Федеральное государственное унитарное предприятие
«НАУЧНО-ТЕХНИЧЕСКИЙ ЦЕНТР «АТЛАС»

название изделия

Программно-аппаратный комплекс (ПАК) «Криптосервер»

назначение, область применения

Программно-аппаратный комплекс (ПАК) «Криптосервер» осуществляет криптографическую защиту конфиденциальной информации и защиту от несанкционированного доступа.
Поставляется в версии 1.0 (Сертификат соответствия ФСБ России – СФ/124-2336 от 10.03.2014, класс защиты КВ2) и в версии 3.0 (Сертификат соответствия ФСБ России – СФ/124-2337 от 10.03.2014, класс защиты КС3).

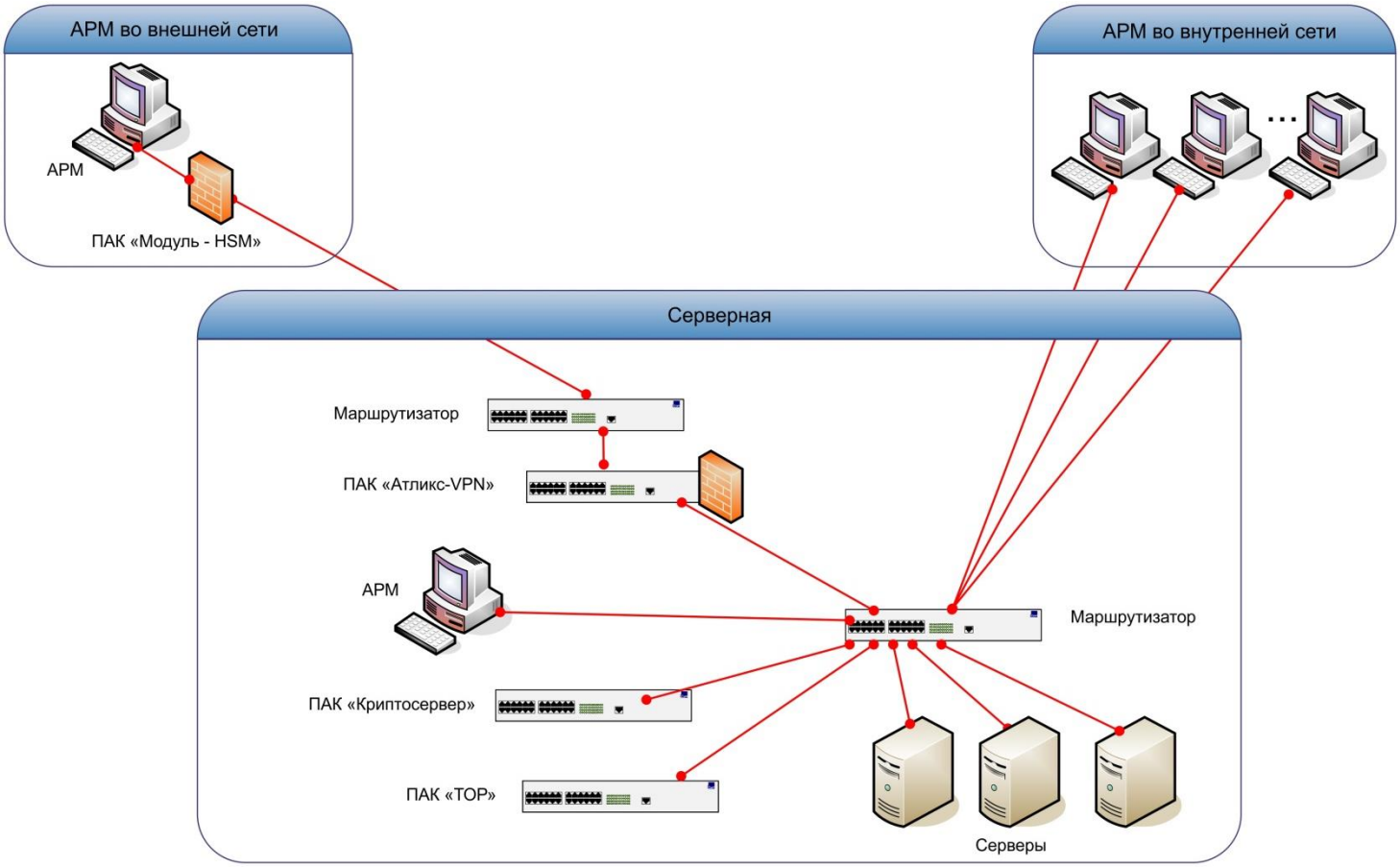
Комплекс выполнен в виде отдельного аппаратного модуля, подключаемом к ЛВС и АРМ пользователя согласно схеме.

