127018, Москва, ул. Сущёвский 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 Комплектация 3 Инструкция по использованию

ЖТЯИ.00096-02 90 01

Листов 153

2020 г.

Содержание

1. АННОТАЦИЯ

Данный документ содержит инструкцию по использованию программно-аппаратного модуля (ПАКМ) «КриптоПро HSM», его состав и описание ключевой системы.

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. ОСНОВНЫЕ ТЕРМИНЫ И ПОЛОЖЕНИЯ

Автоматизированная информационная система

Комплекс программных и технических средств, предназначенных для сбора, хранения, поиска и выдачи информации по запросам.

Автоматизированная система

Система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

Авторство информации

Однозначное соответствие между содержанием и/или формой информации и субъектом (объектом), сформировавшим эту информацию. Для пользователя авторство полученной им из системы или канала связи информации означает однозначное установление источника, сформировавшего эту информацию (ее автора).

Актуальность информации

Свойство информации сохранять свои свойства (ценность) для субъекта (пользователя) в течение определенного периода времени.

Администратор безопасности

Субъект доступа, основной обязанностью которого является обеспечение безопасности конфиденциальной связи на том участке сети, которую он курирует. Система административного управления безопасностью включает в себя комплекс организационно-технических мер, направленных на обеспечение конфиденциальности связи.

Основные направления деятельности администратора безопасности:

1. контроль целостности программного обеспечения;
2. управление ключевой системой: хранение, ввод в действие и смена ключей пользователей, генерация ключей пользователей;
3. управление доступом пользователей системы к программному обеспечению и данным, включая установку и периодическую смену паролей, управление средствами защиты коммуникаций, передаваемых, хранимых и обрабатываемых данных.

Администратор защиты

Субъект доступа, ответственный за защиту автоматизированной системы от несанкционированного доступа к информации.

Аутентификация

Проверка принадлежности субъекту доступа предъявленного им идентификатора, подтверждение подлинности.

Аутентификация информации

Установление подлинности информации исключительно на основе внутренней структуры самой информации независимо от источника этой информации, установление законным получателем (возможно арбитром) факта, что полученная информация наиболее вероятно была передана законным отправителем (источником) и что она при этом не заменена и не искажена. Любые преднамеренные и случайные попытки искажений информации обнаруживаются с соответствующей вероятностью.

Безопасность

1. Состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз.
2. Отсутствие недопустимого риска, связанного с возможностью нанесения ущерба.

Безопасность информации (информационная безопасность)

1. Состояние информации, информационных ресурсов и информационных систем, при котором с требуемой вероятностью обеспечивается защита информации (данных) от утечки, хищения, утраты, несанкционированного уничтожения, искажения, модификации (подделки), копирования, блокирования и т.п.
2. Состояние защищенности информации, обрабатываемой средствами вычислительной техники или автоматизированной системы, от внутренних или внешних угроз.

Блокирование информации

Прекращение или затруднение доступа законных пользователей к информации.

Верификация

1. Установление соответствия принятой и переданной информации с помощью логических методов.

2. процесс сравнения двух уровней спецификации средств вычислительной техники или автоматизированных систем на надлежащее соответствие.

Владелец информации

1. Субъект, осуществляющий владение и пользование информацией и реализующий полномочия распоряжения в пределах прав, установленных законом и/или собственником информации.
2. Субъект информационных отношений, обладающий правом владения, распоряжения и пользованием информационным ресурсом по договору с собственником информации.

Владелец информации, информационной системы

Субъект, в непосредственном ведении которого в соответствии с законом находятся информация, информационная структура.

Государственная тайна

Защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации.

Гриф конфиденциальности

Специальная отметка на носителе информации либо в сопроводительных документах на него, свидетельствующая о том, что носитель содержит конфиденциальную информацию.

Гриф секретности

Реквизиты, свидетельствующие о степени секретности сведений, содержащихся в их носителе, проставляемые на самом носителе и/или в сопроводительной документации на него.

Документ

1. Документированная информация, снабженная определенными реквизитами.
2. Материальный объект с информацией, закрепленной созданным человеком способом для ее передачи во времени и пространстве.

Документированная информация (документ)

Зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать.

Примечание. Документированная информация с ограниченным доступом по условиям ее правового режима подразделяется на информацию, отнесенную к государственной тайне, и конфиденциальную.

Документ в электронной форме (Электронный документ)

Электронный образ документа (платежного или иного) - файл, достоверность которого обеспечивается комплексом мероприятий по защите информации. При этом файл может содержать несколько документов (пакет документов).

ЭД представляет собой задокументированную совокупность данных, зафиксированных на материальном носителе (магнитном или бумажном) с реквизитами, позволяющими идентифицировать эту информацию и авторов документа. Идентификация ЭД обеспечивается средствами защита на основе алгоритмов шифрования, электронной подписи и защиты от несанкционированного доступа.

ЭД создается участником системы на основе бумажного документа либо на основании другого электронного документа и полностью повторяет его по содержанию. ЭД обрабатываются и хранятся в ЭВМ и могут передаваться по электронным каналам связи.

Доступ к информации

1. Получение субъектом возможности ознакомления с информацией, в том числе с помощью технических средств.
2. Ознакомление с информацией, ее обработка, в частности, копирование, модификация или уничтожение информации.

Доступность информации

Свойство информации, технических средств и технологии обработки, характеризующееся способностью обеспечивать беспрепятственный доступ к информации субъектов, имеющих на это надлежащие полномочия.

Заверение (нотаризация)

Регистрация данных у доверенного третьего лица для повышения уверенности в правильности таких характеристик, как содержание, источник данных, время доставки.

Защита информации

1. Деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.
2. Комплекс мероприятий, проводимых с целью предотвращения утечки, хищения, утраты, несанкционированного уничтожения, изменения, модификации (подделки), несанкционированного копирования, блокирования информации.

Защита информации от НСД

Составная часть общей проблемы обеспечения безопасности информации. Мероприятия по защите информации от НСД должны осуществляться взаимосвязано с мероприятиями по специальной защите основных и вспомогательных средств вычислительной техники, средств и систем связи от технических средств разведки и промышленного шпионажа. В общем случае, комплекс программно-технических средств и организационных (процедурных) решений по защите информации от НСД реализуется в рамках системы защиты информации от НСД, условно состоящей из следующих четырех подсистем: управления доступом; регистрации и учета; криптографической; обеспечения целостности.

Защищенное средство вычислительной техники (защищенная автоматизированная система)

Средство вычислительной техники (автоматизированная система), в котором реализован комплекс средств защиты.

Идентификация

Присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Имитозащита

Защита системы шифрованной связи от навязывания ложных данных [1].

Имитовставка

Отрезок информации фиксированной длины, полученный по определенному правилу из открытых данных и ключа и добавленный к зашифрованным данным для обеспечения имитозащиты [1].

Ключ (криптографический ключ)

Конкретное секретное состояние некоторых параметров алгоритма криптографического преобразования данных, обеспечивающее выбор одного преобразования из совокупности всевозможных для данного алгоритма преобразований [1].

Ключ электронной подписи

Уникальная последовательность символов, предназначенная для создания электронной подписи.

Ключ проверки электронной подписи

Уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи.

Компрометация ключа

Утрата доверия к тому, что используемые ключи обеспечивают безопасность информации. К событиям, связанным с компрометацией ключей относятся, включая, но не ограничиваясь, следующие:

1. Потеря ключевых носителей.
2. Потеря ключевых носителей с их последующим обнаружением.
3. Увольнение сотрудников, имевших доступ к ключевой информации.
4. Нарушение правил хранения и уничтожения (после окончания срока действия) закрытого ключа (ключа ЭП).
5. Возникновение подозрений на утечку информации или ее искажение в системе конфиденциальной связи.
6. Нарушение печати на сейфе с ключевыми носителями.
7. Случаи, когда нельзя достоверно установить, что произошло с ключевыми носителями (в том числе случаи, когда ключевой носитель вышел из строя и доказательно не опровергнута возможность того, что, данный факт произошел в результате несанкционированных действий злоумышленника)

Различают два вида компрометации закрытого ключа: **явную** и **неявную**. Первые четыре события должны трактоваться как явная компрометация ключей. Три следующих события требуют специального рассмотрения в каждом конкретном случае.

Конфиденциальность информации

Субъективно определяемая (приписываемая) информации характеристика (свойство), указывающая на необходимость введения ограничений на круг субъектов, имеющих доступ к данной информации, и обеспечиваемая способностью системы (среды) сохранять указанную информацию в тайне от субъектов, не имеющих полномочий на право доступа к ней.

Конфиденциальная информация

1. Документированная информация, доступ к которой ограничивается в соответствии с Законодательством РФ.
2. Информация, требующая защиты.

Контроль доступа (управление доступом)

Процесс ограничения доступа к ресурсам системы только разрешенным субъектам или объектам.

Криптографическая защита

Защита данных при помощи криптографического преобразования данных [1].

Криптографическое преобразование

Преобразование данных при помощи шифрования и (или) выработки имитовставки [1].

Лицензирование в области защиты информации

Деятельность, заключающаяся в передаче или получении прав на проведение работ в области защиты информации.

Мероприятия по защите информации

Совокупность действий по разработке и/или практическому применению способов и средств защиты информации.

Мероприятия по контролю эффективности защиты информации

Совокупность действий по разработке и/или практическому применению способов и средств контроля эффективности защиты информации.

Метка конфиденциальности

Элемент информации, который характеризует конфиденциальность информации, содержащейся в объекте.

Нарушитель безопасности информации

Физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности информации при ее обработке техническими средствами.

Нарушитель правил разграничения доступа

Субъект доступа, осуществляющий несанкционированный доступ к информации.

Некорректный электронный документ

Электронный документ, не прошедший процедуры расшифрования данных, проверки электронной подписи информация, контроля формата документов, а также документ, имеющий искажения в тексте сообщения (наличие символов, букв или цифр в расшифрованном (открытом) тексте документа, не позволяющих понять его смысл).

Непреднамеренное воздействие на информацию

Ошибка пользователя информацией, сбой технических и программных средств информационных систем, а также природное явление или иное нецеленаправленное на изменение информации воздействие, связанное с функционированием технических средств, систем или с деятельностью людей, приводящие к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

Несанкционированное воздействие на информацию

Воздействие на защищаемую информацию с нарушением установленных прав и/или правил на изменение информации, приводящее к искажению, уничтожению, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

Несанкционированный доступ к информации (НСД)

1. Получение защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации
2. Доступ к информации, нарушающий установленные правила разграничения доступа, с использованием штатных средств, предоставляемых СВТ или АС. Под штатными средствами понимается совокупность программного, микропрограммного и технического обеспечения СВТ или автоматизированной системы (АС).

Носитель информации

Физическое лицо или материальный объект, в том числе физическое поле, в которых информация находит свое отображение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

Объект доступа

Единица информационного ресурса автоматизированной системы, доступ к которой регламентируется правилами разграничения доступа.

Обработка информации

Передача, прием, хранение, преобразование и отображение информации.

Организация защиты информации

Содержание и порядок действий по обеспечению защиты информации

Открытый ключ

Криптографический ключ, который связан с закрытым с помощью особого математического соотношения. Открытый ключ известен всем другим пользователям системы и предназначен для проверки электронной подписи и расшифрования, позволяет определить автора подписи и достоверность электронного документа, но не позволяет вычислить закрытый ключ. Открытый ключ считается принадлежащим пользователю, если он был зарегистрирован (сертифицирован) установленным порядком.

Пароль

1. Идентификатор субъекта доступа, который является его (субъекта) секретом.
2. Секретная информация аутентификации, обычно представляющая собой строку знаков, которой должен обладать пользователь для доступа к защищенным данным.

Плановая смена ключей

Смена ключей с установленной в системе периодичностью, не вызванная компрометацией ключей.

Побочные электромагнитные излучения и наводки (ПЭМИН)

1. Электромагнитные излучения технических средств обработки информации, не предназначенные для передачи, приема или преднамеренного искажения информации, а также наводки от технических средств в окружающих предметах.

2. Нежелательные излучения и наводки, проявляющиеся в виде побочных, внеполосных, шумовых и наводимых сигналов, потенциально образующих неконтролируемые каналы утечки конфиденциальной.

Побочное электромагнитное излучение

Нежелательное информационное электромагнитное излучение, возникающее в результате нелинейных процессов в электрических цепях при обработке информации техническими средствами и приводящие к утечке информации.

Пользователь (потребитель) информации

1. Субъект, обращающийся к информационной системе или посреднику за получением необходимой ему информации и пользующийся ею.
2. Субъект, пользующийся информацией, полученной от ее собственника, владельца или посредника в соответствии с установленными правами и правилами доступа к информации либо с их.

Полномочный представитель организации

Представитель организации из числа первых должностных лиц в соответствии с уставным документом или, имеющий соответствующую доверенность.

Правила доступа к защищаемой информации

Совокупность правил, регламентирующих порядок и условия доступа к защищаемой информации и ее носителям.

Правила разграничения доступа (ПРД)

Совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

Право доступа к защищаемой информации; право

Совокупность правил доступа к защищаемой информации, установленных правовыми документами или собственником, владельцем информации.

Проверка электронной подписи документа

Проверка соотношения, связывающего хэш-функцию документа, подпись под этим документом и открытый ключ подписавшего пользователя. Если рассматриваемое соотношение оказывается выполненным, то подпись признается правильной, а сам документ - подлинным, в противном случае документ считается измененным, а подпись под ним - недействительной.

Разглашение информации

Несанкционированное доведение защищаемой информации до потребителей, не имеющих права доступа к этой информации.

Расшифрование данных

Процесс преобразования зашифрованных данных в открытые данные при помощи шифра [1].

Регламентация

Способ защиты информации в процессе функционирования системы мероприятий, создающих такие условия переработки защищаемых данных, при которых возможности несанкционированного доступа сводятся к минимуму. Считается, что для эффективной защиты необходимо строго регламентировать здания, помещения, размещение аппаратуры, организацию и обеспечение работы всего персонала, связанного с обработкой конфиденциальной информации.

Санкционированный доступ к информации

Доступ к информации, не нарушающий правила разграничения доступа.

Сертификат ключа проверки электронной подписи

Электронный документ или документ на бумажном носителе, выданные удостоверяющим центром либо доверенным лицом удостоверяющего центра и подтверждающие принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи.

Сертификат защиты

Документ, удостоверяющий соответствие средства вычислительной техники или автоматизированной системы набору определенных требований по защите от несанкционированного доступа к информации и дающий право разработчику на использование и/или распространение их как защищенных.

Сертификат открытого ключа

Сертификат открытого ключа подписи или шифрования представляет собой структурированную двоичную запись в формате ASN.1, состоящую из:

- имени субъекта или объекта системы, однозначно идентифицирующего его в системе;
- открытого ключа субъекта или объекта системы;
- дополнительных атрибутов, определяемых требованиями использования сертификата в системе;

- ЭП Издателя (Центра Сертификации), заверяющую совокупность этих данных.

Формат сертификата определен в рекомендациях ITU-T 1997 года X.509 [X.509] и рекомендациях IETF 1999 года RFC 2459 [PKIX]. В настоящее время основным принятым форматом является формат версии 3, позволяющий определить дополнения (**extensions**), с помощью которых реализуется определенная политика безопасности в системе.

Сертификат соответствия

Документ, выданный по правилам системы сертификации для подтверждения соответствия сертифицированной продукции установленным требованиям.

Секретный (закрытый) ключ

Криптографический ключ, который хранится пользователем системы в тайне. Он используется для формирования электронной подписи и шифрования.

Система защиты информации

Совокупность органов и/или исполнителей, используемая ими техника защиты информации, а также объекты защиты, организованные и функционирующие по правилам, установленным соответствующими правовыми, организационно-распорядительными и нормативными документами по защите информации.

Система защиты информации от НСД

Комплекс организационных мер и программно-технических (в том числе криптографических) средств защиты от несанкционированного доступа к информации в автоматизированных системах.

Способ защиты информации

Порядок и правила применения определенных принципов и средств защиты информации.

Средства вычислительной техники

Совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

Средство защиты информации

Техническое, программное средство, вещество и/или материал, предназначенные или используемые для защиты информации.

Средство защиты от несанкционированного доступа

Программное, техническое или программно-техническое средство, предназначенное для предотвращения или существенного затруднения несанкционированного доступа.

Средство криптографической защиты информации

Средство вычислительной техники, осуществляющее криптографическое преобразование информации для обеспечения ее безопасности.

Субъект доступа

Лицо или процесс, действия которого регламентируются правилами разграничения доступа.

Субъект информационных отношений

Физическое или юридическое лицо, обладающее определенным правом по отношению к информационному ресурсу. В зависимости от уровня полномочий субъект информационных отношений может быть источником, собственником, владельцем или пользователем информации.

Техническое средство обработки информации

Техническое средство, предназначенное для приема, накопления, хранения, поиска, преобразования, отображения и передачи информации по каналам связи.

Угроза безопасности

Совокупность условий и факторов, создающих опасность жизненно важным интересам личности, общества и государства.

Уничтожение информации

Действие, в результате которого информация перестает физически существовать в технических средствах ее обработки.

Управление ключами

Создание (генерация) ключей, их хранение, распространение, удаление (уничтожение), учет и применение в соответствии с политикой безопасности.

Утечка информации

1. Неконтролируемое распространение защищаемой информации в результате ее разглашения, несанкционированного доступа к информации и получения защищаемой информации разведкой.
2. Неправомерный выход конфиденциальной информации за пределы организации или круга лиц, которым эта информация доверена.

Функция хэширования

Заключается в сопоставлении произвольного набора данных в виде последовательности двоичных символов и его образа фиксированной небольшой длины,

что позволяет использовать эту функцию в процедурах электронной подписи для сокращения времени подписи и проверки подписи. Эффект сокращения времени достигается за счет вычисления подписи только под образом подписываемого набора данных [2].

Целостность информации

1. Способность средства вычислительной техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).
2. Свойство информации, заключающееся в ее существовании в неискаженном виде (неизменном по отношению к некоторому фиксированному ее состоянию).

Цель защиты информации

Заранее намеченный результат защиты информации.

1. Целью защиты информации может быть предотвращение ущерба собственнику, владельцу, пользователю информации в результате возможной утечки информации и/или несанкционированного и непреднамеренного воздействия на информацию.
2. Целями защиты являются: предотвращение утечки, хищения, утраты, искажения, подделки информации; предотвращение угроз безопасности личности, общества, государства; предотвращение несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию информации; предотвращение других форм незаконного вмешательства в информационные ресурсы и информационные системы, обеспечение правового режима документированной информации как объекта собственности; защита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных, имеющихся в информационных системах, сохранение государственной тайны конфиденциальности документированной информации в соответствии с законодательством; обеспечение прав субъектов в информационных процессах и при разработке, производстве и применении информационных систем, технологий и средств их обеспечения.

Шифр

Совокупность обратимых преобразований множества возможных открытых данных на множество возможных зашифрованных данных, осуществляемых по определенным правилам с применением ключей [1].

Шифрование

Процесс зашифрования или расшифрования [1].

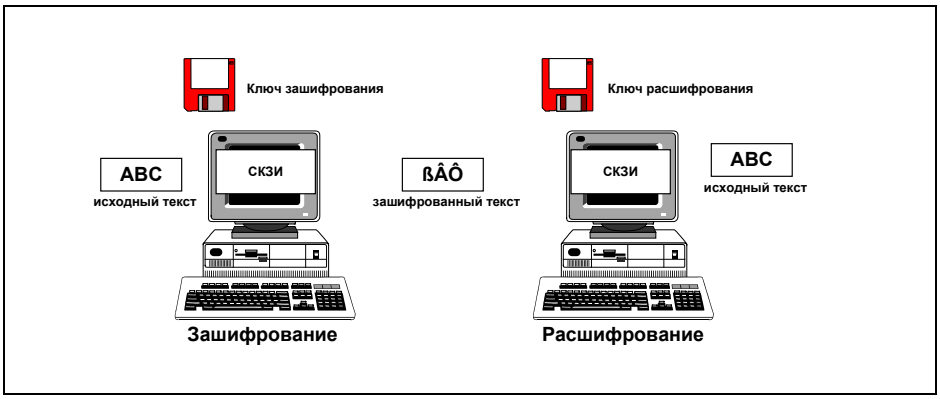


Рисунок 1. Шифрование информации

Шифрование информации – взаимно-однозначное математическое (криптографическое) преобразование, зависящее от ключа (секретный параметр преобразования), которое ставит в соответствие блоку открытой информации, представленной в некоторой цифровой кодировке, блок шифрованной информации, также представленной в цифровой кодировке. Термин шифрование объединяет в себе два процесса: зашифрование и расшифрование информации.

Если зашифрование и расшифрование осуществляются с использованием одного и того же ключа, то такой алгоритм криптографического преобразования называется симметричным, в противном случае — асимметричным.

Прочитать зашифрованное сообщение (информацию) может только пользователь, имеющий тот же закрытый ключ шифрования.

Шифрование документов (текстов)

Преобразование формы исходных (открытых) текстов сообщений таким образом, что их смысл становится непонятным для любого лица, не владеющего секретом обратного преобразования.

Шифровальные средства

Средства криптографической защиты информации:

1. реализующие криптографические алгоритмы преобразования информации аппаратные, программные и аппаратно-программные средства, системы и комплексы, предназначенные для защиты информации (в том числе и входящие в системы и комплексы защиты информации от несанкционированного доступа), циркулирующей в технических средствах, при ее обработке, хранении и передаче по каналам связи, включая шифровальную технику;

2. реализующие криптографические алгоритмы преобразования информации аппаратные, программные и аппаратно-программные средства, системы и комплексы защиты от навязывания ложной информации, включая средства имитозащиты и "электронной подписи";
3. аппаратные, программные и аппаратно-программные средства, системы и комплексы, предназначенные для изготовления и распределения ключевых документов, используемых в шифровальных средствах, независимо от вида носителя ключевой информации.
4. ручные шифры, документы кодирования и другие носители ключевой информации.

Электронная подпись (ЭП), электронная цифровая подпись (ЭЦП)

Данные, добавляемые к блоку данных полученные в результате его криптографического преобразования, зависящего от закрытого ключа и блока данных, которые позволяют приемнику данных удостовериться в целостности блока данных и подлинности источника данных, а также обеспечить защиту от подлога со стороны приемника данных.

Проверка электронной подписи под блоком открытой информации производится с помощью криптографического преобразования и ключа проверки ЭП, соответствующего ключу ЭП, участвовавшему в процессе установки ЭП.

Рисунок 2. Формирование и проверка ЭП

Электронная подпись обеспечивает целостность сообщений (документов), передаваемых по незащищенным телекоммуникационным каналам общего пользования в системах обработки информации различного назначения, с гарантированной идентификацией ее автора (лица, подписавшего документ).

Электронная подпись позволяет заменить при безбумажном документообороте традиционные печать и подпись. При построении подписи вместо обычной связи между печатью или рукописной подписью и листом бумаги выступает сложная математическая зависимость между электронным документом, закрытым и открытым ключами.

Практическая невозможность подделки электронной подписи опирается на очень большой объем определенных математических вычислений.

Проставление подписи под документом не меняет самого документа, она только дает возможность проверить подлинность и авторство полученной информации.

3. СОСТАВ И НАЗНАЧЕНИЕ ПАКМ

3.1. 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 (хосту), 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:

- формирования/проверки электронной подписи (ЭП) под блоком данных по запросу пользователей.
- шифрования/расшифрования блоков данных по запросам пользователей;

При этом ПАКМ «КриптоПро HSM» обеспечивает:

- реализацию криптографических функций и интерфейс взаимодействия с серверами и рабочими станциями пользователей;
- интерфейс к прикладным криптографическим функциям в соответствии со спецификацией Microsoft Cryptographic Service Provider;
- возможность использования функций ПАКМ «КриптоПро HSM» через интерфейсы Microsoft CryptoAPI;
- идентификацию и аутентификацию пользователей при локальном и удаленном доступе к ПАКМ «КриптоПро HSM»;
- проверку целостности критичного к безопасному функционированию ПО при инициализации ПАКМ «КриптоПро HSM»;
- генерацию случайных чисел с использованием аппаратного ДСЧ;
- генерацию закрытых ключей обмена и ключей ЭП с использованием исходного материала, предоставленного уполномоченной организацией;
- срок действия ключа ЭП до 3-х лет. При использовании ПАКМ в качестве СКЗИ в программных комплексах удостоверяющих центров, реализованных и сертифицированных по классу защиты КВ2, срок действия ключа подписи уполномоченного лица удостоверяющего центра может достигать 7 лет. Максимальный срок действия ключей проверки ЭП — 15 лет после окончания

срока действия соответствующего ключа ЭП. Максимальный срок действия открытых ключей обмена — не более 3-х лет. Максимальный срок действия закрытого ключа обмена совпадает со сроком действия закрытого ключа[1];

- сопряжение с сервером/серверной группой по отдельному сегменту Ethernet;
- ввод закрытого ключа/ключа ЭП с ключевых носителей на интеллектуальной карте;
- выполнение функций создания и проверки электронной подписи (ЭП) согласно ГОСТ Р 34.10-2001 и ГОСТ Р 34.10-2012 (ГОСТ 34.10-2018), вычисление хэш-функции согласно ГОСТ Р 34.11-94 и ГОСТ Р 34.11-2012 (ГОСТ 34.11-2018);
- шифрование и имитозащита согласно ГОСТ 28147-89;
- опционально, поддержку алгоритмов RSA в части генерации ключей, формирования и проверки ЭП, шифрования и расшифрования;
- возможность встречной работы ПАКМ «КриптоПро HSM» с СКЗИ «КриптоПро CSP»;
- уничтожение ключей;
- сопряжение с устройством доступа по криптографически защищенному каналу «К2». Канал «К2» – локальный защищенный канал, используется для защищенного обмена информацией между ПАКМ и устройством доступа к ПАКМ;
- сопряжение с устройством доступа по криптографически защищенному каналу «К»[2]. Канал «К» – локальный защищенный канал, используется для защищенного обмена информацией между ПАКМ и устройством доступа к ПАКМ;
- регистрация событий в журнале аудита криптографических вызовов ПАКМ.

Примечания:

1. Сроки действия ключей ЭП и закрытых ключей обмена могут уточняться при проведении работ по встраиванию ПАКМ «КриптоПро HSM» в системы по ТЗ, согласованным с 8 Центром ФСБ России.

2. Канал «К» используется только в рамках Головного удостоверяющего центра (ГУЦ).

ПАКМ «КриптоПро HSM» Комплектация 1 Исполнение 1 удовлетворяет классу КВ/КВ2, Комплектация 1 Исполнения 2-5 — классу КС3 при выполнении требований данного документа в части условий применения и требований документа «ЖТЯИ.00096-02 91 01. КриптоПро HSM. Руководство Администратора безопасности».

ПАКМ «КриптоПро HSM» предполагает различные варианты комплектации, включающие автономные СКЗИ по различным уровням защиты:

- Комплектация 1 Исполнение 1 ПАКМ «КриптоПро HSM», уровень защиты КВ/КВ2
- Комплектация 1 Исполнение 2 ПАКМ «КриптоПро HSM», уровень защиты КС3

- Комплектация 1 Исполнение 3 ПАКМ «КриптоПро HSM», уровень защиты КС3
- Комплектация 1 Исполнение 4 ПАКМ «КриптоПро HSM», уровень защиты КС3
- Комплектация 1 Исполнение 5 ПАКМ «КриптоПро HSM», уровень защиты КС3
- Комплектация 2 Исполнение 1 ПАКМ «КриптоПро HSM», уровень защиты КС1
- Комплектация 2 Исполнение 2 ПАКМ «КриптоПро HSM», уровень защиты КС2
- Комплектация 2 Исполнение 3 ПАКМ «КриптоПро HSM», уровень защиты КС3
- Комплектация 3 Исполнение «DSS + CSP версия 4.0 Исполнение 1-Base», уровень защиты КС1
- Комплектация 3 Исполнение «DSS + CSP версия 4.0 Исполнение 2-Base», уровень защиты КС2
- Комплектация 3 Исполнение «DSS + CSP версия 4.0 Исполнение 3-Base», уровень защиты КС3
- Комплектация 3 Исполнение «DSS + CSP версия 4.0 Исполнение 1-Lic», уровень защиты КС1
- Комплектация 3 Исполнение «DSS + CSP версия 4.0 Исполнение 2-Lic», уровень защиты КС2
- Комплектация 3 Исполнение «DSS + CSP версия 5.0 КС1 Исполнение 1-Base», уровень защиты КС1
- Комплектация 3 Исполнение «DSS + CSP версия 5.0 КС2 Исполнение 2-Base», уровень защиты КС2
- Комплектация 3 Исполнение «DSS + CSP версия 5.0 КС3 Исполнение 3-Base», уровень защиты КС3
- Комплектация 3 Исполнение «DSS + JCP версия 2.0 Исполнение 2», уровень защиты КС1
- Комплектация 3 Исполнение «DSS + SIM (QES)», уровень защиты КС1
- Комплектация 3 Исполнение «DSS + SIM (M2M)», уровень защиты КС1
- Комплектация 3 Исполнение «DSS + myDSS», уровень защиты КС1
- Комплектация 3 Исполнение «DSS + AirKey Lite», уровень защиты КС1
- Комплектация 3 Исполнение «myDSS SDK», уровень защиты КС1
- Комплектация 3 Исполнение «Сбербанк myDSS SDK», уровень защиты КС1
- Комплектация 3 Исполнение «DSS Client SDK», уровень защиты КС1

Примечание: Комплектации 2 и 3 могут использоваться с любой аппаратной компонентой Комплектации 1.

Компонент «КриптоПро HSM Client» является ответной частью, устанавливаемой на рабочие станции и сервера, необходимой для трансляции криптографических вызовов к ПАКМ «КриптоПро HSM» по безопасным каналам «К», «К2».

ПО «КриптоПро HSM Client» поставляется на CD-ROM совместно с ПАКМ «КриптоПро HSM». Предусмотрена поставка клиентской компоненты отдельно от ПАКМ

«КриптоПро HSM» в соответствующей комплектации согласно Формуляру ЖТЯИ.00096-02 30 01.

Порядок установки и использования «КриптоПро HSM Client» описан в документе «ЖТЯИ.00096-02 90 02. КриптоПро HSM. Использование интерфейсных модулей», а также в документе «ЖТЯИ.00096-02 93 01. КриптоПро HSM. Руководство пользователя».

3.2. 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» версий 4.0/5.0.

Реализация ПАКМ, 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 1) или КС3 (Комплектация 1 Исполнения 2-5), общий уровень безопасности системы может быть повышен, и наоборот, при замене ПАКМ «КриптоПро HSM» средством криптографической защиты информации «КриптоПро CSP» версий 4.0/5.0 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.

Также возможно применение ПАКМ в персональных (не серверных) системах.

3.3. 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») электронного замка («Соболь») (не менее 2 шт.);
- Эксплуатационная документация.

Для использования ПАКМ на компьютер пользователя/сервер необходимо установить дистрибутив ПО интерфейсных модулей.

Таблетки ЭЗ 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 3). 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 «x» (отмена).

Рисунок 3 Панель управления ПАКМ

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

3.4. Сведения об используемых криптопровайдерах

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

- **Crypto-Pro HSM CSP (тип 75)**
- **Crypto-Pro HSM Svc CSP (тип 75)**
- **Crypto-Pro HSM RSA CSP (тип 1)**
- **Crypto-Pro HSM RSA Svc CSP (тип 1)**
- **Crypto-Pro GOST R 34.10-2001 HSM CSP (тип 75)**
- **Crypto-Pro GOST R 34.10-2012 HSM CSP (тип 80)**
- **Crypto-Pro GOST R 34.10-2012 Strong HSM CSP (тип 81)**
- **Crypto-Pro GOST R 34.10-2001 HSM Svc CSP (тип 75)**
- **Crypto-Pro GOST R 34.10-2012 HSM Svc CSP (тип 80)**
- **Crypto-Pro GOST R 34.10-2012 Strong HSM Svc CSP (тип 81)**

Криптопровайдер **Crypto-Pro GOST R 34.10-2001 HSM CSP** (синоним имени "Crypto-Pro HSM CSP") — основной криптопровайдер 75-го типа, который должен использоваться внешними приложениями. Он реализует:

- 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 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 (см. п. 4.3.4).

Криптопровайдеры **Crypto-Pro GOST R 34.10-2012 HSM CSP и Crypto-Pro GOST R 34.10-2012 Strong HSM CSP** 80 и 81 типа соответственно 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;

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 (см. п. 4.3.4).

Криптопровайдеры, включающие лексему «Svc» в имени, отличается от криптопровайдеров без её наличия тем, что позволяет выводить запросы на ввод пин-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 - EKU) «1.2.643.2.2.34.22».

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

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-ти ключе активации ПАКМ, то все ключи, созданные на считывателе «HSMDB», невозможно открыть без активации ПАКМ (активации разделенного «ключа активации ПАКМ»).

В ПАКМ «КриптоПро HSM» устанавливаются криптопровайдеры **Crypto-Pro HSM RSA CSP** (тип 1) и **Crypto-Pro HSM RSA Svc CSP** (тип 1), которые реализуют алгоритмы электронной подписи RSA:

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

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

Обычному пользователю не следует использовать криптопровайдеры «"… Svc … "». Система всё равно не позволит ему работать 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 (простым языком – «не залогинился»).

