127018, Москва, ул. Сущёвский вал, д. 16 строение 5
Телефон: +7 (495) 780 4820
Факс: +7 (495) 780 4820
http://www.CryptoPro.ru
E-mail: info@CryptoPro.ru

КРИПТО ПРО

СРЕДСТВО КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

КРИПТОПРО HSM.

РУКОВОДСТВО АДМИНИСТРАТОРА БЕЗОПАСНОСТИ

ЖТЯИ.00046-01 90 03

Листов 33

2009 г.

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 СКЗИ ПАКМ "КриптоПро HSM" должны разрабатываться с учетом требований настоящего Руководства.

Содержание

1. ВВЕДЕНИЕ

1.1. Функциональные схемы применения ПАКМ "КриптоПро HSM".

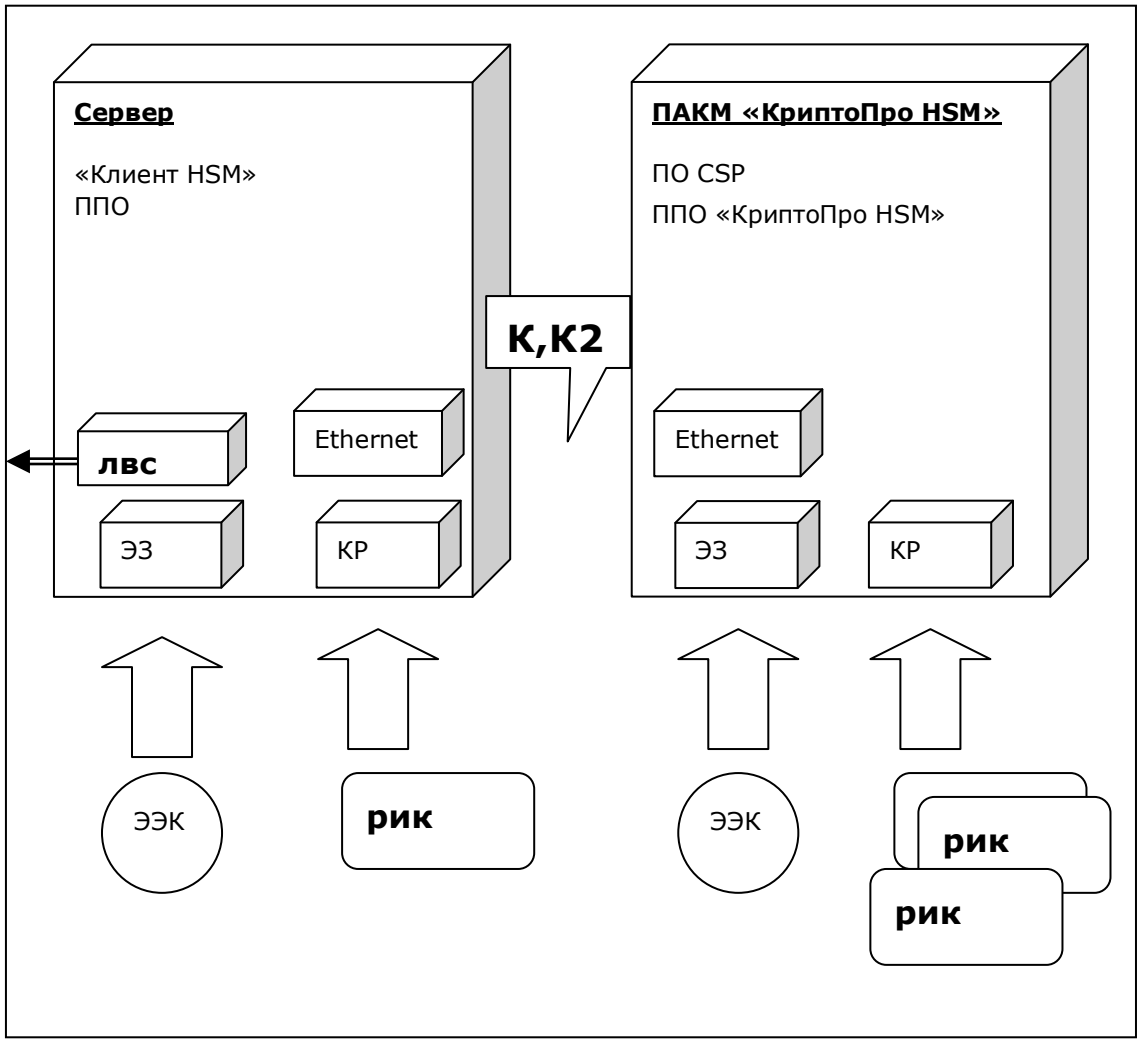

Рисунок 1 Функциональная схема применения ПАКМ "КриптоПро HSM" с сервером приложений.

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;
- ЭК - ключ электронного замка;

- РИК – российская интеллектуальная карта (ключевой носитель), в настоящее время применяется РИК типа ОСКАР, МАГИСТР;
- КР – считыватель для РИК;
- 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;
- ЭК - ключ электронного замка;
- РИК – российская интеллектуальная карта (ключевой носитель), в настоящее время применяется карта типа ОСКАР, МАГИСТР;
- КР – считыватель для РИК.

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 ЭЦП, хранящегося в ПАКМ (например, уполномоченное лицо УЦ);
- Привелигированные пользователиПАКМ «КриптоПро HSM.» (администратор ПАКМ, аудитор ПАКМ, администратор резервного копирования ПАКМ);
- группа доверенных лиц (для обеспечения хранения и ввода защитного ключа в разделенном виде).
- администратор ППО сервера;
- администратор безопасности сервера.

Управление доступом к ПАКМ "КриптоПро HSM" и аудит криптографических вызовов ПАКМ "КриптоПро HSM" производится с ПЭВМ сервера, либо с удаленного рабочего места администратора ПАКМ.

Примерная схема подключения ПАКМ к серверу изображена ниже.

