземпляров DSS. Тест выполняет загрузку метаданных Сервиса Подписи и Центра Идентификации, тем самым проверяя сетевую доступность служб и активацию служб.	-	+
Тест криптопровайдеров Сервиса Подписи DSS	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 <количество> часов/дней/месяцев/лет	-
Тест лицензии Сервиса Подписи DSS	Тест проверяет количество и сроки действия лицензий Сервиса Подписи DSS. Необходимо указать сроки предупреждения об её истечении. Если необходимо тестировать лицензии нескольких типов, нужно создать несколько экземпляров данного теста.	➤Сообщать об истечении срока действия за <количество> часов/дней/месяцев/лет ➤Сообщать об окончании числа доступных пользователей за <количество> пользователей	-
Тест лицензии Центра Идентификации DSS	Тест проверяет количество и сроки действия лицензий Центра Идентификации DSS. Необходимо указать в параметрах теста тип тестируемой лицензии и сроки предупреждения об её истечении. Если необходимо тестировать лицензии нескольких типов, нужно создать несколько экземпляров данного теста.	➤Тип лицензии (CloudCSP/MobileAuth/SimAuth) ➤Сообщать об истечении срока действия за <количество> часов/дней/месяцев/лет ➤Сообщать об окончании числа доступных пользователей за <количество> пользователей	-
Тест подключения	Тест проверяет доступность БД Сервиса Подписи DSS. Строка подключения к SQL-	-	-

Тест	Описание	Параметры	Min режим
к БД Сервиса Подписи DSS	серверу заполняется автоматически из настроек экземпляра Сервиса Подписи. Если используется Windows-аутентификация, то подключение к SQL-серверу будет осуществляться с учётными данными службы HealthMonitor. Если используется SQL-аутентификация, подключение к SQL-серверу будет осуществляться с учётными данными, указанными в строке подключения.		
Тест подключения к БД Центра Идентификации DSS	Тест проверяет доступность БД Центра Идентификации DSS. Строка подключения к SQL-серверу заполняется автоматически из настроек экземпляра Центра Идентификации. 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.	-	-
Тест подключения к БД Центра Регистрации УЦ	Тест проверяет доступность БД Центра Регистрации УЦ. Строка подключения к SQL-серверу заполняется автоматически из настроек Центра Регистрации. 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.	-	-
Тест Сервиса Проверки Подписи	Тест проверяет доступность Сервиса Проверки Подписи (SVS). Проверяется только сетевая доступность сервиса. Если требуется проверить доступность нескольких SVS, то необходимо создать несколько экземпляров данного теста.	➤Адрес SVS	+
Тест состояния HSM	Тест получает текущие 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 состояния очередей ЦР УЦ	Тест проверяет доступность системных очередей Центра Регистрации УЦ. Если одна из очередей не принимает сообщения, тест завершается с ошибкой.	-	-
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 протестировать несколько экземпляров тестирования или агентов - необходимо создать несколько экземпляров теста.	➤Адрес веб-службы агента мониторинга ➤Имя экземпляра тестирования (на агенте мониторинга)	+

Тест	Описание	Параметры	Min режим
Тест срока 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.	➤ Тип источника CRL (URL/Папка/Хранилище сертификатов) ➤ Путь к CRL ➤ Имя издателя	+
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.	➤ Имя криптопровайдера (текстовое) ➤ Тип криптопровайдера (число)	+
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.	➤ Имя хранилища сертификатов (Подгружается автоматически) ➤ Расположение хранилища сертификатов (Current User/Local Machine) ➤ Отпечаток сертификата (подгружается автоматически в зависимости от выбранного хранилища) ➤ Проверять период действия закрытого ключа (чекбокс) ➤ Проверять отзыв сертификата (чекбокс) ➤ Сообщать об истечении за <количество> часов/дней/месяцев/лет	+
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.	➤ Строка подключения к БД	+
Тест указанной службы	Тест проверяет статус указанной локальной службы. Если состояние службы отличается от «Выполняется», тест завершается с ошибкой.	➤ Имя локальной Windows-службы	+
Тестирование связи с Центром Сертификации и УЦ	Тест проверяет связь Центра Регистрации с Центром Сертификации. Если связь присутствует, но Центр Сертификации не может выпускать сертификаты, выводится предупреждение. Если связь отсутствует, тест завершается с ошибкой. Если имя ЦС не было задано, будет использовано значение по умолчанию.	➤ Имя Центра Сертификации УЦ	-

Тест	Описание	Параметры	Min режим
Тестовая аутентификация	Тест аутентификации. Для выполнения теста необходимо настроить подключение к Центру Идентификации DSS (в параметрах экземпляра тестирования DSS); задать учётные данные (логин/пароль) Пользователя, от имени которого будет произведена аутентификация. Тест использует учётные данные пользователя ЦИ, для которого настроена аутентификация по логину/паролю или только идентификация.	-	+
Тестовая подпись	Тест создания подписи. Тест проверяет корректность выполнения операций в DSS по созданию электронных подписей следующих форматов: 1. Усовершенствованная подпись (CMS Advanced Electronic Signatures, CAdES); 2. XML Digital Signature (XMLDSig); 3. Электронная подпись ГОСТ 34.10–2001, ГОСТ 34.10–2012; 4. Подпись документов формата PDF; 5. Подпись документов Microsoft Office; 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.	➤ Тип подписи (XMLDSig/GOST3410/CAdES/PDF/MSOffice/CMS) ➤ Параметры подписи Для XMLDSig: - Enveloped - Enveloping - подпись по шаблону ГОСТ 34.10-2001 и ГОСТ 34.11–94 - подпись по шаблону ГОСТ 34.10-2012 с длиной хэш-кода 256 бит - подпись по шаблону ГОСТ 34.10-2012 с длиной хэш-кода 512 бит Для CAdES: - CAdES-BES - CAdES-T - CAdES-X Long Type 1 Для PDF: - CMS - CAdES-T - CAdES-X Long Type 1 ➤ Адрес TSP-службы (только для CAdES-T и CAdES XLT1) ➤ Идентификатор сертификата	+

