

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 R3 Комплектации 1 и 2 Руководство администратора безопасности
---	---

ЖТЯИ.00096-03 91 01

Листов 43

2023 г.

Содержание

1. Аннотация.....	3
2. Концепция и архитектура компонентов ПАКМ	4
3. Функциональные схемы применения ПАКМ «КриптоПро HSM»	5
3.1. Применение ПАКМ с сервером приложений	5
3.2. Подключение ПАКМ к нескольким серверам	8
3.3. Подключение рабочих станций пользователей к ПАКМ.....	9
3.4. Использование Платежного HSM	11
4. Состав аппаратной платформы и ПО ПАКМ.....	13
4.1. Аппаратная платформа ПАКМ.....	13
4.2. Программное обеспечение ПАКМ.....	14
5. Ролевая модель доступа	15
6. Ключи и сертификаты ПАКМ.....	21
6.1. Ключ активации ПАКМ, защитные ключи	21
6.2. Ключ подписи ПАКМ.....	21
6.3. Самоподписанный сертификат ключа подписи ПАКМ.....	22
6.4. Ключ шифрования ПАКМ	22
6.5. Сессионный ключ канала «K2»	23
6.6. Ключ TLS сервера	23
6.7. Сертификат ключа TLS сервера.....	24
6.8. Ключ аутентификации пользователя	24
6.9. Сертификат ключа аутентификации пользователя	24
6.10. Сертификат ключа аутентификации Администратора	25
6.11. Ключи канала «K»	26
6.12. Ключ подписи журнала аудита.....	26
6.13. Локальный мастер-ключ (LMK).....	27
7. Совместный доступ различных пользователей ПАКМ к общим ключам	28
8. Ведение журналов	29
9. Настройка аудита	31
9.1. База данных и структура записей журнала аудита	33
9.2. Типы событий.....	36
9.3. Анализ журналов аудита	38
10. Нештатные ситуации при эксплуатации СКЗИ	39
Приложение 1. Акт готовности к работе	41
Приложение 2. Журнал регистрации администраторов безопасности и пользователей.....	42
Приложение 3. Журнал пользователя сети.....	43

1. АННОТАЦИЯ

Настоящий документ содержит инструкции по обеспечению информационной безопасности при эксплуатации программно-аппаратного криптографического модуля (ПАКМ) «КриптоПро HSM» совместно с серверами и рабочими станциями пользователей, использующими криптографические функции ПАКМ.

Данный документ предназначен для администратора безопасности Сервера, сетевых ресурсов предприятия и других работников службы информационной безопасности.

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

2. КОНЦЕПЦИЯ И АРХИТЕКТУРА

КОМПОНЕНТОВ ПАКМ

Общую схему компонент среды функционирования ПАКМ (СФ) можно представить на следующих диаграммах (см. Рис. 1, Рис. 2).

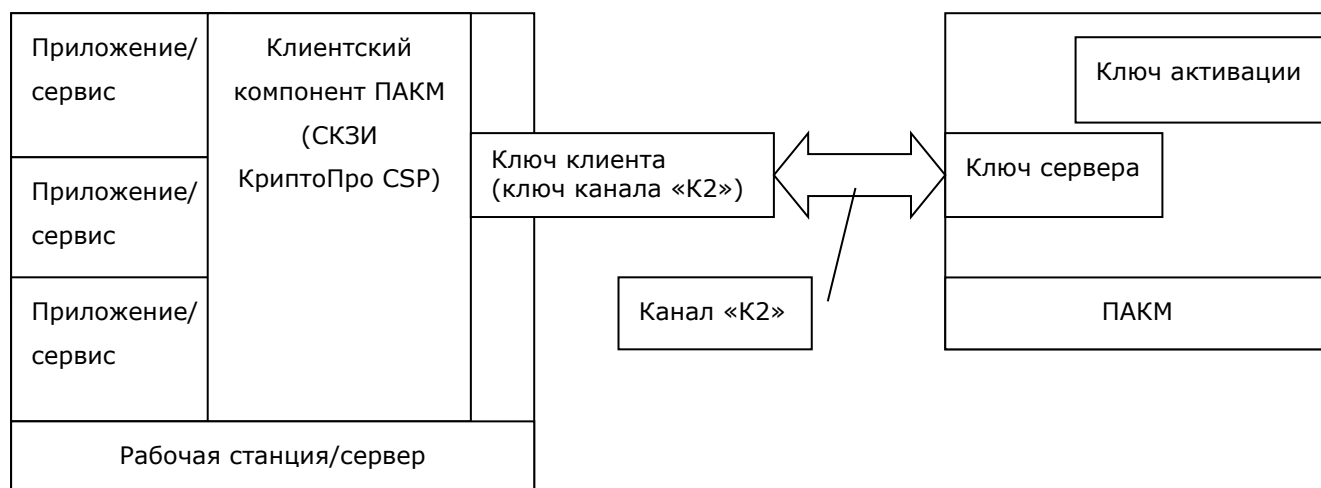


Рисунок 1. Общая схема компонент СФ при взаимодействии ПАКМ с клиентским компонентом

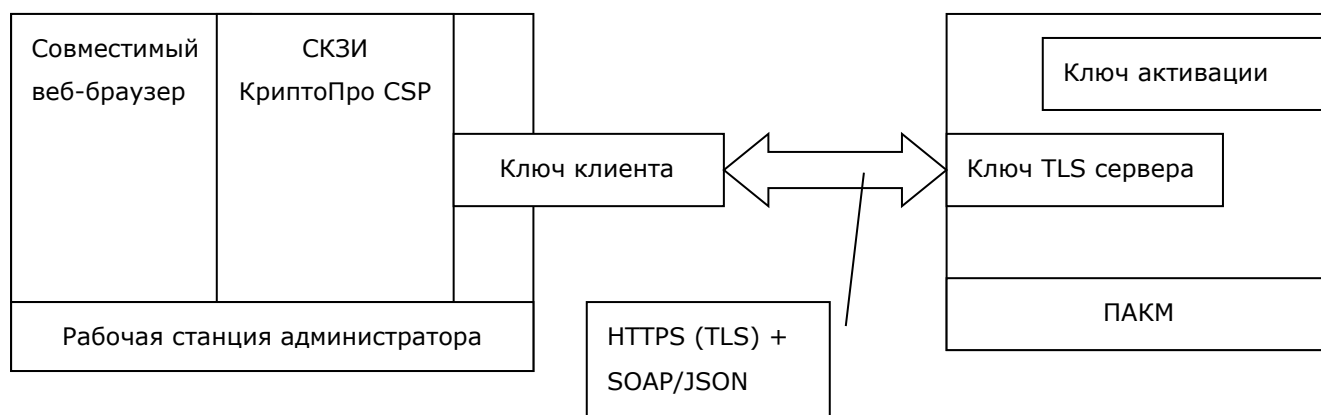


Рисунок 2. Общая схема компонент удаленного рабочего места администратора

3. ФУНКЦИОНАЛЬНЫЕ СХЕМЫ ПРИМЕНЕНИЯ

ПАКМ «КРИПТОПРО HSM»

3.1. Применение ПАКМ с сервером приложений

Функциональная схема применения ПАКМ с сервером приложений изображена на Рис. 3.