Клиентская часть **обычных** провайдеров (без лексемы Svc в имени) реализована в виде обычного 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 «КриптоПро HSM Client» нет активной Windows сессии (ни одного «залогиненного» пользователя), то никто не сможет обслужить криптографические запросы, обращенные к обычным криптопровайдерам.

Администраторам серверов, наоборот, рекомендуется установить для провайдеров типов 75, 80, 81 по-умолчанию соответствующие имена **сервисных** провайдеров (включающие лексему «Svc» в имени), т.к. некоторые вызовы сервисы Windows делают, используя провайдеры «по умолчанию».

Кроме этого, обращения к криптопровайдерам, работающим с ПАКМ через сервис, могут быть сделаны только пользователями с учетными именами SYSTEM (LocalSystem), NetworkService, 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 «КриптоПро HSM Client» не изменяет значение провайдера по умолчанию для 1 типа. Обычно, в ОС Windows им является криптопровайдер «Microsoft Strong Cryptographic Provider».

В целях обеспечения возможности создания высокопроизводительных систем повышенной надежности, создания пулов из ПАКМ, горячего резервирования средств СКЗИ в ПАКМ «КриптоПро HSM» зарегистрировано дополнительно по 8 имен криптопровайдеров 1-го и 75-го типа:

Crypto-Pro HSM RSA CSP 01

….

Crypto-Pro HSM RSA CSP 08

и

Crypto-Pro HSM CSP 01

….

Crypto-Pro HSM CSP 08,

которые являются дублерами имен, соответственно Crypto-Pro HSM RSA CSP и Crypto-Pro HSM CSP. Приложения могут использовать эти имена для доступа к различным ПАКМ из пула ПАКМ, размещенных в корпоративной сети. При необходимости эти криптопровайдеры на устройствах доступа должны быть зарегистрированы вручную.

4. КОНЦЕПЦИЯ И АРХИТЕКТУРА КОМПОНЕНТ ПАКМ

Общую схему компонент среды функционирования ПАКМ (СФ) можно представить на следующих диаграммах (см. Рисунок 4, Рисунок 5, Рисунок 6).

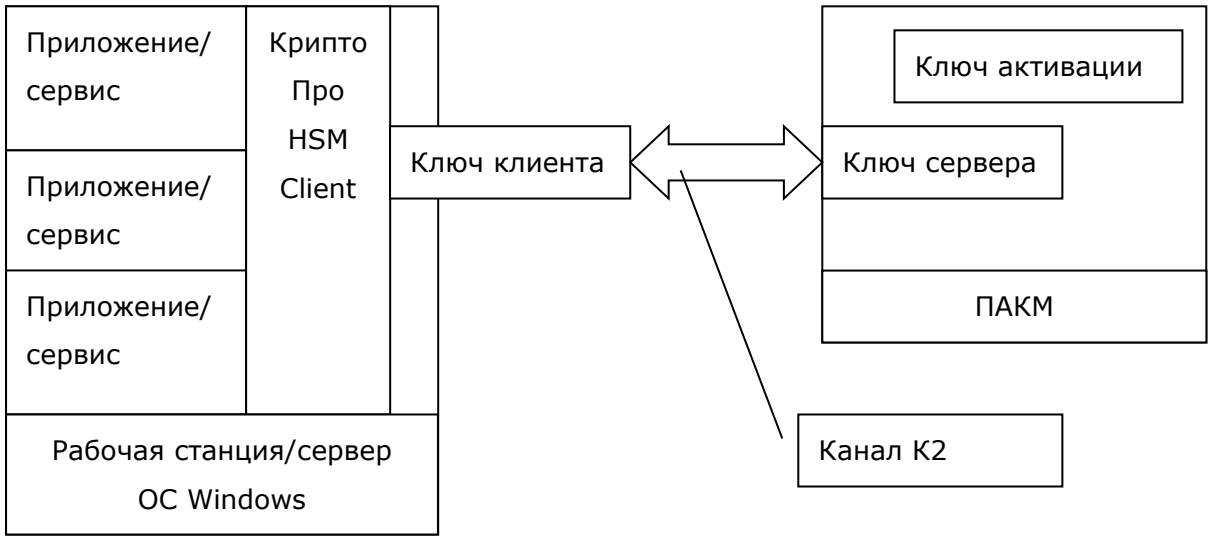


Рисунок 4. Общая схема компонент СФ при использовании с рабочими станциями пользователей/серверами с установленной ОС семейства Windows.

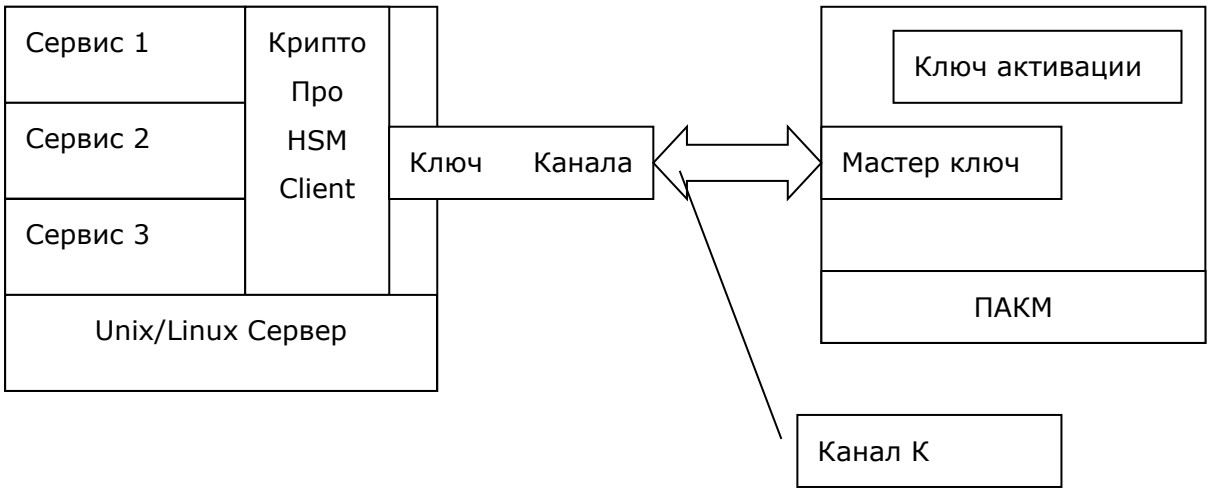


Рисунок 5. Общая схема компонент СФ при использовании с серверами приложений, базирующимися на ОС семейства Unix/Linux.

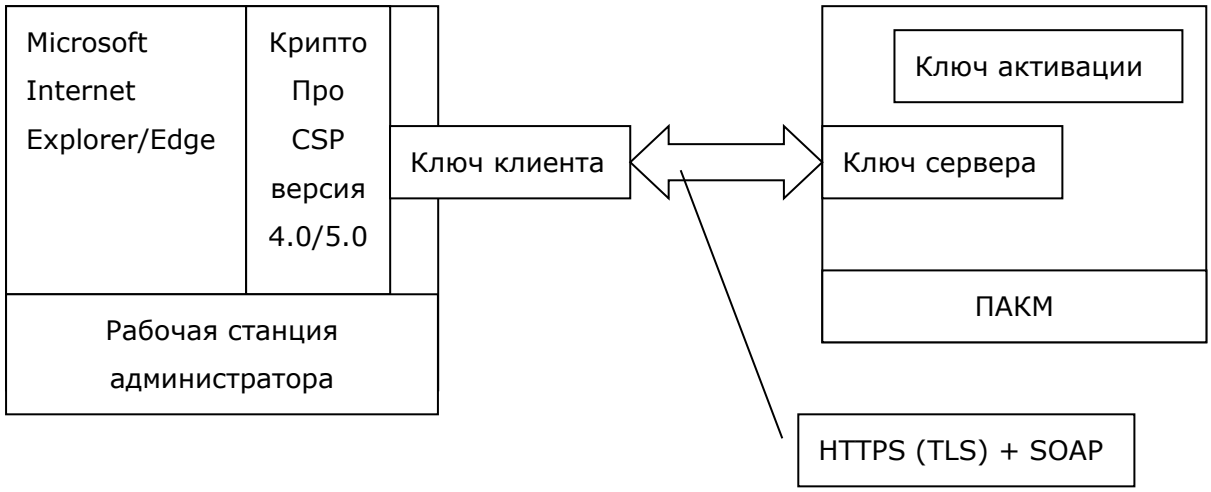


Рисунок 6. Общая схема компонент удаленного рабочего места администратора.

4.1. Ролевая модель доступа к функциям ПАКМ

ПАКМ «КриптоПро HSM» может использоваться в корпоративных локальных сетях, как разделяемое СКЗИ, обслуживающее криптографические запросы обычных пользователей сети. При этом закрытые ключи/ключи ЭП пользователей формируются и хранятся в ПАКМ в зашифрованном виде, и ответственность за их сохранность и несанкционированное использование разделяется между владельцами-служащими и службой безопасности компании. Таким образом, снижается вероятность компрометации ключей пользователей вследствие утери или хищения ключевого носителя, обеспечивается дополнительный контроль над использованием ключа, снижаются затраты компании на сопровождение средств криптографической защиты информации.

ПАКМ «КриптоПро HSM» может обслуживать криптографические запросы как обычных пользователей сети, так и системных сервисов серверных компонент (например, Microsoft CA, Microsoft IIS, КриптоПро УЦ, Служб Штампов времени, Служб проверки статусов сертификатов и др.). В соответствии с этим все пользователи, как потребители сервисов ПАКМ делятся на две группы:

- Клиенты ПАКМ – Пользователи
- Клиенты ПАКМ – Сервера (Администраторы серверов)

На компьютеры пользователей ПАКМ устанавливается клиентская компонента – ПО «КриптоПро HSM Client». Взаимодействие клиентов с ПАКМ производится по так называемым защищенным каналам: канал «К2» для ПЭВМ клиентов с установленной ОС семейства Windows, Unix/Linux и канал «К» для ПЭВМ клиентов с установленной ОС семейства Unix/Linux.

Механизм работы с клиентами ПАКМ – Unix/Linux серверами (реализация канала «К») унаследован от предыдущих реализаций ПАКМ (ПАКМ «Феникс-М», ПАКМ «АТЛИКС HSM»), и в целях совместимости остался без изменений.

Реализация канала «К2» на ОС семейства Windows и Unix/Linux полностью основана на реализации протокола TLS с учетом рекомендаций по стандартизации Технического комитета по стандартизации «Криптографическая защита информации» (ТК 26) «Использование наборов алгоритмов шифрования на основе ГОСТ 28147-89 для протокола безопасности транспортного уровня (TLS)».

Все клиенты ПАКМ проходят процедуру аутентификации, прежде чем им будет разрешено обращение к криптографическим функциям ПАКМ.

Каждый клиент ПАКМ, будь то обычный пользователь, либо администратор сервера, получает уникальный номер (нумерация начинается с 1000), номер группы, обычно совпадающий с номером пользователя, и имя при регистрации в ПАКМ, а также ключи доступа к ПАКМ. При этом клиенты ПАКМ, непривилегированные «пользователи», регистрируются в ПАКМ администратором ПАКМ. На специальный носитель (обычно смарт-карта – карта канала «К2») записывается секретный ключ доступа пользователя к ПАКМ, сертификат этого ключа (сертификат открытого ключа), изданный ПАКМ, и сертификат открытого ключа подписи ПАКМ, которым подписан сертификат ключа доступа.

Смарт-карты для доступа к ПАКМ при использовании канала «К» имеют внутри другой формат. Клиенты ПАКМ, сервера, регистрируются автоматически при первом обращении к ПАКМ. При этом в считывателе сервера постоянно должна находиться карта канала «К».

Каждый ПАКМ имеет уникальный серийный номер – идентификатор ПАКМ.

Уникальное имя клиента ПАКМ (аналог LogonName) формируется следующим образом:

- для клиентов ПАКМ пользователей в формате UPN имени <номер пользователя>.<номер группы>@<идентификатор ПАКМ>;
- для клиентов ПАКМ, серверов (реализация старого «канала «К»»), - <UID пользователя>.<GID пользователя>.

Администратор ПАКМ является обычным пользователем ПАКМ, у которого в расширении сертификата ключа доступа Extended Key Usage указан специальный OID.

Управление пользователями ПАКМ заключается в добавлении новых пользователей, изменении их регистрационной информации, переиздании пользователям ключей и сертификатов доступа, блокировании сертификатов доступа пользователей (временном приостановлении их действия), удалении пользователей вместе со всеми объектами, относящимися к ним (включая ключи подписи пользователей).

Кроме обычных пользователей ПАКМ, потребителей криптографического сервиса ПАКМ, существуют привилегированные пользователи ПАКМ.

ПАКМ «КриптоПро HSM» разработан с учетом того, что привилегированные пользователи ПАКМ (члены группы администраторов, имеющие доступ в контролируемую зону) могут являться потенциальными нарушителями. При этом возможность сговора между ними исключается. В соответствии с этим в ПАКМ реализована ролевая модель доступа к различным функциям. Это означает, что каждому отдельному члену административной группы дается доступ только к строго определенному набору административных функций, не позволяющих провести успешную атаку на получение контроля над ключами пользователей, хранящимися в ПАКМ «КриптоПро HSM».

Программное обеспечение ПАКМ «КриптоПро HSM» различает следующие роли:

- Обычный пользователь ПАКМ «КриптоПро HSM»;
- Администратор сервера, сервисы которого используют ПАКМ «КриптоПро HSM»;
- Администратор ПАКМ «КриптоПро HSM»;
- Аудитор ПАКМ «КриптоПро HSM»;
- Администратор резервного копирования ПАКМ «КриптоПро HSM»;
- Суперпользователь ПАКМ «КриптоПро HSM».

Признак того, что пользователю назначена та или иная роль хранится в сертификате ключа доступа к функциям ПАКМ, как специальное расширение (Extended Key Usage) сертификата. Доступ к ПАКМ (локальный или удаленный) осуществляется только с использованием данного сертификата ключа доступа и самого ключа (секретной его части).

Ключи и сертификат доступа к ПАКМ формируется ПАКМ и выдается обычным пользователям администратором ПАКМ. Ключи и сертификат доступа к ПАКМ для привилегированных пользователей формируется ПАКМ и выдается суперпользователем ПАКМ.

Суперпользователь ПАКМ — группа привилегированных пользователей, как минимум из 3-х человек – держателей частей разделенного секрета ключа активации ПАКМ. Т.е. это любые три из пяти лиц, хранителей частей разделенного секрета ключа активации ПАКМ. Только данная группа лиц может локально получить доступ к функциям ПАКМ, позволяющим добавлять и изменять учетные записи привилегированных пользователей (администраторов, аудиторов, администраторов резервного копирования ПАКМ) и формировать им ключи и сертификаты ключей доступа к функциям ПАКМ. Кроме этого, суперпользователь может выполнять любые функции, присущие любой «привилегированной» роли. Т.е. суперпользователь совмещает роли администраторов, аудиторов, администраторов резервного копирования ПАКМ. Смена разделенного ключа активации ПАКМ, включающая смену ключа шифрования ПАКМ, невозможна без активации старого ключа активации, т.е. без присутствия «суперпользователя». Суперпользователи

ПАКМ могут являться одновременно привилегированными пользователями ПАКМ – администратором, аудитором, администратором резервного копирования ПАКМ;

Любое другое совмещение ролей привилегированных пользователей ПАКМ в одном лице не допускается.

Обычный пользователь ПАКМ не имеет локального доступа к ПАКМ, не может выполнять ни одной административной функции ПАКМ. Получает удаленный доступ к криптографическим функциям ПАКМ «КриптоПро HSM» при помощи ключа и сертификата ключа доступа, выдаваемого ему администратором ПАКМ. Администратор ПАКМ имеет доступ к учетной записи пользователя в ПАКМ.

Администратор сервера, сервисы которого используют ПАКМ «КриптоПро HSM», с точки зрения доступа к функциям ПАКМ почти ничем не отличается от обычного пользователя ПАКМ, за исключением того, что в сертификате ключа доступа к функциям ПАКМ прописывается специальное расширение (EKU) «1.2.643.2.2.34.22». Наличие в сертификате такого расширения приводит к тому, что запросы на ввод пин-кодов для ключей, создаваемых приложениями (сервисами операционной системы сервера) на сервере, выдаются не на рабочий стол рабочей станции, как это происходит для обычных пользователей СКЗИ, а на LCD панель ПАКМ. Это важно, так как многие сервисы операционной системы на сервере, использующие функции СКЗИ, не имеют доступа к рабочему столу (консоли) и не могут запросить с нее pin-код на доступ к контейнеру ключа. Кроме того, использование указанного сертификата ключа доступа к функциям ПАКМ в процессе аутентификации позволяет при соответствующих настройках отменить режим шифрования канала «К2», что может потребоваться для повышения производительности сервера приложений (например, при использовании ПАКМ для операций шифрования/расшифрования TLS/SSL трафика сильно загруженных WEB серверов). Необходимо отметить, что данный сертификат ключа доступа может использоваться только при организации канала «К2».

Администратор ПАКМ «КриптоПро HSM» имеет локальный и удаленный (через web интерфейс администрирования) доступ к следующим функциям управления ПАКМ:

- управление учетными записями обычных (непривилегированных) пользователей и администраторов серверов, включая функции обновления их ключей и сертификатов ключей доступа к ПАКМ;
- обновления внутренних ключей и сертификатов ПАКМ (ключи и сертификаты TLS сервера, ключа подписи и самоподписанного сертификата ПАКМ);
- управление настройками режимов работы ПАКМ, исключая некоторые настройки работы с журналом аудита;
- управление сетевыми настройками ПАКМ;
- управление настройками встроенного межсетевого экрана ПАКМ;
- управление системными часами ПАКМ;

- изменение состояния ПАКМ;
- выгрузка резервных копий ПАКМ;
- инициация процедуры восстановления ПАКМ из резервной копии (требует присутствия администратора резервного копирования с картой с ключом шифрования резервной копии).

В сертификате ключа доступа к функциям ПАКМ данной роли прописывается специальное расширение (EKU) «1.2.643.2.2.34.21».

Аудитор ПАКМ «КриптоПро HSM» осуществляет контроль за событиями, так или иначе связанными с функционированием ПАКМ. Основными источниками информации для него служат внутренние журналы событий СКЗИ и аудита ПАКМ. Аудитор ПАКМ имеет локальный и удаленный (через web интерфейс администрирования) доступ к следующим функциям управления ПАКМ:

- управление настройками ПАКМ, связанными с режимом очистки журнала аудита;
- управление настройками регистрации тех или иных видов событий в журнале аудита ПАКМ;
- управление полнотой отражения событий в журнале ПАКМ;
- очистка журнала аудита (с подтверждением данного действия Администратором ПАКМ).
- В сертификате ключа доступа к функциям ПАКМ данной роли прописывается специальное расширение (EKU) «1.2.643.2.2.34.28».

Администратор резервного копирования ПАКМ «КриптоПро HSM» осуществляет создание, удаление резервных копий ПАКМ. Хранит смарт-карты с ключами шифрования резервных копий. Осуществляет загрузку в ПАКМ ранее выгруженных Администратором из ПАКМ резервных копий.

Не имеет права на выгрузку из ПАКМ резервных копий и на запуск процедуры восстановления ПАКМ из резервной копии (данные режимы доступны Администратору ПАКМ и суперпользователю).

В сертификате ключа доступа к функциям ПАКМ данной роли прописывается специальное расширение (EKU) «1.2.643.2.2.34.27».

В случае использования web-интерфейса администрирования рекомендуется иметь в системе как минимум по две учетные записи каждой роли привилегированных пользователей. Одна необходима для доступа к функциям управления с LCD панели, другая - для доступа к функциям управления с удаленного рабочего места администратора. Это связано с тем, что ПАКМ «КриптоПро HSM» формирует ключи доступа на смарт-карте с высоким уровнем криптографической защиты (до КВ), при использовании этого ключа на компьютере с СКЗИ «КриптоПро CSP», реализованным по более низкому классу защиты, уровень защиты ключа будет понижен (при согласии пользователя), после чего

использовать такой ключ снова в СКЗИ более высокого уровня будет невозможно. Это означает, что ПАКМ откажется работать с ключевыми контейнерами, реализованными с более низкими уровнями защиты при попытке доступа к нему с LCD панели.

В случае утери по какой-либо причине всех ключей привилегированных пользователей ПАКМ, доступ к LCD панели ПАКМ может быть осуществлен суперпользователем с помощью разделенного по схеме «3-и из 5-ти» ключа активации ПАКМ. После чего может быть сформирован новый ключ любого из администраторов ПАКМ.

4.2. Ключевая система и ключевые носители

4.2.1. Общие положения

Ключевая система ПАКМ «КриптоПро HSM» включает в себя ключи ЭП, шифрования и обмена (экспорта ключей).

Ключи ЭП представляются ключевой парой: ключ ЭП – для формирования ЭП, ключ проверки ЭП.

Ключи шифрования – симметричные ключи сообщения (пакета), случайные или диверсифицированные из случайного ключа сессии по открытому заголовку сообщения (пакета).

Ключи обмена строятся на основе открытого распределения ключей по алгоритму Диффи-Хеллмана на базе ключевых пар закрытый/открытый ключи алгоритма ГОСТ Р 34.10-2001 и ГОСТ Р 34.10-2012 (ГОСТ 34.10-2018).

На ключевых носителях ключи хранятся в формате ключевого контейнера. Ключевой контейнер содержит также информацию, необходимую для обеспечения криптографической защиты ключей и их целостности.

Закрытые ключи (ключи ЭП), хранящиеся в памяти ПАКМ, шифруются прямо или косвенно (через промежуточные ключи – ключи шифрования) на ключе активации ПАКМ.

Ключ активации ПАКМ использует схему разделения секрета с вводом ключевой информации с любых 3-х (k) из 5-ти (n) носителей для формирования функционального ключа. При этом обеспечивается защита функционального ключа при компрометации ключевой информации на любых не более k-1 носителях. В случае компрометации ключевой информации хотя бы с одного носителя, необходимо перевыпустить все 5 (n) ключей.

Интеллектуальные карты поставляются с ПАКМ «КриптоПро HSM» отформатированными, с предустановленным pin-кодом «11111111». При записи ключей на карту pin-код необходимо сменить.

Использование ПАКМ с выключенным режимом усиленного контроля использования ключей **не допускается**. Включение режима усиленного контроля использования ключей

(**StrengthenedKeyUsageControl**) осуществляется с помощью утилиты cpconfig с помощью команды:

```
./cpconfig -ini '\config\parameters' -add long StrengthenedKeyUsageControl 1
```

4.2.2. Маркировка ключевых носителей на интеллектуальных картах

При выпуске/записи карт с ключами на карту наносится тип карты: номер компоненты ключа защиты, символ «К» (для карты аутентификации Администратора UNIX/Linux Сервера – ПК «КриптоПро HSM»), символ «К2» (для карты аутентификации Пользователь/Администратор Windows сервера – ПК «КриптоПро HSM»). Кроме этого на карту записывается фамилия лица (пользователя - владельца), ответственного за данный ключевой носитель.

Надписи производятся разборчивым почерком (предпочтительно – печатными буквами), фломастером типа Staedtler Lumocolor permanent № 318 (с водостойким красителем).

4.2.3. Хранение ключевых носителей

Личные ключевые носители пользователей (с ключами доступа к ПАКМ) рекомендуется хранить в сейфе. Пользователь несет персональную ответственность за хранение личных ключевых носителей.

Администратор безопасности организации, эксплуатирующей СКЗИ, при централизованном хранении ключевых носителей несет персональную ответственность за хранение личных ключевых носителей пользователей. Личные ключевые носители администратора безопасности должны храниться в его личном сейфе.

Не допускается копирование ключевых носителей.

При использовании ПАКМ «КриптоПро HSM» ключи ЭП/закрытые ключи пользователей хранятся в зашифрованном виде внутри ПАКМ. Служба безопасности должна обеспечить ограничение доступа в помещение, в котором установлен ПАКМ.

4.2.4. Уничтожение ключей на ключевых носителях

Ключи на ключевых носителях – интеллектуальных картах, срок действия которых истек, уничтожаются путем переформатирования (очистки) с использованием ПО СКЗИ. Ключевые носители могут быть использованы в дальнейшем при условии записи на них новой ключевой информации.

Ключи ЭП/закрытые ключи, хранящиеся внутри ПАКМ, уничтожаются пользователями с использованием штатных средств ПО «КриптоПро HSM Client».

4.3. Ключи и сертификаты субъектов ПАКМ

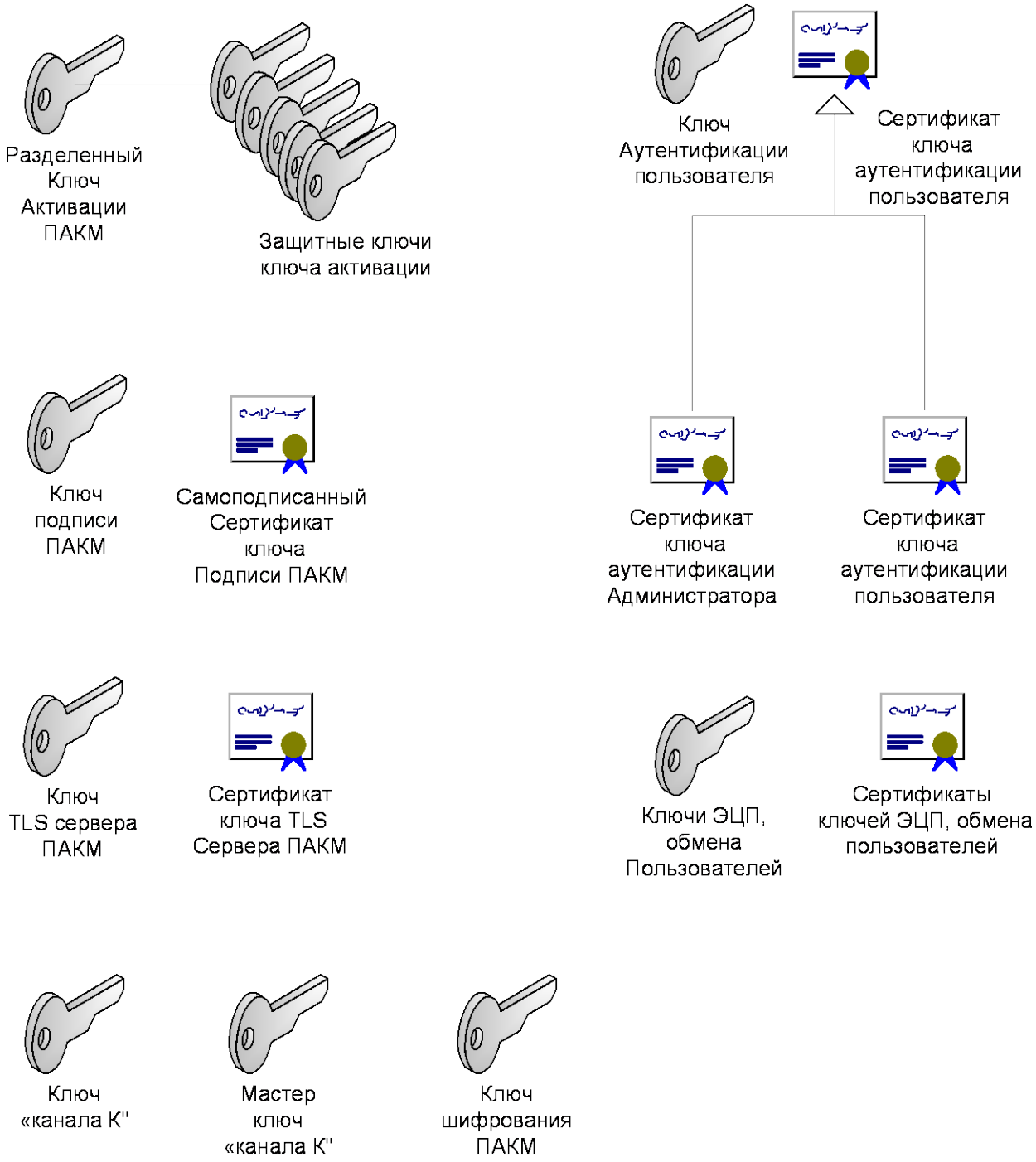


Рисунок 7. Ключи и сертификаты субъектов ПАКМ

В общем случае, по функциональному назначению ключевая информация предназначена для:

- формирования электронной подписи и ее проверки (далее, ключи подписи);

- аутентификации субъектов при доступе к сервисам (далее, ключи аутентификации, доступа, обмена);
- шифрования каналов передачи информации и самих симметричных ключей шифрования при экспорте, обмене (далее, ключи шифрования).

В ПАКМ «КриптоПро HSM» действует контроль сроков действия ключей. При превышении срока действия ключа операции подписи и шифрования на нем будут блокированы. При превышении срока действия служебных (внутренних) ключей ПАКМ, он может стать нефункциональным.

При превышении срока действия ключа в журнале событий отображается следующая информация:

cryptsrv_hsm[41244]: <cpcsp>[0x66973adf6700]SetupAndCheckKeyTimeValidity Key expired: signing will be forbidden

cryptsrv_hsm[41244]: <cpcsp>[0x66973adf6700]SetupAndCheckKeyTimeValidity Key expired: encryption will be forbidden

Максимальные сроки действия ключей перечислены в Формуляре на ПАКМ «КриптоПро HSM».

4.3.1. Ключ активации ПАКМ, защитные ключи

Ключ активации ПАКМ создается в момент инициализации ПАКМ и защищается с использованием разделенных секретов по схеме «3-и из 5-ти». Периодичность смены ключа активации определяется уровнем безопасности, которому соответствует ПАКМ.

Срок действия ключа: рекомендуется 3 месяца, но не более чем 1 год и 3 месяца.

На данном ключе защищаются ключи шифрования ПАКМ.

Также может производиться внеплановая смена ключа активации (увольнение сотрудников, владеющих защитными ключами, порча, утеря носителей защитных ключей и т.п.).

Ключ хранится в разделенном на 5 частей виде на 5-ти смарт-картах. Для активации ключа необходимо ввести любые три части.

Каждая часть (смарт-карта) защищена pin-кодом из 8-и цифр.

Части ключа активации распределяются между работниками службы безопасности организации.

Без активирования данного ключа невозможно привести ПАКМ в состояние, способное обслуживать запросы пользователей по сети. Невозможно расшифровать ключи пользователей системы.

При помощи данного ключа можно получить доступ к меню управления ПАКМ на LCD панели.

Ключ активации является основным ключом ПАКМ, обеспечивающим безопасность при доступе к ПАКМ.

В случае компрометации ключевой информации хотя бы с одного носителя, необходимо перевыпустить все 5 (n) ключей.

При смене ключа активации все ключи шифрования ПАКМ перешифровываются на новом ключе активации ПАКМ.

С точки зрения ролевой модели доступа к функциям ПАКМ данным ключом владеет **Суперпользователь ПАКМ**.

4.3.2. Ключ подписи ПАКМ

Ключ подписи ПАКМ создается в момент инициализации ПАКМ и защищается на ключе шифрования ПАКМ.

Срок действия ключа: периодичность смены ключа подписи определяется уровнем безопасности, которому соответствует ПАКМ. При создании ключа автоматически создается самоподписанный сертификат.

Ключ подписи ПАКМ служит для издания сертификатов ключей аутентификации пользователей ПАКМ.

4.3.3. Самоподписанный сертификат ключа подписи ПАКМ

Самоподписанный сертификат ключа подписи ПАКМ создается всякий раз в момент создания/плановой смены ключа подписи ПАКМ.

Срок действия ключа: Периодичность смены ключа подписи определяется уровнем безопасности, которому соответствует ПАКМ. При создании ключа автоматически создается самоподписанный сертификат.

Самоподписанные сертификаты ПАКМ сохраняются в хранилище корневых доверенных сертификатов ПАКМ (хранилище root).

Самоподписанный сертификат ключа подписи ПАКМ помещается в специальное расширение контейнера ключа аутентификации пользователя всякий раз при его (ключа аутентификации пользователя) генерации и может быть извлечен из этого контейнера при помощи ПО «КриптоПро HSM Client».

Самоподписанные сертификаты могут быть извлечены из ПАКМ при помощи web-интерфейса администратора ПАКМ.

Содержание отдельных полей самоподписанного сертификата формируется следующим образом:

Издатель сертификата: CN=<Серийный номер ПАКМ>.

Владелец сертификата: CN=<Серийный номер ПАКМ>.

Срок действия: 10 лет.

Основные ограничения: Центр Сертификации

Назначение ключа: Подпись сертификатов, шифрование ключей

4.3.4. Ключ шифрования ПАКМ

Ключ шифрования ПАКМ формируется при инициализации ПАКМ. На ключе шифрования ПАКМ шифруются все закрытые ключи/ключи ЭП пользователей, хранимые в долговременной памяти ПАКМ, ключ TLS сервера ПАКМ (ключ канала К2), мастер ключ «канала «К»» и ключ подписи ПАКМ.

Срок действия ключа: рекомендуется 3 месяца, но не более чем 1 год и 3 месяца.

Ключ шифрования ПАКМ зашифровывается на ключе активации ПАКМ и хранится на диске в ПАКМ. В случае смены ключа активации ПАКМ меняется и ключ шифрования ПАКМ. При этом ранее действующий ключ шифрования ПАКМ перешифровывается на новом ключе активации ПАКМ.

При смене ключа шифрования ПАКМ все вновь создаваемые ключи будут шифроваться на новом ключе шифрования ПАКМ. Старые ключи, как и ранее, будут зашифрованы на ключе шифрования ПАКМ, который был текущим в момент их создания.