5.3.2.1. Особенности теста «Загрузка журналов HSM»

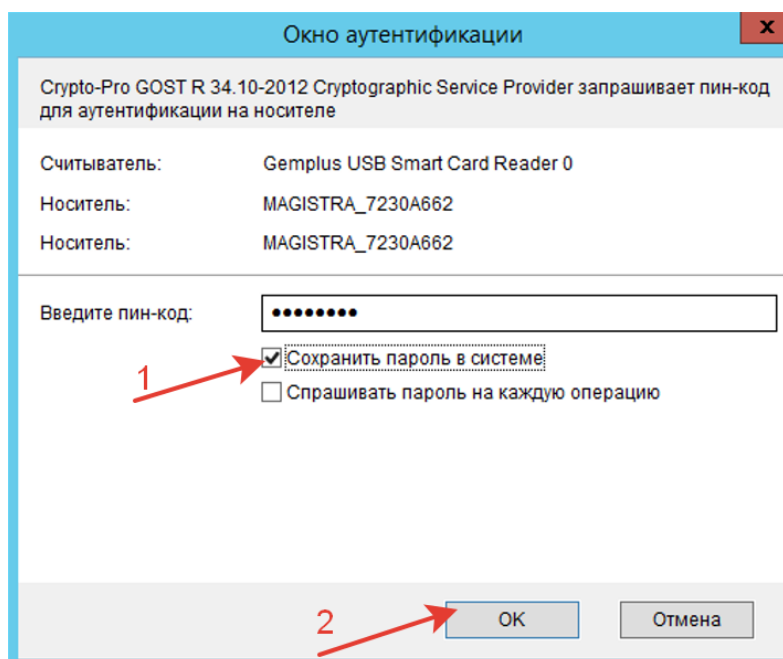


Тест не проверяет журналы HSM на наличие ошибок, а только выгружает их.

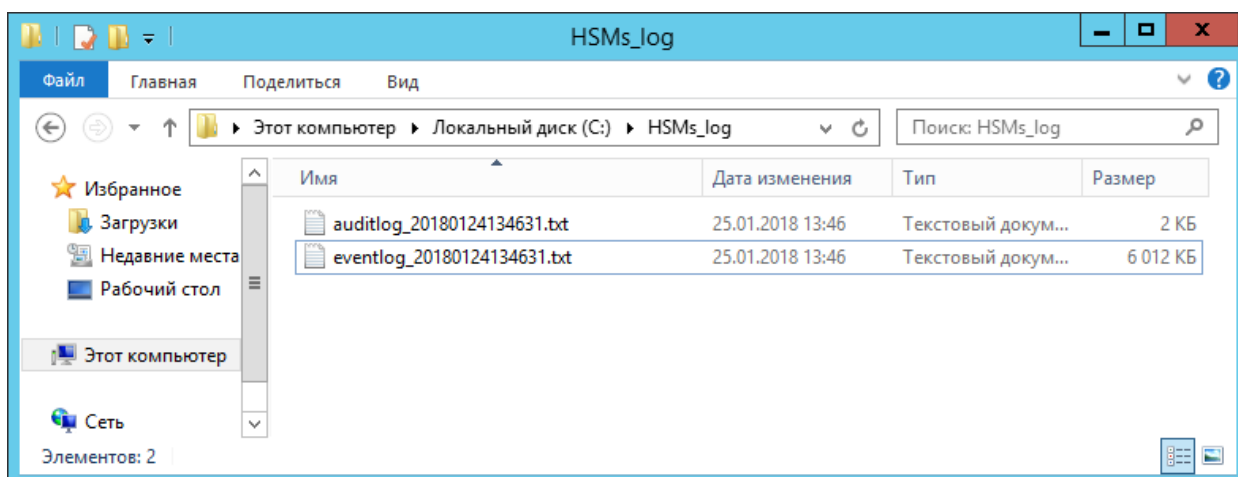
Для корректной работы теста необходим соответствующий сертификат доступа к HSM — **сертификат Аудитора**. Только привилегированный пользователь с правами Аудитора имеет возможность просмотра и выгрузки журналов аудита и событий HSM. Сертификат привилегированного пользователя с правами Аудитор HSM должен быть установлен в хранилище локального компьютера с привязкой к закрытому ключу.

Подробное описание по созданию привилегированных пользователей в ПАКМ HSM описано в документе ЖТЯИ.00046-02 91 01 КриптоПро HSM. Инструкция по использованию.

Важной особенностью теста является необходимость сохранить пароль в системе для того, чтобы последующие выполнения теста происходили автоматически. Для этого создайте и настройте экземпляр теста «Загрузка журналов HSM» (см. раздел 5.3.1), добавьте его к экземпляру тестирования (см. раздел 5.3.3), сохраните конфигурацию и запустите тест вручную при помощи кнопки «Запустить тесты». В процессе выполнения теста потребуется в появившемся окне установить чекбокс «Сохранить пароль в системе» (1) и нажать кнопку «ОК» (2) для продолжения. Если тест завершится успешно, в последующих тестированиях он будет выполняться автоматически.



Если все настройки заданы верно, после выполнения теста в указанной папке появятся файлы **auditlog_<дата и время>** и **eventlog_<дата и время>**.