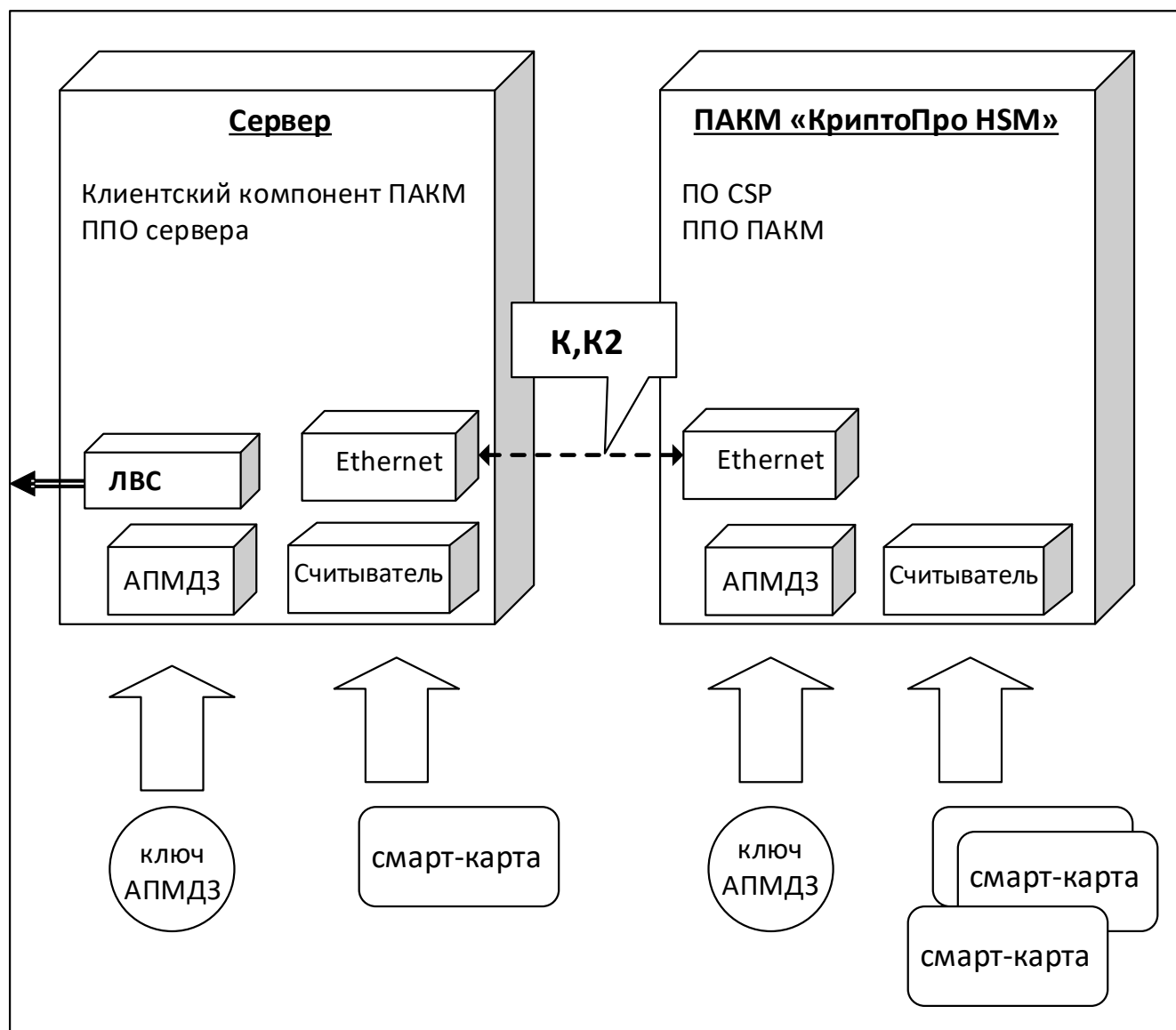


**Рисунок 3. Схема применения ПАКМ «КриптоПро HSM»
с сервером приложений**

На стороне сервера используются программно-аппаратные средства:

- ПЭВМ с установленной ОС;
- Клиентский компонент ПАКМ (СКЗИ «КриптоПро CSP») — реализует интерфейс криптографических функций для взаимодействия ПАКМ «КриптоПро HSM» с

сервером в части обеспечения контроля целостности данных обмена между ними, шифрования информации в каналах K2 и K, обеспечения протокола сетевой аутентификации;

- ППО сервера — прикладное программное обеспечение сервера, взаимодействующее с ПО ПАКМ, а также с АПМДЗ и считывателем смарт-карт;
- АПМДЗ — аппаратно-программный модуль доверенной загрузки;
- Ключи АПМДЗ;
- Считыватель смарт-карт;
- Смарт-карты — ключевые носители;
- ЛВС — интерфейс для взаимодействия по локальной сети с внешними абонентами пользователями функций СКЗИ;
- K2 — локальный защищенный канал, базирующийся на протоколе TLS, используется для серверов с установленной ОС семейства Windows.
- K — локальный защищенный канал (ЛЗК), используется специализированным ПО (ПАК ГУЦ) в доверенных ОС;

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

- ПЭВМ с установленной ОС ALT Linux SPT Server 7.0 и двумя/тремя оптическими сетевыми платами;
- ПО CSP — криптопровайдер типа «КриптоПро CSP»;
- ППО ПАКМ — прикладное программное обеспечение ПАКМ для взаимодействия с сервером, а также работы с АПМДЗ и считывателем смарт-карт;
- АПМДЗ — аппаратно-программный модуль доверенной загрузки;
- Ключи АПМДЗ;
- Считыватель смарт-карт;
- Смарт-карты — ключевые носители.

Взаимодействие между ПАКМ «КриптоПро HSM» и устройствами доступа осуществляется по каналу K2. Локальный защищенный канал K используется специализированным ПО (ПАК ГУЦ) в доверенной ОС.

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

- владелец ключа ЭП, хранящегося в ПАКМ (например, уполномоченное лицо УЦ);

- привилегированные пользователи ПАКМ «КриптоПро HSM» (подробнее см. раздел 5);
- группа доверенных лиц (для обеспечения хранения и ввода ключа активации в разделенном виде) — Суперпользователь ПАКМ.
- администратор ППО сервера;
- администратор безопасности сервера.

Управление доступом к ПАКМ «КриптоПро HSM» и аудит криптографических вызовов ПАКМ «КриптоПро HSM» производится с удаленного рабочего места администратора ПАКМ.

Примерная схема подключения ПАКМ к серверу изображена на Рис. 4.