4.3.5. Сессионный ключ канала «К2»

Сессионный ключ канала «К2» (ключ шифрования) служит для защиты (шифрования) передаваемых данных по каналу «К2».

Срок действия ключа: сессионный ключ канала К2 вырабатывается всякий раз при процедуре аутентификации пользователя с использованием TLS протокола, а также через заданные промежутки времени (1 час).

Сессионный ключ канала «К2» вырабатывается в процессе установления TLS сессии (на основе ключей и сертификатов аутентификации обычного пользователя и администратора сервера).

4.3.6. Ключ TLS сервера

Ключ TLS сервера (пара открытый и закрытый ключи аутентификации, обмена) ПАКМ создается в момент инициализации ПАКМ, после создания ключей активации и подписи ПАКМ.

Срок действия ключа: ключ TLS сервера подлежит плановой смене 1 раз в год.

Предназначен для поддержки TLS протокола со стороны сервера при организации канала «К2», а также при удаленном HTTPS доступе администратора ПАКМ к функциям управления ПАКМ.

Ключи хранятся на диске в ПАКМ.

Закрытый ключ TLS сервера шифруется ключом шифрования ПАКМ.

Ключ TLS сервера подлежит плановой смене 1 раз в год.

4.3.7. Сертификат ключа TLS сервера

Сертификат ключа TLS сервера создается в момент генерации ключа TLS сервера и подписывается ключом подписи ПАКМ. Таким образом, смена ключа TLS сервера ПАКМ может происходить только при активированном ПАКМ.

Срок действия: 1 год и 3 месяца.

Содержание отдельных полей сертификата TLS сервера формируется следующим образом:

Издатель сертификата: CN=<Серийный номер ПАКМ>.

Владелец сертификата: CN=<IP адрес сетевого интерфейса ПАКМ>.

Срок действия: 1 год и 3 месяца.

EKU: 1.3.6.1.5.5.7.3.1 «Проверка подлинности сервера»

При наличии в ПАКМ трех рабочих сетевых интерфейсов, у каждого из которых свой IP адрес, формируется три различных сертификата со значениями CN (commonName), соответствующими данным IP адресам.

4.3.8. Ключ аутентификации пользователя

Ключ аутентификации пользователя (открытый и закрытый ключи аутентификации, обмена) формируется при регистрации нового пользователя, а также при плановой/внеплановой смене ключа.

Срок действия ключа: ключ подлежит плановой смене 1 раз в год.

Предназначен для поддержки TLS протокола со стороны клиента при организации канала «К2», а также при удаленном HTTPS доступе привилегированных пользователей ПАКМ к функциям управления ПАКМ.

Ключ записывается на отчуждаемый ключевой носитель (смарт-карту, дискету, USB токен) и используется на рабочем месте пользователя.

4.3.9. Сертификат ключа аутентификации пользователя

Сертификат ключа аутентификации пользователя создается в момент генерации ключа аутентификации пользователя и подписывается ключом Подписи ПАКМ. Таким образом, генерация/смена ключа аутентификации пользователя может происходить только при активированном ПАКМ.

Содержание отдельных полей сертификата TLS сервера формируется следующим образом:

Издатель сертификата: CN=<Серийный номер ПАКМ>.

Владелец сертификата: CN=<Номер пользователя ПАКМ>.<Номер группы ПАКМ>.

Срок действия: 1 год и 3 месяца.

EKU: 1.3.6.1.5.5.7.3.2 «Проверка подлинности клиента»

Дополнительное имя субъекта:

Другое имя:

Имя участника=<Номер пользователя ПАКМ>.<Номер группы ПАКМ>@<Серийный номер ПАКМ>

Сертификат ключа аутентификации пользователя в поле EKU содержит стандартное расширение «Проверка подлинности клиента».

Если пользователем является Администратор сервера, то в EKU заносится дополнительное расширение

«1.2.643.2.2.34.22» – Пользователь – Администратор Сервера;

Данное расширение позволяет организовать доступ серверам приложений, не имеющим консоли для интерактивного обмена с пользователем, к криптографическим функциям ПАКМ. При этом сообщения и запросы на ввод pin-кодов выдаются на LCD панели ПАКМ.

Сертификат хранится в контейнере ключа аутентификации на отчуждаемом носителе, а также в профиле учетной записи пользователя в БД пользователей ПАКМ.

Контейнеры с таким ключом обмена и сертификатом Администратора сервера должны иметь фиксированный pin-код – восемь единиц. Pin-код для доступа к данному контейнеру на карте не запрашивается. Это обуславливает требование, что сервер должен находиться в контролируемой зоне со строго регламентированным доступом в эту зону привилегированных пользователей.

4.3.10. Сертификат ключа аутентификации Администратора

Сертификат ключа аутентификации привилегированного пользователя ПАКМ – члена группы Администраторов ПАКМ (Администратора, Аудитора, Администратора резервного копирования ПАКМ) == сертификат ключа аутентификации пользователя с дополнительными объектными идентификаторами (OID) в поле EKU сертификата.

Срок действия: 1 год и 3 месяца.

«1.2.643.2.2.34.21» – Администратор ПАКМ;

«1.2.643.2.2.34.28» – Аудитор ПАКМ;

«1.2.643.2.2.34.27» - Администратор резервного копирования ПАКМ;

Наличие данного EKU в сертификате дает право на выполнение Административных функций, как с LCD панели, так и с использованием удаленного доступа по HTTPS протоколу.

Сертификат хранится в контейнере ключа аутентификации на отчуждаемом носителе, а также в профиле учетной записи пользователя в БД пользователей ПАКМ.

4.3.11. Ключи канала «К»

Взаимодействие серверных приложений, базирующихся на ОС семейства Unix/Linux, с ПАКМ, характеризующихся тем, что они исполняются в фоновом режиме при отсутствии возможности выдачи окон на экран монитора (например, окно-запрос на ввод pin-кода), осуществляется по защищенному каналу – каналу К. Шифрование трафика в канале «К» обеспечивается использованием набора ассиметричных и симметричных ключей. Серверная часть (ПАКМ) использует ключ обмена, так называемый мастер ключ канала «К». Связанные с ним ключи обмена для клиентских частей (серверов приложений) записываются на одну или более (по количеству физических серверов) смарт-карт – карт канала «К». В процессе работы между конкретным сервером и ПАКМ вырабатывается симметричный ключ – ключ шифрования канала «К».

Карты канала «К» не имеют pin-кода.

Срок действия: ключ шифрования меняется каждый час автоматически. Мастер ключ и ключи канала «К» подлежат смене один раз в год.

На ключи канала «К» сертификаты не издаются.

4.4. Компрометация ключей

Определение термина **Компрометация**, виды компрометации и основные события, приводящие к компрометации, приведены в разделе 2.

По факту компрометации ключей должно быть проведено служебное расследование.

Выведенные из действия, скомпрометированные ключевые носители после проведения служебного расследования уничтожаются, о чем делается запись в «Журнал пользователя сети».

4.5. Совместный доступ различных пользователей ПАКМ к общим ключам

Изначально каждый пользователь ПАКМ «КриптоПро HSM» получает свой раздел в ПАКМ для безопасного хранения там своих криптографических ключей. И никакие другие пользователи ПАКМ не могут получить доступ к этому разделу, не имея соответствующего ключа доступа. Но в некоторых случаях требуется иметь разделяемые среди некоторой группы пользователей ключи. Часто это используется в высокопроизводительных системах, когда несколько серверов приложений (физически разных компьютеров) выполняют одну и ту же задачу и используют для этого одни и те же криптографические ключи, хранимые в ПАКМ. Каждому серверу приложения необходим свой ключ доступа, свой сертификат ключа доступа (чтобы можно было авторизовать исполнителя той или иной конкретной операции). Для этого было введено понятие группы пользователей ПАКМ.

Для создания группы никаких особых действий производить не нужно. Изначально создается обычный пользователь ПАКМ, которому присваивается номер пользователя (UID) и равный ему номер группы пользователя (GID). Данный пользователь получает отдельный раздел в ПАКМ для хранения своих ключей в виде каталога «GID.GID» (что равнозначно «UID.GID»). Теперь, если данному пользователю необходим ещё один ключ и сертификат доступа (например, для одновременного доступа к ключам с другого компьютера), или, если необходимо дать доступ другому пользователю к этому же разделу, то создается ещё один пользователь ПАКМ с уникальным номером (UID), но его номер группы совпадает с номером группы первого пользователя. В результате оба пользователя ПАКМ будут разделять один и тот же раздел ПАКМ «GID.GID».

Количество членов группы не ограничено.

Следует особо отметить, что привилегированные пользователи не могут содержать группу, равно как и быть членом группы. Член какой-либо группы (у которого UID != GID), не может содержать группу (т.е. у него нет своего раздела «UID.GID», который он мог бы разделить с другими пользователями ПАКМ).

При удалении пользователя - члена группы, удаляется только его профиль, а раздел с ключами остается. При удалении пользователя, содержащего группу

(UID==GID), удаляется раздел с ключами, профиль данного пользователя и профили всех пользователей – членов группы.

Номер пользователя (UID) и номер группы заносится в сертификат ключа доступа к ПАКМ, по которому производится идентификация, аутентификация пользователя и идентификация ключевого раздела ПАКМ.

4.6. Состояния ПАКМ

ПАКМ «КриптоПро HSM» может находиться в различных состояниях, характеризующихся отсутствием/наличием удаленного доступа к криптографическим функциям (по каналу «К» и каналу «К2») 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.

  - Сервис канала «К» и канала «К2» не запущен.

  - Web-интерфейс администрирования не отвечает.

- HSM-STATE-FULLACTIVE

  ПАКМ активен.

  - Ключ «3 из 5» и ключи шифрования активированы.

  - Канал «К» и канал «К2» обрабатывают все запросы пользователей.

  - Web-интерфейс может быть использован для администрирования.

- HSM-STATE-ACTIVE-ADMIN-ONLY

  ПАКМ активен.

  - Ключ «3 из 5» и ключи шифрования активированы.

  - Канал «К» и канал «К2» не работают.

  - Web-интерфейс может быть использован для администрирования.

- 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-и из 5-ти») – 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).

4.7. ПО ПАКМ

ПО ПАКМ включает:

- сервисы (демоны), реализующие различные внешние интерфейсы доступа к ПАКМ;
- библиотеки и модули, реализующие криптографические функции;
- библиотеки и модули обработки команд с LCD панели, от Web-интерфейса администратора ПАКМ;
- Web-сервис, обеспечивающий удаленное администрирование ПАКМ по HTTPS протоколу, с необходимыми библиотеками, модулями, HTML страницами;
- библиотеки и сервисы поддержки каналов «К» и «К2», процедур идентификации и аутентификации;
- библиотеки и сервисы издания сертификатов ключей аутентификации пользователей и сервисов ПАКМ.

ПАКМ может находиться в «выключенном», «неактивном», «активном», «активном только для администратора» состоянии.

В активном состоянии ПАКМ может обслуживать запросы пользователей по сети, включая и запросы с удаленного рабочего места администратора ПАКМ.

В неактивном состоянии ПАКМ может обслуживать только запросы привилегированных пользователей с LCD панели.

В активном «только для администрирования» состоянии ПАКМ может обслуживать только запросы привилегированных пользователей с LCD панели и с удаленного АРМ Администрирования ПАКМ.

В «выключенном» состоянии все процессы, включая ОС, выгружены из памяти ПАКМ.

При загрузке ПАКМ он переходит в неактивный режим.

Для перевода ПАКМ в активное состояние необходимо активировать специальный разделенный по схеме «3 из 5» ключ активации ПАКМ.

4.8. 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.

Обращение к функциям управления ПАКМ с удаленного рабочего места администратора осуществляется по стандартному HTTPS протоколу через 443 порт. В качестве клиентской части должен использоваться Microsoft Internet Explorer версии не ниже 5.5/Microsoft Edge.

На компьютер рабочего места администратора с установленной ОС семейства Windows[1] устанавливается СКЗИ «КриптоПро CSP» (включено в дистрибутив ПО ПАКМ), свободно распространяемый программный компонент MS CAPICOM 2.0 (включено в дистрибутив ПО ПАКМ) в соответствии с руководствами по их установке. Компьютер должен быть оснащен считывателем смарт-карт.

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 напрямую соединяться с сетевым интерфейсом компьютера администратора.

Обращение к ПАКМ осуществляется по IP адресу ПАКМ в сети, например, таким образом:

https://192.168.26.2

При этом в браузере Internet Explorer/Edge отображается страница Рабочего места администратора ПАКМ, производится автоматическая инсталляция необходимых компонент. При первом подключении в Internet Exporer/Edge временно должны быть сняты ограничения системы безопасности, не позволяющие установку активного содержимого (ActiveX компонент).

---

[1] В новых ОС Windows для генерации ключей доступа пользователей вместо компонента Microsoft XEnroll.dll используется новый компонент Microsoft CertEnroll.dll. В настоящий момент при обращении к ПАКМ просто по IP адресу без указания имени страницы по умолчанию загружается страница, использующая CertEnroll. Если на АРМ Администратора установлена более старая ОС, то необходимо указывать имя загружаемой страницы явно, например https://192.168.26.2/default.htm.

Для работы с web-интерфейсом администрирования необходимо, чтобы в настройках ПАКМ была установлена опция «Enable WEB», а сам ПАКМ находился в состоянии либо «активном», либо «активном только для администрирования».

Доступ к ПАКМ осуществляется по стандартному 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. Кроме этого на компьютер администратора должен быть установлен самоподписанный сертификат ключа подписи ПАКМ. Данный сертификат и сертификат администратора могут быть извлечены из смарт-карты администратора при помощи специальной утилиты cardman (входит в дистрибутив ПАКМ), после чего самоподписанный сертификат должен быть установлен в хранилище корневых доверенных центров сертификации пользователя при помощи штатных средств ОС Windows, а сертификат администратора должен быть установлен в личное хранилище пользователя средствами «КриптоПро CSP».

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.

Канал Web администрирования использует порт для входящих соединений ПАКМ – 443.

4.9. Журнал аудита ПАКМ

При заполнении памяти отведенной под данные журнала аудита эта память должна быть очищена. Очистка журнала аудита производится либо по распоряжению Суперпользователя ПАКМ, либо по распоряжению Аудитора ПАКМ с подтверждением действия Администратором ПАКМ, либо автоматически (настраивается Аудитором ПАКМ).

Для автоматической очистки журнала аудита издается специальное распоряжение Аудитора ПАКМ (включаемое в настройки ПАКМ), в котором указывается максимальное количество записей, при достижении которого часть журнала аудита должна быть очищена.

Для использования автоматической очистки журнала аудита ПАКМ в конфигурации ПАКМ должна быть установлена соответствующая опция. Если опция не установлена, то при переполнении журнала аудита (достижении указанного максимального количества записей) работа обычных пользователей с ПАКМ блокируется.

Ручная очистка журнала возможна только с LCD панели, так как её может выполнить только Суперпользователь ПАКМ или Аудитор совместно с Администратором ПАКМ.

Для долговременного хранения данных журнала аудита используется режим выгрузки журнала аудита из ПАКМ.

Журналы аудита в текстовом виде переписываются на рабочую станцию Администраторов ПАКМ при помощи web-интерфейса администратора ПАКМ с использованием защищенного протокола TLS. При этом журналы не уничтожаются, остаются в ПАКМ. Подобный просмотр журналов доступен любому из привилегированных пользователей. Для долговременного хранения извлеченных из ПАКМ журналов привилегированный пользователь должен подписать их, используя свой ключ и сертификат ключа доступа к ПАКМ, при помощи утилиты cryptcp, входящей в состав дистрибутива сертифицированного СКЗИ «КриптоПро CSP», устанавливаемого на рабочей станции удаленного администрирования ПАКМ.

Журнал аудита может служить также для сбора статистической информации для каждого пользователя, а по некоторым типам событий для конкретной пары открытого/закрытого ключа. Для этого каждая запись журнала имеет ключ, уникально идентифицирующий её среди других записей журнала аудита, чтобы избежать возможного дублирования информации при выгрузке данных и их последующей обработке.

Привилегированный пользователь ПАКМ может просмотреть/выгрузить журнал аудита с использованием web-интерфейса администрирования. При просмотре журнала имеется возможность указать различные условия поиска требуемых записей, включая интервал дат времени события, статус завершения события, идентификатор пользователя, инициировавшего событие.

При выгрузке журнала имеется возможность указать дату и время начала временного интервала (конец интервала – текущее время), за который необходимо выгрузить записи журнала.

4.9.1. База данных и структура записи журнала аудита ПАКМ

Журнал аудита ведется в ПАКМ в виде базы данных (sqlite см. www.sqlite.org). Для оптимальной работы в настройки ПАКМ вынесен ряд параметров, регулирующих работу с ней.

ПАКМ предоставляет возможность настроить режим синхронизации страниц БД, в КЭШе с диском (pragma Synchronous), влияющий на производительность ПАКМ и надежность (выше надежность, меньше производительность, и наоборот). Не стоит без необходимости (требование производительности ПАКМ - более 10 операций подписи в секунду, отражаемых в журнале аудита) изменять данный параметр на значения, уменьшающие надежность (NORMAL, OFF). При установке журналирования операций электронной подписи пользователями и использовании значения OFF данного параметра ПАКМ способен обрабатывать до 3000 запросов на ЭП в секунду. Но при этом необходимо позаботиться о бесперебойном электропитании ПАКМ. В случае внезапного отключения ПАКМ данные журнала аудита могут быть разрушены. Если такое произошло, то в LCD меню ПАКМ предусмотрен специальный режим восстановления БД журнала аудита (Repair Audit log), который доступен только Суперпользователю ПАКМ.

Объем БД журнала аудита ограничен используемой флэш-памятью ПАКМ. Как минимум, ПАКМ позволяет хранить до 1 Гб данных журнала аудита, что позволяет накапливать данные, например, записи о событиях формирования ЭП, в течение суток, исходя из производительности ПАКМ – 100 операций типа SignHash в секунду.

БД журнала аудита оптимизирована на добавление новых записей. Поиск записей, просмотр БД журнала аудита с использованием web-интерфейса администратора может быть затруднен из-за большого объема БД. При этом, например, операция поиска в БД, блокирует БД на запись на время, в течение которого эта операция осуществляется, и заставляет процессы, пишущие в БД, ожидать. Таймаут времени ожидания при блокировке БД составляет 1 мин., после чего операции, которым не удалось дождаться своей очереди на запись в БД журнала аудита, завершаются с кодом ошибки. Поэтому рекомендуется периодически выгружать данные журнала аудита, и очищать БД. Для обработки больших объемов данных журнала аудита рекомендуется использовать промышленные системы управления базами данных (СУБД).

Журнал аудита ПАКМ может очищаться автоматически. Для этого в настройках ПАКМ нужно установить специальный флаг, указать максимально допустимое количество записей в БД, после превышения которого должна запуститься процедура очистки, а также интервал времени, через который осуществлять проверку на превышение этого количества. Рекомендуется использовать следующие данные для расчета этих параметров:

- максимальный объём данных, желательно не превышать 1Гб;
- усредненный размер записи ~ 120 байт.

Процедура очистки БД журнала аудита сводится к удалению записей журнала. При этом сначала удаляемые страницы с записями переписываются в журнал транзакции, после чего удаляются записи, и при успешном завершении удаляется журнал транзакции. При большом объеме данных данная процедура может занимать значительное время и

дополнительное место на флэш-памяти под журнал транзакции, БД при этом блокируется на время исполнения операции. Поэтому при очистке используется порционное удаление данных журнала. Записи удаляются большими порциями в цикле. Размер удаляемой порции за один запрос в цикле регулируется специальным параметром, вынесенным в настройки ПАКМ. Не рекомендуется использовать слишком большое и слишком малое значение этого параметра. В одном случае БД будет блокироваться на слишком большие промежутки времени, в другом – очистка может не успевать за наполнением БД. Рекомендуемые значения количества записей в порции – от 10 000 до 100 000 записей.

Перечень событий, отражаемых в журнале аудита ПАКМ, может быть настроен аудитором ПАКМ, как с LCD панели, так и с использованием web-интерфейса администратора ПАКМ. При этом все события различаются и по статусу их завершения, т.е. можно указать, что некоторое событие должно отражаться в журнале только при успешном завершении, или наоборот, или вообще не отражаться.

Выгрузка данных журнала аудита может быть осуществлена только с использованием web-интерфейса администрирования.

Выгружаемые из ПАКМ данные представляются в текстовом формате. Каждая строка представляет собой отдельную запись журнала. Поля записи разделяются символом TAB (табуляция). Строки разделяются символом LF – перевод строки.

Структура записи содержит следующие поля:

ID - внутренний (числовой) идентификатор отдельной записи журнала аудита, уникален в пределах существования порции журнала аудита от одного момента восстановления БД журнала аудита до другого, т.е. при обычной очистке журнала нумерация записей продолжается, а после выполнения операции восстановления БД начинается с единицы.

HSMID – идентификатор (серийный номер) ПАКМ;

UserID – идентификатор (номер) пользователя в данном ПАКМ, автор события;

EventTime – дата и время события;

EventStatus – статус завершения события (0 – успех, 1 – неудача);

EventType - тип события;

StringData – дополнительные строковые данные журналируемого события (идентификатор контейнера/ключа на котором производилась криптографическая операция события, количество зашифрованных/расшифрованных данных, и т.п.);

BinaryData – дополнительные двоичные данные - результат выполнения криптографической операции (значение ЭП, значение сформированного открытого ключа).

Поле UserID – автор события обычно содержит внутренний номер (UID) зарегистрированного пользователя ПАКМ. В том случае, если пользователя еще не удалось идентифицировать (событие неудачного подключения пользователя), то запись в журнал аудита попадает с кодом UserID = -2.

Запись событий автоматическим процессом очистки журнала аудита, процессом начальной инициализации ПАКМ (когда еще нет ни одного зарегистрированного пользователя) осуществляется со значением поля UserID = 0.

В целях минимизации объема памяти, занимаемой журналом аудита, поле BinaryData заполняется только в событиях, связанных с генерацией пользователями ключевых пар (заносится значение открытого ключа) и формированием ЭП (заносится значение ЭП).

Поле StringData заполняется только в событиях формирования пользователями ПАКМ ключевых пар (заносится идентификатор формируемого ключевого контейнера), генерации пользователями ЭП (заносится идентификатор используемого ключевого контейнера), шифрования и расшифрования данных (заносится количество зашифрованных/расшифрованных байт), создания, удаления, модификации информации о пользователе (заносится идентификатор пользователя, данные о котором изменялись, в виде <UID>.<GID>@<HSMID>).

Поле EventTime содержит дату и время возникновения события. Значение данного поля представляется в формате строки generalizedTime с точностью до 6 знаков после точки, т.е. в формате YYMMDDHHNNSS[.X[X[X[X[X[X]]]]]]Z.

4.9.2. Типы журналируемых событий ПАКМ

Тип события имеет цифровой и символьный код. Различают следующие типы событий журнала аудита:

EVENT_TYPE_UNDEFINED (-1) - тип события не определен;

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

EVENT_TYPE_AUTH_USER_REMOTE (2) - попытка подключения по удаленному (каналы К и К2, web-интерфейс администрирования) интерфейсу ПАКМ (только неуспешная аутентификация пользователя);

EVENT_TYPE_CHANGE_HSM_STATE (3) - изменение состояния ПАКМ;

EVENT_TYPE_ADD_USER (4) - регистрация нового пользователя ПАКМ;

EVENT_TYPE_MODIFY_USER (5) - изменение информации о пользователе ПАКМ;

EVENT_TYPE_DELETE_USER (6) - удаление информации о пользователе ПАКМ;

EVENT_TYPE_CHANGE_USER_TOKEN (7) - изменение аутентификационной информации пользователя (генерация нового сертификата);

EVENT_TYPE_CHANGE_USER_STATE (8) - блокирование/разблокирование пользователя ПАКМ;

EVENT_TYPE_CLEAR_AUDIT_LOG (9) - очистка журнала аудита;

EVENT_TYPE_DOWNLOAD_AUDIT_LOG (10) - выгрузка журнала аудита;

EVENT_TYPE_CHANGE_SYSTEM_TIME (11) - изменение системного времени ПАКМ;

EVENT_TYPE_CHANGE_HSM_OPTIONS (12) - изменение настроек ПАКМ;

EVENT_TYPE_CHANGE_NETWORK_SETTINGS (13) - изменение сетевых настроек ПАКМ;

EVENT_TYPE_FW_ADD_SUBNET (14) - добавление клиентской подсети в настройки межсетевого экрана;

EVENT_TYPE_FW_DELETE_SUBNET (15) - удаление клиентской подсети из настроек межсетевого экрана;

EVENT_TYPE_FW_MODIFY_SUBNET (16) - изменение адресов клиентской подсети в настройках межсетевого экрана;

EVENT_TYPE_FW_RESTART (17) - перезапуск сервиса межсетевого экрана ПАКМ;

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

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

EVENT_TYPE_CHANGE_USERENCRYPTION_KEY (20) - смена ключа активации ПАКМ (ключа «3-и из 5-ти»);

EVENT_TYPE_LOAD_GAMMA (21) - загрузка ключевого материала уполномоченной организации;

EVENT_TYPE_CRYPT_GENKEY (22) - генерация ключа пользователем;

EVENT_TYPE_CRYPT_SIGNHASH (23) - формирование ЭП пользователем ПАКМ;

EVENT_TYPE_CRYPT_VERIFYSIGNATURE (24) - проверка ЭП пользователем ПАКМ;

EVENT_TYPE_CRYPT_ENCRYPT (25) - шифрование блока данных пользователем;

EVENT_TYPE_CRYPT_DECRYPT (26) - расшифрование блока данных пользователем;

EVENT_TYPE_OVERFILLING_AUDIT_LOG (27) – переполнение журнала аудита (журналируется со статусом - неудача);

EVENT_TYPE_REPAIR_AUDIT_LOG (28) – восстановление журнала аудита;

EVENT_TYPE_DELETE_KEY (29) – удаление ключа пользователя пользователем;

EVENT_TYPE_CRYPT_EXPORT_KEY (30) – экспорт закрытого ключа;

EVENT_TYPE_CRYPT_IMPORT_KEY (31) – импорт закрытого ключа в контейнер ПАКМ;

EVENT_TYPE_CREATE_NEW_BACKUP (32) – создание резервной копии внутри ПАКМ;

EVENT_TYPE_DELETE_BACKUP (33) – удаление резервной копии внутри ПАКМ;

EVENT_TYPE_RESTORE_FROM_BACKUP (34) – восстановление из резервной копии ПАКМ;

EVENT_TYPE_DOWNLOAD_BACKUP (35) – выгрузка резервной копии;

EVENT_TYPE_CHANGE_AUDIT_OPTIONS (36) – изменение настроек аудита;

EVENT_TYPE_MEMORY_ERROR (37) – ошибки контроля оперативной (ECC) памяти ПАКМ.

EVENT_TYPE_UPLOAD_BACKUP (38) – выгрузка резервной копии;

4.10. Резервирование и восстановление ПАКМ

Для обеспечения надежности ПАКМ «КриптоПро HSM» имеет возможность резервирования ключевой информации и, при необходимости, её восстановления.

4.10.1. Холодное резервирование ПАКМ

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

Основной режим холодного резервирования – внутренний. Он подразумевает создание резервной копии состояния ПАКМ, включая настройки ПАКМ и текущее состояние всей ключевой системы, и сохранение её внутри ПАКМ на отдельном, специально предназначенном для хранения резервных копий, флэш-диске.

В случае порчи ключевой информации в основном разделе файловой системы ПАКМ, её можно попытаться восстановить из ранее созданной резервной копии. В случае порчи флэш-диска с основным разделом ПАКМ такой, что восстановление на этом диске невозможно, только этот флэш-диск можно заменить, после чего заново развернуть ПАКМ и восстановиться с резервной копии.

Если требуется ещё более надежное хранение ключа уполномоченного лица, например, в другом помещении или даже районе, имеется возможность выгрузки

резервной копии из ПАКМ и транспортировка её в нужное место для хранения. Обратную загрузку в ПАКМ такого файла резервной копии может выполнить привилегированный пользователь, которому назначена роль Администратора резервного копирования, через интерфейс удаленного рабочего места Администратора ПАКМ. При этом Администратором ПАКМ должен быть выставлен специальный параметр ПАКМ «Enable Upload» в значение, разрешающее производить такую загрузку файлов. В целях безопасности в обычном режиме функционирования ПАКМ данный параметр должен быть отключен. Таким образом можно изготовить резервный ПАКМ и в случае выхода из строя основного, быстро переключиться на резервный.

Загрузка файла резервной копии не означает восстановление. Данная операция только сохраняет файл с резервной копией в соответствующем разделе. Для восстановления ПАКМ из данной резервной копии используйте соответствующий режим LCD меню ПАКМ.

Резервную копию следует делать каждый раз при смене ключевой информации ПАКМ.

Для создания резервной копии предусмотрена роль - «Администратор резервного копирования». Чтобы получить доступ к его функциям, в сертификате ключа доступа к ПАКМ привилегированного пользователя должно присутствовать специальное расширение (см. п. 4.1).

Кроме того, что вся ключевая информация, хранящаяся в ПАКМ зашифрована в конечном итоге на разделенном на 5 частей ключе активации ПАКМ, и именно в таком виде она попадает в файл с резервной копией, получаемый файл резервной копии подписывается для контроля целостности и после этого ещё раз шифруется на уникальном для данной копии ключе, формируемом на смарт-карте. На соответствующий открытый ключ формируется самоподписанный сертификат ключа, изданный ПАКМ, и тоже помещается на карту. Данная смарт-карта формируется в момент создания резервной копии Администратором резервного копирования и должна храниться только у него.

Выгрузить файл резервной копии и/или запустить процедуру восстановления ПАКМ из резервной копии может только Администратор ПАКМ, но без ключа шифрования и подписи резервной копии (смарт-карты), хранящейся у Администратора резервного копирования, процедура восстановления невозможна. Таким образом, чтобы провести атаку с использованием резервной копии, необходим сговор, как минимуму двух привилегированных пользователей категории II (имеющих доступ в контролируемую зону). Кроме того, все подобные операции отражаются в журнале аудита ПАКМ, доступном для очистки только Суперпользователю ПАКМ.

Необходимо помнить, что восстановление с резервной копии не имеет смысла, если утеряны или неработоспособны, как минимум, 3 из 5 карт с защитными ключами ключа активации ПАКМ, действовавшего на момент создания резервной копии. Таким образом, после каждой успешной смены ключа активации ПАКМ, необходимо пересоздать резервную копию.

Если в резервировании информации нет необходимости, то в регламенте не должно быть предусмотрено роли «Администратора резервного копирования». Пользователь с такими привилегиями просто не должен создаваться.

4.10.2. Горячее резервирование ПАКМ

Данный режим резервирования может применяться в системах высокой степени доступности с часто меняющейся ключевой информацией пользователей ПАКМ.

Он требует наличия, как минимум, одного дополнительного ПАКМ «КриптоПро HSM» включенного в кластер с основным ПАКМ.

Горячее резервирование ПАКМ «КриптоПро HSM» подразумевает перенос новых и изменённых в основном ПАКМ данных в резервный ПАКМ в онлайн режиме. Фактически, изменения отображаются в резервном ПАКМ сразу после обновления данных в основном ПАКМ.

Это относится ко всем данным ПАКМ (информация о пользователях ПАКМ, ключи пользователей, служебные ключи ПАКМ, настройки ПАКМ), за исключением настроек сетевых интерфейсов, настроек горячего резервирования, ключа активации и ключей шифрования ПАКМ, хранилищ сертификатов служебных ключей ПАКМ.

Таким образом, можно говорить, что в момент отказа в работе основного ПАКМ, резервные ПАКМ будут содержать информацию максимально близкую к информации основного ПАКМ на момент отказа. Для восстановления работы системы необходимо лишь переключить «клиента HSM» на резервный ПАКМ.

Механизм горячего резервирования основывается на механизмах репликации баз данных. При этом основной ПАКМ «КриптоПро HSM» называется MASTER сервером репликации, а ПАКМ-ы горячего резерва называются SLAVE серверами.

SLAVE сервера отслеживают события изменения данных на MASTER сервере и при их обнаружении «забирают» и отображают все изменения у себя.

Между SLAVE и MASTER сервером создается шифрованный канал, аналогичный каналу «К2», т.е. все данные передаются при помощи протокола TLS с взаимной аутентификацией сторон при помощи сертификатов отрытых ключей обмена алгоритма ГОСТ Р 34.10-2012 (ГОСТ 34.10-2018).

Для организации этого канала используются закрытые ключи и сертификаты открытых ключей обмена TLS серверов, т.е. те же самые, которые используются для организации канала «К2» при взаимодействии с клиентами ПАКМ.

Т.к. эти ключи зашифрованы на ключах шифрования ПАКМ, которые в свою очередь зашифрованы на ключе активации ПАКМ, то механизм репликации может работать только после активации ПАКМ (в режимах ACTIVE или ADMIN_ONLY). При правильно настроенной репликации она автоматически запускается при входе в один из этих режимов и останавливается при переводе ПАКМ в неактивное (INACTIVE) состояние.

Изначально между двумя разными ПАКМ нет никакого доверия, сертификаты ключей TLS серверов неизвестны друг, т.к. изданы различными (каждый своим) ПАКМ-ами, что не позволяет установить доверенный канал между ними, даже для синхронизации данных. Поэтому для того, чтобы развернуть сервер горячего резервирования его необходимо клонировать с MASTER сервера ПАКМ, используя механизм холодного резервирования ПАКМ, описанный в предыдущей главе.