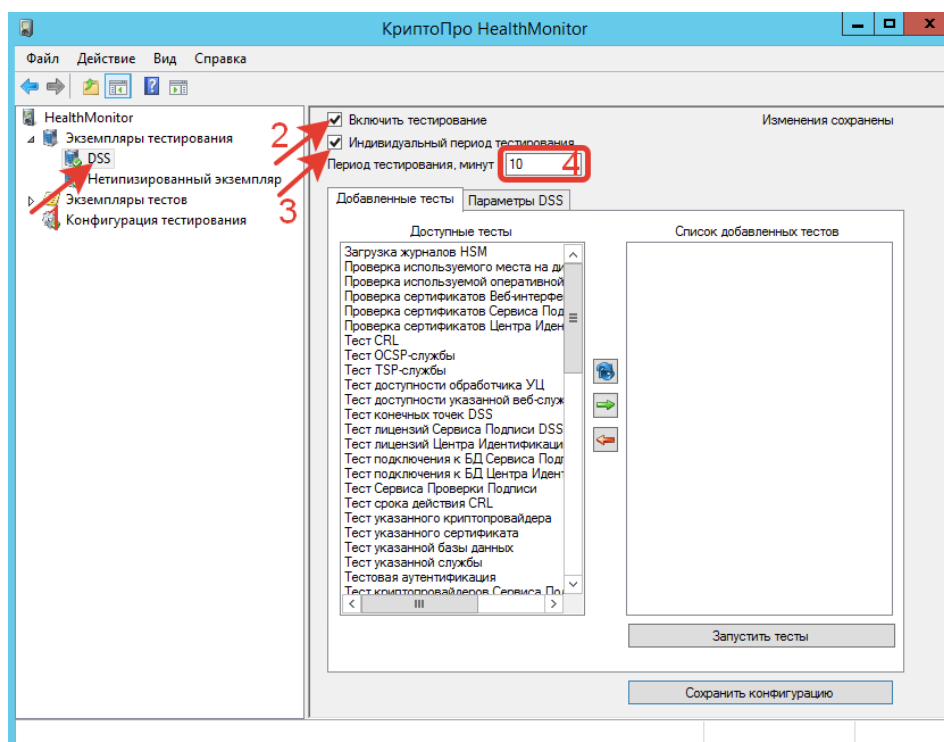


5.3.3. Добавление теста к экземпляру тестирования

Перед добавлением теста к экземпляру тестирования убедитесь, что соответствующая лицензия экземпляра Центра Мониторинга введена (см. разделы 2.3, 5.1), выбран правильный режим работы КриптоПро Центр Мониторинга (Default или Min,

см. раздел 5.4.1), а также добавлены и настроены все необходимые экземпляры тестирования (см. раздел 5.2) и экземпляры тестов (см. разделы 5.3.1, 5.3.2).

Перейдите к разделу «Экземпляры тестирования» и нажмите на экземпляр (1), к которому нужно добавить тесты (например, DSS). Автоматически откроется вкладка «Добавленные тесты» в правой части Оснастки мониторинга. **ОБЯЗАТЕЛЬНО** поставьте чекбокс «Включить тестирование» (2). При необходимости задать для данного экземпляра тестирования собственный период тестирования, поставьте чекбокс «Индивидуальный период тестирования» (3) и задайте этот период в минутах (4).



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 значок .

Сохраните конфигурацию экземпляра перед добавлением/удалением тестов путем нажатия кнопки «Сохранить конфигурацию». В противном случае вносить изменения будет невозможно.

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

Для **удаления** тестов их экземпляра тестирования необходимо выделить один или несколько тестов в области «Список добавленных тестов» и нажать на значок . Выбранные тесты будут удалены из экземпляра тестирования.

Работоспособность добавленных тестов и корректность их конфигурации можно проверить при помощи кнопки «Запустить тесты». В этом случае произойдет **ЕДИНОВРЕМЕННЫЙ** запуск тестов, находящихся в области «Список добавленных тестов», и будет выведено информационное окно с результатами их работы. В данном случае тестирование производится Оснасткой мониторинга, поэтому перезапуск службы не требуется. Но для осуществления полноценного тестирования при помощи КриптоПро Центр Мониторинга необходимо выполнить указанные ниже действия.



После добавления тестов к экземпляру тестирования или их удаления **НЕОБХОДИМО** сохранить изменения путем нажатия кнопки «Сохранить конфигурацию» и перезапустить Службу мониторинга.



Обратите внимание на значок около имени экземпляра тестирования. Когда в конфигурацию экземпляра вносятся изменения, около него появляется значок . Сохранение конфигурации приводит экземпляр в готовое к тестированию состояние, о чем свидетельствует значок .

5.4. Конфигурация тестирования

Раздел «Конфигурация тестирования» позволяет настроить общие параметры тестирования, оповещение и лицензирование Центра Мониторинга. Данные настройки представлены следующими вкладками:

- Основные настройки (см. раздел 5.4.1);
- Настройка почтовой рассылки (см. раздел 5.4.2);
- Настройка СМС-рассылки (см. раздел 5.4.3);
- Настройка мониторинга журналов (см. раздел 5.4.3);
- Лицензия (см. раздел 5.1);
- Веб-служба (см. раздел 0).

5.4.1. Основные настройки

Для ввода основных настроек КристоПро Центр Мониторинга в разделе «Конфигурация тестирования» перейдите на вкладку «Основные настройки» (1). Для настройки доступны следующие параметры:

- **Период тестирования по умолчанию** (2) — интервал времени в минутах, через который будут запускаться настроенные в разделе 5.3 тесты и рассылаться почтовые и СМС-сообщения.
- **Режим мониторинга** (3) — **Default** (по умолчанию) или **Min** (минимальный).

Режим **Default** используется, если экземпляр Центра Мониторинга развернут на одной рабочей станции с объектом(-ами) мониторинга и выполняет проверки экземпляров тестирования локально.

Режим **Min** используется в тех случаях, когда экземпляр Центра Мониторинга установлен на отдельном от объектов мониторинга сервере и выполняет только удаленные проверки. В минимальном режиме доступно ограниченное число тестов. Список тестов, доступных в минимальном режиме, представлен в Таблица 6.