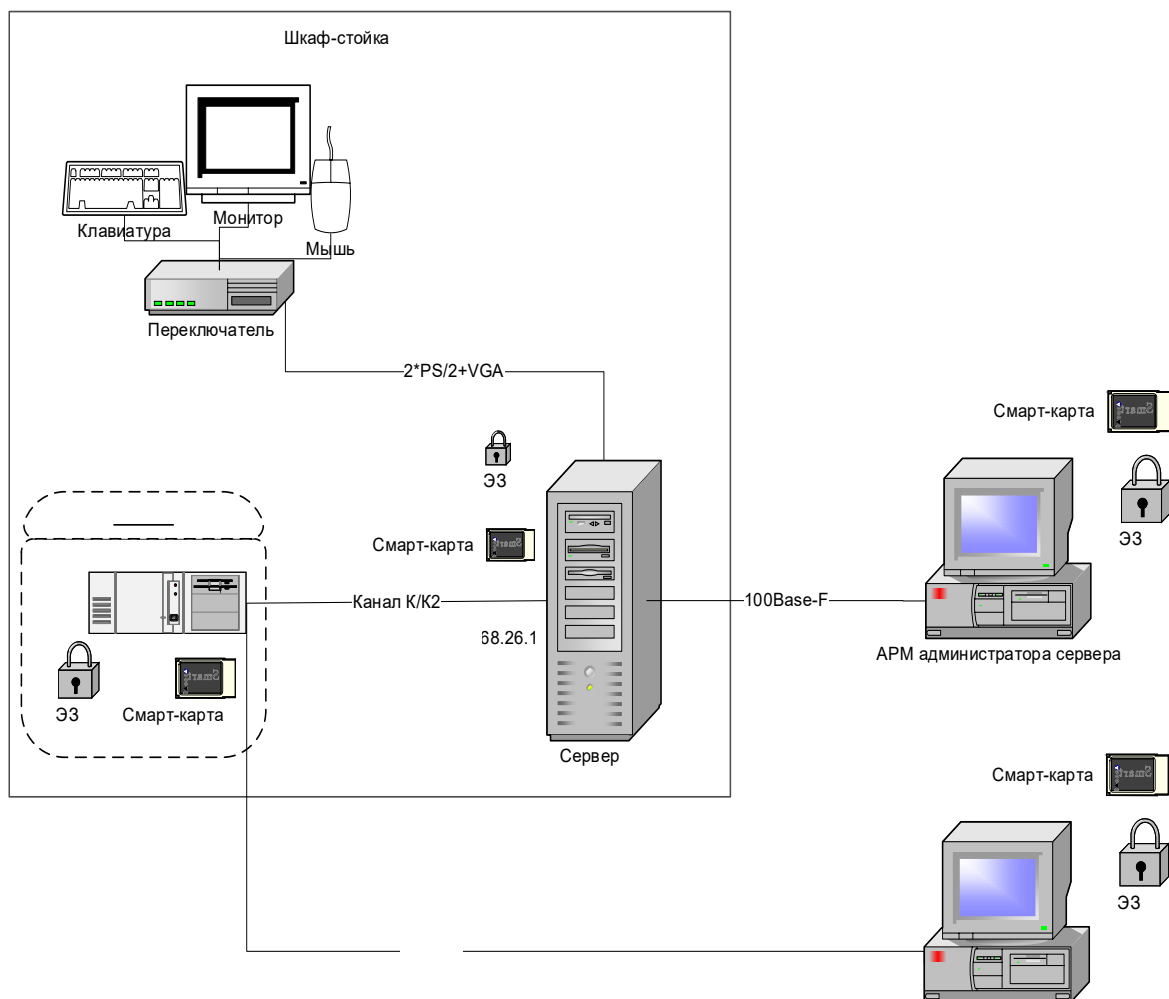


Рисунок 4. Схема подключения ПАКМ к серверу

Комплекс, включающий сегмент локальной сети, сервера, рабочие станции пользователей, использующие ПАКМ «КриптоПро HSM», может быть введен в эксплуатацию после проведения следующих организационно-технических мероприятий по специальной защите:

- категорирования в соответствии с требованиями нормативных документов;
- монтажа основных и вспомогательных технических средств объекта информатизации и требуемых средств защиты информации;
- аттестации объекта информатизации установленным порядком.

3.2. Подключение ПАКМ к нескольким серверам

Допускается использовать ПАКМ как групповое СКЗИ, обслуживающее несколько серверов. При этом, каждый сервер должен иметь отдельный считыватель смарт-карт, используемый для карт канала К/К2. Так как ввод PIN 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, пин-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 Рис. 5.