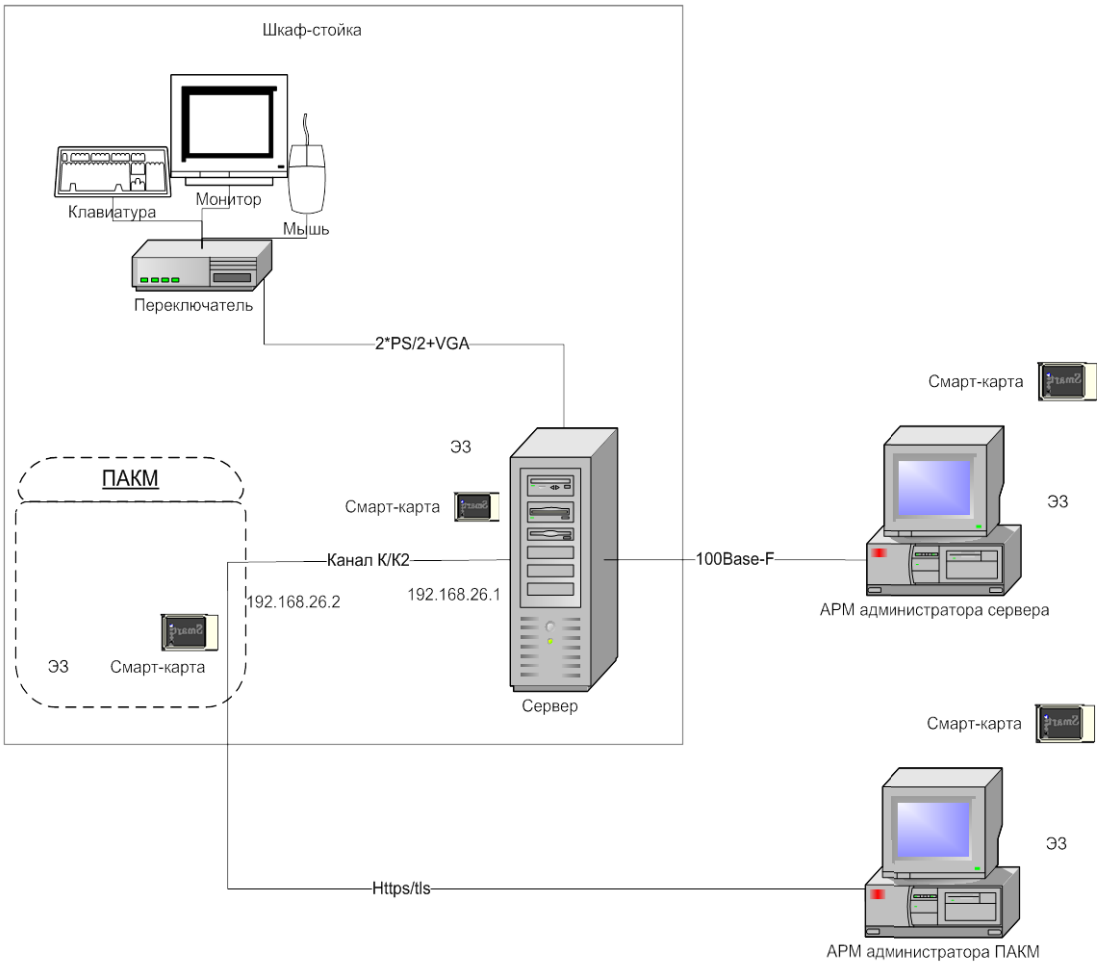

Рисунок 2 Схема подключения ПАКМ к серверу

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 пин-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.