Таблица 6 — Удаленные проверки

Экземпляр тестирования	Доступные в минимальном режиме тесты
DSS	Выполнение указанного скрипта Загрузка журналов HSM Проверка используемого места на диске Проверка используемой оперативной памяти Тест CRL

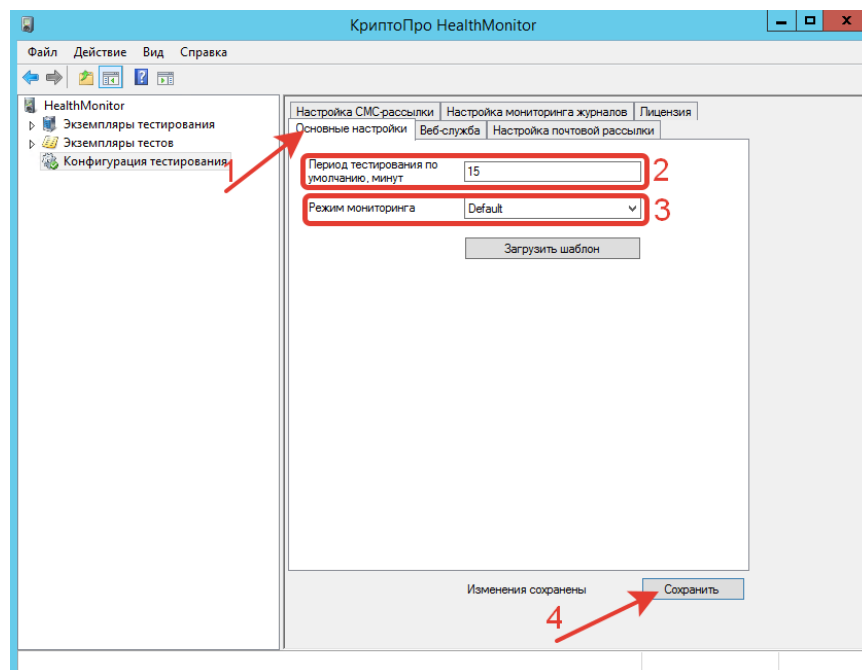
Экземпляр тестирования	Доступные в минимальном режиме тесты
	Тест OCSP-службы Тест TSP-службы Тест доступности указанной веб-службы Тест конечных точек DSS Тест Сервиса Проверки Подписи Тест срока действия CRL Тест указанного криптопровайдера Тест указанного сертификата Тест указанной БД Тест указанной службы Тестовая аутентификация Тестовая подпись Получение журналов Агента Мониторинга Тест состояния удаленного Агента Мониторинга Тест состояния HSM
Нетипизированный экземпляр	Выполнение указанного скрипта Загрузка журналов HSM Проверка используемого места на диске Проверка используемой оперативной памяти Тест CRL Тест OCSP-службы Тест TSP-службы Тест доступности указанной веб-службы Тест Сервиса Проверки Подписи Тест срока действия CRL Тест указанного криптопровайдера Тест указанного сертификата Тест указанной БД Тест указанной службы Тестирование связи с Центром Сертификации УЦ Получение журналов Агента Мониторинга Тест состояния удаленного Агента Мониторинга Тест состояния HSM



От выбора режима зависит, в какой Файл Конфигурации (**DefaultModeConfig.xml** ИЛИ **MinModeConfig.xml**) будут записываться текущие настройки всего экземпляра Центра Мониторинга. Если изменить режим, настройки экземпляров тестирования и экземпляров тестов будут получены из другого Файла Конфигурации.

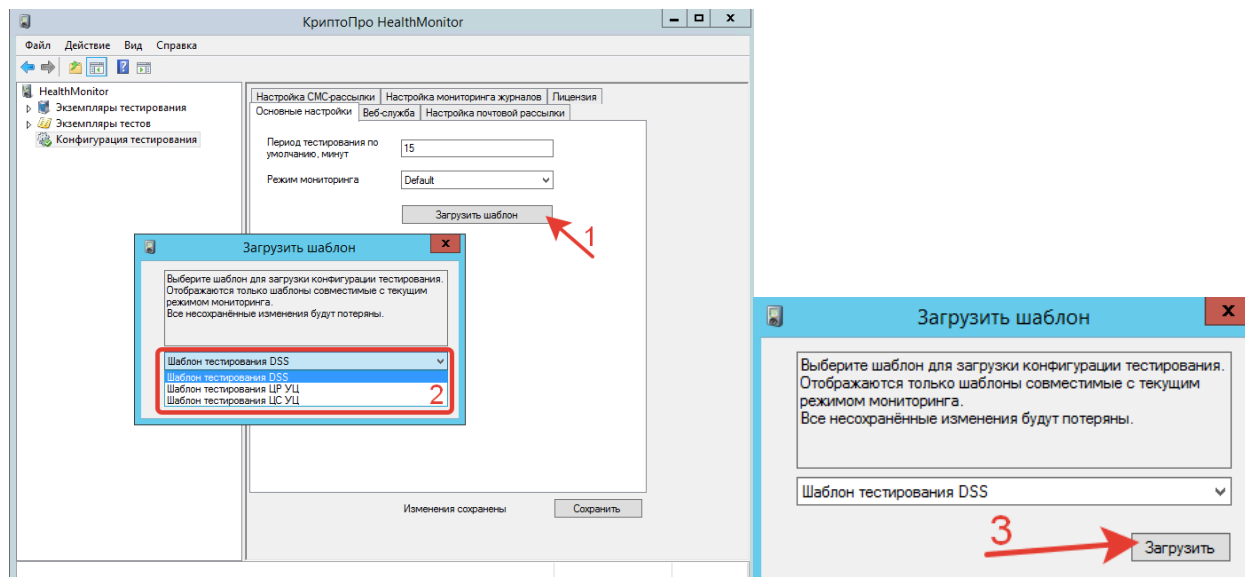


После изменения режима мониторинга необходимо сохранить изменения (4), перезапустить оснастку и службу мониторинга.



- Кнопка «**Загрузить шаблон**» — позволяет загрузить набор предустановленных (частично) тестов и экземпляров тестирования с уже настроенной конфигурацией и добавленными тестами. По умолчанию доступны шаблоны тестирования **DSS**, **ЦР УЦ** и **ЦС УЦ**.

