

127018, Москва, ул. Сушёвский вал, д. 18
Телефон: +7 (495) 995 4820
Факс: +7 (495) 995 4820
<https://www.CryptoPro.ru>
E-mail: info@CryptoPro.ru



Средство Криптографической Защиты Информации	КриптоПро HSM версия 2.0 R3 Комплектации 1 и 2 Инструкция по использованию
---	--

ЖТЯИ.00096-03 90 01

Листов 135

2023 г.

Содержание

1. АННОТАЦИЯ	4
2. СОСТАВ И НАЗНАЧЕНИЕ ПАКМ	5
2.1. Назначение ПАКМ	5
2.2. Область применения ПАКМ «КриптоПро HSM»	6
2.3. Состав изделия	7
2.4. Сведения об используемых криптопровайдерах	8
2.5. Состояния ПАКМ	12
3. УСТАНОВКА ПАКМ	15
3.1. Порядок установки ПАКМ	16
3.2. Проверка комплектации и подключение ПАКМ	18
3.3. Инициализация ПАКМ	18
3.4. Установка сетевых настроек ПАКМ	20
3.5. Установка системного времени ПАКМ	21
3.6. Выпуск карты локального защищенного канала (канала «К»)	21
3.7. Установка интерфейсных модулей	21
3.8. Настройка удаленного рабочего места Web администрирования ПАКМ	22
3.9. Установка лицензий ПАКМ	24
3.10. Настройка ограничения использования алгоритма ГОСТ Р 34.10-2001	25
3.11. Параметры, устанавливаемые изготовителем	25
3.12. Требования безопасности	26
4. ВКЛЮЧЕНИЕ ПАКМ	27
5. АДМИНИСТРИРОВАНИЕ ПАКМ	28
5.1. Ввод pin-кода	28
5.2. Возможные меню LCD панели ПАКМ	29
5.3. Работа с LCD меню администрирования ПАКМ	29
5.3.1. Изменение состояния ПАКМ	33
5.3.2. Показ сообщений журнала событий	35
5.3.3. Смена pin-кода на карте	36
5.3.4. Установка часового пояса ПАКМ	37
5.3.5. Установка системного времени/даты ПАКМ	38
5.3.6. Показ системных характеристик	39
5.3.7. Очистка содержимого ПАКМ	39
5.3.8. Смена мастер-ключа аутентификации/выпуск карт канала «К»	41
5.3.9. Просмотр и изменение сетевых настроек	42
5.3.10. Просмотр и изменение параметров ПАКМ	44
5.3.11. Управление пользователями	50

5.3.12.	Настройки межсетевого экрана	55
5.3.13.	Изменение внутренних ключей и сертификатов ПАКМ	57
5.3.14.	Корректная очистка журнала аудита	59
5.3.15.	Восстановление журнала аудита	60
5.3.16.	Резервное копирование и восстановление ПАКМ	61
5.3.17.	Смена пароля для доступа к режиму полной очистки ПАКМ в меню неавторизованных операций (Change password).....	63
5.3.18.	Ввод лицензии на использование ПАКМ (License(s)).	63
5.4.	Работа с LCD меню платежной системы	64
5.5.	Работа с LCD меню неавторизованных операций	66
5.6.	Работа с журналом событий ПАКМ	67
6.	УДАЛЕННОЕ АДМИНИСТРИРОВАНИЕ ПАКМ (WEB ИНТЕРФЕЙС)	69
6.1.	Удаленное рабочее место Администратора	69
6.2.	Открытие окна администрирования ПАКМ	72
6.3.	Работа с окном администрирования ПАКМ.....	73
6.3.1.	Информация ПАКМ	74
6.3.2.	Сертификаты ПАКМ	80
6.3.3.	Параметры ПАКМ	83
6.3.4.	Настройки сети	85
6.3.5.	Настройки межсетевого экрана	86
6.3.6.	Настройки аудита	89
6.3.7.	Пользователи	91
6.3.8.	Особенности выполнения операций, требующих подтверждения вторым привилегированным пользователем.....	102
6.3.9.	Резервные копии.....	115
6.3.10.	Журнал аудита.....	118
6.3.11.	Журнал событий.....	122
6.3.12.	Настройки PCI HSM	123
6.3.13.	Обновление PCI HSM	124
6.3.14.	Сервисы PCI HSM	126
6.3.15.	Лицензии HSM	127
7.	ДОСТУП К ФУНКЦИЯМ ПЛАТЕЖНОГО МОДУЛЯ	131
7.1.	Подключение к консоли	131
8.	ПОРЯДОК ВЫПОЛНЕНИЯ ТЕХНИЧЕСКОГО ОБСЛУЖИВАНИЯ И РЕМОНТА ПАКМ	133
8.1.	Порядок действий при отказе оборудования ПАКМ	133
8.2.	Порядок действий при проведении технического обслуживания ПАКМ	134

1. АННОТАЦИЯ

Данный документ содержит инструкцию по использованию программно-аппаратного модуля (ПАКМ) «КриптоПро HSM», его состав, порядок установки и администрирования.

Документ предназначен для администраторов информационной безопасности учреждений, осуществляющих установку, обслуживание и контроль за соблюдением требований к эксплуатации средств СКЗИ, а также для администраторов Серверов, сетевых ресурсов предприятия и других работников службы информационной безопасности, осуществляющих настройку рабочих мест для работы со средствами СКЗИ.

Инструкции администраторам безопасности и пользователям различных автоматизированных систем, использующих ПАКМ «КриптоПро HSM», должны разрабатываться с учетом требований настоящей инструкции.

2. СОСТАВ И НАЗНАЧЕНИЕ ПАКМ

2.1. Назначение ПАКМ

ПАКМ «КриптоПро HSM» — программно-аппаратный криптографический модуль, предназначенный для использования в сетях/системах хранения и обработки информации, не составляющей государственной тайны.

ПАКМ «КриптоПро HSM» представляет собой сетевое устройство, подключаемое либо непосредственно к серверу, использующему криптографические сервисы ПАКМ, либо в сегмент локальной сети через стандартные сетевые устройства (коммутаторы, маршрутизаторы, концентраторы) для обслуживания групп серверов и компьютеров пользователей сети.

ПАКМ может быть использован в качестве СКЗИ в различных системах/подсистемах криптографической защиты информации, поддерживающих криптографические интерфейсы «КриптоПро CSP» (Microsoft CryptoAPI 2.0).

ПАКМ «КриптоПро HSM» предназначен для выполнения следующих функций:

- создание/проверка электронной подписи;
- вычисление значения хэш-функции областей памяти и файлов;
- шифрование/расшифрование областей памяти и файлов;
- вычисление имитовставки областей памяти и файлов;
- генерация и хранение ключей, уничтожение ключей;
- обеспечение защиты чувствительной информации, обрабатываемой в платёжной системе, и безопасного хранения криптографических ключей.

ПАКМ «КриптоПро HSM» предполагает различные варианты комплектации, сертифицированные по различным уровням защиты:

- Комплектация 1 Исполнение 1К ПАКМ «КриптоПро HSM», уровень защиты KB/KB2
- Комплектация 1 Исполнение 5К ПАКМ «КриптоПро HSM», уровень защиты KC3
- Комплектация 2 Исполнение 1К ПАКМ «КриптоПро HSM», уровень защиты KC1
- Комплектация 2 Исполнение 2К ПАКМ «КриптоПро HSM», уровень защиты KC2
- Комплектация 2 Исполнение 3К ПАКМ «КриптоПро HSM», уровень защиты KC3

Состав аппаратного и программного компонентов соответствующих исполнений ПАКМ описан в документе «ЖТЯИ.00096-03 95 01. Правила пользования».

В состав Комплектации 2 входит ПО клиентского компонента ПАКМ, который является ответной частью, устанавливаемой на рабочие станции и сервера, необходимой для трансляции криптографических вызовов к ПАКМ «КриптоПро HSM» по безопасным каналам «К», «К2».

Клиентский компонент ПАКМ, включающий СКЗИ «КриптоПро CSP», поставляется на компакт-диске совместно с ПАКМ. Предусмотрена поставка клиентской компоненты отдельно от ПАКМ «КриптоПро HSM» в соответствующей комплектации согласно «ЖТЯИ.00096-03 30 01. Формуляр».

Порядок установки и использования клиентского компонента ПАКМ описан в документе «ЖТЯИ.00096-03 90 02. Использование интерфейсных модулей», а также в документе «ЖТЯИ.00096-03 93 01. Руководство пользователя».

2.2. Область применения ПАКМ «КриптоПро HSM»

ПАКМ «КриптоПро HSM» может быть использован в качестве СКЗИ в различных системах/подсистемах криптографической защиты информации, поддерживающих криптографический интерфейс (Cryptographic Service Provider (CSP)) «КриптоПро CSP».

Реализация ПАКМ и поддержка им стандартизированного интерфейса позволяет осуществлять взаимозаменяемость ПАКМ «КриптоПро HSM» и СКЗИ «КриптоПро CSP». При этом необходимо обязательно учитывать уровень безопасности используемых версий каждого СКЗИ. То есть, при замене «КриптоПро CSP», сертифицированного по уровню КС2, средством криптографической защиты информации ПАКМ «КриптоПро HSM», обеспечивающим уровень безопасности по классу КВ/КВ2 (Комплектация 1 Исполнение 1К) или КС3 (Комплектация 1 Исполнения 5К), общий уровень безопасности системы может быть повышен, и наоборот, при замене ПАКМ «КриптоПро HSM» средством криптографической защиты информации «КриптоПро CSP» общий уровень безопасности системы может быть понижен.

В первую очередь рекомендуется использовать ПАКМ «КриптоПро HSM» в серверных компонентах распределенных систем, требующих обеспечить высокий уровень защиты (до КВ/КВ2) и срок действия ключа ЭП до 3 лет. К таким системам относятся программные, программно-аппаратные комплексы Удостоверяющих центров, а именно те их компоненты, которые выполняют функции использования ключа Уполномоченного лица удостоверяющего центра для подписи (издания) сертификатов и списков отзыва сертификатов.

Другим важным вариантом применения ПАКМ является его использование в дополнительных службах удостоверяющих центров. Примером таких служб могут служить Службы Штампов Времени (Time Stamp Service - TSS), Службы актуальных статусов сертификатов (Online Certificate Status Service - OCSS), службы электронного нотариата.

В сетях передачи конфиденциальной информации ПАКМ «КриптоПро HSM» может быть использовано для реализации протокола TLS, обеспечивая более надежный уровень защиты ключа TLS-сервера и выполняя трудоемкие операции по шифрованию/расшифрованию передаваемых по сети пакетов данных. В данном случае

ПАКМ может быть использован в web-серверах, серверах баз данных, серверах приложений.

Наличие в ПАКМ «КриптоПро HSM» платежного модуля (КриптоПро PCI HSM) позволяет использовать его в банках, кредитных и финансовых организациях для проведения банковских транзакций, эмиссии платежных карт и др. операций, выполняемых банковскими платежными сервисами. Документация на платежный модуль поставляется отдельно.

Также возможно применение ПАКМ в персональных (не серверных) системах, требующих использования криптографических операций.

2.3. Состав изделия

Изделие ПАКМ «КриптоПро HSM» содержит в комплекте компоненты, перечисленные в формуляре. Как правило, это:

- Системный блок ПАКМ;
- Кабель электропитания;
- Кабель сетевой оптический (Ethernet, 1 Гигабит);
- Ключевые носители — смарт-карты;
- Персональные идентификаторы («таблетки») ПАК «Соболь» (не менее 2 шт.);
- Эксплуатационная документация.

Для использования ПАКМ на компьютер пользователя/сервер необходимо установить и настроить ПО клиентского компонента ПАКМ (подробнее см. «ЖТЯИ.00096-03 90 02. Использование интерфейсных модулей»).

Таблетки ПАК «Соболь» и смарт-карты должны храниться у администратора безопасности до момента выдачи пользователям.

Для локального администрирования ПАКМ служит панель с жидкокристаллическим экраном и кнопками управления (LCD-панель) (См. Рисунок 1). Корпус ПАКМ выполнен в 2U форм-факторе. При этом LCD панель может незначительно отличаться от изображенной на рисунке. Обычно, вместо обозначения кнопки <- (стрелка влево), может использоваться обозначение этой кнопки, как «х» (отмена).



Рисунок 1 Панель управления ПАКМ

ПАКМ «КриптоПро HSM» имеет возможность удаленного администрирования через web-интерфейс рабочего места администратора ПАКМ.

2.4. Сведения об используемых криптопровайдерах

Для внешнего доступа к криптографическим функциям ПАКМ могут использоваться следующие имена и типы криптопровайдеров:

- 'Crypto-Pro GOST R 34.10-2012 HSM CSP[01-04]' (тип 80)
- 'Crypto-Pro GOST R 34.10-2012 HSM Svc CSP' (тип 80)
- 'Crypto-Pro GOST R 34.10-2012 HSM 1.0 CSP[01-04]' (тип 80)
- 'Crypto-Pro GOST R 34.10-2012 HSM 1.0 Svc CSP' (тип 80)
-
- 'Crypto-Pro GOST R 34.10-2012 Strong HSM CSP[01-04]' (тип 81)
- 'Crypto-Pro GOST R 34.10-2012 Strong HSM Svc CSP' (тип 81)
- 'Crypto-Pro GOST R 34.10-2012 Strong HSM 1.0 CSP[01-04]' (тип 81)
- 'Crypto-Pro GOST R 34.10-2012 Strong HSM 1.0 Svc CSP' (тип 81)
-
- 'Crypto-Pro ECDSA and AES HSM CSP[01-04]' (тип 16)
- 'Crypto-Pro ECDSA and AES HSM Svc CSP' (тип 16)
- 'Crypto-Pro ECDSA and AES HSM 1.0 Svc CSP' (тип 16)
- 'Crypto-Pro ECDSA and AES HSM 1.0 CSP[01-04]' (тип 16)
-
- 'Crypto-Pro Enhanced RSA and AES HSM CSP[01-04]' (тип 24)
- 'Crypto-Pro Enhanced RSA and AES HSM Svc CSP' (тип 24)
- 'Crypto-Pro Enhanced RSA and AES HSM 1.0 CSP[01-04]' (тип 24)
- 'Crypto-Pro Enhanced RSA and AES HSM 1.0 Svc CSP' (тип 24)
-
- 'Crypto-Pro Curve25519 and AES HSM CSP' (тип 32)
- 'Crypto-Pro Curve25519 and AES HSM Svc CSP' (тип 32)

- **'Crypto-Pro Curve25519 and AES HSM 1.0 CSP[01-04]'** (тип 32)
- **'Crypto-Pro Curve25519 and AES HSM 1.0 Svc CSP'** (тип 32)
-
- **'Crypto-Pro HSM RSA CSP[01-08]'** (тип 1)
- **'Crypto-Pro HSM RSA Svc CSP'** (тип 1)
- **'Crypto-Pro RSA HSM CSP'** (тип 1)
- **'Crypto-Pro RSA HSM Svc CSP'** (тип 1)
- **'Crypto-Pro RSA HSM 1.0 CSP[01-04]'** (тип 1)
- **'Crypto-Pro RSA HSM 1.0 Svc CSP'** (тип 1)
-
- **'Crypto-Pro HSM CSP[01-08]'** (тип 75)
- **'Crypto-Pro HSM Svc CSP'** (тип 75)
- **'Crypto-Pro GOST R 34.10-2001 HSM CSP'** (тип 75)
- **'Crypto-Pro GOST R 34.10-2001 HSM Svc CSP'** (тип 75)
- **'Crypto-Pro GOST R 34.10-2001 HSM 1.0 CSP'** (тип 75)
- **'Crypto-Pro GOST R 34.10-2001 HSM 1.0 Svc CSP'** (тип 75)
- **'Crypto-Pro HSM 1.0 CSP[01-04]'** (тип 75)
- **'Crypto-Pro HSM 1.0 Svc CSP[01-04]'** (тип 75)

Для генерации и хранения ключей используется внутренний считыватель ПАКМ с именем «HSMDB». Его отличительной особенностью является то, что все закрытые ключи/ключи ЭП шифруются на ключах шифрования ПАКМ (подробнее см. раздел 6 «ЖТЯИ.00096-03 91 01. Руководство администратора безопасности»).

В приведенном выше списке криптопровайдеров встречаются имена с суффиксами вида "...[01-04]" или "...[01-08]". Это означает, что кроме основного имени, например, **'Crypto-Pro GOST R 34.10-2012 HSM CSP'** зарезервировано ещё несколько синонимов имени данного криптопровайдера, например, **'Crypto-Pro GOST R 34.10-2012 HSM CSP 01'**, **'Crypto-Pro GOST R 34.10-2012 HSM CSP 02'...**, и т.д. Они служат для создания высокопроизводительных систем повышенной надежности, а именно для создания пулов из ПАКМ. На серверах, использующих СКЗИ «КриптоПро HSM» можно зарегистрировать эти имена таким образом, что при обращении к криптопровайдерам с подобными именами запросы будут направляться в конкретный ПАКМ, связанный с данным именем криптопровайдера. Т.е. манипулируя в приложении именами криптопровайдеров, по сути производится манипуляция IP-адресами, по которым будут направляться CryptoAPI запросы, разных клонов «КриптоПро HSM». При необходимости эти имена криптопровайдеров на устройствах доступа должны быть зарегистрированы вручную.

Криптопровайдеры с именами, включающими лексему «Svc», отличается от криптопровайдеров без её наличия тем, что их использование позволяет выводить запросы на ввод pin-кодов для ключей пользователей не на «рабочий стол» рабочей

станции пользователя, а на LCD панель ПАКМ. Кроме этого они позволяют организовать обмен между сервером и ПАКМ по более производительному нешифрованному каналу, при условии осуществления однозначной двусторонней аутентификации «сервер<->ПАКМ», нахождении сервера и ПАКМ в одной контролируемой зоне и условии, что используется специальный сертификат ключа доступа, включающий расширение (extended key usage - ECU) «1.2.643.2.2.34.22».

Такие криптопровайдеры используются в основном в серверных конфигурациях серверами приложений, работающими в фоновом режиме и не имеющими консоли для вывода сообщений и/или запроса pin-кодов. Они реализованы в виде отдельного сервиса ОС Windows, запускаемого при загрузке ОС.

Криптопровайдеры с именами, включающими лексему «HSM 1.0», отличается от криптопровайдеров без её наличия тем, что ключевые контейнеры используют считыватель «HSM» вместо «HSMDB».

Считыватель «HSMDB» — это внутренняя память (flash диск) ПАКМ, которая защищается ключами шифрования ПАКМ, т.е. все ключи, сформированные на считывателе «HSMDB», автоматически шифруются. А так как ключи шифрования ПАКМ защищены на разделенном по схеме «3 из 5» ключе активации ПАКМ, то все ключи, созданные на считывателе «HSMDB», невозможно открыть без активации ПАКМ (активации разделенного «ключа активации ПАКМ»). При этом ключевые контейнеры хранятся во внутренней Базе данных ПАКМ и могут реплицироваться подсистемой горячего резервирования в другой ПАКМ.

Считыватель «HSM» — это также внутренняя память (flash диск) ПАКМ, которая защищается ключами шифрования ПАКМ также, как и для считывателя «HSMDB». Но ключевые контейнеры хранятся не в БД, а в виде файлов ОС и не могут реплицироваться подсистемой горячего резервирования в другой ПАКМ. Для резервирования таких ключевых контейнеров может быть применено только клонирование ПАКМ (холодное резервирование).

Криптопровайдеры 75-го типа **Crypto-Pro GOST R 34.10-2001 HSM CSP** (синоним имени "Crypto-Pro HSM CSP") реализуют:

- выполнение функций создания и проверки электронной подписи (ЭП) согласно ГОСТ Р 34.10-2001, возможность вычисления хэш-функции согласно ГОСТ Р 34.11-94;
- возможность шифрования и имитозащиты согласно ГОСТ 28147-89;

Для хранения ключей используется внутренний считыватель ПАКМ с именем «HSMDB».

Алгоритмы подписи данного криптопровайдера выводятся из обращения, используются только для проверки ЭП, и расшифрования ранее созданных

криптографических сообщений. Для формирования новых криптографических сообщений используйте более новые алгоритмы и соответствующие криптопровайдеры.

Криптопровайдеры 80 и 81 типа **Crypto-Pro GOST R 34.10-2012 HSM CSP** и **Crypto-Pro GOST R 34.10-2012 Strong HSM CSP** (и их синонимы) реализуют:

- выполнение функций создания и проверки электронной подписи (ЭП) согласно ГОСТ Р 34.10-2012 (ГОСТ 34.10-2018), вычисление хэш-функции согласно ГОСТ Р 34.11-2012 (ГОСТ 34.11-2018);
- возможность шифрования и имитозащиты согласно ГОСТ 28147-89, ГОСТ Р 34.12-2015 (ГОСТ 34.12-2018), ГОСТ Р 34.13-2015 (ГОСТ 34.13-2018);

На настоящий момент криптопровайдеры 80-го типа являются основными и используются для всех служебных ключей ПАКМ «КриптоПро HSM».

Помимо криптопровайдеров, реализующих алгоритмы ГОСТ, в ПАКМ «КриптоПро HSM» устанавливаются криптопровайдеры, реализующие зарубежные алгоритмы.

Криптопровайдеры 1-го типа **Crypto-Pro HSM RSA CSP** и **Crypto-Pro HSM RSA Svc CSP** (тип 1) устаревшей реализации (wine) оставлены для совместимости с предыдущими версиями. Не рекомендуется их использовать в новых приложениях. Следует использовать более новую реализацию - криптопровайдер **Crypto-Pro RSA HSM CSP** (и его синонимы). Они реализуют алгоритмы электронной подписи RSA:

- генерацию ключевых пар с размером открытого ключа до 16K;
- формирование и проверку ЭП (RSA);
- вычисление значения хэш-функции с использованием алгоритмов SHA1, SHA256, SHA384, MD5;
- генерацию симметричных ключей DES, 3DES, 3DES_112;
- шифрование/расшифрование по указанным алгоритмам.

Но, если необходимо использовать зарубежные алгоритмы, рекомендуется использовать более современные их модификации, которые реализуются криптопровайдерами 16-го, 24 и 32 типов: "... **ECDSA and AES ...**", "...**Enhanced RSA and AES ...**" и "...**Curve25519 and AES ...**".

Все необходимые криптопровайдеры должны быть зарегистрированы на ПЭВМ, использующих криптографические сервисы.

Обычному пользователю не следует использовать криптопровайдеры «"... Svc ... "». ПО клиентского компонента не позволяет работу с данными провайдерами, если в сертификате ключа доступа к ПАКМ нет соответствующего расширения.

Администраторам серверов при использовании ПАКМ «КриптоПро HSM» с такими сервисами как Microsoft CA, «КриптоПро УЦ», Microsoft IIS и другими, реализованными в виде служб ОС Windows, необходимо использовать криптопровайдеры «"...Svc ...».

Клиентская часть таких провайдеров (на машине клиента ПАКМ «КриптоПро HSM») реализована в виде службы ОС Windows, которая запускается в момент загрузки ОС и может обслуживать криптографические запросы других служб, даже если никто из пользователей не открыл Windows сессию («не залогинился»).

Клиентская часть **обычных** провайдеров (без лексемы Svc в имени) реализована в виде пользовательского приложения, которое грузится в момент входа («логона») пользователя, и отображается в виде иконки в системном трее. Таким образом, если на ПЭВМ с установленным ПО «Клиент КриптоПро HSM» нет активной Windows сессии (ни одного «залогиненного» пользователя), то никто не сможет обслужить криптографические запросы, обращенные к обычным криптопровайдерам.

Администраторам серверов следует с осторожностью относиться к установке криптопровайдеров «КриптоПро HSM» в качестве «провайдеров по-умолчанию» в ОС Windows. Некоторые системные сервисы ОС Windows перечисляют установленные типы криптопровайдеров и реализуемые ими алгоритмы, путем обращения к этим криптопровайдерам. При этом, если КриптоПро HSM выключен в данный момент, не активирован, или в считывателе отсутствует ключ доступа к ПАКМ, то может наблюдаться эффект зависания ОС. Рекомендуется для «провайдеров по-умолчанию» использовать криптопровайдеры с локальной реализацией криптоалгоритмов. Сервера приложений, которым необходимо использовать криптографию «КриптоПро HSM», должны всегда явно обращаться по именам криптопровайдеров (HSM), а не по типам, и не надеяться на то что прописано в ветках реестра «Провайдеры по умолчанию» (Default Provider Types).

Обращения к криптопровайдерам, работающим с ПАКМ через сервис, могут быть сделаны только пользователями с учетными именами SYSTEM (LocalSystem), пользователями, входящими в группу локальных администраторов компьютера или в группу **«Привилегированные пользователи КриптоПро HSM»**. Группу «Привилегированных пользователей КриптоПро HSM» можно создать вручную и добавить туда, например, учетные имена, под которыми исполняются сервисные приложения (например, пул приложений .NET под управлением Microsoft IIS). Эти же правила действуют при обращении пользователей к любым криптопровайдерам ПАКМ через системный трей, при использовании специального флага в вызовах интерфейса CryptoAPI — CRYPT_MACHINE_KEYSET.

Процесс установки дистрибутива ПО «Клиент КриптоПро HSM» не изменяет значение провайдера по умолчанию для 1 типа. Обычно, в ОС Windows им является криптопровайдер «Microsoft Strong Cryptographic Provider».

2.5. Состояния ПАКМ

ПАКМ «КриптоПро HSM» может находиться в различных состояниях, характеризующихся отсутствием/наличием удаленного доступа к криптографическим

функциям (по каналу «К» и каналу «K2») и функциями управления ПАКМ (web-интерфейс администратора ПАКМ), а также состоянием ключа активации ПАКМ (активирован/не активирован), а соответственно, имеется ли доступ ко всем остальным ключам, хранящимся в ПАКМ, т.к. они прямо или косвенно (через ключ шифрования ПАКМ) зашифрованы на нем.

Выделяются следующие состояния ПАКМ:

- **HSM-STATE-INACTIVE**

ПАКМ неактивен.

- Ключ «3 из 5» и ключи шифрования не активированы.
- Сервисы каналов удаленного доступа пользователей к ПАКМ не запущены.
- сервисы платежного приложения не могут быть запущены.
- Web-интерфейс администрирования не отвечает.
- ПАКМ может обслуживать только запросы привилегированных пользователей с LCD панели.

- **HSM-STATE-FULLACTIVE**

ПАКМ активен.

- Ключ «3 из 5» и ключи шифрования активированы.
- Сервисы удаленного доступа к ПАКМ могут быть запущены и обрабатывать все запросы пользователей.
- сервисы платежного приложения могут быть запущены.
- Web-интерфейс может быть использован для администрирования.
- ПАКМ может обслуживать запросы пользователей по сети, включая и запросы с удаленного рабочего места администратора ПАКМ.

- **HSM-STATE-ACTIVE-ADMIN-ONLY**

ПАКМ активен.

- Ключ «3 из 5» и ключи шифрования активированы.
- Сервисы удаленного доступа пользователей к ПАКМ не могут быть запущены.
- сервисы платежного приложения могут быть запущены.
- Web-интерфейс может быть использован для администрирования.
- ПАКМ может обслуживать только запросы привилегированных пользователей с LCD панели и с удаленного АРМ Администрирования ПАКМ.

- **HSM-STATE-HALT**

Полный останов ПАКМ.

- Все сервисы деактивируются.
- ОС выгружается.

При включении ПАКМ после загрузки его системных сервисов ПАКМ находится в неактивном состоянии - HSM-STATE-INACTIVE.

Для его активации (полной или частичной) необходимо активировать ключ активации ПАКМ (ключ «3 из 5») – произвести процедуру ввода любых трех из возможных пяти защитных карт. Каждая из карт может иметь индивидуальный pin-код, вводимый с LCD панели ПАКМ. При этом автоматически активируются ключи шифрования ПАКМ, на которых зашифрованы все закрытые ключи/ключи ЭП пользователей, включая ключ TLS сервера ПАКМ (можно устанавливать соединения с ПАКМ), ключ подписи ПАКМ (можно выпускать сертификаты ключей доступа ПАКМ) и закрытые ключи/ключи ЭП пользователей (пользователи могут использовать свои ключи для формирования ЭП).

3. УСТАНОВКА ПАКМ

ПАКМ «КриптоПро HSM» представляет собой сложное сетевое устройство, работающее под управлением операционной системы, специализированного программного обеспечения и, кроме того, являющееся средством хранения данных. Поэтому, как и для любого подобного компьютерного устройства очень важно соблюдать требования к среде и правилам его эксплуатации. Внезапное непреднамеренное или неправильное отключение питания может приводить к потерям данных и разрушениям структур файловой системы ОС.

Перед установкой и началом использования ПАКМ внимательно ознакомьтесь с эксплуатационной документацией на ПАКМ, а также следующими важными правилами установки и эксплуатации ПАКМ:

1. Используйте источники бесперебойного питания (**ИБП**).
2. Для выключения работающего устройства при невозможности сделать это штатно с использованием LCD-панели используйте только **кнопку включения/отключения питания** на передней панели корпуса ПАКМ. Одно кратковременное нажатие на неё вызывает процедуру корректного завершения процессов с сохранением данных.
3. Не выдергивайте шнур питания, не выключайте ИБП пока ПАКМ «КриптоПро HSM» не завершит работу и не выключится.



4. Вовремя создавайте **резервные копии данных (РК) устройства**. Резервные копии создаются и сохраняются на отдельном флэш диске ПАКМ, менее подверженном каким-либо разрушениям. Имея актуальную резервную копию, даже внутри ПАКМ, наши специалисты смогут помочь вам в восстановлении работоспособности вашего устройства с сохранением ключевой информации, либо подмененного аппаратного модуля с актуальными данными из резервной копии. Создавайте резервную копию сразу после изменения служебной ключевой информации (плановой смены разделенного ключа активации, корневого ключа, ключа TLS сервера ПАКМ).
5. Бережно относитесь к **смарт-картам разделенного ключа активации**. Потеря, порча, зачистка более двух карт действующего разделенного ключа

приведет к невозможности эксплуатации устройства, к потере (невозможности расшифровать) всех хранимых внутри ПАКМ ключевых контейнеров.

6. Ответственно относитесь к процедуре создания и плановой смены ключа активации ПАКМ. **Обеспечьте непрерывность подачи электропитания на устройство** на всё время выполнения этой операции.
7. **При начальной инициализации** устройства заранее подготовьте комплект смарт-карт, зачистите их при необходимости и промаркируйте. В случае возникновения неисправимой ошибки в момент создания ключа активации произойдет откат ПАКМ к неинициализированному состоянию. Однако после успешного создания ключа активации дальнейшие возможные ошибки уже не приведут к откату. В этом случае не зачищайте карты ключа активации, иначе эксплуатация устройства будет невозможна. Вы можете корректно (с использованием кнопки питания ПАКМ) выключить ПАКМ, загрузить его снова и, используя только что созданный ключ активации, зайти в меню LCD-панели ПАКМ и продолжить процесс инициализации: создание привилегированных пользователей (администраторов ПАКМ), корректировку настроек сети, межсетевого экрана и др.
8. Помните, что из меню LCD-панели происходит автоматический выход, если в течение одной минуты не нажималось ни одной аппаратной кнопки на LCD-панели (не производилась навигация по меню).
9. **При плановой смене ключа активации** не зачищайте комплект карт старого ключа до тех пор, пока не убедитесь в работоспособности нового ключа и не создадите образ резервной копии данных ПАКМ, перешифрованных на новом ключе.
10. Резервная копия актуальна, только если существует соответствующий ей ключ активации (действующий на момент создания РК комплект защитных карт разделенного ключа) и соответствующий ключ защиты РК.

3.1. Порядок установки ПАКМ

Для установки ПАКМ «КриптоПро HSM» необходимо выполнить следующую последовательность действий:

1. Распаковать изделие;
2. Проверить комплектацию изделия;
3. Подключить изделие к сегменту локальной сети, либо к серверу и линиям электропитания;
4. Произвести инициализацию ПАКМ;

5. Завести учетные записи привилегированных пользователей ПАКМ: администратора, аудитора, администратора резервного копирования (при необходимости, т.к. все функции привилегированных пользователей с LCD панели может выполнять **суперпользователь** — 3 из 5 доверенных лиц, держателей защитных карт разделенного ключа активации);
6. При необходимости создать учетные записи Администраторов платежной системы (как минимум двоих);
7. Произвести сетевые настройки ПАКМ;
8. Произвести настройки (проверить корректность) системного времени ПАКМ;
9. При изменении сетевых настроек (IP-адресов интерфейсов ПАКМ) перевыпустить сертификаты TLS сервера ПАКМ.
10. Добавить необходимое число учетных записей привилегированных пользователей для работы через Web интерфейс администрирования, и сформировать для них ключи и сертификаты аутентификации на смарт-картах.
11. При необходимости выпустить на ПАКМ комплект рабочих карт канала «К» для подключения серверов приложений по каналу К (согласно процедуре, описанной в п. 5.3.8);
12. Произвести установку программного обеспечения интерфейсных модулей для взаимодействия с ПАКМ на рабочих станциях пользователей/серверах, автоматизированном рабочем месте администратора ПАКМ (Web интерфейс);
13. Произвести запуск Web интерфейса администратора, произвести дополнительные настройки ПАКМ, добавить тестового пользователя и сформировать для него ключи и сертификат аутентификации;
14. При помощи Web интерфейса Администратора ПАКМ или пункта меню «License(s)» LCD панели установить PKI HSM лицензию на базовые программные модули (БПМ) ПАКМ. Без этого ПАКМ «КриптоПро HSM» не может быть переведен в активное состояние (FULL ACTIVE), и доступ к нему по сети со стороны пользователей криптографического модуля будет запрещен, за исключением Web интерфейса Администратора ПАКМ. Web интерфейс работает в состоянии ПАКМ – ADMIN_ONLY;
15. При необходимости с помощью Web интерфейса Администратора ПАКМ установить лицензию для PCI HSM (использование ПАКМ в качестве Платежного HSM). Платежные сервисы могут быть запущены в состоянии ПАКМ – ADMIN_ONLY;
16. В случае использования ПАКМ в качестве СКЗИ (PKI HSM) произвести тестовый запрос на генерацию ключа подписи пользователя с рабочего места

пользователя. После чего удалить тестовые ключи пользователя и Пользователя в ПАКМ.

3.2. Проверка комплектации и подключение ПАКМ

После распаковки необходимо проверить комплектацию устройства. Комплектация должна соответствовать указанной в прилагаемой эксплуатационной документации («ЖТЯИ.00096-03 30 01. Формуляр»).

Подключить интерфейсный кабель между Сервером и ПАКМ, либо между ПАКМ и сетевым устройством (хабом, маршрутизатором, концентратором).

Подключить интерфейсный кабель между ПАКМ и компьютером рабочего места администратора. Опционально.

Подключить кабель электропитания ПАКМ.

На панели управления ПАКМ нажать клавишу включения питания.

Выполнить действия по включению ПАКМ (см. раздел 4)

3.3. Инициализация ПАКМ

После включения и загрузки ПАКМ, LCD меню будет отображать текущее состояние ПАКМ (INACTIVE) и строчку с кодом последнего события в журнале событий. Если в этом состоянии нажать любую кнопку LCD меню, то на экран будет выдан запрос «Init HSM? Yes/No». При выборе опции «NO» ПАКМ автоматически перейдет в состояние выгрузки и выключения (Halt).

Если же будет выбран ответ «YES», то начнется процедура инициализации ПАКМ:

- формирование ключа активации ПАКМ по схеме разделения секрета «3 из 5» (означает, что для активации ПАКМ могут быть использованы любые 3 защитные карты из пяти сформированных). Защитные ключи записываются на смарт-карты. Смарт-карты раздаются доверенным лицам. Данные доверенные лица могут выполнять роли привилегированных пользователей ПАКМ: Администраторов, Аудиторов, Администраторов резервного копирования ПАКМ;
- формирование ключа шифрования ключей подписи пользователей, хранящихся в ПАКМ, защищенного на ключе активации ПАКМ (производится в автоматическом режиме);
- формирование ключа подписи ПАКМ и самоподписанного сертификата, зашифрованного на ключе шифрования ПАКМ (производится в автоматическом режиме);
- формирование ключа и сертификата аутентификации TLS сервера, зашифрованного на ключе шифрования ПАКМ (производится в автоматическом режиме);
- формирование ключа подписи журнала аудита ПАКМ, зашифрованного на

ключе шифрования ПАКМ, и соответствующего сертификата (производится в автоматическом режиме);

Внешне это будет выглядеть следующим образом:

На LCD будут поочередно выдаваться запросы на вставку и ввод pin-кодов для 5 защитных карт ключа активации ПАКМ.

После этого еще раз будут запрашиваться поочередно 5 защитных карт ключа активации для записи на них сформированных ключей.

Если в процессе выполнения процедуры инициализации ПАКМ какое-то действие будет произведено некорректно, ПАКМ откатывает все изменения к первоначальному состоянию (удаляет все созданные ключи, пользователей, фактически выполняет процедуру полной очистки ПАКМ (FullClean)) и процедуру инициализации можно будет начать заново. Но использованные смарт-карты необходимо будет зачистить вручную с использованием специальной утилиты, либо обратившись в организацию по сервисному обслуживанию ПАКМ.

Сразу после успешного создания разделенного ключа активации будет предложено создание первых пользователей ПАКМ. В данной процедуре следует создать привилегированных пользователей ПАКМ (Администратора, Аудитора, Администратора резервного копирования и других, при необходимости) и их ключи доступа на смарт-картах. Процедура добавления пользователя с использованием меню LCD панели описана в п.5.3.11. При возникновении ошибки в этой процедуре, не зачищайте защитные карты ранее успешно созданного разделенного ключа активации! Используя их, позже всегда можно войти в меню LCD панели и продолжить создание привилегированных пользователей. Рекомендуется, как минимум, создать двух Администраторов ПАКМ. При помощи смарт-карты одного из них можно будет входить в меню LCD панели, а с картой другого Администратора можно будет подключаться к ПАКМ, используя Web доступ к настройкам ПАКМ (смарт-карта Администратора, используемая для Web доступа, может стать нефункциональной для входа в меню LCD панели, т.к. класс защиты ключевого контейнера будет понижен до уровня СКЗИ, используемого на APM Web администрирования ПАКМ).

После успешно проведенной процедуры инициализации ПАКМ доступ к LCD меню может быть осуществлен как с помощью смарт-карты аутентификации администратора ПАКМ (например, сформированной на последнем шаге процедуры инициализации) или, если таковые испорчены или заблокированы, с помощью ключа активации ПАКМ (при этом ПАКМ должен находиться в неактивном состоянии). Для доступа к LCD меню с помощью ключа активации необходимо нажать любую кнопку LCD меню, а в ответ на запрос карты Администратора ПАКМ, не вставляя карты, нажать любую клавишу ещё раз. При этом будет выдан запрос на использование ключа активации («Use 3 of 5?»).

Если ПАКМ находится в одном из активных состояний, то в ответ на повторное нажатие без вставки смарт-карты администратора на LCD будет выдан запрос на корректное выключение ПАКМ (Halt), что очень важно для сохранения целостности данных ПАКМ.

3.4. Установка сетевых настроек ПАКМ

Аппаратная платформа ПАКМ «КриптоПро HSM» имеет 2 сетевых оптических интерфейса (в отдельных случаях по согласованию сторон допускается установка ещё одного оптического сетевого интерфейса). Одновременно могут быть задействованы оба интерфейса. Необходимо один интерфейс использовать для прямого подключения рабочей станции с Web интерфейсом администрирования ПАКМ, отдельный интерфейс – для подключения сервера/группы серверов и для обслуживания криптографических запросов от рабочих станций обычных пользователей. Если Web интерфейс не используется, то свободный интерфейс можно использовать для другой подсети пользователей, либо для разделения подключений серверов и рабочих станций пользователей, либо просто не задействовать, оставить в резерве на случай выхода из строя какого-либо рабочего интерфейса. При выходе из строя рабочего интерфейса, возможно придется переконфигурировать сеть и настройки межсетевого экрана.

В сетевом сегменте ПАКМ имеет заданные по умолчанию (изготовителем) IP-адреса интерфейсов: <192.168.26.2>, <192.168.27.2>.

Предполагается, что сервер и/или рабочая станция Web администрирования, подключаемые напрямую к ПАКМ, в этом локальном сетевом сегменте (по умолчанию) имеют IP-адреса: <192.168.26.1> или <192.168.27.1>.

Кроме адресов для всех интерфейсов задаются: маска и, возможно, доп. параметры (скорость, дуплекс). Таким образом существует возможность описывать подключаемые подсети.

Отдельно задается шлюз (gateway), используемый по умолчанию.

При необходимости сетевые настройки ПАКМ всегда могут быть изменены Администратором через LCD-панель (см. п. 6.2.4) или с использованием web-интерфейса.

Кроме сетевых настроек, необходимо установить правила межсетевого экрана для сетевого доступа к ПАКМ. Для каждого порта (1501 – порт «канала «K2»», 1502 – порт канала «K», 443 – порт для доступа с web-интерфейса администратора, 1503– порт канала «K2» для серверной группы с отключенным режимом шифрования в канале, 1505 для репликации (горячего резервирования)) указываются наборы IP-адресов, сетевых масок подсетей, с которых будет разрешен доступ к ПАКМ через заданный сетевой интерфейс.

Если вы изменяете IP-адрес ПАКМ любого сетевого интерфейса, то сразу после этого необходимо сменить ключ и сертификаты TLS сервера ПАКМ, т.к. поле CommonName сертификата TLS сервера содержит IP-адрес сетевого интерфейса ПАКМ. Это критично для работы канала «K2».

При этом надо иметь ввиду, что любое изменение ключевой информации, хранимой в ПАКМ (за исключением ключа активации ПАКМ), может быть осуществлено только в одном из активных состояний ПАКМ (ACTIVE или ADMIN_ONLY), т.к. вся ключевая информация прямым или косвенным образом зашифрована на ключе активации ПАКМ, а без его активации изменение невозможно осуществить.

Соответственно, после изменения IP-адреса интерфейса, возможно, потребуется переконфигурация правил межсетевого экрана.

3.5. Установка системного времени ПАКМ

Процедура установки времени описана в данном документе в разделе 5.3.4.

3.6. Выпуск карты локального защищенного канала (канала «K»)

Для защиты информации, циркулирующей между Серверами приложений на базе операционных систем семейства Unix/Linux и ПАКМ, в системе организуется специальный локальный защищенный канал (канал K), работающий в локальном сетевом сегменте Ethernet между ПЭВМ Сервера и ПАКМ. Для активации этого канала на ПАКМ должна быть выпущена карта с ключом сетевой аутентификации. Во время взаимодействия Сервера и ПАКМ эта карта должна быть вставлена в считыватель на Сервере.