Состав комплекса ПАК «Криптосервер»:

- Криптографическая система;
- Средства защиты от сетевых атак;
- Средства защиты от НСД;
- Система аудита;
- Система разграничения доступа;
- Система интерфейсов взаимодействия с пользователем: CORBA-интерфейс и XML RPC-интерфейс;
- Сервисы работы с цифровыми сертификатами.

Программное обеспечение комплекса образует замкнутую программную среду, образованную данными компонентами.

схема подключения ПАК «Криптосервер» и ПАК «ТОР»



основные технические характеристики изделия

ПАК «Криптосервер» обеспечивает реализацию следующих алгоритмов криптографической защиты информации:

- ГОСТ 28147-89;
- ГОСТ Р34.10-2001;
- ГОСТ Р34.11 – 94.

Криптографическая система на основе вышеперечисленных алгоритмов реализует функции криптографической защиты, позволяющие гарантировать конфиденциальность, подлинность и целостность данных.

ПАК «Криптосервер» также поддерживает протокол EAC (BSI TR 069) для защищенного взаимодействия с машинно-читаемыми проездными документами включая рекомендованный ICAO набор криптографических алгоритмов.

ПАК «Криптосервер» обеспечивает возможность удаленного вызова функций криптографической защиты на основе технологии удаленного вызова процедур.

ПАК «Криптосервер» содержит комплекс программных средств защиты от сетевых атак, направленных на захват и эскалацию привилегий.

Программное обеспечение ПАК «Криптосервер» обеспечивает невозможность несанкционированного доступа к закрытым ключам электронной подписи (ЭП).

ПАК «Криптосервер» обеспечивает выполнение следующих функций:

- контроль подлинности и целостности данных;
- вычисление электронной подписи на основе закрытых ключей ЭП.

Время инициализации ПАК «Криптосервер» не превышает 3 минут.

Инициализация работы ПАК «Криптосервер» происходит при получении запроса на установление соединения с АРМ при вставленной в кардридер карте РИК.

ПАК «Криптосервер» имеет функции самотестирования.

Информация аудита работы ПАК хранится в файлах аудита комплекса с возможностью перенаправления данных аудита на внешнее хранилище данных аудита.

Криптосистема комплекса «Криптосервер» использует ключи двух типов:

- ключи шифрования, реализованного в соответствии с ГОСТ 28147-89.
- ключи электронной подписи.

Используемые ключевые носители – РИК-2.

Комплекс обеспечивает аутентификацию владельца ключевой информации в ходе загрузки ключей с ключевых носителей на основе кода доступа (PIN-кода).

Обмен информацией между АРМ пользователя и ПАК «Криптосервер» производится с использованием протокола TLS на основе отечественных криптоалгоритмов.

Управление комплексом осуществляется с АРМ администратора или локально.

ПАК «Криптосервер» предоставляет администратору комплекса Web-интерфейс управления.

Через интерфейс должно быть доступно управление следующими параметрами:

- Конфигурация сетевых интерфейсов (IP-адрес, маска подсети и т.д.);
- Конфигурация интерфейсов взаимодействия с пользователями;
- Конфигурация параметров ведения журналов аудита;

Настройки правил фильтрации.

контакты

127018, г. Москва, ул. Образцова, 38
телефон: (495) 689-14-64
e-mail: info@stcnet.ru
http://web.stcnet.ru