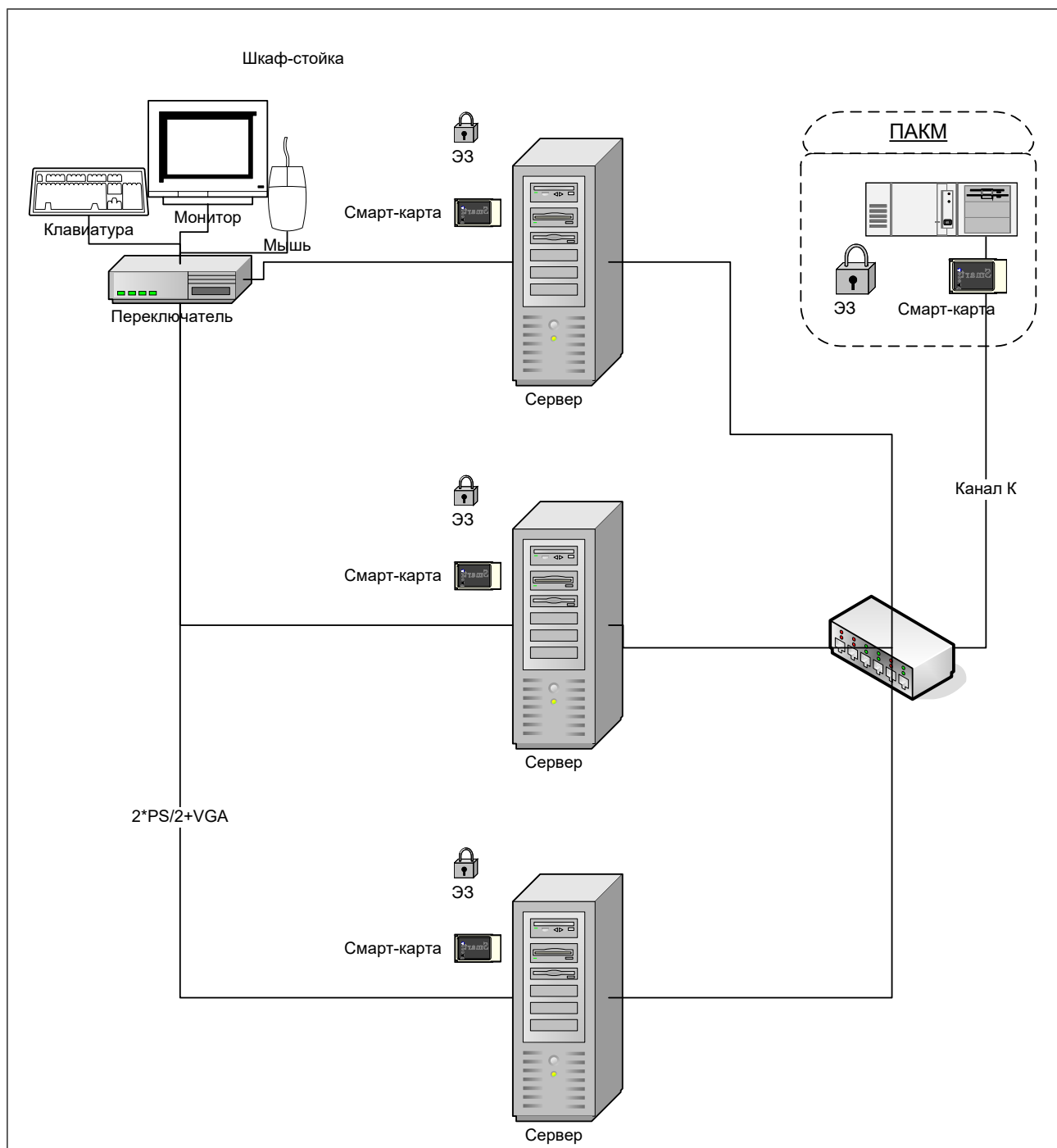


Рисунок 5. Схема подключения ПАКМ к нескольким серверам

3.3. Подключение рабочих станций пользователей к ПАКМ

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 K2 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 K2, а также рабочая станция, предназначенная для удаленного администрирования ПАКМ.

Примерная схема подключения рабочих станций пользователей к ПАКМ изображена на Рис. 6.

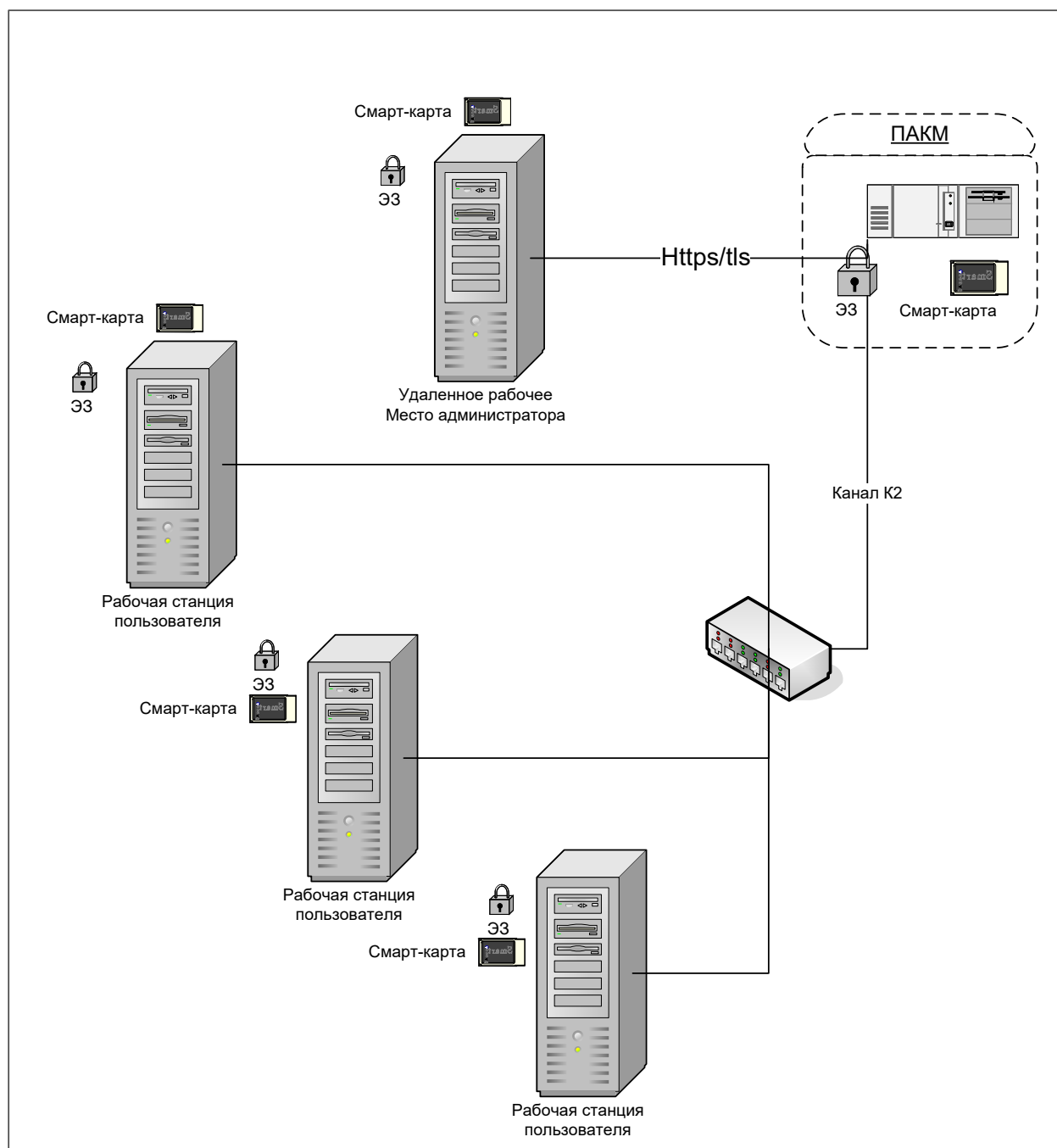


Рисунок 6. Схема подключения рабочих станций пользователей к ПАКМ

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 K2 с использованием порта с номером 1501; сервера, взаимодействующие с ПАКМ по каналу К обращаются к нему через порт с номером 1502, а ПО удаленного администрирования ПАКМ использует порт 443 для взаимодействия с ПАКМ. Для увеличения производительности серверных приложений имеется возможность организовать нешифрованный канал K2 (K2s) 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.

Настройки межсетевого экрана выполняются в соответствии с «ЖТЯИ.00096-03 90 01. Инструкция по использованию».

3.4. Использование Платежного HSM

При использовании ПАКМ в качестве платежного HSM (с использованием «Модуля обеспечения защиты платежных систем») для настройки платежных функций HSM и доступа к командам используются устройства доступа — терминал и хост-компьютер.

Терминал используется для подключения к консоли ПАКМ с использованием tenet-клиента и доступа к интерфейсу консольных команд, которые используются для конфигурации и диагностики платежного модуля ПАКМ, а также управления платежными мастер-ключами.

Хост-компьютер осуществляет взаимодействие с ПАКМ посредством направления команд хоста и получения ответов от ПАКМ. Хостовые команды реализует управление ключами, обработку транзакций, операции, требуемые для инициализации и эмиссии платежных карт.

Примерная схема подключения хост-компьютера и терминала к ПАКМ изображена на Рис. 7.