Для загрузки шаблона тестирования перейдите в разделе «Конфигурация тестирования» на вкладку «Основные настройки» и нажмите кнопку «Загрузить шаблон» (1). В окне «Загрузить шаблон» выберите из выпадающего списка необходимый шаблон тестирования (2) и нажмите кнопку «Загрузить» (3). В данном случае сохранение конфигурации необязательно, но обязателен перезапуск Службы КриптоПро HealthMonitor.



5.4.2. Настройка почтовой рассылки

Для настройки почтовой рассылки в разделе «Конфигурация тестирования» перейдите на вкладку «Настройка почтовой рассылки» (1).

Чтобы настройка почтовой рассылки стала доступной, включите чекбокс «**Включить отправку отчетов**» (2).

Описание параметров почтовой рассылки представлено в Таблица 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 w (Предупреждение, см раздел 2.4.4). Внимание: 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 получателя рассылки	В данном поле необходимо указать адрес получателя писем с оповещением. Можно указать несколько адресов через «;».
Число попыток отправки сообщений	Количество попыток отправки письма с оповещением, после достижения которого будет выведено сообщение об ошибке.
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 (Windows-аутентификация/Имя пользователя и пароль/Без аутентификации).
Имя пользователя (отправителя)	Логин пользователя (отправителя) для подключения к почтовому серверу.
Пароль (отправителя)	Пароль пользователя (отправителя) для подключения к почтовому серверу.

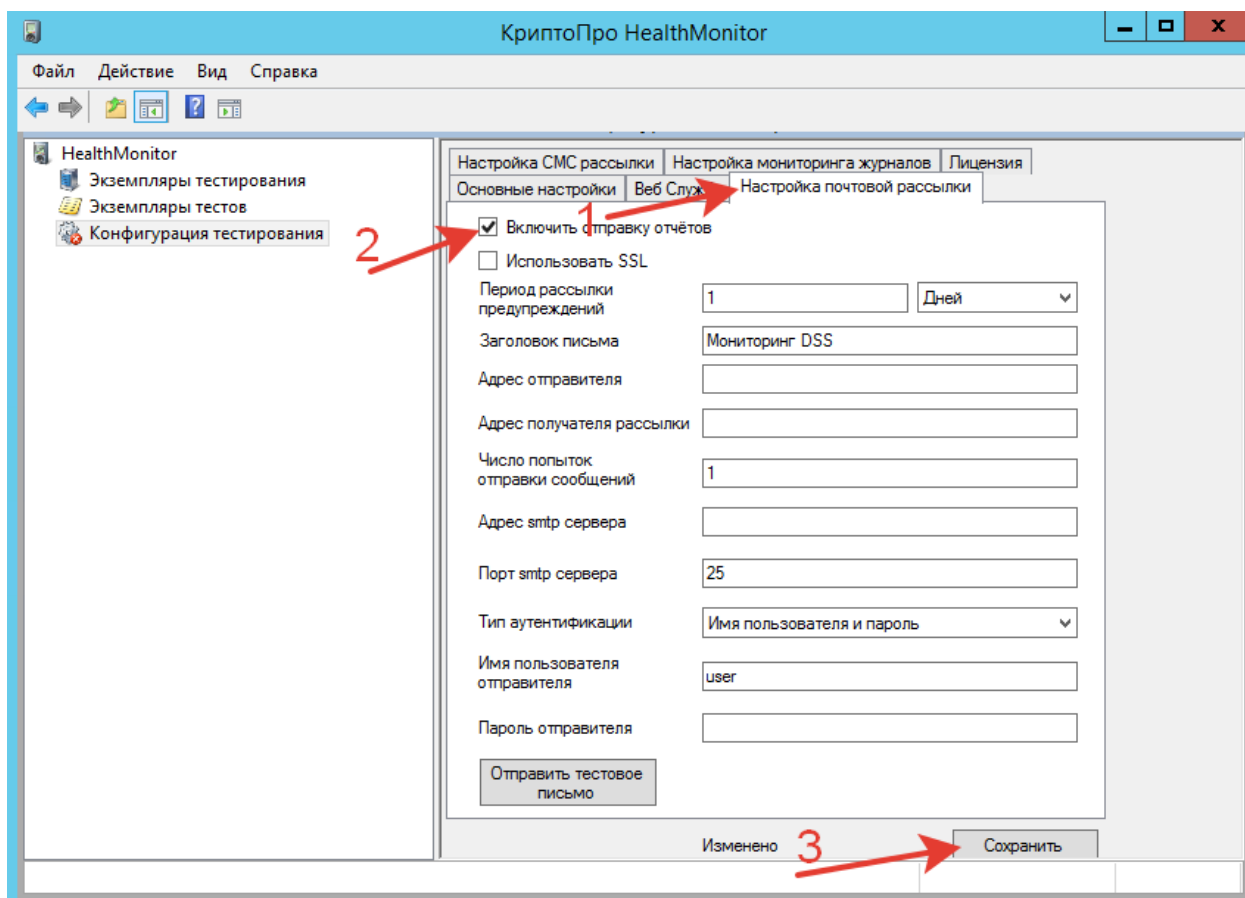
Проверить введенные настройки можно при помощи кнопки «**Отправить тестовое письмо**». В случае успеха на указанные в поле «Адрес получателя» адреса придет письмо с текстом «Если вы видите этот текст, рассылка почтовых сообщений настроена верно.»



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



Период рассылки почтовых сообщений зависит **ИСКЛЮЧИТЕЛЬНО** от периода тестирования по умолчанию, настроенного на вкладке «Основные настройки» раздела «Конфигурация тестирования».

