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 Комплектации 1 и 2 Руководство администратора безопасности

ЖТЯИ.00096-01 91 01

Листов 26

2020 г.

Содержание

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. ФУНКЦИОНАЛЬНЫЕ СХЕМЫ ПРИМЕНЕНИЯ ПАКМ «КРИПТОПРО HSM»

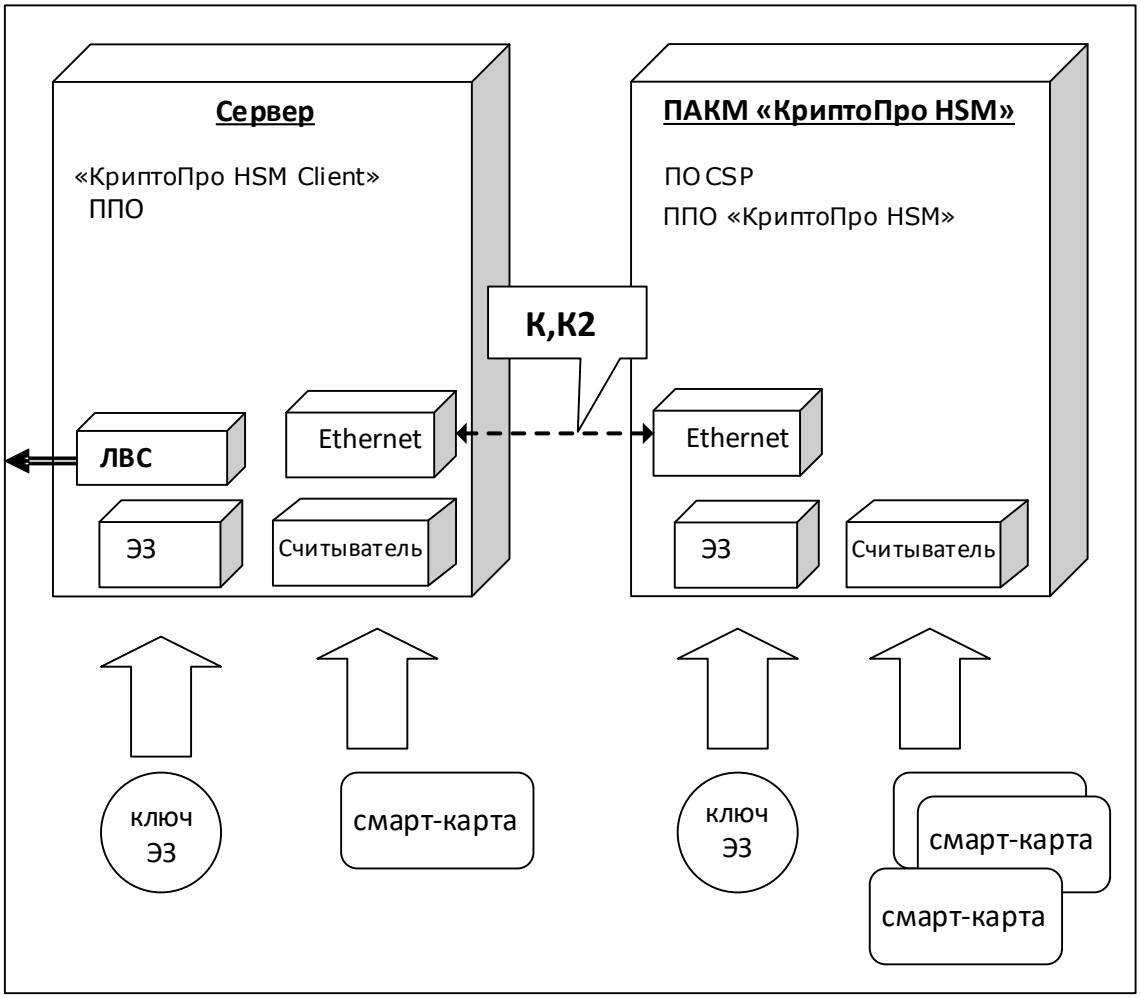

Рисунок 1. Функциональная схема применения ПАКМ «КриптоПро HSM» с сервером приложений.