Канал K – специальный канал, используемый специально разработанными приложениями. Для обычного использования ПАКМ в качестве СКЗИ следует использовать канал K2.

Процедура выпуска карт канала «K» описана в данном документе в п. 5.3.8.

После перевыпуска карт канала «K» ранее выпущенные карты становятся недействительными.

3.7. Установка интерфейсных модулей

В процессе установки используется установочный комплект ПО «Клиент КриптоПро HSM», позволяющий инсталлировать на рабочую станцию/Сервер интерфейс криптопровайдера ПАКМ.

Для функционирования сервиса криптопровайдера ПАКМ на сервере приложений требуется вставить в считыватель смарт-карт Сервера карту аутентификации (карта канала «K» или «K2»), выпущенную на ПАКМ.

Для функционирования сервиса криптопровайдера ПАКМ на рабочей станции пользователя/сервере приложений с установленной ОС семейства Windows требуется вставить в считыватель смарт-карт рабочей станции смарт-карту аутентификации (карта канала «K2») пользователя/администратора сервера, выпущенную на ПАКМ или на удаленном рабочем месте администратора ПАКМ, и активировать канал «K2», кликнув соответствующую иконку в системном трее ОС Windows (только для обычных пользователей). При использовании карты, имеющей в сертификате ключа аутентификации специальное расширение «Администратор сервера», запускающий криптосервис (возможно при загрузке ОС) обращается к карте и пытается установить соединение с ПАКМ. Никаких pin-кодов для доступа к карте при этом не запрашивается. На контейнер должен быть установлен pin-код с восемью единицами. Если в момент старта криптосервиса карта не вставлена, то в журнал событий сервера будет добавлена соответствующая запись.

3.8. Настройка удаленного рабочего места Web администрирования ПАКМ

Для более удобного управления ПАКМ используется удаленное рабочее место Web администрирования ПАКМ, позволяющее осуществлять все настройки ПАКМ, управлять пользователями, журналами ПАКМ удаленно по защищенному TLS протоколом каналу.

Интерфейс рабочего места администратора реализован в виде HTML страницы с использованием активных элементов управления и языка сценариев javascript. Для работы с активным содержимым HTML страницы требуется web-обозреватель на основе Chromium: Chromium-Gost, Yandex Browser, новый Microsoft Edge (chromium) с включенным режимом совместимости с Internet Explorer), а также Internet Explorer версии не ниже 7.

Взаимодействие рабочей станции администратора ПАКМ с ПАКМ осуществляется по стандартному HTTPS (TLS) протоколу с использованием российских криптографических алгоритмов.

Для этого на рабочую станцию администратора должен быть установлен криптопровайдер КриптоПро CSP версии 5.0 и выше (входит в комплект поставки ПАКМ).

Для генерации ключей доступа, запросов на сертификат ключа доступа, установки сертификата в контейнер используется расширение для указанных браузеров — КриптоПро ЭЦП Browser plug-in. Данное расширение можно скачать с сайта ООО «КРИПТО-ПРО» по ссылке <https://www.cryptopro.ru/products/cades/plugin>. Инструкция по установке, настройке и проверке корректности работы плагина приведена по ссылке <https://docs.cryptopro.ru/cades/plugin/plugin-installation-windows>.

Рабочая станция должна быть оснащена считывателем смарт-карт. Для некоторых операций, требующих подтверждения (путем формирования ЭП) вторым

привилегированным пользователем желательно иметь 2 считывателя смарт-карт. Один из которых всегда используется ключом на смарт-карте для поддержки TLS протокола, а второй для подписи данных подтверждаемых вторым привилегированным пользователем и для генерируемых ключей новых пользователей ПАКМ.

Для корректной работы TLS протокола на рабочей станции администратора должен быть установлен самоподписанный сертификат ключа подписи ПАКМ и сертификат ключа аутентификации удаленного администратора ПАКМ. Самоподписанный сертификат ключа подписи ПАКМ помещается в специальное расширение контейнера ключа аутентификации (администратора или любого пользователя) и при первоначальной настройке удаленного рабочего места Web администрирования может быть извлечен при помощи специальной утилиты (cardman), входящей в дистрибутив. Данная утилита представляет собой консольное интерактивное приложение и позволяет извлечь из расширений контейнера ключа аутентификации, находящегося на смарт-карте, сертификат ключа аутентификации пользователя и самоподписанный сертификат ПАКМ, содержащий открытый ключ, необходимый для проверки пользовательского сертификата.

Извлеченный таким образом самоподписанный сертификат ключа подписи ПАКМ должен быть установлен в доверенное хранилище корневых сертификатов ОС Windows стандартным образом.

Извлеченный сертификат пользователя должен быть установлен в личное хранилище пользователя в связке с закрытым ключом через Панель управления КриптоПро.

При смене ключа подписи ПАКМ новый корневой сертификат этого ключа может быть получен с использованием уже работающего Web интерфейса (в разделе «Сертификаты ПАКМ»).

После настройки удаленного рабочего места администратора необходимо в настройках ПАКМ разрешить использование web-интерфейса ПАКМ (установить опцию «Enable WEB»), а также внести IP-адрес и маску подсети рабочей станции администратора в настройки межсетевого экрана ПАКМ для порта № 443 и соответствующего сетевого интерфейса, перезапустить сервис межсетевого экрана («Restart FW») с использованием LCD меню.

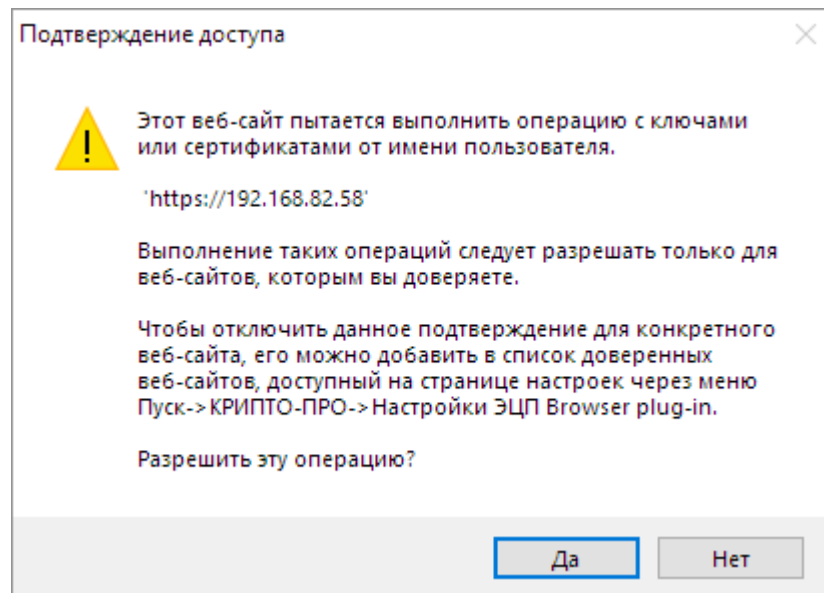
Если ПАКМ находится в неактивном состоянии, необходимо его активировать (перевести в любое из активных состояний ПАКМ: ACTIVE или ADMIN_ONLY).

После этого, введя в Интернет обозревателе URL ПАКМ в виде:

`https://<ip-адрес сетевого интерфейса Web администрирования ПАКМ>`,

с ПАКМ загрузится страница управления ПАКМ.

В некоторых режимах работы может выдаваться специальное предупреждение Браузера



Для корректной работы следует разрешить эту операцию.

3.9. Установка лицензий ПАКМ

После успешного запуска интерфейса Web Администрирования ПАКМ следует сразу ввести необходимые лицензии на использование модулей ПАКМ.

Без каких-либо установленных лицензий будет доступен только режим настройки HSM, либо через меню LCD панели, либо с использованием APMa Web администрирования ПАКМ (доступно в состоянии ПАКМ - ADMIN_ONLY). Перевод ПАКМ в состояние ACTIVE (FULL ACTIVE) невозможно. Запуск платежных сервисов невозможен.

Существует два возможных вида лицензий:

- Лицензия на PKI HSM;
- Лицензия на PCI HSM.

Лицензия на PKI HSM является лицензией на базовые программные модули (БПМ). Должна устанавливаться всегда. Позволяет использовать ПАКМ в качестве разделяемого СКЗИ. Позволяет активировать каналы доступа пользователей к ПАКМ.

Лицензия на PCI HSM позволяет использовать ПАКМ в качестве Платежного HSM и активировать платежные сервисы.

Номера лицензий выдаются при приобретении ПАКМ.

Лицензии могут быть временными – на срок 3 месяца с момента первой установки, срочными – с указанием срока окончания действия лицензии, и бессрочными. Вся информация о виде лицензии и сроке её действия зашифрована в номере лицензии.

Для ввода номера лицензии необходимо в Web Интерфейсе Администрирования ПАКМ выбрать режим «Лицензии HSM». Там, кроме отображения информации об уже установленных лицензиях, есть поле ввода номера лицензии. Введите выданный номер,

нажмите Ок, и при успешном завершении операции информация о новой лицензии отобразится в списке.

В номере лицензии допускаются латинские буквы в верхнем регистре, цифры и символы «-» (дефис), без пробелов.

При невозможности использования интерфейса Web Администрирования ПАКМ, номера лицензий можно ввести, используя пункт основного меню LCD панели «License(s)». Для этого потребуется флэш диск («флэшка») с записанным в её корень текстовым файлом "LicenseSN", содержащим номер лицензии (только один). При необходимости ввести другой номер лицензии, то файл LicenseSN необходимо будет перезаписать на флэшку с новым номером и повторить процедуру установки лицензии.

3.10. Настройка ограничения использования алгоритма ГОСТ Р 34.10-2001

Для включения ограничения на использование алгоритма создания и проверки ЭП ГОСТ Р 34.10-2001 необходимо в Web интерфейсе ПАКМ указать следующие строки:

1. Для ограничения **создания ключа** ЭП ГОСТ Р 34.10-2001:

`https://<ip-адрес ПАКМ>/registry/putlonglong/config/parameters?warning_time_gen_2001=N`

где N — число (типа long long), соответствующее дате вступления действия ограничения на использования алгоритма.

2. Для ограничения **использования ключа** ЭП ГОСТ Р 34.10-2001:

`https://<ip-адрес ПАКМ>/registry/putlonglong/config/parameters?warning_time_sign_2001=N`

где N — число (типа long long), соответствующее дате вступления действия ограничения на использования алгоритма.

3.11. Параметры, устанавливаемые изготовителем

Параметрами, устанавливаемыми изготовителем, являются количество случайной информации (гаммы), используемой для генерации ключа ЭП или ключа шифрования пользователя (можно посмотреть на LCD панели ПАКМ, а также на странице информации ПАКМ web-интерфейса администратора ПАКМ).

Случайная информация расходуется при генерации ключа ЭП или ключа шифрования пользователя. Запас случайной информации рассчитан на плановый срок эксплуатации ПАКМ, определенный заказчиком. При расходе случайной информации сверх расчетного следует обратиться на предприятие-изготовитель для пополнения объема.

3.12. Требования безопасности

При установке программного обеспечения интерфейсных модулей следует руководствоваться следующими рекомендациями:

- выполнить действия, предписываемые в «ЖТЯИ.00096-03 95 01. Правила пользования»;
- все устанавливаемое программное обеспечение ПЭВМ Серверов/рабочих станций, которые будут подключаться ПАКМ, должно быть лицензионно чистым, при этом не допускается наличие средств разработки и отладки программ;
- для обеспечения защиты от НСД ПЭВМ должен использоваться АПМДЗ (для исполнений с уровнем защиты КС2 и выше);
- должны быть предприняты меры, препятствующие извлечению платы защиты от НСД из ПЭВМ - системные блоки ПЭВМ должны быть опечатаны специально выделенной для этих целей печатью. Наряду с этим допускается применение других средств контроля доступа к ПЭВМ;
- к эксплуатации программного обеспечения допускаются лица, прошедшие соответствующую подготовку и изучившие эксплуатационную документацию на установленные программные средства.

После завершения процесса установки должны быть выполнены действия, необходимые для осуществления регулярного контроля установленного программного обеспечения с помощью ПО контроля целостности АПМДЗ.

Контроль целостности должен охватывать следующие файлы:

- ПО интерфейсных модулей;
- драйверы устройств и портов ввода смарт-карт, com-порта, сети Ethernet;
- программы отображения log-файлов;
- драйвер ПАК «Соболь».

В составе аппаратных средств ПАКМ применяется АПМДЗ для обеспечения защиты от НСД и контроля целостности установленного в нем ПО.

Ключи АПМДЗ ПАКМ администратор безопасности должен выдавать лицам, выполняющим работу с использованием ПАКМ, осуществляющим включение и загрузку ПАКМ.

Ключи АПМДЗ ПАКМ относятся к категории ключевых носителей, подлежат соответствующему учету и хранению (подробнее см. «ЖТЯИ.00096-03 95 01. Правила пользования»).

4. ВКЛЮЧЕНИЕ ПАКМ

Предварительные условия:

1. ПАКМ подключен к Серверу в соответствии с разделом 3.
2. У администратора, осуществляющего включение, имеется в наличии ключ АПМДЗ («таблетка»).
3. Питание ПАКМ выключено.

Действия администратора:

1. Нажать кнопку включения питания.
2. Ожидать появления на LCD надписи <Loading>.
3. Приложить «таблетку» к считывателю АПМДЗ и поддержать в течение 10 сек.
4. Примерно через 1 мин. на LCD панели ПАКМ начнет отображаться процесс загрузки и проверки контрольных сумм базового и прикладного ПО ПАКМ (в процентах). Таблетку при этом можно отпустить.
5. Ждать появления надписи, показывающей текущее состояние ПАКМ (INACTIVE), означающей, что процедуры загрузки пройдены, завершена загрузка ОС и прикладного ПО ПАКМ.
6. ПАКМ включен.

5. АДМИНИСТРИРОВАНИЕ ПАКМ

Администрирование ПАКМ производится привилегированным пользователем ПАКМ при предъявлении (а именно - помещении в считыватель ПАКМ) действующей карты привилегированного пользователя ПАКМ (Администратора, Аудитора или Администратора резервного копирования) и вводе pin-кода карты. Некоторые действия могут производиться только Суперпользователем ПАКМ, то есть, 3 из 5 доверенных лиц, при предъявлении карт с частями ключа активации и вводе pin-кодов.

5.1. Ввод pin-кода

При работе с картами на ПАКМ требуется вводить pin-код с помощью LCD панели.

На панели ПАКМ отображается меню ввода pin-кода в виде ряда из 8 знаков, где «*» обозначает уже введенный символ, «X» – еще не определенный символ, вводимый символ подсвечивается мигающим полем курсора.

После выбора всех 8 цифр pin-кода, при необходимости, автоматически происходит переход к следующим возможным запросам.

- На LCD-панели отображается запрос («Input pin-code») на ввод pin-кода для считывания карты. (8 знаков).

Курсор находится в крайней левой позиции, соответствующей первой цифре pin-кода. В окне выводится случайная начальная цифра. Нажатие клавиши «Вверх» на LCD-панели приводит к увеличению цифры на 1, нажатие клавиши «Вниз» - к уменьшению на 1. По клавише «Enter» LCD-панели введенная цифра сохраняется, курсор переходит на позицию вправо, ввод повторяется для следующей цифры pin-кода. Клавиша «Влево» возвращает к вводу предыдущей цифры (ввод снова начинается со случайного значения). В любой момент времени введенными считаются все цифры слева от курсора, не введенными - все цифры справа от курсора, вводимой - цифра в позиции курсора. Клавиша «Вправо» не влияет на ввод. Если нажать клавишу «Влево» при текущем расположении курсора в крайней левой позиции, будет выведено меню «Return to input?» («Повторить ввод?») с предложенным выбором «YES» («ДА») или «NO» («НЕТ»). При выборе ответа «YES» ввод pin-кода будет повторен сначала, при выборе ответа «NO» ввод pin-кода будет досрочно неуспешно завершен. При нажатии клавиши «Enter» в крайней правой позиции ввода pin-код считается успешно введенным, ввод завершается.

- В случае успешного ввода pin-кода ПАКМ считывает/записывает карту. Если pin-код введен ошибочно, то запрос на ввод pin-кода повторится. Максимальное число попыток ввода pin-кода 3, после чего смарт-карта будет заблокирована и использование записанных на неё ключей будет невозможно.

5.2. Возможные меню LCD панели ПАКМ

В ПАКМ существует несколько возможных меню LCD панели.

- Основное меню администрирования (управления) ПАКМ
- Меню платежной системы
- Меню неавторизованных операций

Все три меню доступны после успешной инициализации ПАКМ.

Вход в основное меню администрирования ПАКМ осуществляется нажатием любой кнопки LCD панели за исключением «Стрелки вниз» и предъявлением смарт-карты либо Администратора ПАКМ, либо Аудитора ПАКМ, либо администратора резервного копирования ПАКМ, либо по трем из пяти карт «суперпользователя ПАКМ».

Вход в меню платежной системы осуществляется нажатием любой кнопки LCD панели за исключением «Стрелки вниз» и предъявлением смарт-карты Администратора платежной системы.

Вход в меню неавторизованных операций осуществляется нажатием кнопки «стрелка вниз» LCD панели.

В зависимости от состояния ПАКМ некоторые пункты меню могут быть скрыты или недоступны.

5.3. Работа с LCD меню администрирования ПАКМ

Для входа в меню Администратор, Аудитор или Администратор резервного копирования ПАКМ должен нажать любую клавишу на LCD-панели (стрелки перемещения курсора, Enter), дождаться приглашения «Insert the Card», вставить действующую карту привилегированного пользователя ПАКМ в считыватель ПАКМ, снова нажать любую клавишу на панели, и затем в ответ на запрос ввести pin-код.

В неактивном состоянии ПАКМ имеется вариант входа в меню с правами Суперпользователя ПАКМ, с использованием карт ключа активации лиц по схеме 3 из 5. Для этого после приглашения «Insert the Card» надо нажать на LCD-панели любую клавишу, не вставляя карту. После этого на панели появится вопрос «No card.Use 3/5?», на который надо ответить «YES». Затем 3 из 5 доверенных лиц должны, следуя приглашениям на LCD-панели, вставить карты с частями ключа активации и ввести pin-коды. После этого ПАКМ перейдет в режим «Только администрирование», и дальнейшие действия будут производиться с правами Суперпользователя ПАКМ.

В активном состоянии или в состоянии «Только администрирование» при невозможности использования карты администратора существует возможность корректной остановки ПАКМ через LCD-панель. Для этого после приглашения «Insert the Card» надо нажать на LCD-панели любую клавишу, не вставляя карту. После этого на панели

появится вопрос «No card. Halt?», на который надо ответить «YES», затем появится вопрос «Really halt?», на который надо ответить «YES».

Выход из меню происходит по завершении времени ожидания (тайм-аут), по нажатию клавиши «Влево», или по команде меню «Exit» («Выход»).

Структура меню (в скобках приводится текст надписи на LCD панели):

- изменение состояния ПАКМ (Change HSM State)

Включает подменю:

- Неактивное состояние (Inactive);
- Активное состояние (Full active);
- Только администрирование (Admin only);
- Выключить HSM (Halt);

- показ сообщений журнала событий (View Log);

- смена Pin-кода на карте (Change pin-code);

- установка часового пояса (Change timezone);

- установка системного времени ПАКМ (Set system time);

- установка системной даты ПАКМ (Set system date);

- показ системных характеристик ПАКМ (View system parameters)

Включает подменю:

- Системное время (View sys.time);
- Просмотр сетевых настроек, для просмотра текущих сетевых настроек ПАКМ (View net. par.);
- Остаток доверенной случайной информации, используемой для генерации ключей пользователей (Gamma for keys);
- Свободное место на диске, в килобайтах (Free on disk, KB);
- Количество созданных за все время эксплуатации ПАКМ ключей

Уполномоченных Лиц (для УЦ на базе ОС семейства Unix) (Made root keys);

- Количество криптографических операций за все время эксплуатации ПАКМ (Crypt. oper-s);
- Количество карт канала «K», созданных во время последней сессии создания мастер-ключей (Made cards K);
- Количество мастер-ключей аутентификации, созданных за все время эксплуатации ПАКМ (Changes Kcards);

- Общее количество созданных за все время эксплуатации ПАКМ ключей пользователей (Keys made);
- Номер версии сборки дистрибутива ПО ПАКМ (Build);
- Выход из подменю (Exit).
- **очистка содержимого ПАКМ (Full Clean);**
- **выход из меню администрирования (Exit);**
- **смена мастер-ключа аутентификации и выпуск карт канала «К» (Make cards K);**
- **изменение сетевых настроек (Set up network)**

Включает подменю:

Eth0 (первый сетевой интерфейс)

Eth1 (Если присутствует. Второй сетевой интерфейс)

Настройка каждого сетевого интерфейса включает:

- IP-адрес (ip_address);
- маска подсети (net_mask);
- шлюз локальной сети (gateway);
- настройка режима передачи данных (media),

Включает режимы:

- Полный дуплекс, скорость 1000 Mb/сек (1000mbps_fd);
- Полудуплекс, скорость 1000 Mb/сек (1000mbps_hd);
- Полный дуплекс, скорость 100 Mb/сек (100mbps_fd);
- Полудуплекс, скорость 100 Mb/сек (100mbps_hd);
- Автоопределение (autosense);

- просмотр и изменение параметров ПАКМ (HSM options)

Включает подменю:

- Разрешить администрирование через сеть (Enable web);
- Разрешить использование канала K2 (Enable K2);
- Разрешить использование канала K2s (Enable K2s);
- Подробное журналирование (Detail event log);
- Установить автоочистку журнала аудита (Autoclean audit log);

- Пороговое значение количества записей журнала аудита (Audit log max records count);
- Интервал проверки журнала аудита на переполнение, в секундах (Autoclean poll interval);
- таймаут неактивных соединений (Timeout Idle);
- Максимальное количество соединений (Max clients);
- Разрешить загрузку резервных копий (Enable upload);
- Режим синхронизации базы данных журнала аудита (Audit sync mode);
- Регистрируемые события (Logged events);
- Тип сервера репликации (Repl Server Type);
- Идентификационный номер сервера репликации (Repl Server ID);
- IP-адрес MASTER сервера репликации (Repl Master IP);

- управление пользователями (User management)

Включает подменю:

- Добавление пользователя (Add user);
- Удаление пользователя (Delete user);
- Заблокировать пользователя (Lock user);
- Разблокировать пользователя (Unlock user);
- перевыпустить ключ и сертификат доступа пользователя (Change user card);
- Импортировать ключ пользователю со смарт-карты (Import user key);

- настройки межсетевого экрана (FW settings)

Включает подменю:

- Канал К (K channel);
- Канал К2 (K2 channel);
- Сетевой администратор (Remote admin);
- Репликация (Replication);

- Смена служебных ключей и сертификатов ПАКМ (Update keys)

Включает подменю:

- Смена ключа активации (ACT(ivation) key);
- Смена корневого сертификата ПАКМ (CA key);
- Смена сертификата TLS сервера ПАКМ (TLS server key);
- Смена ключа администратора (ADM(in) key);
- **корректная очистка журнала аудита (Clear audit log);**
- **Перезапуск репликации ПАКМ в системе горячего резервирования (Restart repl-n);**
- **зачистка смарт-карты (Clear smart card);**
- **восстановление журнала аудита (Repair audit log);**
- **резервное копирование и восстановление ПАКМ (Backups).**
- **Смена пароля для доступа к режиму полной очистки ПАКМ в меню неавторизованных операций (Change password).**
- **Ввод лицензии на использование ПАКМ (License(s)).**

5.3.1.Изменение состояния ПАКМ

Данная процедура доступна для пользователя с правами Администратора ПАКМ.

Предварительные условия:

1. ПАКМ находится во включенном состоянии.
2. Администратор имеет при себе действующую карту администратора, либо (если ПАКМ находится в неактивном состоянии) присутствуют 3 из 5 доверенных лиц с картами ключа активации.

Для изменения состояния ПАКМ:

1. Администратор нажимает на любую клавишу на LCD-панели ПАКМ.
2. На LCD появляется приглашение: «Insert the Card, Press any key...»
3. Администратор вставляет карту администратора в считыватель ПАКМ.
Администратор нажимает на любую клавишу на LCD-панели ПАКМ.
4. На LCD появляется приглашение: «Input pin-code».
5. Администратор вводит pin-код карты.
6. ПАКМ переходит в режим меню.

В неактивном состоянии ПАКМ возможен альтернативный вариант входа в меню с использованием карт ключа активации по схеме 3 из 5. Для этого после приглашения «Insert the Card» надо нажать на LCD-панели любую клавишу, не вставляя карту. После

этого на панели появится вопрос «No card. Use 3/5?», на который надо ответить «YES». Затем 3 из 5 доверенных лиц должны, следуя приглашениям на LCD-панели, вставить карты с частями ключа активации и ввести pin-коды. При этом ПАКМ автоматически перейдет в состояние «Активен для администратора» (ADMIN ONLY)

Если по какой-либо причине у вас не оказалось ни одной действующей карты администратора ПАКМ, войдите в меню ПАКМ с правами суперпользователя с помощью карт ключа активации и выпустите новую карту Администратора ПАКМ или другого привилегированного пользователя.

Во время входа в меню на LCD-панели могут возникнуть сообщение, свидетельствующее об ошибочной ситуации: «Card not correct» (после пункта 3) - неправильная карта, или «Card not insert» – карта не вставлена.

7. Кнопками вверх/вниз администратор листает и кнопкой Enter выбирает пункт меню:
 - изменение состояния HSM (**Change HSM state**);
8. Происходит вход в подменю выбора состояния ПАКМ (текущее состояние в меню не входит). Кнопками вверх/вниз администратор листает и кнопкой Enter выбирает нужное состояние.

Варианты состояний HSM:

- неактивное состояние (ключи не активированы, каналы закрыты) – INACTIVE;
- активное состояние (ключи активированы, все разрешенные (в «HSM Options» и настройках брэндмауэра) каналы открыты) – FULL ACTIVE;
- только администрирование (ключи активированы, каналы закрыты, за исключением канала Web администрирования, и спец каналов платежного приложения) – ADMIN ONLY;
- остановка ПАКМ – HALT.

Для прекращения работы ПАКМ надо выбрать состояние - HALT. После этого на панели появляется вопрос «Really halt? YES [x] [x] NO». Стрелками вправо/влево надо переместить курсор на пункт «YES» и кнопкой Enter выбрать этот пункт.

После этого на LCD панели отображается индикация останова процессов ОС ПАКМ. Появление надписи halt на LCD панели означает окончание процесса останова. Питание ПАКМ можно выключить через 10сек. после появления этой надписи.

При выборе неактивного состояния (**Inactive**) на панели появляется вопрос «Make inactive? YES [x] [x] NO». Стрелками вправо/влево надо переместить курсор на пункт «YES» и кнопкой Enter выбрать этот пункт. После этого ПАКМ перейдет в неактивное состояние.

Для перехода в активное состояние или в состояние «только администрирование» из неактивного состояния необходимо присутствие 3 из 5 доверенных лиц с картами ключа активации.

При выборе активного состояния (**Full active**) на панели появляется вопрос «Full active?», на который надо ответить «YES». После этого на панели появится приглашение «Enter #1 of 5».

Если 1-е доверенное лицо присутствует, надо вставить его карточку в считыватель ПАКМ, переместить курсор на пункт «YES» и кнопкой Enter выбрать этот пункт, а затем в ответ на приглашение «Input pin-code» доверенное лицо должно ввести свой pin-код. Если 1-е доверенное лицо отсутствует, надо выбрать пункт «NO».

Далее появится приглашение «Enter #2 of 5», и процедура повторяется, пока не будут обработаны доступные 3 из 5 карт ключа активации.

При выборе состояния «Только администрирование» (**Admin only**) на панели появляется вопрос «Full active?», на который надо ответить «YES», и затем провести процедуру активации ключей по схеме «3 из 5», как описано выше.

Если ПАКМ уже находится в одном из активных состояний (FULL ACTIVE или ADMIN ONLY), то переход в другое активное состояние не требует повторной активации ключа «3 из 5».

При изменении состояния ПАКМ из одного из активных на «неактивное» (INACTIVE) будут остановлены сервисы, прослушивающие внешние порты, перезапущены основные криптографические сервисы, закрывая при этом все используемые ключевые контейнеры, и сервис управления ПАКМ. Поэтому ПАКМ при этом выйдет из режима меню.

При переходе из неактивного состояния в одно из активных может возникать ошибка. Это связано в основном с тем, что при таком изменении состояния начинают запускаться разрешенные каналы, и если в настройках сети имеется коллизия с настройками брэндмауэра, или срок действия ключа tls сервера для канала закончился, то данный канал не может стартовать и вся операция по изменению состояния откатывается. Следует проверить указанные настройки ПАКМ.

5.3.2. Показ сообщений журнала событий

Предварительные условия:

1. ПАКМ находится во включенном состоянии.
2. Администратор имеет при себе действующую карту администратора.

Для просмотра сообщений журнала событий:

1. Администратор входит в меню (как описано в п.5.3).

2. Клавишами вверх/вниз администратор листает и кнопкой Enter выбирает пункт меню:
 - показ сообщений журнала событий на LCD (**View log**);
3. Кнопками вверх/вниз на LCD-панели выбирает ту или иную запись из журнала событий (в обратном порядке, т.е. первыми показываются наиболее поздние сообщения).
4. Нажатие Enter приводит к запуску бегущей строки для данного сообщения (позволяет полностью просмотреть текст сообщения). Сообщение будет выводиться до таймаута. Для прекращения вывода бегущей строки необходимо два раза нажать клавишу «стрелка влево».

Во время просмотра журнала на LCD-панели могут возникать следующие сообщения, свидетельствующие об ошибочных ситуациях:

- «Read log error» (пункты 3,4) - ошибка чтения журнала.
- «View log error» (пункты 3,4) - ошибка вывода сообщений.

Данный режим устарел и используется для совместимости с ранее разработанными приложениями (базирующимися на использовании старого Канала К). Намного удобнее просматривать журнал событий с использованием Web интерфейса.

5.3.3. Смена pin-кода на карте

Данная процедура доступна для пользователя с правами Администратора ПАКМ.

Процедура выполняется во время плановой и внеплановой смены pin-кода (пароля) на карте с частью защитного ключа.

Процедуру проводит владелец карты (Доверенное лицо или Пользователь) под руководством администратора.

Предварительные условия:

1. Для смены pin-кода должен явиться владелец карты, для которой будет меняться pin-код, имея при себе саму карту.
2. Должен присутствовать администратор с действующей картой администратора ПАКМ.
3. ПАКМ должен находиться в активном состоянии или в состоянии «только администрирование».

Смена производится при помощи специальной опции меню (на LCD панели ПАКМ).

Смена Pin-кода на карте Доверенного лица или Пользователя:

1. Администратор входит в меню (как описано в п.5.3).

2. Клавишами вверх/вниз администратор листает и кнопкой Enter выбирает пункт меню:
 - смена Pin-кода на карте (**Change pin-code**);
3. На LCD отображается запрос – «Insert the Card, press any key...»
4. Владелец вставляет карту и нажимает любую клавишу на LCD-панели;
5. На LCD-панели отображается запрос («Input pin-code», «old pin») на ввод pin-кода для считывания карты. (8 знаков).
6. В случае успешного ввода pin-кода ПАКМ считывает карту. В противном случае сеанс изменения pin-кода завершается.
7. На ПАКМ отображается запрос («Input pin-code», «1 time:») pin-кода для смены. (8 знаков).
8. На ПАКМ отображается запрос pin-кода для смены - повторно («Input pin-code», «2 time:»). (8 знаков).
9. Если два введенных pin-кода совпадают, то ПАКМ записывает его на карту, выводит на LCD-экран надпись «pin was changed», и ожидает нажатия любой клавиши на LCD-панели, после чего выходит в главное меню.
10. Если pin-коды не совпали, то запрашивается повтор всей операции с п.7.

Во время смены pin-кода на LCD-панели могут возникать следующие сообщения, свидетельствующие об ошибочных ситуациях:

- «Card not insert» (после пункта 4) - ПАКМ не может найти карту в считывателе. После вывода сообщения сеанс изменения pin-кода будет завершен.
- «Pin is incorrect» (после пункта 5) - введен неправильный pin-код. После вывода сообщения сеанс изменения pin-кода будет завершен.
- «Pin's are differ» (после пункта 8) - введенные в пунктах 7 и 8 pin-коды различаются. После вывода сообщения будет выдано меню: «Reinput new pin?». При ответе «YES» сеанс будет повторен с пункта 7. При ответе «NO» и по таймауту будет осуществлено завершение сеанса изменения pin-кода.
- «Can't change pin» (после пункта 9) - ПАКМ не может изменить pin-код на карте. После вывода сообщения сеанс изменения pin-кода будет завершен.

5.3.4. Установка часового пояса ПАКМ

ПАКМ «КриптоПро HSM» работает по внутренним часам, настроенным на время UTC. Для удобства пользователей, эксплуатирующих ПАКМ, можно установить текущий часовой пояс, используя меню LCD панели. Тогда в delay режиме LCD панели время и дата будут отображаться с учетом настроек часового пояса. Также это время будет

использоваться для установки даты и времени ПАКМ (см. ниже в данном разделе). При отображении времени к нему добавляется суффикс в скобках индицирующий часовой пояс. Например, «(Msk)».

Время во всех журналах, время в изданных сертификатах ключей по-прежнему будет вестись по UTC.

Данная процедура доступна для пользователя с правами Администратора ПАКМ.

Предварительные условия:

1. ПАКМ находится во включенном состоянии.
2. Присутствует администратор ПАКМ с действующей картой администратора.

Для установки часового пояса:

1. Администратор входит в меню (как описано в п.5.3).
2. Клавишами вверх/вниз администратор листает и кнопкой Enter выбирает пункт меню (установка часового пояса):
 - установка часового пояса ПАКМ (**Change timezone**)
3. Кнопками вверх/вниз находит подходящий часовой пояс.
4. Нажатие Enter: подтверждение смены часового пояса и выход в основное меню.

5.3.5. Установка системного времени/даты ПАКМ

Данная процедура доступна для пользователя с правами Администратора ПАКМ.

Предварительные условия:

1. ПАКМ находится во включенном состоянии.
2. Присутствует администратор ПАКМ с действующей картой администратора.

Для установки (или корректировки) системного времени (системная дата устанавливается и корректируется аналогичным образом):

5. Администратор входит в меню (как описано в п.5.3).
6. Клавишами вверх/вниз администратор листает и кнопкой Enter выбирает пункт меню (установка системного времени или установка системной даты):
 - установка системного времени ПАКМ (**Set system time**) или
 - установка системной даты ПАКМ (**Set system date**);
7. Кнопками вверх/вниз увеличивает или уменьшает число.
8. Кнопками вправо/влево изменяет положение курсора (переход по цифрам индикации времени).

9. Нажатие Enter: индикация сообщения «Save time?» (для даты – «Save date?»)
10. Кнопками Вправо/Влево – выбор: «YES?» и «NO».
11. Нажатие кнопки Enter – выбор пункта YES / NO. И приводит к переходу в основное меню.

При корректировке времени ПАКМ более чем на 5 минут в любую сторону ПАКМ должен быть перегружен!

Примечание. Время в данной процедуре учитывается и отображается в соответствии с настройкой часового пояса.

5.3.6. Показ системных характеристик

Данная процедура доступна для любого привилегированного пользователя ПАКМ.

Предварительные условия:

1. ПАКМ находится во включенном состоянии.
2. Присутствует администратор ПАКМ с действующей картой администратора.

Для просмотра системных характеристик:

1. Привилегированный пользователь входит в меню (как описано в п.5.3).
2. Клавишами вверх/вниз пользователь листает и кнопкой Enter выбирает пункт меню:
 - показ системных характеристик ПАКМ (**View system parameters**);
3. Кнопками вверх/вниз на панели прокручиваются системные характеристики:
 - Системное время ПАКМ;
 - Сетевые настройки ПАКМ;
 - Серийный номер ПО ПАКМ.
4. Нажатие кнопки Enter или стрелки влево/вправо приводит к выходу в главное меню.

5.3.7. Очистка содержимого ПАКМ

Данная процедура доступна только для пользователя с правами Администратора ПАКМ.

Данный режим приводит ПАКМ в состояние «до инициализации». При этом уничтожаются все ключи пользователей ПАКМ, все пользователи ПАКМ, очищаются журналы, удаляются служебные ключи ПАКМ (подписи, TLS сервера, шифрования). После завершения процедуры очистки ПАКМ автоматически перейдет в состояние HALT и

завершит свою работу. В дальнейшем, при попытке активирования ПАКМ будет выдан запрос на начальную инициализацию ПАКМ (см. п. 3.3).

Предварительные условия:

1. ПАКМ включен.
2. ПАКМ находится в неактивном состоянии.
3. Присутствует Администратор ПАКМ с личной картой доступа.

Для очистки содержимого ПАКМ:

1. Производится вход в меню с использованием карты доступа Администратора ПАКМ;
2. Клавишами вверх/вниз пользователь листает и кнопкой Enter выбирает пункт меню:
 - очистка содержимого ПАКМ (**Full clean**);
3. На LCD панели появляется сообщение «Full Clean? YES [x] [x] NO». Стрелками вправо/влево надо переместить курсор на пункт «YES» и кнопкой Enter выбрать этот пункт. После этого появится сообщение «Really Clean? YES [x] [x] NO». Нужно выбрать пункт «YES».
4. На LCD панели отображается сообщение об окончании очистки содержимого ПАКМ и завершении работы ПАКМ (halting).
5. Пользователь выключает ПАКМ, нажимая на кнопку питания.

Если в сертификате ключа доступа, хранящемся на карте Администратора ПАКМ, не указано соответствующее расширение (пользователь исполняет роль «Администратора ПАКМ»), то на LCD панель будет выдано сообщение «Access denied».

Если ПАКМ находится в одном из активных состояний, то при выборе данного режима на LCD панель будет выдано сообщение «Invalid HSM state». **Внимание!** При входе в режим управления ПАКМ через LCD панель суперпользователем (при предъявлении 3 из 5 карт защиты ключа активации) ПАКМ автоматически переходит в активный режим – ADMIN-ONLY, а значит выполнить операцию full clean в данном случае невозможно.

При неудачной инициализации ПАКМ (например, в случае сбоя питания), или в случае порчи карт доверенных лиц ПАКМ может оказаться в «неопределенном» состоянии, из которого обычными штатными методами его вывести невозможно. Для того, чтобы привести его в неинициализированное состояние, процедуру full clean можно выполнить из меню неавторизованных операций, используя специальный пароль для этого случая (см. раздел «Работа с Меню неавторизованных операций»).

5.3.8.Смена мастер-ключа аутентификации/выпуск карт канала «К»

Данная процедура доступна для пользователя с правами Администратора ПАКМ.

Предварительные условия:

1. ПАКМ перезагружен и находится во включенном состоянии.
2. Ни один из пользователей не активировал свой ключ в ПАКМ.
3. Администратор имеет при себе карты для записи нового ключа канала «К» (новые, предназначенные для записи, или ранее выпущенные – возможна перезапись ключа канала «К» на место ранее выпущенного).
4. Администратор имеет при себе одну действующую карту администратора ПАКМ.

Для выпуска карты канала «К» (плановой или внеплановой смены ключа аутентификации канала «К»):

1. Администратор входит в меню (как описано в п.5.3).
2. Клавишами вверх/вниз администратор листает и кнопкой Enter выбирает пункт меню:
 - создание мастер-ключа аутентификации и выпуск карт канала «К» (**Make cards K**);
3. ПАКМ создает новый ключ канала «К».
4. На LCD высвечивается надпись – «Insert new Card, Press any key...»
5. Вставляется новая чистая карта канала «К» (не использовавшаяся ранее в данном сеансе выпуска карт и не являющаяся картой с текущим ключом канала К), нажимается любая клавиша на LCD-панели.
6. На LCD высвечивается надпись – «Enter - write key, any key - exit». Нажатие Enter на LCD-панели начнет запись ключа на карту (пункт 7), нажатие любой другой клавиши на LCD-панели приведет к завершению записи карт и переходу к пункту 9.
7. ПАКМ записывает на карту новый ключ.
8. Если карта записана успешно, на LCD отображается серийный номер карты, происходит переход к пункту 4.
9. Если записана хотя бы одна карта, происходит установка нового ключа (старый при этом уничтожается) и завершение сеанса выпуска карт.

После выполнения выпуска карты канала «К» «старые» карты (ранее выпущенные) становятся недействительными.

Во время выпуска карт на LCD-панели могут возникать следующие сообщения, свидетельствующие об ошибочных ситуациях:

- «Can't create key» (после пункта 3) - ошибка создания ключа. После вывода этого сообщения сеанс автоматически завершается.
- «Card is absent» (после пункта 4) - ПАКМ не может обнаружить карту в считывающем устройстве. После вывода сообщения будет выведено меню «Try again?». В случае ответа «YES» сеанс повторится с пункта 4. В случае ответа «NO» (а также по таймауту) будет осуществлен переход к пункту 9.
- «Card already used» (после пункта 6, в случае нажатия Enter, или после пункта 7) - карта либо использовалась ранее для записи ключа в данном сеансе, либо является картой с текущим ключом. После вывода сообщения будет осуществлен переход к пункту 4.
- «Can't write card» (после пункта 7) - ключ не был записан на карту. После вывода сообщения будет выведено меню «Continue?». В случае ответа «YES» сеанс повторится с пункта 4. В случае ответа «NO» (а также по таймауту) будет осуществлен переход к пункту 9.
- «Can't change key» (после пункта 9) - ПАКМ не может изменить ключ. После вывода сообщения сеанс будет завершен.

5.3.9.Просмотр и изменение сетевых настроек

Просмотр сетевых настроек доступен для любого привилегированного пользователя ПАКМ. Изменение настроек доступно для пользователя с правами Администратора ПАКМ.

Предварительные условия:

1. ПАКМ находится во включенном состоянии.
2. Привилегированный пользователь имеет при себе действующую карту пользователя или администратора ПАКМ.

Для изменения сетевых настроек:

1. Пользователь входит в меню (как описано в п.5.3).
2. Клавишами вверх/вниз пользователь листает и кнопкой Enter выбирает пункт меню:
- изменение сетевых настроек (**Setup network**);
3. Нажимая стрелки вниз/вверх, выбирается сетевой интерфейс, параметры которого необходимо изменить или настроить. Пункты меню - eth0, eth1, eth2 и.т.д., в соответствии с максимальным числом установленных оптических сетевых плат.

4. Выбрав интерфейс, нажимая стрелки вниз/вверх, просматриваем параметры сетевых настроек и кнопкой «Enter» выбираем тот параметр, который необходимо изменить.

