Continent  
  
1. **Для чего предназначен АПКШ "Континент"?**

АПКШ "Континент" предназначен для организации защиты сетевого периметра и обеспечения конфиденциальности данных при их передаче по общедоступным каналам связи. Использование комплекса в том числе позволяет:

• объединить через сети общего доступа распределенные локальные вычислительные сети или географически удаленные сегменты одной подсети в единую VPN;

• обеспечить безопасное подключение ЛВС к сетям общего пользования с помощью межсетевого экранирования;

• организовать доступ пользователей ЛВС к ресурсам сети Интернет с одного IP-адреса;

• скрыть внутреннюю структуру ЛВС;

• осуществить подключение удаленных пользователей к ресурсам VPN;

• выявить преднамеренный несанкционированный доступ к информации;

• автоматически регистрировать в соответствующих журналах события, связанные с функционированием комплекса и попытками НСД;

• централизованно управлять компонентами комплекса.

Комплекс предназначен для работы в сетях, использующих для передачи данных протоколы семейства TCP/IP версии 4, а также в общих сетях передачи данных, поддерживающих протоколы

2. **Что такое криптографический шлюз?**

криптографический шлюз (КШ) – аппаратно-программное средство на базе компьютера с архитектурой х86 , имеющее несколько вариантов исполнения :

Криптографический шлюз функционирует совместно с предустановленным изделием "Программно-аппаратный комплекс "Соболь". Версия 3.0" (далее — ПАК "Соболь") и имеет следующие варианты исполнения:

• криптографический шлюз. В данном исполнении КШ обеспечивает:

- криптографическую защиту данных, передаваемых по каналам связи общих сетей передачи данных между составными частями VPN (локальными вычислительными сетями и отдельными компьютерами удаленных пользователей);

- защиту составных частей VPN от несанкционированного доступа (НСД) посредством межсетевого экранирования;

• криптографический коммутатор – обеспечивает защищенную передачу Ethernet-кадров (L2) через сети общего пользования между территориально разделенными сегментами сети предприятия с использованием шифрованных (L3) VPN-туннелей Континент (L2VPN);

3. **Можно ли установить ПО ЦУС без КШ?**

Нет, ВМ **KSH-main** предназначена для установки ПО основного криптографического шлюза "Континент".

**4. Какие криптошлюзы могут иметь одинаковый идентификатор?**

Исключение составляют основное и резервное сетевые устройства в кластере, – у них идентификатор должен быть одинаковым

**5. Что означает число 7 в строке конфигурации КШ 000000074em0\*02BDem1\*02BDem2\*02BDem3\*02BDffff?**

- номер модели аппаратной платформы **7** – IPC-100 (S102);

- внешний интерфейс:

номер – **1** (em0), IP-адрес шлюза – **196.115.92.1/24**;

- внутренний интерфейс:

номер – **3** (em2), IP-адрес шлюза – **10.0.1.1/24**;

- адрес маршрутизатора по умолчанию – **196.115.92.254**;

- пароль ключа администратора ЦУС – **11111**.

**6. В какой момент формируется ключ главного администратора ЦУС?**

В процессе инициализации ЦУС из исходного ключевого материала формируются ключ главного администратора комплекса и ключ хранения ЦУС (в качестве такого источника может быть использован ПАК "Соболь" или заказанный в установленном порядке в ЦБС ФСБ России комплект ключевого блокнота РДП-006). Одновременно на ЦУС также формируются ключ связи с ЦУС и главный ключ КШ. В данном случае КШ устанавливается и функционирует совместно с ЦУС.

**7.** **Где устанавливается подсистема управления комплексом?**

На АРМ администратора комплекса (ВМ ARM) установлена подсистема управления ЦУС.

**8. Что нужно предъявить при подключении ПУ ЦУС к ЦУС?**

После подключения ПУ ЦУС к ЦУС с использованием ключа главного администратора становится доступным функционал по созданию криптографических устройств (КШ, КК, ДА)

**Глава 2.**

1. **Для чего используется ключ хранения ЦУС? На каком этапе и где он формируется?**

Ключ хранения ЦУС используется для безопасного хранения БД ЦУС на жестком диске КШ с ЦУС. Он сохраняется в энергонезависимой памяти ПАК "Соболь", установленного на ЦУС.