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) при использовании с серверами, базирующимися на ОС семейства Unix/Linux, либо каналу К2 для серверов и рабочих станций с установленными ОС семейства Windows.

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) – Суперпользователь ПАКМ.
- администратор ППО сервера;
- администратор безопасности сервера.

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

Примерная схема подключения ПАКМ к серверу изображена ниже.

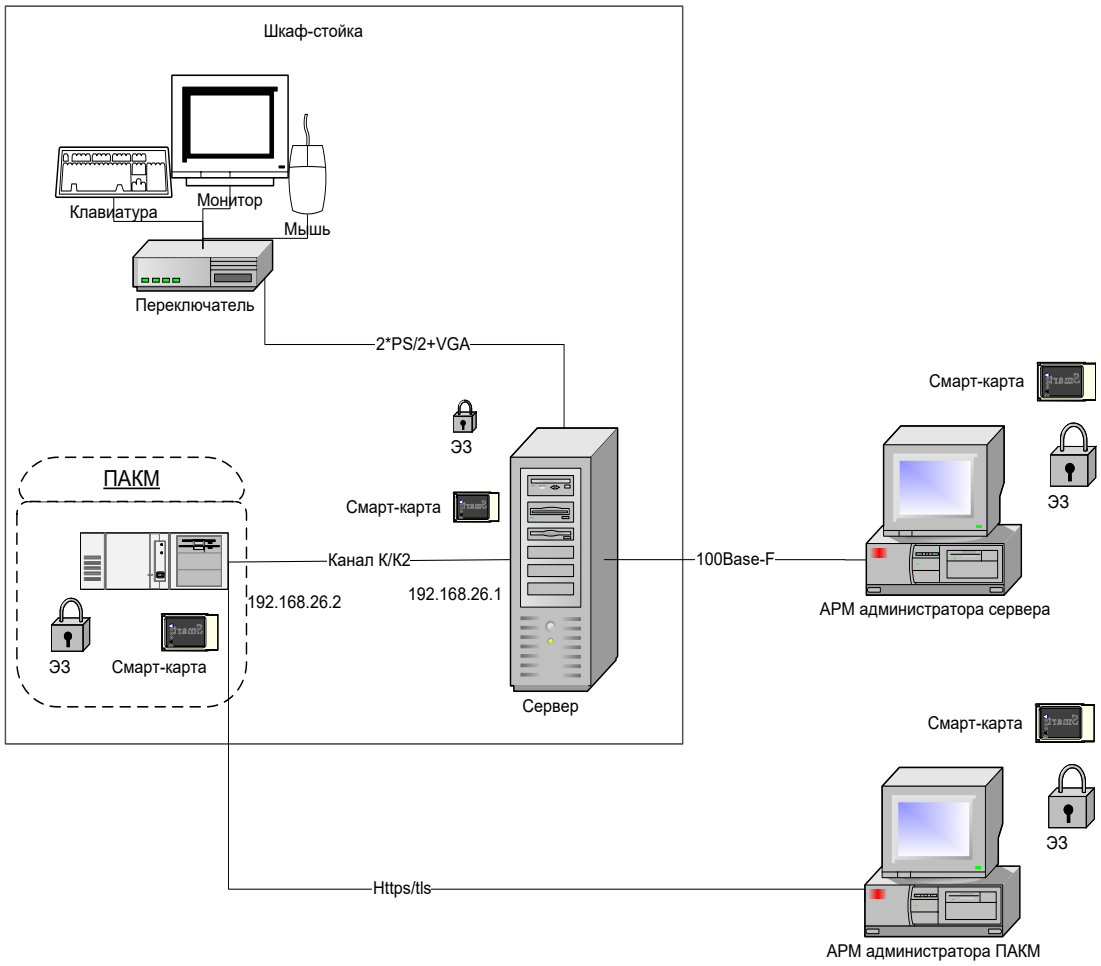

Рисунок 2. Схема подключения ПАКМ к серверу

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, 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 Рисунок 3.