Например, необходимо изменить IP-адрес. После выбора этого пункта клавишей «Enter» на первой цифре IP-адреса появляется мигающий курсор. Кнопками стрелка вверх/вниз можно изменить эту цифру, а после нажатия кнопки «Enter» курсор перейдет на следующую цифру и т.д. Если какие-то цифры менять не нужно, то при нажатии кнопки «Enter» курсор будет просто передвигаться слева на право. После нажатия кнопки «Enter» на последней цифре курсор исчезнет, это означает, что параметр изменен, и нажимая кнопку стрелка вниз, можно переходить к следующему параметру.

Кроме IP-адреса HSM можно изменить следующие параметры сетевых настроек: маску подсети для HSM, IP-адрес шлюза локальной сети, список других сетевых интерфейсов, с которыми данный интерфейс агрегируется (bonding), а также режим передачи данных (full duplex, half duplex, 100/1000 Mb/сек, или автоопределение. Данный параметр зависит от типа используемой сетевой карты и может включать лишь подмножество из указанных режимов). Современные карты поддерживают режим autosense, поэтому рекомендуется использовать именно его.

Способ изменения маски подсети и адреса шлюза аналогичен способу изменения IP-адреса HSM, режим передачи данных выбирается с помощью меню.

Параметр Bonding. HSM поддерживает агрегирование нескольких сетевых интерфейсов в один логический. В общем случае, объединенные интерфейсы могут работать в режиме горячего резерва (отказоустойчивости) или в режиме балансировки нагрузки.

В ненастроенном состоянии данный параметр отображается как:

Bonding

--UNUSED--

При выборе данного пункта (кнопка Enter) высветится новое меню, первым пунктом которого будет:

Use link as

eth1 (имя настраиваемого интерфейса)

Здесь стрелками вверх/вниз можно выбрать нужный бондинг.

Будут высвечиваться надписи типа

Bonding Device

bond0

.....

Bonding Device

BondN (N – по количеству установленных сетевых интерфейсов)

Таким образом можно либо подключить интерфейс к уже существующему бондингу либо создать новый.

А первый пункт меню:

Use link as

eth1

существует либо для пропуска настройки бондинга, либо для выключения данного интерфейса из уже существующего бондинга.

Если хоть один параметр сетевых настроек был изменен, в конце меню сетевых настроек появится пункт «Save and restart». После выбора этого пункта на LCD-панели появится вопрос «Really save? YES [x] [x] NO». Выбор осуществляется нажатием кнопок стрелка влево/вправо и клавиши «Enter». При выборе «NO» меню настроек сетевых параметров будет покинуто и в силе останутся предыдущие значения сетевых настроек. При выборе «YES» изменение сетевых настроек будет принято, и появится вопрос «Restart network?».

При выборе «YES» сетевая служба будет перезапущена. Новые параметры сетевых настроек вступят в силу, когда перезапуск будет завершен.

Необходимо помнить, что при изменении IP-адреса какого-либо из интерфейсов, для нормальной работы потребуется регенерация TLS серверных сертификатов ПАКМ, а также, возможно, корректировка правил межсетевого экрана.

5.3.10. Просмотр и изменение параметров ПАКМ

Просмотр параметров ПАКМ доступен для любого привилегированного пользователя ПАКМ. Изменение параметров **Autoclean audit log**, **Audit log max records count**, **Enable event log** и **Logged events** доступно пользователю с правами Аудитора ПАКМ. Изменение остальных параметров ПАКМ доступно пользователю с правами Администратора ПАКМ.

Предварительные условия:

1. ПАКМ находится во включенном состоянии.
2. Привилегированный пользователь имеет при себе действующую карту привилегированного пользователя ПАКМ.

Для просмотра/изменения параметров:

1. Пользователь входит в меню (как описано в п.5.3).
2. Клавишами вверх/вниз пользователь листает и кнопкой Enter выбирает пункт меню:
- изменение параметров ПАКМ (**HSM options**);
3. Нажимая стрелки вниз/вверх, просматриваем параметры и кнопкой «Enter» выбираем тот параметр, который необходимо изменить.

Для разрешения/запрещения сетевого администрирования надо выбрать пункт **Enable web**. После этого на LCD-панели появится вопрос «Enable web? YES [x] [x] NO». Выбор осуществляется нажатием кнопок стрелка влево/вправо и клавиши «Enter».

Для разрешения/запрещения работы канала «K2» (шифрованного) надо выбрать пункт **Enable K2**. После этого на LCD-панели появится вопрос «Enable K2? YES [x] [x] NO». Выбор осуществляется нажатием кнопок стрелка влево/вправо и клавиши «Enter».

Для разрешения/запрещения работы канала «K2» (нешифрованного) надо выбрать пункт **Enable K2s**. После этого на LCD-панели появится вопрос «Enable K2s? YES [x] [x] NO». Выбор осуществляется нажатием кнопок стрелка влево/вправо и клавиши «Enter».

Перечисленных выше опции (**Enable K2s**, **Enable K2**, **Enable web**) влияют на запуск/останов процессов/слушателей соответствующих портов. Для запуска процесса слушателя, кроме всего прочего, необходимо, чтобы было описано хотя бы одно правило в настройках межсетевого экрана ПАКМ для данного порта.

Для установки/отмены автоочистки журнала аудита надо выбрать пункт **Autoclean audit log**. После этого на LCD-панели появится вопрос «Autoclean log? YES [x] [x] NO». Выбор осуществляется нажатием кнопок стрелка влево/вправо и клавиши «Enter».

Для установки/отмены режима ведения более подробного журнала событий надо выбрать пункт **Detail event log**. После этого на LCD-панели появится вопрос «Enable? YES [x] [x] NO». Выбор осуществляется нажатием кнопок стрелка влево/вправо и клавиши «Enter».

Event log – это журнал событий ПАКМ «КриптоПро HSM». Если для параметра «Detail event log» установлено значение NO. То в журнал событий будут писаться только ошибки выполнения криптографических запросов. Если установлено значение YES, то в журнал событий будут попадать все значимые с криптографической точки зрения события (генерация ключей, экспорт, импорт ключей, формирование и проверка ЭП и другие).

Для изменения порогового значения количества записей журнала аудита надо выбрать пункт **Audit log max records count**. После этого на LCD-панели появится приглашение «Enter max rec count» и текущее значение этого параметра.

На первой цифре вводимого числа появляется мигающий курсор. Кнопками стрелка вверх/вниз можно изменить эту цифру, а после нажатия кнопки «Enter» курсор перейдет на следующую цифру и т.д. Если какие-то цифры менять не нужно, то при нажатии кнопки «Enter» курсор будет просто передвигаться слева направо. Стрелка влево передвигает курсор налево.

Если нажать стрелку влево при положении курсора на первой цифре, будет выведено меню «Return to input?» («Повторить ввод?») с предложенным выбором «YES» («ДА») или «NO» («НЕТ»). При выборе ответа «YES» ввод числа будет повторен сначала, при выборе ответа «NO» ввод будет отменен.

После нажатия кнопки «Enter» на последней цифре параметр будет изменен, и произойдет выход в главное меню.

Для изменения интервала времени проверки журнала аудита на переполнение надо выбрать пункт **Autoclean poll interval**. После этого на LCD-панели появится приглашение «Enter interval» и текущее значение этого параметра. Новое значение вводится способом, описанным выше.

Для изменения длительности удерживания неактивного сетевого соединения (в секундах) надо выбрать пункт **Timeout idle**. После этого на LCD-панели появится приглашение «Enter timeout idle» и текущее значение этого параметра. Новое значение вводится способом, описанным выше. Если в организации, эксплуатирующей ПАКМ «КриптоПро HSM» ограниченное количество пользователей, позволяющее им всем одновременно работать с ПАКМ, то данный параметр рекомендуется устанавливать в «0», т.е. ПАКМ не будет разрывать соединения с клиентом. У пользователей на рабочих станциях не будет при этом возникать ошибок разрыва соединения и им не надо будет постоянно производить процедуру переустановления соединения с ПАКМ. Если же пользователей больше, чем максимальное количество одновременно удерживаемых соединений ПАКМ, то необходимо поставить данному параметру разумную величину, чтобы дать возможность освобождать неактивные соединения пользователей. Данный параметр не влияет на соединения, установленные с помощью ключа и сертификата доступа, в котором присутствует расширение «Администратор сервера», т.е. для серверных приложений. Такие соединения удерживаются сервером всегда.

Для изменения значения максимального количества одновременно удерживаемых сетевых соединений надо выбрать пункт **Max clients**. После этого на LCD-панели появится приглашение «Enter max clients» и текущее значение этого параметра. Новое значение вводится способом, описанным выше. По-умолчанию (значение «0») ПАКМ явно

не ограничивает количество одновременно удерживаемых соединений. В этом случае всё определяется доступными ресурсами ПАКМ (оперативной памятью, максимальным количеством открытых файловых дескрипторов, включая сокеты, и прочими характеристиками). При очень большом количестве одновременно работающих клиентов желательно ограничить количество одновременно удерживаемых соединений, например, 1000, чтобы не вызвать непредвиденную ошибку ПАКМ, связанную, например, с нехваткой свободного файлового дескриптора для системных целей. При этом необходимо установить разумный параметр длительности удерживания неактивного соединения (TimeoutIdle).

Для изменения режима синхронизации базы данных журнала аудита надо выбрать пункт **Audit sync mode**. После этого появится меню режимов синхронизации, состоящее из пунктов «OFF», «NORMAL» и «FULL».

Если режим синхронизации установлен как «FULL», ПАКМ будет работать медленно, но в случае внезапного выключения питания или сбоя операционной системы данные будут сохранены. При режиме «OFF» ПАКМ работает быстрее, но при сбое операционной системы есть высокий шанс, что база данных будет испорчена. Вариант «NORMAL» - промежуточный.

Для разрешения/запрета загрузки в ПАКМ файлов резервных копий с АРМ Администратора необходимо выбрать пункт **Enable Upload**. Установка данного параметра в значение NO (режим по умолчанию) приведет к запрету загрузок файлов в ПАКМ через интерфейс АРМ Администратора. Разрешайте загрузку только тогда, когда это действительно необходимо, после чего отключайте данную возможность.

Для просмотра или изменения набора событий, регистрируемых в журнале аудита, надо выбрать пункт **Logged events**. Далее с помощью стрелок вниз/вверх просматриваются названия событий и информация об их регистрации в журнале аудита. Кнопкой «Enter» выбирается событие, регистрацию которого надо изменить, и далее делается выбор из пунктов меню:

- 1: on success (регистрировать в случае успеха действия)
- 2: on error (регистрировать в случае неудачи действия)
- 3: always log (регистрировать всегда)

Перечень возможных событий:

Auth local admin (1) - попытка подключения по локальному (LCD) интерфейсу администрирования ПАКМ, успешная или неуспешная аутентификация пользователя;

Auth remote user (2) - попытка подключения по удаленному (каналы К и К2, ВЭБ интерфейс администрирования) интерфейсу ПАКМ (только неуспешная аутентификация пользователя);

Change HSM state (3) - изменение состояния ПАКМ;

Add user (4) - регистрация нового пользователя ПАКМ;

Modify user (5) - изменение информации о пользователе ПАКМ;

Delete user (6) - удаление информации о пользователе ПАКМ;

Change usr token (7) - изменение аутентификационной информации пользователя (генерация нового сертификата);

Change usr state (8) - блокирование/разблокирование пользователя ПАКМ;

Clear audit log (9) - очистка журнала аудита;

D-load audit log (10) - выгрузка журнала аудита;

Change sys time (11) - изменение системного времени ПАКМ;

Change HSM opts (12) - изменение настроек ПАКМ;

Change net set-s (13) - изменение сетевых настроек ПАКМ;

Add FW subnet (14) - добавление клиентской подсети в настройки межсетевого экрана;

Delete FW subnet (15) - удаление клиентской подсети из настроек межсетевого экрана;

Modify FW subnet (16) - изменение адресов клиентской подсети в настройках межсетевого экрана;

Restart FW (17) - перезапуск сервиса межсетевого экрана ПАКМ;

Change HSM key (18) - плановая смена ключа подписи и самоподписанного сертификата ПАКМ, ключа шифрования ключевых контейнеров ПАКМ;

Change TLS key (19) - плановая смена ключа и сертификата TLS сервера ПАКМ;

Change act key (20) - смена ключа активации ПАКМ (ключа «3 из 5»);

Load gamma (21) - загрузка ключевого материала уполномоченной организации;

Generate key (22) - генерация ключа пользователем;

Sign hash (23) - формирование ЭП пользователем ПАКМ;

Verify signature (24) - проверка ЭП пользователем ПАКМ;

Encrypt (25) - шифрование блока данных пользователем;

Decrypt (26) - расшифрование блока данных пользователем;

Overfill audit log (27) – переполнение журнала аудита (журналируется со статусом - неудача);

Repair audit log (28) – переполнение журнала аудита;

Delete key (29) – удаление ключа пользователя пользователем;

Crypt export key (30) - экспорт закрытого ключа;

Crypt import key (31) - импорт закрытого ключа в контейнер;

New backup (32) – создание новой резервной копии ПАКМ;

Delete backup (33) - удаление резервной копии ПАКМ;

Restore from bkp (34) – восстановление ПАКМ из резервной копии;

Download backup (35) – выгрузка резервной копии из ПАКМ;

Change audit opts (36) – изменение настроек аудита;

Memory error (37) – ошибка контроля памяти.

Upload Backups (38) – загрузка в ПАКМ файлов резервных копий.

Start P Service (39) – запуск платежных сервисов.

Stop P Service (40) – останов платежных сервисов.

P Console cmd (41) – регистрация выполнения консольной команды платежного модуля.

P firmware upd (42) – изменение прошивки платежного модуля.

P firmware upd (43) – изменение прошивки платежного модуля.

Chnge UnAuth Pwd (44) – смена пароля выполнения неавторизованной операции.

Registry Access (45) – Регистрация доступа к параметрам СКЗИ.

GetHashParam (46) – Регистрация выполнения криптографической операции.

Set HSM License (47) –Установка лицензии ПАКМ.

Изменения в параметрах **Logged events** или **Audit sync mode** вступят в силу только после перезагрузки ПАКМ, поэтому, если эти параметры изменены, после выхода из меню изменения параметров появится вопрос "Halt? ". При выборе ответа «YES» ПАКМ будет остановлен.

Для настройки механизма горячего резервирования используются следующие параметры:

- Repl Server Type;
- Repl Server ID;
- Repl Master IP.

Repl Server Type – тип сервера, участвующего в репликации. Может принимать значения:

- 0 – сервер не участвует в репликации (default)
- 1 – MASTER сервер репликации
- 2 – SLAVE сервер репликации

Repl Server ID – уникальный номер сервера, участвующего в репликации. Может принимать значения от 1 до 99 для.

Repl Master IP – IP-адрес MASTER сервера репликации. Устанавливается только для SLAVE серверов.

Подробнее о механизме репликации описано в «ЖТЯИ.00096-03 95 01. Правила пользования».

Enable Stat – разрешить ведение статистики по общему количеству созданных в ПАКМ ключей и ЭП. Установка данной опции может влиять на производительность ПАКМ. Данные статистики можно увидеть в Web интерфейсе администрирования ПАКМ.

5.3.11. Управление пользователями

Добавление, изменение и удаление пользователей ПАКМ доступно пользователю с правами Администратора ПАКМ. Импорт ключей пользователей ПАКМ доступен пользователю с правами Администратора ПАКМ при участии пользователя, ключи которого импортируются. Добавление, изменение и удаление привилегированных пользователей ПАКМ доступно только Суперпользователю ПАКМ. В Web интерфейсе ПАКМ добавление, изменение и удаление привилегированных пользователей ПАКМ также доступно, но требует подтверждения вторым (другим) Администратором ПАКМ.

Предварительные условия:

1. ПАКМ находится во включенном состоянии.
2. Администратор имеет при себе действующую карту администратора ПАКМ, или же ПАКМ находится в неактивном состоянии и присутствуют 3 из 5 доверенных лиц с картами ключа активации.
3. Если предполагается добавлять не привилегированных пользователей или изменять ключи не привилегированных пользователей, то необходимо, чтобы ПАКМ находился в активном состоянии или в состоянии «только администрирование».

Для управления пользователями:

1. Администратор входит в меню, или же производится вход в меню по схеме 3 из 5 (как описано в п.5.3).

2. Клавишами вверх/вниз пользователь листает и кнопкой Enter выбирает пункт меню:
 - управление пользователями (**User management**);
3. Нажимая стрелки вниз/вверх, просматривает подменю и кнопкой «Enter» выбирает нужный пункт подменю.

Для добавления пользователя надо выбрать пункт подменю **Add user**. (Если ПАКМ находится в неактивном состоянии, пользователь будет создан, но генерации ключа и сертификата аутентификации не произойдет. Чтобы впоследствии создать ключ и сертификат, необходимо привести ПАКМ в активное состояние, войти в подменю управления пользователями и выбрать пункт **Change user card**.)

После выбора пункта **Add user** на LCD-панели появится вопрос «Add user?», на который надо ответить «YES».

Затем появится вопрос «Computer account?». Если ответить «YES», то будет создано специальное учетное имя пользователя-**администратора сервера**. Карточки с ключами доступа, формируемые для такого пользователя, будут содержать специальный признак, который обеспечивает:

- запрос pin-кодов на ключи, формируемые для данного пользователя, на LCD-панели ПАКМ;
- возможность отключения шифрования в канале доступа для увеличения пропускной способности и повышения производительности серверных систем.

Пользователями данного учетного имени являются сервера приложений и системные сервисы, которые не имеют интерактивного взаимодействия с рабочим столом клиентского компьютера и обычно используются в серверах.

Затем появится вопрос «Payment Admin?». Если создается новый пользователь – Администратор Платежной системы, на вопрос надо ответить «YES», если нет, надо ответить «NO».

Затем появится вопрос «Statist Admin?». Если создается новый пользователь – Администратор Статистики, на вопрос надо ответить «YES», если нет, надо ответить «NO». У данной роли отсутствуют какие-либо права на изменения любых параметров и внутренних данных ПАКМ. Данная роль используется для процессов удаленного мониторинга состояния ПАКМ. Также ей доступно автоматическое скачивание журналов ПАКМ.

Затем появится вопрос «Administrator?». Если создается новый пользователь – Администратор, на вопрос надо ответить «YES», если нет, надо ответить «NO».

Затем появится вопрос «Auditor?». Если создается новый пользователь - Аудитор, на вопрос надо ответить «YES», если нет, надо ответить «NO».

Затем появится вопрос «Backup admin?». Если создается новый пользователь – Администратор резервного копирования, на вопрос надо ответить «YES», если нет, надо ответить «NO».

Роли Администратора, Аудитора и Администратора резервного копирования могут совмещаться одним и тем же пользователем, но для систем с требуемым уровнем криптозащиты информации KB/KB2 это недопустимо. Допускается выполнение ролей привилегированных пользователей доверенными лицами (суперпользователя) – хранителями частей разделенного секрета ключа активации ПАКМ. Создание новых привилегированных пользователей ПАКМ с использованием меню LCD панели доступно только Суперпользователю ПАКМ.

Если создаваемому пользователю ПАКМ не назначена ни одна из ролей привилегированных пользователей ПАКМ, то будет выдан запрос «Sub. User?». Это означает – «Является ли создаваемый пользователь членом какой-либо существующей группы пользователей ПАКМ?» (подробнее см. раздел 5 «ЖТЯИ.00096-03 91 01. Руководство администратора безопасности»). Если создаваемый пользователь должен иметь доступ к разделяемым ключам группы, то надо ответить «YES», в противном случае – «NO». Если ответ «YES», то далее на LCD панели появится запрос на ввод номера группы («Enter parent UID:»), в которую требуется включить данного пользователя.

После этого создается новый пользователь с именем «user_<UID пользователя>» или «admin_<UID пользователя>».

Если ПАКМ находится в активном состоянии или в состоянии «только администрирование», появится вопрос «Make user card?» («сформировать карту пользователя?»). После ответа «YES» появится приглашение «Insert card: YES [x] [x] NO». Необходимо вставить карту пользователя (карта должна быть зачищена), стрелками влево/вправо переместить курсор на пункт «YES» и кнопкой «Enter» выбрать этот пункт. Затем появится приглашение «Input new pin» («введите новый pin-код»). После ввода pin-кода будет создан ключ и сертификат аутентификации пользователя. Сертификат аутентификации пользователя устанавливается в контейнер ключа на смарт-карту пользователя. Туда же устанавливается и самоподписанный сертификат ключа подписи ПАКМ, с помощью которого был издан сертификат аутентификации пользователя. На LCD появится сообщение «User: <UID пользователя> added».

Если карта пользователя не была сформирована, появится сообщение «User: <UID пользователя> added w-out card».

Внимание. При формировании ключей аутентификации пользователей в ПАКМ класс защиты ключа устанавливается в соответствии с уровнем безопасности защиты ПАКМ. Если уровень безопасности СКЗИ, на котором будет использоваться данный ключ ниже уровня безопасности ПАКМ, то класс защиты ключа в используемом СКЗИ должен быть понижен до необходимого уровня. Это можно сделать, например, процедурой изменения pin-кода на смарт-карте на рабочем месте пользователя (где установлено СКЗИ, которое будет работать с ключом пользователя).

Для удаления пользователя надо выбрать пункт подменю **Delete user**. На LCD-панели появится вопрос «Delete user?», на который надо ответить «YES». Затем появится приглашение «Enter user UID:» («введите UID пользователя») и значение UID удаляемого пользователя по умолчанию.

На первой цифре вводимого числа появляется мигающий курсор. Кнопками стрелка вверх/вниз можно изменить эту цифру, а после нажатия кнопки «Enter» курсор перейдет на следующую цифру и т.д. Если какие-то цифры менять не нужно, то при нажатии кнопки «Enter» курсор будет просто передвигаться слева направо. Стрелка влево передвигает курсор налево.

Если нажать стрелку влево при положении курсора на первой цифре, будет выведено меню «Return to input?» («Повторить ввод?») с предложенным выбором «YES» («ДА») или «NO» («НЕТ»). При выборе ответа «YES» ввод числа будет повторен сначала, при выборе ответа «NO» ввод будет отменен.

После нажатия кнопки «Enter» на последней цифре UID будет введен, пользователь будет удален, и на LCD-панели появится сообщение «User deleted. Press any key...». После нажатия любой клавиши или по истечению таймаута произойдет выход в основное меню.

При удалении пользователя – члена группы, будет удален только профиль данного пользователя, ключевой раздел группы будет сохранен. При удалении пользователя – владельца группы будет удален раздел с ключами группы, профиль данного пользователя и профили всех пользователей – членов данной группы.

Чтобы заблокировать или разблокировать пользователя, надо выбрать пункт подменю **Lock user** или **Unlock user**. После выбора появится вопрос «Lock user?» или «Unlock user?», на который надо ответить «YES». Затем появится приглашение «Enter user UID:». Надо ввести значение UID пользователя, как описано выше.

После ввода UID пользователь будет заблокирован или разблокирован, и на LCD-панели появится сообщение «User locked» или «User unlocked».

Для изменения ключа и сертификата аутентификации пользователя (плановой смены) надо выбрать пункт подменю **Change user card**. Этот пункт доступен в активном состоянии ПАКМ или в состоянии «только администрирование».

После выбора этого пункта появится вопрос «Change card?», на который надо ответить «YES», затем появится приглашение «Enter user UID:». Надо ввести значение UID изменяемого пользователя, как описано выше.

Затем появится приглашение «Insert card: YES [x] [x] NO». Необходимо вставить новую карту пользователя (карта должна быть зачищена), стрелками влево/вправо переместить курсор на пункт «YES» и кнопкой «Enter» выбрать этот пункт. Затем появится приглашение «Input new pin» («введите новый pin-код»).

После ввода pin-кода будет создан новый ключ и сертификат аутентификации пользователя. Сертификат аутентификации пользователя устанавливается в контейнер ключа на смарт-карту пользователя. Туда же устанавливается и самоподписанный сертификат ключа подписи ПАКМ, с помощью которого был издан сертификат пользователя. На LCD появится сообщение «Card changed. Press any key...». После нажатия любой клавиши или по истечению таймута произойдет выход в основное меню.

Внимание. При формировании ключей аутентификации пользователей в ПАКМ класс защиты ключа устанавливается в соответствии с уровнем безопасности защиты ПАКМ. Если уровень безопасности СКЗИ, на котором будет использоваться данный ключ ниже уровня безопасности ПАКМ, то класс защиты ключа в используемом СКЗИ должен быть понижен до необходимого уровня. Это можно сделать, например, процедурой изменения pin-кода на смарт-карте на рабочем месте пользователя (где установлено СКЗИ, которое будет работать с ключом пользователя).

При миграции пользователей с одного криптопровайдера на другой, например, с «КриптоПро CSP» на ПАКМ «КриптоПро HSM» часто требуется сохранить действовавшие ключи подписи пользователя (Например, ключи подписи уполномоченного лица удостоверяющего центра). Для этого необходимо, чтобы сохраняемый ключ подписи хранился на смарт-карте. Этот ключ может быть перемещен внутрь ПАКМ.

Для импорта ключа пользователя со смарт-карты надо выбрать пункт подменю **Import user key**. Этот пункт доступен в активном состоянии ПАКМ или в состоянии «только администрирование».

После выбора этого пункта появится приглашение «Insert user card, press any key...». Необходимо вставить карту с ключом аутентификации пользователя, ключ которого будет импортироваться, и нажать любую клавишу. Затем появится приглашение «Input pin-code», после чего пользователь, ключ которого будет импортироваться, должен ввести pin-код ключа аутентификации.

Затем появится приглашение «Insert card with imported key», после которого надо вставить карту с импортируемым ключом и нажать любую клавишу. После этого появится приглашение «Input pin», и затем пользователь должен ввести pin-код импортируемого ключа.

После этого происходит импорт ключевого контейнера со вставленной карты на ПАКМ.

Если импорт ключевого контейнера завершен успешно, появится вопрос «Set pin code?». Если пользователь хочет установить pin-код на скопированный контейнер, надо ответить «YES». Если пользователь является пользователем-администратором сервера, вопрос «Set pin code?» задан не будет, так как в этом случае необходимо установить pin-код в обязательном порядке. В противном случае, если ответить «NO», на контейнер будет установлен код по умолчанию – «11111111».

Если получен ответ «YES» или пользователь является пользователем-администратором сервера, появится приглашение «Input new pin», после которого надо ввести pin-код. Затем появится приглашение «Confirm new pin», после которого надо ввести pin-код повторно. После этого, при совпадении двух введенных pin-кодов, появится сообщение «New pin set» - «Новый pin-код установлен». При несовпадении pin-кодов появится сообщение «Pins don't match. Try again», после которого следует нажать любую клавишу, и затем снова появится приглашение «Input new pin».

Если пользователь отказывается от ввода pin-кода, появляется сообщение «Can't set new pin. Press any key...», и на контейнер будет установлен код «11111111». Если пользователь-администратор сервера отказывается от ввода pin-кода, контейнер уничтожается, о чем появляется сообщение: «Can't set new pin. New key deleted».

5.3.12. Настройки межсетевого экрана

Просмотр настроек межсетевого экрана доступен любому привилегированному пользователю ПАКМ. Изменение настроек доступно для пользователя с правами Администратора ПАКМ.

ПАКМ «КриптоПро HSM» имеет встроенный межсетевой экран, ограничивающий доступ к сервисам ПАКМ по описанным правилам. По умолчанию, сетевой доступ к сервисам ПАКМ запрещен. Администратор ПАКМ должен добавить правила межсетевого экрана (прописать списки IP-адресов/подсетей, из которых разрешен доступ к тому или иному сервису ПАКМ). Если используется дополнительный внешний межсетевой экран, то необходимо помнить, что канал «К» использует 1502 порт для входящих соединений, канал K2 – 1501, канал K2s – 1503, канал для Web администрирования ПАКМ – 443, канал репликаций – 1504, канал K0 – 1505, канал платежного сервиса Host – 1500 (при открытии данного порта автоматически откроются дополнительно 10 портов 1511-1520),

канал платежного сервиса Console – 22222, канал платежного сервиса SNMP – udp порт 161.

Предварительные условия:

1. ПАКМ находится во включенном состоянии.
2. Привилегированный пользователь имеет при себе действующую карту привилегированного пользователя ПАКМ.

Для просмотра и изменения настроек межсетевого экрана:

1. Пользователь входит в меню (как описано в п.5.3).
2. Клавишами вверх/вниз пользователь листает и кнопкой Enter выбирает пункт меню:
- настройки межсетевого экрана (**FW settings**);
3. Нажимая стрелки вниз/вверх, просматривает и кнопкой «Enter» выбирает сочетание канал-интерфейс: «K» (**K channel**), «K2» (**K2 channel**), «K2 нешифрованный» (**K2s channel**), удаленное администрирование (**Remote admin**), репликация (**Replication**), «K0 открытый» (**K0 channel**), «PCI Host» (**PCI Host**), «PCI Console» (**PCI Console**), «SNMP» (**SNMP**) в сочетании с интерфейсами **eth0**, **eth1**, **eth2** и т.д.
4. Нажимая стрелки вниз/вверх, просматриваем и кнопкой «Enter» выбираем пункт подменю: просмотр списка разрешенных подсетей (**List subnets**) или добавить подсеть (**Add subnet**).

Для добавления новой подсети канала надо выбрать пункт **Add subnet**. Затем после появления приглашения «Input IP address» надо ввести адрес подсети, и после появления приглашения «Input net mask» - маску подсети. После ввода маски новая подсеть будет добавлена, и появится сообщение «Subnet added».

После нажатия любой кнопки или по истечении таймута появится вопрос «Restart Net/FW?». При выборе «YES» сетевая служба и межсетевой экран будут перезапущены. Новые настройки межсетевого экрана вступят в силу, когда перезапуск будет завершен.

Для просмотра подсетей канала надо выбрать пункт **List subnets**. После этого кнопками вверх/вниз можно просматривать подсети канала для данного интерфейса (первая строка — IP-адрес, вторая строка — маска). Если для пары канал-интерфейс не задано ни одной подсети, после выбора пункта **List subnets** появится сообщение «No FW settings».

Для удаления подсети канала надо выбрать пункт **List subnets**, затем кнопками вверх/вниз пролистать подсети и кнопкой «Enter» выбрать удаляемую подсеть. После

этого появится вопрос «Delete?», на который надо ответить «YES». Подсеть будет удалена, и появится сообщение «Subnet deleted». После нажатия любой клавиши или по истечению таймаута произойдет выход в основное меню.

5.3.13. Изменение внутренних ключей и сертификатов ПАКМ

Изменение ключа и сертификата TLS, ключа и самоподписанного сертификата ПАКМ, или ключа активации доступно для пользователя с правами Администратора ПАКМ. Изменение ключа и сертификата аутентификации администратора доступно только Суперпользователю ПАКМ.

Предварительные условия:

1. ПАКМ находится во включенном состоянии.

2. Если предполагается изменять ключ и сертификат TLS сервера или ключ и самоподписанный сертификат ПАКМ, необходимо, чтобы администратор имел при себе действующую карту администратора ПАКМ, и ПАКМ находился в активном состоянии или в состоянии «только администрирование».

3. Если предполагается изменять ключ и сертификат аутентификации администратора, необходимо, чтобы ПАКМ находился в неактивном состоянии и присутствовали 3 из 5 доверенных лиц с картами ключа активации.

Если предполагается изменять ключ активации, необходимо, чтобы

1. ПАКМ находился в неактивном состоянии.

2. Администратор имел при себе действующую карту администратора ПАКМ.

3. Присутствовали 5 доверенных лиц с 5 чистыми картами для записи частей нового ключа активации, и с 3 из 5 картами с частями старого ключа активации.

Для изменения ключей и сертификатов уполномоченных лиц:

- Администратор входит в меню (как описано в п.5.3). Для изменения ключа и сертификата аутентификации администратора производится вход в меню по схеме 3 из 5, после чего ПАКМ перейдет в состояние «только администрирование».
- Клавишами вверх/вниз пользователь листает и кнопкой Enter выбирает пункт меню:
 - изменение ключей (**Update keys**);

- Нажимая стрелки вниз/вверх, просматриваем подменю и кнопкой «Enter» выбираем нужный пункт подменю.

Для смены ключа активации (возможно только в неактивном состоянии ПАКМ) надо выбрать пункт **ACT(ivation) key**, на вопрос «Change ACT key?» ответить «YES».

После этого на панели появится приглашение «Insert #1 of 5». Если 1-е доверенное лицо имеет при себе старую карту ключа активации, надо вставить его карту в считыватель ПАКМ, переместить курсор на пункт «YES» и кнопкой Enter выбрать этот пункт, а затем в ответ на приглашение «Input pin-code» доверенное лицо должно ввести свой pin-код. Если старая карта у 1-го доверенного лица отсутствует, надо выбрать пункт «NO».

Далее появится приглашение «Insert #2 of 5», и процедура повторяется, пока не будут обработаны 3 из 5 карт старого ключа.

После этого снова появляется приглашение «Insert #1 of 5». Надо вставить в считыватель ПАКМ 1-ю карту для записи нового ключа активации, и выбрать пункт «YES». Затем в ответ на приглашение «Input new pin» 1-е доверенное лицо должно ввести pin-код для новой карты. Эта процедура повторяется для каждого из 5 доверенных лиц.

Затем снова появляется приглашение «Insert #1 of 5», после этого надо вставить 1-ю карту нового ключа активации и выбрать «YES». Процедура повторяется для каждой из 5 карт нового ключа.

После этого ключ активации будет сменен, и появится сообщение «ACT key changed». После нажатия любой клавиши или по истечению таймаута произойдет выход в основное меню.

Для смены ключа подписи и самоподписанного сертификата ПАКМ (невозможно в неактивном состоянии ПАКМ) надо выбрать пункт **CA key**, и на вопрос «Change CA key?» ответить «YES».

После этого ключ будет сменен, сформирован новый самоподписанный сертификат ПАКМ и появится сообщение «CA key changed». После нажатия любой клавиши или по истечению таймаута произойдет выход в основное меню.

Для смены ключа и сертификата TLS сервера (невозможно в неактивном состоянии ПАКМ) надо выбрать пункт **TLS server key**, и на вопрос «Change TLS key?» ответить «YES».

После этого ключ TLS сервера будет сменен, и появится сообщение «TLS key changed». После нажатия любой клавиши или по истечению таймаута произойдет выход в основное меню.

Чтобы ввести ключ TLS сервера в действие, надо привести ПАКМ в неактивное состояние и затем снова активировать.

Для смены ключа и сертификата аутентификации привилегированного пользователя ПАКМ (невозможно в неактивном состоянии ПАКМ) надо выбрать пункт **ADM(in) key**, и на вопрос «Change ADM key?» ответить «YES».

Для смены ключа подписи журнала аудита и соответствующего сертификата (невозможно в неактивном состоянии ПАКМ) надо выбрать пункт **AuditSigning key**, и на вопрос «Change Audt key?» ответить «YES».

Помните, что все действия по добавлению/удалению/изменению учетных записей привилегированных пользователей доступны только суперпользователю! (т.е. в LCD меню необходимо войти при использовании ключа активации ПАКМ – «3 из 5»).

После этого появится приглашение «Enter admin UID» («введите UID администратора») и значение UID администратора по умолчанию.

На первой цифре вводимого числа появляется мигающий курсор. Кнопками стрелка вверх/вниз можно изменить эту цифру, а после нажатия кнопки «Enter» курсор перейдет на следующую цифру и т.д. Если какие-то цифры менять не нужно, то при нажатии кнопки «Enter» курсор будет просто передвигаться слева направо. Стрелка влево передвигает курсор налево.

Если нажать стрелку влево при положении курсора на первой цифре, будет выведено меню «Return to input?» («Повторить ввод?») с предложенным выбором «YES» («ДА») или «NO» («НЕТ»). При выборе ответа «YES» ввод числа будет повторен сначала, при выборе ответа «NO» ввод будет отменен.

После нажатия кнопки «Enter» на последней цифре UID будет введен.

После ввода UID появится приглашение «Insert card: YES [x] [x] NO». Необходимо вставить карту администратора (карта должна быть зачищена), стрелками влево/вправо переместить курсор на пункт «YES» и кнопкой «Enter» выбрать этот пункт. Затем появится приглашение «Input new pin» («введите новый pin-код»). После ввода pin-кода ключ и сертификат администратора будет изменен, и появится сообщение «ADM key changed».

5.3.14. Корректная очистка журнала аудита

Данная процедура доступна для пользователя с правами Аудитора ПАКМ с подтверждением действия Администратором ПАКМ.

Предварительные условия:

1. ПАКМ находится во включенном состоянии.
2. Аудитор имеет при себе одну действующую карту аудитора ПАКМ.

Для очистки журнала аудита:

1. Аудитор входит в меню (как описано в п.5.3).
2. Клавишами вверх/вниз аудитор листает и кнопкой Enter выбирает пункт меню:
- Корректная очистка журнала аудита (**Clear audit log**).
3. На панели появится вопрос «Clear audit log?», на который надо ответить «YES».
4. На панели появится запрос на подтверждение действия при помощи карты Администратора ПАКМ - «Insert Adm card». Необходимо, чтобы Администратор ПАКМ вставил свою карту и после нажатия кнопки Ок ввел корректный pin-код для нее.
5. База данных журнала аудита будет очищена, и на панели появится надпись «Audit log cleared». После нажатия любой кнопки или по истечению таймута произойдет переход в основное меню.

5.3.15. Восстановление журнала аудита

В случае сбоев питания, или неосознанного выключения ПАКМ кнопкой питания без корректной процедуры остановки (HALT) база данных журнала аудита ПАКМ может быть разрушена. Данная процедура позволяет восстановить базу данных журнала аудита путем её пересоздания (файл БД создается заново по изначальной схеме БД). При этом все записи журнала будут потеряны. Процедура доступна только в неактивном состоянии ПАКМ, для пользователя с правами Аудитора ПАКМ с подтверждением действия Администратором ПАКМ.

Предварительные условия:

1. ПАКМ включен и находится в неактивном состоянии.
2. Аудитор имеет при себе одну действующую карту аудитора ПАКМ.

Для восстановления журнала аудита:

1. Аудитор входит в меню (как описано в п.5.3).
2. Клавишами вверх/вниз аудитор листает и кнопкой Enter выбирает пункт меню:
- Простая очистка журнала аудита (**Repair audit log**).
3. На панели появится вопрос «Repair aud log?», на который надо ответить «YES».
4. На панели появится запрос на подтверждение действия при помощи карты Администратора ПАКМ - «Insert Adm card». Необходимо, чтобы Администратор

ПАКМ вставил свою карту и после нажатия кнопки Ок ввел корректный pin-код для нее.

5. Журнал аудита будет очищен. На панели появится надпись «Audit log repaired». После нажатия любой кнопки или по истечению таймаута произойдет переход в основное меню.

По окончании процедуры ПАКМ необходимо перезагрузить.

5.3.16. Резервное копирование и восстановление ПАКМ

Для обеспечения надежности ПАКМ «КриптоПро HSM» имеет возможность резервирования ключевой информации и, при необходимости, её восстановления (подробнее см. п. 5.3.16).

Данный режим применяется, в основном, для сохранения важной ключевой информации, например, ключа уполномоченного лица удостоверяющего центра, предназначенного для подписи сертификатов открытых ключей и ключей ЭП пользователей.

Предварительные условия:

1. ПАКМ находится во включенном состоянии.

Просмотр списка ранее созданных резервных копий ПАКМ доступен всем привилегированным пользователям.

Создание новой резервной копии и удаление существующей резервной копии доступно только пользователю, наделенному полномочиями «Администратора резервного копирования».

Запуск процедуры восстановления ПАКМ из резервной копии доступен только «Администратору ПАКМ», но при этом должен присутствовать «Администратор резервного копирования ПАКМ» со смарт-картой, на которой сформирован ключ шифрования резервной копии, той, с которой предстоит восстановление.

Выполнение процедур создания резервной копии и восстановления ПАКМ из резервной копии возможно только в том случае, когда ПАКМ находится в неактивном состоянии.

Имена файлов резервных копий именуются следующим образом:

ГГГГММДД_ЧЧммСС, где

ГГГГ – четырехзначное обозначение года даты создания резервной копии;

ММ – двухзначное обозначение месяца даты создания резервной копии;

ДД – двухзначное обозначение дня даты создания резервной копии;

ЧЧ – двухзначное обозначение часа времени создания резервной копии;

мм – двухзначное обозначение минуты времени создания резервной копии;

СС – двухзначное обозначение секунды времени создания резервной копии;

Для просмотра списка ранее созданных резервных копий привилегированный пользователь:

1. Входит в меню (как описано в п.5.3).
2. Клавишами вверх/вниз листает и кнопкой Enter выбирает пункт меню «**Backups**».
3. Если не создано ни одной резервной копии и ПАКМ находится в неактивном состоянии, то система предложит создать новую резервную копию (соответственно пользователь должен играть роль Администратора резервного копирования).
4. Если не создано ни одной резервной копии и ПАКМ находится в одном из активных состояний, то на LCD панель будет просто выведено сообщение об отсутствии резервных копий.
5. Если есть хоть одна резервная копия, то на LCD панель выводится список ранее созданных существующих резервных копий.
6. Привилегированный пользователь, используя клавиши вверх/вниз, может просматривать данный список.
7. Нажатие клавиши Enter на выбранном наименовании файла с резервной копией вызовет контекстное меню:

- **Delete** (Удаление выбранного файла резервной копии);

- **Restore** (восстановление ПАКМ из выбранного файла резервной копии);

- **Create new** (создание новой резервной копии);

Для удаления файла резервной копии **Администратор Резервного копирования** должен выбрать пункт **Delete**. При этом система запросит подтверждение выполнения операции «**Delete file?**» и только при утвердительном ответе выполнит операцию удаления. Выбранный элемент из списка файлов резервных копий также будет удален.

Для восстановления ПАКМ из выбранной резервной копии **Администратор** ПАКМ должен выбрать пункт меню «**Restore**». Администратор резервного копирования должен вставить смарт-карту с ключом и сертификатом ключа подписи и шифрования выбранного файла резервной копии, и на запрос pin-кода для доступа к ключу на смарт-карте ввести его, используя клавиши управления LCD панели. Система также запросит подтверждение

выполнения операции и после утвердительного ответа запустится процедура восстановления. В случае успешного восстановления на LCD панель будет выведено сообщение «HSM restored from backup». Администратор ПАКМ должен перезагрузить ПАКМ.