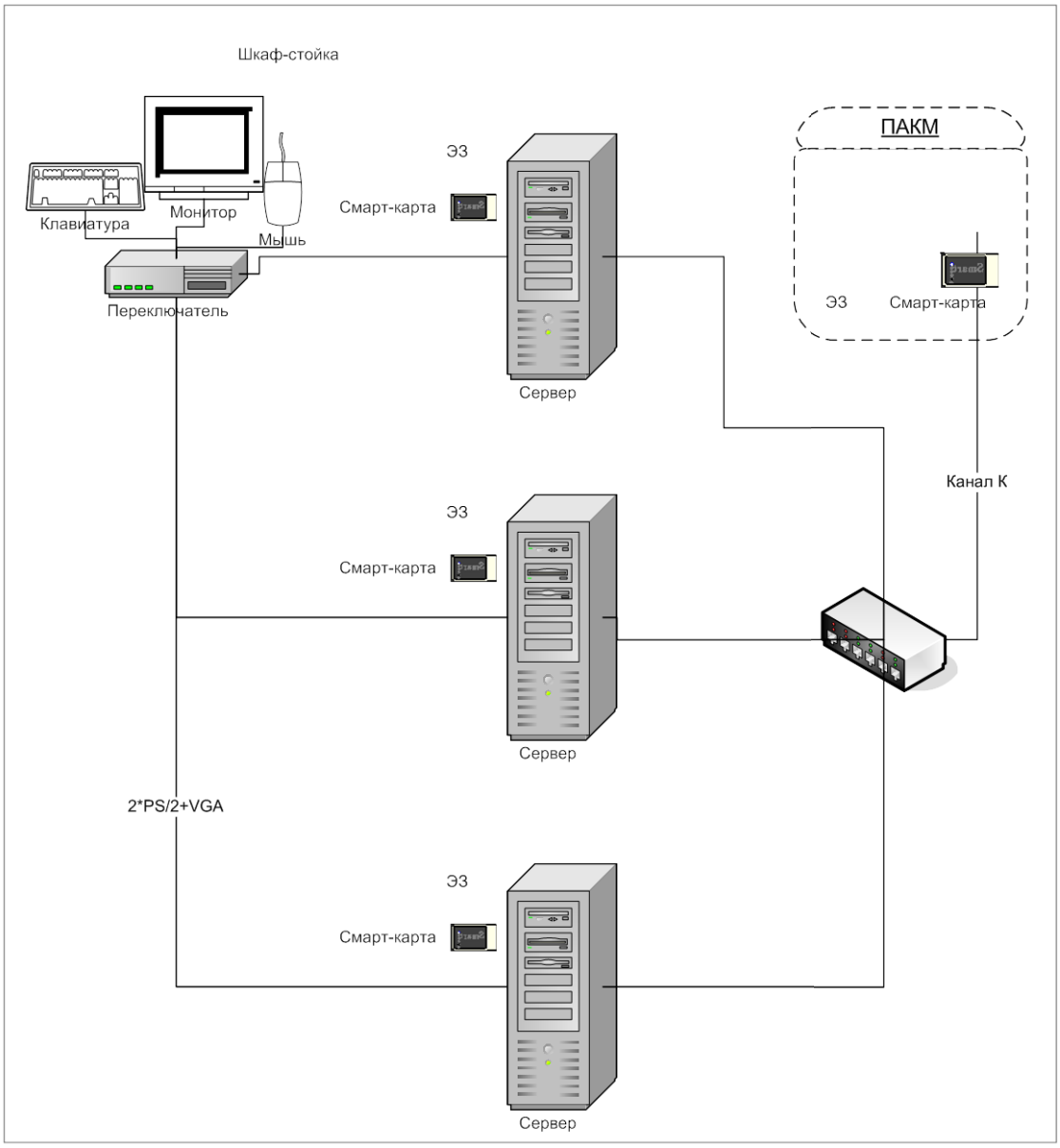

Рисунок 3 Схема подключения ПАКМ к нескольким серверам.

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.

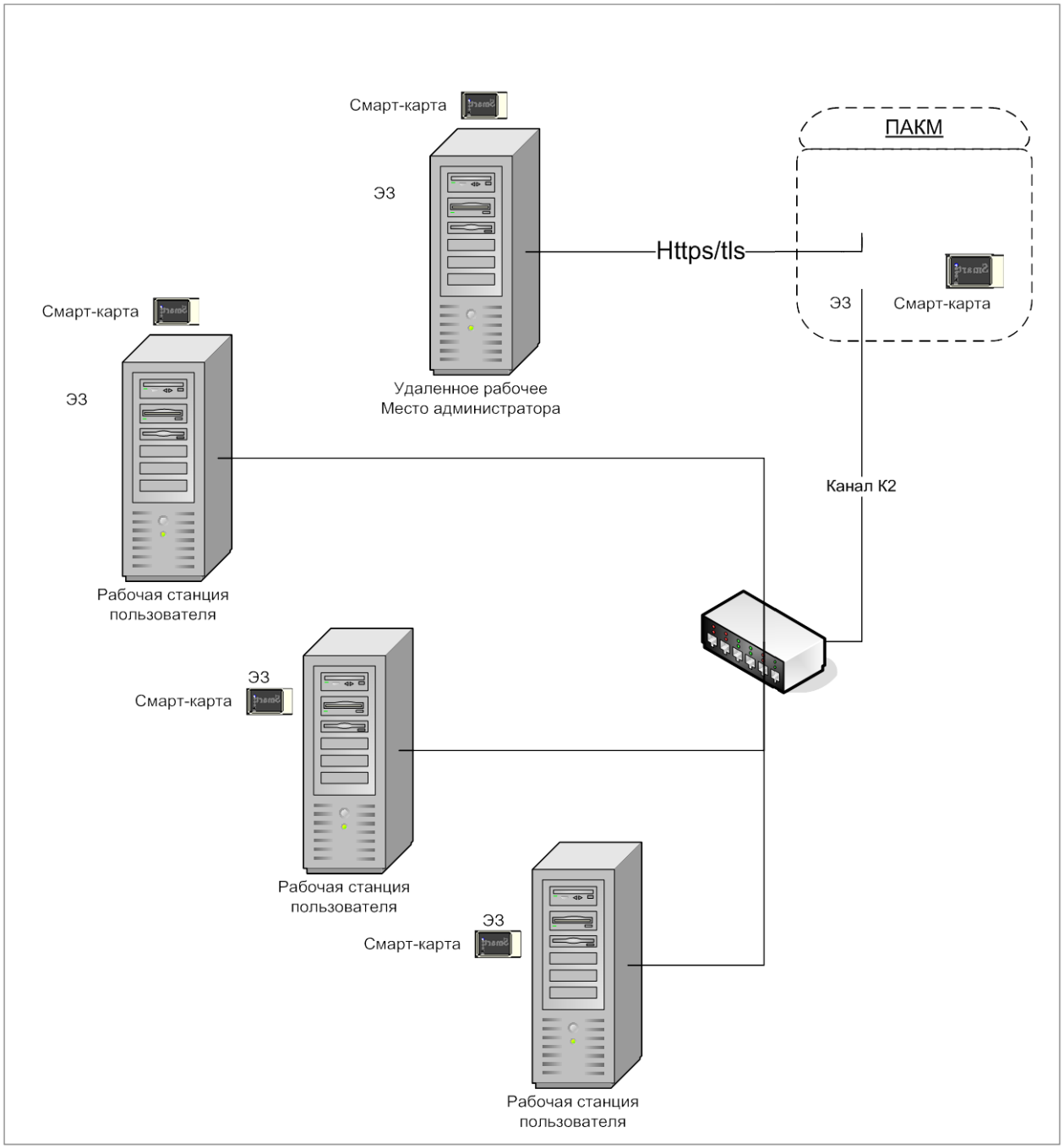

Рисунок 4. Схема подключения рабочих станций пользователей к ПАКМ.

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 контролируемой зоне, подключению сервера к ПАКМ по отдельному сетевому интерфейсу в отдельном выделенном для этой цели сегменте локальной сети. 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.

2. ОСНОВНЫЕ СВЕДЕНИЯ ОБ АППАРАТНОЙ ПЛАТФОРМЕ ПАКМ И СЕРВЕРА

Установка и эксплуатация СКЗИ ПАКМ «КриптоПро HSM» осуществляется в соответствии с документом "ЖТЯИ.00046-01 90 02. Правила пользования ПАКМ «КриптоПро HSM».