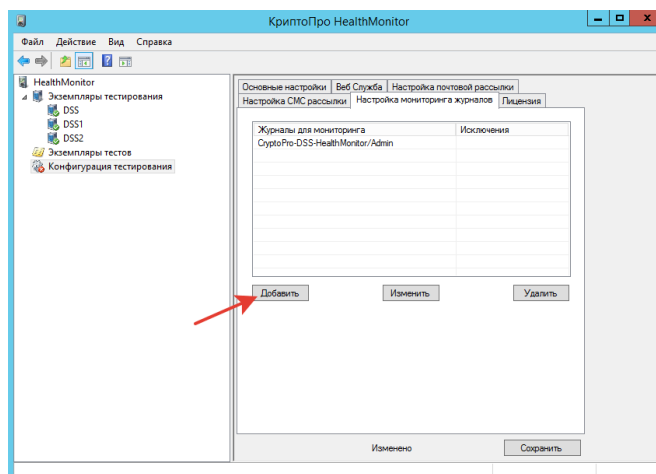


5.4.3. Настройка мониторинга журналов

Настройка мониторинга журналов является поднастройкой почтовой рассылки и доступна **ТОЛЬКО** при включенном чекбоксе «**Включить отправку отчетов**» на вкладке «Настройка почтовой рассылки».

На данной вкладке указываются журналы Windows, из которых КриптоПро Центр Мониторинга считывает события после прохождения тестов и оповещает администратора о событиях типов **e** и **w** (см. раздел 2.4.4) посредством email-сообщений, настроенных на вкладке «Настройка почтовой рассылки». По умолчанию уже добавлен собственный журнал КриптоПро Центр Мониторинга **CryptoPro-DSS-HealthMonitor/Admin**.

Чтобы добавить новый журнал мониторинга, нажмите «Добавить».



При добавлении журнала мониторинга укажите тип журнала (1) (выберите из выпадающего списка), исключения (2) (коды событий, о которых **НЕ НУЖНО** оповещать) и нажмите кнопку «Добавить» (3).

Доступные типы журналов мониторинга:

- Журнал утилиты мониторинга;
- Журнал Сервиса Подписи DSS;
- Журнал Центра Идентификации DSS;
- Журнал Веб-интерфейса DSS;
- Журнал Сервиса Аудита DSS;
- Журнал myDSS;
- Журнал Сервиса Проверки Подписи;
- Журнал приложений Windows (Приложение);
- Системный журнал Windows (Система);
- Журнал OCSP-службы;
- Журнал TSP-службы;
- **Произвольный журнал.**

Произвольный журнал позволяет настроить считывание событий из любого журнала событий Windows. В этом случае поле «Название журнала» становится доступным при добавлении, и его необходимо заполнить верным названием журнала.

Чтобы изменить или удалить журнал мониторинга из списка, выделите его и нажмите «Изменить» или «Удалить» соответственно.



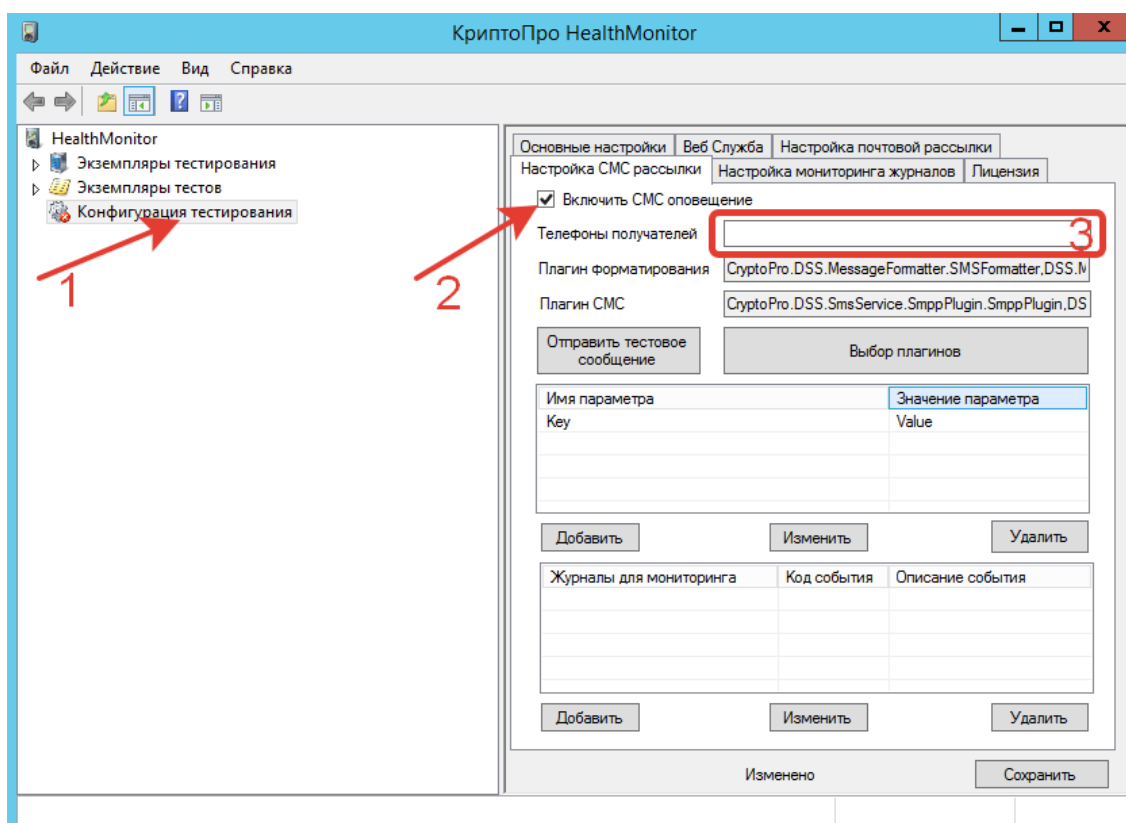
В процессе изменения журнала можно вносить изменения только в поле «Исключения». Исключения для журналов мониторинга представляют собой список кодов событий определенного журнала, записанных через «;» (Например: 1;128;1024).



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

5.4.4. Настройка СМС-рассылки

Для настройки СМС-рассылки в разделе «Конфигурация тестирования» перейдите на вкладку «Настройка СМС-рассылки» (1). Активируйте чекбокс «Включить СМС-оповещение», чтобы продолжить настройку рассылки (2). Задайте номер(-а) телефон(-ов) (3), на которые необходимо доставлять СМС-сообщения. Номера телефонов могут быть перечислены через «;».