Сразу после создания резервной копии MASTER сервера, следует объявить его (настроить) MASTER сервером, создать правила фаервола, разрешающие подключение к нему SLAVE серверов через порт репликации (1504) с заданных ip адресов и, перестартовав сетевые сервисы, включить в работу (перевести в состояние ACTIVE). Удаленные пользователи уже могут начинать штатную работу.

На SLAVE серверах необходимо произвести инициализацию обычным способом. Временно настроить их таким образом, чтобы была возможность подключиться к ним по Web интерфейсу, дополнительно разрешив загрузку файлов резервных копий в них. Далее необходимо выгрузить файл резервной копии из MASTER сервера и загрузить его в SLAVE сервера, восстановить SLAVE сервера из данной резервной копии. В результате получим клоны MASTER сервера на момент создания его резервной копии, включая разделенный ключ активации MASTER сервера, ключевую систему привилегированных и обычных пользователей, сетевые настройки и настройки брэндмауэра. Данные настройки на SLAVE серверах необходимо изменить (как минимум IP адреса сетевых интерфейсов), после чего выполнить процедуру перегенерации ключа и сертификата сервера (TLS). В настройках репликации необходимо указать тип сервера (SLAVE), уникальный номер SLAVE сервера (от 1 до 9), IP адрес MASTER сервера.

Если всё сделано правильно, то после активации SLAVE серверов все изменения данных, произошедшие на MASTER сервере с момента создания на нём резервной копии, использовавшейся для клонирования, отобразятся на SLAVE серверах, а информация о состоянии репликации, отображаемая в Web интерфейсе, не будет содержать данных о возникшей ошибке.

Не следует без надобности использовать SLAVE сервера HSM для штатной работы с ними клиентов HSM. Изменения реплицируются только в одну сторону - с MASTER сервера на SLAVE сервера. Безответственное постоянное переключение клиентов с MASTER на SLAVE и обратно, в конечном итоге может привести к потере данных. SLAVE сервера должны использоваться только в качестве горячего резерва.

В случае необходимости SLAVE сервера можно останавливать, деактивировать, перегружать. Их можно использовать для периодического создания образов HSM в виде обычных резервных копий. Только необходимо помнить, что данные резервные копии будут содержать информацию и о типе сервера (SLAVE) и соответствующих настройках, и после восстановления ПАКМ из такой копии, возможно придется данные настройки сразу изменить.

После активации SLAVE серверов после простоя все изменения, произошедшие на MASTER сервере с момента остановки SLAVE сервера, автоматически будут реплицированы.

Объем накапливаемых изменений на MASTER сервере ограничен, поэтому не следует останавливать надолго SLAVE сервера. Чтобы не забивать дисковую память, файлы с накопленными изменениями на MASTER сервере автоматически будут удаляться через 3 суток после их ротации (смены на новый файл изменений).

Изменения, связанные со сменой ключа активации, ключа подписи ПАКМ, не реплицируются. Поэтому после проведения данных процедур необходимо заново пересобрать репликацию.

Количество используемых SLAVE серверов диктуется требованиями к надежности системы и бюджетом эксплуатирующей организации. В общем случае достаточно одного сервера горячего резерва. Необходимо иметь в виду, что отказ оборудования может наступить и на SLAVE сервере. И если используется только один SLAVE сервер, для ввода нового сервера горячего резерва придется заново пересобрать репликацию (если прошло более 3 суток с момента создания резервной копии на MASTER сервере).

В случае сбоя на MASTER сервере (например, отключения питания), его база данных может оказаться в разрушенном состоянии. Программное обеспечение ПАКМ будет пытаться осуществить максимально возможное восстановление данных. Но может оказаться так, что часть данных будет потеряна. В таком случае это может стать поводом для переключения работы клиентов HSM на один из резервных (SLAVE) серверов, равно как и отказ оборудования MASTER сервера.

Сразу после такого переключения следует остановить репликацию на SLAVE сервере и изменить его тип, сделав MASTER сервером. Быстрое переключение на резервный сервер дает возможность продолжить штатную работу клиентам ПАКМ. Если использовалось более одного SLAVE сервера, то оставшиеся сервера можно остановить.

Они становятся мало функциональными. Необходимо запланировать работы по настройке новой системы горячего резервирования. Для этого потребуется кратковременная остановка работы клиентов ПАКМ для создания на новом MASTER сервере резервной копии, которая будет использоваться для клонирования новых SLAVE серверов.

В настоящий момент ПАКМ не поддерживает автоматическое переключение с основного севера на резервный. С ПАКМ КриптоПро HSM может работать несколько устройств доступа (серверов, рабочих станций пользователей), которые ничего не знают друг о друге. Отказ какому-либо устройству в доступе к ПАКМ, не означает, что ПАКМ нефункционален и данному устройству следует переключаться на резервный ПАКМ. ПАКМ может быть просто перегружен в данный момент (превышение количества соединений и т.п.) и абсолютное большинство пользователей успешно работают с ним в данный момент.

Чтобы избежать потери данных, переключение на резервный ПАКМ «КриптоПро HSM» должно осуществляться синхронно для всех клиентов (устройств доступа) ПАКМ.

Работоспособность ПАКМ должна отслеживаться Администратором ПАКМ.

Для сетевого соединения между собой MASTER и SLAVE серверов в целях репликации следует использовать выделенные сетевые интерфейсы. При наличии только одного SLAVE сервера рекомендуется подключать сервера напрямую. При наличии нескольких SLAVE серверов следует использовать выделенный оптический коммутатор, используя при этом выделенный сегмент сети.

Настройки репликации (IP адрес MASTER сервера, типы и номера серверов репликации, а также настройки брэндмауэра, связанные с репликацией) выполняются привилегированным пользователем с правами Администратора ПАКМ. Репликацию невозможно создать без предварительной процедуры клонирования ПАКМ, а соответственно без участия привилегированного пользователя с правами «Администратора резервного копирования ПАКМ».

5. ОСНОВНЫЕ ТЕХНИЧЕСКИЕ ДАННЫЕ И ХАРАКТЕРИСТИКИ ПАКМ

ПАКМ — программно–аппаратный криптографический модуль, внешний программный интерфейс которого соответствует криптографическому интерфейсу «КриптоПро CSP» версия 4.0/5.0.

ПАКМ представляет собой средство криптографической защиты информации, удовлетворяющее классу КВ/КВ2 (Комплектация 1 Исполнение 1) или КС3 (Комплектация 1 Исполнения 2-5) (при выполнении требований эксплуатационной документации на ПАКМ).

Средствами ПАКМ «КриптоПро HSM» не допускается защищать информацию, составляющую государственную тайну.

ПАКМ обеспечивает одновременное обслуживание до 100 устройств доступа с возможностью формирования до 3000 подписей хэш-значений в секунду.

ПАКМ «КриптоПро HSM» обеспечивает хранение до 500000 ключевых контейнеров пользователей.

5.1. Операционные системы

Программные средства ПАКМ «КриптоПро HSM» функционируют на базе ОС Альт Линукс СПТ 7.0 с защитой ядра ОС средствами пакета GRSecurity.

ОС Альт Линукс СПТ 7.0 сертифицирована Федеральной службой по техническому и экспортному контролю (ФСТЭК России). Классификация по уровню контроля отсутствия недекларированных возможностей - 4 уровень. Показатели защищенности от несанкционированного доступа к информации - по 5 классу защищенности.

ПАКМ предназначен для использования с серверными приложениями, приложениями пользователей на базе операционных систем Unix/Linux и Windows, включая 64-разрядные их исполнения (список операционных систем приведен в документе «ЖТЯИ.00096-02 30 01. КриптоПро HSM. Формуляр»).

5.2. Функциональные схемы применения ПАКМ

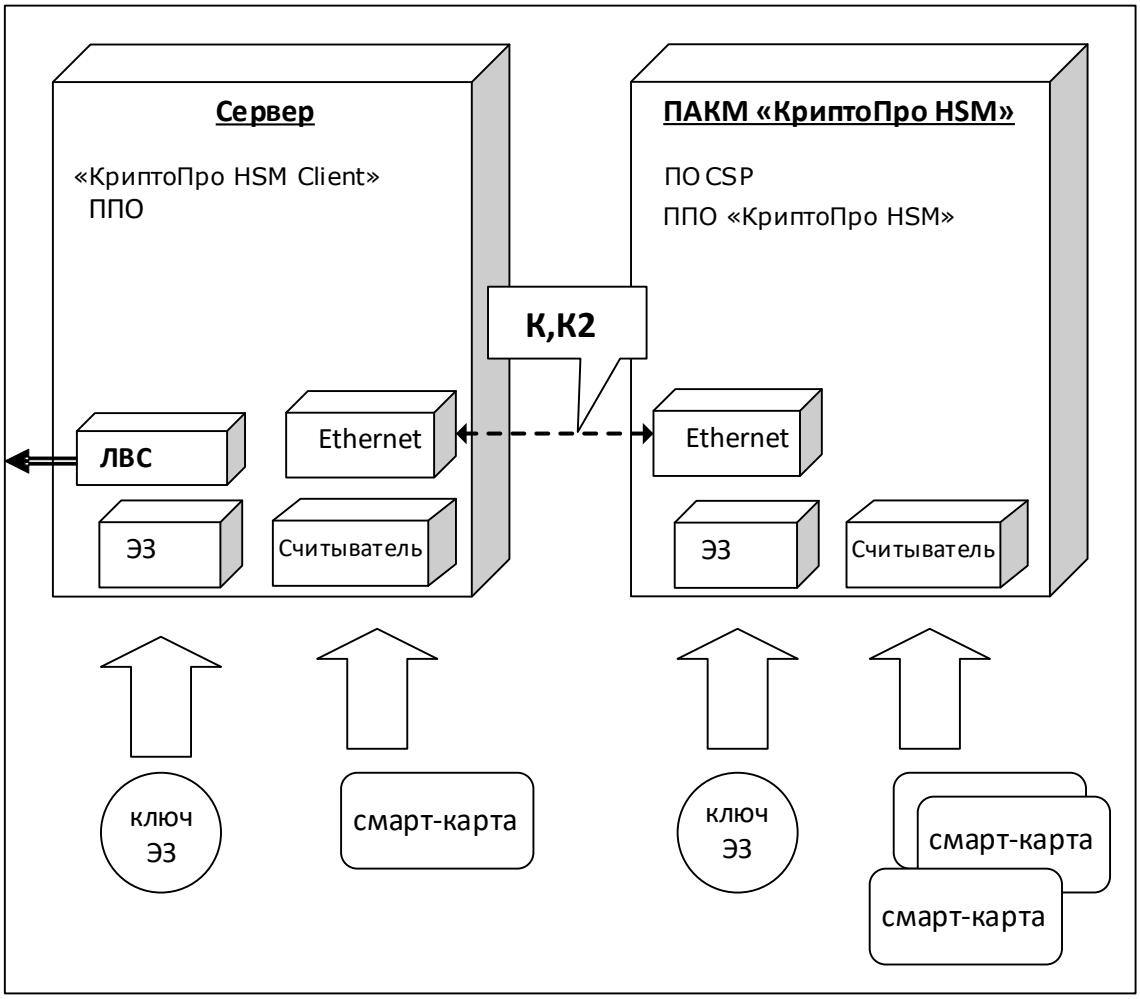


Рисунок 8. Функциональная схема применения ПАКМ «КриптоПро HSM» с сервером приложений.

В сервере используются программно-аппаратные средства:

- ПЭВМ с установленной ОС;
- CSP – реализует интерфейс криптографических функций для взаимодействия ПАКМ «КриптоПро HSM» с сервером в части обеспечения контроля целостности данных обмена между ними, шифрования информации в канале К, обеспечения протокола сетевой аутентификации;
- ППО – прикладное программное обеспечение сервера, взаимодействующее с ПО «КриптоПро HSM», а также с электронным замком и считывателем карт;
- ЭЗ – электронный замок;
- Ключи электронного замка;
- Считыватель смарт-карт;

- Смарт-карты – ключевые носители;
- ЛВС – интерфейс для взаимодействия по локальной сети с внешними абонентами пользователями функций СКЗИ;
- К – локальный защищенный канал (ЛЗК). Используется для серверов с установленной ОС семейства Unix/Linux;
- К2 – локальный защищенный канал, базирующийся на протоколе TLS. Используется для серверов с установленной ОС семейства Windows.

В ПАКМ «КриптоПро HSM» используются программно-аппаратные средства:

- ПЭВМ с установленной ОС ALT Linux Server 4.0 и тремя оптическими сетевыми платами;
- CSP – криптопровайдер типа "КриптоПро CSP";
- ППО «КриптоПро HSM» – прикладное программное обеспечение ПК «КриптоПро HSM» для взаимодействия с сервером, а также работы с электронным замком и считывателем карт;
- ЭЗ – электронный замок;
- Ключи электронного замка;
- Считыватель смарт-карт;
- Смарт-карты – ключевые носители.

Взаимодействие между ПАКМ «КриптоПро HSM» и сервером осуществляется по специально выделенному локальному защищенному каналу «К» (ЛЗК, реализуется отдельным сегментом Ethernet).

Субъектами, обеспечивающими функционирование ПАКМ «КриптоПро HSM», являются:

- владелец ключа ЭП, хранящегося в ПАКМ (например, уполномоченное лицо УЦ);
- привилегированные пользователи ПАКМ «КриптоПро HSM» (администратор ПАКМ, аудитор ПАКМ, администратор резервного копирования ПАКМ);
- группа доверенных лиц (для обеспечения хранения и ввода ключа активации в разделенном виде);
- администратор ППО сервера;
- администратор безопасности сервера.

Примерная схема подключения ПАКМ к серверу изображена ниже.

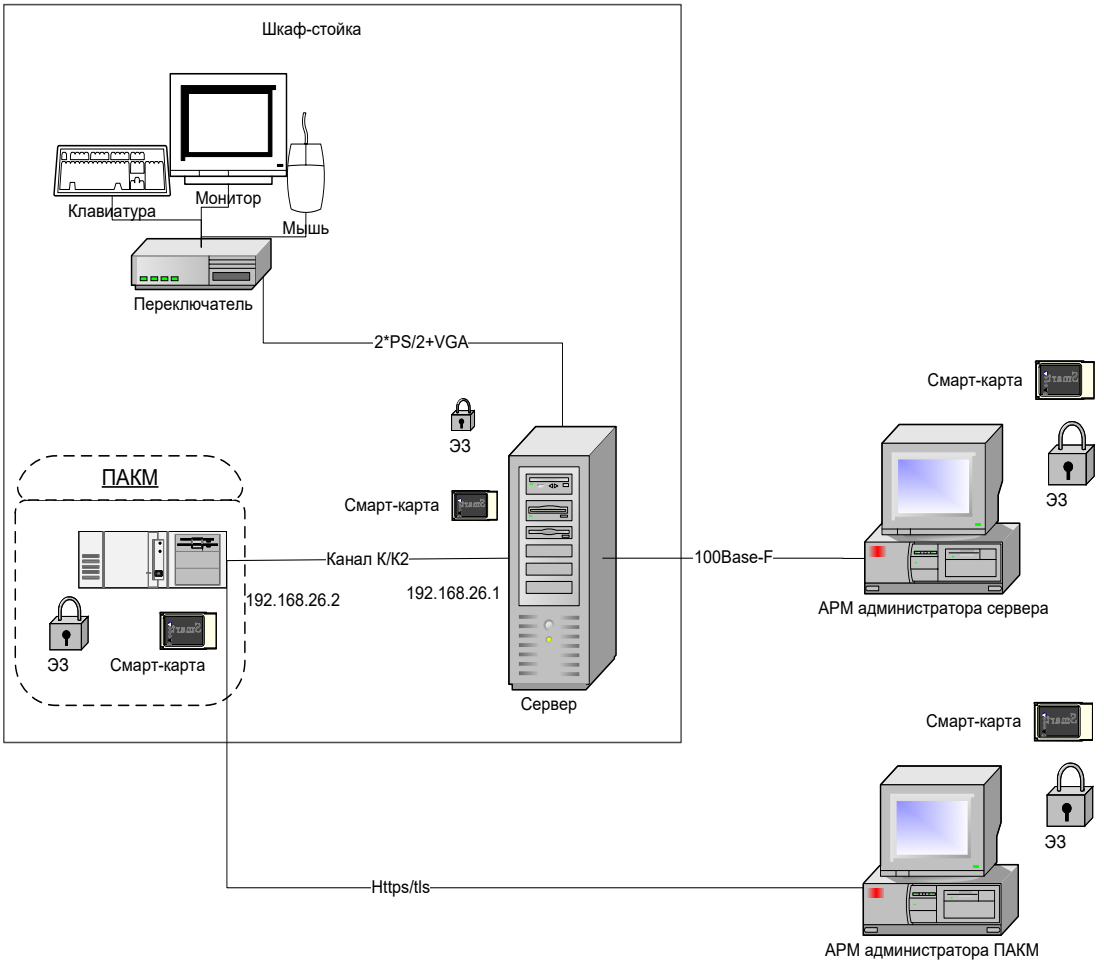


Рисунок 9. Схема подключения ПАКМ к серверу

Допускается использовать ПАКМ как групповое СКЗИ, обслуживающее несколько серверов. При этом каждый сервер должен иметь отдельный считыватель смарт-карт, используемый для карт канала «К». Так как ввод pin-кодов при активации ключей производится с LCD панели ПАКМ, со стороны обслуживающего персонала должен обеспечиваться контроль за активацией ключей приложениями серверов (чтобы не было двусмысленных ситуаций – pin-код какого именно ключа (какого приложения/сервера) запрашивается на LCD панели в данный момент).

Такое подключение серверов осуществляется через маршрутизатор. Маршрутизатор с ПАКМ соединяется строго оптическим кабелем, сервера с маршрутизатором соединяются либо оптическими кабелями, либо обычной витой парой. Для перехода с витой пары на оптику может быть использован соответствующий конвертор.

Примерная схема подключения нескольких серверов к ПАКМ изображена на Рисунок 10.

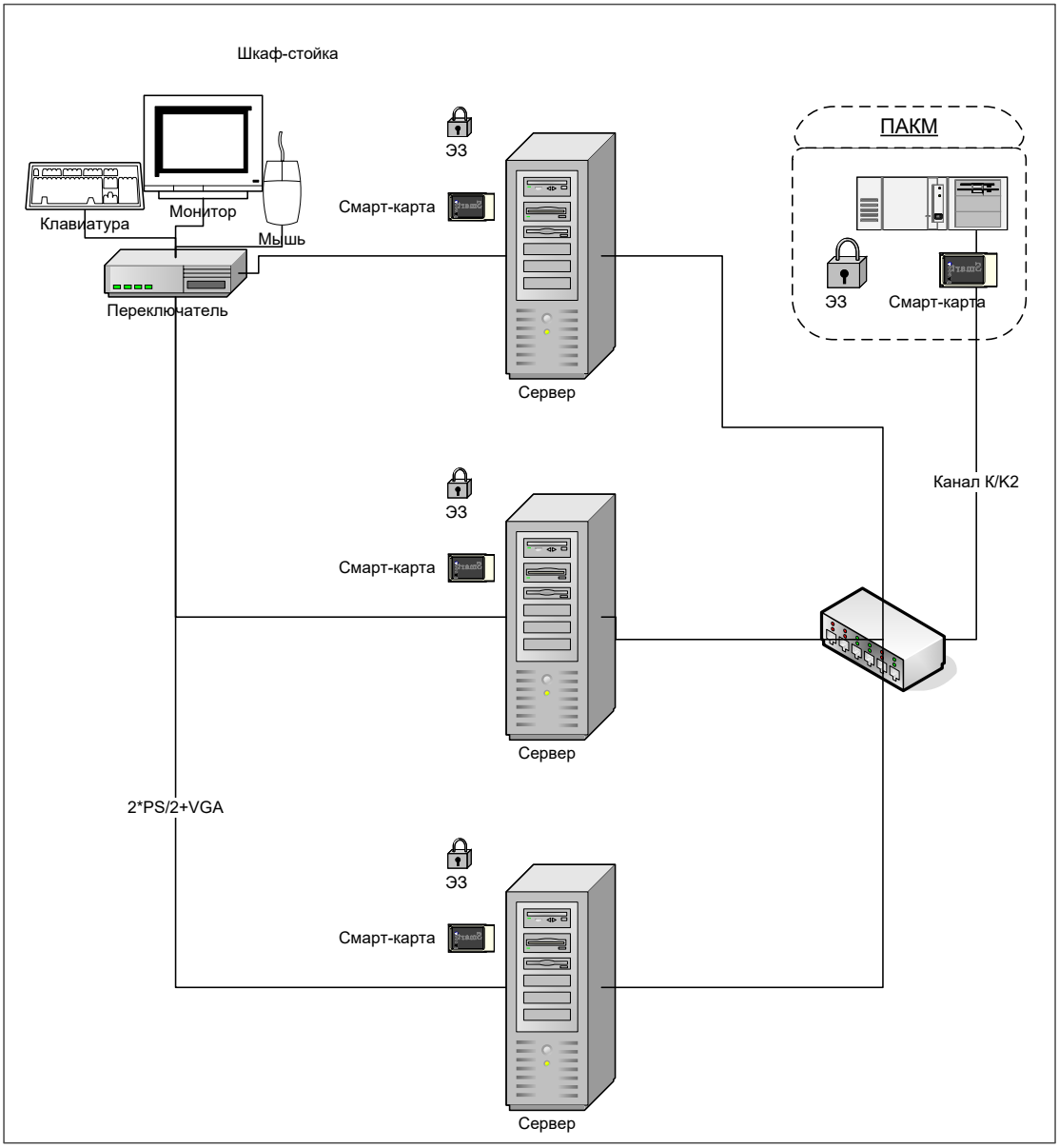


Рисунок 10. Схема подключения ПАКМ к нескольким серверам

При использовании ПАКМ в качестве разделяемого корпоративного СКЗИ пользователей сети, ПАКМ включается в любой сегмент локальной сети. Рабочие станции пользователей взаимодействуют с ПАКМ по каналу «К2» и могут находиться как в том же, так и в других сегментах сети.

Одновременно с рабочими станциями обычных пользователей, клиентами ПАКМ могут быть и сервера приложений, взаимодействующих с ПАКМ по каналу К, а также рабочая станция, предназначенная для удаленного администрирования ПАКМ (должна подключаться на отдельный сетевой интерфейс ПАКМ при его наличии).

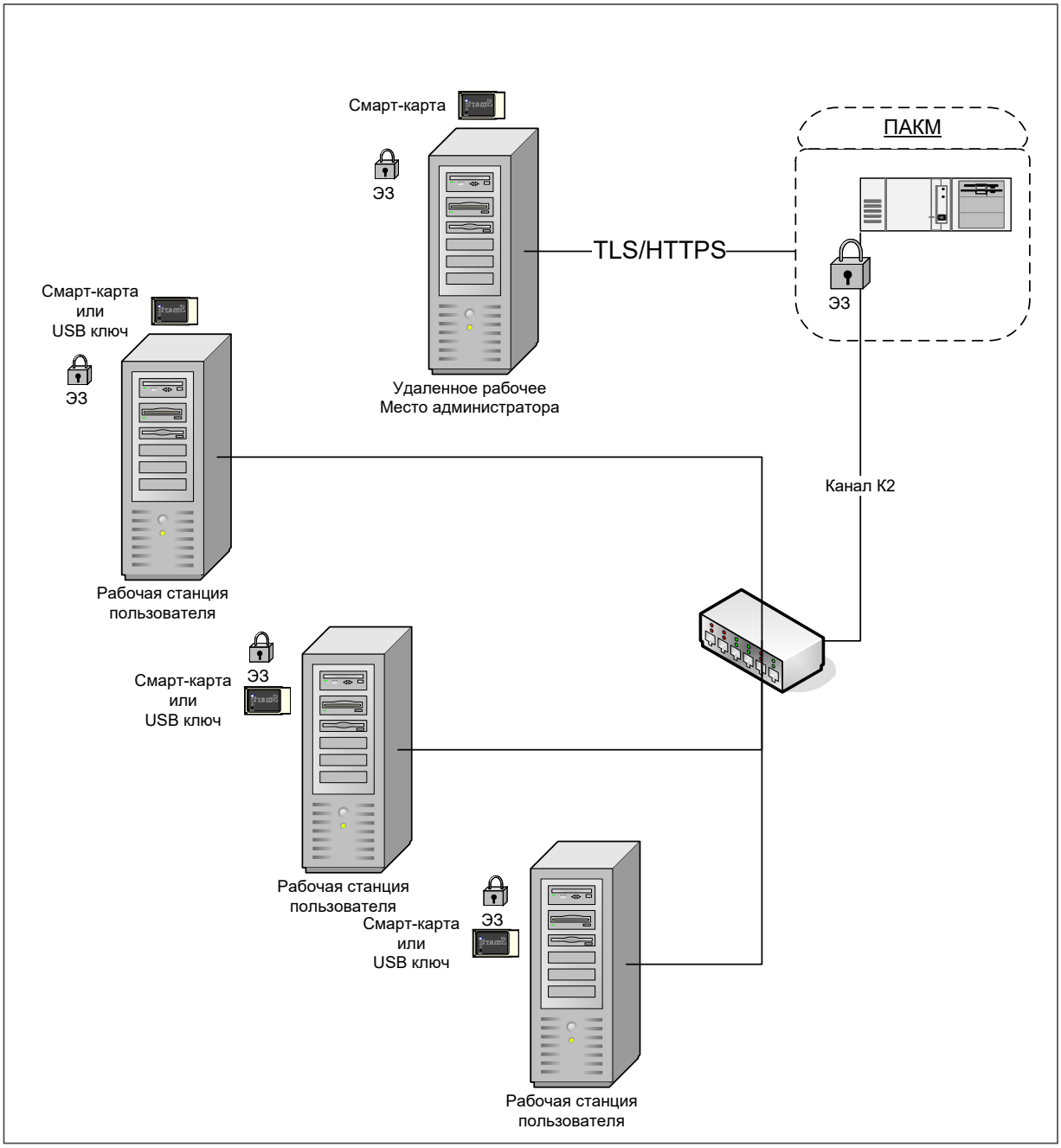


Рисунок 11. Схема подключения рабочих станций пользователей к ПАКМ

Администратор ПАКМ имеет возможность описать правила встроенного в ПАКМ межсетевого экрана. При этом надо иметь ввиду, что рабочие станции пользователей и сервера приложений обращаются к ПАКМ по каналу «К2» с использованием порта с номером 1501; сервера с установленными ОС семейства Unix/Linux, обращающиеся к ПАКМ по каналу «К», используют порт с номером 1502, а ПО удаленного администрирования ПАКМ использует порт 443 для взаимодействия с ПАКМ. Для увеличения производительности серверных приложений, базирующихся на ОС семейства Windows, имеется возможность организовать нешифрованный канал К2 (К2s) при соблюдении требований по безопасности, включающих организационные меры по

размещению ПАКМ и сервера в одной серверной стойке. При этом в ПАКМ используется отдельный порт для входящих соединений 1503.

Для каждого канала можно указать как конкретные IP адреса, так и подсети, с которых разрешено обращение к ПАКМ на указанный порт.

5.3. Условия применения

Функции криптографической защиты ПАКМ «КриптоПро HSM» обеспечивают защиту ключевой информации от угрозы чтения по побочным каналам (ПЭМИН и ЛП). Для этого в криптографической системе ПАКМ «КриптоПро HSM» реализован комплекс мер по защите:

- маскирование ключевой информации;
- шифрование хранящихся на диске ПАКМ ключевых контейнеров пользователей;
- ограничение возможности использования ключей;
- механизм производных ключей.

При применении ПАКМ «КриптоПро HSM» необходимо выполнять требования документа «ЖТЯИ.00096-02 91 01. КриптоПро HSM. Руководство администратора безопасности».

6. ВЕДЕНИЕ ЖУРНАЛОВ

Администратор безопасности Серверов и ПАКМ «КриптоПро HSM» ведет следующие журналы:

- «Журнал регистрации администраторов безопасности и пользователей»;
- «Журнал пользователя сети».

В «Журнале регистрации администраторов безопасности и пользователей» фиксируются факты регистрации администраторов Серверов, ПАКМ «КриптоПро HSM», администраторов безопасности организации, пользователей системы. Для этого может использоваться журнал пользователей ПАКМ, доступный через web-интерфейс администратора ПАКМ.

В «Журнал пользователя сети» записываются факты изготовления и плановой смены ключей, факты компрометации ключевых документов, нештатные ситуации, происходящие в сети и на ПАКМ «КриптоПро HSM», проведение регламентных работ, данные о полученных у администратора безопасности ключевых носителях, нештатных ситуациях, произошедших на АРМ с установленным ПО СКЗИ.

В «Журнале пользователя сети» может отражаться следующая информация:

- дата, время;
- запись о компрометации ключа;
- запись об изготовлении личного ключевого носителя пользователя, идентификатор носителя;
- запись об изготовлении копий личного ключевого носителя пользователя, идентификатор носителя;
- запись об изготовлении резервного ключевого носителя пользователя, идентификатор носителя
- запись о получении сертификата ключа проверки ЭП, полный номер ключевого носителя, соответствующий сертификату;
- записи, отражающие выдачу на руки пользователям (ответственным исполнителям) и сдачу ими на хранение личных ключевых носителей, включая резервные ключевые носители;
- события, происходившие на сервере с установленным ПО СКЗИ, с указанием причин и предпринятых действий.

Примечание. Примерные графы журналов приведены в приложениях 2, 3 документа «ЖТЯИ.00096-02 91 01. КриптоПро HSM. Руководство администратора безопасности».

В автоматизированном виде в ПАКМ ведется 3 журнала:

1. Журнал аудита ПАКМ

2. Журнал событий СКЗИ
3. Журнал пользователей ПАКМ

Журнал событий ПАКМ «КриптоПро HSM» ведется средствами операционной системы, под управлением которой функционирует ПАКМ. События ОС, подвергаемые аудиту в ПАКМ:

- старт/останов операционной системы;
- старт/останов системных сервисов;
- идентификация/аутентификация/авторизация пользователей в системе;
- использование криптографических функций;
- запуск процессов;
- монтирование/демонтирование;
- вызов сервисов межпроцессного взаимодействия;
- отказ в создании дополнительных процессов.

Дополнительно к штатным событиям ОС в журнал событий ПАКМ «КриптоПро HSM» заносятся данные о событиях, генерируемых прикладным программным обеспечением ПАКМ, реализующим криптографические функции. Аудиту подвергаются следующие функции управления СКЗИ и криптографические операции:

- генерация ключа;
- операции подписи/проверки подписи;
- операции шифрования/расшифрования;
- операции экспорта/импорта ключа;
- изменение системного времени.

Журнал аудита ПАКМ предназначен для отражения и сохранения информации о значимых событиях, так или иначе меняющих состояние ПАКМ и о событиях, связанных с выполнением СКЗИ своих целевых функций. Журнал аудита ведется в хронологическом порядке возникновения событий.

При заполнении памяти отведенной под данные журнала аудита эта память должна быть очищена. Очистка журнала аудита производится либо по распоряжению Суперпользователя ПАКМ, либо по распоряжению Аудитора ПАКМ с подтверждением действия Администратором ПАКМ, либо автоматически (настраивается Аудитором ПАКМ).

Журнал пользователей ПАКМ содержит информацию о зарегистрированных в ПАКМ пользователях, и дополнительную информацию о них (сертификат доступа, роль, признак блокирования, идентификаторы). Журнал доступен к просмотру через web-интерфейс администратора. Функции ведения журнала доступны также с LCD панели управления ПАКМ.

7. КОНТРОЛЬ УСТАНОВОК ВРЕМЕНИ

В ходе эксплуатации необходимо контролировать установки времени на ПАКМ «КриптоПро HSM». Время, установленное в ПАКМ, не должно отличаться от установленного в Сервере более, чем на 5 мин.

Текущее время ПАКМ «КриптоПро HSM» отображается в окне панели управления «КриптоПро HSM Client» на вкладке «Параметры HSM», на LCD панели ПАКМ, а также на странице с информацией о ПАКМ в web-интерфейсе администратора. Время предустанавливается предприятием-изготовителем и корректируется администратором ПАКМ (процедура установки системного времени описана в п. 9.5).

При изменении системного времени ПАКМ на значительную величину (больше 5 мин) ПАКМ необходимо перезагрузить.

8. НЕШТАТНЫЕ СИТУАЦИИ ПРИ ЭКСПЛУАТАЦИИ СКЗИ

Ниже приведен основной перечень нештатных ситуаций и соответствующие действия персонала при их возникновении.