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 2.0");
- 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.

Обработка совершенно секретной и секретной информации с применением ПАКМ на объекте информатизации **запрещается.**

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 он применяется.

3. ИНСТРУКЦИИ ПО РАЗМЕЩЕНИЮ ТЕХНИЧЕСКИХ СРЕДСТВ

При размещении технических средств, имеющих в своем составе ПАКМ «КриптоПро HSM», следует руководствоваться следующими рекомендациями:

При эксплуатации ПАКМ необходимо обеспечить контролируемую зону не менее 6 метров при работе с конфиденциальной информацией без применения дополнительных мер спецзащиты.

Технические средства Серверов и ПАКМ «КриптоПро HSM» должны размещаться на единой контролируемой территории.

Вспомогательные технические средства и системы (телефонные аппараты, аппаратура оперативно-командной связи, модемы, датчики пожарной и охранной сигнализации, батареи центрального отопления и др. оборудование) необходимо располагать от ПАКМ не ближе расстояния = 0,3 метра.

Кабели связи телефонных аппаратов, аппаратуры связи, модемов необходимо располагать от ПАКМ не ближе расстояния = 0,15 метра.

Должны быть приняты меры по исключению несанкционированного доступа в помещения, в которых установлены технические средства Серверов, посторонних лиц, по роду своей деятельности не являющихся персоналом, допущенным к работе в этих помещениях.

Входные двери режимных помещений должны быть оборудованы замками, гарантирующими надежное закрытие помещений в нерабочее время.

Окна и двери должны быть оборудованы охранной сигнализацией, связанной с пультом централизованного наблюдения за сигнализацией.

Электропитание ПАКМ должно осуществляться от мотор-генераторной установки или понижающей трансформаторной подстанции, расположенных в пределах контролируемой зоны и не имеющих выхода низковольтных цепей за ее пределы, или через сетевой фильтр, например, типа ФП, ФСП или аналогичные. Цепи электропитания не должны иметь гальванических контактов с другими цепями, выходящими за пределы контролируемой зоны.

Контур заземления должен быть расположен в пределах контролируемой зоны объекта. Цепи заземления не должны иметь гальванических контактов с другими цепями, выходящими за пределы контролируемой зоны.

Размещение оборудования, технических средств, предназначенных для обработки конфиденциальной информации, должно соответствовать требованиям техники безопасности, санитарным нормам, а также требованиям пожарной безопасности.

Внутренняя планировка и расположение рабочих мест в помещениях должны обеспечивать исполнителям работ сохранность доверенных им конфиденциальных документов и сведений.

По окончании рабочего дня помещения закрываются и опечатываются. Помещения с опечатанными входными дверьми сдаются под охрану отделу безопасности или дежурному по

предприятию (по установленному порядку) с указанием времени приема-сдачи с отметкой о включении и выключении охранной сигнализации в журнале учета.

Сдачу ключей и помещений под охрану, также получение ключей и вскрытие помещений производят сотрудники, работающие в этих помещениях, по утвержденному руководством учреждения списку с образцами подписей этих сотрудников, который находится у охраны или у дежурного по учреждению.

Перед вскрытием помещений должна быть проверена целостность оттисков печатей и исправность замков. При обнаружении нарушения целостности оттисков печатей, повреждения замков или других признаков, указывающих на возможное проникновение в эти помещения посторонних лиц, помещение не вскрывается, а о случившемся немедленно ставится в известность руководство и отдел безопасности.

В случае утраты ключа от входной двери помещения немедленно ставится в известность отдел безопасности учреждения.

На случай пожара, аварии или стихийного бедствия должны быть разработаны специальные инструкции, утвержденные руководством учреждения, в которых предусматривается порядок вызова администрации, должностных лиц, вскрытие помещений, очередность и порядок спасения конфиденциальных документов и дальнейшего их хранения.

Запрещается использовать в помещении, где размещены рабочие места с установленным СКЗИ, радиотелефоны и другую радиоаппаратуру.

4. РОЛЕВАЯ МОДЕЛЬ ДОСТУПА К ФУНКЦИЯМ 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.

Данное требование реализовано с использованием ролевой модели доступа к различным функциям ПАКМ. 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, хранящихся в ПАКМ «КриптоПро HSM».

Программное обеспечение ПАКМ «КриптоПро HSM» различает следующие роли:

- Обычный пользователь СКЗИ ПАКМ «КриптоПро HSM»;
- Администратор сервера, сервисы которого используют СКЗИ ПАКМ «КриптоПро HSM»;
- Администратор ПАКМ «КриптоПро HSM»;
- Аудитор ПАКМ «КриптоПро HSM»;
- Администратор резервного копирования ПАКМ «КриптоПро HSM»;
- Привилегированный пользователь ПАКМ «КриптоПро HSM» - хранитель одной части разделенного секрета ключа активации ПАКМ;
- Суперпользователь ПАКМ «КриптоПро HSM».

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

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

Суперпользователь ПАКМ – группа привилегированных пользователей, как минимум из 3-х человек – держателей частей разделенного секрета ключа активации ПАКМ. Т.е. это любые три из пяти лиц, хранителей частей разделенного секрета ключа активации ПАКМ. Только данная группа лиц может локально получить доступ к функциям ПАКМ, позволяющим добавлять 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. Т.е. суперпользователь совмещает роли администраторов, аудиторов, администраторов резервного копирования ПАКМ. Смена разделенного ключа активации ПАКМ, включающая смену ключа шифрования ПАКМ, невозможна без активации старого ключа активации, т.е. без «присутствия суперпользователя».