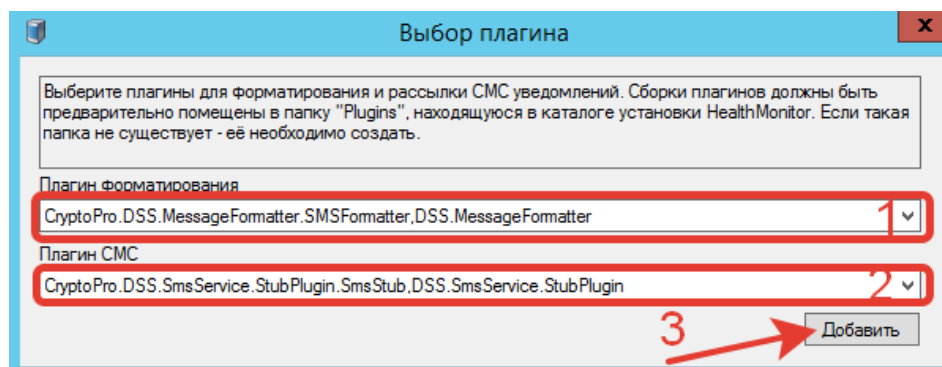


Записи журналов мониторинга могут быть преобразованы и доставлены в СМС-сообщении только после настройки **плагинов форматирования** и **транспортного плагина**. По умолчанию в КриптоПро Центр Мониторинга могут отсутствовать необходимые плагины. Поэтому перед началом настройки СМС-оповещения необходимо поместить плагины в папку <Путь установки>\Crypto Pro\DSS\HealthMonitor\Plugins. Если папка Plugins отсутствует, создайте ее.



Поля «Плагин форматирования» и «Плагин СМС» могут быть по умолчанию заполнены. Это **НЕ** значит, что плагины уже добавлены и используются. Необходимо подтвердить их использование при помощи кнопки «Выбор плагинов».

Настройка плагинов производится при помощи кнопки «Выбор плагинов». После нажатия появится окно «Выбор плагина». Выберите из выпадающего списка плагин форматирования (1) и транспортный плагин (2). Доступные плагины из папки <Путь установки>\Crypto Pro\DSS\HealthMonitor\Plugins подгружаются в выпадающие списки автоматически. После выбора плагинов нажмите кнопку «Добавить» (3).



После выбора плагинов необходимо настроить подключение к СМС-шлюзу, с которого будет производиться рассылка сообщений. Для этого используется область параметров, представляющая собой набор пар «Имя параметра — Значение параметра». Для того, чтобы добавить новый параметр, нажмите кнопку «Добавить». Для изменения или удаления параметра выделите этот параметр в списке и нажмите кнопку «Изменить» или «Удалить» соответственно.

Имя параметра	Значение параметра
Key	Value

➔ Добавить
Изменить
Удалить

После нажатия кнопки «Добавить» или «Изменить» откроется окно настройки параметров СМС-шлюза. Заполните необходимыми значениями поля «Имя параметра» (1), «Значение параметра» (2) и нажмите кнопку «Добавить/Изменить» (3). Новые параметры появятся в таблице.

Добавить/изменить значение

Имя параметра

Значение параметра

➔ Добавить/Изменить

Чтобы проверить корректность выполненных настроек плагинов и шлюза СМС-оповещения, сохраните конфигурацию при помощи кнопки «Сохранить» и нажмите кнопку «Отправить тестовое сообщение». Если предыдущие настройки верны, на телефоны получателей придет сообщение «Рассылка настроена корректно».

Следующим этапом настройки СМС-оповещения является настройка мониторинга журналов, о событиях из которых могут быть разосланы СМС-сообщения.



Основным отличием настройки журналов мониторинга для СМС-оповещения от журналов мониторинга почтовой рассылки является настройка событий. Для почтовой рассылки настраиваются исключения, т.н. «черный список», а для СМС-рассылки — «белый список».

Для того, чтобы добавить журнал для мониторинга, нажмите кнопку «Добавить».

Журналы для мониторинга	Код события	Описание события

➔ Добавить
Изменить
Удалить

При добавлении журнала мониторинга укажите тип журнала (1) (выберите из выпадающего списка) и события для рассылки (2) (коды событий, о которых **НУЖНО** оповещать). События указываются при помощи кодов событий определенного журнала, записанных через «;» (Например: 1;128;1024).

По желанию задайте описание события (4) (данный текст будет помещен в СМС-сообщение) и нажмите кнопку «Добавить» (5).

Доступные типы журналов мониторинга:

- Журнал утилиты мониторинга;
- Журнал Сервиса Подписи DSS;
- Журнал Центра Идентификации DSS;
- Журнал Веб-интерфейса DSS;
- Журнал Сервиса Аудита DSS;
- Журнал myDSS;
- Журнал Сервиса Проверки Подписи;
- Журнал приложений Windows (Приложение);
- Журнал OSCP-службы;
- Журнал TSP-службы;
- **Произвольный журнал.**

Произвольный журнал позволяет настроить считывание событий из любого журнала событий Windows. В этом случае поле «Название журнала» становится доступным при добавлении, и его необходимо заполнить верным названием журнала.

Для изменения или удаления журнала мониторинга выделите этот журнал в списке и нажмите кнопку «Изменить» или «Удалить» соответственно.



В процессе изменения журнала можно вносить изменения только в поле «События для рассылки». События для указываются при помощи кодов событий определенного журнала, записанных через «;» (Например: 1;128;1024).



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

После выполнения всех описанных выше настроек на телефоны указанных получателей начнут приходить СМС-сообщения о событиях, коды которых указаны в настройках добавленных журналов мониторинга.

Для журнала «Журнал утилиты мониторинга» СМС-сообщение выглядит следующим образом: **<Имя журнала мониторинга>:<Код события> <Описание события>**.

Для всех остальных журналов СМС-сообщение выглядит следующим образом: **<Имя журнала мониторинга>:<Код события>**.