ПАКМ, принтер для печати PIN-конвертов и терминал находятся в контролируемой зоне. Хост-компьютер и ПАКМ располагаются в защищенной частной сети, отдельно от любой ориентированной на пользователя сети и любого подключения к Интернету. При необходимости консольный терминал подключается непосредственно к ПАКМ. В случае подключения ПАКМ к хосту через сеть Ethernet, рекомендуется использовать выделенный сегмент сети, единственными устройствами в котором должны быть хост-компьютер и связанный(-ые) с ним ПАКМ.

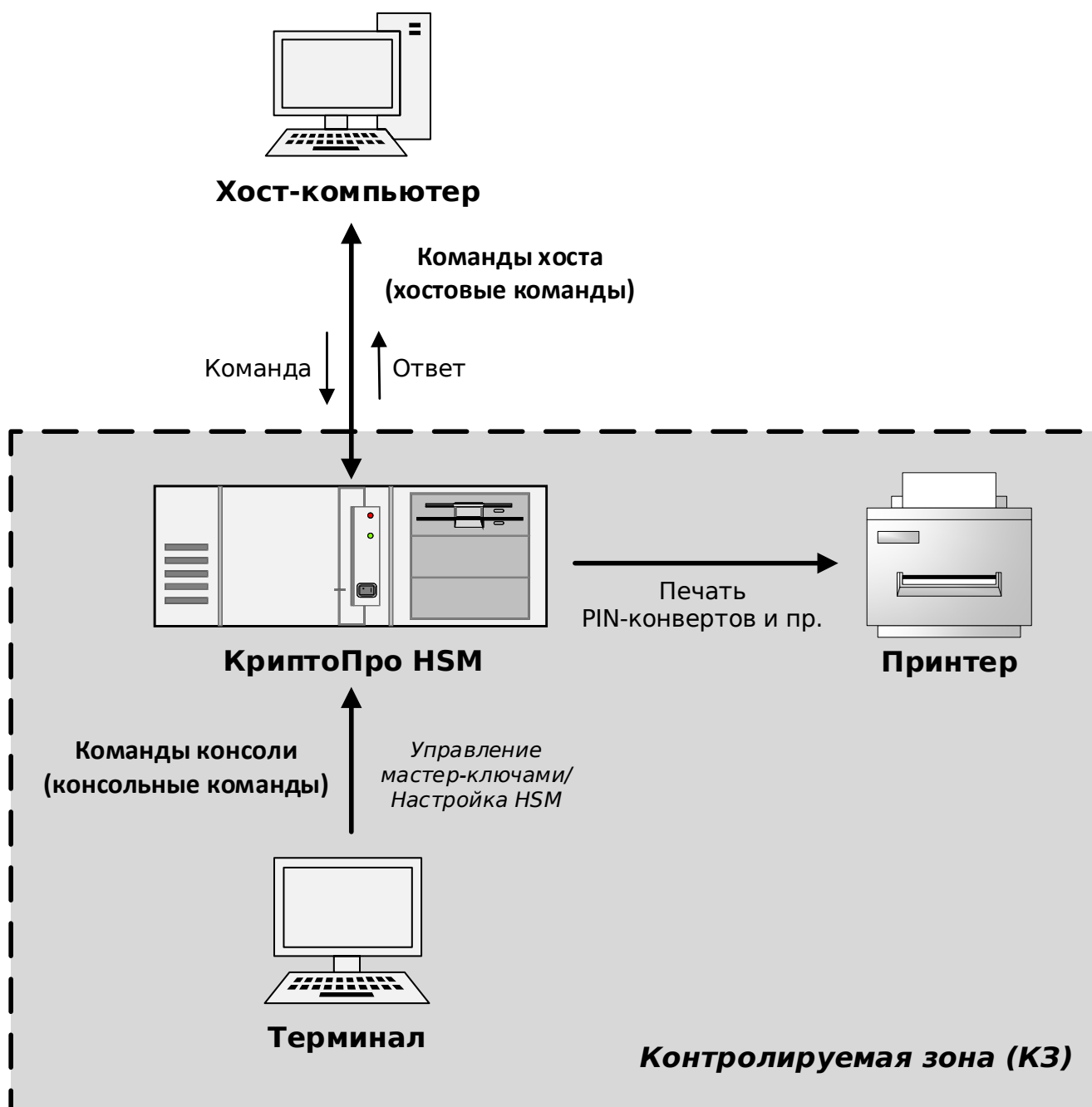


Рисунок 7. Схема подключения устройств доступа к платежному HSM

4. СОСТАВ АППАРАТНОЙ ПЛАТФОРМЫ И ПО ПАКМ

4.1. Аппаратная платформа ПАКМ

Установка и эксплуатация ПАКМ «КриптоПро HSM» осуществляется в соответствии с документом «ЖТЯИ.00096-03 90 01. Инструкция по использованию».

К эксплуатации ПАКМ «КриптоПро HSM» допускаются лица, прошедшие соответствующую подготовку и изучившие эксплуатационную документацию на программно-аппаратные средства, входящие в состав ПАКМ.

Аппаратная часть ПАКМ «КриптоПро HSM» включает следующие специализированные устройства:

- встроенный считыватель смарт-карт;
- ПАК «Соболь» с физическим ДСЧ;
- сетевая плата Ethernet с оптическим выходом для подключения к каналам «К», «К2» (взаимодействие с сервером) / сегменту локальной сети (для каналов «К» и «К2»);
- сетевая плата Ethernet с двумя оптическим выходами для подключения к каналам «К», «К2» (взаимодействие с сервером) / сегменту локальной сети (для каналов «К» и «К2»)/удаленному рабочему месту администраторов ПАКМ;
- панель с жидкокристаллическим экраном и кнопками управления для администрирования ПАКМ.

Все аппаратные средства ПАКМ «КриптоПро HSM» размещены в одном корпусе. Корпус ПАКМ «КриптоПро HSM» защищен от несанкционированного вскрытия путем опечатывания системного блока и разъемов системного блока.

Спецификация аппаратной платформы ПАКМ приведена в разделе 1.3 «ЖТЯИ.00096-03 95 01. Правила пользования».

В процессе эксплуатации ПАКМ должны выполняться требования по размещению технических средств и требования к использованию аппаратных компонент ПАКМ в соответствии с «ЖТЯИ.00096-03 95 01. Правила пользования».

Сервера и рабочие станции (клиенты ПАКМ) должны быть оснащены устройствами:

- считыватель смарт-карт для ввода/вывода информации на смарт-карту;
- АПМДЗ с физическим ДСЧ (в случае использования клиентского компонента по уровню защиты КС2 или КС3);

- сетевая плата Ethernet для подключения к каналам «К»/«К2» (взаимодействие ПЭВМ с ПАКМ «КриптоПро HSM»);
- сетевая плата для подключения к ЛВС предприятия.

Все аппаратные средства должны быть размещены в одном корпусе.