Только суперпользователю доступен режим полной очистки содержимого ПАКМ;

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

Администратор сервера, сервисы которого используют СКЗИ ПАКМ «КриптоПро HSM» с точки зрения доступа к функциям ПАКМ почти ничем не отличается от обычного пользователя СКЗИ ПАКМ, за исключением того, что в сертификате ключа доступа к функциям ПАКМ прописывается специальное расширение (EKU) «1.2.643.2.2.34.22». Наличие в сертификате такого расширения приводит к тому, что запросы на ввод пин-кодов для ключей, создаваемых приложениями (сервисами операционной системы сервера) на сервере выдаются не на рабочий стол рабочей станции, как это происходит для обычных пользователей СКЗИ, а на LCD панель ПАКМ, 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 пин-код на доступ к контейнеру ключа. Кроме этого использование указанного сертификата ключа доступа к функциям ПАКМ в процессе аутентификации, позволяет при соответсвующих 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 СКЗИ ПАКМ;

- Очистка журнала аудита;

- Восстановление журнала аудита;

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".

Хранители частей секрета разделенного ключа активации ПАКМ могут являться одновременно привилегированными пользователями ПАКМ – администратором, аудитором, администратором резервного копирования ПАКМ;

Любое другое совмещение ролей привилегированных пользователей ПАКМ в одном лице при удовлетворении ПАКМ уровню криптографической защиты информации КВ2 не допускается.

5. ЗАЩИТА ОТ НСД

СКЗИ ПАКМ «КриптоПро HSM», обеспечивает защиту конфиденциальной информации, не содержащией сведений составляющих государственную тайну, от внешнего и внутреннего нарушителя, осуществляющего создание способов и подготовку атак с привлечением специалистов, имеющих опыт разработки и анализа криптосредств. Привилегированные пользователи, имеющие доступ в контролируемую зону, осуществляющие техническое обслуживание, настройку, конфигурирование ПАКМ и управление ключевой системой, относятся к потенциальным нарушителям. Возможность сговора между данными пользователями исключается.

5.1. Принципы защиты информации от НСД

Защита информации от НСД в автоматизированной системе обеспечивается комплексом программно-технических средств и поддерживающих их организационных мер. В их числе:

- применение специальных программно-аппаратных средств защиты;
- организация системы контроля безопасности информации;
- физическая охрана ПЭВМ и ее средств;
- администрирование информационной безопасности, основанное на разделении ролей административной группы;
- учет носителей информации;
- сигнализация о попытках нарушения защиты;
- периодическое тестирование технических и программных средств защиты;
- использование сертифицированных программных и технических и средств.

Защита информации от НСД должна обеспечиваться на всех технологических этапах обработки информации и во всех режимах функционирования, в том числе, при проведении ремонтных и регламентных работ.

Защита информации от НСД должна предусматривать контроль эффективности средств защиты от НСД. Этот контроль может быть либо периодическим, либо инициироваться по мере необходимости пользователем или контролирующими органами.

В организации, эксплуатирующей ПО СКЗИ, должна быть выпущена инструкция по защите от НСД к системе, разработанная на базе настоящего документа, руководящих документов Гостехкомиссии (ФСТЭК России), действующих нормативных документов самой эксплуатирующей организации.

В организации - пользователе системы должно быть выделено специальное должностное лицо - администратор безопасности, функции которого должны заключаться в выполнении процедур установки ПО, настройки системного окружения, установки, настройки, обслуживания и обеспечения функционирования средств защиты.

Администратор безопасности должен иметь возможность доступа ко всей информации, обрабатываемой на рабочем месте.

Каждый исполнитель работ как пользователь сети конфиденциальной связи должен быть зарегистрирован у администратора службы безопасности.

Должны быть приняты меры, исключающие возможность воздействия нарушителя на СКЗИ по каналам связи, выходящим за пределы контролируемой зоны.

5.2. Требования по защите от НСД.

СКЗИ ПАКМ «КриптоПро HSM» должно соответствовать требованиям по условиям применения – документ "ЖТЯИ.00046-01 90 02. Правила пользования ПАКМ «КриптоПро HSM».

Ремонт и сервисное обслуживание ПАКМ осуществляется в организациях, имеющих Лицензию Гостехкомиссии (ФСТЭК России) с правом проведения работ по п.п.3.8, 3.9 (ремонт и сервисное обслуживание средств защиты информации и средств информатизации в защищенном исполнении). При эксплуатации ПАКМ запрещается внесение изменений в состав компонент ПАКМ. После ремонта при необходимости проводится специальная проверка и специальные исследования отремонтированного оборудования.

Технические средства ПАКМ «КриптоПро HSM» не накладывают ограничений на ведение в помещении разговоров секретного содержания.

5.3. Применяемая модель защиты

Субъектами, связанными с функционированием Серверов/рабочих станций, взаимодействующих с ПАКМ «КриптоПро HSM», и потенциально могущими осуществить НСД, являются:

1) персонал службы безопасности - держатели ключей;
2) привилегированные пользователи ПАКМ: администратор ПАКМ, аудитор ПАКМ, администратор резервного копирования ПАКМ (осуществляют установку, настройку ПАКМ «КриптоПро HSM» и поддержку его функционирования);
3) администратор безопасности (осуществляет настройку подсистемы безопасности серверов приложений (например, Удостоверяющего центра) и поддержку организационных, организационно-технических и технических мер обеспечения безопасности);
4) операторы ППО Серверов/рабочих станций;
5) персонал, допущенный к работе на Сервере/рабочей станции;
6) технический персонал информационной системы, не допущенный к работе на ПАКМ «КриптоПро HSM», на Серверах и рабочих станциях учреждения;
7) пользователи ЛВС;
8) пользователи глобальной сети.