Для создания нового файла с резервной копией ПАКМ **Администратор резервного копирования** должен выбрать пункт «**Create new**», вставить чистую смарт-карту в считыватель ПАКМ для формирования на ней ключа подписи и шифрования файла резервной копии. Система запросит подтверждение выполнения операции «**New backup file?**» и после утвердительного ответа запустит процедуру создания резервной копии. После записи ключа и сертификата ключа на карту система предложит задать pin-код для доступа к ключу на этой карте. Администратор резервного копирования должен задать данный pin-код и хранить его в тайне от других пользователей, как и саму карту. В результате успешного создания файла с резервной копией на экран LCD панели будет выведено сообщение «New backup created». В списке файлов резервных копий появится новый элемент.

5.3.17. Смена пароля для доступа к режиму полной очистки ПАКМ в меню неавторизованных операций (Change password)

При неудачной инициализации ПАКМ (например, в случае сбоя питания), или в случае порчи карт доверенных лиц ПАКМ может оказаться в «неопределенном» состоянии, из которого обычными штатными методами его вывести невозможно. Для того, чтобы перевести его в неинициализированное состояние, процедуру full clean можно выполнить из меню неавторизованных операций, используя специальный пароль для этого случая.

При изготовлении ПАКМ этот пароль устанавливается и имеет значение «11111111». После успешной инициализации ПАКМ Администратор ПАКМ должен его сменить, используя пункт основного меню LCD панели «**Change password**».

При выборе данного режима на LCD панели будет предложено ввести текущий пароль «Input old passwd» и, если пароль корректен, будет предложено ввести новый пароль «Input new passwd» 2 раза (с подтверждением). Если значения новых паролей совпадают, то новый пароль будет установлен в ПАКМ.

5.3.18. Ввод лицензии на использование ПАКМ (License(s)).

Существует два возможных вида лицензий:

- Лицензия на PKI HSM;
- Лицензия на PCI HSM.

Лицензия на PKI HSM является лицензией на базовые программные модули (БПМ). Должна устанавливаться всегда. Позволяет использовать ПАКМ в качестве разделяемого СКЗИ. Позволяет активировать каналы доступа пользователей к ПАКМ. Может иметь расширение, позволяющее активировать модуль Дистанционного Электронного Голосования (ДЭГ).

Лицензия на PCI HSM позволяет использовать ПАКМ в качестве Платежного HSM и активировать платежные сервисы.

Номера лицензий выдаются при приобретении ПАКМ.

Лицензии могут быть временными – на срок 3 месяца с момента первой установки, срочными – с указанием срока окончания действия лицензии, и бессрочными. Вся информация о виде лицензии и сроке её действия зашифрована в номере лицензии.

Использование данного пункта меню LCD панели позволяет ввести номера указанных лицензий ПАКМ. Для этого потребуется флэш диск («флэшка») с записанным в её корень текстовым файлом "LicenseSN", содержащим номер лицензии (только один). При необходимости ввести другой номер лицензии, то файл LicenseSN необходимо будет перезаписать на флэшку с новым номером и повторить процедуру установки лицензии.

В номере лицензии допускаются латинские буквы в верхнем регистре, цифры и символы «-» (дефис), без пробелов.

Для установки лицензии выберите данный пункт меню. На LCD панели отобразится требуемое имя файла с лицензией и строка "... waiting ...". Вставьте флэш диск в USB разъем ПАКМ. При успешном считывании серийного номера лицензии из файла LicenseSN его номер отобразится на LCD панели в виде «бегущей строки». Нажмите кнопку подтверждения LCD панели. И на последующий запрос «Apply LICENSE?» ещё раз нажмите кнопку подтверждения. Для отмены установки лицензии нажмите кнопку отмены.

Права на установку лицензии есть у Администратора ПАКМ или Суперпользователя ПАКМ.

5.4. Работа с LCD меню платежной системы

Если при входе в меню LCD панели будет предъявлена смарт-карта Администратора Платежной системы, то высветится специальное меню Платежной системы.

В зависимости от состояния ПАКМ и состояния сервисов платежной системы некоторые режимы могут не отображаться.

Полное меню включает:

- **Enable Host** – запуск сервиса HOST;
- **Enable Host (TLS)** – запуск сервиса HOST с шифрованным каналом;
- **Enable Console** – запуск сервиса CONSOLE ;

- **Disable Host** – останов сервиса HOST;
- **Disable Console** – останов сервиса HOST;
- **Firmware version** – отображение версии текущей и базовой прошивки платежного модуля;
- **Reset firmware** – сброс версии ПО платежного модуля к заводской прошивке;
- **Update firmware** – обновление прошивки модуля платежной системы с Flash накопителя.
- **Exit** – выход из меню платежной системы.

Запуск сервисов платежной системы HOST и CONSOLE (secure mode) возможен только после предъявления смарт-карты второго Администратора платежной системы. ПАКМ должен находиться в одном из активных состояний (достаточно состояния ADMIN_ONLY).

Кроме этого требуется наличие действующей лицензии на использование модуля платежной системы.

Сервис CONSOLE может быть запущен в двух режимах – Secure и offline. Для этого при запуске сервиса будет выдан запрос-подтверждение «Secure mode?». Если ответить «Yes», то сервис будет запущен в Secure режиме, в противном случае – в offline режиме.

При сбросе прошивки к заводскому ПО платежного модуля будет выдан запрос-подтверждение на выполнение этой операции «Really reset?». И только при выборе «Yes», данная операция будет произведена.

Обновление прошивки модуля платежной системы может быть произведено, как в Web интерфейсе администрирования ПАКМ, так и выбрав соответствующий режим в меню LCD панели. В последнем случае файл с прошивкой модуля платежной системы записывается в корень Flash накопителя, имеющего только один раздел. Имя файла должно быть фиксированным fwupdate.bin.

Данный режим позволяет произвести обновление ПО платежного модуля ПАКМ. Правом на загрузку обновлений платежного модуля обладает пользователь с ролью «Администратор платежной системы». Обычный Администратор ПАКМ может разрешить или запретить загрузку файлов в ПАКМ путем настройки опции «Enable upload» в настройках Параметров ПАКМ. Таким образом, разрешение на выполнение данной операции может быть разделено между привилегированными пользователями с указанными ролями.

Файл, содержащий прошивку, представляет собой подписанное электронной подписью производителя CMS (#pkcs7) сообщение SIGNED_DATA, включающее архив программных модулей и сопровождающей информации. При загрузке файла обновления будет производиться проверка ЭП данного CMS сообщения на открытом ключе

производителя, записанном в ПАКМ при изготовлении. Если проверка ЭП выполнена без ошибок, файл распаковывается и ожидает перезагрузки ПАКМ для дальнейшего внутреннего обновления прошивки. Каждая прошивка содержит номер версии, который можно просмотреть, выбрав режим «Firmware version». Кроме установленной таким образом прошивки всегда сохраняется базовая прошивка, установленная в ПАКМ при изготовлении. В случае ошибки обновления, может производиться автоматический сброс к заводским настройкам.

Выполнение операции обновления или сброса будет заблокировано, если запущен какой-либо из rsd сервисов (Хост и/или Консоль) с выдачей соответствующего сообщения об ошибке. Необходимо предварительно остановить RSD сервисы, после чего повторить операцию обновления или сброса.

По окончании успешного выполнения процедур обновления или сброса к заводской прошивке ПАКМ должен быть перезагружен. Поэтому он автоматически выключится (перейдет в состояние «HALT»).

5.5. Работа с LCD меню неавторизованных операций

Если при входе в меню LCD панели будет нажата кнопка «стрелка вниз», то высветится специальное меню Неавторизованных операций.

В зависимости от состояния ПАКМ и состояния delay режима (не в режиме меню) отображения информации на LCD некоторые режимы меню могут не отображаться.

Полное меню включает:

- **Show date/time** – отображение текущей даты и времени в delay режиме меню;
- **Show resources** – отображение статистической информации об используемых ресурсах ПАКМ;
- **Full Clean** – полная очистка ПАКМ, приведение его к неинициализированному состоянию;
- **Clr Magistra card** – быстрая зачистка смарт-карт Магистра;
- **Exit** – выход из меню;

Выбор режимов **Show date/time** и **Show resources** управляет выводом информации на LCD панель, когда она находится в неактивном состоянии (не в режиме меню, запросов на pin-коды, подтверждений или вывода спец. сообщений). Если выбирается режим **Show date/time**, то помимо состояния ПАКМ в delay режиме будет отображаться текущие дата и время в соответствии с выбранным часовым поясом.

Если выбирается режим **Show resources**, то помимо состояния ПАКМ в delay режиме LCD панели во второй строке будет отображаться информация об используемых ресурсах ПАКМ. Через каждые 2 секунды, сменяя друг друга будет отображаться:

- Текущая загрузка процессора;
- Пиковая загрузка процессора;
- Текущее использование Оперативной памяти (ОП);
- Пиковое использование ОП;
- Текущее использование дискового пространства в разделе ключей;
- Пиковое использование дискового пространства в разделе ключей;
- Текущее количество сетевых подключений к ПАКМ;
- Пиковое количество сетевых подключений к ПАКМ.

(пиковое значение — максимальное значение с момента загрузки или переактивации ПАКМ.)

Режим **Clr Magistra card** предназначен для быстрой зачистки «на месте» смарт-карт Магистра. Данный режим полезен, когда в случае неудачной инициализации требуется её повтор, но при этом отсутствуют средства зачистки использованных карт. При выборе этого режима будет выдан запрос-подтверждение на проведение операции "Clear card?", ответив утвердительно, будет предложено вставить карту и нажать любую клавишу. После нажатия кнопки на LCD карта будет зачищена.

При неудачной инициализации ПАКМ (например, в случае сбоя питания), или в случае порчи карт доверенных лиц ПАКМ может оказаться в «неопределенном» состоянии, из которого обычными штатными методами его вывести невозможно. Для того, чтобы перевести его в неинициализированное состояние, процедуру **full clean** можно выполнить из меню неавторизованных операций, используя специальный пароль для этого случая (см. раздел «Смена пароля для доступа к режиму полной очистки ПАКМ в меню неавторизованных операций (Change password)»).

Порядок выполнения операции «**Full Clean**» описан в разделе 5.3.7 Очистка содержимого ПАКМ.

5.6. Работа с журналом событий ПАКМ

При работе с ПАКМ периодически требуется просматривать журнал событий, ведущийся в устройстве.

Код и время последнего события отображаются на LCD панели устройства.

Для просмотра журнала событий ПАКМ администратор может воспользоваться пунктом меню устройства на LCD панели (см. п. 5.3.2). Этот способ используется для оперативного анализа нескольких последних событий в ПАКМ.

Для сохранения журналов событий и их детального анализа следует воспользоваться средствами web-администрирования ПАКМ (см. п. 6.2.12). Журнал

отображается на HTML странице и, при необходимости может быть сохранен в виде файла, а также подписан на ключе подписи журнала аудита.

Для обеспечения защиты содержимого журнала событий ПАКМ от сбоев в системе рекомендуется регулярно (не реже, чем раз в сутки) выгружать журнал из ПАКМ на Сервер. При этом период, задаваемый для считывания записей журнала, обязательно должен охватывать предыдущие сутки (т.е. должно быть организовано перекрытие предыдущего периода между считываниями журнала).

6. УДАЛЕННОЕ АДМИНИСТРИРОВАНИЕ ПАКМ (WEB ИНТЕРФЕЙС)

6.1. Удаленное рабочее место Администратора

Управление ПАКМ «КриптоПро HSM» может осуществляться как локально, с использованием LCD панели ПАКМ, так и удаленно, с использованием web-интерфейса администрирования ПАКМ.

Интерфейс рабочего места администратора реализован в виде HTML страницы с использованием активных элементов управления и языка сценариев javascript. Для работы с активным содержимым HTML страницы требуется web-обозреватель на основе Chromium: Chromium-Gost, Yandex Browser, новый Microsoft Edge (chromium) с включенным режимом совместимости с Internet Explorer, а также Internet Explorer версии не ниже 7.

Для поддержки криптографических операций на стороне APM Web администрирования ПАКМ (TLS протокол, генерация ключей доступа пользователей) на рабочую станцию администратора должен быть установлен криптопровайдер КриптоПро CSP версии 5.0 и выше (входит в комплект поставки ПАКМ).

Взаимодействие рабочей станции администратора ПАКМ с ПАКМ осуществляется по стандартному HTTPS (TLS) протоколу с использованием российских криптографических алгоритмов с двусторонней аутентификацией сторон. Поэтому для работы администратору необходим ключ и сертификат администратора, изданные ПАКМ и записанные на смарт-карту. Сертификат ключа доступа(аутентификации) администратора должен быть установлен в личное хранилище пользователя средствами «КриптоПро CSP».

Для корректной работы TLS протокола на рабочей станции администратора также должен быть установлен самоподписанный сертификат ключа подписи ПАКМ. Самоподписанный сертификат ключа подписи ПАКМ находится в специальном расширении контейнера ключа аутентификации (администратора или любого пользователя) и при первоначальной настройке удаленного рабочего места Web администрирования может быть извлечен либо средствами панели управления КриптоПро CSP, либо при помощи специальной утилиты (cardman), входящей в дистрибутив. Данная утилита представляет собой консольное интерактивное приложение и позволяет извлечь из расширений контейнера ключа аутентификации, находящегося на смарт-карте, сертификат ключа аутентификации пользователя и самоподписанный сертификат ПАКМ, содержащий открытый ключ, необходимый для проверки пользовательского сертификата.

Извлеченный таким образом самоподписанный сертификат ключа подписи ПАКМ должен быть установлен в доверенное хранилище корневых сертификатов ОС Windows стандартным образом.

Извлеченный сертификат пользователя должен быть установлен в личное хранилище пользователя в связке с закрытым ключом через Панель управления КриптоПро.

При смене ключа подписи ПАКМ новый корневой сертификат этого ключа может быть получен с использованием уже работающего Web интерфейса (в разделе «Сертификаты ПАКМ»).

Для генерации ключей доступа, запросов на сертификат ключа доступа, установки сертификата в контейнер используется бесплатное расширение для указанных выше браузеров – «КриптоПро ЭЦП Browser plug-in». Данное расширение можно скачать с сайта ООО «КРИПТО-ПРО» — <https://www.cryptopro.ru/products/cades/plugin>. Инструкция по установке, настройке и проверке корректности работы плагина приведена по ссылке <https://docs.cryptopro.ru/cades/plugin/plugin-installation-windows>.

Рабочая станция должна быть оснащена считывателем смарт-карт. Для некоторых операций, требующих подтверждения (путем формирования ЭП) вторым привилегированным пользователем, крайне желательно иметь 2 считывателя смарт-карт: один всегда используется для смарт-карты с ключом доступа Администратора для поддержки TLS протокола (двусторонняя аутентификация и шифрование канала), а второй — для подписи данных, подтверждаемых вторым привилегированным пользователем, и для генерируемых ключей новых пользователей ПАКМ.

Для подключения удаленного компьютера-рабочего места администратора в ПАКМ предусмотрен отдельный сетевой интерфейс. В целях безопасности данный сетевой интерфейс не должен коммутироваться с локальной сетью, а должен напрямую соединяться с сетевым интерфейсом компьютера с APM Web-администратора.

На стороне ПАКМ необходимо разрешить использование web-интерфейса ПАКМ (установить опцию «Enable WEB»), а также внести IP-адрес и маску подсети рабочей станции администратора в настройки межсетевого экрана ПАКМ для порта № 443 и соответствующего сетевого интерфейса, перезапустить сервис межсетевого экрана («Restart FW») с использованием LCD меню. ПАКМ должен находиться в состоянии либо «активном» (ACTIVE), либо «активном только для администрирования» (ADMIN_ONLY).

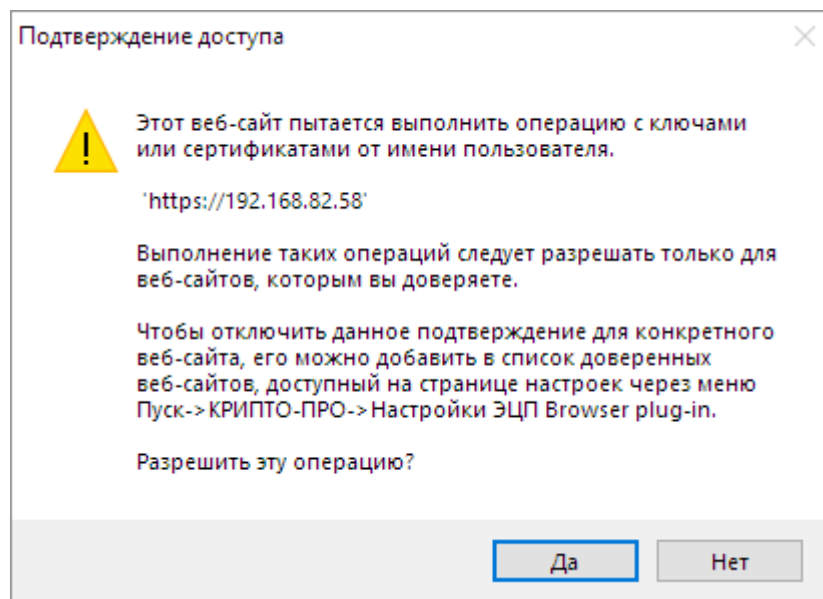
Подключение к ПАКМ осуществляется путем ввода URL строки в браузере в виде:

<https://<ip-адрес сетевого интерфейса Web администрирования ПАКМ>>, например, <https://192.168.26.2>

ПАКМ не издает списки отзыва (CRL) для изданных им сертификатов ключей доступа пользователей ПАКМ. Поэтому в браузерах может появляться информация о

недоверии к сайту из-за отсутствия информации об отзыве. Для продолжения работы необходимо игнорировать такие предупреждения.

В некоторых режимах работы может выдаваться специальное предупреждение браузера:



Для корректной работы следует разрешить эту операцию.

Внимание! ПАКМ «КриптоПро HSM» формирует ключи, соответствующие классу защиты до КВ. СКЗИ «КриптоПро CSP», используемое на рабочем месте администратора, реализовано по классу защиты КС1/КС2/КС3, поэтому при первом использовании ключа аутентификации, сформированном на смарт-карте в ПАКМ, будет выдано соответствующее предупреждение о понижении класса защиты ключа. Необходимо иметь в виду, что данной картой впоследствии нельзя будет воспользоваться для аутентификации администратора в ПАКМ при входе через LCD панель. Поэтому необходимо для каждого привилегированного пользователя (члена группы администраторов ПАКМ) создать две учетные записи, и, соответственно, 2 карты доступа: одну использовать для локального входа через LCD панель ПАКМ, а вторую (с пониженным классом защиты) для доступа с удаленного рабочего места.

Для удаленного администрирования ПАКМ необходимо, чтобы ПАКМ был включен и находился в активном состоянии или в состоянии «только администрирование», в параметрах ПАКМ пункт «разрешить Web-интерфейс» (**Enable web**) был установлен в «YES», и в настройках межсетевого экрана для канала управления ПАКМ (**Remote admin**, 443 порт) был добавлен IP-адрес компьютера, с которого производится администрирование.

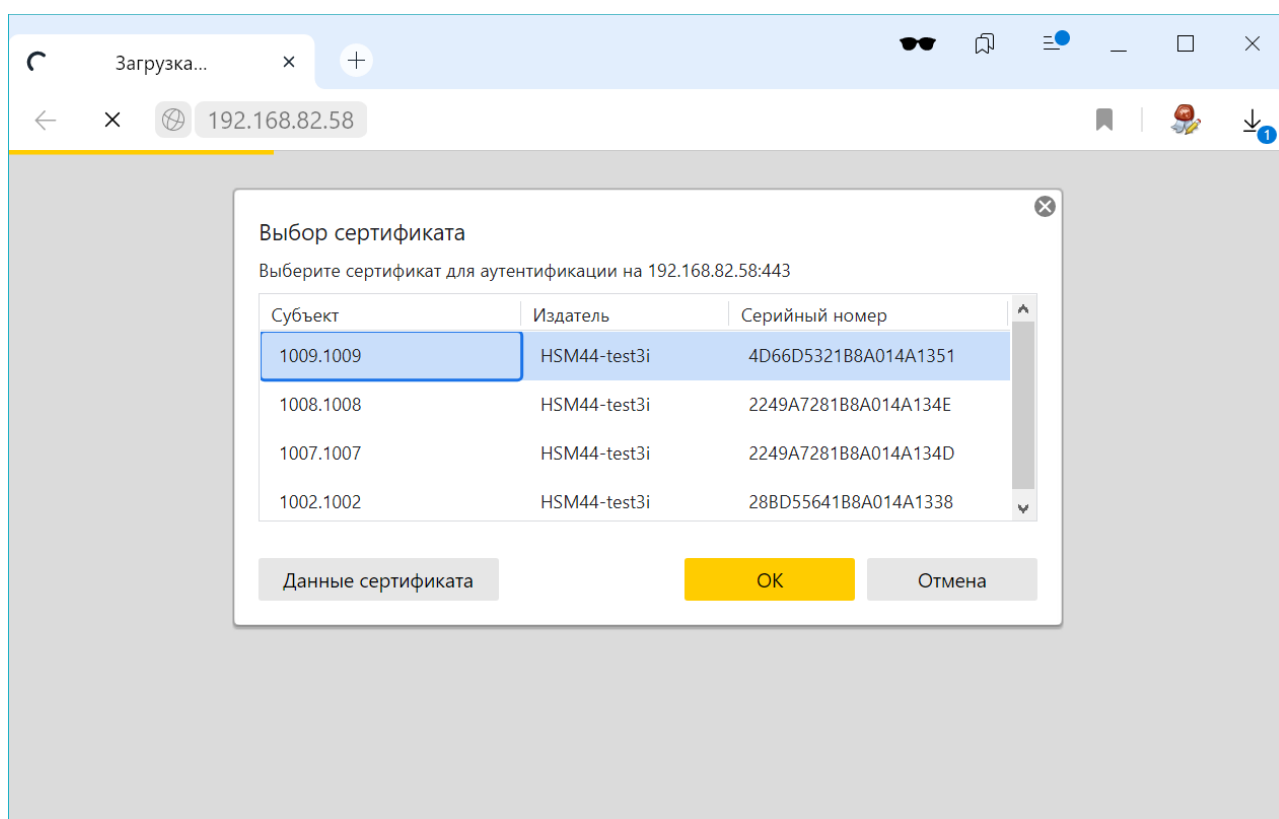
Удаленное администрирование ПАКМ производится привилегированным пользователем при предъявлении (а именно - помещении в считыватель) действующей карты Администратора, Аудитора или Администратора резервного копирования. После

использования такой карты для Web-администрирования эта карта не может быть использована для администрирования с LCD-панели ПАКМ, так как на рабочем месте администратора используется СКЗИ более низкого уровня безопасности, чем ПАКМ, и класс защиты ключей на карте администратора будет понижен до данного уровня.

Настройки рабочего места администратора ПАКМ выполняются в соответствии с пунктом 3.8 данного документа.

6.2. Открытие окна администрирования ПАКМ

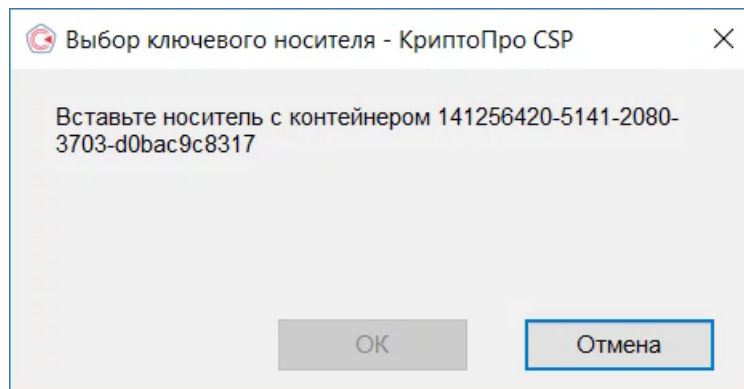
Для открытия страницы администрирования ПАКМ надо ввести в адресной строке Интернет обозревателя IP-адрес ПАКМ (с префиксом `https://`). После подтверждения ввода адреса появится окно «Выбор цифрового сертификата»:



Следует выбрать сертификат и нажать **ОК**.

Если нажать «**Данные сертификата**», появится стандартное окно просмотра сертификата в Windows.

После выбора сертификата и нажатия «**ОК**» может появиться окно-приглашение вставить карту в считыватель, если она не была вставлена:



После того, как карта привилегированного пользователя ПАКМ будет вставлена в считыватель, это окно исчезнет, и появится приглашение ввести pin-код карты. Если во время предыдущего ввода pin-кода был установлен флажок «запомнить», этап ввода pin-кода будет пропущен.

Если двусторонняя аутентификация клиента и сервера произведена успешно, загрузится основная страница APM Web администрирования ПАКМ.

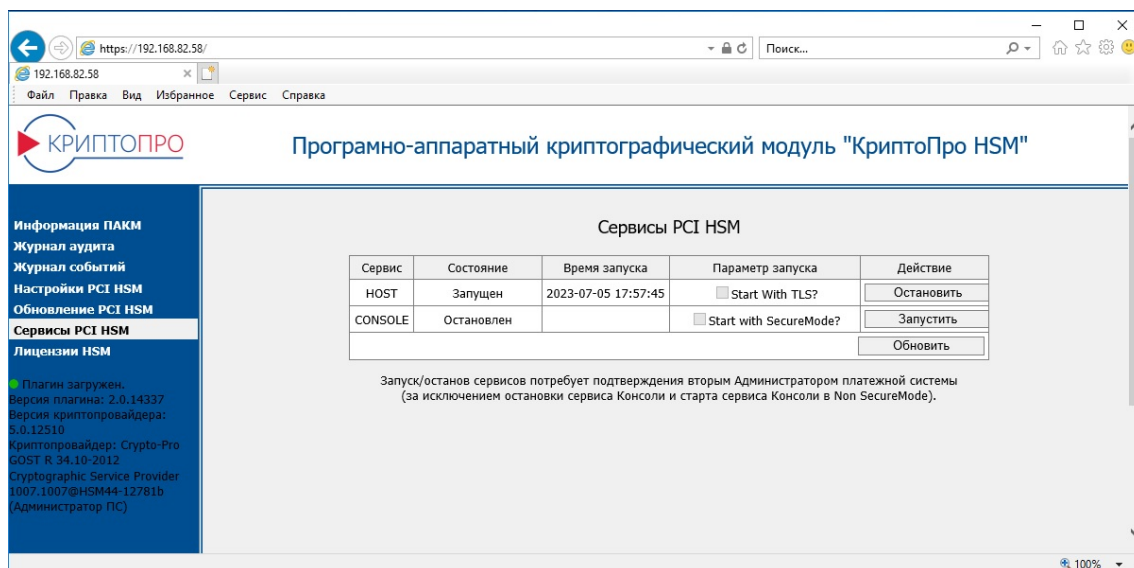
6.3. Работа с окном администрирования ПАКМ

Основная страница APM разбита на 2 части. В левой части отображается основное меню режимов работы. В правой части находится рабочая область, отображающая информацию по выбранному режиму работы основного меню.

Под основным меню отражается также информация о состоянии загруженного плагина: красный индикатор – плагин не загружен, зеленый индикатор – плагин загружен. Для загрузки плагина требуется некоторое время. Если зеленый индикатор при первой загрузке страницы не зажегся, попробуйте просто обновить страницу (F5).

Ещё ниже, под индикатором загрузки плагина, отображается информация о привилегированном пользователе, инициировавшем сессию Web администрирования. Данная информация извлекается из сертификата ключа доступа пользователя, при помощи которого создается защищенный TLS канал для APM Web администрирования, и включает идентификатор пользователя и его роль(и).

Основное меню APM является динамическим, и формируется на основе информации сертификата ключа доступа привилегированного пользователя, а именно его роли. В меню отображаются только те пункты, которые доступны данной роли. Тем не менее, ввиду сложных функциональных взаимосвязей, а также различии прав на чтение и изменение информации, в рабочей области могут встречаться ссылки, режимы, использование которых может быть недоступно данной роли, и при попытке их использования, обычно выдается сообщение об ошибке «Access denied» (доступ запрещён).



Пример окна APM Web администрирования ПАКМ с ограничением по роли – «Администратор платежной системы».

Для удобства восприятия в следующих пунктах данного раздела приводятся снимки экрана с основным меню, не ограниченном по ролям пользователя, инициировавшего сессию APM Web администрирования.

6.3.1. Информация ПАКМ

Для просмотра информации о ПАКМ и изменения времени ПАКМ, изменения состояния или остановки ПАКМ надо выбрать в меню слева пункт «Информация ПАКМ». Изменение времени, состояния или остановка ПАКМ возможны при использовании карточки Администратора ПАКМ.

https://192.168.82.58 x +

192.168.82.58 https://192.168.82.58

КРИПТОПРО Программно-аппаратный криптографический модуль "КриптоПро HSM"

Информация ПАКМ

Информация ПАКМ

Сертификаты ПАКМ
Параметры ПАКМ
Настройки сети
Настройки МЭ
Настройки аудита
Пользователи
Резервные копии
Журнал аудита
скачать
очистить
Журнал событий
Настройки PCI HSM
Обновление PCI HSM
Лицензии HSM

Плагин загружен.

Информация ПАКМ

Серийный номер ПАКМ: HSM44-test3i
Версия сборки ПАКМ: 12722
Build Date: Dec 15 2022 03:40:20
SVN Revision: 2022-12-15 14:26:57 +0300
Текущее время ПАКМ (UTC): 02.03.2023 11:20:40
Доступное пространство на диске в разделе ключей: 29606424
Доступное пространство на диске в разделе backup: 30062568
Количество созданных ключей: 185
Количество выполненных криптографических операций: 1267
Количество зарегистрированных пользователей: 9
в т.ч. привилегированных: 7
Количество единиц ключевого материала (Гаммы) в байтах: 3586320
Загрузка CPU (%): 05.60 (Пик: 05.80 в 2023-03-01 13:56:42)
Использование памяти (%): 06.78 (Пик: 06.78 в 2023-03-02 14:20:40)
Использование пространства в разделе ключей (%): 01.66 (Пик: 01.66 в 2023-03-02 14:20:40)
Общее количество TCP соединений: 00039 (Пик: 00103 в 2023-02-28 10:07:28)
Текущее состояние ПАКМ: FULLACTIVE

Обновить

Дополнительная информация: Получить

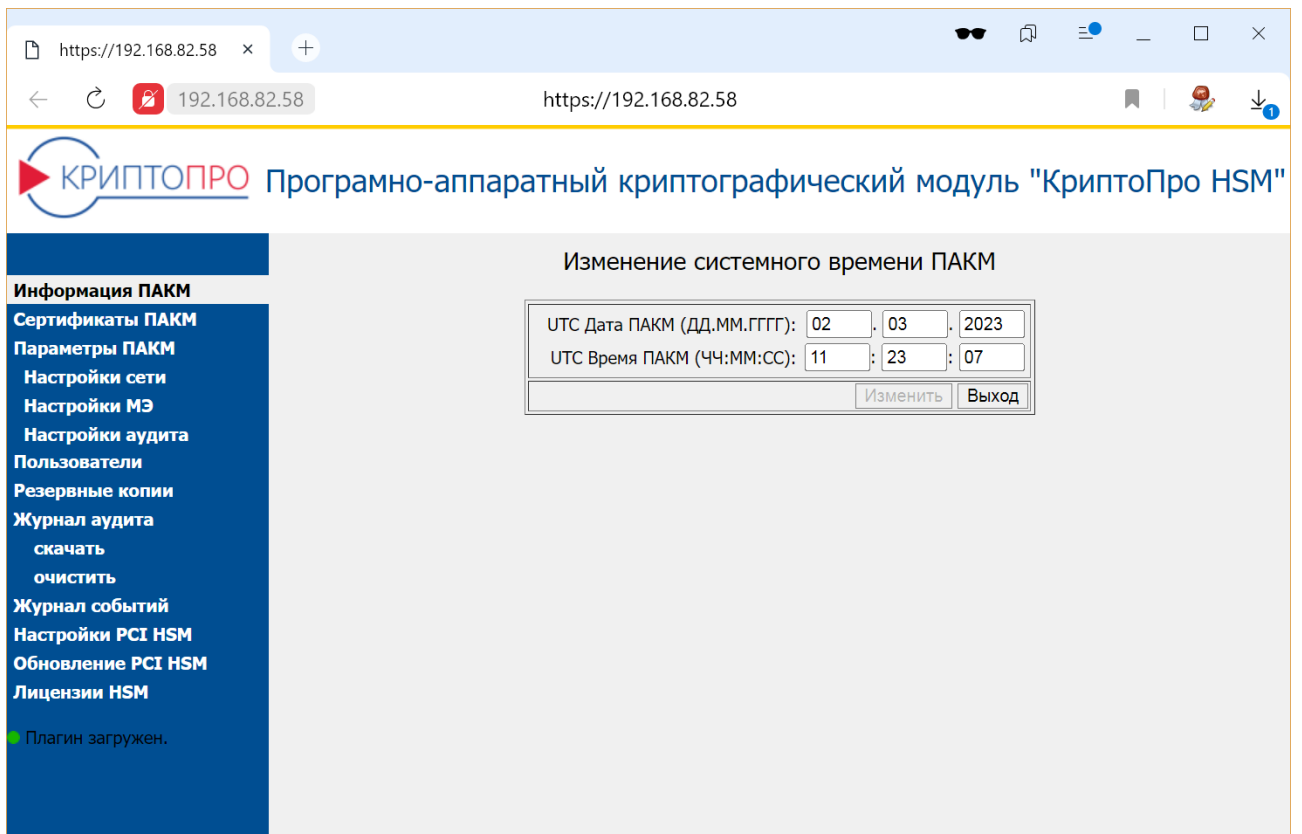
[О TCP/IP соединениях](#) | [Об использовании памяти](#) | [О репликации](#)

Чтобы просмотреть текущие данные ПАКМ, надо нажать кнопку **«Обновить»**.

Кроме базовой информации ПАКМ, в данном окне отображаются текущие и пиковые значения загрузки процессора, оперативной памяти, дисковой памяти и количество TCP соединений с ПАКМ.

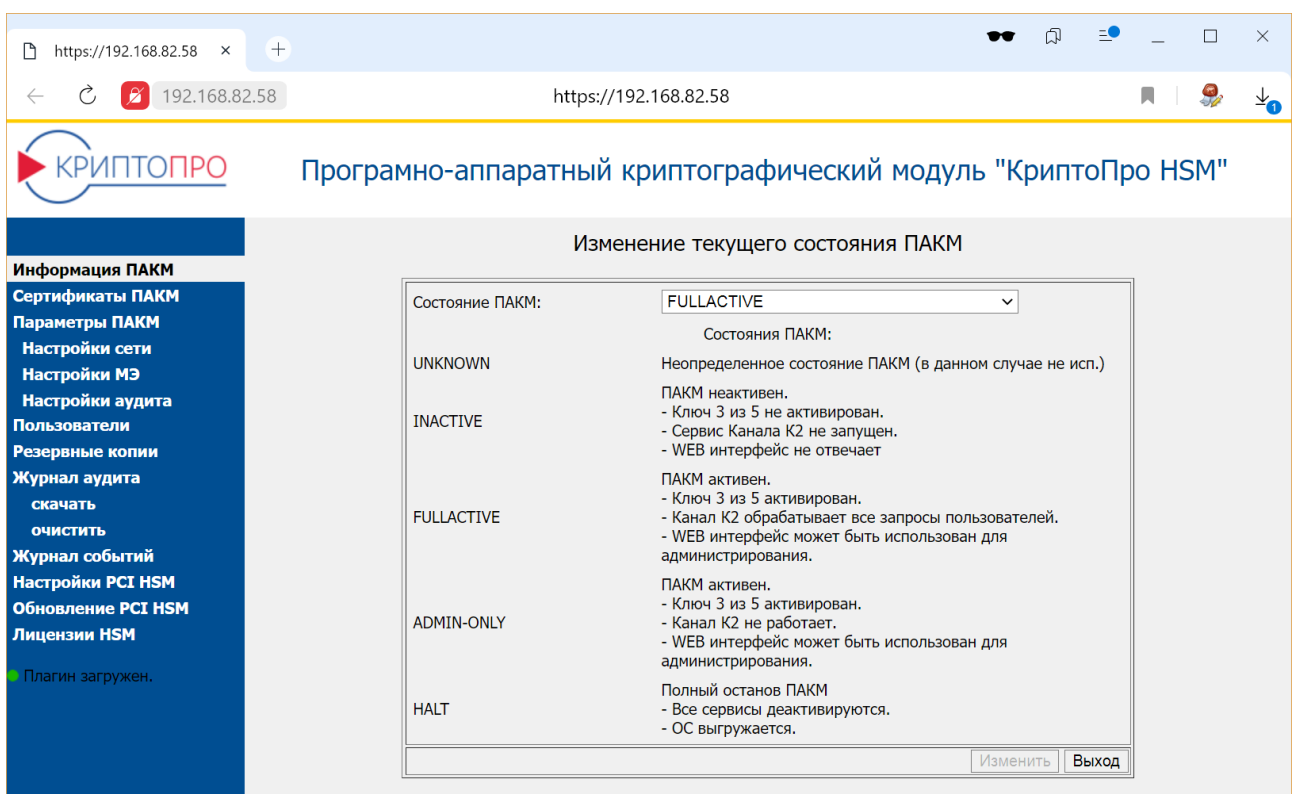
Пиковые значения – это максимальные значения данных параметров с момента последней загрузки или переактивации ПАКМ.

Для изменения даты или времени ПАКМ надо щелкнуть мышью на строке **«Текущее время ПАКМ»**. После этого появится форма для ввода нового времени:



Следует ввести новую дату/время (по UTC) и нажать «**Изменить**». Для отказа надо нажать «**Выход**».

Для изменения состояния ПАКМ или остановки ПАКМ надо щелкнуть мышью на строке «**Текущее состояние ПАКМ**». После этого появится форма для изменения состояния:



Следует выбрать в выпадающем меню нужное состояние и нажать **«Изменить»**, или нажать **«Выход»** для отказа от изменения состояния.

Если изменить состояние на HSM-STATE-HALT, ПАКМ будет выключен.

Если изменить состояние на HSM-STATE-INACTIVE, дальнейшее сетевое администрирование будет невозможно.

Для просмотра списка tcp соединений ПАКМ необходимо нажать на ссылку **«О TCP/IP соединениях»**:

The screenshot shows the 'КриптоПро HSM' web interface. The left sidebar contains a menu with options like 'Информация ПАКМ', 'Сертификаты ПАКМ', 'Параметры ПАКМ', etc. The main area displays 'Информация ПАКМ' with various system metrics and status. Below this, there is a section for 'Дополнительная информация' with a dropdown menu set to 'net/tcp' and a 'Получить' button. The bottom part of the interface shows a list of TCP connections in a table format.

sl	local_address	rem_address	st	tx_queue	rx_queue	tr	tm->when	retrnsmt	uid	timeout	inode
0:	0100007F:006F	00000000:0000	0A	00000000	00000000	00	00000000	00000000	0	0	27653 1 ffff88046a114740 100 0 0 10 0
1:	00000000:1F90	00000000:0000	0A	00000000	00000000	00	00000000	00000000	0	0	38577995 1 ffff8808697f5840 100 0 0 10 0
2:	00000000:1F91	00000000:0000	0A	00000000	00000000	00	00000000	00000000	0	0	38577996 1 ffff8808697f5140 100 0 0 10 0
3:	00000000:1F93	00000000:0000	0A	00000000	00000000	00	00000000	00000000	0	0	21551491 1 ffff8804693e3780 100 0 0 10 0
4:	00000000:0016	00000000:0000	0A	00000000	00000000	00	00000000	00000000	0	0	22875 1 ffff8804693e3080 100 0 0 10 0
5:	021BA8C0:01B8	00000000:0000	0A	00000000	00000000	00	00000000	00000000	0	0	39303766 1 ffff8808697a98c0 100 0 0 10 0
6:	3A52A8C0:01B8	00000000:0000	0A	00000000	00000000	00	00000000	00000000	0	0	39303765 1 ffff8808697f449180 100 0 0 10 0
7:	3A52A8C0:05DD	00000000:0000	0A	00000000	00000000	00	00000000	00000000	0	0	39303773 1 ffff8808697a91c0 100 0 0 10 0
8:	00000000:05DE	00000000:0000	0A	00000000	00000000	00	00000000	00000000	0	0	33128073 1 ffff8808697f449880 100 0 0 10 0
9:	3A52A8C0:0016	CE53A8C0:04E9	01	00000000	00000000	02	00072FE9	00000000	0	0	21017584 2 ffff880466b611c0 22 4 30 10 -1
10:	3A52A8C0:0016	CE53A8C0:69B2	01	00000000	00000000	02	0006A982	00000000	0	0	36656188 2 ffff880466b87040 24 4 30 10 9
11:	0100007F:91BA	0100007F:1F90	01	00000000	00000000	02	0008031C	00000000	1007	0	40998355 3 ffff880869fa4740 20 0 0 10 -1
12:	0100007F:1F90	0100007F:91BA	01	00000000	00000000	00	00000000	00000000	0	0	40994903 1 ffff880869fa4040 20 4 30 10 -1
13:	3A52A8C0:01B8	CE53A8C0:2273	01	00000000	00000000	02	0008031C	00000000	0	0	41050109 4 ffff88046949f880 20 4 27 10 -1
14:	3A52A8C0:0016	CE53A8C0:3C5B	01	00000000	00000000	02	00048FE9	00000000	0	0	21538150 2 ffff88046abd5840 22 4 30 10 70
15:	3A52A8C0:0016	CE53A8C0:06B4	01	00000000	00000000	02	00002982	00000000	0	0	21043718 2 ffff88046a114040 24 4 30 10 -1
16:	3A52A8C0:0016	CE53A8C0:6621	01	00000000	00000000	02	00090FE9	00000000	0	0	28112006 2 ffff880466b618c0 22 4 30 10 -1
17:	0100007F:91B9	0100007F:1F90	06	00000000	00000000	03	0000176D	00000000	0	0	3 ffff88086b14fbc0
18:	3A52A8C0:0016	1753A8C0:E3CB	01	00000000	00000000	02	00036982	00000000	0	0	16706194 2 ffff88046abd5140 22 4 24 10 -1

При этом высветится список всех tcp соединений используемых в данный момент ПАКМ «КриптоПро HSM». Формат списка соответствует содержимому файла /proc/net/tcp в ОС Linux.

Для просмотра информации об использовании оперативной памяти ПАКМ необходимо нажать на ссылку **«Об использовании памяти»**:

https://192.168.82.58

192.168.82.58

https://192.168.82.58

КРИПТОПРО Программно-аппаратный криптографический модуль "КриптоПро HSM"

Информация ПАКМ

Сертификаты ПАКМ

Параметры ПАКМ

Настройки сети

Настройки МЭ

Настройки аудита

Пользователи

Резервные копии

Журнал аудита

Журнал событий

Настройки PCI HSM

Обновление PCI HSM

Лицензии HSM

Плагин загружен.