Таблица 1. Действия персонала в нештатных ситуациях

№ п/п	Нештатная ситуация	Действия персонала
1.	Эвакуация, угроза нападения, взрыва и т.п., стихийные бедствия, аварии общего характера	Остановить все ЭВМ. Персонал, имеющий доступ к ключам, обязан сдать все имеющиеся у него в наличии ключевые носители администратору безопасности. Администратор безопасности упаковывает все ключевые носители в опечатываемый контейнер, который выносит в безопасное помещение или здание. Опечатанный контейнер должен находиться под охраной до окончания действия нештатной ситуации и восстановления нормальной работы аппаратных и программных средств СКЗИ. Администратор безопасности оповещает по телефонным каналам общего пользования всех пользователей о приостановке работы системы. В случае наступления события, повлекшего за собой долговременный выход из строя аппаратных средств СКЗИ, администратор безопасности уничтожает всю ключевую информацию с носителей, находящихся в контейнере.
2.	Компрометация одного из личных ключевых носителей.	Порядок действий при компрометации ключей описан в Правилах пользования.
3.	Выход из строя личного ключевого носителя. (в том числе: для носителей Touch Memory и смарт-карт).	Необходимо сообщить администратору безопасности о факте выхода из строя личного ключевого носителя и обеспечить его доставку администратору безопасности для выяснения причин выхода из строя. При наличии резервного личного ключевого носителя – использовать его.
4.	Отказы и сбои в	При отказах и сбоях в работе аппаратной части ПАКМ

№ п/п	Нештатная ситуация	Действия персонала
	работе аппаратной части ПАКМ.	необходимо остановить работу, по возможности локализовать неисправность и в дальнейшем произвести ремонт в установленном порядке и, при необходимости, переустановку СКЗИ.
5.	Отказы и сбои в работе средств защиты от НСД.	При отказах и сбоях в работе средств защиты от НСД, администратор безопасности, должен восстановить работоспособность средств НСД. При необходимости переустановить программно-аппаратные средства НСД.
6.	Утеря личного ключевого носителя.	Утеря личного ключевого носителя приводит к компрометации ключей.
7.	Отказы и сбои в работе программных средств вследствие не выявленных ранее ошибок в программном обеспечении.	При отказах и сбоях в работе программных средств вследствие не выявленных ранее ошибок в программном обеспечении необходимо остановить работу, локализовать по возможности причину отказов и сбоев и вызвать разработчика данного ПО или его представителя для устранения причин, вызывающих отказы и сбои.
8.	Отказы в работе программных средств вследствие случайного или умышленного их повреждения.	При отказах в работе программных средств вследствие случайного или умышленного их повреждения лицо, ответственное за безопасность функционирования программных и аппаратных средств, обязано произвести служебное расследование по данному факту с целью установления причины отказа и восстановления правильной работы программных средств в установленном порядке.
9.	Отказы в работе программных средств вследствие ошибок оператора.	При отказах в работе программных средств вследствие ошибок оператора, оператор сообщает о данном факте лицу, ответственному за безопасность функционирования программных и аппаратных средств, которое дает соответствующие указания обслуживающему персоналу по восстановлению правильной работы программных средств в установленном порядке.

Все нештатные ситуации должны отражаться в «Журнале пользователя сети» (см. раздел 6).

9. УСТАНОВКА ПАКМ

9.1. 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);
6. Произвести сетевые настройки ПАКМ;
7. Произвести настройки (проверить корректность) системного времени ПАКМ;
8. При изменении сетевых настроек (IP адресов интерфейсов ПАКМ) перевыпустить сертификаты TLS сервера ПАКМ.
9. При необходимости (желании использовать ВЭБ интерфейс администратора) добавить необходимое число учетных записей привилегированных пользователей для работы через Web интерфейс администрирования, и сформировать для них ключи и сертификаты аутентификации на смарт-картах.
10. При необходимости выпустить на ПАКМ комплект рабочих карт канала «К» для подключения серверов приложений по каналу К (согласно процедуре, описанной в п. 11.2.7);
11. Произвести установку программного обеспечения интерфейсных модулей для взаимодействия с ПАКМ на рабочих станциях пользователей/серверах, автоматизированном рабочем месте администратора ПАКМ (ВЭБ интерфейс);
12. Произвести запуск ВЭБ интерфейса администратора, произвести дополнительные настройки ПАКМ, добавить тестового пользователя и сформировать для него ключи и сертификат аутентификации;
13. Произвести тестовый запрос на генерацию ключа подписи пользователя с рабочего места пользователя.

14. Удалить тестовые ключи пользователя и Пользователя в ПАКМ.

9.2. Проверка комплектации и подключение ПАКМ

После распаковки необходимо проверить комплектацию устройства. Комплектация должна соответствовать указанной в прилагаемой эксплуатационной документации («ЖТЯИ.00096-02 30 01. КриптоПро HSM. 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 10)

9.3. 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-ти» (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 подписи ПАКМ и самоподписанного сертификата (защищенного на ключе активации ПАКМ);
- формирование ключа шифрования ключей подписи пользователей, хранящихся в ПАКМ, защищенного на ключе активации ПАКМ;
- формирование ключа и сертификата аутентификации TLS сервера, зашифрованного на ключе шифрования ПАКМ;
- добавление в базу данных пользователей первого привилегированного пользователя – Администратора ПАКМ и формирование ключа и сертификата аутентификации для него на смарт-карте.

Внешне это будет выглядеть следующим образом:

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

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

После этого будет выдан запрос на вставку чистой смарт-карты для записи на нее ключей и сертификата аутентификации пользователя-администратора ПАКМ. Впоследствии именно эта карта должна будет использоваться для получения доступа к LCD меню ПАКМ для его первоначальной настройки.

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.

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.

9.4. Установка сетевых настроек ПАКМ

Аппаратная платформа ПАКМ «КриптоПро HSM» имеет 2 сетевых оптических 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. 12.2.4) или с использованием web-интерфейса.

Кроме сетевых настроек, необходимо установить правила межсетевого экрана для сетевого доступа к ПАКМ. Для каждого порта (1501 – порт «канала «К2»», 1502 – порт канала «К», 443 – порт для доступа с web-интерфейса администратора, 1503– порт канала «К2» 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 «К2».

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.

9.5. Установка системного времени ПАКМ

Процедура установки времени описана в данном документе в разделе 11.2.4.

9.6. Выпуск карты локального защищенного канала (канала «К»)

Для защиты информации, циркулирующей между Серверами приложений на базе операционных систем семейства Unix/Linux и ПАКМ, в системе организуется специальный локальный защищенный канал (канал К), 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.

Процедура выпуска карт канала «К» описана в данном документе в п. 11.2.7.

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

9.7. Установка интерфейсных модулей

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

Для функционирования сервиса криптопровайдера ПАКМ на сервере приложений требуется вставить в считыватель интеллектуальных карт Сервера карту аутентификации (карта канала «К» или «К2»), выпущенную на ПАКМ.

Для функционирования сервиса криптопровайдера ПАКМ на рабочей станции пользователя/сервере приложений с установленной ОС семейства Windows требуется вставить в считыватель интеллектуальных карт рабочей станции смарт-карту аутентификации (карта канала «К2») пользователя/администратора сервера, выпущенную на ПАКМ или на удаленном рабочем месте администратора ПАКМ, и активировать канал «К2», кликнув соответствующую иконку в системном трее ОС Windows (только для обычных пользователей). При использовании карты, имеющей в сертификате ключа аутентификации специальное расширение «Администратор сервера», стартующий 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.

9.8. 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 Microsoft Internet Explorer версии не ниже 5.5/Microsoft Edge.

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 4.0/5.0 и выше (входит в комплект поставки ПАКМ).

Для просмотра через web-интерфейс сертификатов, издаваемых ПАКМ, в стандартных окнах ОС Windows, необходимо установить свободно распространяемый COM компонент MS CAPICOM (входит в состав дистрибутива ПО), в соответствии с инструкциями производителя (см. readme файл).

Рабочая станция должна быть оснащена считывателем смарт-карт.

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 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 и ключа и сертификата TLS сервера, изданного на новом ключе ПАКМ, необходимо перевыпустить ключ аутентификации привилегированного пользователя ПАКМ и повторить процедуру извлечения и установки нового самоподписанного сертификата ПАКМ на рабочей станции удаленного администрирования.

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. Возможно, в первый раз будет выдан запрос на установку активных элементов управления (ActiveX). Интернет обозреватель должен быть настроен на разрешение работать с указанными активными элементами управления.

9.9. 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.

9.10. 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.

9.11. Требования безопасности

При установке программного обеспечения интерфейсных модулей следует руководствоваться следующими рекомендациями:

- выполнить действия, предписываемые в «ЖТЯИ.00096-02 91 01. КриптоПро HSM. Руководство администратора безопасности»;
- 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 электронный замок (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 электронного замка.

Контроль целостности должен охватывать следующие файлы:

- ПО интерфейсных модулей;
- драйверы устройств и портов ввода интеллектуальных карт, com-порта, сети

Ethernet;

- программы отображения log-файлов;
- драйвер электронного замка.

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

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

Ключи электронного замка ПАКМ относятся к категории ключевых носителей, подлежат соответствующему учету и хранению (см. п. 4.2.3).

10. ВКЛЮЧЕНИЕ ПАКМ

Предварительные условия:

1. ПАКМ подключен к Серверу в соответствии с разделом 9.
2. У администратора, осуществляющего включение, имеется в наличии ключ электронного замка («таблетка»).
3. Питание ПАКМ выключено.

Действия администратора:

1. Нажать кнопку включения питания.
2. Ожидать появления на LCD надписи <Loading>.
3. Приложить «таблетку» к считывателю ЭЗ и подержать в течение 10 сек.
4. Примерно через 1 мин. на LCD панели ПАКМ начнет отображается процесс загрузки прикладного ПО ПАКМ (наименования запущенных служб, а затем в процентах отражаться прохождение процедуры контроля целостности системы). 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.

11. 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.

11.1. 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.

1. 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.

2. 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.

11.2. 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 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 «К», 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 (autosence);

- 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);

- настройки межсетевого экрана (FW settings)

Включает подменю:

- Канал K (K channel);

- Канал K2 (K2 channel);

- Сетевой администратор (Remote admin);

- Репликация (Replication);

- Изменение ключей и сертификатов уполномоченных лиц (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);

- восстановление журнала аудита (Repair audit log);

- резервное копирование и восстановление ПАКМ (Backups).

11.2.1. 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 следующие:

- неактивное состояние (ключи не активированы, каналы закрыты) – INACTIVE;
- активное состояние (ключи активированы, все каналы открыты) – FULL ACTIVE;
- только администрирование (ключи активированы, каналы «К» и «К2» закрыты, возможно сетевое администрирование) – 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.

11.2.2. 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.11.2).
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.

11.2.3. 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 находится 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.11.2).
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.

11.2.4. 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):

1. Администратор входит в меню (как описано в п.11.2).
2. 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);**

3. Кнопками вверх/вниз увеличивает или уменьшает число.
4. Кнопками вправо/влево изменяет положение курсора (переход по цифрам индикации времени).
5. Нажатие Enter: индикация сообщения «Save time?» (для даты – «Save date?»)
6. Кнопками Вправо/Влево – выбор: «YES?» и «NO».
7. 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 ПАКМ ведется вне временных зон. И при отображении, и при установке времени используется UTC time.

11.2.5. 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.11.2).
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;
   - Остаток случайной информации (в «пакетах» для одного генерируемого ключа Пользователя);
   - Свободное место на диске (в килобайтах);

- Количество созданных ключей, защищенных на других ключах (с момента начальной инициализации ПАКМ);
- Количество криптографических вызовов – создания ЭП (с момента начальной инициализации ПАКМ);
- Количество выпущенных при последней смене карт канала «К»;
- Количество операций смен карт канала «К» (с момента начальной инициализации ПАКМ);
- Количество созданных ключей Пользователя (с момента начальной инициализации ПАКМ);
- Номер версии сборки дистрибутива ПО ПАКМ.

4. Нажатие кнопки Enter или стрелки влево/вправо приводит к выходу в главное меню.

11.2.6. 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 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. 9.3).

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, используя процедуру 3 из 5-ти, ПАКМ автоматически переходит в активный режим – ADMIN-ONLY, а значит выполнить операцию full clean в данном случае невозможно.

11.2.7.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.11.2).

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 «K» (не использовавшаяся ранее в данном сеансе выпуска карт и не являющаяся картой с текущим ключом канала K), 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 «K» «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.

11.2.8. 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.11.2).
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.

Можно изменить следующие параметры сетевых настроек (кроме IP-адреса HSM): маску подсети для HSM, IP-адрес шлюза локальной сети, 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). Способ изменения маски подсети и адреса шлюза аналогичен способу изменения IP-адреса HSM, режим передачи данных выбирается с помощью меню.

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 перегенерация TLS серверных сертификатов ПАКМ, а также, возможно, корректировка правил межсетевого экрана.

11.2.9. 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.11.2).
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, состоящие 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)

Названия событий следующие:

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-и из 5-ти»);

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.

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 9 для.

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

Подробнее о механизме репликации описано в п. 4.10.2.

11.2.10. 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.

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.11.2).

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 «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 КВ/КВ2 это недопустимо. Допускается выполнение ролей привилегированных пользователей доверенными лицами (суперпользователя) – хранителями частей разделенного секрета ключа активации ПАКМ. Создание новых привилегированных пользователей ПАКМ 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?» (см. п. 4.4). 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 пин-код»). После ввода пин-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 пин-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 буден 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 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 таймаута 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».

11.2.11. 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 К2 – 1501, канал К2s – 1503, канал для Web администрирования ПАКМ – 443, канал репликаций - 1504.

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.11.2).
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)**, и репликация **(Replication)** 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 таймаута 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.

11.2.12. 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:

1. Администратор входит в меню (как описано в п.11.2). Для изменения ключа и сертификата аутентификации администратора производится вход в меню по схеме 3 из 5, после чего ПАКМ перейдет в состояние «только администрирование».
2. Клавишами вверх/вниз пользователь листает и кнопкой Enter выбирает пункт меню:

   - изменение ключей **(Update keys)**;

3. 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».

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-ти»).

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 буден 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».

Внимание! При смене ключа подписи и самоподписанного сертификата ПАКМ, а также ключа TLS сервера и его сертификата, изданного новым ключом, может возникнуть ситуация, когда пользователи, работающие по каналу К2 не смогут установить соединение с ПАКМ, так как у них не будет нового самоподписанного сертификата ПАКМ, необходимого для проверки сертификата TLS сервера. При смене ключа подписи ПАКМ и самоподписанного сертификата должна быть проработана стратегия перевыпуска необходимых сертификатов.

Каждому пользователю выпускается ключ и сертификат доступа, помещаемый в контейнер ключа. Кроме этого в контейнер ключа помещается и самоподписанный сертификат ключа подписи ПАКМ, на котором издан сертификат пользователя (в том числе и Администратора ПАКМ). При инициализации рабочего места пользователя (первое подключение к ПАКМ), самоподписанный сертификат ПАКМ извлекается из контейнера ключа подписи и по запросу устанавливается в хранилище доверенных корневых сертификатов пользователя. Это необходимо для работы канала «К2», а именно для проверки сертификатов пользователя и TLS сервера ПАКМ.

После смены ключа и самоподписанного сертификата ПАКМ при работе по каналу К2 существует 2 категории пользователей:

- ранее работавшие с ПАКМ пользователи – имеют старый самоподписанный сертификат ПАКМ и имеющие возможность проверить текущий (старый) сертификат TLS сервера.

- новые пользователи – не имеют никаких сертификатов и не имеют возможности проверить текущий сертификат TLS сервера.

Если в этот момент мы перевыпускаем сертификат TLS сервера на новом ключе подписи ПАКМ, то новые пользователи получат свои карточки с новым самоподписанным сертификатом ПАКМ и смогут успешно работать с ПАКМ по каналу К2. Старые

пользователи, как отмечалось выше – не смогут. Им необходимо будет либо доставлять новый сертификат ПАКМ вручную, либо срочно перевыпускать карточки.

Если мы меняем сертификат TLS сервера только после того, как все старые пользователи поменяют карточки с сертификатом доступа, то старые пользователи с новыми карточками смогут работать по каналу К2. Новые пользователи будут иметь карточки с новым самоподписанным сертификатом ПАКМ и на их рабочем месте не будет установленного старого самоподписанного сертификата ПАКМ, поэтому текущий (на старом ключе) сертификат TLS сервера не будет проверяться. Теперь уже этим пользователям необходимо будет установить старый самоподписанный сертификат ПАКМ в доверенное хранилище вручную.

Стратегия – в какой момент перевыпускать ключ и сертификат TLS сервера - выбирается в зависимости от количества существующих (старых) пользователей и предполагаемого количества новых пользователей, которые могут появиться за период, когда всем старым пользователям будут перевыпущены карточки.

11.2.13. 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.11.2).
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 пин 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 таймаута произойдет переход в основное меню.

11.2.14. 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.

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.11.2).
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 пин 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.

11.2.15. Резервное копирование и восстановление ПАКМ

Для обеспечения надежности ПАКМ «КриптоПро HSM» имеет возможность резервирования ключевой информации и, при необходимости, её восстановления (подробнее см. п. 11.2.15).

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.11.2).
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.

11.3. 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. 11.2.2). 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. 12.2.10). Журнал отображается на HTML странице и, при необходимости может быть сохранен в виде файла, а также подписан на любом ключе пользователя-администратора.

Для обеспечения защиты содержимого журнала событий ПАКМ от сбоев в системе рекомендуется регулярно (не реже, чем раз в сутки) считывать 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).

12. УДАЛЕННОЕ АДМИНИСТРИРОВАНИЕ ПАКМ (WEB ИНТЕРФЕЙС)

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.

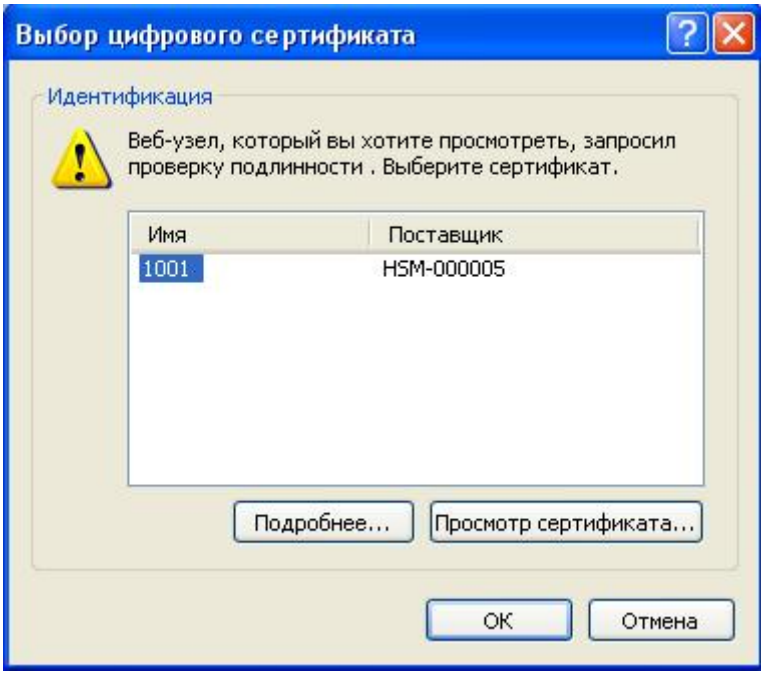
Удаленное администрирование ПАКМ производится привилегированным пользователем при предъявлении (а именно - помещении в считыватель) действующей карты Администратора, Аудитора или Администратора резервного копирования. После использования такой карты для Web-администрирования эта карта не может быть использована 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 «Удаленное рабочее место Администратора» данного документа.

12.1. Открытие окна администрирования ПАКМ

Для открытия страницы администрирования ПАКМ надо ввести в адресной строке Интернет обозревателя (Internet Explorer/Edge) IP-адрес ПАКМ (с префиксом https://). В старых ОС Windows, возможно, понадобится ввести и имя страницы – default.htm. Дело в том, что в ОС Windows Vista, Windows 7, Windows 2008, включая 64-разрядные их версии, для генерации ключей доступа пользователей вместо компонента Microsoft XEnroll.dll используется компонент Microsoft CertEnroll.dll. В настоящий момент при обращении к ПАКМ просто по IP адресу без указания имени страницы по умолчанию загружается страница default_vista.htm, использующая CertEnroll. Если на АРМ Администратора установлена более старая ОС (Windows 2003), то необходимо указывать имя загружаемой страницы явно, например https://192.168.26.2/default.htm. И та, и другая страница работают нормально в любой ОС Windows, пока дело не дойдет до генерации ключей и сертификатов доступа пользователей ПАКМ.

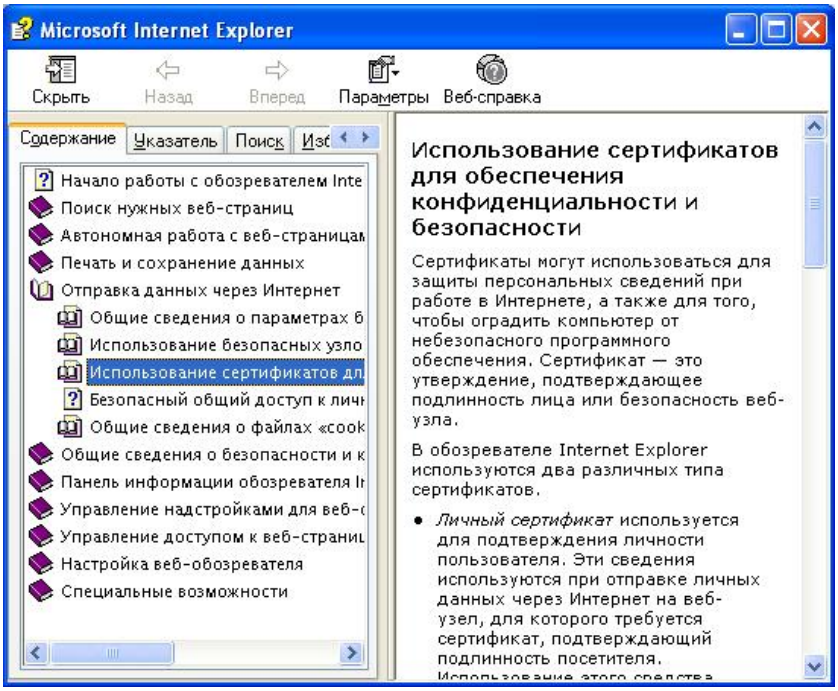
После подтверждения ввода адреса появится окно «Выбор цифрового сертификата»:



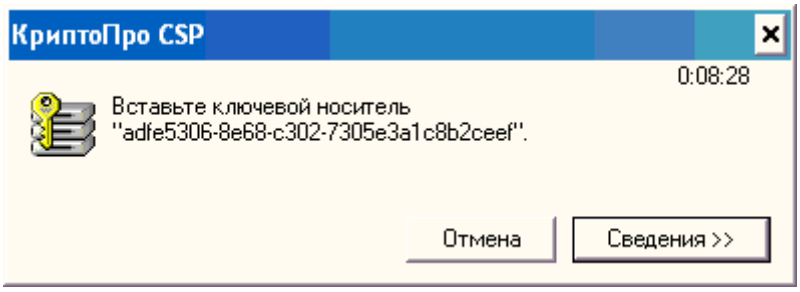
Следует выбрать сертификат и нажать **ОК**.

Если нажать «**Просмотр сертификата**», появится стандартное окно просмотра сертификата в Windows (для него должен быть установлен компонент Microsoft CAPICOM, включенный в дистрибутив).

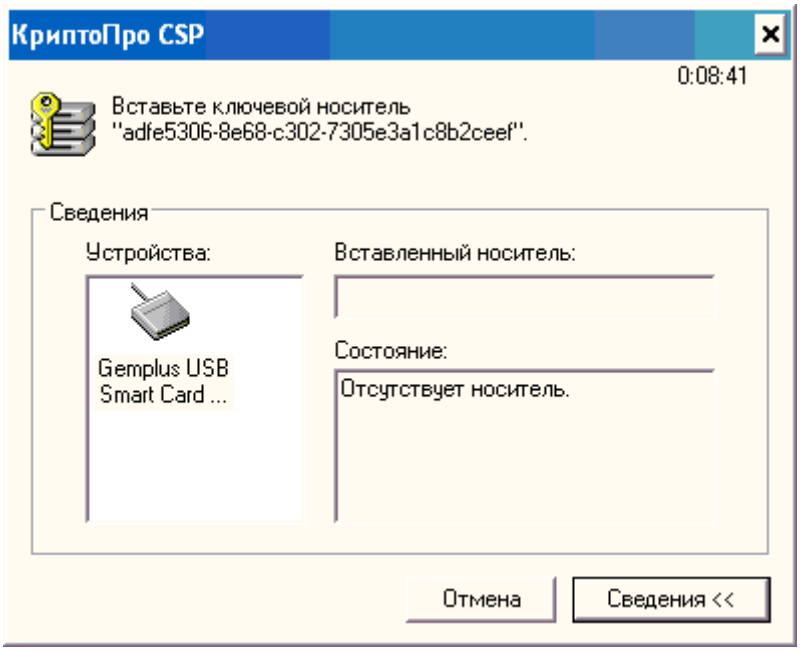
Если нажать «**Подробнее**», появится окно с подсказкой:



После выбора сертификата и нажатия «**ОК**» появится приглашение вставить карту в считыватель:



Если нажать кнопку «**Сведения**», появится более подробная информация:



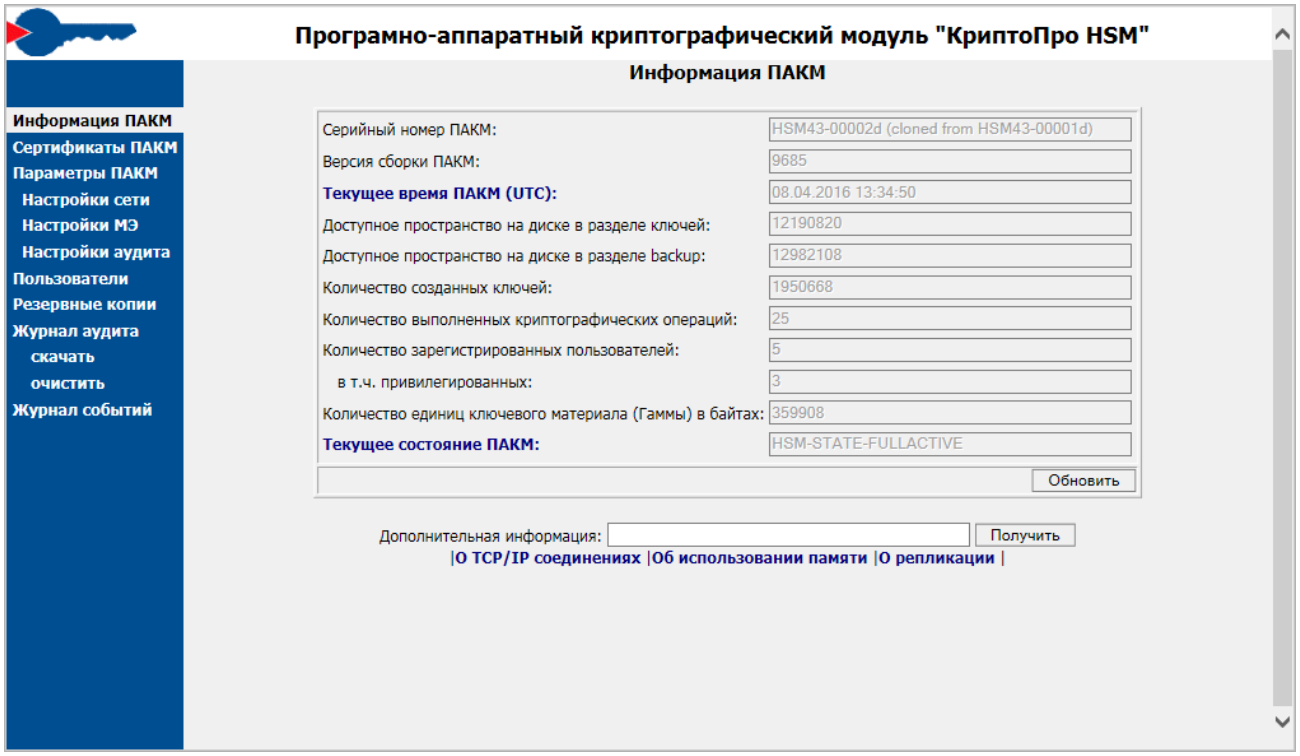
После того, как карта администратора или аудитора будет вставлена в считыватель, это окно исчезнет, и появится приглашение ввести pin-код карты. Если во время предыдущего ввода pin-кода был установлен флажок «запомнить», этап ввода pin-кода будет пропущен.

После этого появится окно администрирования ПАКМ.

12.2. Работа с окном администрирования ПАКМ

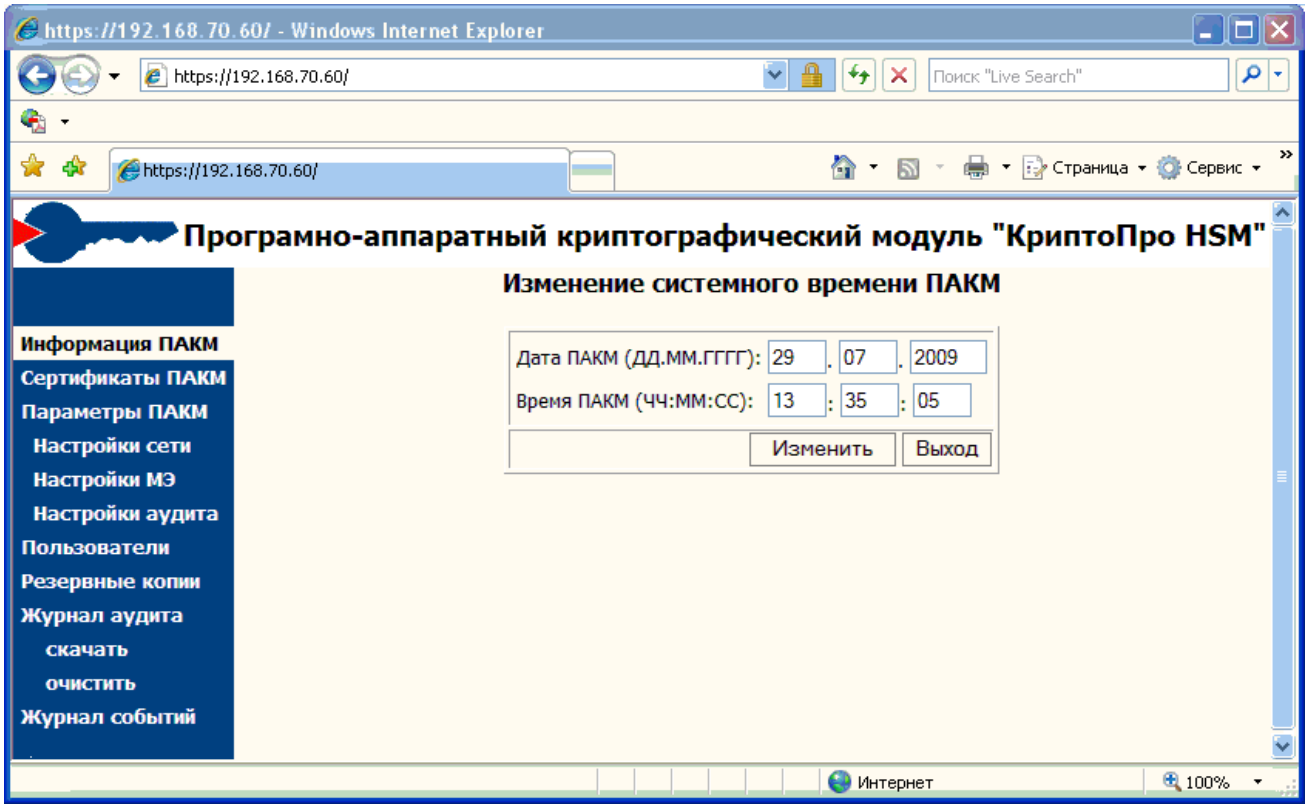
12.2.1. Информация ПАКМ

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.



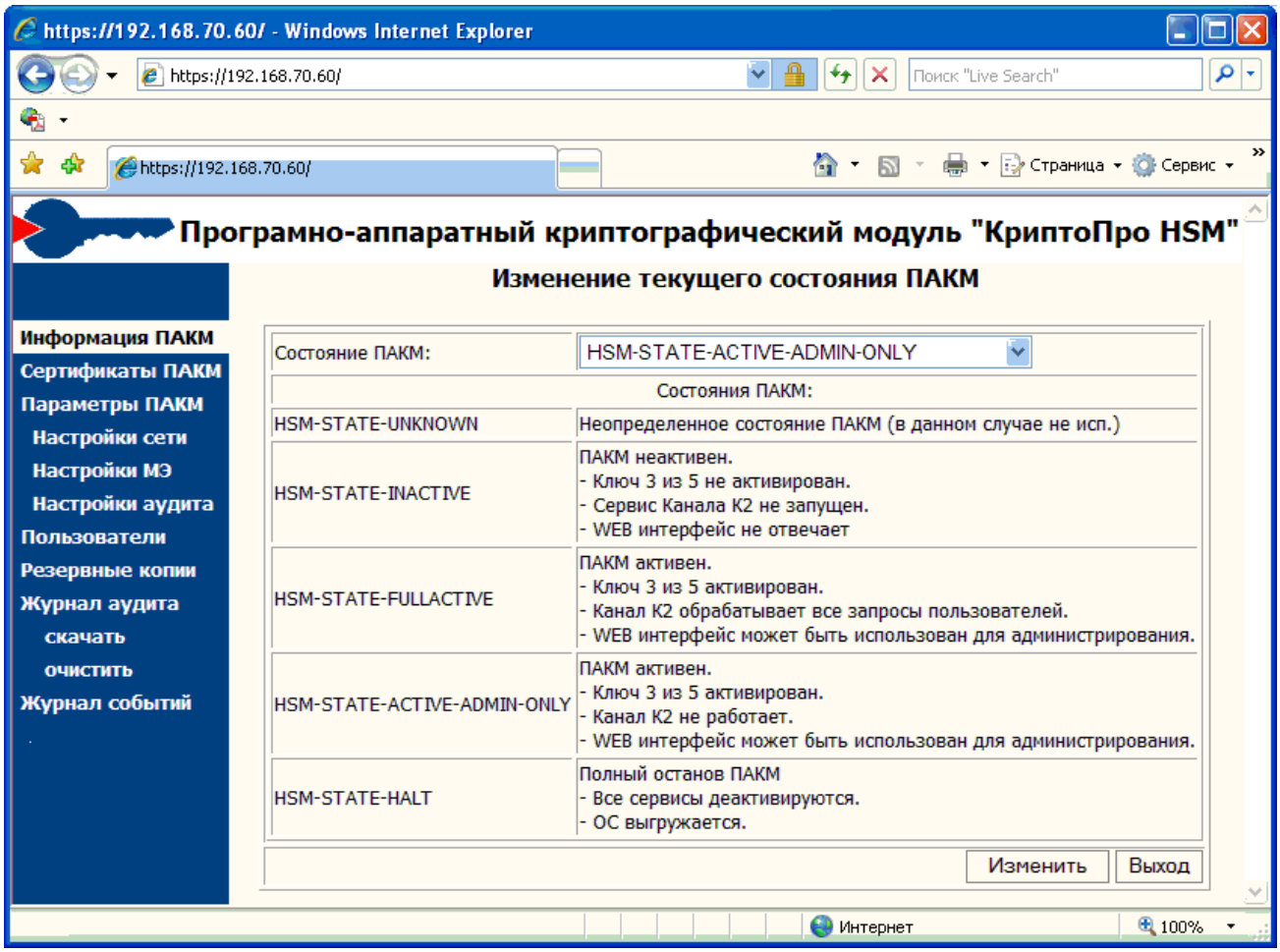
Чтобы просмотреть текущие настройки ПАКМ, надо нажать кнопку «**Обновить**».