Для защиты от НСД с учетом перечисленных потенциальных нарушителей используются следующие средства и меры:

Шифрование всей ключевой системы ПАКМ на ключах шифрования ПАКМ, которые в свою очередь зашифрованы на ключе активации ПАКМ, разделенном по схеме 3 из 5-ти. Защитные ключи с разделенными частями секретов формируются на смарт картах МАГИСТР, ОСКАР (РИК)и распределяются между отдельными привилегированными пользователями из службы информационной безопасности учреждения;

парольная защита ключевого носителя на карте МАГИСТР, ОСКАР (РИК);

парольная система входа в ОС администратора системы, администратора безопасности, оператора (пароль входа в систему должен удовлетворять следующим требованиям: длина пароля не

менее 7 символов, среди символов пароля встречаются заглавные символы, прописные символы, цифры и специальные символы, срок смены пароля не реже одного раза в месяц, доступ к паролю должен быть обеспечен только администратору);

штатные средства разграничения доступа ОС Серверов и рабочих станций и встроенной ОС ПАКМ;

электронный замок "Соболь" для защиты от несанкционированного входа в систему;

ролевое разграничение доступа к ПАКМ со стороны привилегированных пользователей ПАКМ;

аутентификация ПАКМ «КриптоПро HSM» - Сервер с использованием системы аутентификации карты ОСКАР (РИК) (карты канала К);

аутентификация ПАКМ «КриптоПро HSM» - Сервер/рабочая станция с использованием системы аутентификации протокола TLS (реализация канала К2) с использованием ключей обмена на ключевых носителях в виде карт МАГИСТР, ОСКАР (РИК), USB устройств (eToken, ruToken);

локальная аутентификация привилегированных пользователей ПАКМ (из группы администраторов ПАКМ) с использованием системы аутентификации карты МАГИСТР, ОСКАР (карты канала К2);

штатные средства ОС ПАКМ - для защиты от воздействий со стороны Серверов/рабочих станций с целью НСД по каналам К, К2;

межсетевой экран четвертого класса для защиты от воздействия по глобальной сети.

5.4. Контроль целостности

ПАКМ «КриптоПро HSM» имеет встроенные функции контроля целостности ПО, которые выполняются периодически и с каждым запуском ПЭВМ. В качестве средств контроля целостности используются:

- средства электронного замка "Соболь";
- штатные средства встроенной ОС ПАКМ.

Контроль целостности ПО является 2-х этапным.

На первом этапе производится проверка всех файлов на загружаемом разделе /boot ПАКМ «КриптоПро HSM» (в данном разделе расположены загружаемое ядро ОС и конфигурационные файлы ОС, а стаже файлы с контрольными суммами всех файлов неизменяемого и монтируемого только на чтение раздела «/») - выполняется электронным замком "Соболь" до загрузки ОС. Проверка выполняется путем вычисления контрольной суммы и сравнением ее с предвычисленным значением.

На втором этапе (загрузка ОС) средствами ПО СКЗИ ПАКМ «КриптоПро HSM» вычисляются контрольные суммы всех файлов корневого раздела и сравниваются с вычисленными в момент изготовления ПАКМ, хранящимися в разделе /boot, контролируемым электронным замком.

Контроль целостности в ПАКМ «КриптоПро HSM» охватывает:

- модули криптопровайдера;
- ядро, модули ядра ОС, их конфигурационные файлы;
- модули канала К, К2;
- драйверы устройств и портов ввода ГМД, смарт-карт, com-порта, сети Ethernet;
- драйвер электронного замка "Соболь".

Кроме этого проверка контрольных сумм файлов осуществляется по расписанию (один раз в сутки).

В случае, если проверка дала отрицательный результат, ПАКМ останавливается (выполняется процедура halt).

Сервера и рабочие станции также имеют средства контроля целостности. В качестве средств контроля целостности используются:

- средства электронного замка;
- средства ПО криптопровайдера (CSP), обеспечивающего интерфейс к функциям ПАКМ.

Контроль целостности ПО является 2-х этапным.

На первом этапе производится проверка файлов средствами электронного замка до загрузки ОС. Проверка выполняется путем вычисления контрольной суммы и сравнением ее с предвычисленным значением.

На втором этапе средствами ПО криптопровайдера проверяются контрольные суммы файлов, входящих в комплект Сервера/рабочей станции. Контрольные суммы вычисляются при изготовлении дистрибутива для каждого файла отдельно и записываются в его заголовок по определенному смещению. Он охватывает:

- драйверы устройств и портов ввода смарт-карт, com-порта, сети Ethernet;
- программы отображения log-файлов;
- драйвер электронного замка.

Если в результате периодического контроля целостности или при загрузке операционной системы появляется сообщения о нарушении целостности контролируемого файла, пользователь обязан прекратить работу и обратиться к администратору безопасности.

Администратор безопасности, проанализировав причину, приведшую к нарушению целостности, должен переустановить ПО Сервера/рабочей станции с дистрибутива.

5.5. Организационные меры защиты

В данном разделе представлены основные рекомендации по организационным мерам защиты для обеспечения безопасности функционирования Серверов/рабочих станций (ПЭВМ), имеющего подключенное СКЗИ ПАКМ «КриптоПро HSM».

Использование шифровальных средств для криптографической защиты информации (в том числе и ПАКМ «КриптоПро HSM») подлежит лицензированию в соответствии с действующим законодательством РФ.

ПЭВМ должна быть аттестована комиссией. Результаты работы комиссии отражаются в "Акте готовности к работе" (см. Приложения).

Правом доступа к ПЭВМ должны обладать только лица, прошедшие соответствующую подготовку. Администратор безопасности должен ознакомить каждого пользователя с правилами пользования ("Правила пользования ПАКМ «КриптоПро HSM») или с другими нормативными документами, созданными на их основе.

Должностные инструкции администратора безопасности (его заместителя) и ответственного исполнителя должны учитывать требования настоящих Рекомендаций.

Администратором безопасности должно быть проведено опечатывание системного блока ПЭВМ, исключающее возможность несанкционированного изменения аппаратной части.

При каждом включении ПЭВМ необходимо проверять сохранность печатей системного блока и разъемов.

Администратор безопасности должен периодически (не реже 1 раза в 2 месяца) проводить контроль целостности и легальности установленных копий ПО на ПЭВМ с помощью программ контроля целостности.

В случае обнаружения "посторонних" (не зарегистрированных) программ, нарушения целостности программного обеспечения либо выявления факта повреждения печатей на системном блоке работа ПЭВМ должна быть прекращена. По данному факту должно быть проведено служебное расследование службой информационной безопасности организации – владельца ПЭВМ и организованы работы по анализу и ликвидации негативных последствий данного нарушения.