Информация ПАКМ

Серийный номер ПАКМ:	HSM44-test3i
Версия сборки ПАКМ:	12722
Build Date:	Dec 15 2022 03:40:20
SVN Revision:	2022-12-15 14:26:57 +0300
Текущее время ПАКМ (UTC):	02.03.2023 11:20:40
Доступное пространство на диске в разделе ключей:	29606424
Доступное пространство на диске в разделе backup:	30062568
Количество созданных ключей:	185
Количество выполненных криптографических операций:	1267
Количество зарегистрированных пользователей:	9
в т.ч. привилегированных:	7
Количество единиц ключевого материала (Гаммы) в байтах:	3586320
Загрузка CPU (%):	05.60 (Пик: 05.80 в 2023-03-01 13:56:42)
Использование памяти (%):	06.78 (Пик: 06.78 в 2023-03-02 14:20:40)
Использование пространства в разделе ключей (%):	01.66 (Пик: 01.66 в 2023-03-02 14:20:40)
Общее количество TCP соединений:	00039 (Пик: 00103 в 2023-02-28 10:07:28)
Текущее состояние ПАКМ:	FULLACTIVE

Обновить

Дополнительная информация:

[О TCP/IP соединениях](#) | [Об использовании памяти](#) | [О репликации](#)

MemTotal:	32969652 kB
MemFree:	30741844 kB
MemAvailable:	31623972 kB
Buffers:	159552 kB
Cached:	903172 kB
SwapCached:	0 kB
Active:	1466896 kB
Inactive:	390848 kB

При этом отобразится содержимое файла /proc/meminfo ПАКМ (ОС Linux).

Некоторую дополнительную информацию, предоставляемую операционной системой, можно просмотреть, введя имя системного файла в каталоге (подкаталоге) /proc ОС Linux и нажав кнопку «Получить». Например, если ввести cруinfo, то будет выведено содержимое файла /proc/cруinfo ОС Linux.

Если ПАКМ сконфигурирован для работы в системе горячего резервирования (репликации), то кликнув ссылку «**О репликации**» можно получить информацию о текущем статусе репликации. При этом, если ПАКМ является MASTER сервером репликации, то будет выведена следующая информация:

REPLICATION MASTER

File mysql-bin.000047

Position 79074955

Binlog_Do_DB

Binlog_Ignore_DB information_schema,

указывающая на текущую позицию в файле журнала изменений MASTER сервера репликаций.

Если ПАКМ является SLAVE сервером репликации, то будет выведена следующая информация:

REPLICATION SLAVE

Slave_IO_State	Waiting for master to send event
Master_Host	Localhost
Master_User	Repl
Master_Port	1504
Connect_Retry	60
Master_Log_File	mysql-bin.000047
Read_Master_Log_Pos	78595518
Relay_Log_File	mysql-relay-bin.000040
Relay_Log_Pos	78595664
Relay_Master_Log_File	mysql-bin.000047
Slave_IO_Running	Yes
Slave_SQL_Running	Yes
Replicate_Do_DB	
Replicate_Ignore_DB	
Replicate_Do_Table	
Replicate_Ignore_Table	cpcsp_registry.norepl_config
Replicate_Wild_Do_Table	
Replicate_Wild_Ignore_Table	
Last_Errno	0
Last_Error	
Skip_Counter	0
Exec_Master_Log_Pos	78595518
Relay_Log_Space	78595863
Until_Condition	None
Until_Log_File	
Until_Log_Pos	0
Master_SSL_Allowed	No
Master_SSL_CA_File	
Master_SSL_CA_Path	
Master_SSL_Cert	
Master_SSL_Cipher	
Master_SSL_Key	
Seconds_Behind_Master	0
Master_SSL_Verify_Server_Cert	No
Last_IO_Errno	0
Last_IO_Error	
Last_SQL_Errno	0
Last_SQL_Error	
Replicate_Ignore_Server_Ids	

Master_Server_Id

1,

указывающая на позицию в файле журнала изменений MASTER сервера репликаций, которая была получена при последнем удачном обращении к MASTER серверу для последующего поиска изменений данных, текущее состояние репликации (**Slave_IO_State**), информацию об ошибках репликации (**Last_IO_Errno**, **Last_IO_Error**, **Last_SQL_Errno**, **Last_SQL_Error**) и прочие менее значимые параметры для отслеживания состояния работы механизма репликаций.

6.3.2.Сертификаты ПАКМ

Для просмотра информации о служебных ключах и сертификатах ПАКМ, а также для возможности управления ими, надо выбрать в меню слева пункт «Сертификаты ПАКМ».

Программно-аппаратный криптографический модуль "КриптоПро HSM"

Сертификаты ПАКМ

Сертификаты HSM CA

Доверенные корневые | Промежуточные

Доверенные корневые сертификаты ПАКМ						
Серийный номер	Владелец	Издатель	Действителен с	Действителен по	Алгоритм	Действие
0x645cfbd91b8a014a1313	CN=HSM44-test3i	CN=HSM44-test3i	09.02.2023 16:27:09	09.02.2038 16:27:09	RSA	
0x645cfbd91b8a014a1310	CN=HSM44-test3i	CN=HSM44-test3i	09.02.2023 16:27:09	09.02.2038 16:27:09	GOST 2012 256	сменить
0x645cfbd91b8a014a130b	CN=HSM44-test3i	CN=HSM44-test3i	09.02.2023 15:54:35	09.02.2038 15:54:35	GOST 2012 256	
0x1560d59d1b8a014a12cc	CN=HSM44-test3i	CN=HSM44-test3i	16.12.2022 15:38:05	16.12.2037 15:38:05	GOST 2012 256	

Сертификат подписи журнала аудита

Обновить

Личные сертификаты подписи журнала аудита						
Серийный номер	Владелец	Издатель	Действителен с	Действителен по	Алгоритм	Действие
0x3ea546c21b8a014a1322	CN=HSM AUDIT Signer	CN=HSM44-test3i	11.02.2023 07:54:40	11.02.2033 07:54:40	GOST 2012 256	сменить

Сертификаты TLS сервера ПАКМ

Обновить

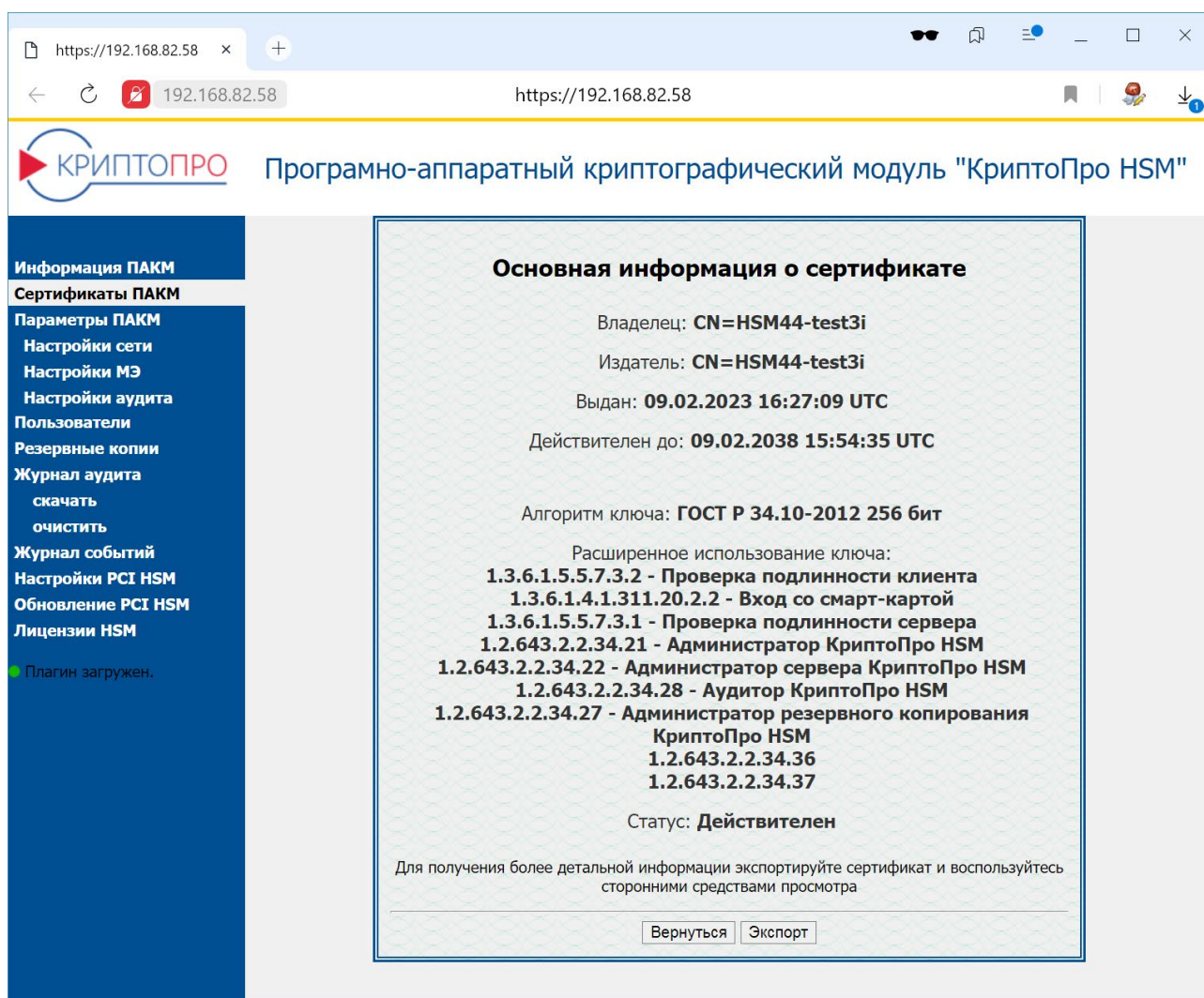
Личные сертификаты TLS сервера ПАКМ						
Серийный номер	Владелец	Издатель	Действителен с	Действителен по	Алгоритм	Действие
0x28bd55641b8a014a133a	CN=192.168.27.2	CN=HSM44-test3i	13.02.2023 15:31:20	13.05.2030 15:31:20	GOST 2012 256	
0x28bd55641b8a014a1339	CN=192.168.82.58	CN=HSM44-test3i	13.02.2023 15:31:20	13.05.2030 15:31:20	GOST 2012 256	
0x3ea546c21b8a014a1321	CN=192.168.27.2	CN=HSM44-test3i	11.02.2023 07:54:04	11.05.2030 07:54:04	GOST 2012 256	удалить

Сменить текущие ключи и сертификаты TLS сервера ПАКМ

Сертификаты Nginx шлюза ПАКМ

В открывшемся окне представлено несколько списков сертификатов ключей ПАКМ из нескольких хранилищ сертификатов ПАКМ.

Для просмотра сертификата в любом списке надо щелкнуть мышью на серийном номере сертификата. После этого откроется окно с основной информацией о сертификате.



Нажав на кнопку «Экспорт», сертификат будет сохранен в «Загрузках» браузера. Там он может быть детально проосмотрен встроенными средствами ОС.

Хранилища сертификатов HSM CA

В списке «Сертификаты HSM CA» представлены корневые сертификаты ключей подписи ПАКМ, при помощи которых издаются сертификаты пользователей ПАКМ. Для текущего корневого сертификата ГОСТ доступно действие «Сменить» (произвести плановую смену ключа и сертификата. Производится обычно раз в 3 года, когда подходит к концу срок действия соответствующего закрытого ключа ЭП).

Кликнув на ссылке «Промежуточные» в данный список будут выведены сертификаты из хранилища «Промежуточных Центров сертификации». В ПАКМ в данном хранилище хранятся только самовыпущенные сертификаты «Старый на новом» и «Новый на старом», создающиеся при плановой смене ключа подписи HSM CA (корневого). Эти сертификаты обеспечивают «непрерывность» функционирования TLS протокола (проверку сертификатов, когда пользователи ПАКМ ещё не успели установить у себя новые самоподписанные корневые сертификаты ПАКМ).

Удаление из хранилищ сертификатов HSM CA и импорт в них сертификатов сторонних УЦ запрещено.

Сертификат ключа подписи журнала аудита ПАКМ

В данном списке присутствует всегда только один сертификат – Сертификат действующего на данный момент ключа ЭП журнала аудита.

Срок действия закрытого ключа – 3 года. Используя действие (ссылку) «сменить», можно произвести плановую смену данного ключа и сертификата.

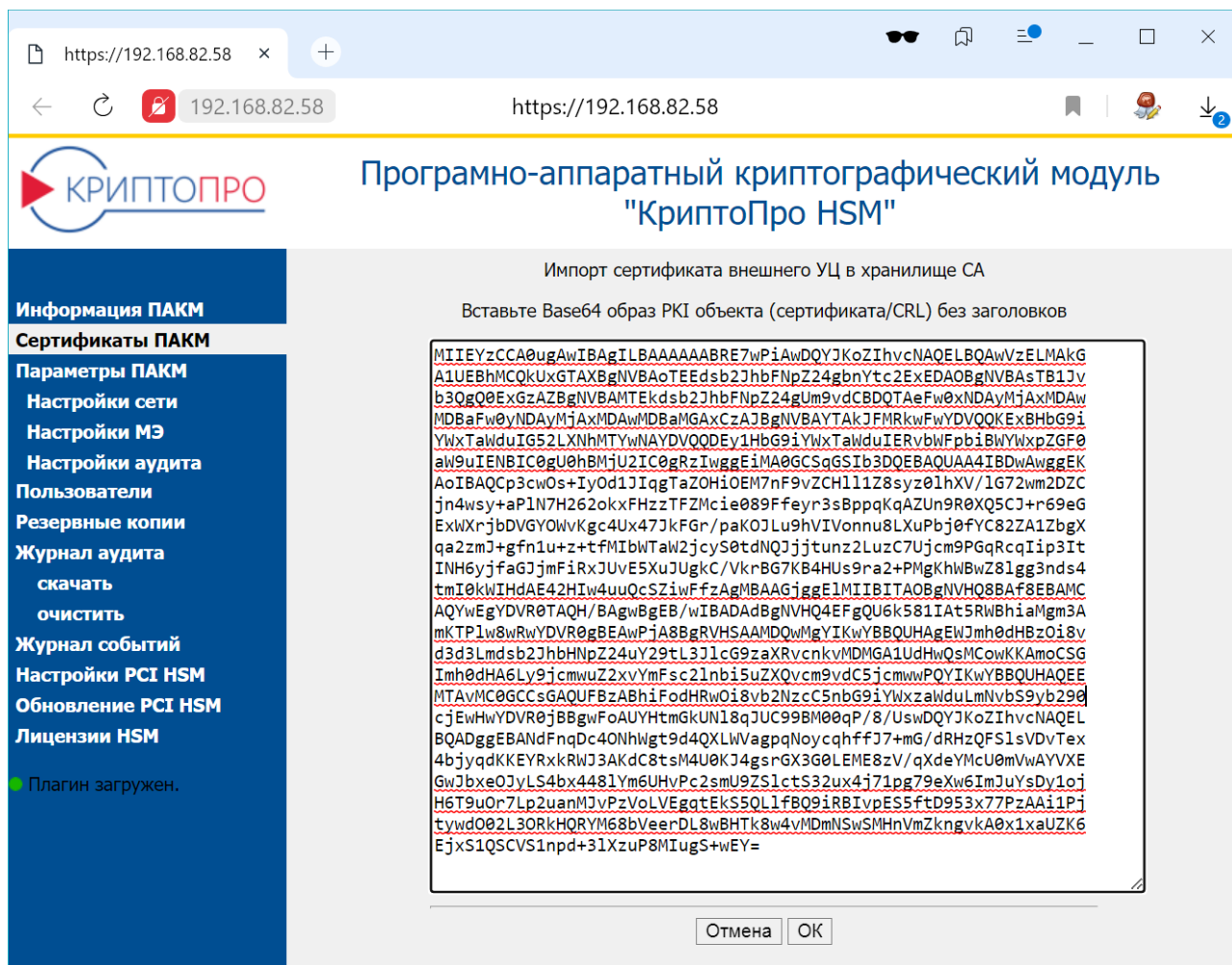
Сертификаты TLS сервера ПАКМ

В данном списке присутствуют сертификаты из личного хранилища сертификатов внутреннего пользователя TlsServer. Данные ключи и сертификаты используются для защиты каналов K2, K2s, канала репликации ПАКМ. При плановой смене ключи и сертификаты Tls сервера формируются для каждого сетевого интерфейса одновременно. В сертификате прописывается IP-адрес сетевого интерфейса. Поэтому если изменяется ip-адрес какого-либо интерфейса, необходимо сменить ключи и сертификаты TLS сервера, используя кнопку «Сменить текущие ключи и сертификаты TLS сервера ПАКМ». Это же действие необходимо использовать при приближении срока окончания действия закрытых ключей (макс. – 3 года).

Используя действие (ссылку) «удалить» можно удалить только старые (выведенные из действия) сертификаты.

Импорт/Установка сертификатов и списков отзыва

При выборе соответствующего режима будет открыто окно, в которое необходимо вставить BASE64 закодированный сертификат/CRL без каких-либо заголовков с типовым для этого формата ограничением длин строк.



После этого необходимо нажать кнопку ОК.

При успешном импорте окно закрывается, а импортированный объект появляется в соответствующем списке-хранилище.

Все выполняемые действия с хранилищем сертификатов доступны Администратору ПАКМ, и отражаются в журнале аудита ПАКМ.

6.3.3. Параметры ПАКМ

Если выбрать в меню слева пункт «Параметры ПАКМ», справа появится форма для просмотра и изменения параметров. Изменение параметров ПАКМ возможно при использовании карточки Администратора ПАКМ.

https://192.168.82.58 x + 192.168.82.58 https://192.168.82.58

КРИПТОПРО Программно-аппаратный криптографический модуль "КриптоПро HSM"

Параметры ПАКМ

Информация ПАКМ
Сертификаты ПАКМ
Параметры ПАКМ
Настройки сети
Настройки МЭ
Настройки аудита
Пользователи
Резервные копии
Журнал аудита
скачать
очистить
Журнал событий
Настройки PCI HSM
Обновление PCI HSM
Лицензии HSM

Плагин загружен.

☒	Разрешить использовать WEB интерфейс администратора ПАКМ
☐	Разрешить использовать канал K0
☒	Разрешить использовать канал K2
☐	Разрешить использовать канал K2s (без шифрования, и только для сервисов)
☒	Разрешить загрузку файлов в ПАКМ (резервные копии, обновления, ...)
☒	Создавать внутреннюю резервную копию БД при выключении HSM (HALT)
☒	Разрешить использование ключевого материала уполномоченной организации (Гаммы) для генерации ключей подписи пользователей
☒	Запретить генерацию ключей подписи при отсутствии ГАММЫ
☒	Разрешить ведение статистики по числу созданных ключей и выполненным криптографическим операциям (ЭП). Требуется переактивации ПАКМ
Количество записей журнала, удаляемое за один запрос в цикле операции очистки журнала аудита (0 - все записи удаляются за один запрос (БД может быть заблокирована на длительное время)):	
100000	
Временной интервал проверки на переполнение (секунд):	
600	
Длительность удерживания неактивного соединения клиента сервером. 0 - не ограничено (секунд):	
0	
Максимальное количество одновременных подключений клиентов к ПАКМ 0 - явно не ограничено, определяется аппаратными и программными ресурсами ПАКМ	
0	
Тип HSM в системе горячего резервирования	
Без резерва	
Уникальный идентификатор HSM в системе горячего резервирования (1-9)	
1	
IP адрес основного HSM в системе горячего резервирования	
000.000.000.000	
Сохранить	

Генерация ключей при отсутствии гаммы разрешается исключительно в тестовых целях.

Опция «Создавать внутреннюю резервную копию БД при выключении HSM (Halt)» влияет на создание временной резервной копии базы данных ПАКМ. Данная копия может быть использована только внутренними механизмами ПАКМ при автовосстановлении БД. Если по каким-либо причинам База данных будет разрушена таким образом, что не сможет стартовать даже сервис управления БД, загрузка ПАКМ будет невозможна. На этот случай в ПАКМ добавлен механизм автоматического пересоздания БД, напоминающий механизм Hard Reset в некоторых электронных устройствах. Т.е. создается абсолютно новая (чистая) БД, сервис СУБД при этом успешно стартует. После этого автоматически ищется файл внутренней резервной копии, о котором идет речь. Если этот файл существует, то все данные в БД восстанавливаются из него. Если этого файла нет, то берется другой файл, сформированный на момент изготовления ПАКМ с настройками по-

умолчанию и хранимый в readonly разделе. Это позволяет в любом случае загрузить ПАКМ и сервисы, отвечающие, как минимум, за работу LCD панели. Далее в зависимости от ситуации можно либо сразу продолжить работу, либо взять последнюю выгруженную резервную копию ПАКМ и восстановить данные с неё.

Остальные опции, присутствующие на данном экране, дублируют опции, описанные в п.5.3.10.

Для изменения параметров следует изменить значения полей на форме и нажать кнопку «**Сохранить**» в нижней части окна.

Если убрать разрешение на использование Web-интерфейса, после сохранения параметров дальнейшее сетевое администрирование будет невозможно.

6.3.4. Настройки сети

Если выбрать в меню слева пункт «Настройки сети», справа появится форма для просмотра и изменения сетевых настроек ПАКМ. Изменение сетевых настроек ПАКМ возможно при использовании карточки Администратора ПАКМ.

192.168.82.58:8080

192.168.82.58:8080

192.168.82.58:8080

КРИПТОПРО Программно-аппаратный криптографический модуль "КриптоПро HSM"

Настройки сети

Сетевой интерфейс eth 0

IP-адрес:
192.168.82.58

Маска подсети:
255.255.255.0

Может использоваться для Web администрирования: ☒

Bonding:
eth0

Сетевой интерфейс eth 1

IP-адрес:
192.168.27.2

Маска подсети:
255.255.255.0

Может использоваться для Web администрирования: ☒

Bonding:
eth1

Default Gateway:
192.168.82.1

Сохранить

Информация ПАКМ
Сертификаты ПАКМ
Параметры ПАКМ
Настройки сети
Настройки МЭ
Настройки аудита
Пользователи
Резервные копии
Журнал аудита
скачать
очистить
Журнал событий
Настройки PCI HSM
Обновление PCI HSM
Лицензии HSM

Плагин загружен.
(Администратор, Аудитор,
Архивариус, Администратор ПС,
Статист)

Для изменения настроек следует изменить значения полей на форме и нажать **«Сохранить»**.

Можно изменить следующие параметры сетевых настроек для каждого сетевого интерфейса: IP-адрес ПАКМ, маску подсети для ПАКМ, признак допустимости использования сетевого интерфейса для канала Web администрирования ПАКМ.

Также важно правильно настроить правила встроенного межсетевого экрана (см. ниже).

Bonding. HSM поддерживает агрегирование нескольких сетевых интерфейсов в один логический. В общем случае, объединенные интерфейсы могут работать в режиме горячего резерва (отказоустойчивости) или в режиме балансировки нагрузки.

В настройках сетевого интерфейса указывается – с какими (другими) сетевыми интерфейсами он агрегируется. Если Bonding не используется, то в качестве связанного сетевого интерфейса отображается идентификатор настраиваемого сетевого интерфейса.

Настройки Bonding-а осуществляются в меню LCD панели ПАКМ.

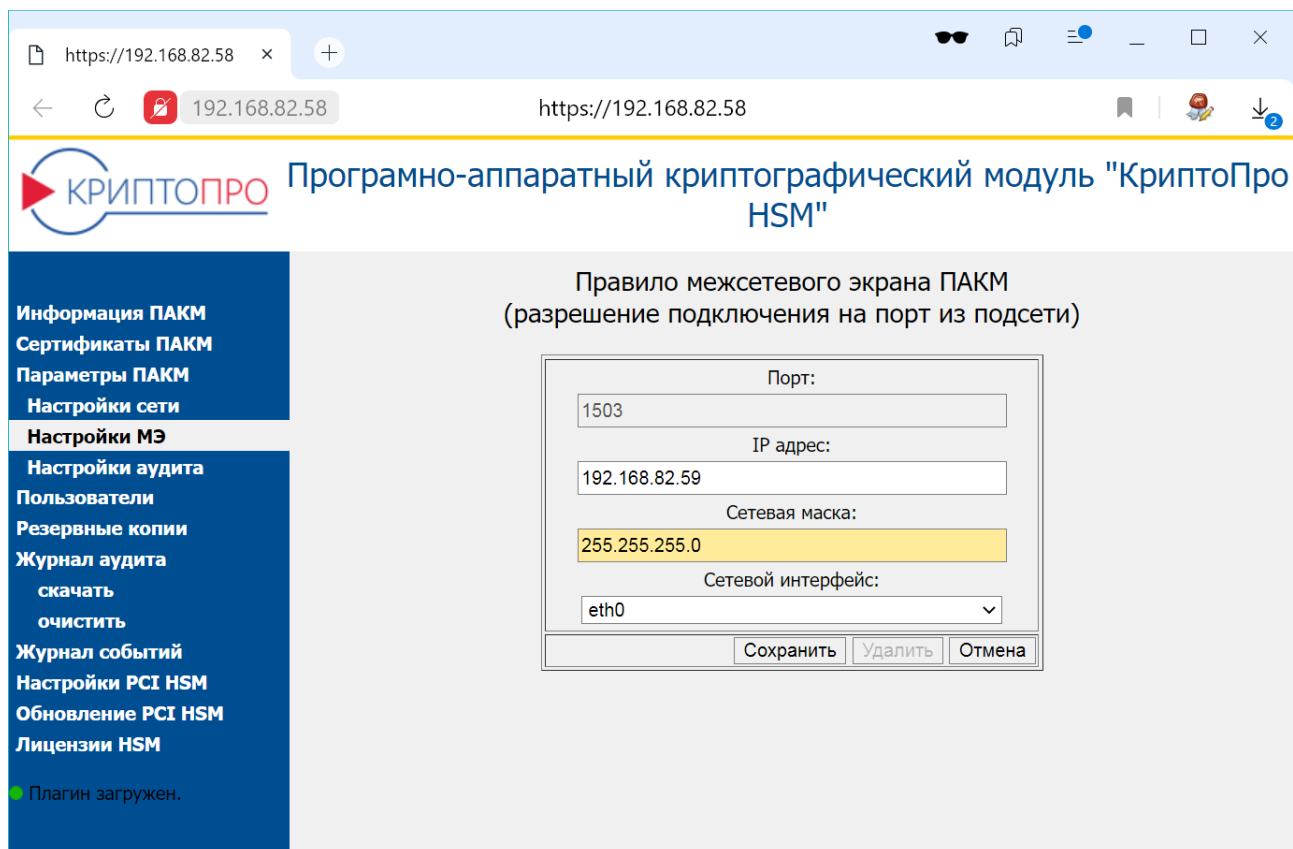
В конце страницы указывается шлюз по умолчанию (Default gateway).

Новые настройки сети вступят в силу после перезапуска сетевых сервисов. Для перезапуска надо перейти на форму «Настройки межсетевого экрана» и щелкнуть мышью на строке **«Перезапустить сетевые сервисы»**.

При изменении IP-адресов сетевых интерфейсов следует пересоздать сертификаты Tls сервера ПАКМ для включения новых IP-адресов в соответствующие сертификаты.

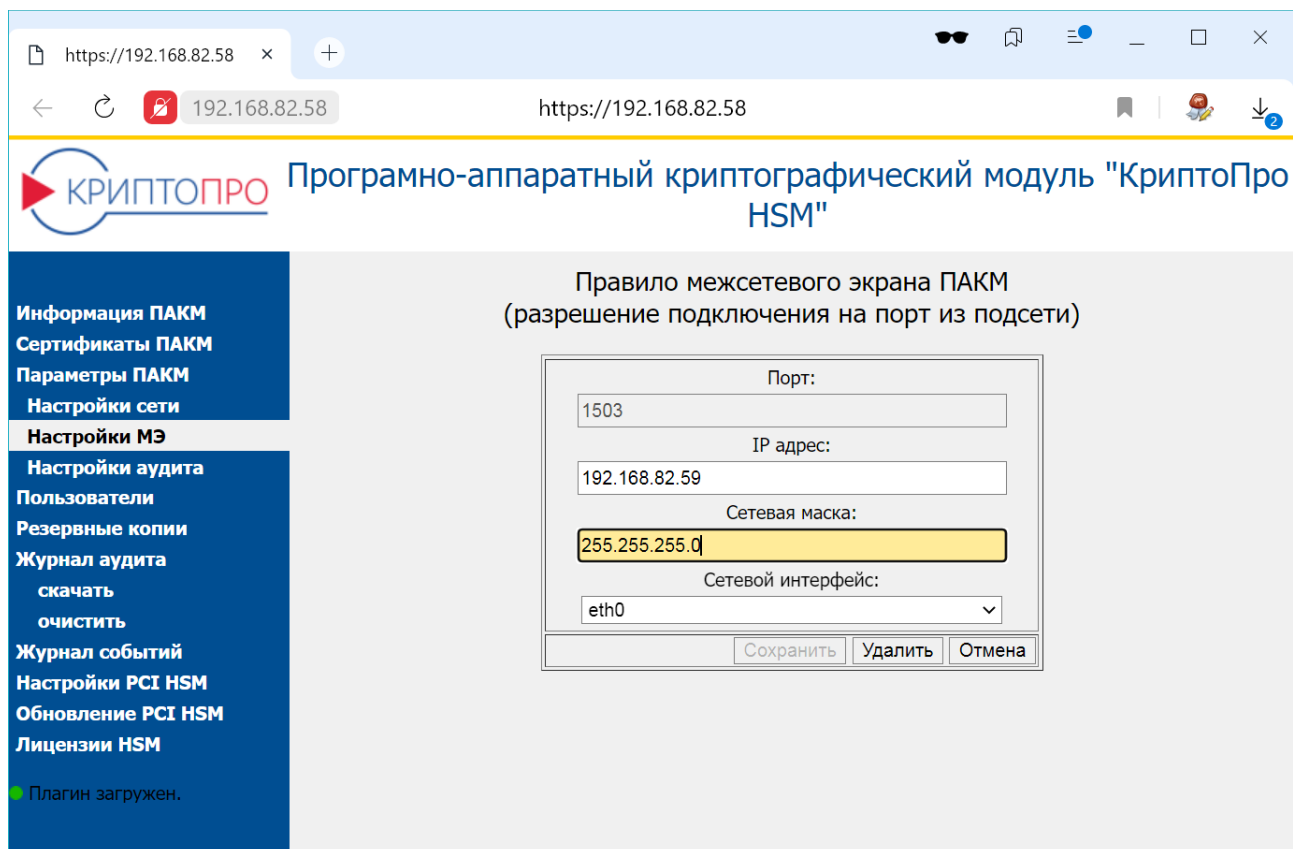
6.3.5. Настройки межсетевого экрана

Если выбрать в меню слева пункт «Настройки МЭ», справа появится форма для просмотра и изменения настроек межсетевого экрана ПАКМ. Изменение настроек межсетевого экрана ПАКМ возможно при использовании карточки Администратора ПАКМ.



Следует ввести адрес и маску и нажать «**Сохранить**». После этого изменение сетевых настроек будет принято.

Для изменения или удаления правила надо щелкнуть мышью на IP-адресе правила. Затем появится форма для редактирования правила:



Для удаления правила надо нажать **«Удалить»**, для изменения надо отредактировать адрес и маску и нажать **«Сохранить»**.

Новые настройки межсетевого экрана вступят в силу после перезапуска межсетевого экрана. Для перезапуска надо щелкнуть мышью на строке «Перезапустить сетевые сервисы» и дождаться сообщения «Задание выполнено успешно».

6.3.6. Настройки аудита

Если выбрать в меню слева пункт «Настройки аудита», справа появится форма для просмотра и изменения параметров аудита ПАКМ. Изменение параметров аудита ПАКМ возможно при использовании карточки Аудитора ПАКМ.

https://192.168.82.58 x +

192.168.82.58 https://192.168.82.58

EVENT_TYPE_REPAIR_AUDIT_LOG		
Удаление ключа EVENT_TYPE_DELETE_KEY	☒	☒
Импорт ключа в ПАКМ EVENT_TYPE_IMPORT_KEY	☐	☐
Создание резервной копии ПАКМ EVENT_TYPE_CREATE_NEW_BACKUP	☒	☒
Удаление резервной копии ПАКМ EVENT_TYPE_DELETE_BACKUP	☒	☒
Восстановление ПАКМ из резервной копии EVENT_TYPE_RESTORE_FROM_BACKUP	☒	☒
Выгрузка резервной копии из ПАКМ EVENT_TYPE_DOWNLOAD_BACKUP	☒	☒
Загрузка резервной копии в ПАКМ EVENT_TYPE_UPLOAD_BACKUP	☒	☒
Изменение настроек аудита ПАКМ EVENT_TYPE_CHANGE_AUDIT_OPTIONS	☒	☒
События ошибок модулей памяти (ECC) EVENT_TYPE_MEMORY_ERROR	☒	☒
Запуск сервисов платежной системы (HOST и CONSOLE) EVENT_TYPE_START_PCI_SERVICE	☒	☒
Останов сервисов платежной системы (HOST и CONSOLE) EVENT_TYPE_STOP_PCI_SERVICE	☒	☒
Смена ключа подписи журнала аудита EVENT_TYPE_CHANGE_AUDIT_SIGNING_KEY	☐	☐
Выполнение команды в консоли платежной системы EVENT_TYPE_PCI_CONSOLE_COMMAND	☒	☒
Изменение прошивки платежной системы EVENT_TYPE_CHANGE_PCIHSM_FIRMWARE	☒	☒
Смена пароля для выполнения неавторизованных операций EVENT_TYPE_CHANGE_UNAUTH_PASSWORD	☒	☒
Доступ к реестру настроек СКЗИ EVENT_TYPE_REGISTRY_ACCESS	☒	☒
Установка лицензий HSM EVENT_TYPE_SET_LICENSE	☒	☒

☐ Разрешить отражать подробную информацию в журнале событий (иначе - отражать только ошибки)

Сохранить

Для изменения параметров следует изменить значения полей на форме и нажать кнопку «**Сохранить**» в нижней части окна.

Чтобы изменения в списке событий, отражаемых в журнале аудита, вступили в силу, необходимо, как минимум, переактивировать ПАКМ.

6.3.7. Пользователи

Если выбрать в меню слева пункт «Пользователи», справа появится форма для просмотра и редактирования данных о пользователях ПАКМ и их ключах доступа к ПАКМ. Редактирование данных о пользователях ПАКМ возможно при использовании карточки Администратора ПАКМ.

Примечание. Фактически в данном разделе ведется информация по ключам и сертификатам доступа к ПАКМ. Понятие «Пользователь» в данном случае равнозначно понятию ключ доступа или карта ключа доступа. Физический пользователь, может иметь несколько ключей (карт) доступа, поэтому в данном разделе ему будет соответствовать несколько записей.

Понятия «Блокировка пользователя», «Удаление пользователя» фактически сводятся к блокировке/удалению указанного ключа и сертификата (карты) доступа.

Пользователи ПАКМ

Введите условия запроса:

Имя пользователя : Номер пользователя:

Идентификатор пользователя: Тип пользователя:

Активность: Окончание срока действия сертификата (yyyyymmddZ):

Найдено 9 записей. Страница № 1 из 1.

Пользователь				Сертификат доступа	Информация	
Идентификатор пользователя	Группа	Имя	Тип	Срок действия	Время создания (UTC)	Время изменения (UTC)
1001.1001@HSM44-test3i	1001	admin_1001.1001	Админ, Аудит, Архив	16.03.2024 15:38:51	16.12.2022 15:38:20	16.12.2022 15:38:53
1002.1002@HSM44-test3i	1002	admin_1002.1002	Админ, Аудит, Архив	13.05.2024 15:30:19	16.12.2022 15:39:24	13.02.2023 15:30:21
1003.1003@HSM44-test3i	1003	admin_1003.1003	АдминПС	16.03.2024 15:41:03	16.12.2022 15:40:26	16.12.2022 15:41:06
1004.1004@HSM44-test3i	1004	admin_1004.1004	АдминПС	16.03.2024 15:42:00	16.12.2022 15:41:24	16.12.2022 15:42:03
1005.1005@HSM44-test3i	1005	User 1	Польз	12.04.2024 14:25:46	12.01.2023 14:19:35	12.01.2023 14:25:46
1006.1006@HSM44-test3i	1006	КриптоПро	Польз		16.02.2023 16:26:22	16.02.2023 16:26:22
1007.1007@HSM44-test3i	1007	Администратор Иванов	Админ	27.05.2024 14:04:59	27.02.2023 13:59:31	27.02.2023 14:04:59
1008.1008@HSM44-test3i	1008	Администратор Петров	Админ	27.05.2024 14:08:54	27.02.2023 14:07:29	27.02.2023 14:08:54
1009.1009@HSM44-test3i	1009	Аудитор Сидоров	Аудит	28.05.2024 07:02:37	28.02.2023 07:01:25	28.02.2023 07:02:37

В форме имеется таблица со списком всех зарегистрированных в ПАКМ пользователей. В таблице указаны идентификатор пользователя, номер пользователя (UID), имя и тип пользователя, срок действия сертификата, время создания информации (по UTC) о пользователе и время ее последнего изменения. Выделение розовым цветом означает, что пользователь заблокирован. Для просмотра других страниц списка в заголовке списка имеются ссылки «>>>» / «<<<» (следующая/предыдущая страница) и «>|» / «|<» (последняя/первая страница).

Если требуется просмотреть часть списка выборочно, надо ввести условия запроса в верхней части таблицы и щелкнуть мышью на строке «**Применить фильтр**». Если

требуется просмотреть весь список, надо очистить условия запроса и применить фильтр снова.

Если требуется просмотреть, изменить или удалить пользователя, надо щелкнуть мышью на идентификаторе пользователя. После этого справа появится форма с информацией о пользователе ПАКМ:

The screenshot shows a web browser window with the URL <https://192.168.82.58>. The page title is "Программно-аппаратный криптографический модуль "КриптоПро HSM"". The left sidebar contains a menu with the following items: "Информация ПАКМ", "Сертификаты ПАКМ", "Параметры ПАКМ", "Настройки сети", "Настройки МЭ", "Настройки аудита", "Пользователи" (highlighted), "Резервные копии", "Журнал аудита", "скачать", "очистить", "Журнал событий", "Настройки PCI HSM", "Обновление PCI HSM", "Лицензии HSM", and "Плагин загружен.". The main content area is titled "Информация о пользователе ПАКМ" and displays the following details for the user "Администратор Иванов":

Имя пользователя:	Администратор Иванов
Тип пользователя:	Администратор
Идентификатор пользователя:	1007.1007@HSM44-test3i
Номер пользователя:	1007
Номер группы пользователя:	1007
Время создания (UTC):	27.02.2023 13:59:31
Время изменения (UTC):	27.02.2023 14:04:59

Below the table, there is a "Блокировать" button. Underneath, the "Сертификат доступа" section shows "UTC Время действия (до): 27.05.2024 14:04:59" and a checkbox for "Использовать готовый PKCS10 запрос:" which is currently unchecked. A "Сменить" button is located next to the checkbox. At the bottom of the form, there are three buttons: "Сохранить", "Удалить", and "Выход".

Для возврата к форме просмотра пользователей надо нажать «**Выход**».

Для изменения имени пользователя надо откорректировать значение поля «**Имя пользователя**». После этого кнопка «**Сохранить**» станет активной, и для сохранения имени пользователя надо ее нажать. Для блокирования пользователя надо нажать кнопку «**Блокировать**». Если пользователь блокирован, надо нажать кнопку «**Разблокировать**»:

https://192.168.82.58

КРИПТОПРО Программно-аппаратный криптографический модуль "КриптоПро HSM"

Информация о пользователе ПАКМ

Имя пользователя:	Аудитор Сидоров
Тип пользователя:	Аудитор
Идентификатор пользователя:	1009.1009@HSM44-test3i
Номер пользователя:	1009
Номер группы пользователя:	1009
Время создания (UTC):	28.02.2023 07:01:25
Время изменения (UTC):	03.03.2023 08:25:24

Разблокировать

Сертификат доступа

UTC Время действия (до): 28.05.2024 07:02:37

Использовать готовый PKCS10 запрос: ☐

Сменить

Сохранить Удалить Выход

Для удаления пользователя надо нажать кнопку **«Удалить»**. После этого появится окно с просьбой подтвердить удаление:

https://192.168.82.58

КРИПТОПРО Программно-аппаратный криптографический модуль "КриптоПро HSM"

Подтвердите действие на сайте 192.168.82.58

Удаление пользователя ПАКМ.
Будут удалены:
- учетная запись пользователя
- ключевые контейнеры пользователя и группы
- пользователи, входящие в данную группу
Продолжить?