Для обеспечения функционирования серверов и рабочих станций необходимо установить на предназначенных для них компьютерах ОС и ПО клиентского компонента ПАКМ, предоставляющее серверам и рабочим станциям интерфейс к криптографическим функциям ПАКМ.

Необходимо выполнять требования по обеспечению безопасности и защиты от НСД ПЭВМ с установленным клиентским компонентом ПАКМ в соответствии с документацией на СКЗИ «КриптоПро CSP», входящее в состав данного клиентского компонента ПАКМ.

4.2. Программное обеспечение ПАКМ

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

ПО ПАКМ включает:

1. Базовые программные модули
2. Модуль обеспечения защиты платежных систем
3. Модуль обеспечения защиты систем ДЭГ

ПО клиентского компонента ПАКМ включает:

1. ПО «Клиент КриптоПро HSM» (КриптоПро HSM Client)
2. Утилита командной строки HsmGenArm
3. СКЗИ «КриптоПро CSP»
4. Модули «КриптоПро JavaCSP», «КриптоПро JavaTLS»

5. РОЛЕВАЯ МОДЕЛЬ ДОСТУПА

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 SA, Microsoft IIS, КриптоПро УЦ, Служб Штamped 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 клиентский компонент ПАКМ. Взаимодействие клиентов с ПАКМ производится по защищенным каналам «K2» и «K».

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

Каждый клиент ПАКМ при регистрации в ПАКМ получает уникальный номер (нумерация начинается с 1000), номер группы, обычно совпадающий с номером пользователя, и имя, 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 «K2») 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 «K» имеют внутри другой формат. Клиенты ПАКМ – сервера регистрируются автоматически при первом обращении к ПАКМ. При этом в считывателе сервера постоянно должна находиться карта канала «K».

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 «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»;
- Администратор Статистики;
- Администратор Платежной системы;
- Держатель части разделенного секрета LMK.

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 формируются ПАКМ и выдаются обычным пользователям администратором ПАКМ. Ключи и сертификат доступа к ПАКМ для привилегированных пользователей формируются ПАКМ и выдаются суперпользователем ПАКМ.

Суперпользователь ПАКМ — группа привилегированных пользователей, любые 3 из 5 лиц, держателей частей разделенного секрета ключа активации ПАКМ. Только данная группа лиц может локально получить доступ к функциям ПАКМ, позволяющим добавлять новые 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. 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. Держатель части разделенного секрета ключа активации ПАКМ может являться одновременно привилегированным пользователем ПАКМ: администратором ПАКМ, аудитором ПАКМ, администратором резервного копирования ПАКМ.

Держатель части разделенного секрета LMK — привилегированный пользователь, хранитель смарт-карты с ключевой компонентой LMK. Группа держателей части разделенного секрета LMK, состоящая минимум из 2 человек, участвует в формировании главного ключа защиты платежных данных (LMK), предъявляя ключевые носители с компонентами во время выполнения команды сборки LMK из ключевых компонент и загрузки его в хранилище. Функционирование Модуля обеспечения защиты платежных систем невозможно без загруженного LMK. Общее количество частей LMK, а также количество частей, необходимых для формирования LMK (параметры n и k соответственно в схеме разделения ключа « k из n »), определяется администратором Платежной системы при генерации LMK. Держатель части разделенного секрета LMK может являться одновременно привилегированным пользователем 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, выдаваемых 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 PIN 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, что важно, т.к. многие сервисы операционной системы на сервере, использующие функции СКЗИ не имеют доступа к рабочему столу (консоли) и не могут запросить там PIN на доступ к контейнеру ключа. Кроме этого использование указанного сертификата ключа доступа к функциям ПАКМ в процессе аутентификации, позволяет при соответствующих настройках отменить режим шифрования канала K2, 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 K2.

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 (требуется 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 (РК) 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). Администратор (РК) хранит у себя смарт-карту с ключом расшифровки конкретной резервной копии, поэтому восстановление ПАКМ из резервной копии возможно только при совместном доступе к данной операции Администратора ПАКМ и Администратора РК.

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

Администратор Статистики «КриптоПро HSM» не имеет каких-либо прав на изменения любых параметров и внутренних данных ПАКМ. Данная роль используется для процессов удаленного мониторинга состояния ПАКМ. Также ей доступно автоматическое скачивание журналов ПАКМ.

В сертификате ключа доступа к функциям ПАКМ данной роли прописывается специальное расширение (EKU) «1.2.643.2.2.34.37».

Администратор Платежной системы осуществляет управление настройками платежной системы, запуском/остановом соответствующих сервисов платежной системы, обновлением прошивки ПО платежной системы. В ПАКМ должно быть зарегистрировано как минимум две учетные записи администратора Платежной системы, т.к. некоторые операции требуют двойного подтверждения.

В сертификате ключа доступа к функциям ПАКМ данной роли прописывается специальное расширение (EKU) «1.2.643.2.2.34.36».

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 KB), 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 из 5» ключа активации ПАКМ. После чего может быть сформирован новый ключ любого из администраторов ПАКМ.

6. КЛЮЧИ И СЕРТИФИКАТЫ ПАКМ

6.1. Ключ активации ПАКМ, защитные ключи

Ключ активации ПАКМ создается в момент инициализации ПАКМ и защищается с использованием разделенных секретов по схеме «3 из 5» («k из n»).

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

Периодичность смены ключа активации определяется уровнем безопасности, которому соответствует ПАКМ. Также может производиться внеплановая смена ключа активации (увольнение сотрудников, владеющих защитными ключами, порча, утеря носителей защитных ключей и т.п.).

Ключ активации является основным ключом ПАКМ, обеспечивающим безопасность при доступе к ПАКМ. Без формирования данного ключа невозможно привести ПАКМ в состояние, способное обслуживать запросы пользователей по сети, а также расшифровать ключи пользователей системы. На данном ключе защищаются ключи шифрования ПАКМ. Также при помощи данного ключа можно получить доступ к меню управления ПАКМ на LCD панели.

Ключ хранится в разделенном на 5 частей виде на 5 смарт-картах. Для формирования ключа необходимо ввести любые 3 части. Каждая часть (смарт-карта) защищена PIN из 8 цифр. Части ключа активации распределяются между работниками службы безопасности организации.

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

В случае компрометации 3 и более ключей разделения секрета ключ активации ПАКМ, а также все ключи, защищенные на ключе активации, считаются также скомпрометированными. Под компрометацией ключа активации также понимается хранение 3 и более частей разделенного секрета у одного субъекта.

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.

6.2. 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 (корневой) сертификат.

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

6.3. 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 (ГОСТ) 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.

При плановой смене ключа подписи ПАКМ, наряду с новым самоподписанным сертификатом ключа будут сформированы самовыпущенные сертификаты «Старый на новом» и «новый на старом». Эти сертификаты обеспечивают «непрерывность» функционирования TLS протокола (проверку сертификатов, когда пользователи ПАКМ ещё не успели установить у себя новые самоподписанные корневые сертификаты ПАКМ).