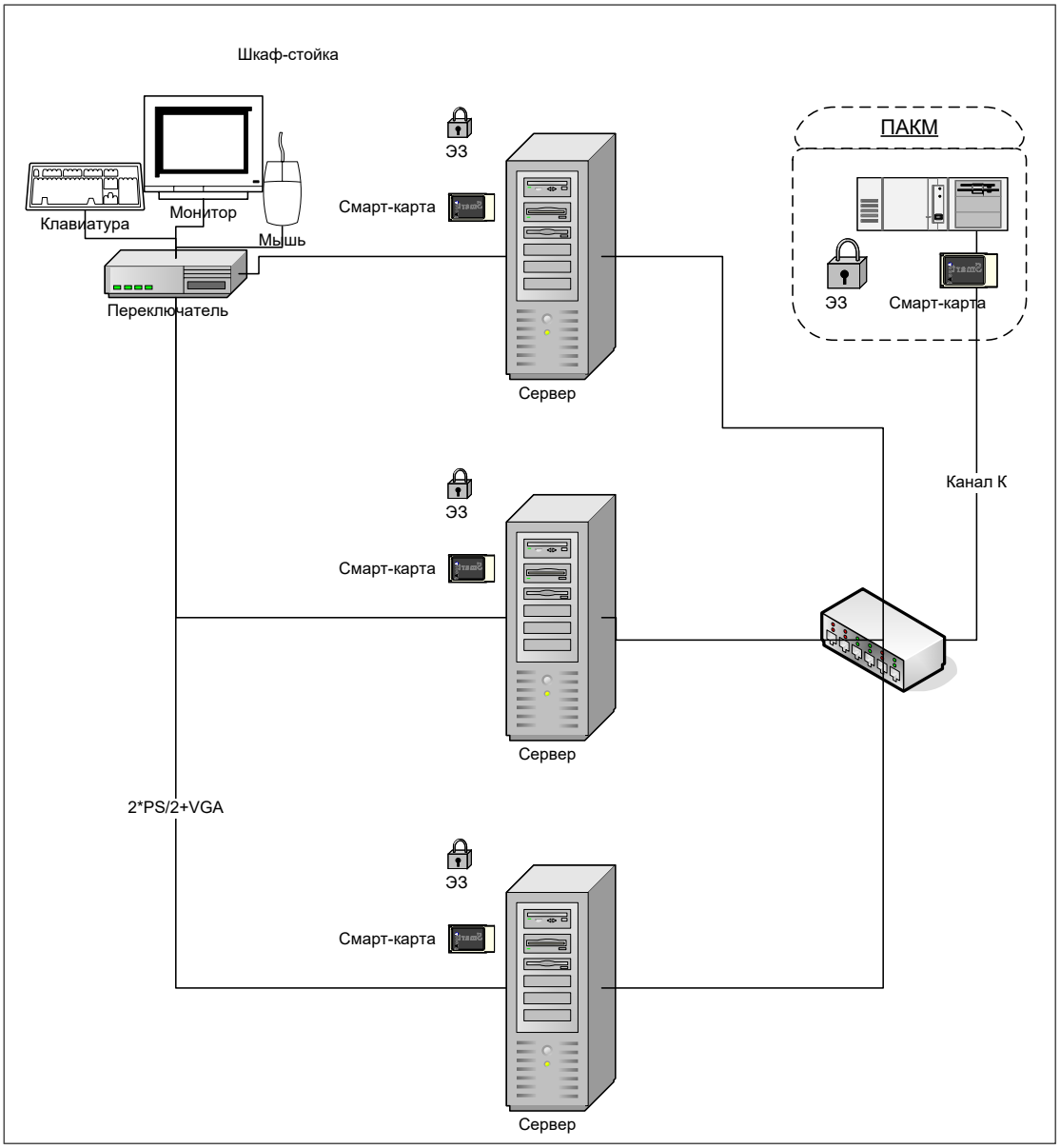

Рисунок 3. Схема подключения ПАКМ к нескольким серверам.