Пользователь должен запускать только те приложения, которые разрешены администратором безопасности.

ПО, установленное на ПЭВМ, не должно иметь встроенных средств разработки и отладки программ.

Пароли, назначаемые пользователям, должны отвечать требованиям соответствующих инструкции и нормативных документов.

На технических средствах ПЭВМ должно использоваться только лицензионное программное обеспечение фирм-производителей.

Необходимо исключить попадание в систему программ, позволяющих, пользуясь ошибками ОС, получать привилегии администратора.

Должны быть приняты меры по исключению несанкционированного доступа посторонних лиц в помещения, в которых установлены технические средства ПЭВМ, по роду своей деятельности не являющихся персоналом, допущенным к работе в указанных помещениях.

Из состава системы должно быть исключено все оборудование, которое может создавать угрозу безопасности ОС. Также следует избегать использования любых нестандартных аппаратных средств, имеющих возможность влиять на нормальный ход работы компьютера или ОС.

Если ПЭВМ подключена к общедоступным сетям связи, должны быть предприняты дополнительные меры, исключающие возможность несанкционированного доступа к системным ресурсам используемых операционных систем, к программному обеспечению, в окружении которого функционирует Сервер, и к компонентам ПЭВМ со стороны указанных сетей.

Не допускается:

Осуществлять несанкционированное копирование ключевых носителей.

Разглашать содержимое носителей ключевой информации или передавать сами носители лицам, к ним не допущенным, выводить ключевую информацию на дисплей и принтер (за исключением случаев, предусмотренных данными правилами).

Использовать ключевой носитель в режимах, не предусмотренных штатным режимом использования ключевого носителя.

Записывать на ключевой носитель постороннюю информацию.

Оставлять без контроля уполномоченных лиц вычислительные средства, входящие в состав СКЗИ, при включенном питании и загруженном программном обеспечении СКЗИ. При кратковременном перерыве в работе рекомендуется производить гашение экрана с возобновлением активности экрана по паролю доступа.

Подключать к Серверу и ПАКМ дополнительные устройства и соединители, не предусмотренные штатной комплектацией.

Эксплуатировать ПЭВМ и ПАКМ, если во время его начальной загрузки не проходит встроенный тест ОЗУ.

Вносить какие-либо изменения в программное обеспечение ПЭВМ и ПАКМ.

Изменять настройки, установленные программами установки ПАКМ «КриптоПро HSM» или администратором.

Использовать синхропосылки, вырабатываемые не средствами СКЗИ.

Обрабатывать на ПЭВМ информацию, содержащую государственную тайну.

Использовать бывшие в работе ключевые носители для записи новой информации без предварительного уничтожения на них ключевой информации средствами СКЗИ.

Осуществлять несанкционированное вскрытие системных блоков ПЭВМ и ПАКМ.

Запускать на ПЭВМ сервисы для удаленного входа пользователей из глобальной сети.

Устанавливать средства разработки и отладки ПО на ПЭВМ.

Приносить и использовать в помещении, где размещены ПЭВМ, радиотелефоны и другую радиопередающую аппаратуру (требование носит рекомендательный характер).

5.6. Организационно-технические меры защиты

На ПЭВМ должны быть установлены последние обновления программных продуктов, касающиеся безопасности.

Должен быть реализован следующий комплекс организационно-технических мер защиты от НСД:

В системе регистрируется один пользователь, обладающий правами администратора, на которого возлагается обязанность конфигурировать операционную систему ПЭВМ, настраивать безопасность ОС, а также конфигурировать оборудование ПЭВМ.

Для администратора выбирается надежный пароль входа в систему, удовлетворяющий следующим требованиям: длина пароля не менее 7 символов, среди символов пароля встречаются заглавные символы, прописные символы, цифры и специальные символы, срок смены пароля не реже одного раза в месяц, доступ к паролю должен быть обеспечен только администратору.

Всем пользователям, зарегистрированным в ОС, администратор в соответствии с политикой безопасности, принятой в организации, дает минимально возможные для нормальной работы права. Каждый пользователь ОС, не являющийся администратором, может просматривать и редактировать только свои установки в рамках прав доступа, назначенных ему администратором.

На компьютере устанавливается только одна ОС. Не должны использоваться нестандартные, измененные или отладочные версии операционных систем.

Права доступа к каталогам ПЭВМ должны быть установлены в соответствии с политикой безопасности, принятой в организации.

Должна быть проведена установка атрибутов безопасности процессов и потоков в соответствии с требованиями безопасности всей системы в целом.

В случае подключения ПЭВМ с установленным ПАКМ к общедоступным сетям передачи данных должно быть исключено использование JavaScript, VBScript, ActiveX и других программных объектов, загружаемых из сети.

Должна быть отключена возможность удаленного администрирования ПЭВМ с установленным ПАКМ для всех пользователей.

Должен быть закрыт доступ ко всем не используемым портам.

Должны быть исключены исполнение и открытие файлов, полученных из общедоступных сетей передачи данных, без проведения соответствующих проверок на предмет содержания в них программных закладок и вирусов.

Должны быть удалены все общие ресурсы на ПЭВМ, которые не используются. Права доступа к используемым общим ресурсам должны быть заданы в соответствии с политикой безопасности, принятой в организации.

Должна быть разработана система назначения и смены паролей.

Должно быть ограничено количество неудачных попыток входа в систему, в соответствие с политикой безопасности, принятой в организации. Рекомендуется блокировать систему после трех неудачных попыток.

Должна использоваться система аудита в соответствие с политикой безопасности, принятой в организации, и организован регулярный анализ результатов аудита.

Должен проводиться регулярный просмотр сообщений в журналах событий ОС, ППО ПЭВМ и ПАКМ «КриптоПро HSM».

Должна быть исключена возможность создания аварийного дампа оперативной памяти, так как он может содержать криптографически опасную информацию.