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:

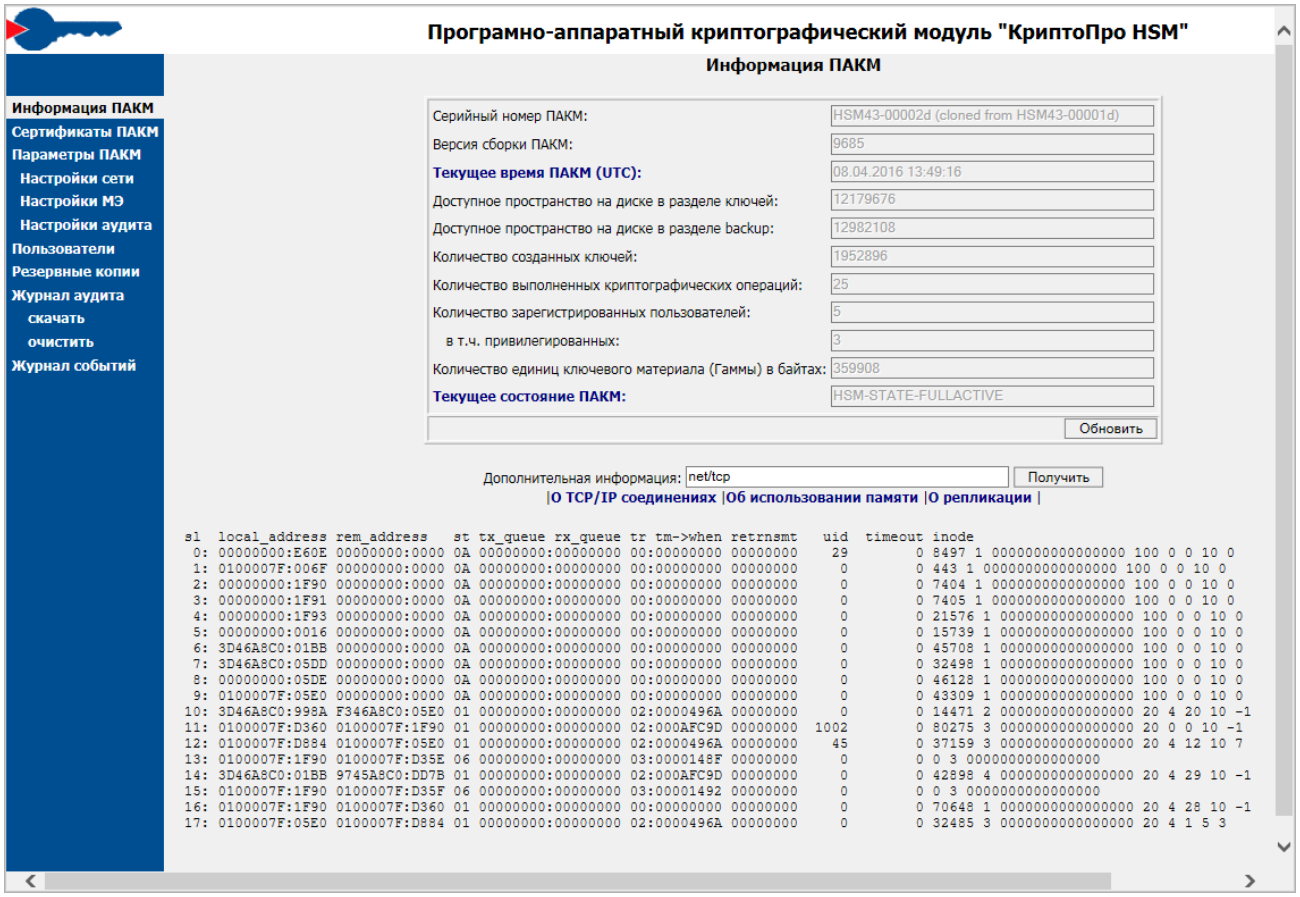


Следует выбрать в выпадающем меню нужное состояние и нажать «**Изменить**», или нажать «**Выход**» для отказа от изменения состояния.

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

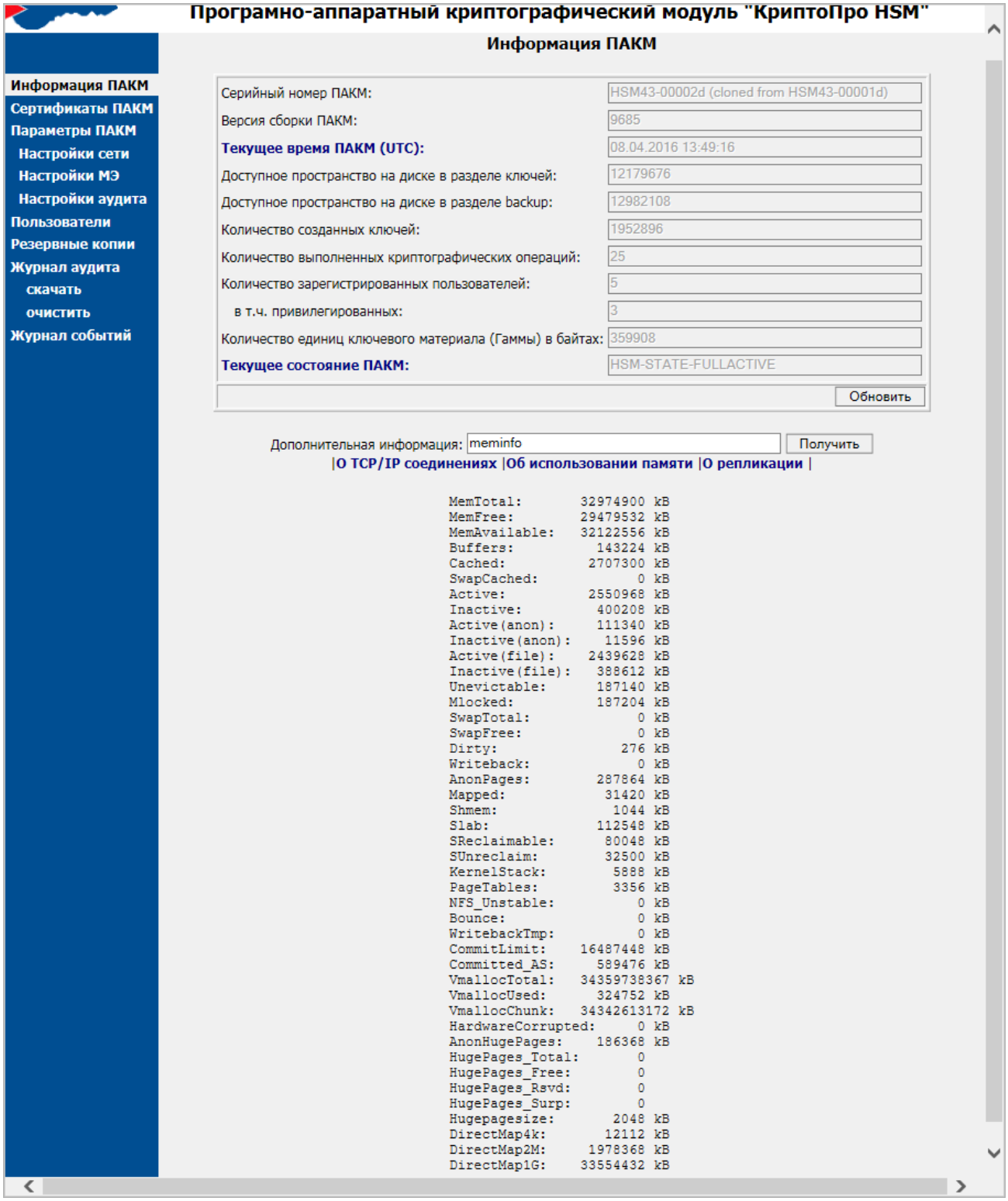
Если изменить состояние на HSM-STATE-INACTIVE, дальнейшее сетевое администрирование будет невозможно.

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



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**»:



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 нажать кнопку «Получить». Например, если ввести cpuinfo, то будет выведено содержимое файла /proc/cpuinfo 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

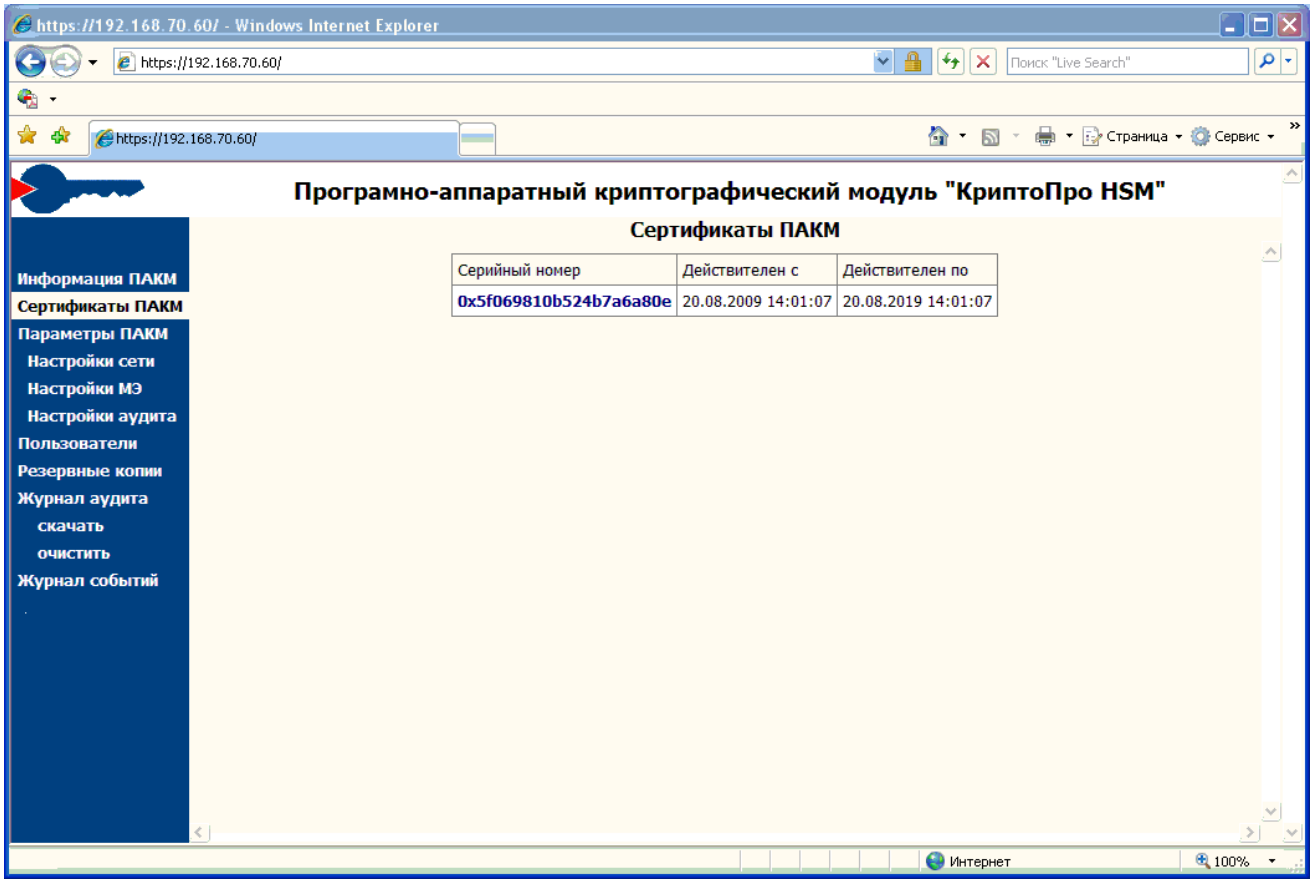
Slave_IO_State	Waiting for master to send event
Master_Host	Localhost
Master_User	Repl
Master_Port	1504
Connect_Retry	60
Master_Log_File	mysql-bin.000047
Read_Master_Log_Pos	78595518
Relay_Log_File	mysql-relay-bin.000040
Relay_Log_Pos	78595664
Relay_Master_Log_File	mysql-bin.000047
Slave_IO_Running	Yes
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.

12.2.2. Сертификаты ПАКМ

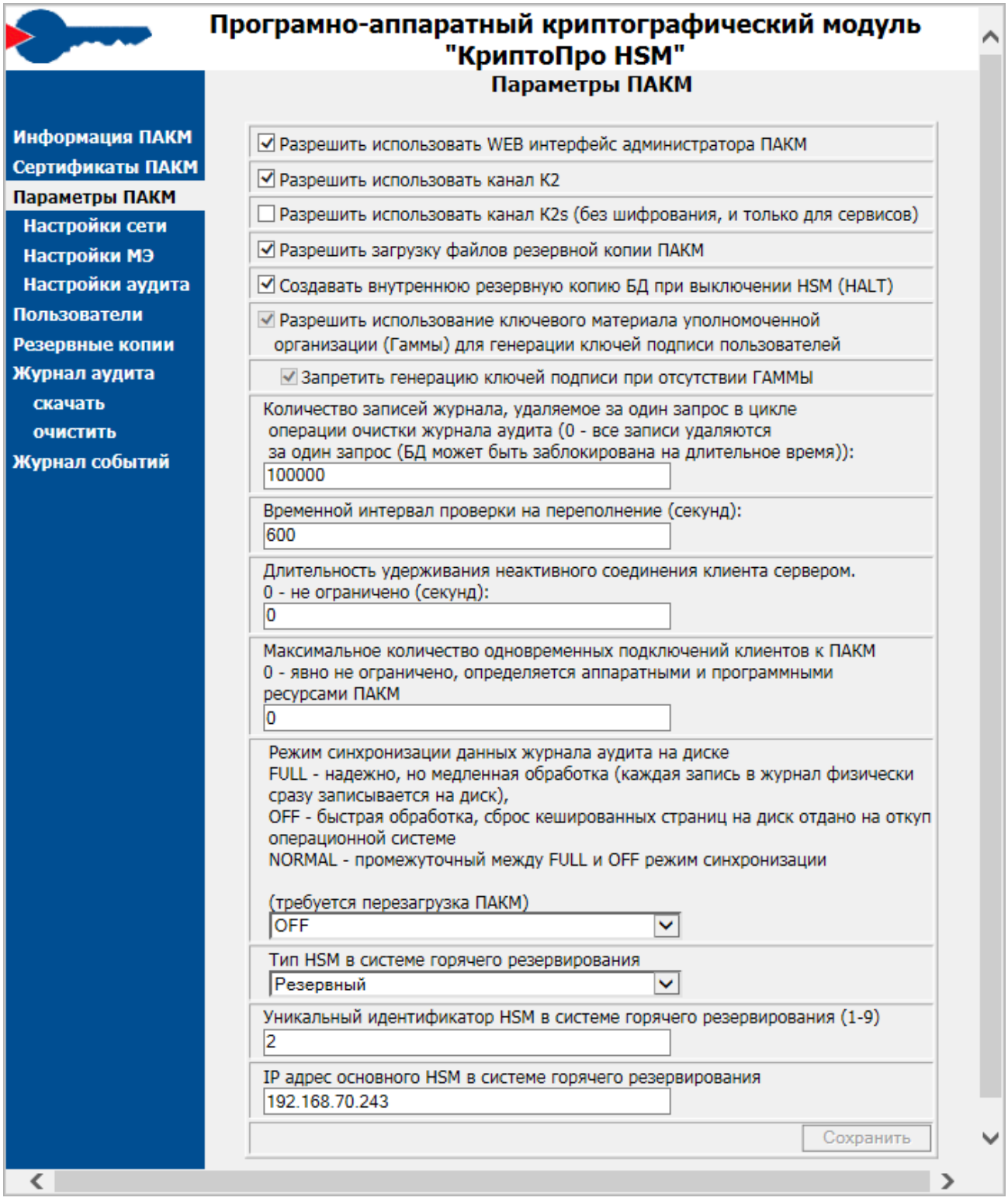
Для просмотра сертификатов ключей подписи ПАКМ (ключей, при помощи которых издаются сертификаты ключей доступа пользователей) надо выбрать в меню слева пункт «Сертификаты ПАКМ».



Для просмотра сертификата надо щелкнуть мышью на серийном номере сертификата. После этого появится стандартное окно просмотра сертификата в Windows (для него должен быть установлен компонент Microsoft CAPICOM, включенный в дистрибутив).

12.2.3. 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.



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.

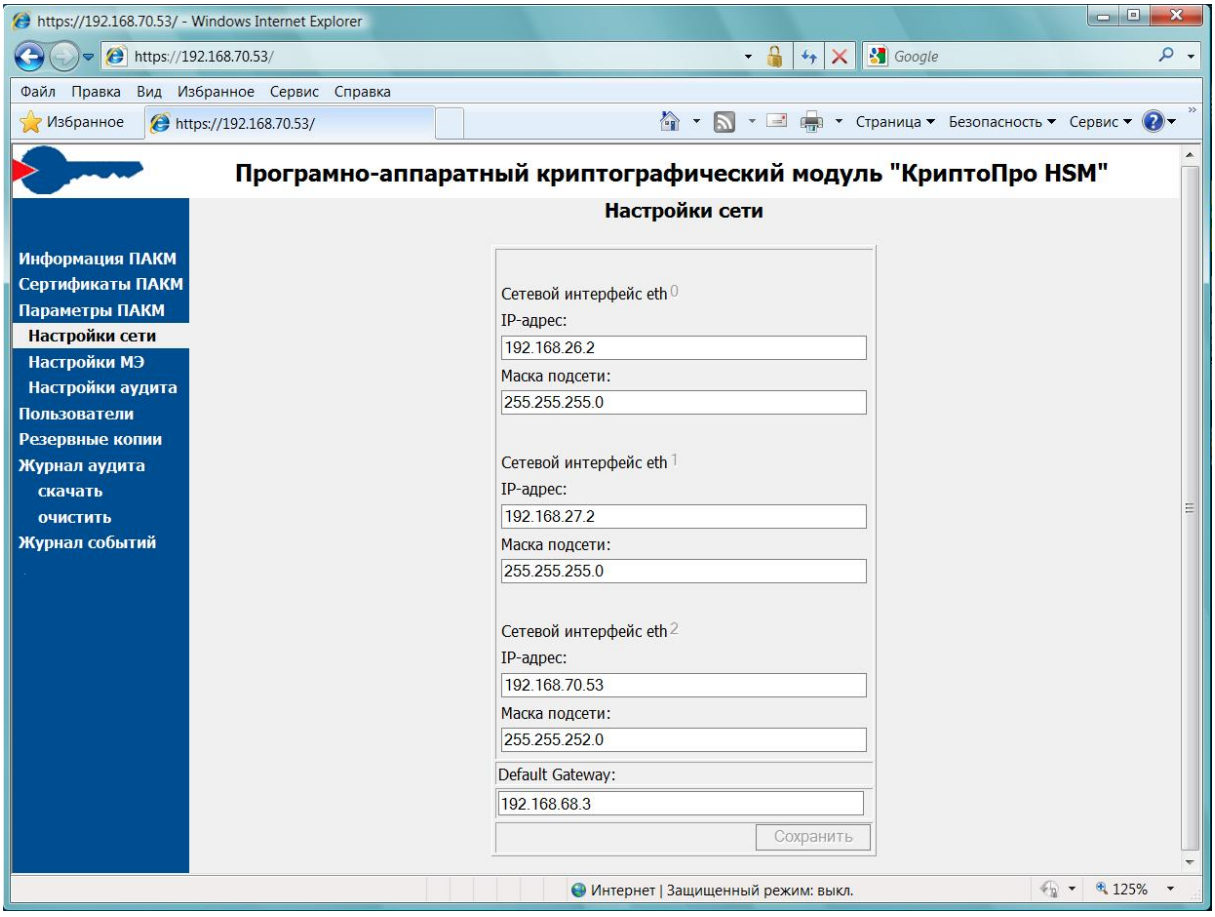
Остальные опции, присутствующие на данном экране, дублируют опции, описанные в п. 11.2.9.

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.

12.2.4. 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.



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

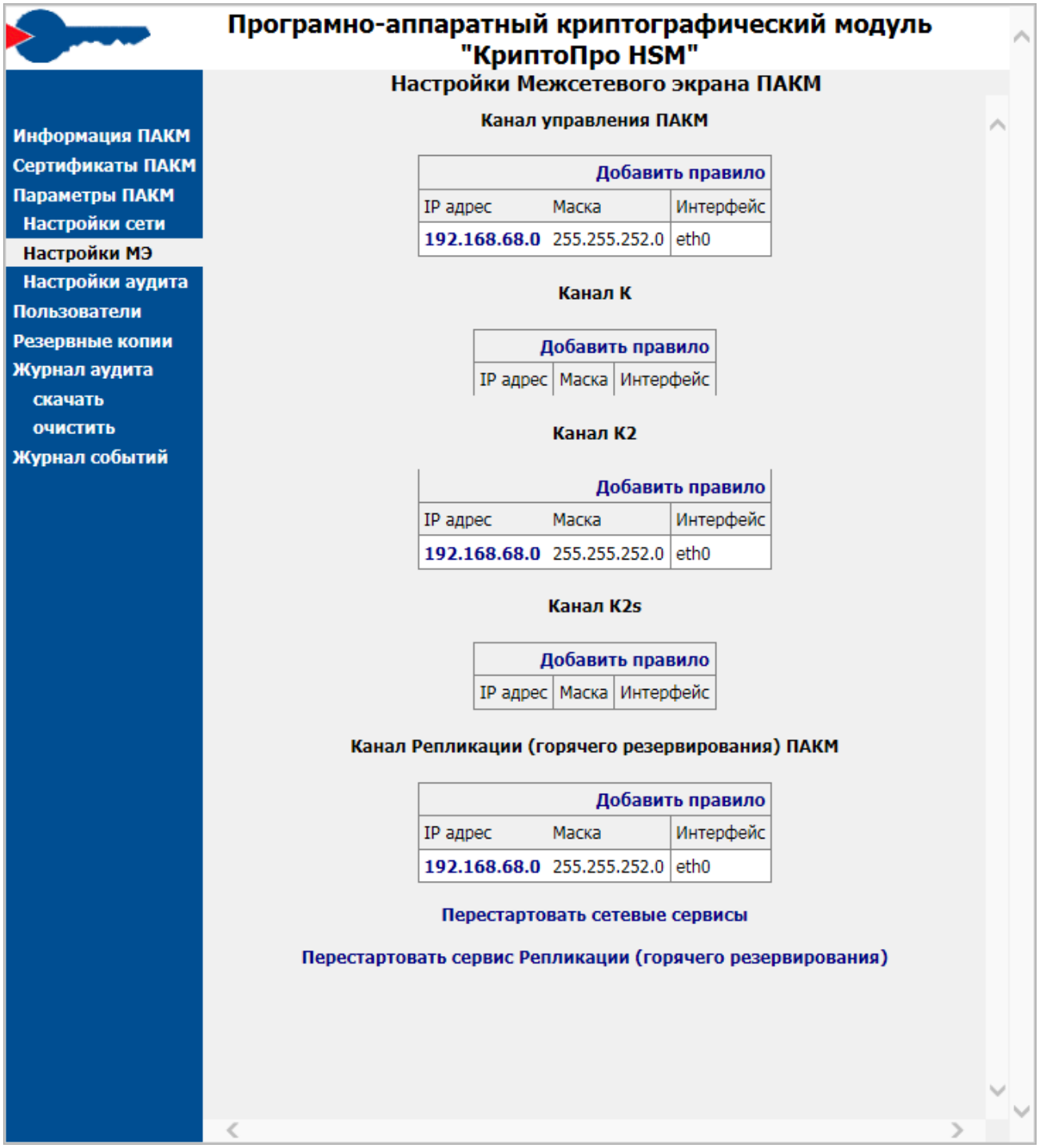
Можно изменить следующие параметры сетевых настроек для каждого сетевого интерфейса: IP-адрес ПАКМ и маску подсети для ПАКМ.

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

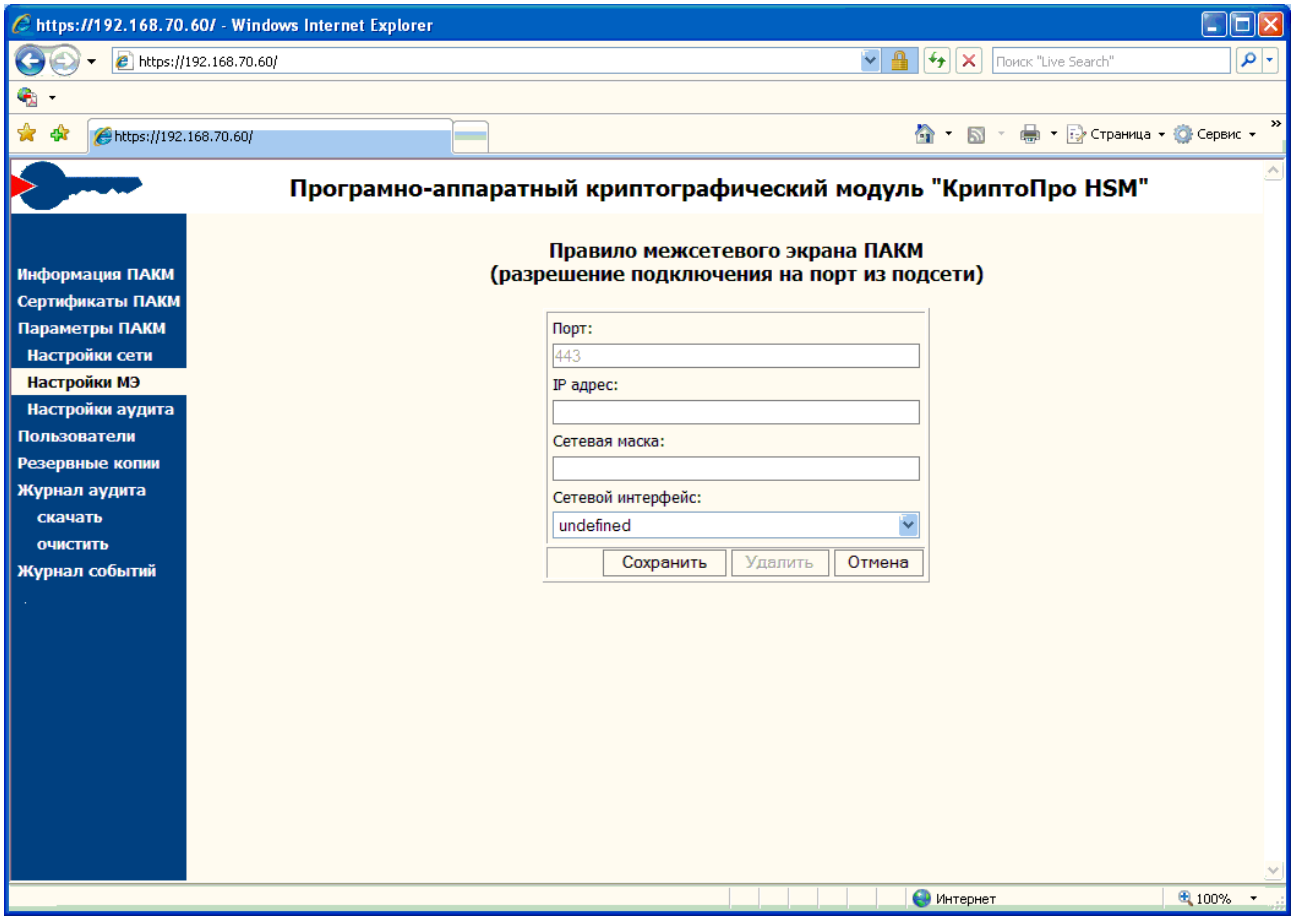
Новые настройки сети вступят в силу после перезапуска сетевых сервисов. Для перезапуска надо перейти на форму «Настройки межсетевого экрана» и щелкнуть мышью на строке «**Перестартовать сетевые сервисы**».

12.2.5. 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.

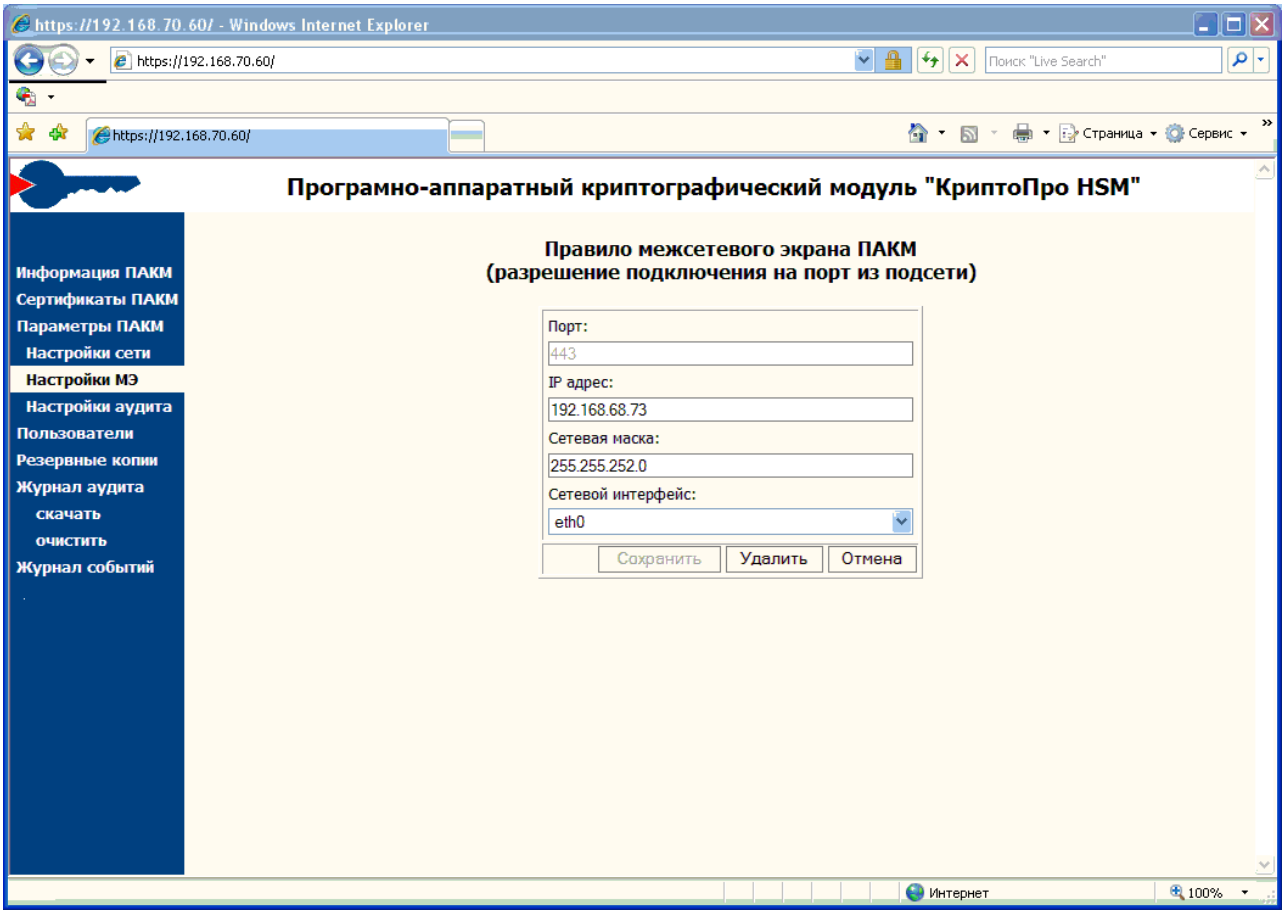


Для добавления нового правила для канала надо щелкнуть мышью на строке «**Добавить правило**». Затем появится форма для редактирования правила:



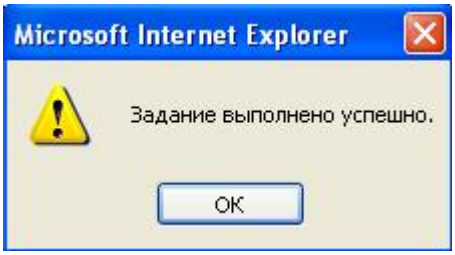
Следует ввести адрес и маску и нажать «**Сохранить**». После этого изменение сетевых настроек будет принято.