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 К2, а также рабочая станция, предназначенная для удаленного администрирования ПАКМ.

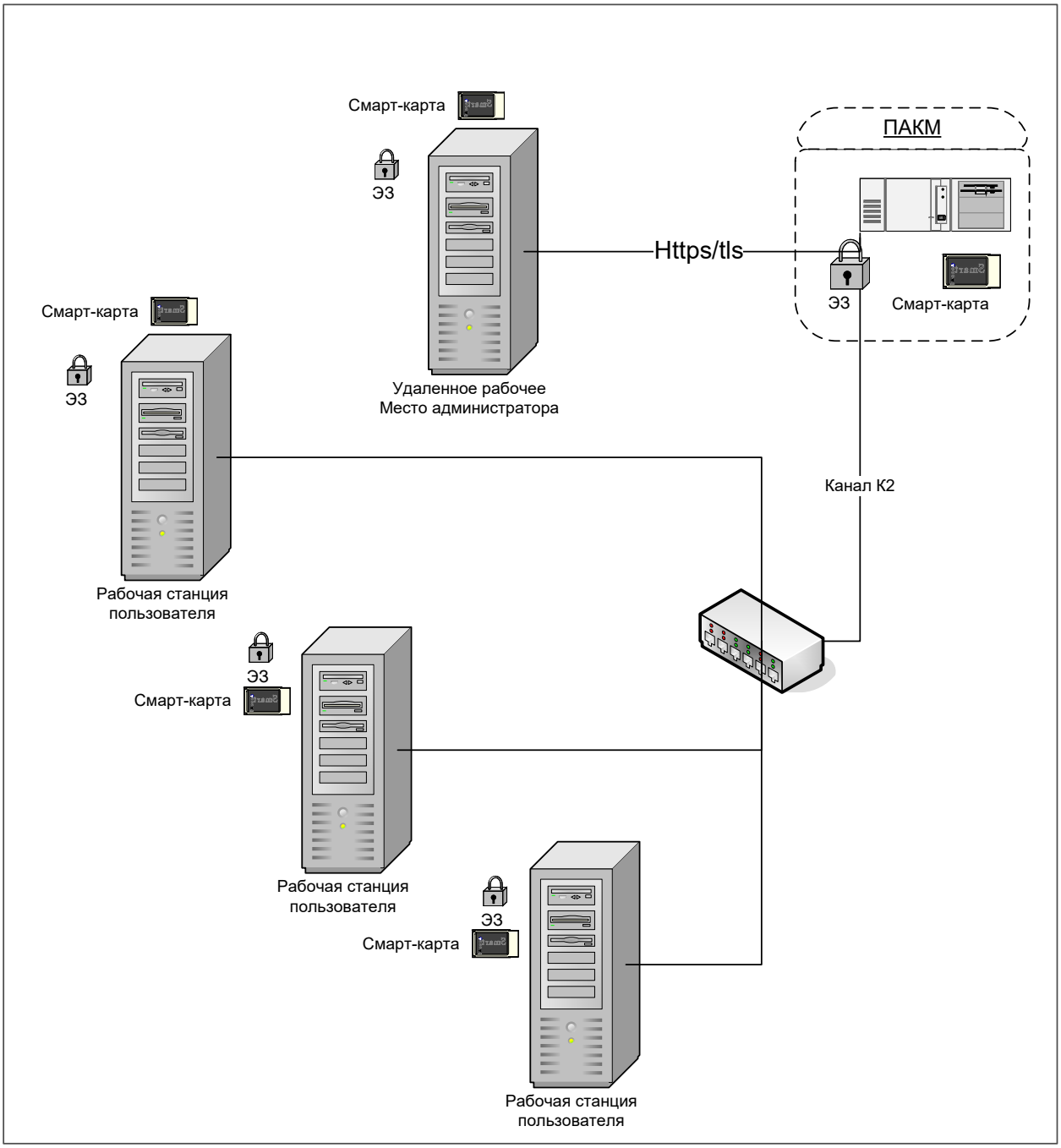

Рисунок 4. Схема подключения рабочих станций пользователей к ПАКМ.