Да Нет

Время изменения (UTC): 16.02.2023 16:26:22

Блокировать

Сертификат доступа

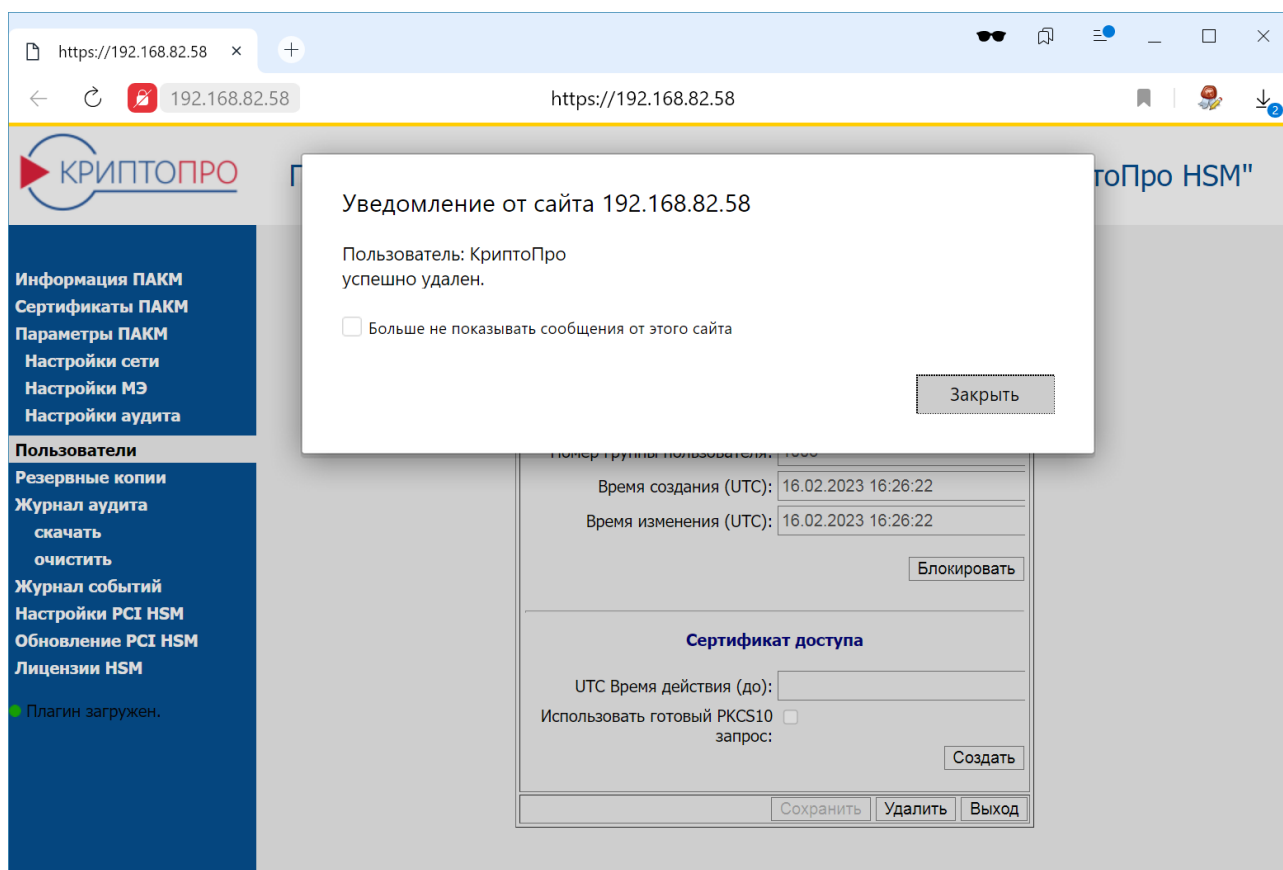
UTC Время действия (до):

Использовать готовый PKCS10 запрос: ☐

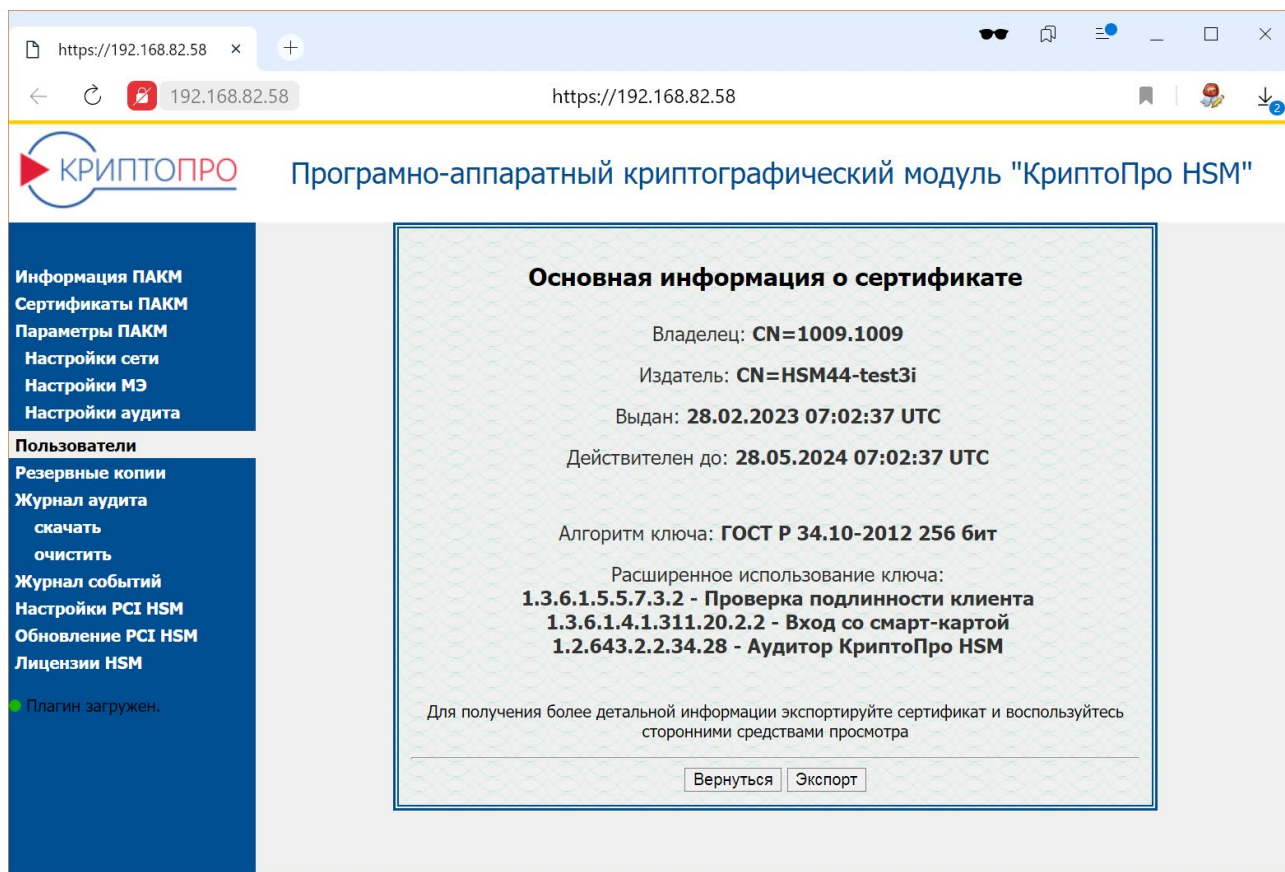
Создать

Сохранить Удалить Выход

Если нажать «**ОК**», пользователь будет удален, о чем появится сообщение:



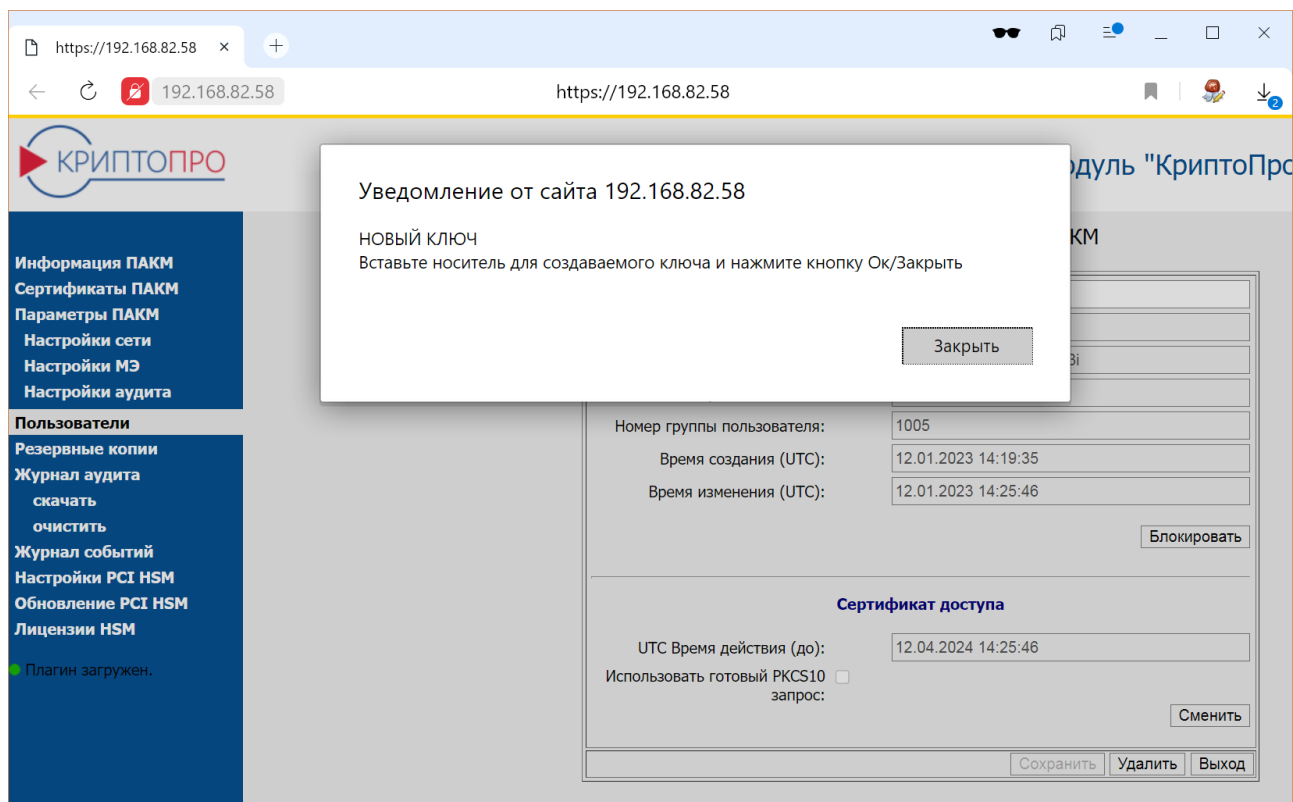
Для просмотра сертификата доступа надо щелкнуть мышью на строке «**Сертификат доступа**». После этого появится окно просмотра основных свойств сертификата.



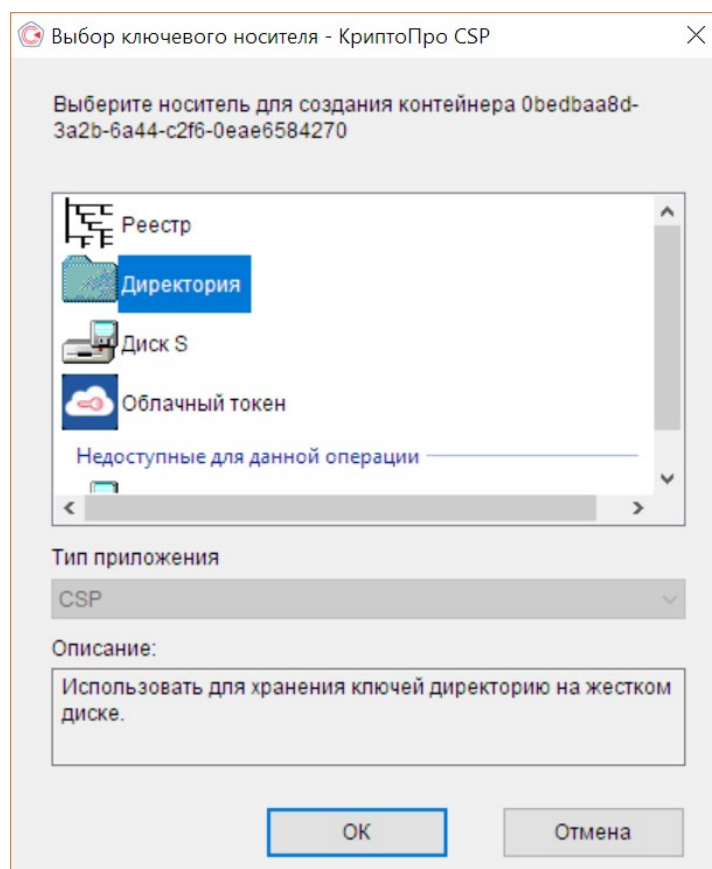
Для просмотра всех свойств сертификата его можно экспортировать и воспользоваться штатными средствами ОС и утилит КриптоПро.

Для смены сертификата надо нажать кнопку **«Сменить»** в окне просмотра информации о пользователе.

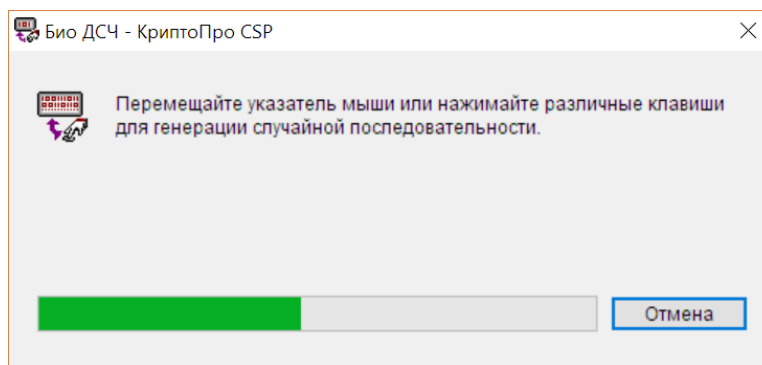
При этом, если не указана опция «Использовать готовый PKCS10 запрос», то вначале будет создана ключевая пара (закрытый и открытый ключ доступа):



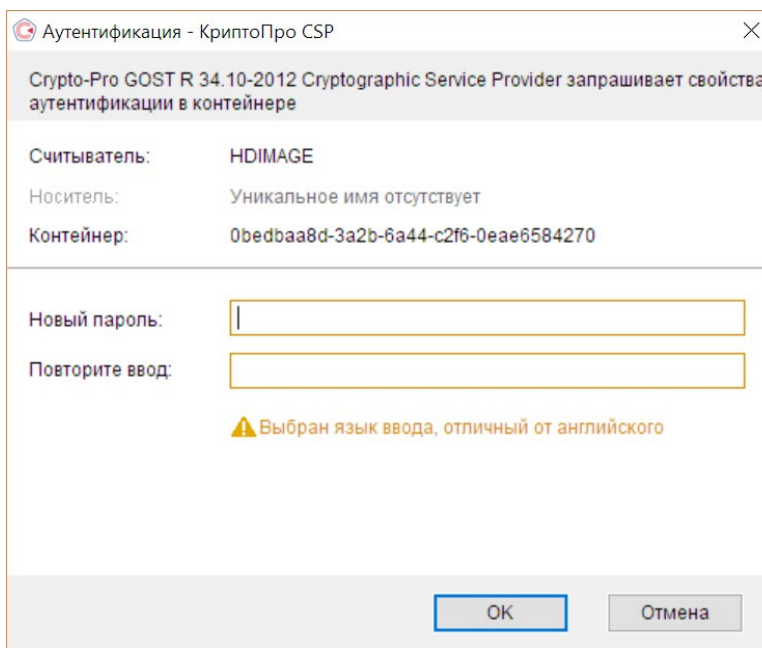
Если нажать «ДА», появится приглашение выбрать устройство для считывания и вставить ключевой носитель:



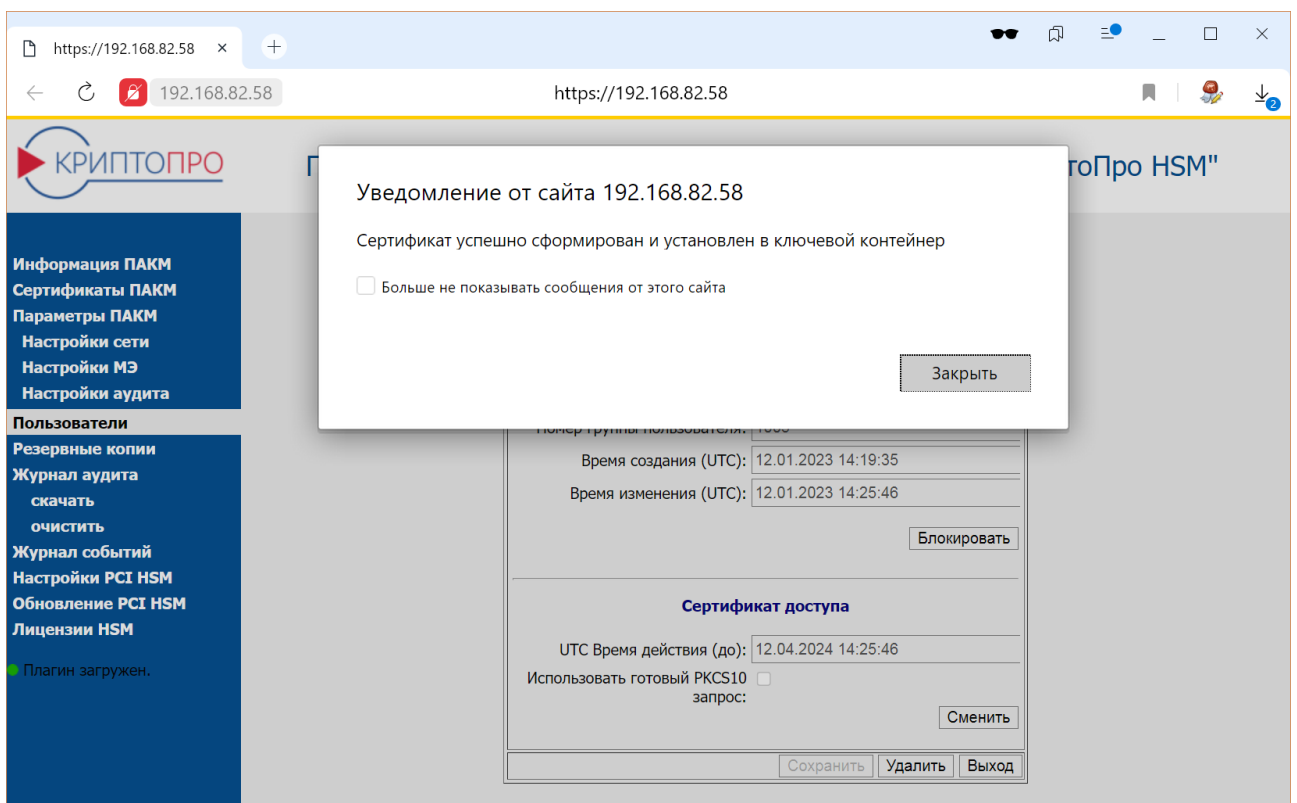
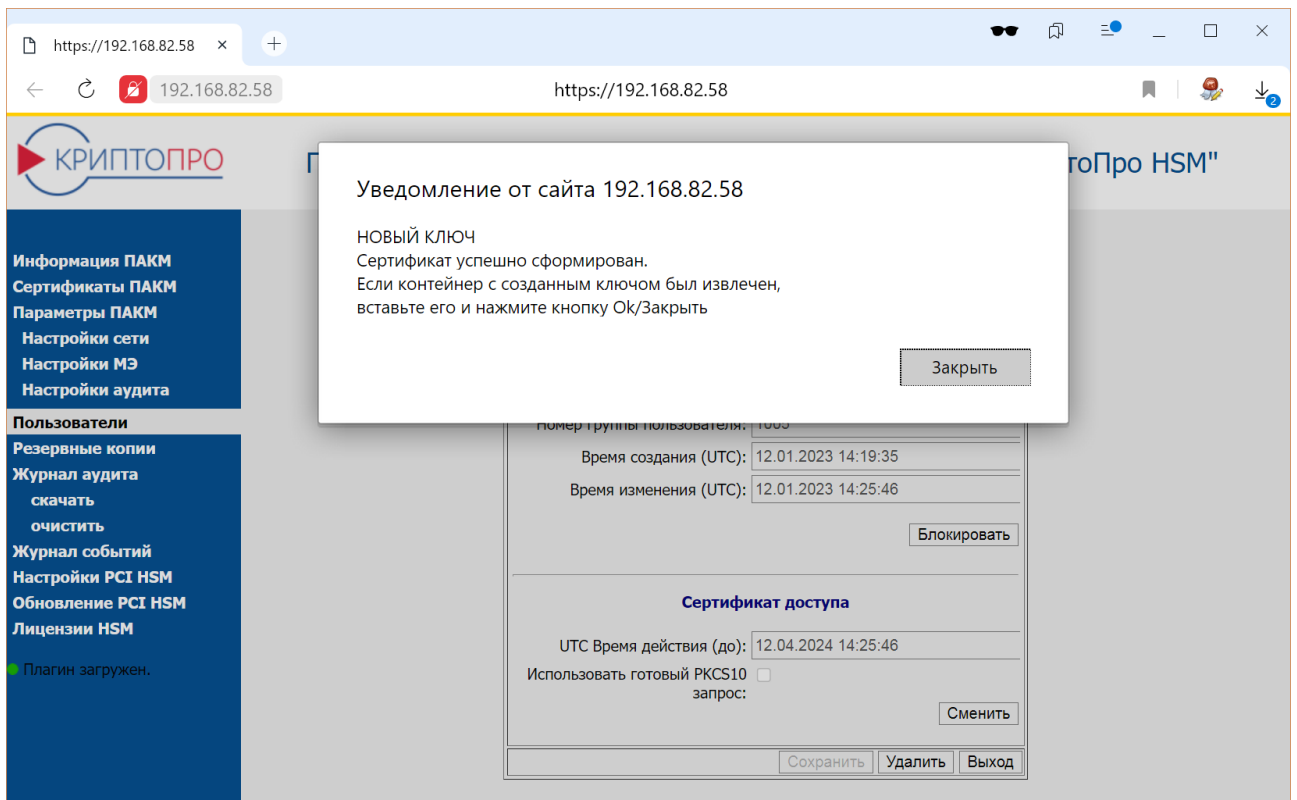
Если вставить носитель в устройство и нажать «ОК», появится окно формирования ключа. Для создания ключа надо перемещать над окном указатель мыши или нажимать клавиши на клавиатуре.



После создания ключа окно закроется. После этого новый сертификат будет создан, появится окно для ввода нового pin-кода для доступа к созданному закрытому ключу:



После ввода нового pin-кода и нажатия Ок появится сообщение:



Если при смене сертификата указана опция «Использовать готовый PKCS10 запрос», то ключевая пара должна быть создана заранее на целевой машине/устройстве (например, в некоторых Unix подобных системах, где нет возможности использовать смарт-карты или другие ключевые носители, кроме как внутреннюю память самого устройства). Вместе с формированием ключа должен быть создан и запрос на сертификат

в формате самоподписанного PKCS#10 запроса. Данный запрос должен быть представлен в BASE64 кодировке с заголовками «-----BEGIN NEW CERTIFICATE REQUEST-----», «-----END NEW CERTIFICATE REQUEST-----».

Запрос в таком виде вставляется в открывающееся для этого окно:

https://192.168.82.58

192.168.82.58

https://192.168.82.58

КРИПТОПРО Программно-аппаратный криптографический модуль "КриптоПро HSM"

Информация ПАКМ
Сертификаты ПАКМ
Параметры ПАКМ
Настройки сети
Настройки МЭ
Настройки аудита

Пользователи
Резервные копии
Журнал аудита
скачать
очистить
Журнал событий
Настройки PCI HSM
Обновление PCI HSM
Лицензии HSM

Плагин загружен.

Информация о пользователе ПАКМ

Имя пользователя: Василий Петров
Тип пользователя: Обычный Пользователь
Идентификатор пользователя: 1035.1035@alt_test
Номер пользователя: 1035
Номер группы пользователя: 1035
Время создания: 29.02.2012 10:39:48
Время изменения: 29.02.2012 10:39:48

Блокировать

Сертификат доступа

Время действия (до):
Использовать готовый PKCS10 запрос: ☒

Вставьте текст PKCS10 запроса (base64 с заголовком):