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



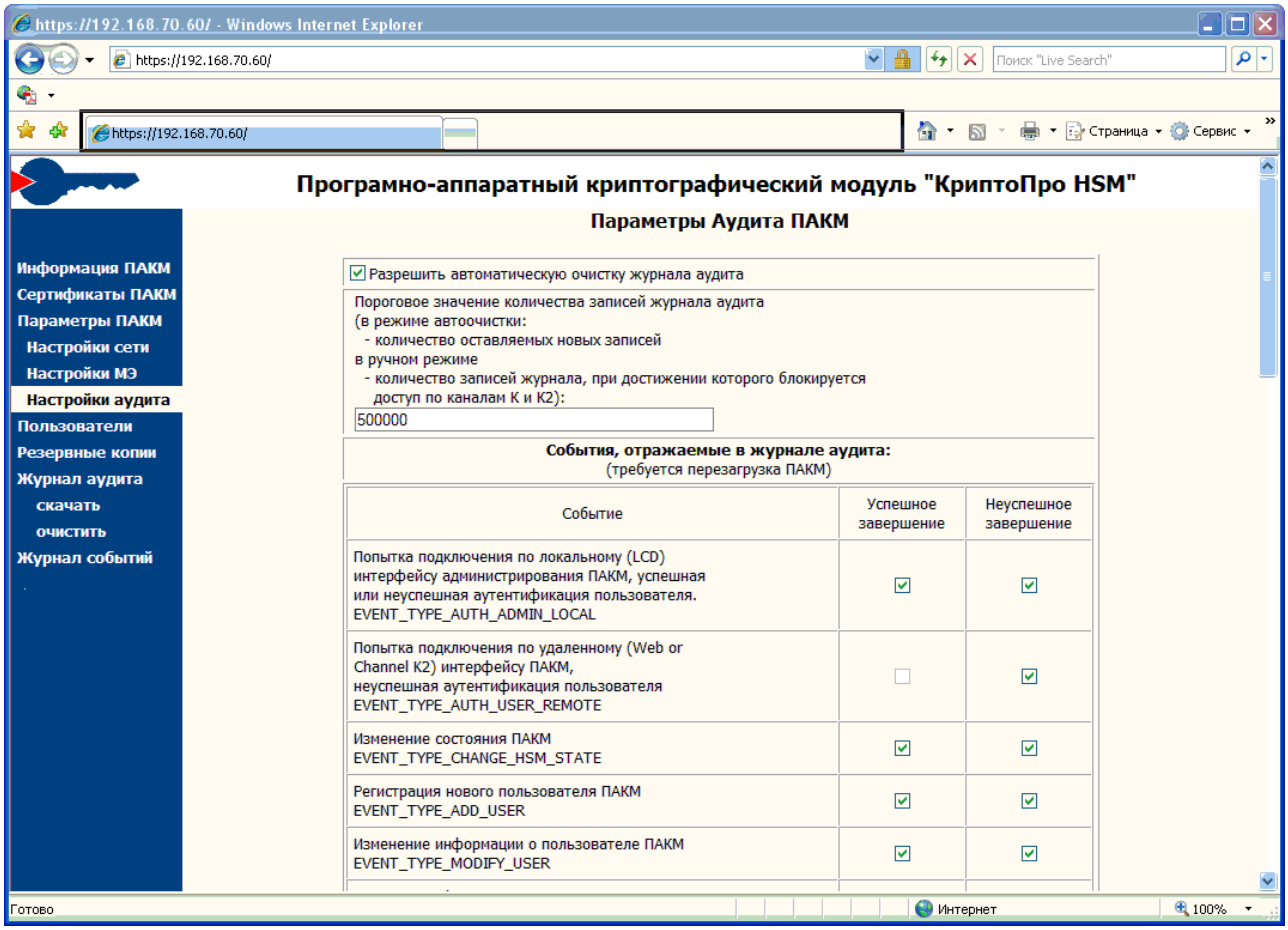
Для удаления правила надо нажать «**Удалить**», для изменения надо отредактировать адрес и маску и нажать «**Сохранить**».

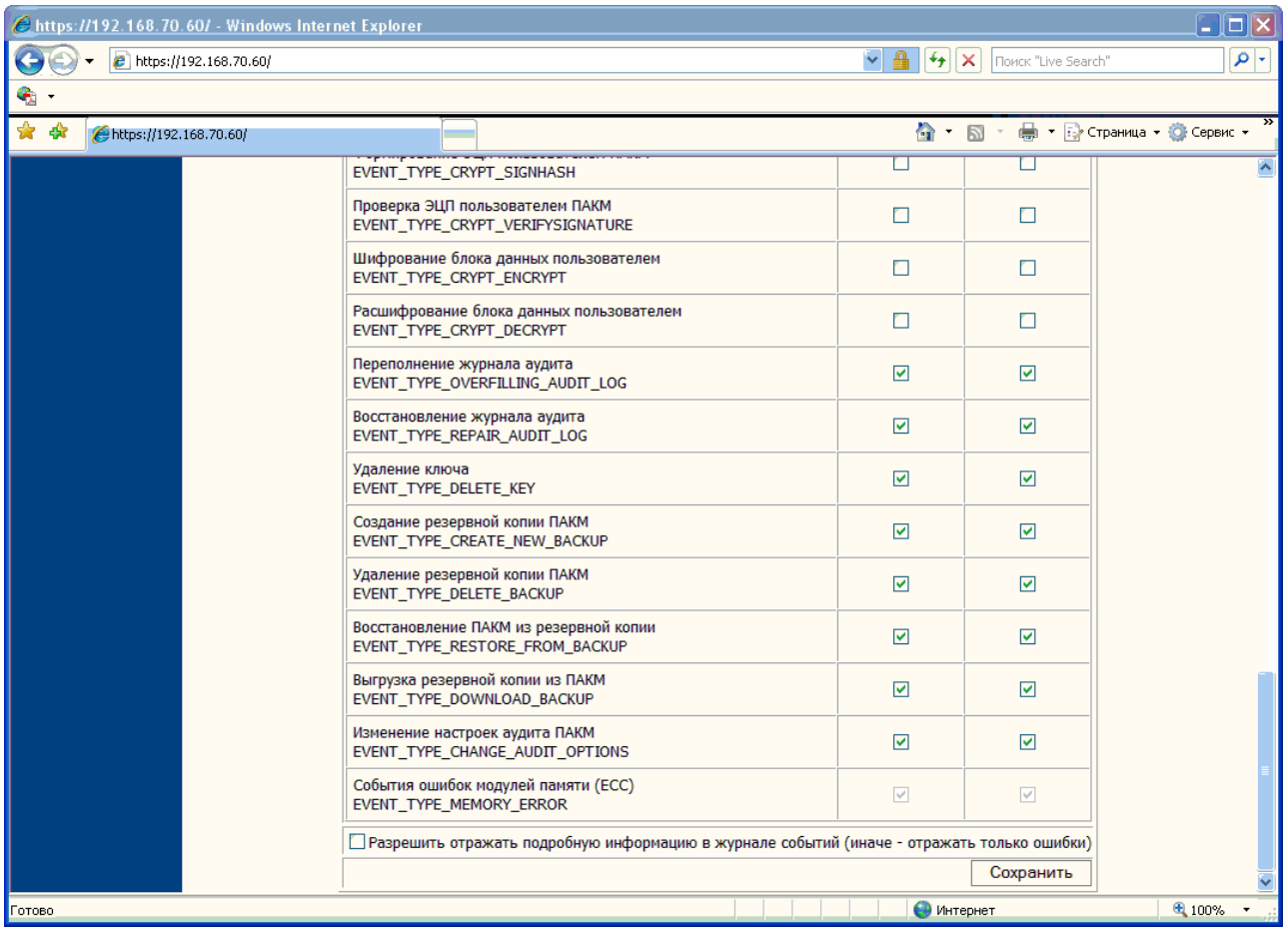
Новые настройки межсетевого экрана вступят в силу после перезапуска межсетевого экрана. Для перезапуска надо щелкнуть мышью на строке «Перестартовать сетевые сервисы» и дождаться сообщения «Задание выполнено успешно»:



12.2.6. 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://192.168.70.60/ - Windows Internet Explorer
https://192.168.70.60/
Программно-аппаратный криптографический модуль "КриптоПро HSM"
Параметры Аудита ПАКМ
Информация ПАКМ
Сертификаты ПАКМ
Параметры ПАКМ
Настройки сети
Настройки МЭ
Настройки аудита
Пользователи
Резервные копии
Журнал аудита
скачать
очистить
Журнал событий
Разрешить автоматическую очистку журнала аудита
Пороговое значение количества записей журнала аудита
(в режиме автоочистки:
- количество оставляемых новых записей
в ручном режиме
- количество записей журнала, при достижении которого блокируется
доступ по каналам К и К2):
500000
События, отражаемые в журнале аудита:
(требуется перезагрузка ПАКМ)
Событие
Успешное завершение
Неуспешное завершение
Попытка подключения по локальному (LCD) интерфейсу администрирования ПАКМ, успешная или неуспешная аутентификация пользователя. EVENT_TYPE_AUTH_ADMIN_LOCAL
Попытка подключения по удаленному (Web or Channel K2) интерфейсу ПАКМ, неуспешная аутентификация пользователя EVENT_TYPE_AUTH_USER_REMOTE
Изменение состояния ПАКМ EVENT_TYPE_CHANGE_HSM_STATE
Регистрация нового пользователя ПАКМ EVENT_TYPE_ADD_USER
Изменение информации о пользователе ПАКМ EVENT_TYPE_MODIFY_USER
Готово
Интернет
100%

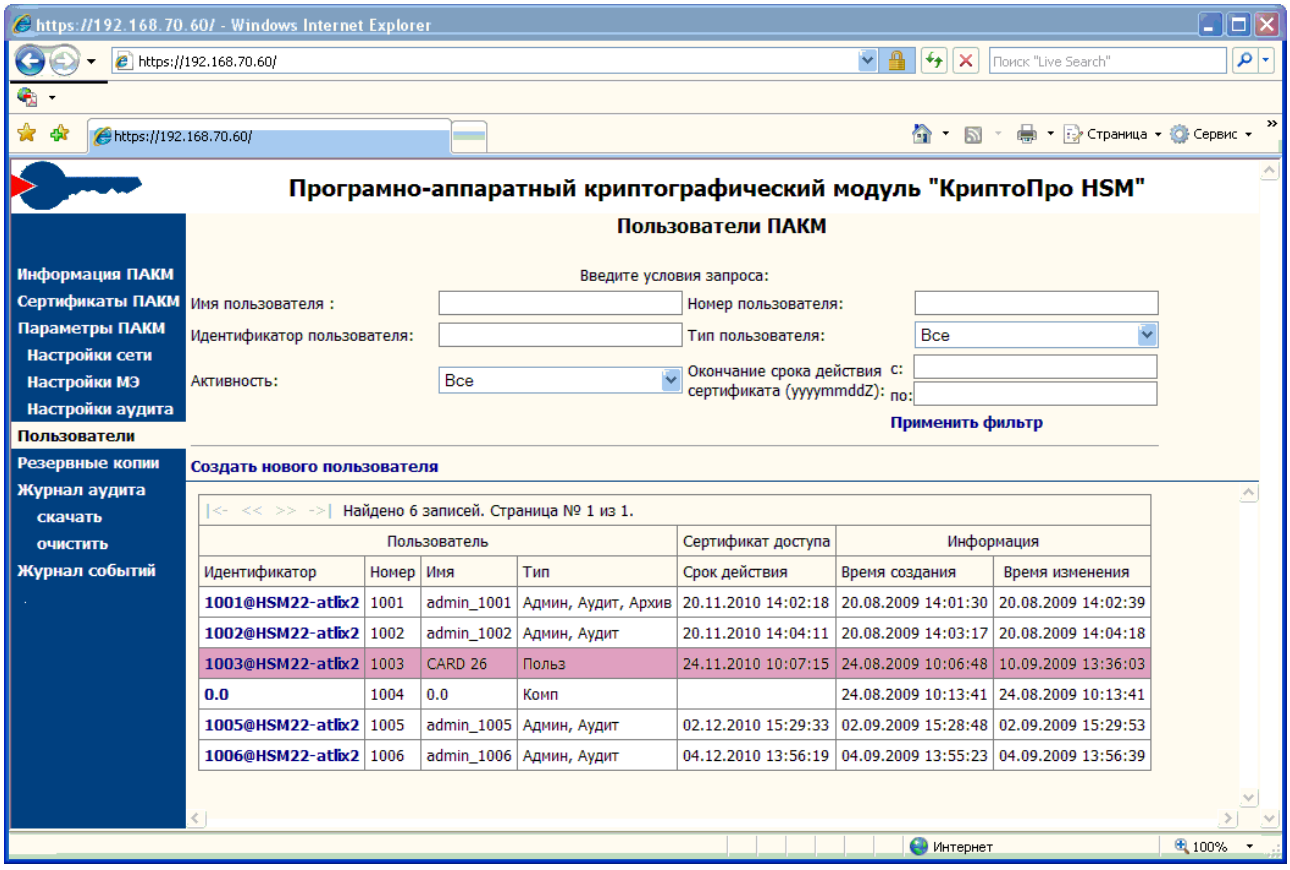

https://192.168.70.60/ - Windows Internet Explorer
https://192.168.70.60/
EVENT_TYPE_CRYPT_SIGNHASH
Проверка ЭЦП пользователем ПАКМ EVENT_TYPE_CRYPT_VERIFYSIGNATURE
Шифрование блока данных пользователем EVENT_TYPE_CRYPT_ENCRYPT
Расшифрование блока данных пользователем EVENT_TYPE_CRYPT_DECRYPT
Переполнение журнала аудита EVENT_TYPE_OVERFILLING_AUDIT_LOG
Восстановление журнала аудита EVENT_TYPE_REPAIR_AUDIT_LOG
Удаление ключа EVENT_TYPE_DELETE_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
Изменение настроек аудита ПАКМ EVENT_TYPE_CHANGE_AUDIT_OPTIONS
События ошибок модулей памяти (ECC) EVENT_TYPE_MEMORY_ERROR
Разрешить отражать подробную информацию в журнале событий (иначе - отражать только ошибки)
Сохранить
Готово
Интернет
100%

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 заново переактивировать ПАКМ.

12.2.7. Пользователи

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

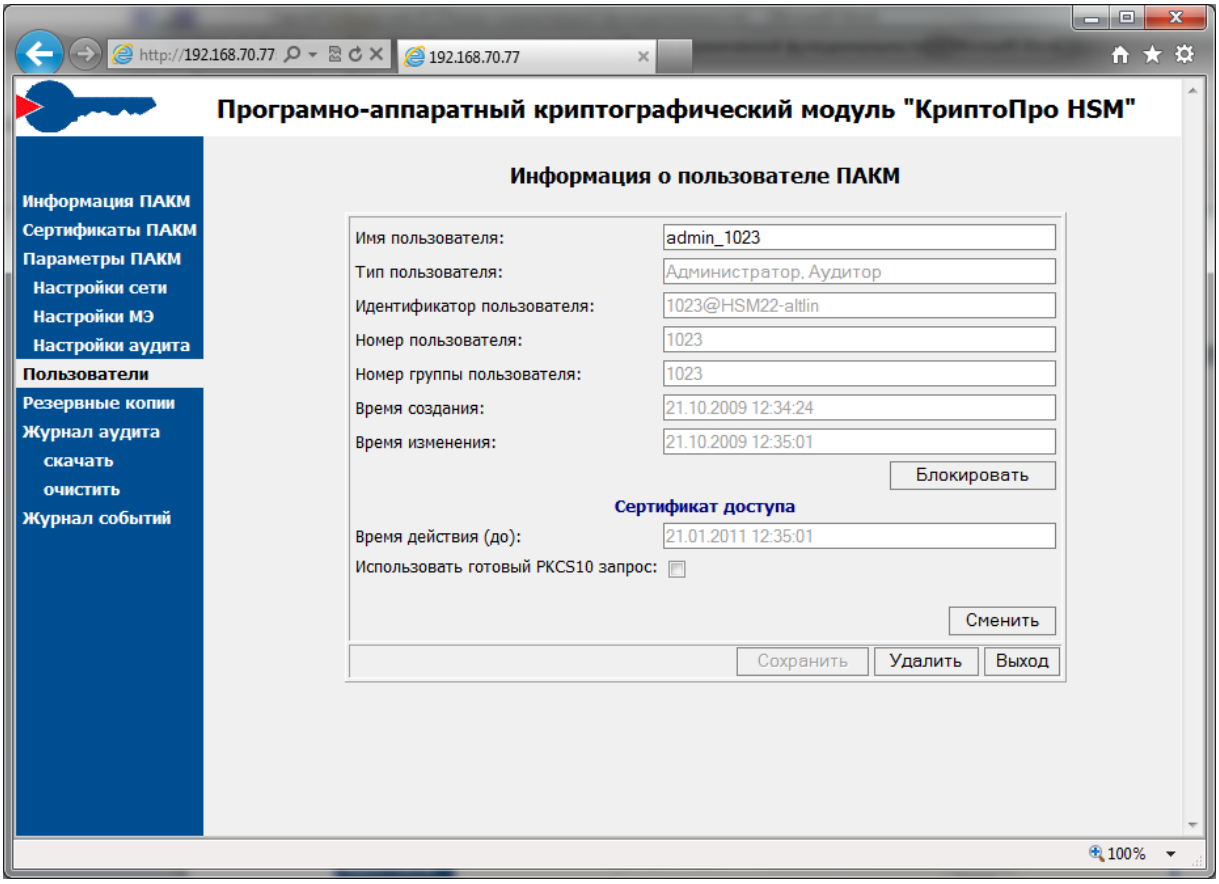


В форме имеется таблица со списком всех зарегистрированных в ПАКМ пользователей. В таблице указаны идентификатор пользователя, номер пользователя (UID), имя и тип пользователя, срок действия сертификата, время создания информации (по UTC) о пользователе и время ее последнего изменения. Выделение розовым 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

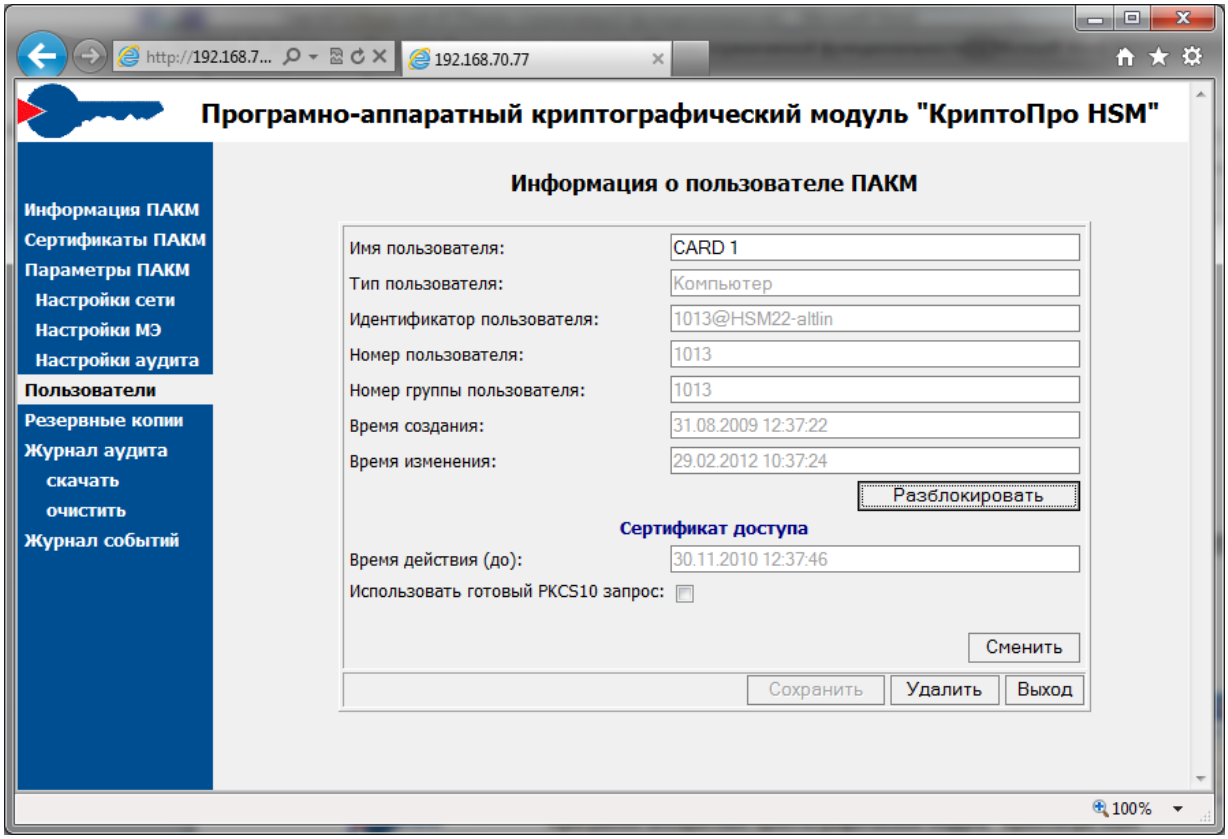
требуется просмотреть весь список, надо очистить условия запроса и применить фильтр снова.

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

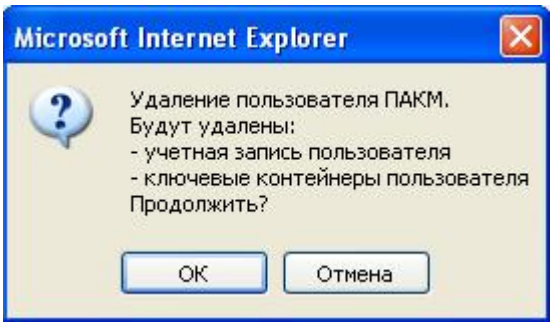


Для возврата к форме просмотра пользователей надо нажать «**Выход**».

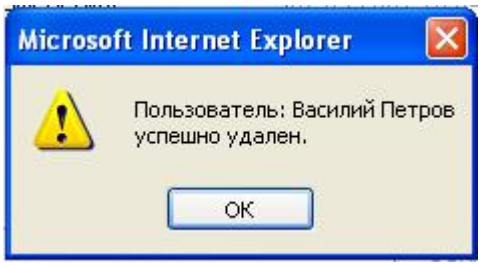
Для изменения имени пользователя надо откорректировать значение поля «**Имя пользователя**». После этого кнопка «**Сохранить**» станет активной, и для сохранения имени пользователя надо ее нажать. Для блокирования пользователя надо нажать кнопку «**Блокировать**». Если пользователь блокирован, надо нажать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



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



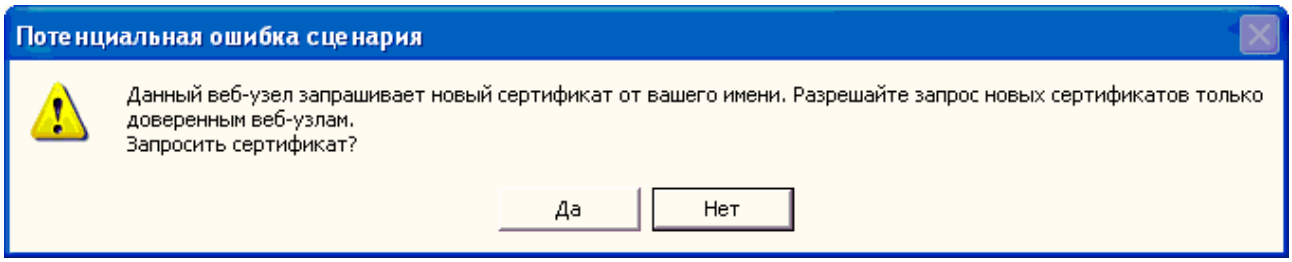
Если нажать «**OK**», пользователь будет удален, о чем появится сообщение:



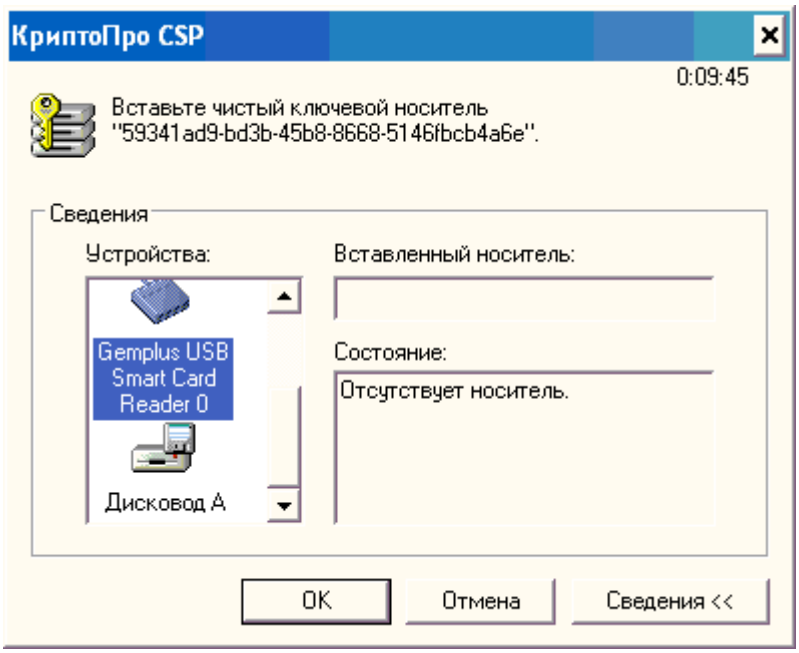
Для просмотра сертификата доступа надо щелкнуть мышью на строке «**Сертификат доступа**». После этого появится стандартное окно просмотра сертификата в Windows.

Для смены сертификата надо нажать кнопку «**Сменить**».

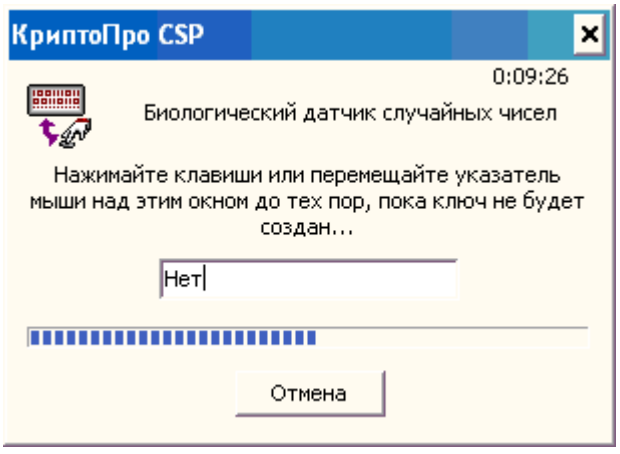
При этом, если не указана опция «Использовать готовый PKCS10 запрос», то вначале будет создана ключевая пара (закрытый и открытый ключ доступа):



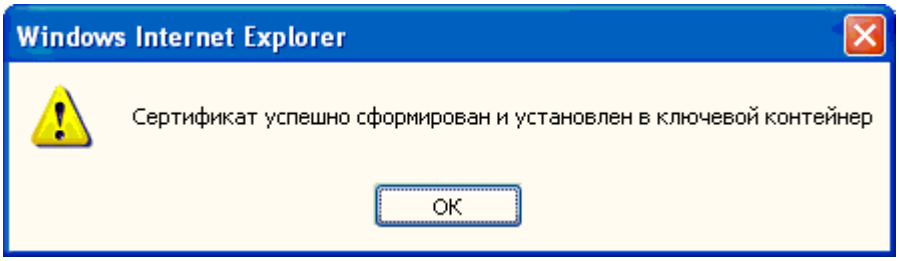
Если нажать «ДА», появится приглашение выбрать устройство для считывания и вставить ключевой носитель:



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.

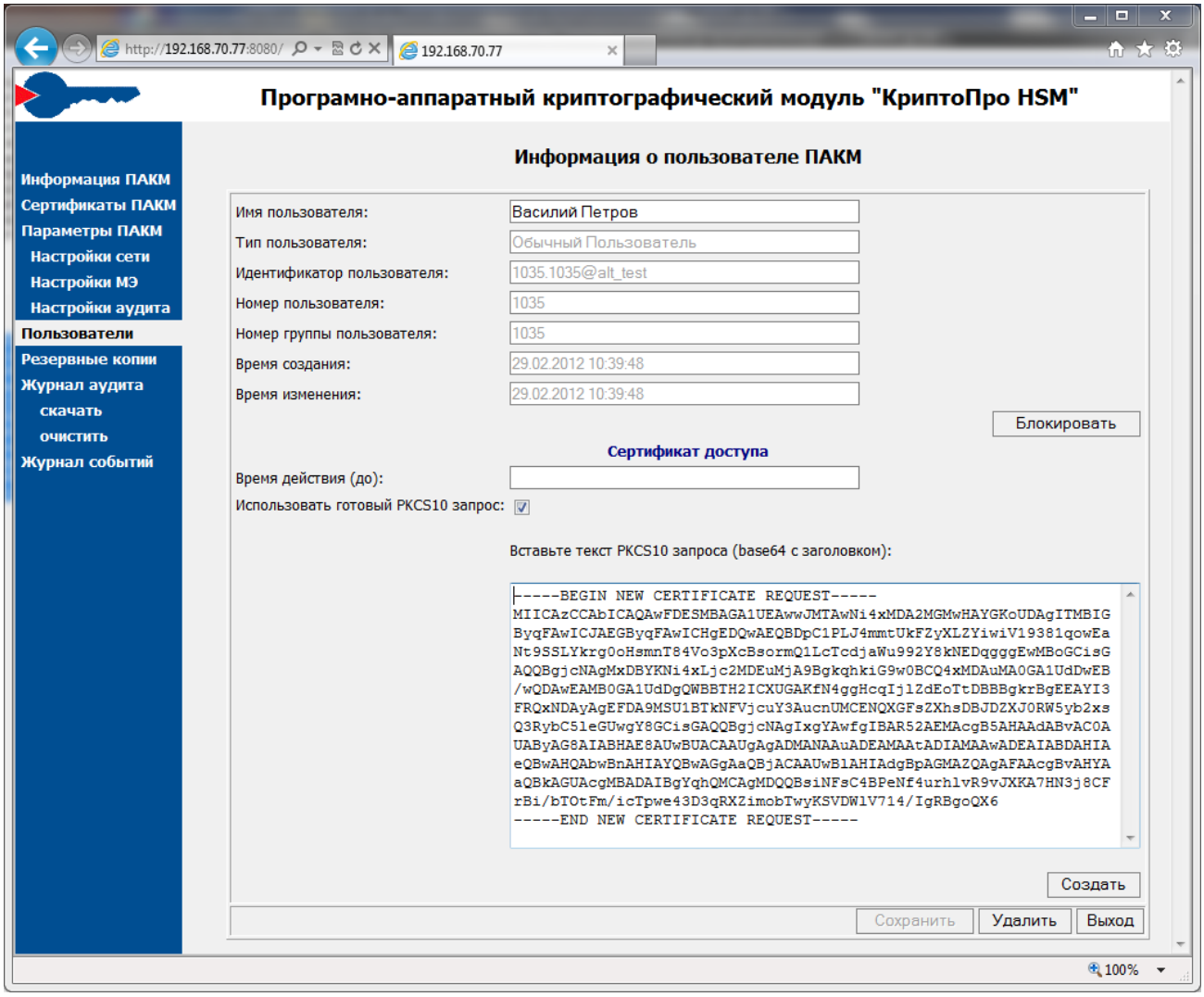


После создания ключа окно закроется. После этого новый сертификат будет создан, о чем появится сообщение:



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:

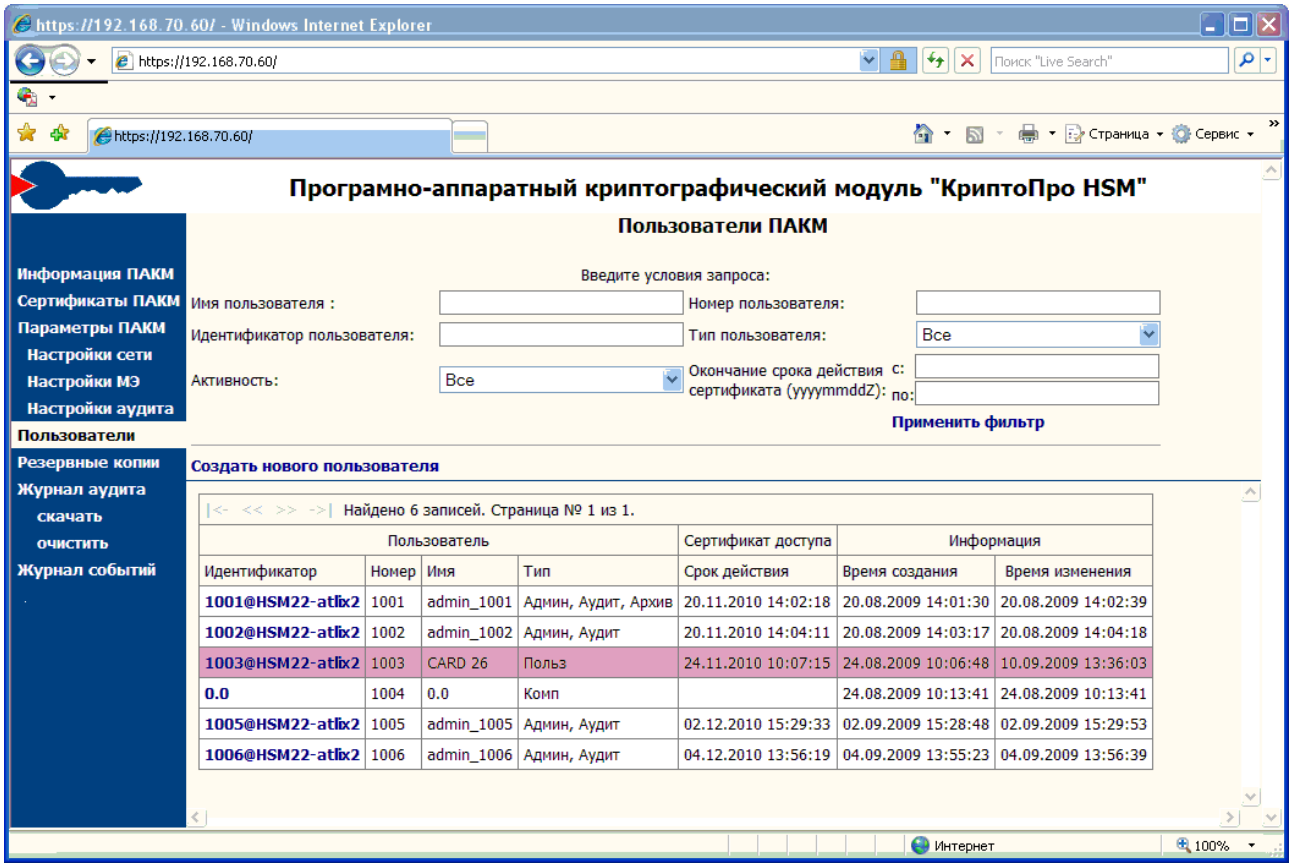


После вставки запроса необходимо нажать кнопку «Создать» (или «Обновить», если производится смена сертификата).