Администратор ПАКМ имеет возможность описать правила встроенного в ПАКМ межсетевого экрана. При этом надо иметь ввиду, что рабочие станции пользователей и сервера приложений, с установленными на них ОС семейства Windows обращаются к ПАКМ по каналу К2 с использованием порта с номером 1501; сервера с установленными ОС семейства Unix/Linux обращаются к ПАКМ по каналу К с использованием порта 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.

Компоненты информационной системы предприятия могут быть подвержены различного рода угрозам. Угроза, реализованная с использованием уязвимостей информационно-программной системы, называется атакой.

Для блокирования возможностей нарушителя по осуществлению атак персоналу, обслуживающему Сервера и локальную сеть, следует провести ряд организационных и организационно-технических мер.

Для обнаружения атак пользуются аудитом журналов (регистрационных файлов) общесистемного и прикладного программного обеспечения комплекса Серверов (в том числе, журналов ПАКМ). Целью аудита является сбор информации об удачных и неудачных попытках доступа к объектам, применении привилегий и других важных, с точки зрения безопасности, действиях и протоколирование этих событий для дальнейшего анализа.

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. ОСНОВНЫЕ СВЕДЕНИЯ ОБ АППАРАТНОЙ ПЛАТФОРМЕ ПАКМ И СЕРВЕРА

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

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

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

- встроенный считыватель смарт-карт для ввода/вывода информации на интеллектуальную карту;
- электронный замок с физическим ДСЧ «Соболь»;
- 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» должен быть защищен от несанкционированного вскрытия (путем опечатывания системного блока и разъемов системного блока и контроля печатей администратором безопасности).

Сервера и рабочие станции пользователей должны быть оснащены устройствами:

- встроенный считыватель смарт-карт для ввода/вывода информации на интеллектуальную карту (допускается использование других считывателей ключевой информации с отчуждаемых носителей: дискет, USB токенов);
- электронный замок с физическим ДСЧ;
- сетевая плата Ethernet для подключения к каналам «К»/«К2» (взаимодействие с ПЭВМ ПАКМ «КриптоПро HSM»);
- сетевая плата для подключения к ЛВС предприятия.

Все аппаратные средства должны быть размещены в одном корпусе.

Корпуса серверов и рабочих станций должны быть защищены от несанкционированного вскрытия (путем опечатывания системного блока и разъемов и контроля печатей администратором безопасности).

Для обеспечения функционирования серверов и рабочих станций необходимо установить на предназначенных для них компьютерах операционную систему и программные компоненты, предоставляющие серверам и рабочим станциям интерфейс к криптографическим функциям ПАКМ.

Перед установкой следует проверить программное обеспечение на отсутствие вирусов и программных закладок. Также необходимо исключить из программного обеспечения средства разработки и отладки программ.

После завершения процесса установки ПО Сервера/рабочей станции и ПАКМ «КриптоПро HSM» следует провести контроль целостности установленного ПО.

Разрешается использовать ПАКМ для работы с конфиденциальной информацией при соблюдении ниже перечисленных организационно-технических мероприятий.

Достаточность принятых мер защиты определяется на этапе инструментальной проверки в ходе аттестационных испытаний информационной системы, в которой применяется ПАКМ.

4. РОЛЕВАЯ МОДЕЛЬ ДОСТУПА

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 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, как минимум из 3 человек, держателей частей разделенного секрета ключа активации ПАКМ. 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 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. 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.

Только суперпользователю доступен режим полной очистки содержимого ПАКМ.

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-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, 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-код 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 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 на серверах с установленной ОС семейства Windows при организации канала К2. На серверах с установленной ОС семейства Unix/Linux используется канал К, унаследованный из предыдущих версий ПАКМ «Феникс-М», «Атликс HSM».

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.

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».