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIICAzCCAbICAQAwFDESMBAGA1UEAwMTAwNi4xMDA2MGMwHAYGKoUDAgITMBIG
ByqFAwICJAEGByqFAwICHgEDQwAEQBDpC1PLJ4mmUkFZyXLZY1wV19381qowEa
Nt9SSLYkrq0oHsmnt84Vo3pXcBsozmQ1LcTcdjaWu992Y8kNEdggggEwMBoGCisG
AQQBggjcnAgMxDBYKNi4xLjc2MDEuMjA9BgkqhkiG9w0BCQ4xMDAuMA0GA1UdDwEB
/wQDAwEAMB0GA1UdDgQWBH2ICXUGAKfn4ggHcqIj12dEoTtDBBBgkrBgEAYI3
FRQxNDAYAgEFDA9MSU1BTkNFVjcuY3AucnUMCENQXGFsZXhsDBJDZXJ0RW5yb2xs
Q3RybC5leGUwY8GCisGAQQBgjcNAgIxgYAwFgIBAR52AEMAcgB5AHAAdABvAC0A
UABYAG8AIAAHAE8AUwBUACAAUgAgADMANAuADEAMAAtADIAMAAdADEAIAADAHIA
eQBwAHQABwBnAHIAyQSwAGGAAQSBjACAAUwB1AHIAAgBpAGMAZQAgaFAAcgBvAHYA
aQBkAGUAcmMBADAIBgYqhQMCAGMDQwBsiNFsC4BPeNf4urhlvR9vJXKA7HN3j8CF
rBi/bTOtFm/icTpwe43D3qRXZimobTwyKSVdW1V714/IgRBgoQX6
-----END NEW CERTIFICATE REQUEST-----
```

Создать

Сохранить Удалить Выход

После вставки запроса необходимо нажать кнопку «Создать» (или «Обновить», если производится смена сертификата).

При этом важно, чтобы запрос содержал отличительное имя субъекта (Subject DN) в виде «CN=UUUU.GGGG», где UUUU – «номер пользователя», а GGGG – «номер группы пользователя», для которого производится создание/обновление сертификата. Использовать в запросе какие-либо расширения бессмысленно, т.к. ПАКМ «КриптоПро HSM» сам формирует их, исходя из описания пользователя, хранящегося у него в БД.

При расхождении номеров пользователя и/или группы, а также при использовании недопустимых криптографических алгоритмов в запросе будет выдано сообщение об ошибке. При успешном завершении операции будет выдано сообщение: «Сертификат

успешно сформирован. Экспортируйте и установите его в ключевой контейнер». Для экспорта сертификата используйте ссылку «Сертификат доступа», при клике по которой откроется стандартное окно ОС «Windows» просмотра сертификата.

Если требуется добавить пользователя, в форме просмотра пользователей надо щелкнуть мышью на строке-ссылке **«Создать нового пользователя»**:

В появившейся форме надо ввести имя и тип пользователя (обычный пользователь, компьютер (администратор сервера) или один из типов привилегированных пользователей ПАКМ):

The screenshot shows a web browser window with the address bar displaying 'https://192.168.82.58'. The page title is 'Программно-аппаратный криптографический модуль "КриптоПро HSM"'. The main content area is titled 'Создание пользователя ПАКМ' (Create PAKM user). On the left, there is a blue sidebar menu with the following items: 'Информация ПАКМ', 'Сертификаты ПАКМ', 'Параметры ПАКМ', 'Настройки сети', 'Настройки МЭ', 'Настройки аудита', 'Пользователи' (highlighted), 'Резервные копии', 'Журнал аудита' (with sub-items 'скачать' and 'очистить'), 'Журнал событий', 'Настройки PCI HSM', 'Обновление PCI HSM', 'Лицензии HSM', and 'Плагин загружен.' (with a green dot icon). The main form contains the following fields: 'Имя пользователя:' (text input), 'Тип пользователя:' (dropdown menu with 'Обычный пользователь' selected), and 'Является членом группы (UID):' (checkbox, currently unchecked). Below these fields is a text input for the group name. At the bottom right of the form are two buttons: 'Далее' (Next) and 'Отмена' (Cancel).

Если пользователь является членом какой-либо группы, необходимо отметить опцию «Является членом группы» и ввести номер существующей группы пользователей ПАКМ.

Затем надо нажать кнопку **«Далее»**. После этого пользователь будет создан, и появится форма с информацией о пользователе:

The screenshot shows a web browser window with the URL <https://192.168.82.58>. The page title is "Программно-аппаратный криптографический модуль "КриптоПро HSM"". The left sidebar contains a menu with the following items: "Информация ПАКМ", "Сертификаты ПАКМ", "Параметры ПАКМ", "Настройки сети", "Настройки МЭ", "Настройки аудита", "Пользователи", "Резервные копии", "Журнал аудита", "Журнал событий", "Настройки PCI HSM", "Обновление PCI HSM", "Лицензии HSM", and "Плагин загружен.". The main content area is titled "Информация о пользователе ПАКМ" and displays the following user details:

Имя пользователя:	Пользователь Кузнецов
Тип пользователя:	Обычный Пользователь
Идентификатор пользователя:	1010.1010@HSM44-test3i
Номер пользователя:	1010
Номер группы пользователя:	1010
Время создания (UTC):	03.03.2023 09:04:55
Время изменения (UTC):	03.03.2023 09:04:55

Below the user information, there is a "Сертификат доступа" section with the following fields and buttons:

UTC Время действия (до):	
Использовать готовый PKCS10 запрос:	☐

Buttons at the bottom of the form include "Блокировать", "Создать", "Сохранить", "Удалить", and "Выход".

Для создания сертификата пользователя надо нажать кнопку «**Создать**». Дальнейшая процедура создания сертификата аналогична процедуре смены сертификата, которая описана выше.

При выполнении операций с учетными записями привилегированных пользователей потребуется подтверждение вторым администратором ПАКМ!

Порядок выполнения подобных операций описан в разделе "Особенности выполнения операций, требующих подтверждения вторым привилегированным пользователем".

6.3.8. Особенности выполнения операций, требующих подтверждения вторым привилегированным пользователем

Некоторые ответственные операции, производимые в Web интерфейсе администрирования ПАКМ требуют участия двух привилегированных пользователей ПАКМ. Обычно одним из них является привилегированный пользователь, начинающий сеанс Web администрирования на своем ключе доступа. Данный пользователь вставляет карту с ключом доступа в считыватель и в браузере открывает страницу удаленного администрирования ПАКМ. Желательно, чтобы данная карта с ключом постоянно находилась в считывателе.

При выполнении операций, требующих подтверждения вторым привилегированным пользователем, в определенный момент необходимо будет предоставить ключ доступа этого (второго) администратора для формирования ЭП под данными операции, подтверждающей выполнение этой операции. Если при этом сама операция включает работу с ключами и ключевыми контейнерами пользователей (генерация ключа, установка сертификата в контейнер), то может потребоваться и считыватель для этих контейнеров.

В таких случаях крайне желательно, чтобы рабочее место Web администрирования было оборудовано двумя считывателями смарт-карт. В одном считывателе всегда должна находиться карта пользователя, инициировавшего сессию web администрирования, а другой считыватель может быть использован для ключа второго, подтверждающего администратора и для генерируемых ключей пользователей.

Подобные операции сопровождаются окнами с указаниями и предупреждениями о том, какую карту с каким контейнером необходимо в данный момент вставить, чтобы не запутаться, на тот случай, если присутствует только один считыватель смарт-карт.

Все операции подтверждения включают в себя подпись данных операции на ключе подтверждающего пользователя. Механизм напоминает двухфакторную аутентификации. В начале данные операции отправляются на сервер, который вырабатывает специальный уникальный токен для данной операции, запоминает его у себя и начинает отсчет времени для ограничения транзакции «по времени» (5 минут), и отправляет данные вместе со своим уникальным токеном обратно браузеру. В браузере эти данные показываются подтверждающему пользователю и запрашивается ключ подтверждающего пользователя для формирования ЭП под пришедшими с сервера данными. Подтверждающий подписывает эти данные и отправляет обратно на сервер вместе с ЭП. Сервер находит у себя в таблице токенов данные по операции, проверяет время действия токена, сверяет данные операции, проверяет подпись, проверяет, что используемые ключи доступа для проведения операции и для подписи – разные. Если все проверки прошли успешно, то операция на сервере проводится. В журнале аудита при этом в строковых данных отображается информация о пользователе, подтвердившем операцию.

На настоящий момент следующие операции требуют подтверждения:

- Добавление нового привилегированного пользователя ПАКМ ;
- Изменение атрибутов привилегированного пользователя;
- Удаление привилегированного пользователя ;
- Временная Блокировка/разблокировка доступа привилегированного пользователя;
- генерация нового сертификата ключа доступа/аутентификации привилегированного пользователя ПАКМ;

- Очистка журнала аудита ПАКМ.

Пример выполнения операции с подтверждением (наиболее сложный) – создание ключа доступа и соответствующего сертификата для нового привилегированного пользователя.

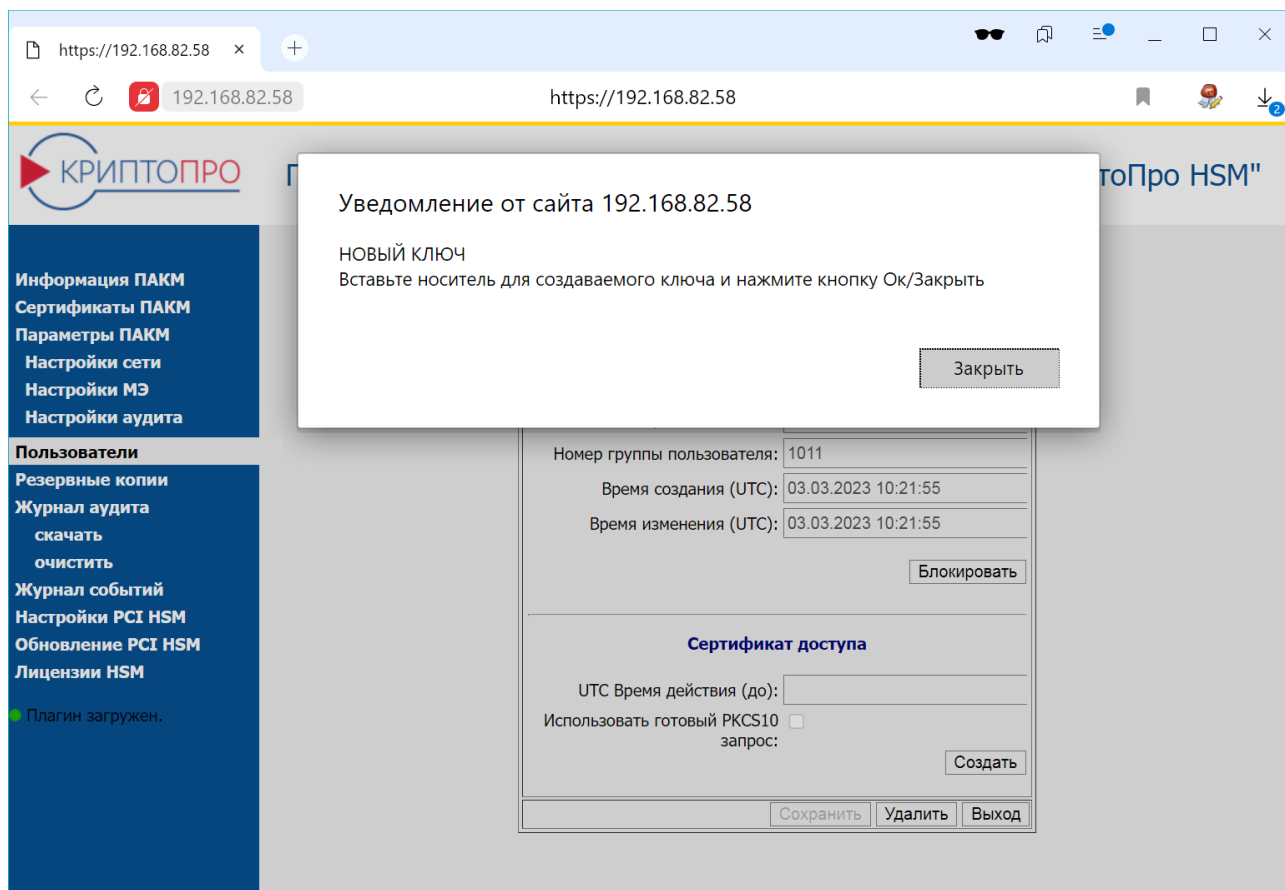
После создания нового пользователя откроем окно редактирования данных этого пользователя:

The screenshot shows a web browser window with the URL `https://192.168.82.58`. The page title is "Программно-аппаратный криптографический модуль "КриптоПро HSM"". The left sidebar contains a menu with the following items: "Информация ПАКМ", "Сертификаты ПАКМ", "Параметры ПАКМ", "Настройки сети", "Настройки МЭ", "Настройки аудита", "Пользователи", "Резервные копии", "Журнал аудита" (with sub-items "скачать" and "очистить"), "Журнал событий", "Настройки PCI HSM", "Обновление PCI HSM", "Лицензии HSM", and a status indicator "Плагин загружен.". The main content area is titled "Информация о пользователе ПАКМ" and displays the following user details:

Имя пользователя:	Администратор РК Крутов
Тип пользователя:	Архивариус
Идентификатор пользователя:	1011.1011@HSM44-test3i
Номер пользователя:	1011
Номер группы пользователя:	1011
Время создания (UTC):	03.03.2023 10:21:55
Время изменения (UTC):	03.03.2023 10:21:55

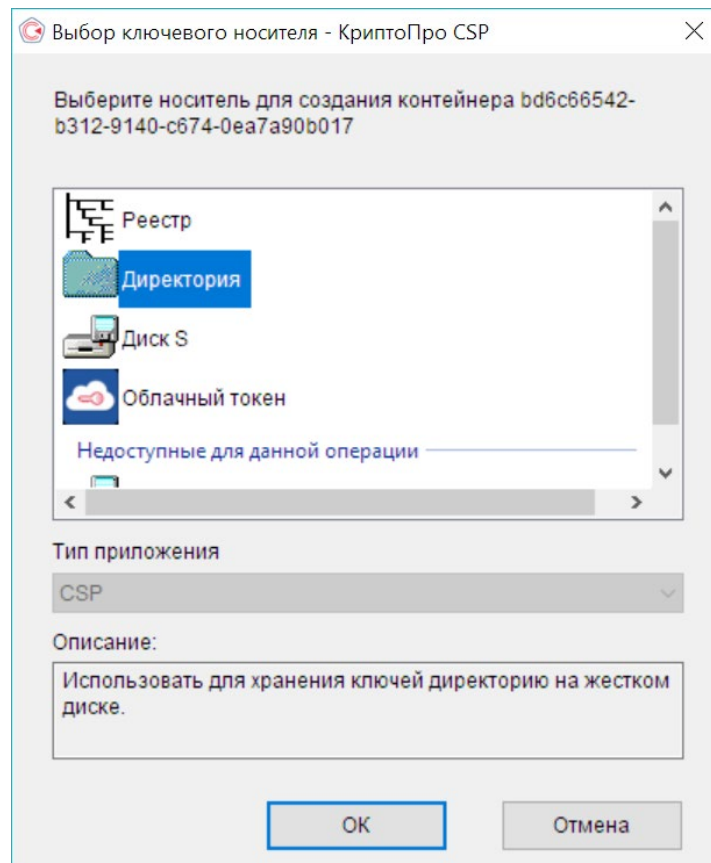
Below the details is a "Блокировать" button. The section "Сертификат доступа" includes a field for "UTC Время действия (до):", a checkbox for "Использовать готовый PKCS10 запрос:" (which is currently unchecked), and a "Создать" button. At the bottom of the form are buttons for "Сохранить", "Удалить", and "Выход".

У данного пользователя ещё нет ключа доступа. Кликаем на кнопке «Создать»:

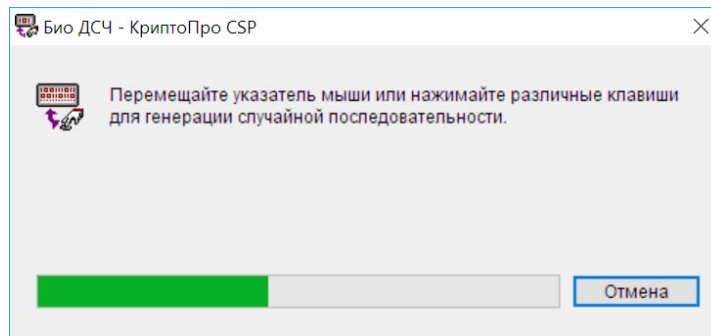


Необходимо вставить носитель для вновь создаваемого контейнера ключа нового пользователя.

После этого будет предложено выбрать считыватель в котором будет производиться генерация нового ключа доступа:



Начнется процедура генерации ключа:



Будет запрошен новый pin-код на созданный закрытый ключ:

Аутентификация - КриптоПро CSP

Crypto-Pro GOST R 34.10-2012 Cryptographic Service Provider запрашивает свойства аутентификации в контейнере

Считыватель:	REGISTRY
Носитель:	Уникальное имя отсутствует
Контейнер:	bd6c66542-b312-9140-c674-0ea7a90b017

Новый пароль:	
Повторите ввод:	

OK Отмена

Далее необходимо будет выбрать ключ/сертификат подтверждающего администратора на котором будет сформирована ЭП подтверждения:

https://192.168.82.58

192.168.82.58

https://192.168.82.58

КРИПТОПРО

Информация ПАКМ
Сертификаты ПАКМ
Параметры ПАКМ
Настройки сети
Настройки МЭ
Настройки аудита

Пользователи

Резервные копии
Журнал аудита
скачать
очистить
Журнал событий
Настройки PCI HSM
Обновление PCI HSM
Лицензии HSM

Плагин загружен.

Уведомление от сайта 192.168.82.58

КЛЮЧ ПОДТВЕРЖДЕНИЯ/ПОДПИСИ
Вставьте Контейнер с ключом подтверждающего администратора
и нажмите Ок/закрыть
В списке выберите требуемый сертификат (данного ключа)
И нажмите кнопку Подтвердить

Заккрыть

Время создания (UTC): 03.03.2023 10:21:55
Время изменения (UTC): 03.03.2023 10:21:55

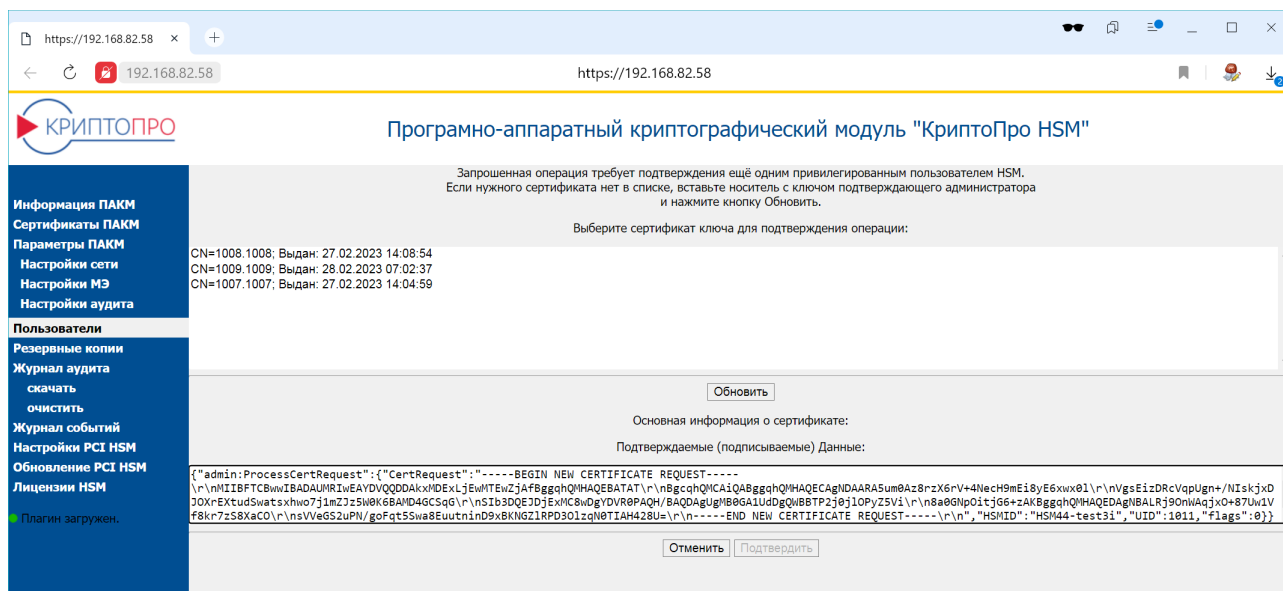
Блокировать

Сертификат доступа

UTC Время действия (до):
Использовать готовый PKCS10 ☐
запрос:

Создать

Сохранить Удалить Выход



В верхней части отобразится список сертификатов ключей из личного хранилища сертификатов APM Web администрирования (сертификаты предварительно должны быть установлены в Личное хранилище сертификатов ОС пользователя под которым запущен браузер с APM Web администрирования).

В нижней части окна отображаются подписываемые данные.

Выбрав из списка нужный сертификат, информация о нем отобразится в средней части окна:

https://192.168.82.58

192.168.82.58

КРИПТОПРО

Программно-аппаратный криптографический модуль "КриптоПро HSM"

Запрошенная операция требует подтверждения ещё одним привилегированным пользователем HSM.
Если нужного сертификата нет в списке, вставьте носитель с ключом подтверждающего администратора
и нажмите кнопку Обновить.

Выберите сертификат ключа для подтверждения операции:

- CN=1008.1008; Выдан: 27.02.2023 14:08:54
- CN=1009.1009; Выдан: 28.02.2023 07:02:37
- CN=1007.1007; Выдан: 27.02.2023 14:04:59

Обновить

Основная информация о сертификате:

Владелец: **CN=1008.1008**
Издатель: **CN=HSM44-test3i**
Выдан: **27.02.2023 14:08:54 UTC**
Действителен до: **27.05.2024 14:08:54 UTC**
Алгоритм ключа: **ГОСТ Р 34.10-2012 256 бит**

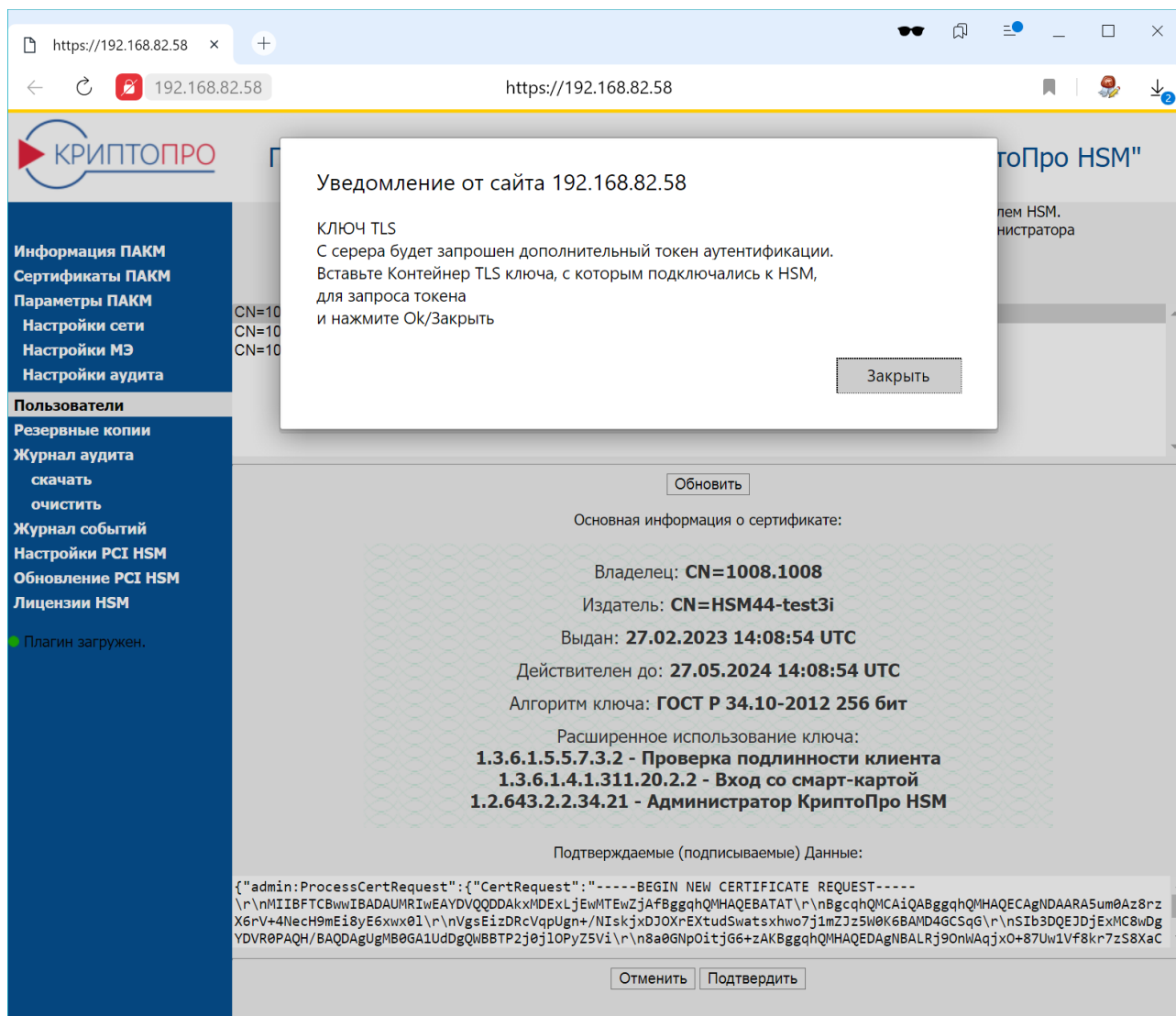
Расширенное использование ключа:
1.3.6.1.5.5.7.3.2 - Проверка подлинности клиента
1.3.6.1.4.1.311.20.2.2 - Вход со смарт-картой
1.2.643.2.2.34.21 - Администратор КриптоПро HSM

Подтверждаемые (подписываемые) Данные:

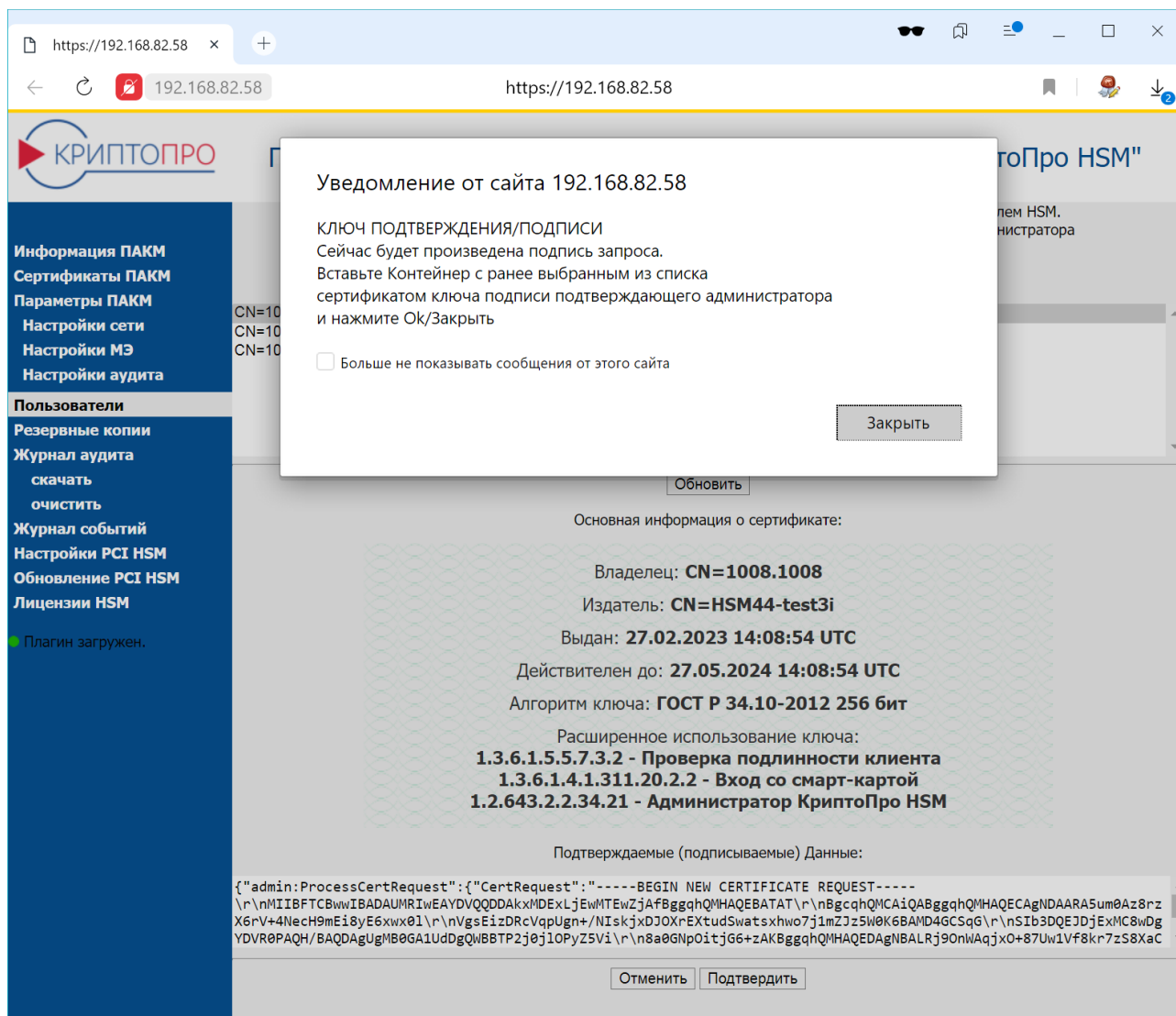
```
{
  "admin:ProcessCertRequest": {
    "CertRequest": "-----BEGIN NEW CERTIFICATE REQUEST-----
\r\nMIIBFTCBwwIBADAUMRIwEAYDVQQDDAkxMDEwLjEwMTUwZjA0BggqhQMHAQEBATAT\r\nBgcqhQMCAiQABggqhQMHAQECAGNDAARA5um0Az8rz
X6rV+4NecH9mEi8yE6xwx01\r\nVgsEizDRcVqpUgn+/NIskjxDJOXrEXtudSwatsxhwo7j1mZJz5W0K6BAMD4GCSqG\r\nnSiB3DQeJDDjExMC8wDg
YDVR0PAQH/BAQDAgUgMB0GA1UdDgQWBTP2j0j10PyZ5Vi\r\nn8a0GNP0itjG6+zAKBggqhQMHAQEDAgNBALRj90nWaqjxO+87Uw1Vf8kr7zS8XaC
-----END NEW CERTIFICATE REQUEST-----"
  }
}
```

Отменить Подтвердить

Если данный сертификат удовлетворяет условиям операции (в данном случае требуется ключ и сертификат другого Администратора ПАКМ) нажимаем кнопку «Подтвердить»:



В данный момент необходимо вставить в считыватель карту с ключом, на котором создавалась защищенная (HTTPS/Tls) Web сессия, если она была извлечена из считывателя. По нажатию кнопки «Заккрыть» в окошке сообщения, данные будут отправлены на сервер ПАКМ, который пришлет токен безопасности для подтверждения его и данных электронной подписью.



Проверьте, что карта с ключом подтверждения вставлена в считыватель и нажмите кнопку «Заккрыть» в окошке сообщения.

На ключ подтверждения будет запрошен pin-код. Подтверждающий администратор должен его ввести и нажать Ок.

Аутентификация - КриптоПро CSP

Crypto-Pro GOST R 34.10-2012 Cryptographic Service Provider запрашивает пароль для аутентификации в ключевом контейнере

Считыватель: REGISTRY

Носитель: Уникальное имя отсутствует

Контейнер: 174202ecd-a781-7c35-9376-a600008e84b

Введите пароль:

☐ Сохранить пароль в системе

☐ Требовать пароль при каждой операции

⚠ Выбран язык ввода, отличный от английского

ОК Отмена

https://192.168.82.58 x +

192.168.82.58 https://192.168.82.58

КРИПТОПРО

Информация ПАКМ
Сертификаты ПАКМ
Параметры ПАКМ
Настройки сети
Настройки МЭ
Настройки аудита

Пользователи
Резервные копии
Журнал аудита
скачать
очистить
Журнал событий
Настройки PCI HSM
Обновление PCI HSM
Лицензии HSM

Плагин загружен.

Уведомление от сайта 192.168.82.58

КЛЮЧ TLS
Запрос подписан. Чтобы отправить его,
Вставьте Контейнер TLS ключа, с которым подключались к HSM
и нажмите Ок/Закрыть

Закрыть

номер группы пользователя: 1011

Время создания (UTC): 03.03.2023 10:21:55

Время изменения (UTC): 03.03.2023 10:21:55

Блокировать

Сертификат доступа

UTC Время действия (до):

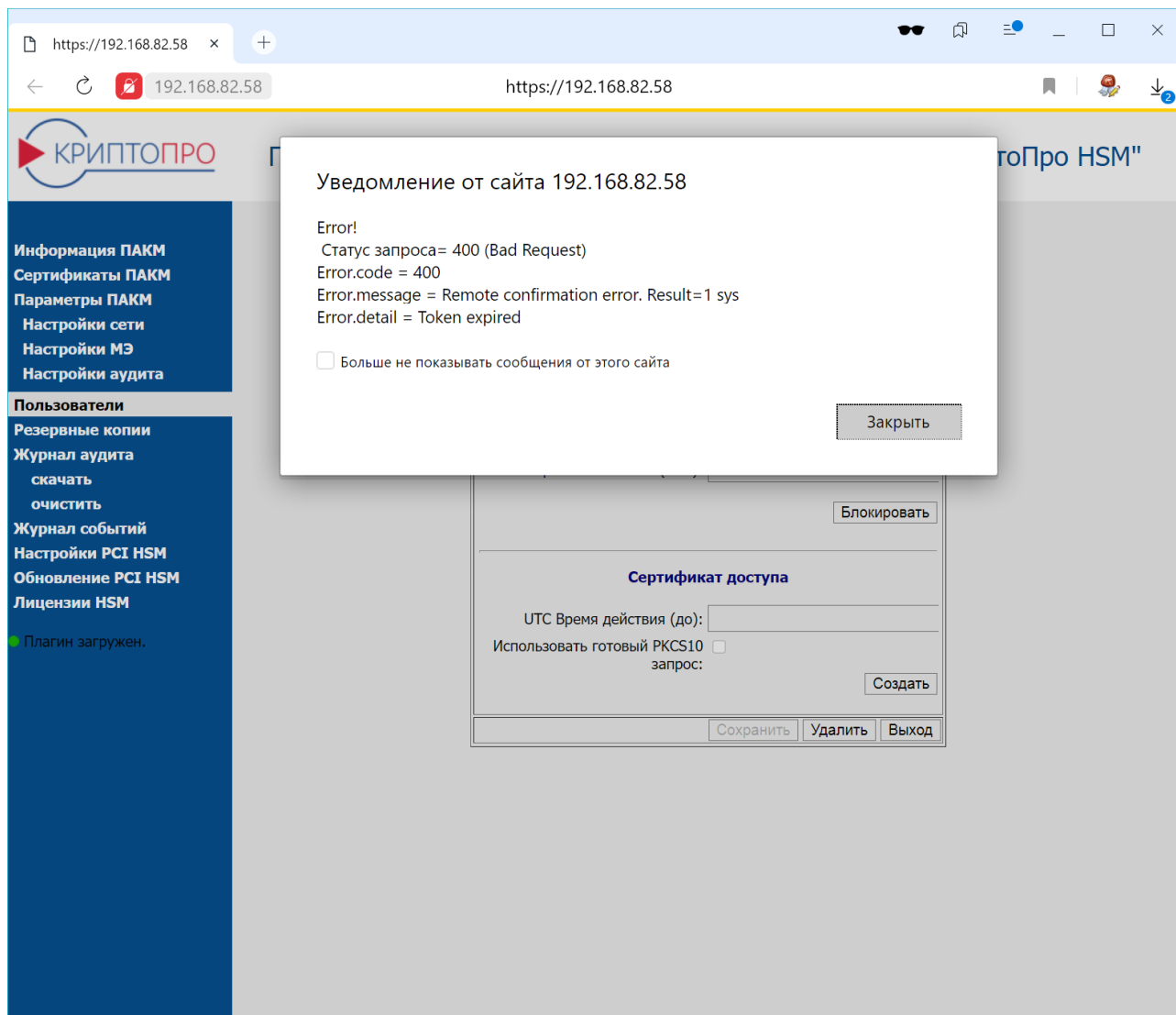
Использовать готовый PKCS10 ☐
запрос:

Создать

Сохранить Удалить Выход

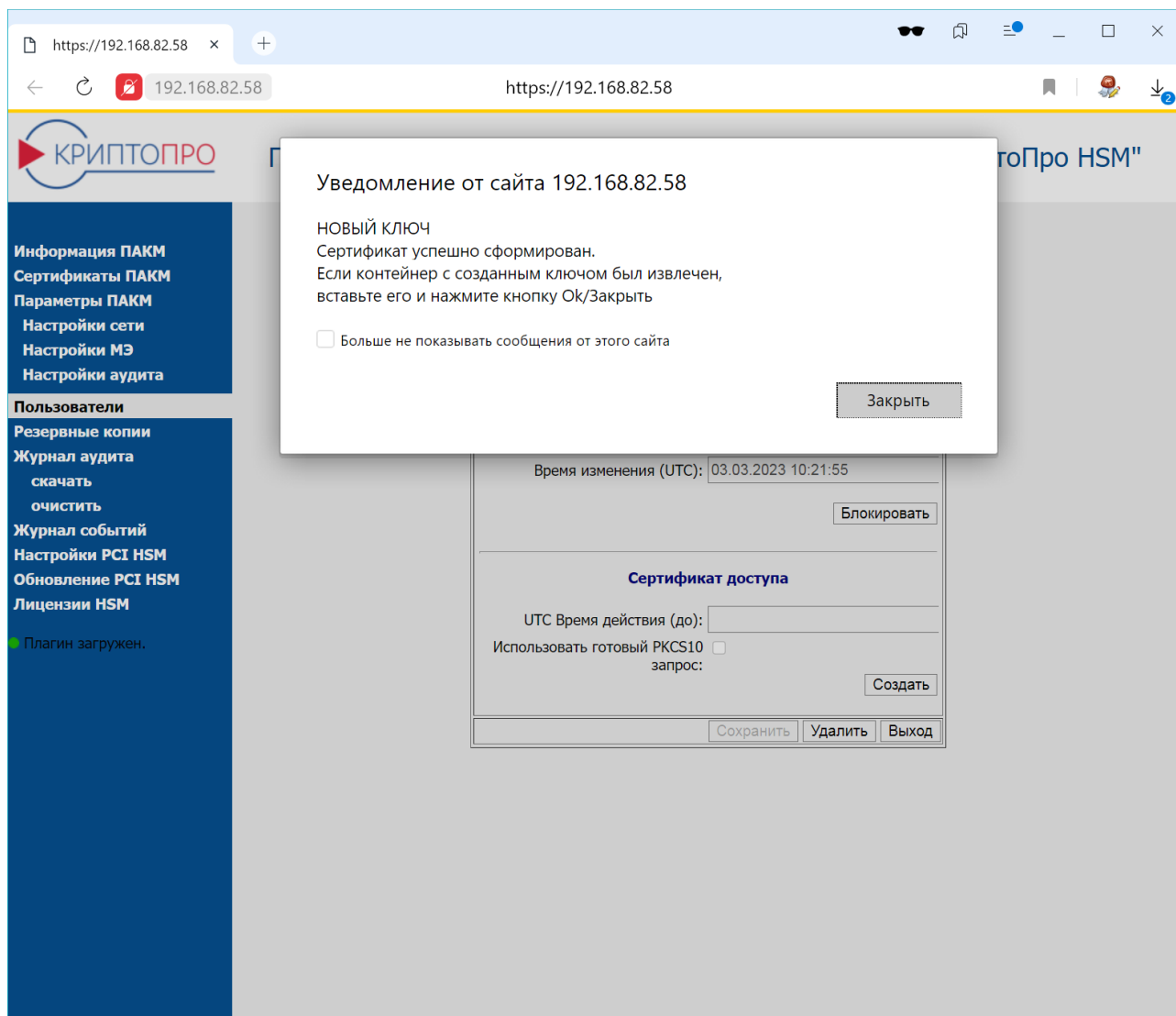
Проверьте, что ключ администратора, который инициировал операцию (Tls сессию) вставлен в считыватель и нажмите кнопку «Заккрыть».

Если вы очень долго выполняли все предыдущие шаги, то токен безопасности выданный сервером на операцию может стать просроченным и будет выдано сообщение об ошибке.

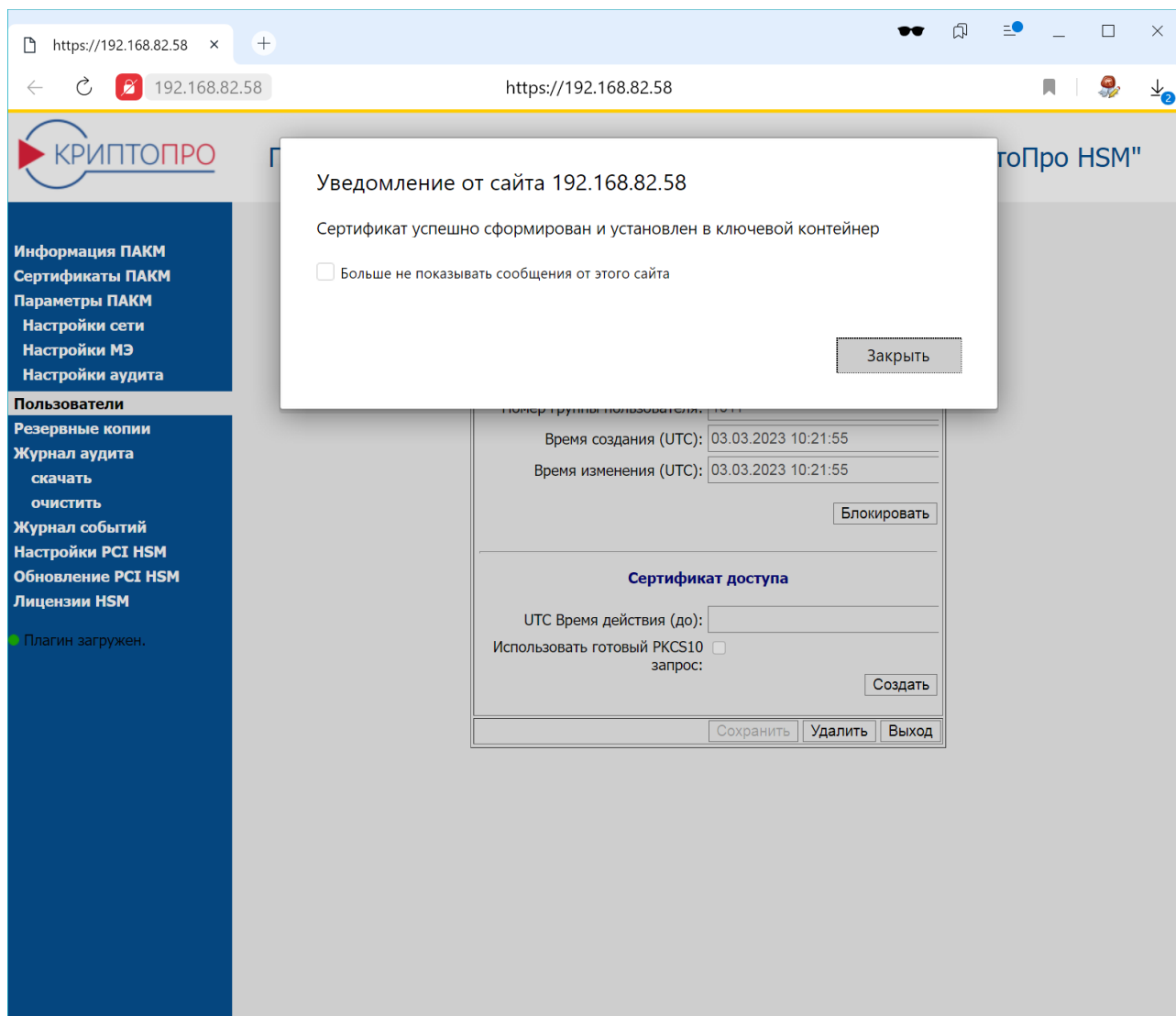


Срок действия токена – 5 минут! Если такая ошибка возникла, то следует повторить всю операцию, при этом зачистив карту, на которой создавался новый ключ пользователя.

Если же вы нормально успели обработать запрос, то далее продолжится установка изданного сертификата нового ключа в контейнер этого ключа:



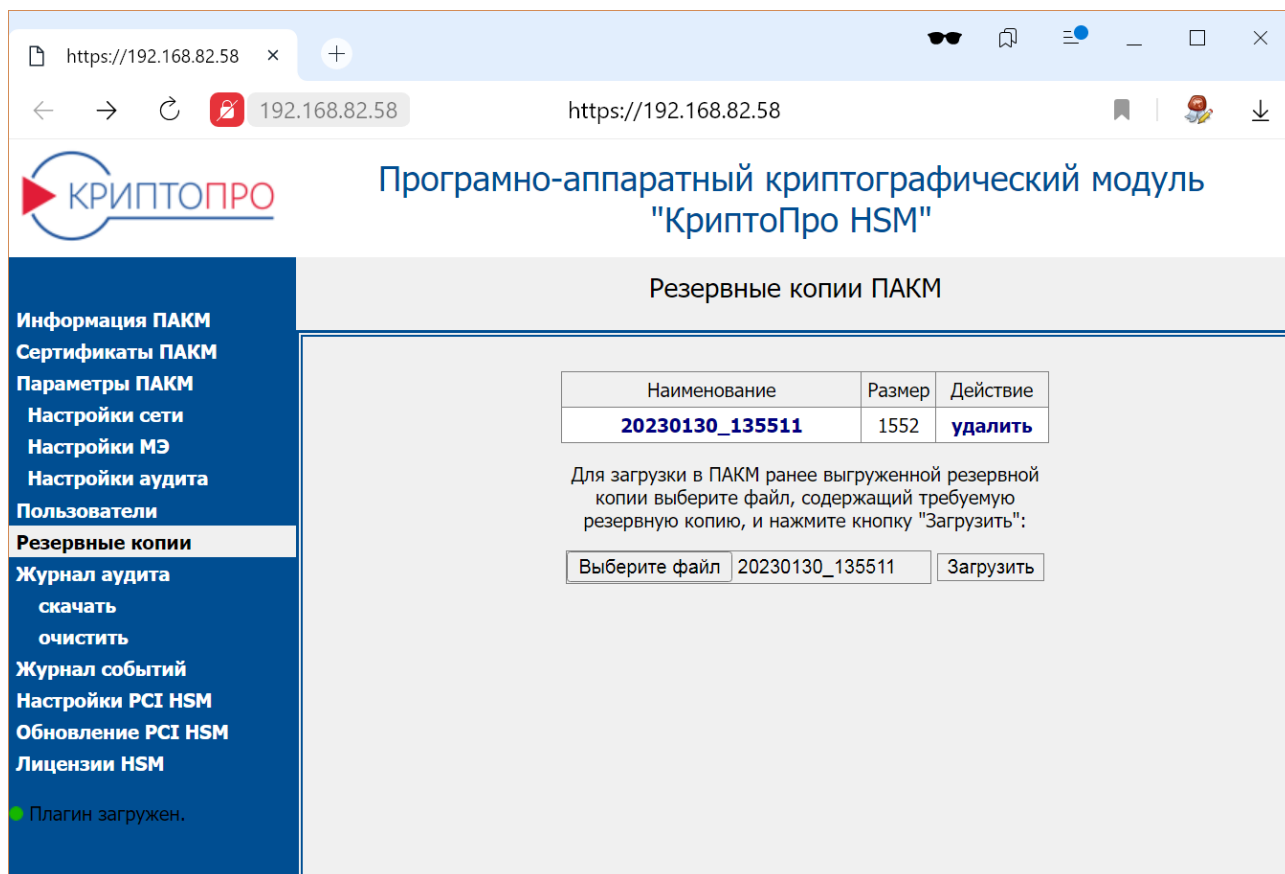
Проверьте, что носитель с вновь созданным ключом пользователя вставлен в считыватель и нажмите кнопку «Заккрыть».



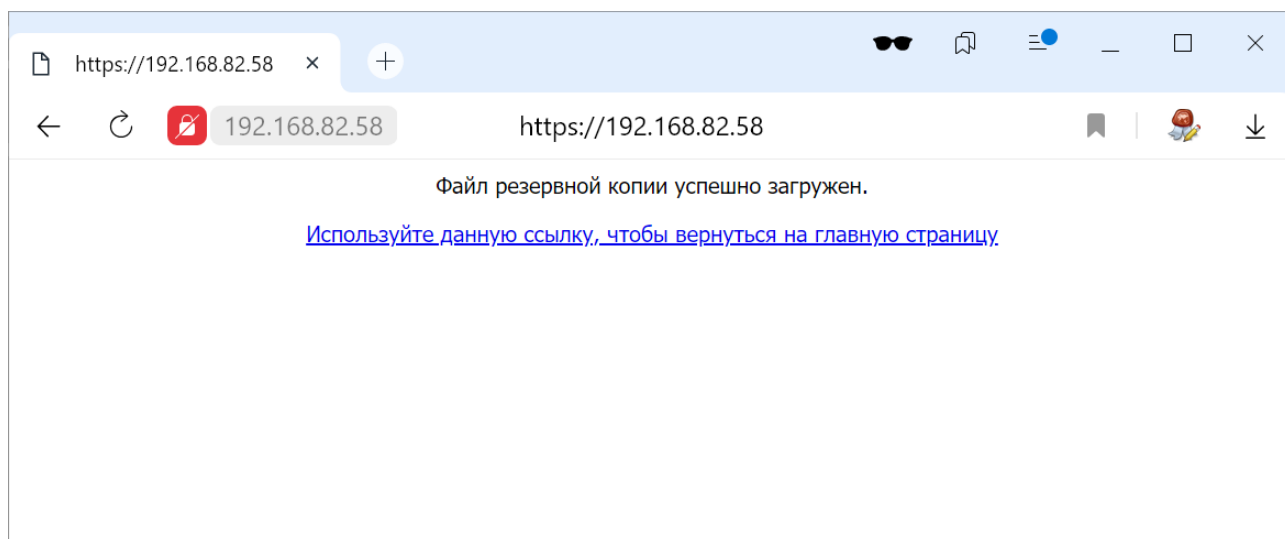
Операция завершена успешно!

6.3.9.Резервные копии

Если выбрать в меню слева пункт «Резервные копии», справа появится форма для работы с резервными копиями ПАКМ. Выгрузка резервных копий ПАКМ возможна при использовании карточки Администратора ПАКМ. Удаление и загрузка в ПАКМ резервных копий ПАКМ возможны только при использовании карточки Администратора резервного копирования ПАКМ.

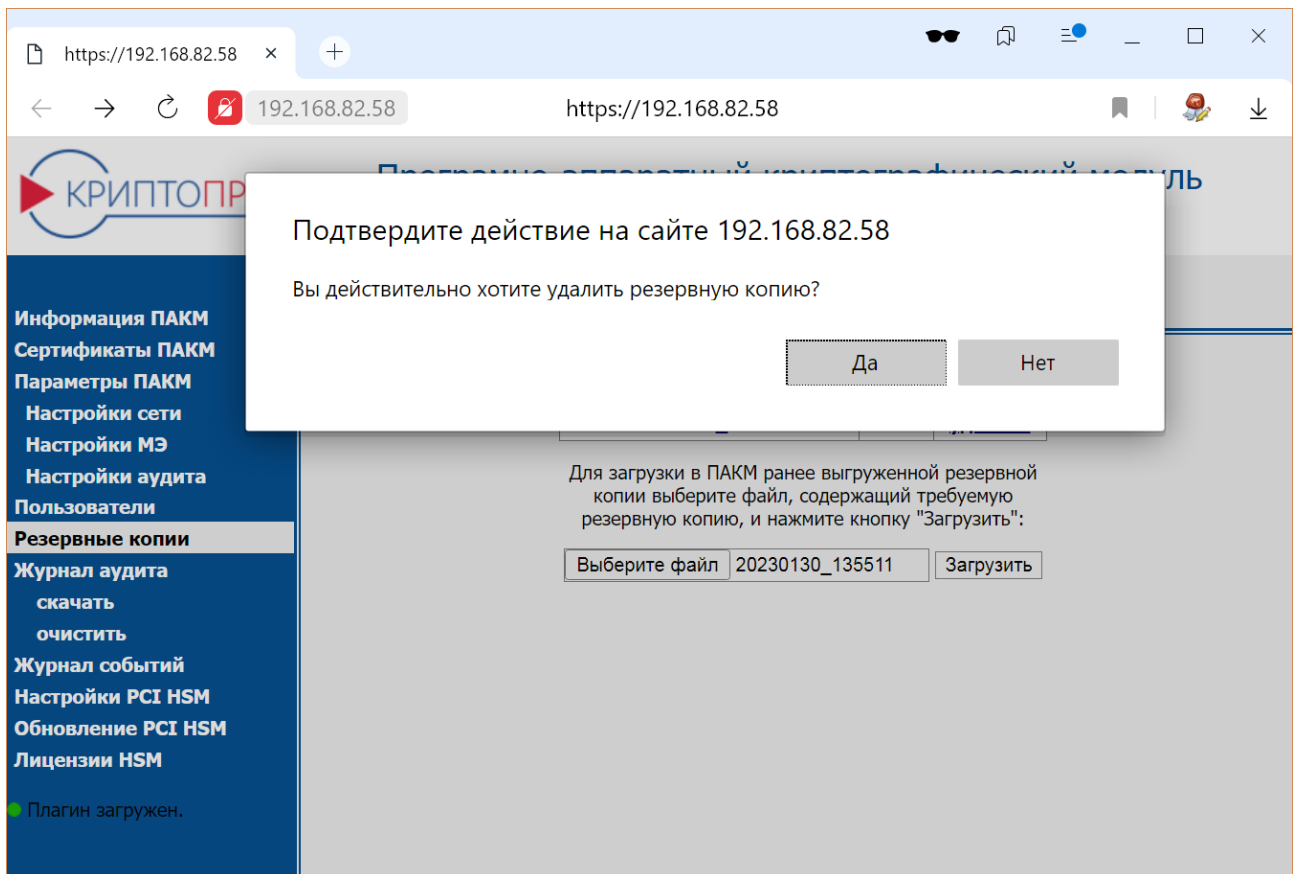


Если у привилегированного пользователя нет прав для операций с резервными копиями, то при попытке осуществить таковую будет выдано сообщение

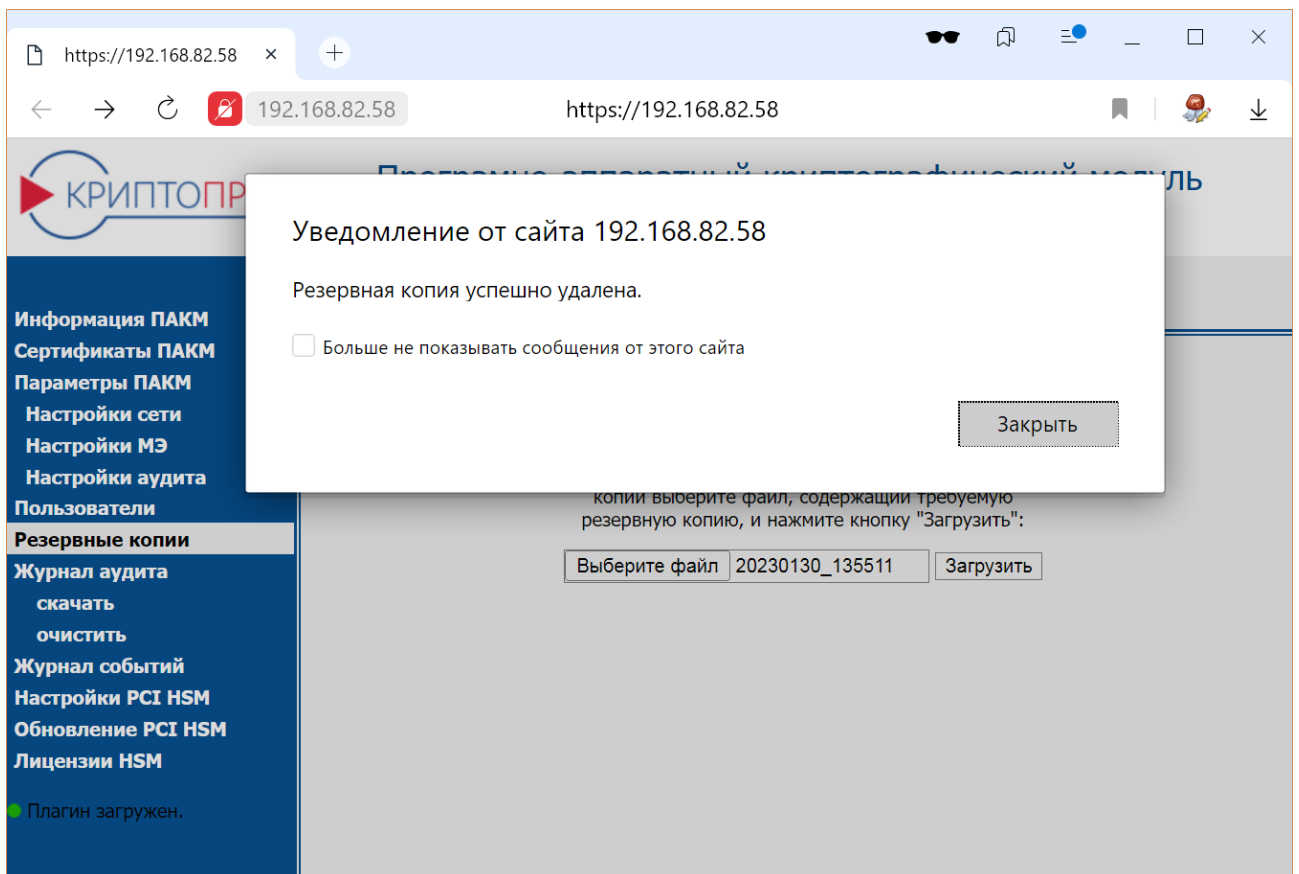


Если требуется выгрузить резервную копию, надо щелкнуть мышью на наименовании копии. После этого появится стандартное окно Windows для скачивания файлов.

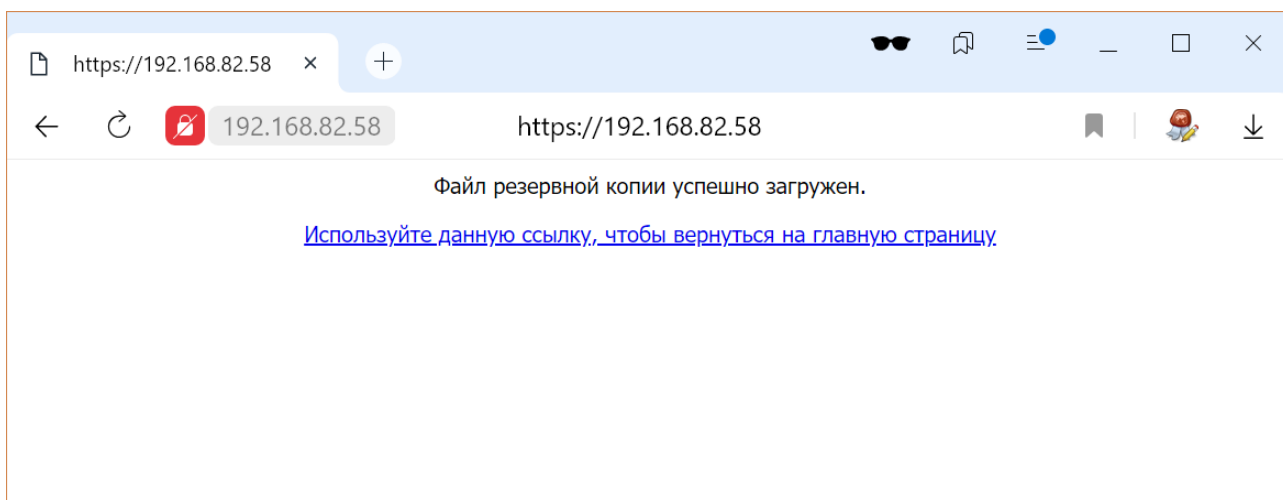
Если требуется удалить резервную копию, надо щелкнуть мышью на ссылке «удалить» в соответствующей строке таблицы. После этого появится окно:



Если нажать «ОК», резервная копия будет удалена, о чем появится сообщение:



Для загрузки ранее выгруженной из ПАКМ резервной копии необходимо выбрать файл, содержащий данную копию (используйте для этого кнопку «Обзор...»), после чего нажать кнопку «Загрузить». При успешном завершении операции, либо при ошибке выполнения будет выдано соответствующее сообщение.



Операция загрузки в ПАКМ файлов резервных копий допустима только при установленном Администратором ПАКМ параметре «Enable Upload» в значение «True».

6.3.10. Журнал аудита

Если выбрать в меню слева пункт «Журнал аудита», справа появится форма для работы с журналом аудита ПАКМ. Скачивание и очистка журнала аудита ПАКМ возможны при использовании карточки Аудитора ПАКМ. Операция очистки журнала аудита требует подтверждения/подписи ключом Администратора ПАКМ!

https://192.168.82.58 x +

192.168.82.58 https://192.168.82.58

КРИПТОПРО Программно-аппаратный криптографический модуль "КриптоПро HSM"

Журнал аудита ПАКМ

Автор (Номер пользователя): Тип события:

Дата события ("YYYYMMDD[hhnnss]Z"): Статус завершения:

Сортировать по возрастанию: ☐

[Применить фильтр](#)

[Скачать](#)

Информация ПАКМ
Сертификаты ПАКМ
Параметры ПАКМ
Настройки сети
Настройки МЭ
Настройки аудита
Пользователи
Резервные копии
Журнал аудита
скачать
очистить
Журнал событий
Настройки PCI HSM
Обновление PCI HSM
Лицензии HSM
Плагин загружен.

Найдено 10 записей. Страница № 1 из 1.

Время события(UTC)	Тип события	Автор	Строковые данные	Двоичные данные
03.03.2023 11:08:01.8544	MODIFY_USER	1007	1011.1011@HSM44-test...	
03.03.2023 10:21:55.2358	ADD_USER	1007	1011.1011@HSM44-test...	
03.03.2023 09:04:55.6274	ADD_USER	1007	1010.1010@HSM44-test...	
03.03.2023 08:54:31.4877	MODIFY_USER	1007	1005.1005@HSM44-test...	
03.03.2023 08:43:40.2958	CHANGE_USER_STATE	1007	1009.1009@HSM44-test...	
03.03.2023 08:28:05.1873	DELETE_USER	1007	1006.1006@HSM44-test...	
03.03.2023 08:25:24.5352	CHANGE_USER_STATE	1007	1009.1009@HSM44-test...	
02.03.2023 16:04:17.3695	FW_DELETE_SUBNET	1007	192.168.82.59; 255.2...	
02.03.2023 16:02:41.8526	FW_ADD_SUBNET	1007	192.168.82.59; 255.2...	
28.02.2023 07:14:40.0097	CLEAR_AUDIT_LOG	1009	8; confirmed by 1008...	

В форме имеется таблица со списком событий. В таблице указаны время события (по UTC), тип события, UID пользователя, производившего действие, и дополнительные данные. Выделение розовым цветом означает, что действие завершилось неуспешно. Для просмотра других страниц списка в заголовке списка имеются ссылки «>>>» / «<<<» (следующая/предыдущая страница) и «<->|» / «|<-» (последняя/первая страница).

Если требуется отсортировать записи по возрастанию времени события или просмотреть часть списка выборочно, надо ввести условия запроса в верхней части таблицы и щелкнуть мышью на строке «**Применить фильтр**». Если требуется просмотреть весь список, надо очистить условия запроса и применить фильтр снова.

Если требуется скачать часть журнала аудита и сохранить ее в виде файла, надо щелкнуть мышью на строке «**Скачать**». В появившейся форме надо ввести дату и время, начиная с которого (и до текущего времени) надо получить список событий. Если поле оставить пустым, журнал будет скачан целиком.

Формат задаваемой строки времени:

YYYYMMDD[HH[NN[SS[Z]]]]

где:

YYYY – год события;

MM – месяц события (1-12);

DD – день события (1-31);

HH – часы события (0-23) – указывается опционально;

NN – минуты события (0-59) – указывается опционально;

SS – секунды события (0-59) – указывается опционально;

Z – завершающий символ в обозначении generalizedTime, указывается опционально.

Для того, чтобы журнал был подписан ключом подписи журнала аудита ПАКМ можно указать опцию «**Подписать журнал**». В этом случае скачанный файл будет представлять собой CMS (#pkcs7) сообщение SIGNED_DATA с присоединенной электронной подписью. Впоследствии для проверки ЭП журнала можно воспользоваться утилитами КриптоПро. Для этого может понадобиться установить сертификат ключа проверки ЭП журнала аудита в хранилище сертификатов, например, в хранилище «Другие пользователи». При этом, при проверке подписи необходимо помнить, что ПАКМ не ведет списков отзыва (CRL) на издаваемые им служебные сертификаты, как и любую другую информацию об отзыве. Некоторым утилитам необходимо явно указывать на это.

Пример использования утилиты **cryptcp** для проверки выгруженного файла журнала с присоединенной подписью:

```
C:\Program Files\Crypto Pro\CSP>cryptcp.exe -verify -attached -dn "CN=HSM AUDIT Signer" e:\hsm_audit_log_.sig  
e:\hsm_audit_log_out.txt  
CryptCP 5.0 (с) "КРИПТО-ПРО", 2002-2021.  
Утилита командной строки для подписи и шифрования файлов.
```

Будет использован следующий сертификат:
Субъект:HSM AUDIT Signer
Действителен с 11.02.2023 07:54:40 по 11.02.2033 07:54:40

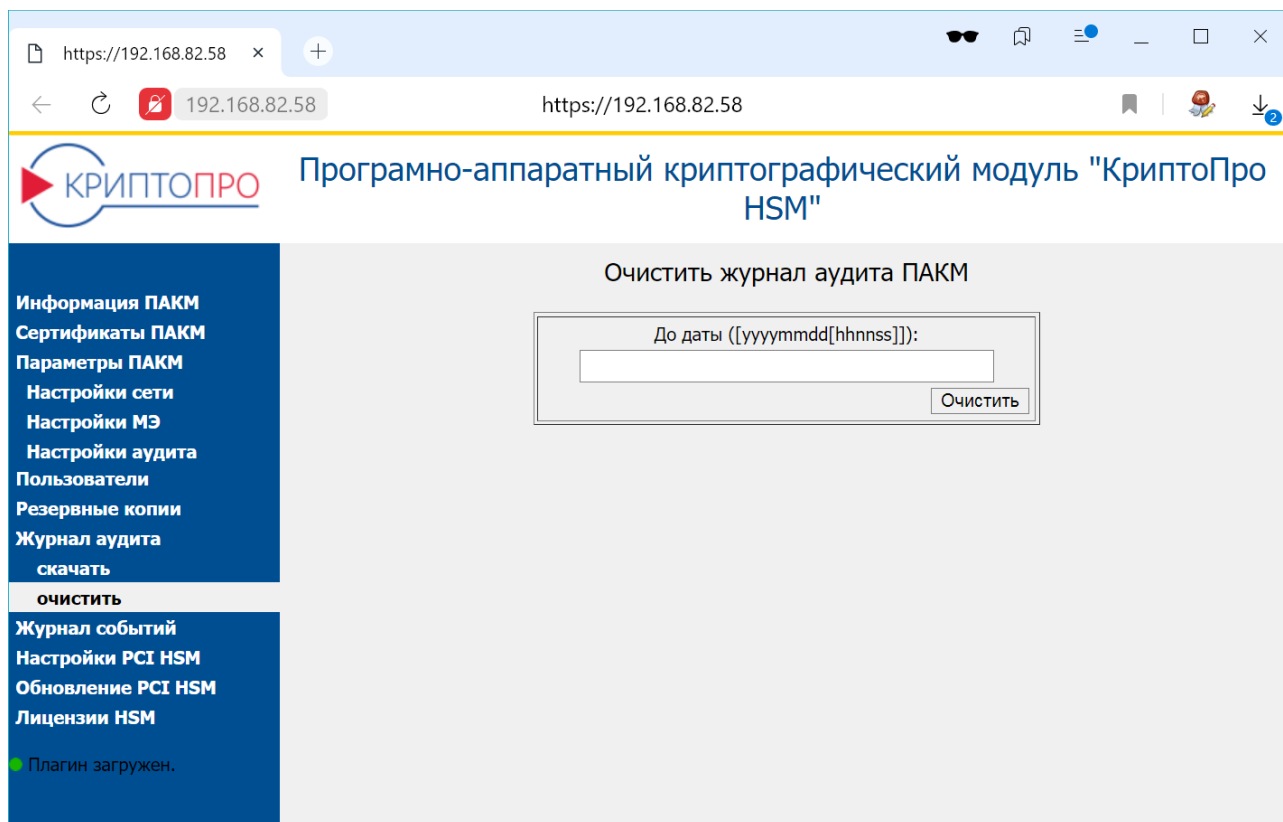
Цепочка сертификатов не проверена для следующего сертификата:
Субъект:HSM AUDIT Signer
Действителен с 11.02.2023 07:54:40 по 11.02.2033 07:54:40

Один из сертификатов в цепочке возможно отозван.
Вы хотите использовать этот сертификат (Да[Y], Нет[N], Отмена[C])? Y
Цепочки сертификатов проверены.
Папка 'e:\':
e:\hsm_audit_log_.sig... Проверка подписи...
Автор подписи: HSM AUDIT Signer
Один из сертификатов в цепочке возможно отозван.
Вы хотите использовать этот сертификат (Да[Y], Нет[N], Отмена[C])? Y
Подпись проверена.
[ErrorCode: 0x00000000]

После ввода параметров скачивания надо нажать кнопку **«Скачать»**. Если объем журнала большой, то потребуется некоторое время на скачивание. Скачанный файл журнала будет помещен в папку «Загрузки» браузера.

Если в форме для ввода даты не ввести ничего, журнал аудита будет скачан целиком.

Если требуется очистить журнала аудита, надо щелкнуть мышью на строке **«Очистить»**, или выбрать пункт «очистить» в меню слева. В появившейся форме надо ввести дату и время, до которого список событий будет очищен. Если поле оставить пустым, журнал будет очищен целиком, после чего в него будет добавлена одна запись о выполненной процедуре очистки.



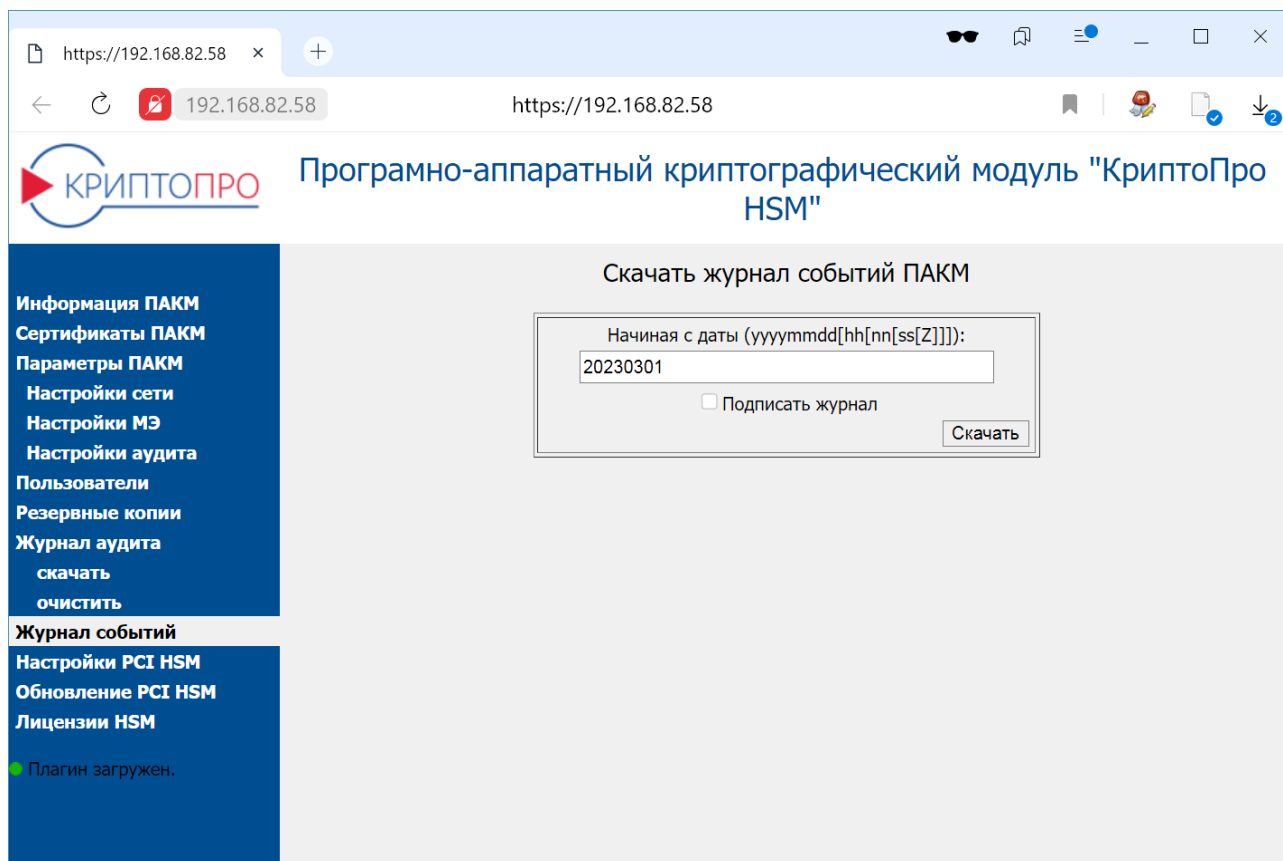
Операция очистки инициируется Аудитором ПАКМ и должна быть подтверждена электронной подписью на ключе Администратора ПАКМ. Действия производимые в процессе подтверждения операции описаны в разделе "Особенности выполнения операций, требующих подтверждения вторым привилегированным пользователем".

После выполнения операции очистки и обновления списка записей журнала (для этого надо использовать «Применить фильтр») в списке будет присутствовать запись об очистке журнала (тип события EVENT-TYPE-CLEAR-AUDIT-LOG).

6.3.11. Журнал событий

Если выбрать в меню слева пункт «Журнал событий» (журнал СКЗИ), справа появится форма для получения журнала событий ПАКМ. В ней надо ввести дату и время, начиная с которого надо получить список событий (буква «Z» в конце даты означает время по UTC). Если поле оставить пустым, журнал будет скачан целиком.

При необходимости, также, как и в случае выгрузки журнала аудита, можно указать, чтобы журнал был подписан ключом подписи журнала аудита ПАКМ. В этом случае скачанный файл будет представлять собой CMS (#pkcs7) сообщение SIGNED_DATA с присоединенной электронной подписью.



После ввода даты надо нажать кнопку **«Скачать»**. Если объем журнала большой, то потребуются некоторое время на скачивание. Скачанный файл журнала будет помещен в папку «Загрузки» браузера.

Для более быстрого скачивания полного файла журнала событий можно после взаимной TLS аутентификации браузера и ПАКМ набрать в строке ввода адреса ПАКМ URL:

`https://<ip-адрес ПАКМ>/var/log/messages`

а также

`https://<ip-адрес ПАКМ>/var/log/messages.N`

где N – номер (от 1 до 5) более строго отротированного файла журнала событий.

Эти файлы ОС ПАКМ могут быть на короткие промежутки времени блокированы, поэтому иногда следует несколько раз нажать кнопку F5 («Обновить страницу» в браузере).

6.3.12. Настройки PCI HSM

Данный режим позволяет просмотреть содержимое конфигурационного файла платежного модуля. Подробнее о том, что означают данные настройки смотрите в документации на Платежный модуль ПАКМ. Правом на просмотр конфигурации платежной системы обладает пользователь с ролью «Администратор платежной системы».

192.168.82.75

КРИПТОПРО

Программно-аппаратный криптографический модуль "КриптоПро HSM"

Параметры PCI HSM

Настройки безопасности

Настройка	Значение
PIN length	4
Atalla ZMK variant support	F
Default LMK identifier	0
Enforce Atalla variant match to variant key type	NO
Select clear PINs	NO
Encrypt clear PINs	NO
Enable ZMK translate command	NO
Enable X9.17 for import	NO
Enable X9.17 for export	NO
Solicitation batch size	1024
Decimalization tables: Encrypted/Plaintext	E
Enable decimalization table checks	YES
PIN encryption algorithm	A
Minimum HMAC length in bytes	10
Enable PKCS#11 import and export for HMAC keys	NO
Enable ANSI X9.17 import and export for HMAC keys	NO
Enable ZEK/TEK encryption of ASCII data or Binary data or None	N
Restrict Key Check Values to 6 hex chars	YES
Enable variable length PIN offset	NO
Enable weak PIN checking	NO
Check new PINs using global list of weak PINs	NO
Check new PINs using local list of weak PINs	NO
Check new PINs using rules	NO

Информация ПАКМ
Сертификаты ПАКМ
Параметры ПАКМ
Настройки сети
Настройки МЭ
Настройки аудита
Пользователи
Резервные копии
Журнал аудита
скачать
очистить
Журнал событий

Настройки PCI HSM

Обновление PCI HSM

Лицензии HSM

Плагин загружен.
Версия плагина: 2.0.14337
Версия криптопровайдера: 5.0.12510
Криптопровайдер: Crypto-Pro
GOST R 34.10-2012
Cryptographic Service Provider
1005.1005@HSM24-08275c
(Администратор ПК)

6.3.13. Обновление PCI HSM

Данный режим позволяет произвести обновление ПО платежного модуля ПАКМ. Правом на загрузку обновлений платежного модуля обладает пользователь с ролью «Администратор платежной системы». Обычный Администратор ПАКМ может разрешить или запретить загрузку файлов в ПАКМ путем настройки опции «Enable upload» в настройках Параметров ПАКМ. Таким образом, разрешение на выполнение данной операции может быть разделено между привилегированными пользователями с указанными ролями.

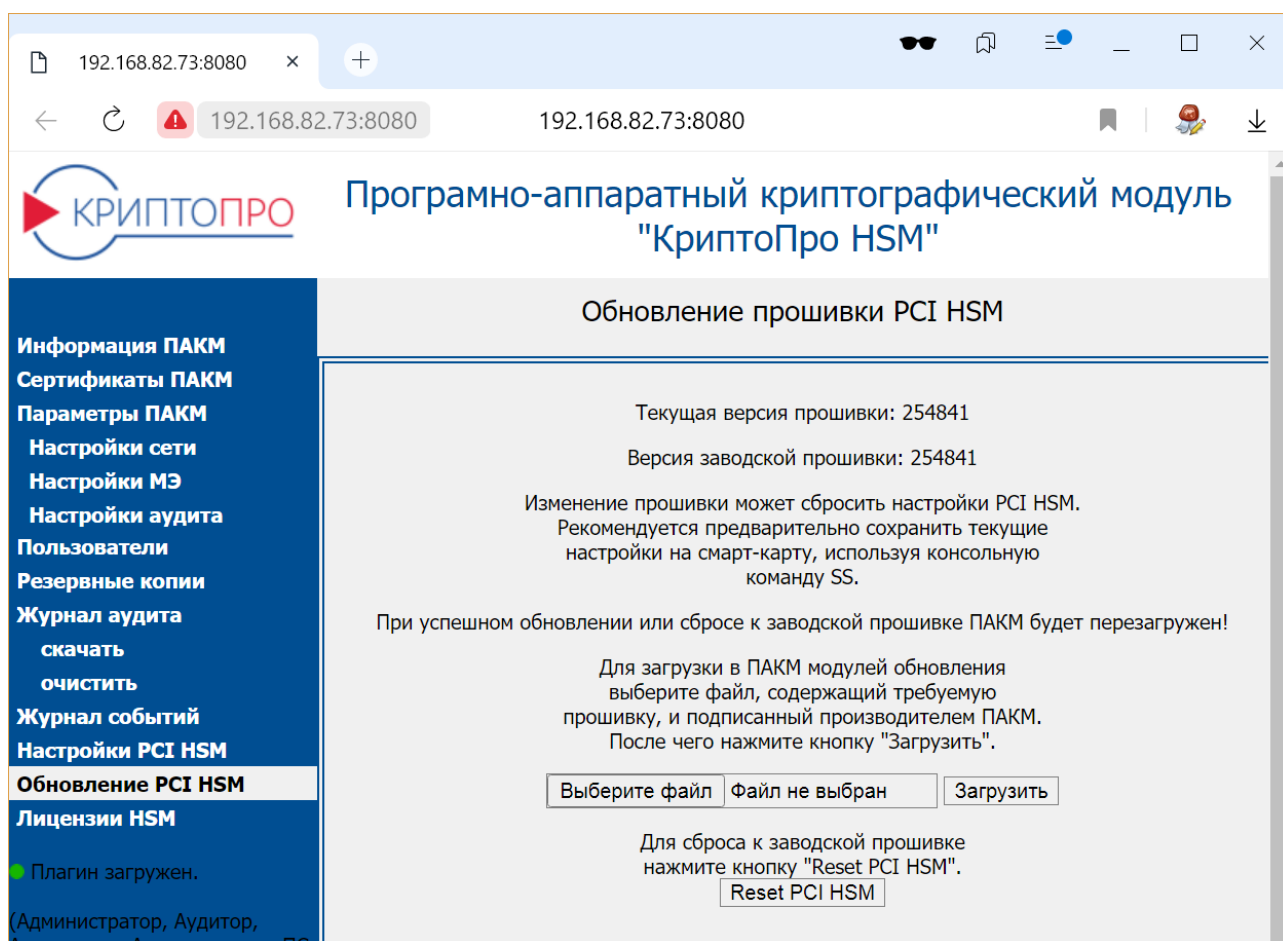
Файл, содержащий прошивку, представляет собой подписанное электронной подписью производителя CMS (#pkcs7) сообщение SIGNED_DATA, включающее архив программных модулей и сопровождающей информации. При загрузке файла обновления будет производиться проверка ЭП данного CMS сообщения на открытом ключе производителя, записанном в ПАКМ при изготовлении. Если проверка ЭП выполнена без ошибок, файл распаковывается и ожидает перезагрузки ПАКМ для дальнейшего внутреннего обновления прошивки. Каждая прошивка содержит номер версии, который отображается в окне «Обновлений PCI HSM». Кроме установленной таким образом прошивки всегда сохраняется базовая прошивка, установленная в ПАКМ при

изготовлении. В случае ошибки обновления, может производиться автоматический сброс к заводским настройкам.

Сброс к заводским настройкам может производиться также Администратором Платежной системы либо в меню Платежной системы LCD панели, либо в данном окне Web интерфейса.

Подробнее о работе платежного модуля смотрите в документации на Платежный модуль ПАКМ.

При выборе данного режима работы откроется окно:



В верхней части отображаются номера текущей и базовой версии прошивки. В случае, если обновлений не производилось, или был произведен сброс к заводским настройкам, то номера базовой и текущей версий совпадают.

Порядок установки обновлений не зависит от номеров их версий. Т.е. всегда модно установить прошивку версии более ранней, чем текущая.

Для загрузки обновления необходимо нажать на кнопку «Выберите файл» и в стандартном окне диалога выбора файла указать на файл прошивки.

После этого следует нажать кнопку «Загрузить».

Для сброса ПО Платежного модуля к заводской версии следует нажать на кнопку «Reset PCI HSM».

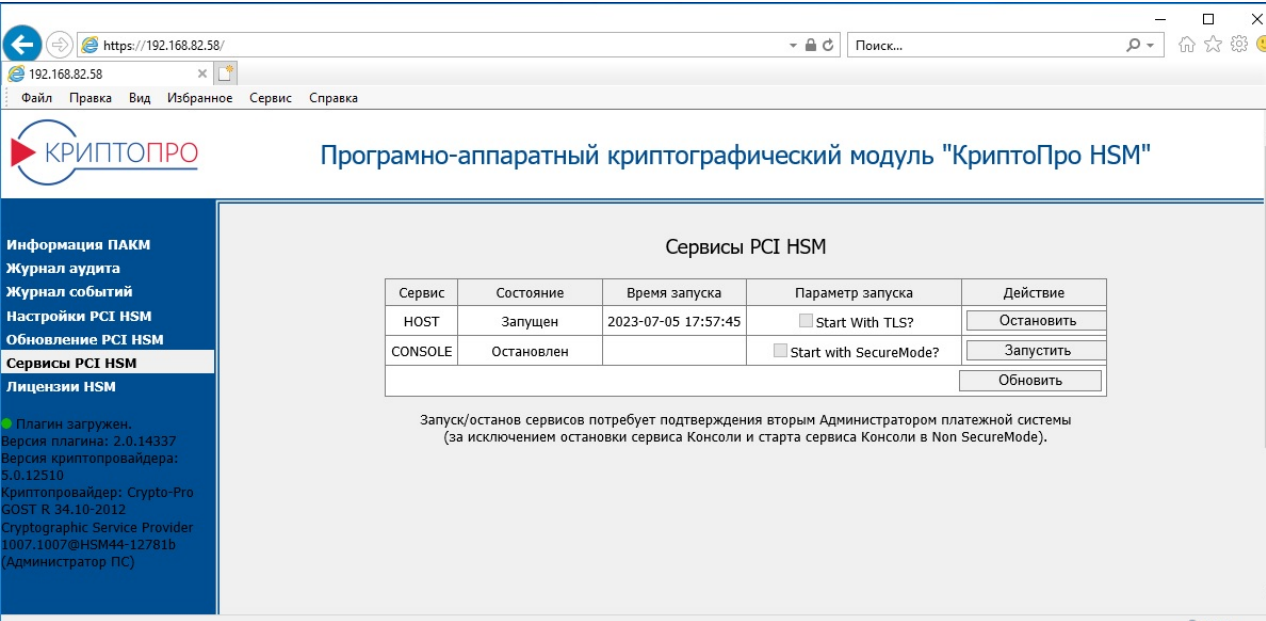
Выполнение операции обновления или сброса будет заблокировано, если запущен какой-либо из pci сервисов (Хост и/или Консоль) с выдачей соответствующего сообщения об ошибке. Необходимо предварительно остановить PCI сервисы, после чего повторить операцию обновления или сброса.

Обращаем внимание, что после успешной операции обновления или сброса к заводским настройкам ПАКМ должен быть перезагружен, поэтому он выключится (перейдет в состояние HALT).

6.3.14. Сервисы PCI HSM

Данный режим позволяет удаленно запускать и останавливать сервисы PCI HSM - Host и Console. Он доступен только привилегированному пользователю с ролью "Администратор платежной системы"

Запуск и останов сервиса HOST, а также запуск сервиса CONSOLE в безопасном режиме (SecureMode) потребует подтверждения вторым привилегированным пользователем с ролью "Администратор платежной системы".



Скриншот веб-интерфейса "КриптоПро". В центре экрана отображается таблица "Сервисы PCI HSM".

Сервис	Состояние	Время запуска	Параметр запуска	Действие
HOST	Запущен	2023-07-05 17:57:45	☐ Start With TLS?	Остановить
CONSOLE	Остановлен		☐ Start with SecureMode?	Запустить
				Обновить

Под таблицей находится предупреждение: "Запуск/останов сервисов потребует подтверждения вторым Администратором платежной системы (за исключением остановки сервиса Консоли и старта сервиса Консоли в Non SecureMode)".

В левом меню видны ссылки: "Информация ПАКМ", "Журнал аудита", "Журнал событий", "Настройки PCI HSM", "Обновление PCI HSM", "Сервисы PCI HSM" (выделено), "Лицензии HSM".

В зависимости от состояния платежных сервисов (какие из них запущены и в каком режиме, а какие остановлены) названия кнопок в правой колонке таблицы могут меняться на значения "Остановить", "Запустить", "Недоступно".

Параметр запуска (режим) также зависит от состояния сервисов и может быть недоступен для изменения.

Можно выделить следующие правила:

- Сервис Консоли не может быть запущен в SecureMode, если запущен Host. Но может быть запущен в Online mode (без указания опции "Start with SecureMode");
- Сервис Хоста может быть запущен только тогда, когда все pci сервисы остановлены;
- Сервис Хоста может быть остановлен только тогда, когда он стартован и сервис консоли остановлен;
- При запуске сервиса консоли без указания опции "Start with SecureMode" при остановленном сервисе Хоста, она будет стартована в offline mode.

Для запуска требуемого сервиса отметьте режим его запуска (если соответствующая опция доступна) и нажмите кнопку "Запустить" в соответствующей строке (если доступно).

Для останова сервиса следует нажать кнопку "Остановить" в соответствующей строке (если доступно).

После успешного запуска сервиса в колонке "Время запуска" будет отражено время (локальное в соответствии с Timezone).

Опции в колонке "Параметр запуска" служат в основном для указания режима запуска соответствующего сервиса. Для уже запущенного сервиса Консоли не следует его учитывать при просмотре состояния. Он не отражает реальный параметр, который был задан при старте.

Для просмотра текущего (в конкретный момент времени) состояния сервисов служит кнопка "Обновить" внизу таблицы.

События запуска и останова сервисов отображаются в журнале аудита ПАКМ.

6.3.15. Лицензии HSM

Данный режим позволяет ввести лицензии на использование ПАКМ КриптоПро HSM в качестве разделяемого СКЗИ и на использование модуля платежной системы.

Правом на установку лицензий обладает пользователь с ролью «Администратор ПАКМ».

После успешного процесса инициализации ПАКМ и запуска интерфейса Web Администрирования следует сразу ввести необходимые лицензии на использование модулей ПАКМ.

Без установки каких либо лицензий будет доступен только режим настройки HSM, либо через меню LCD панели, либо с использованием APM Web администрирования ПАКМ (доступно в состоянии ПАКМ - ADMIN_ONLY). Перевод ПАКМ в состояние ACTIVE (FULL ACTIVE) невозможно. Запуск платежных сервисов невозможен.

Существует два возможных вида лицензий:

- Лицензия на PKI HSM;
- Лицензия на PCI HSM.

Лицензия на PKI HSM является лицензией на базовые программные модули (БПМ). Должна устанавливаться всегда. Позволяет использовать ПАКМ в качестве разделяемого СКЗИ. Позволяет активировать каналы доступа пользователей к ПАКМ.

Лицензия на PCI HSM позволяет использовать ПАКМ в качестве Платежного HSM и активировать платежные сервисы.

Номера лицензий выдаются при приобретении ПАКМ.

Лицензии могут быть временными – на срок 3 месяца с момента первой установки, срочными – с указанием срока окончания действия лицензии, и бессрочными. Вся информация о виде лицензии и сроке её действия зашифрована в номере лицензии.

При выборе данного режима работы откроется окно:

The screenshot shows a web browser window with the URL <https://192.168.82.58>. The page title is "Програмно-аппаратный криптографический модуль "КриптоПро HSM"". The main heading is "Лицензии HSM". Below this is a table with the following data:

Продукт	Дата первой установки	Срок действия	Тип лицензии	Статус
PKI HSM	26.01.2023	Unlimited	Постоянная	Действует
PCI HSM	25.01.2023	28.04.2023	Временная	Действует

Below the table, there is a text prompt: "Установка новой лицензии. Введите номер лицензии:". This is followed by a text input field and a button labeled "Установить".

On the left side of the interface, there is a blue sidebar menu with the following items:

- Информация ПАКМ
- Сертификаты ПАКМ
- Параметры ПАКМ
- Настройки сети
- Настройки МЭ
- Настройки аудита
- Пользователи
- Резервные копии
- Журнал аудита
- скачать
- очистить
- Журнал событий
- Настройки PCI HSM
- Обновление PCI HSM
- Лицензии HSM**

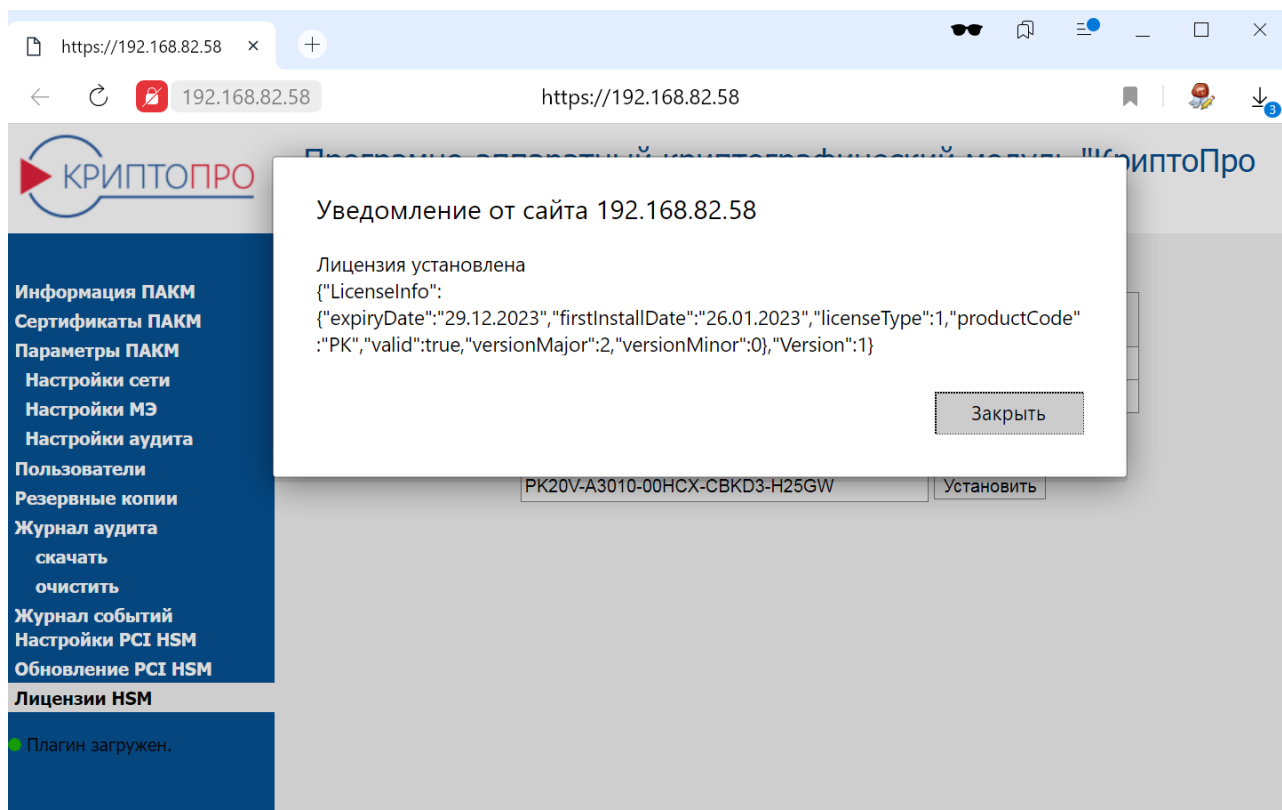
At the bottom of the sidebar, there is a status indicator: "Плагин загружен." with a green dot.

В верхней части окна отображается список установленных лицензий с указанными сроками их действия и типом лицензии.

Для ввода номера лицензии необходимо в специальное поле ввести выданный производителем номер и нажать кнопку «Установить»

В номере лицензии допускаются латинские буквы в верхнем регистре, цифры и символы «-»(дефис), без пробелов.

При успешной установке будет выдано соответствующее сообщение



В списке лицензий отобразится информация о только что установленной лицензии.

https://192.168.82.58 x +

192.168.82.58 https://192.168.82.58

КРИПТОПРО Программно-аппаратный криптографический модуль "КриптоПро HSM"

Информация ПАКМ

Сертификаты ПАКМ

Параметры ПАКМ

Настройки сети

Настройки МЭ

Настройки аудита

Пользователи

Резервные копии

Журнал аудита

скачать

очистить

Журнал событий

Настройки PCI HSM

Обновление PCI HSM

Лицензии HSM

Плагин загружен.

Лицензии HSM

Продукт	Дата первой установки	Срок действия	Тип лицензии	Статус
PKI HSM	26.01.2023	29.12.2023	Постоянная	Действует
PCI HSM	25.01.2023	28.04.2023	Временная	Действует

Установка новой лицензии. Введите номер лицензии:

Лицензия на PKI HSM может содержать расширение, позволяющее использовать дополнительный модуль «Дистанционного Электронного Голосования» (ДЭГ). В этом случае в колонке «Продукт» для данной строки таблицы будет отображаться следующее наименование: «PKI HSM (+ДЭГ)».

7. ДОСТУП К ФУНКЦИЯМ ПЛАТЕЖНОГО МОДУЛЯ

7.1. Подключение к консоли

В рамках реализации функций обеспечения безопасности платежных операций ПАКМ поддерживает 2 сервиса, предоставляющих фиксированный набор команд: консоль (CONSOLE) и хост (HOST).

Консольные команды используются для управления настройками платежного модуля, диагностики работы модуля, управления LMK и платежными ключами. Полный перечень и описание поддерживаемых консольных команд приведены в документе «ЖТЯИ.00096-03 97 01. Команды консоли».

Взаимодействие ПЭВМ, с которого осуществляется передача консольных команд, с ПАКМ осуществляется по протоколу TELNET с защитой канала с использованием российских криптографических алгоритмов с аутентификацией клиента. Для защиты канала используется приложение для создания TLS-туннеля (stunnel_msspi).

Для поддержки TLS-протокола на ПЭВМ должно быть установлено СКЗИ КриптоПро CSP версии 5.0 и выше (входит в комплект поставки ПАКМ).

Для доступа к консольным командам управления ПАКМ необходимо:

1. ПАКМ должен находиться в активном состоянии, должен быть настроен межсетевой экран (подробнее см. раздел 5).
2. Запустить консоль (Enable Console) с помощью LCD меню (подробнее см. 5.4) в одном из режимов работы:

a. secure

Доступен, если хост в данный момент выключен, требуется аутентификация второго Администратора платежной системы.

b. offline

Доступен, если хост в данный момент выключен

c. online

Доступен, если хост в данный момент запущен

3. На клиентской ПЭВМ выполнить настройку stunnel_msspi (подробнее см. документ «Приложение для создания TLS-туннеля»):
 - a. Для доступа к консоли платёжного модуля потребуются ключ и сертификат администратора Платежной системы, изданные ПАКМ и записанные на смарт-карту. Сертификат ключа доступа (аутентификации) администратора

должен быть установлен в личное хранилище пользователя с привязкой к закрытому ключу средствами СКЗИ «КриптоПро CSP». Самоподписанный сертификат ключа подписи ПАКМ должен быть установлен в доверенное хранилище корневых сертификатов (подробнее см. п. 6.1).

- b. После установки сертификата ключа доступа (аутентификации) администратора в хранилище необходимо дополнительно сохранить этот сертификат в файл на диске (без закрытого ключа, без цепочки сертификатов (файл *.cer) в формате BASE64 или DER).
- c. Сформировать файл конфигурации (stunnel.conf) и поместить его в директорию с исполняемым файлом stunnel.

Файл конфигурации должен содержать следующие строки:

```
debug = 4
[https]
client = yes
connect = 192.168.82.59:22222
cert=C:\admin.cer
accept = 127.0.0.1:22221
pin = 11111111
verify = 0
```

Параметры:

- connect — IP-адрес HSM и порт консоли
- cert — путь к файлу сертификата ключа доступа администратора
- pin — pin-код смарт-карты с ключом администратора

- 4. На клиентской ПЭВМ выполнить запуск утилиты stunnel_msspi (stunnel_msspi_cli в случае использования ОС Windows). Для ОС Windows также необходимо дополнительно нажать правой кнопкой мыши на значок утилиты в трее и в контекстном меню выбрать пункт Connections.
- 5. Выполнить подключение к консоли ПАКМ:

```
telnet localhost 22221
```

8. ПОРЯДОК ВЫПОЛНЕНИЯ ТЕХНИЧЕСКОГО ОБСЛУЖИВАНИЯ И РЕМОНТА ПАКМ

8.1. Порядок действий при отказе оборудования ПАКМ

При отказе оборудования ПАКМ, приведшем к невозможности выполнения пользователями ПАКМ своих функций, связанных с обращением к криптографическим функциям ПАКМ, необходимо:

- 1) Вызвать представителя предприятия-изготовителя для проведения ремонта.
- 2) Создать комиссию совместно с представителем предприятия-изготовителя для определения и возможного устранения причин отказа оборудования ПАКМ.
- 3) На месте провести диагностику и, возможно, устранение недостатков в работе ПАКМ.
- 4) Составить акт о проведении ремонта ПАКМ, подписанный обеими сторонами.

При невозможности устранения недостатков в работе ПАКМ на месте, если есть резервная копия ПАКМ:

- 1) Вызвать представителя предприятия-изготовителя для проведения ремонта.
- 2) Создать комиссию совместно с представителем предприятия-изготовителя для определения и возможного устранения причин отказа оборудования ПАКМ.
- 3) Провести отключение ПАКМ от сети/Сервера;
- 4) Уничтожить ключи пользователей, хранящиеся в ПАКМ, либо специальной процедурой «Full Clean» (если это возможно), либо физическим уничтожением Flash диска;
- 5) Подключить новый ПАКМ;
- 6) Установить в ПАКМ имеющуюся резервную копию при помощи специалистов предприятия изготовителя.
- 7) Провести процедуру инициализации нового ПАКМ;
- 8) Используя карту с ключами шифрования резервной копии произвести процедуру восстановления ПАКМ из резервной копии;
- 9) Перезапустить и активировать ПАКМ используя ключ активации восстановленного ПАКМ;
- 10) Отправить неработающий ПАКМ на предприятие-изготовитель для проведения ремонта.

При невозможности устранения недостатков в работе ПАКМ на месте и при отсутствии резервной копии ПАКМ:

- 1) Провести отключение ПАКМ от сети/Сервера;
- 2) Уничтожить защитные ключи (смарт-карты) ключей ЭП, хранящихся в ПАКМ;
- 3) Подключить новый ПАКМ;
- 4) Создать новые ключи пользователей на новом ПАКМ;
- 5) Вызвать представителя предприятия-изготовителя или отправить ПАКМ на предприятие-изготовитель для проведения ремонта.
- 6) Вскрывать корпус ПАКМ в отсутствие представителей предприятия-изготовителя категорически запрещается.

8.2. Порядок действий при проведении технического обслуживания ПАКМ

В ходе эксплуатации ПАКМ может возникнуть ситуация, требующая проведения технического обслуживания представителем предприятия-изготовителя. Такой ситуацией может быть, например, исчерпание запаса гаммы - случайной информации, используемой для генерации ключей пользователей.

Для проведения технического обслуживания ПАКМ представителем предприятия-изготовителя, необходимо:

- 1) Вызвать представителя предприятия-изготовителя для проведения технического обслуживания.
- 2) Создать комиссию совместно с представителем предприятия-изготовителя для проведения технического обслуживания ПАКМ на месте эксплуатации.
- 3) Провести техническое обслуживание на месте.
- 4) Составить акт о проведении технического обслуживания, подписанный обеими сторонами.

При невозможности технического обслуживания на месте, если есть резервная копия ПАКМ:

- 1) Вызвать представителя предприятия-изготовителя для проведения технического обслуживания.
- 2) Создать комиссию совместно с представителем предприятия-изготовителя для определения и возможного устранения причин отказа оборудования ПАКМ.
- 3) Провести отключение ПАКМ от сети/Сервера;

- 4) Уничтожить ключи пользователей, хранящиеся в ПАКМ, либо специальной процедурой «Full Clean», если это возможно, либо физическим уничтожением Flash диска;
- 5) Подключить новый ПАКМ;
- 6) Установить в ПАКМ имеющуюся резервную копию при помощи специалистов предприятия изготовителя.
- 7) Провести процедуру инициализации нового ПАКМ;
- 8) Используя карту с ключами шифрования резервной копии произвести процедуру восстановления ПАКМ из резервной копии;
- 9) Перезапустить и активировать ПАКМ используя ключ активации восстановленного ПАКМ;
- 10) Отправить ПАКМ на предприятие-изготовитель для проведения технического обслуживания.

При невозможности технического обслуживания на месте и при отсутствии резервной копии ПАКМ:

- 1) Провести отключение ПАКМ от сети/Сервера;
- 2) Уничтожить защитные ключи (смарт-карты) ключей ЭП, хранящиеся в ПАКМ;
- 3) Подключить новый ПАКМ;
- 4) Создать новые ключи пользователей на новом ПАКМ;
- 5) Вызвать представителя предприятия-изготовителя или отправить ПАКМ на предприятие-изготовитель для проведения технического обслуживания.