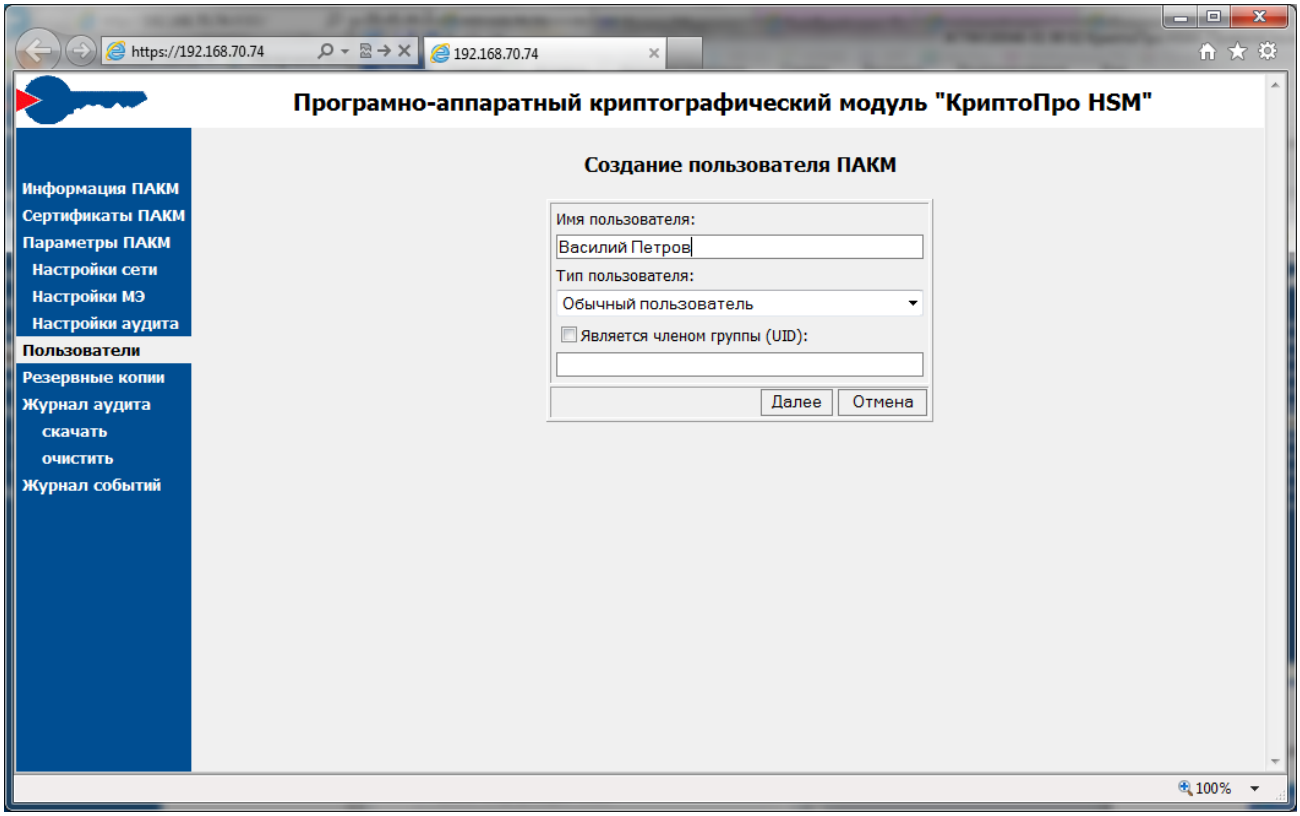
При этом важно, чтобы запрос содержал отличительное имя субъекта (Subject DN) в виде «CN=UUUU.GGGG», где UUUU – «номер пользователя», а GGGG – «номер группы пользователя», для которого производится создание/обновление сертификата. Использовать в запросе какие-либо расширения бессмысленно, т.к. ПАКМ «КриптоПро 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 «**Создать нового пользователя**»:

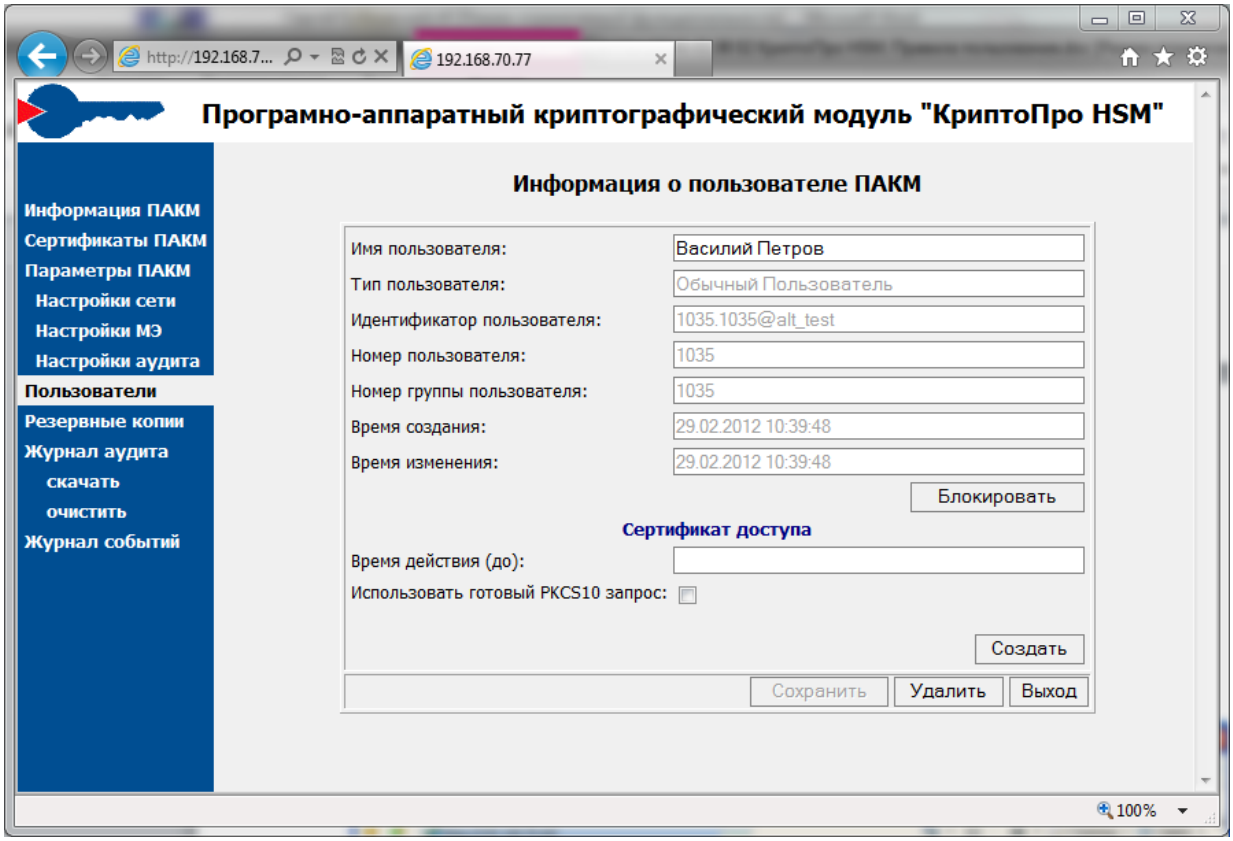


В появившейся форме надо ввести имя и тип пользователя (обычный пользователь или компьютер (администратор сервера)):



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

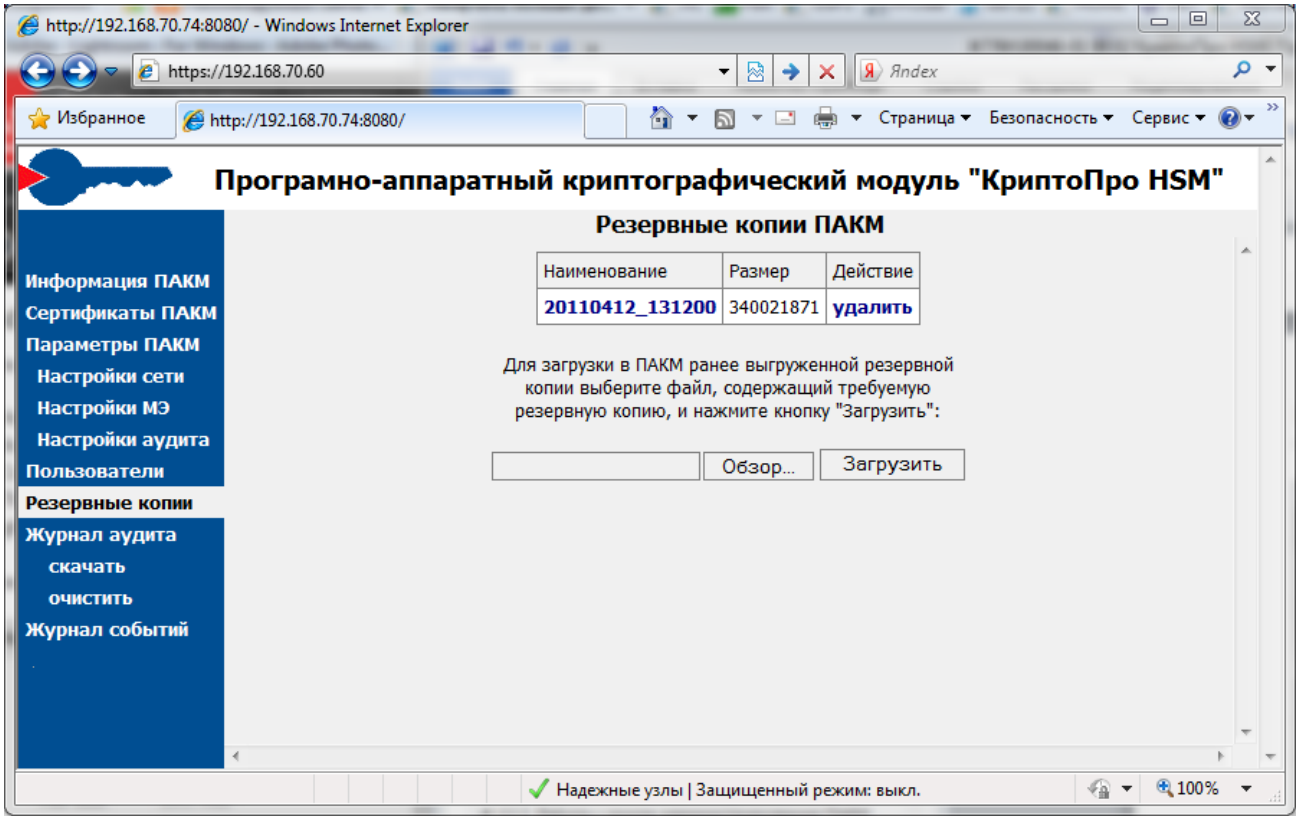
Затем надо нажать кнопку «**Далее**». После этого пользователь будет создан, и появится форма с информацией о пользователе:



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

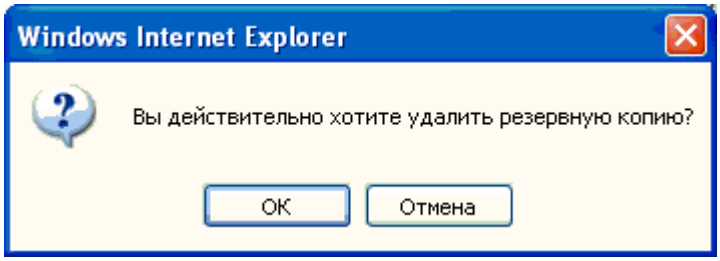
12.2.8. Резервные копии

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.

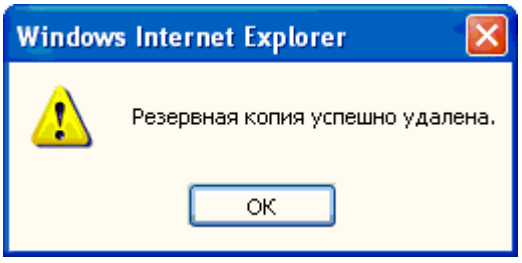


Если требуется выгрузить резервную копию, надо щелкнуть мышью на наименовании копии. После этого появится стандартное окно Windows для скачивания файлов.

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



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



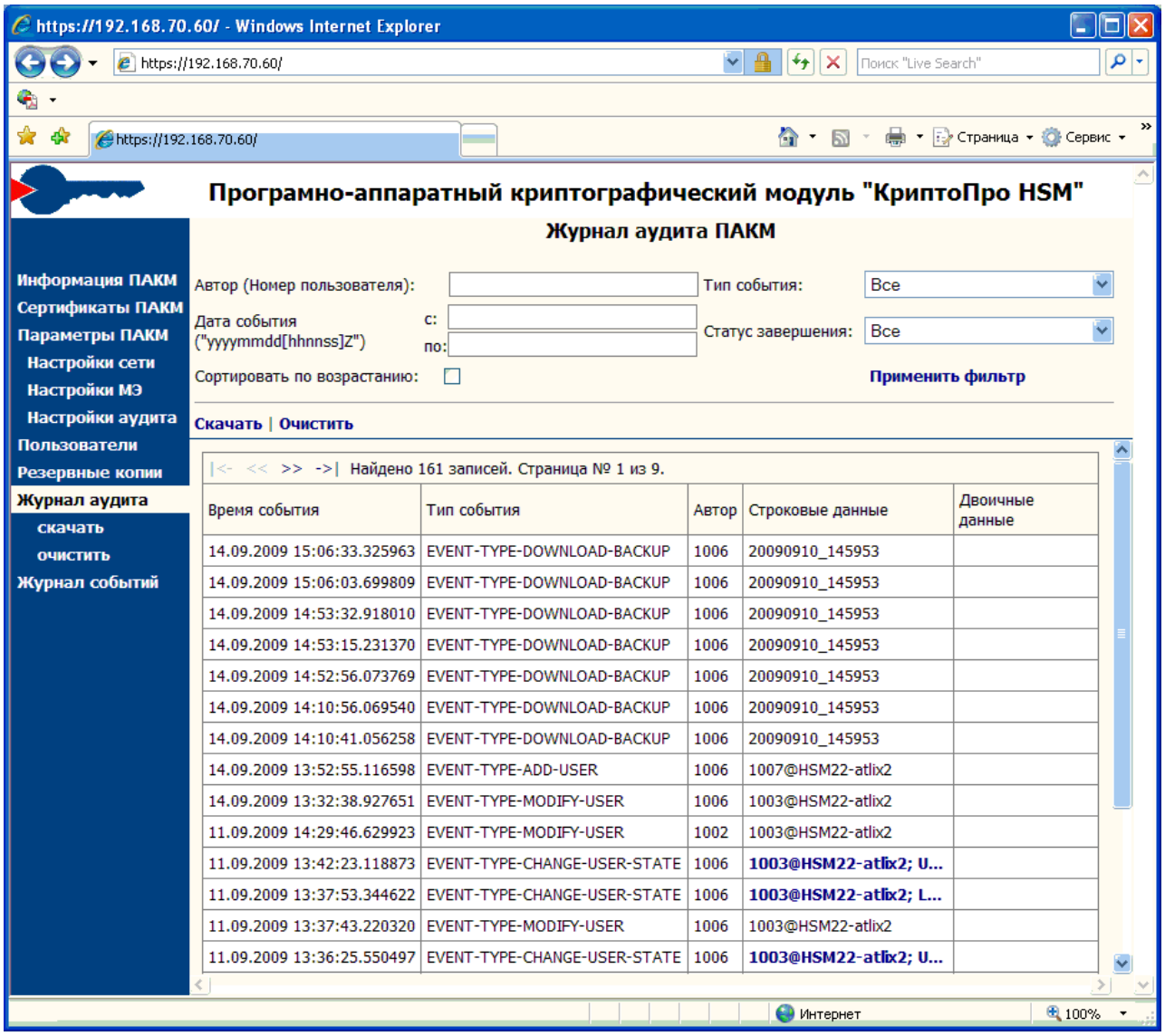
Для загрузки ранее выгруженной из ПАКМ резервной копии необходимо выбрать файл, содержащий данную копию (используйте для этого кнопку «Обзор…»), после чего нажать

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».

12.2.9. 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.



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);

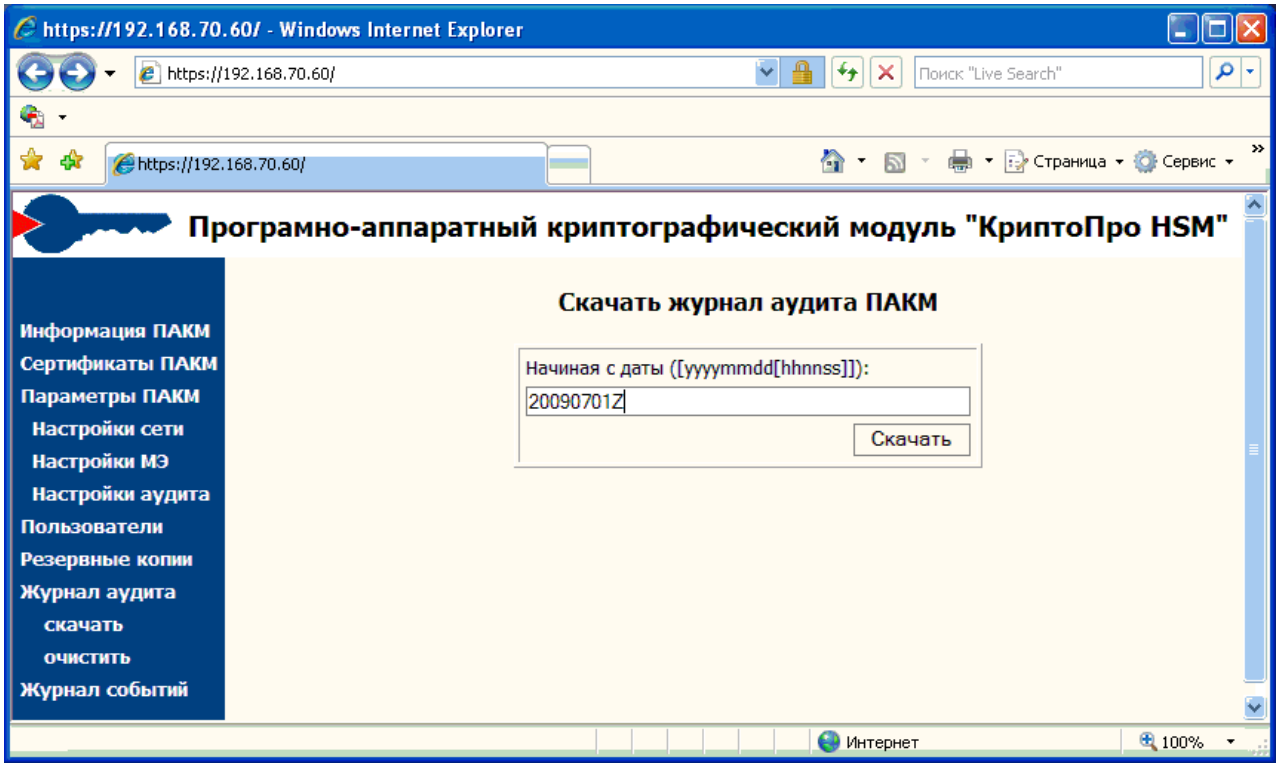
DD – день события (1-31);

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

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

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

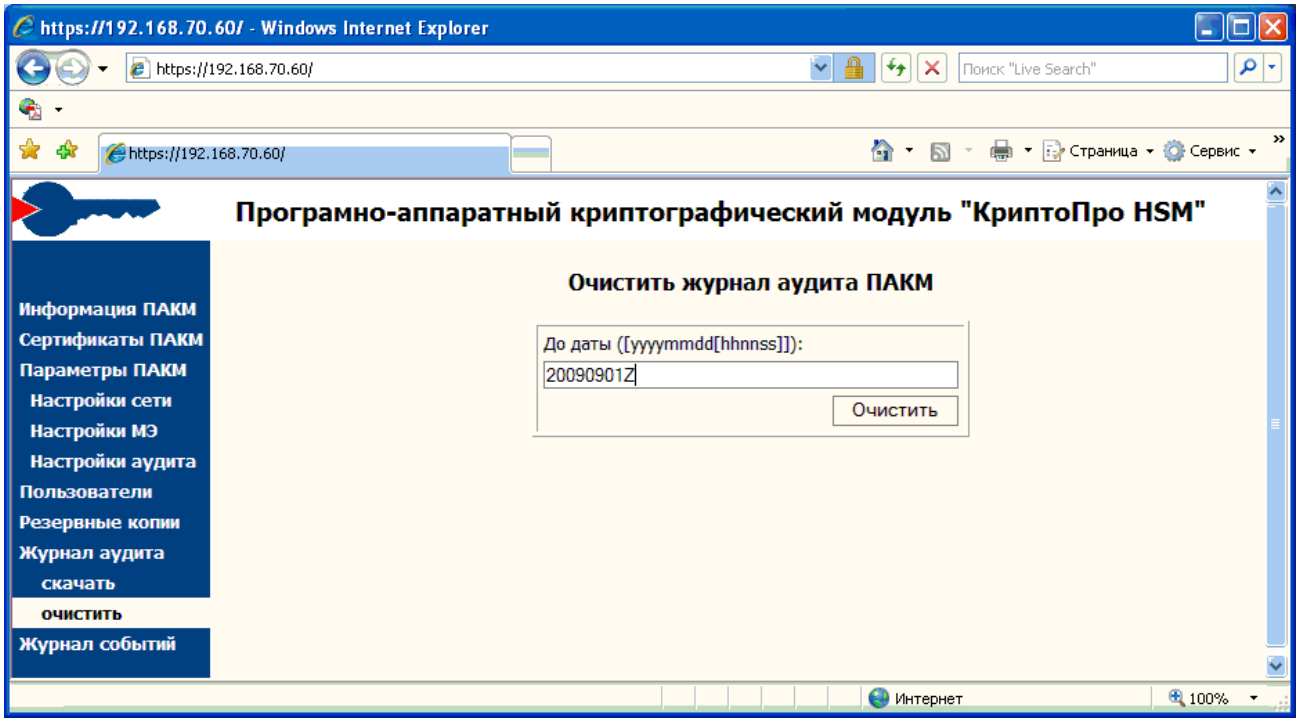
Z – завершающий символ в обозначении generalizedTime, указывается опционально.



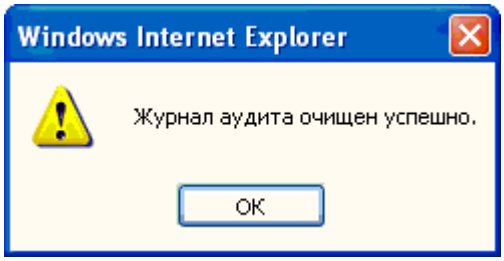
После ввода даты надо нажать кнопку **«Скачать»** или выбрать пункт «скачать» в меню слева. Затем последует стандартное сообщение Windows с предупреждением о загрузке файла, и окно, в котором надо ввести имя и тип сохраняемого файла.

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

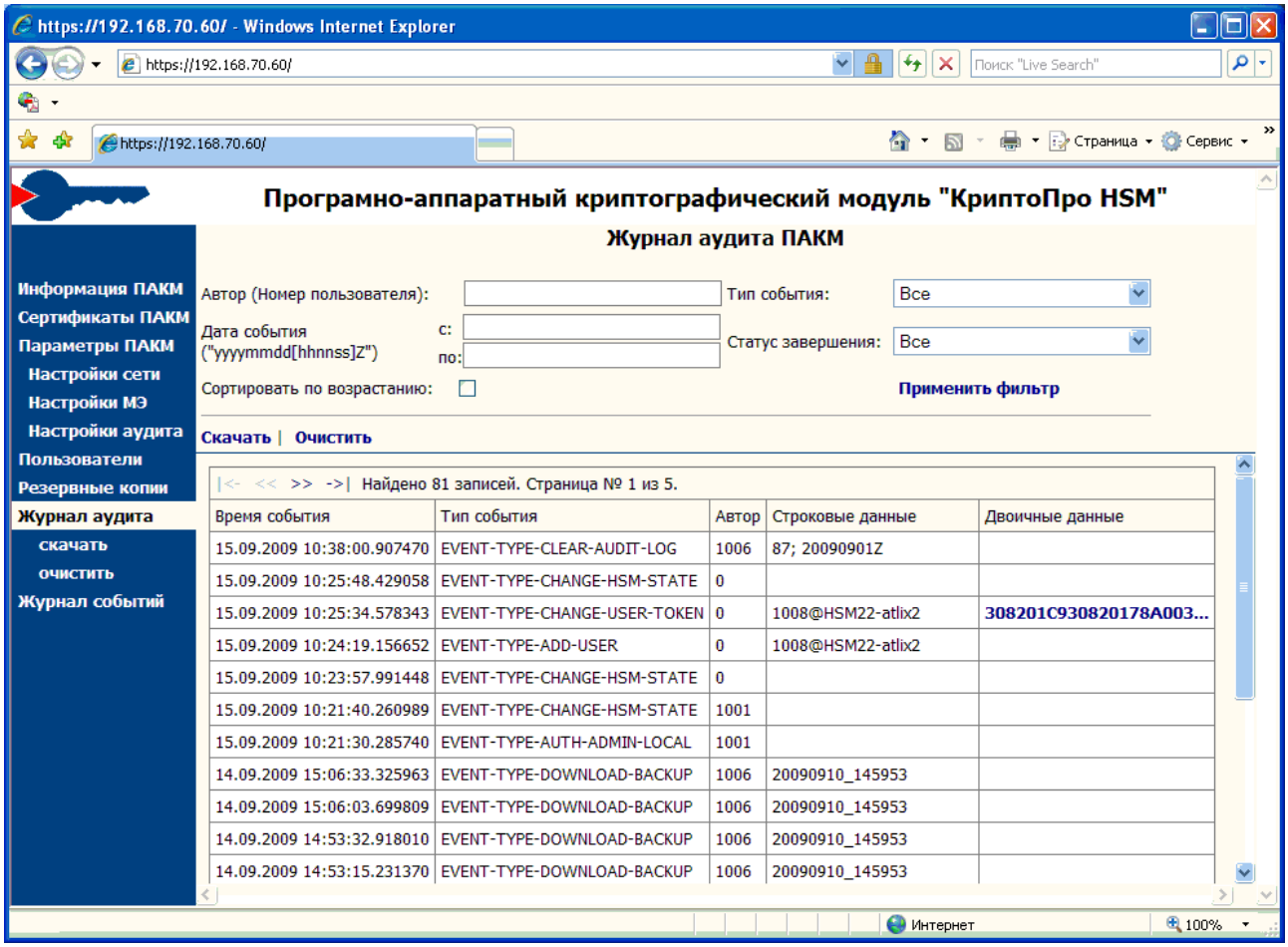
Если требуется очистить журнала аудита, надо щелкнуть мышью на строке «**Очистить**», или выбрать пункт «очистить» в меню слева. В появившейся форме надо ввести дату и время, до которого список событий будет очищен. Если поле оставить пустым, журнал будет очищен целиком.



Если нажать «Очистить», журнал аудита будет очищен, о чем появится сообщение:

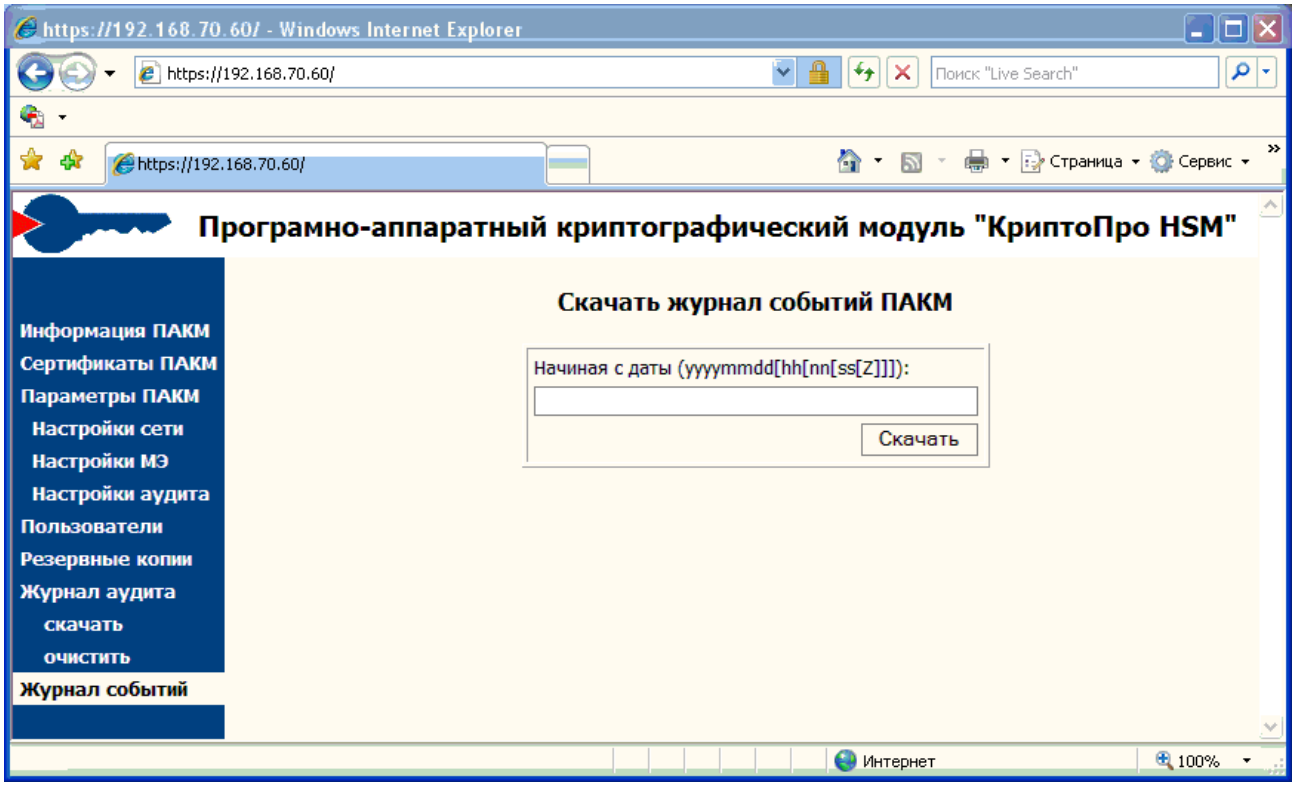


После обновления списка записей (для этого надо использовать «Применить фильтр») в списке будет присутствовать запись об очистке журнала (тип события EVENT-TYPE-CLEAR-AUDIT-LOG):



12.2.10. 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.



После ввода даты надо нажать кнопку **«Скачать»**. Затем последует стандартное сообщение Windows с предупреждением о загрузке файла, и окно, в котором надо ввести имя и тип сохраняемого файла.

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 IE).

13. ПОРЯДОК ВЫПОЛНЕНИЯ ТЕХНИЧЕСКОГО ОБСЛУЖИВАНИЯ И РЕМОНТА ПАКМ

13.1. 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 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.

13.2. 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.