Средствами BIOS должна быть исключена возможность отключения пользователями ISA и PCI устройств при использовании программно-аппаратных средств защиты от НСД, устанавливаемых в ISA и PCI разъем. В BIOS ПЭВМ определяются установки, исключающие возможность загрузки операционной системы, отличной от установленной на жестком диске: отключается возможность загрузки с гибкого диска, привода CD-ROM и прочие нестандартные виды загрузки ОС, включая сетевую загрузку. Не применяются ПЭВМ с BIOS, исключающим возможность отключения сетевой загрузки ОС.

Вход в BIOS ПЭВМ должен быть защищен паролем, к которому предъявляются те же требования, что и к паролю администратора (длина пароля не менее 7 символов, среди символов пароля встречаются заглавные символы, прописные символы, цифры и специальные символы, срок смены пароля не реже одного раза в месяц). Пароль для входа в BIOS должен быть известен только администратору и быть отличным от пароля администратора для входа в ОС.

Средствами BIOS должна быть исключена возможность работы на ПЭВМ, если во время его начальной загрузки не проходят встроенные тесты.

При загрузке ОС должен быть реализован контроль целостности программного обеспечения, входящего в состав криптопровайдера, самой ОС и всех исполняемых файлов, функционирующих совместно с СКЗИ. Данное требование обеспечивается средствами электронного замка и встроенными функциями ПАКМ «КриптоПро HSM».

Должно быть реализовано физическое затирание содержимого удаляемых файлов.

Должна быть исключена возможность использования в составе ПЭВМ аппаратных средств поддержки удаленного администрирования (Remote Insight Board/PCI всех модификаций).

Должна быть исключена возможность использования программного обеспечения, поддерживающего технологию удаленного управления (Compaq Insight Manager, Remote ROM Flash Setup Utility, COMPAQ MultiNIC Boot Utility и т.п.).

5.7. Электронный замок

Система Электронного замка в ПАКМ предназначена для организации защиты компьютера от входа посторонних пользователей (защита от НСД). Под посторонними пользователями понимаются все лица, не зарегистрированные в системе электронного замка как пользователи данного компьютера.

Система электронного замка обеспечивает:

- регистрацию пользователей компьютера и назначение им персональных идентификаторов и паролей на вход в систему;
- запрос персонального идентификатора и пароля пользователя при загрузке компьютера;
- возможность блокирования входа в систему зарегистрированного пользователя;
- ведение системного журнала, в котором производится регистрация событий, имеющих отношение к безопасности системы;
- контроль целостности файлов на жестком диске;
- контроль целостности физических секторов жесткого диска;
- аппаратную защиту от несанкционированной загрузки операционной системы с гибкого диска и CD-ROM диска.

Так же система электронного замка включает в себя физический датчик случайных чисел, используемый криптографическими функциями ПАКМ «КриптоПро HSM».

Установка и настройка электронного замка ПАКМ производится предприятием-изготовителем. Настройка исключает возможность вмешательства пользователя в процессы загрузки операционной системы и прикладного ПО и проверки целостности программной среды.

Ключи электронного замка ("таблетки"), без которых невозможна загрузка ПАКМ, должны находиться в ведении администратора безопасности.

Ключи электронного замка разделяются на 2 вида:

- ключи администратора;
- ключи пользователя (в заказанном количестве, не менее 2 шт.).

Ключи администратора используются только сотрудниками предприятия-изготовителя для осуществления изготовления (настройки) ПАКМ и уничтожаются после завершения изготовления изделия.

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

Ключи электронного замка относятся к категории ключевых носителей, подлежат соответствующему учету и хранению.

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 СКЗИ 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;
- Идентификации/аутентификации/авторизации 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 СКЗИ 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 Аудитора 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 аудитором возможна как с LCD панели, так и через web-интерфейс администрирования.

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 порции журнала аудита от одного момента «восстановления» (!!!) БД журнала аудита до другого, т.е. при обычной очистке журнала нумерация записей продолжается, а после выполнения операции восстановления БД начинается с единицы).

HSMID – идентификатор (серийный номер) ПАКМ;

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

EventTime – дата и время события;

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

EventType - тип события;

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

BinaryData – дополнительные двоичные данные - результат выполнения криптографической операции (значение ЭЦП, 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 ЭЦП пользователем ПАКМ;

EVENT_TYPE_CRYPT_VERIFYSIGNATURE (24) - Проверка ЭЦП 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 секретного ключа;

EVENT_TYPE_CRYPT_IMPORT_KEY (31) – Импорт секретного ключа в контейнер ПАКМ;

EVENT_TYPE_CREATE_NEW_BACKUP (32) – создание резервной копии внутри ПАКМ;

EVENT_TYPE_DELETE_BACKUP (33) – удаление резервной копии внутри ПАКМ;

EVENT_TYPE_RESTORE_FROM_BACKUP (34) – восстановление из резервной копии ПАКМ;

EVENT_TYPE_DOWNLOAD_BACKUP (35) – выгрузка резервной копии;

EVENT_TYPE_CHANGE_AUDIT_OPTIONS (36) – изменение настроек аудита;

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

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 опция, влияющих процессы журналирования.

Журналы аудита в текстовом виде переписываются на рабочую станцию Администраторов ПАКМ при помощи web-интерфейса администратора ПАКМ.

Стирание журналов событий СКЗИ и аудита в ПАКМ должно производиться аудитором 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 после аутентификации Администратора ПАКМ.

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. ПРИЛОЖЕНИЯ

Приложение 1. Акт готовности к работе

УТВЕРЖДАЮ

_____

(должность)

_____

(наименование учреждения)

_____

(подпись) (Ф.И.О.)

АКТ

готовности к работе _____ с _____

(наименование учреждения) (наименование изделий)

"_____" _____ 200__г.

Комиссия в составе председателя _____ _____ и членов

(должность) (Ф.И.О.)

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 Должность:	01.05.2000		Оператор расчетной системы

Приложение 3. Журнал пользователя сети

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

Лист регистрации изменений

Номера листов (страниц)					Всего листов (страниц) в докум.	№ документа	Входящий № сопроводи-тельного документа и дата	Подпись	Дата
Изм.	измененных	Замененных	новых	аннули-рованных					