СМС-сообщения могут приходить с небольшой задержкой. Период рассылки СМС-сообщений зависит **ИСКЛЮЧИТЕЛЬНО** от периода тестирования по умолчанию, настроенного на вкладке «Основные настройки» раздела «Конфигурация тестирования».

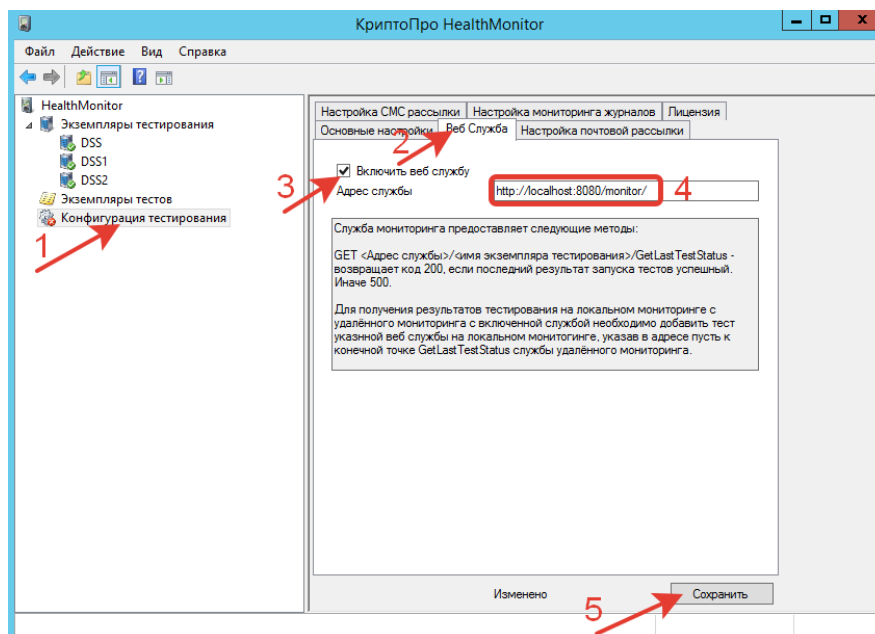
5.4.5. Веб-служба

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 настройку 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** (см. раздел 5.3.1).



Для работы Веб-службы Службе Мониторинга необходимы права локального администратора на рабочей станции, где установлен экземпляр КриптоПро Центр Мониторинга.

Для включения Веб-службы в разделе «Конфигурация тестирования» (1) перейдите на вкладку «Веб-служба» (2) и включите чекбокс «Включить веб-службу» (3). При необходимости скорректируйте поле «Адрес службы» (4) и нажмите кнопку «Сохранить» (5).



После изменения настроек Веб-службы необходимо сохранить изменения путем нажатия кнопки «Сохранить» и перезапустить Службу 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/DSS/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, 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.

Поле	Тип	Описание
Time	String	Время форматирования данного сообщения в UTC.

Пример ответа:

```
{
  "DetailedInformation": [
    "DSS -> Тестовая аутентификация -> успешно завершён",
    "DSS -> Тестовая подпись -> успешно завершён",
    "DSS -> Тест криптопровайдеров DSS -> успешно завершён",
    "DSS -> Проверка сертификатов веб интерфейса DSS -> успешно завершён",
    "DSS -> Проверка сертификатов сервиса ЦИ DSS -> завершён с ошибкой",
    "DSS -> Проверка сертификатов сервиса подписи DSS -> успешно завершён"
  ],
  "ErrorMessage": "DSS: 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** (см. раздел 5.3.1). Укажите следующие настройки данного теста:

- **Адрес службы** (1) — Адрес службы из настроек Веб-службы на Агенте (Например, <http://win-srv:8080/monitor>)
- **Имя экземпляра тестирования** (2) — Имя тестируемого экземпляра на Агенте (Например, DSS).
- Сохраните настройки теста при помощи кнопки «Сохранить» (3).

Пример:

Тест состояния удалённого Агента Мониторинга

Изменения сохранены

Описание

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

Имя экземпляра тестирования

3

Сохранить

СВЕДЕНИЯ О РАЗРАБОТЧИКЕ

Компания КriptoПро создана в 2000 году и в настоящее время занимает лидирующее положение по распространению средств криптографической защиты информации и электронной цифровой подписи.

Основное направление деятельности компании - разработка средств криптографической защиты информации и развитие Инфраструктуры Открытых Ключей (Public Key Infrastructure) на основе использования международных рекомендаций и российских криптографических алгоритмов.

Компания разработала полный спектр программных и аппаратных продуктов для обеспечения целостности, авторства и конфиденциальности информации с применением ЭП и шифрования для использования в различных средах (Windows, Unix, Java). Новое направление продуктов компании – программно-аппаратные средства криптографической защиты информации и использованием смарт-карт и USB ключей, позволяющих существенно повысить безопасность систем, использующих ЭП.

Компания КriptoПро является разработчиком и поставщиком средств применения ЭП в автоматизированных информационных системах. Кроме этого, компания оказывает консультационные услуги по обеспечению деятельности удостоверяющих центров и применению ЭП в автоматизированных информационных системах предприятий различных форм собственности.

Удостоверяющий центр компании КriptoПро предоставляет организациям (юридическим лицам) услуги по изготовлению и управлению открытыми и закрытыми ключами Пользователей информационных систем, включая процедуру подачи и обработки запросов на сертификаты, верификацию запросов на сертификаты, формирования сертификатов, их получения, использования и отзыва. Также Удостоверяющим центром предоставляются иные сервисные функции, связанные с использованием электронных подписей, шифрованием, обеспечением электронного юридически-значимого документооборота.

Контакты:

ООО «КРИПТО-ПРО»

127018, Москва, ул. Сущёвский вал, 18

Телефон: (495) 995 4820

Факс: (495) 995 4820

URL: <http://www.CryptoPro.ru>

E-mail: info@CryptoPro.ru