5. ДЕЙСТВИЯ ПРИ КОМПРОМЕТАЦИИ КЛЮЧЕЙ

В случае компрометации ключей по факту компрометации должно быть проведено служебное расследование. Скомпрометированные ключи выводятся из действия.

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

Скомпрометированные ключи подлежат замене.

При перевыпуске ключей администратором выполняются действия, совершаемые при плановой смене ключей.

При компрометации ключа подписи ПАКМ, использующегося для издания сертификатов ключей аутентификации пользователей, после смены ключа подписи ПАКМ должны быть перевыпущены все сертификаты пользователей.

Ключ шифрования автоматически меняется при смене ключа активации ПАКМ.

6. 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 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.

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.

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.

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).

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) – Переполнение журнала аудита;

EVENT_TYPE_DELETE_KEY (29) – Удаление ключа;

EVENT_TYPE_CRYPT_EXPORT_KEY (30) – Экспорт закрытого ключа (ключа ЭП);

EVENT_TYPE_CRYPT_IMPORT_KEY (31) – Импорт закрытого ключа (ключа ЭП) 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.

7. 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 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.

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 применяются любые средства для просмотра текстовых файлов.

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).

8. ПОРЯДОК РАБОТЫ С ДСДР

8.1. Регистрация датчика dsrf_ex

Для регистрации датчика dsrf_ex для ПАКМ «КриптоПро HSM» нужно последовательно выполнить из директории, в которой расположена утилита cpconfig, следующие команды:

./cpconfig -hardware rndm -add dsrf_ex -name dsrf_ex -level 0

for i in 'seq 1 8'; do './cpconfig -hardware rndm -configure dsrf_ex -add string /hdb$i/kis_1 /var/opt/cprocsp/dsrf/hdb$i/kis_1'; done

for i in 'seq 1 8'; do 'mkdir /var/opt/cprocsp/dsrf/hdb$i'; done

Далее в каждую директорию hdb$i нужно положить свой kis_1. Все kis_1 должны быть различны.

После этого необходимо перезапустить сервис.

8.2. Запись последовательности ДСДР на SSD-диски

К процедуре записи последовательности ДСДР на SSD-диски предъявляется следующее требование: если запись последовательности ДСДР на SSD-диски осуществляется на оборудовании заказчика ПАКМ, данная процедура должна осуществляться на защищенном АРМ с обеспечением контролируемой зоны в соответствии с документацией на данный АРМ.

Примеры возможных типов АРМ:

- персональные ЭВМ в защищенном исполнении серии «ОБРУЧ» разработки АО «РНТ»;
- СВТ «Гамма МБ-16» разработки ФГУП «НПП «Гамма».

8.3. Пополнение последовательности ДСДР

Процедура пополнения последовательности ДСДР:

1. Для пополнения последовательности ДСДР может использоваться специализированное ПО из состава ПАКМ «КриптоПро HSM».
2. В рамках ТО пополнение гаммы производится техническими специалистами ООО «КРИПТО-ПРО».

8.4. Описание программы dsrfcopy

Входные данные расположены на CD-ROM и удовлетворяют следующим требованиям:

- файлы называются kis_1 и расположены в директориях db1/ и db2/;

- длина файлов кратна 36 байтам;
- файлы полностью совпадают, совпадение гарантируется поставщиком CD-ROM.

Выходные файлы удовлетворяют следующим требованиям:

- файлы называются kis_1 и расположены в директориях /var/opt/cprocsp/dsrf/hdb[1..8]/;
- длины файлов совпадают и кратны 36 байтам;
- все файлы попарно различаются.

Порядок работы программы dsrfcopy:

- считываются входные файлы и проверяется их совпадение (дополнительный контроль);
- входные данные разбиваются на 8 равных частей длиной кратной 36 байтам;
- открываются выходные файлы и проверяется равенство их длин;
- дописываются части входных данных и закрываются выходные файлы;
- все части должны различаться между собой;
- выходные файлы открываются, 16 последних байтов считываются и проверяются на несовпадение.

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