6.4. 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 K2), 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. Но по мере обращения к ним пользователей-владельцев, они будут перешифровываться на новых (текущих) ключах шифрования ПАКМ.

6.5. Сессионный ключ канала «K2»

Сессионный ключ канала «K2» (ключ шифрования) служит для защиты (шифрования) передаваемых данных по каналу «K2».

Срок действия ключа: сессионный ключ канала K2 вырабатывается всякий раз при процедуре аутентификации пользователя с использованием TLS протокола, а также через заданные промежутки времени (1 час).

Сессионный ключ канала «K2» вырабатывается в процессе установления TLS сессии (на основе ключей и сертификатов аутентификации обычного пользователя и администратора сервера).

6.6. 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 «K2», 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.

6.7. 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.

6.8. 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 «K2», а также при удаленном HTTPS доступе привилегированных пользователей ПАКМ к функциям управления ПАКМ.

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

6.9. 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 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 = 11111111 (восемь единиц). PIN 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.

6.10. Сертификат ключа аутентификации Администратора

Сертификат ключа аутентификации привилегированного пользователя ПАКМ — члена группы Администраторов ПАКМ (Администратора, Аудитора, Администратора резервного копирования, Администратора статистики, Администратора Платежной системы 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;

«1.2.643.2.2.34.36» - Администратор Платежной системы ПАКМ;

«1.2.643.2.2.34.37» - Администратор Статистики ПАКМ;

Наличие данного ECU 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.

6.11. 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), 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.

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.

6.12. Ключ подписи журнала аудита

При выгрузке журнала аудита и журнала событий ПАКМ с помощью APM Web администрирования, в целях дальнейшего контроля целостности выгруженных и хранимых данных, можно указать, чтобы выгружаемые журналы включали электронную подпись. Для формирования ЭП журналов используется **ключ подписи журнала аудита ПАКМ**. Данный ключ и соответствующий ему сертификат формируется при инициализации ПАКМ и может быть сменен (плановая смена), как с LCD панели, так и в интерфейсе APM Web администрирования.

Данный ключ зашифрован на ключе шифрования ПАКМ, хранится и используется внутри ПАКМ. Максимальный срок действия ключа составляет 3 года.

В случае выгрузки журналов вместе с ЭП скачанный файл будет представлять собой CMS (#pkcs7) сообщение SIGNED_DATA с присоединенной электронной подписью. В последствии для проверки ЭП журнала можно воспользоваться утилитами КриптоПро.

6.13. Локальный мастер-ключ (LMK)

Локальный мастер-ключ (Local Master Key, LMK) — главный криптографический ключ HSM, с помощью которого происходит шифрование других криптографических ключей и данных, используемых в процессе обработки информации в платежных системах.

Создается только в случае использования Модуля обеспечения защиты платежных систем.

LMK генерируется администратором Платежной системы с помощью интерфейса консольных команд и защищается с использованием разделенных секретов по схеме «k из n» (значение k и n устанавливаются при генерации ключа).

Ключ хранится в разделенном на n частей виде на смарт-картах. Для формирования ключа необходимо ввести любые k частей. Ключ формируется администратором Платежной системы с помощью интерфейса консольных команд. Каждая часть (смарт-карта) защищена PIN из 8 цифр. Части (смарт-карты) LMK распределяются между держателями части разделенного секрета LMK, при этом не допускается хранение более одной смарт-карты у любого из таких пользователей.

7. 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, 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 $UID \neq GID$), 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.

8. ВЕДЕНИЕ ЖУРНАЛОВ

Администратор безопасности Серверов и ПАКМ «КриптоПро HSM» ведет следующие журналы (не входят в состав ПО ПАКМ «КриптоПро HSM»):

1. «Журнал регистрации администраторов безопасности и пользователей»;
2. «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:

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

Примечание. Примеры журналов приведены в Приложениях 2, 3.

В автоматизированном виде в ПАКМ ведется 3 журнала:

1. Журнал аудита ПАКМ
2. Журнал событий СКЗИ
3. Журнал пользователей ПАКМ

Журнал событий ПАКМ ведется средствами операционной системы, под управлением которой функционирует ПАКМ.

События ОС, подвергаемые аудиту в ПАКМ:

1. старт/останов операционной системы;
2. старт/останов системных сервисов;
3. идентификация/аутентификация/авторизация пользователей в системе;
4. использование криптографических функций;
5. запуск процессов;
6. монтирование/демонтирование;
7. вызов сервисов межпроцессного взаимодействия;
8. 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:

1. генерация ключа;
2. операции подписи/проверки подписи;
3. операции шифрования/расшифрования;
4. операции экспорта/импорта ключа;
5. 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.

9. НАСТРОЙКА АУДИТА

Для обнаружения атак на ресурсы ПАКМ применяется анализ **журнала событий СКЗИ и журнала аудита**.

После установки и настройки ПАКМ прежде всего необходимо включить аудит на общесистемных компонентах Серверов, подключенных к ПАКМ.

Настройка аудита в ПАКМ производится при установке автоматически.

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 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 как с LCD панели, так и с использованием APM Web администрирования ПАКМ. Выполнить данную операцию может Аудитор, но только с подтверждением Администратора ПАКМ. Суперпользователь ПАКМ также может выполнить эту операцию с использованием меню LCD панели.

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

Журнал аудита может служить также для сбора статистической информации в разрезе каждого пользователя, а по некоторым типам событий в разрезе 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.

При необходимости можно указать, чтобы журнал был подписан ключом подписи журнала аудита ПАКМ. В этом случае скачанный файл будет представлять собой CMS (#pkcs7) сообщение SIGNED_DATA с присоединенной электронной подписью. В последствии для проверки ЭП журнала можно воспользоваться утилитами КриптоПро.

9.1. База данных и структура записей журнала аудита

Журнал аудита ведется в ПАКМ в виде базы данных (mysql).

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 Аудитору ПАКМ с подтверждением Администратором ПАКМ, или Суперпользователем 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.

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 администратора.

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 отрезка 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 и т.п.).

Примечания:

1. 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.
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.

3. В целях минимизации объема памяти, занимаемой журналом аудита, поле BinaryData заполняется только в событиях, связанных с генерацией пользователями ключевых пар (заносится значение открытого ключа), импортом открытых ключей (заносится значение импортируемого открытого ключа и значение открытого ключа, соответствующего импортирующему ключу), экспортом закрытых ключей (заносится значение соответствующего открытого ключа) и симметричных ключей (заносится значение HMAC, вычисленное с использованием алгоритма ГОСТ Р 34.11-2012 с длиной выхода 256 бит от пустой строки, при этом в качестве ключа HMAC используется экспортируемый ключ), вычислением пользователями значения HMAC (заносится значение HMAC) и формированием ЭП (заносится значение открытого ключа и значение ЭП). Если во время формирования ЭП дополнительно осуществлялась проверка установленного значения HMAC или ЭП, то в поле BinaryData также заносится это значение (HMAC или ЭП). При этом значения заносятся в следующей последовательности: значение открытого ключа, значение сформированной ЭП и проверяемое значение (HMAC или ЭП). Значения заносятся через разделитель `::` (в формате HEX представляет из себя строку `3A3A3A3A`).
4. Поле StringData заполняется только в событиях генерации пользователями ПАКМ ключевых пар (заносится идентификатор формируемого ключевого контейнера), удаления пользователями ключевых пар (заносится идентификатор удаляемого ключевого контейнера), экспортом закрытых и симметричных ключей (заносится тип экспортируемого блока: PRIVATEKEYBLOB в случае закрытых ключей и SIMPLEBLOB или OPAQUEKEYBLOB в случае симметричных ключей), формирования пользователями ЭП (заносится строка вида <KEYID>::PK::SGN::VER, где <KEYID> – идентификатор используемого ключевого контейнера, отсутствует в случае создания ЭП в VERIFYCONTEXT; PK, SGN, VER – константы, указывающие на наличие в поле BinaryData значения открытого ключа, значения сформированной ЭП и проверяемого значения соответственно), 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>). При неудаче выполнения отражаемого в журнале события могут заноситься дополнительные данные, позволяющие идентифицировать «данные» события/операции и проблему выполнения операции.
5. 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.

9.2. Типы событий

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 из 5»);

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) - Переполнение журнала аудита;

EVENT_TYPE_DELETE_KEY (29) - Удаление ключа;

EVENT_TYPE_CRYPT_EXPORT_KEY (30) - Экспорт ключа из ПАКМ;

EVENT_TYPE_CRYPT_IMPORT_KEY (31) - Импорт ключа в 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;

EVENT_TYPE_CRYPT_GETHASHPARAM (46) - Получение параметра хэша пользователем;

EVENT_TYPE_SET_LICENSE (47) - Установка лицензий на использование модулей ПАКМ «КриптоПро HSM».

9.3. Анализ журналов аудита

Работа с журналами аудита (извлечение из ПАКМ, стирание в ПАКМ, анализ) является обязанностью аудитора ПАКМ. Только ему доступны режимы очистки, восстановления журнала аудита, настройки опций, влияющих на процессы журналирования.

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 длительного хранения извлеченных из ПАКМ журналов привилегированный пользователь может выгрузить их подписанными ключом подписи журнала аудита. В дальнейшем ЭП выгруженных таким образом журналов может быть проверена при помощи утилит КриптоПро, например, при помощи утилиты `cryptcp`, входящей в состав дистрибутива, сертифицированного СКЗИ «КриптоПро CSP», устанавливаемого на рабочей станции удаленного администрирования ПАКМ.

Стирание журнала аудита в ПАКМ должно производиться Суперпользователем ПАКМ, либо Аудитором совместно с Администратором ПАКМ, при исчерпании свободного места на диске ПАКМ (отображается на панели управления ПАКМ, в web-интерфейсе администратора и в соответствующем пункте меню просмотра системных характеристик на LCD панели ПАКМ). Выполнение операции стирания журналов в ПАКМ возможно, как в автоматическом, так и только в ручном режиме.

Для анализа журналов аудита ПАКМ, выгруженных без формирования ЭП, применяются любые средства для просмотра текстовых файлов. Подписанный Журнал аудита имеет формат CMS (#PKCS7) с присоединенной ЭП. Для проверки подписи и извлечения текстового содержимого журнала из таких файлов можно воспользоваться утилитами КриптоПро (`cryptcp`).

Для оперативного анализа последних событий журнала СКЗИ администратор ПАКМ может воспользоваться средствами просмотра на LCD панели ПАКМ.

Для обеспечения защиты содержимого журналов аудита ПАКМ от искажений в процессе хранения необходимо регулярно (не реже, чем раз в сутки) выгружать журналы из ПАКМ на Сервер или рабочую станцию администратора ПАКМ. При этом период, задаваемый для считывания записей журнала, обязательно должен охватывать предыдущие сутки (т.е. должно быть организовано перекрытие предыдущего периода между считываниями журнала).

10. 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

<i>Нештатная ситуация</i>	<i>Действия персонала</i>
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.
Компрометация одного из личных ключевых носителей	Порядок действий при компрометации ключей описан в Правилах пользования.
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 необходимо использовать его.
Отказы и сбои в работе аппаратной части ПАКМ	Необходимо остановить работу, по возможности локализовать неисправность и в дальнейшем произвести ремонт в установленном порядке и, при необходимости,

	переустановку СКЗИ.
Отказы и сбои в работе средств защиты от НСД	Администратор безопасности должен восстановить работоспособность СЗИ от НСД, при необходимости произвести переустановку соответствующего ПО.
Отказы и сбои в работе программных средств по причине 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.
Отказы в работе программных средств по причине 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.
Отказы 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 8).

ПРИЛОЖЕНИЕ 1. АКТ ГОТОВНОСТИ К РАБОТЕ

УТВЕРЖДАЮ_____
(должность)_____
(наименование учреждения)_____
(подпись) (Ф.И.О.)**АКТ**готовности к работе _____ С _____
(наименование учреждения) (наименование изделий)

" ____ " _____ 20__ г.

Комиссия в составе председателя _____ и
(должность) (Ф.И.О.)членов, назначенная _____, составила настоящий акт о том, что помещение
эксплуатирующего органа _____, размещение _____, хранилища
(название) (оборудование)ключевых носителей, охрана помещений и подготовленность сотрудников к обслуживанию

(оборудование)соответствуют: _____
(ГОСТ, инструкция, руководящие документы, правила пользования и т.п.)Комиссия отмечает, что инсталляция ПО вышеупомянутых изделий проведены в соответствии с

(инструкции)Вывод: комиссия считает, объект _____ отвечает требованиям
(название объекта)_____
(название инструкции)

по обеспечению безопасности связи по уровню _____ и может быть введен в действие.

Председатель:

(подпись)_____
(Ф.И.О.)

Члены комиссии

(подпись)_____
(Ф.И.О.)_____
(подпись)_____
(Ф.И.О.)_____
(подпись)_____
(Ф.И.О.)**М.П.**

ПРИЛОЖЕНИЕ 2. ЖУРНАЛ РЕГИСТРАЦИИ АДМИНИСТРАТОРОВ БЕЗОПАСНОСТИ И ПОЛЬЗОВАТЕЛЕЙ

п/п	Организация	Ф.И.О. администратора безопасности пользователя системы	Данные регистрации	Дата регистрации	Дата выбытия	Примечание (пользователь, администратор)
1		Сидоров А. А.	нет	21.04.2000		Администратор безопасности
2		Иванов И. И.	Почтовый адрес: a.sidorov@acme.ru	01.05.2000		Оператор расчетной системы

ПРИЛОЖЕНИЕ 3. ЖУРНАЛ ПОЛЬЗОВАТЕЛЯ СЕТИ

п/п	Дата Время	Ф.И.О. пользователя системы	Событие	Дополнительные данные	Примечание