Администратор устанавливает на сетевое устройство ПО КШ с ЦУС. При инициализации ЦУС генерируются следующие ключи:

• **ключ хранения ЦУС** – записывается в ПАК "Соболь", установленный на этом КШ. Для администратора этот процесс не виден;

2. **Какие ключи записываются в файл "keyset" с помощью ПУ ЦУС?**

• ключ связи с ЦУС;

• главный ключ КШ.

3. **Как организуется защищенное соединение между ПУ ЦУС и ЦУС?**

При установке и инициализации ПО КШ администратор загружает с полученного внешнего носителя файл "keyset" с ключами на устройство, где ключ связи с ЦУС и главный ключ КШ записываются в ПАК "Соболь", установленный на этом КШ. В результате устанавливается защищенное соединение между КШ и ЦУС.

4. **На каком устройстве формируются главный ключ сетевого устройства и ключ связи с ЦУС по схеме однолетнего хранения? По схеме трехлетнего хранения?**

Пара ключей – главный ключ сетевого устройства и ключ связи с ЦУС – формируется для каждого подчиненного ЦУС сетевого объекта (КШ, КК, ДА).

Если действует вариант схемы трехлетнего хранения ключевой информации, то администратор выполняет следующие действия:

• генерирует ключи (главный ключ сетевого устройства и ключ связи с ЦУС) для управляемых ЦУС устройств на отдельном устройстве АРМ ГК;

• сохраняет ключи (файл "keyset" c парами ключей) на съемный диск;

• устанавливает в настройках ПУ ЦУС режим управления ключевой информацией по схеме трехлетнего хранения;

Автоматизированное рабочее место генерации ключей (АРМ ГК)

**Комплекс поддерживает два режима управления ключами: по схеме однолетнего и трехлетнего хранения ключевой информации.**

**При использовании схемы трехлетнего хранения ключевой информации (усиленной схемы распределения ключей) на отдельном, не имеющем сетевых соединений АРМ ГК генерируются главные ключи КШ и ключи связи с ЦУС. Сгенерированные комплекты ключей записываются на отчуждаемые носители (USB-ключи), которые передаются администраторам. Срок действия/хранения таких ключей составляет три года.**

**АРМ ГК имеет в основе системный блок на аппаратной платформе IPC-10 (см. ниже) с установленным ПО под управлением ОС FreeBSD.**

**Подробнее см. в руководстве администратора по АРМ генерации ключей АПКШ "Континент" 3.7.-**

**ГЛАВА 3**

1. **Какие функции выполняет межсетевой экран?**

Межсетевой экран в комплексе представляет собой программное обеспечение, реализующее выполнение правил, которые определяют условия прохождения сетевых пакетов из одной подсети в другую. Правила формируются на основе IP-адресов отправителя и получателя, типов протоколов, номеров портов TCP/UDP и имен сетевых интерфейсов. МЭ поддерживает технологию Statefull inspection.

защита и изоляция пользователей внутренней сети от нежелательного трафика, поступающего из внешней сети Интернет;

• ограничение или запрещение доступа пользователей внутренней сети к сервисам внешней сети;

• обеспечение отказоустойчивости канала связи;

• выполнение приоритизации трафика (QoS);

• поддержка преобразования сетевых адресов (network address translation, NAT), что дает возможность задействовать во внутренней сети локальные IP-адреса и совместно использовать одно подключение к сети Интернет (либо через один выделенный IP-адрес, либо через адрес из пула автоматически присваиваемых публичных адресов).

МЭ выполняет фильтрацию входящего и исходящего трафика, идущего через КШ, при этом фильтрация сетевого пакета выполняется дважды – на входящем и исходящем сетевом интерфейсе.

МЭ функционирует на 3 уровне модели OSI. Реализация проверки сетевых пакетов обеспечивается с помощью набора правил. Правила фильтрации формируются на основе IP-адресов отправителя и получателя, типов протоколов IP, сервисов. МЭ позволяет контролировать прохождение трафика или блокирует его.

МЭ поддерживает технологию контроля состояния соединений (stateful packet inspection, SPI). МЭ при включенной функции SPI для каждого установленного соединения сохраняет определенную информацию (адрес отправителя, адрес получателя, номера портов) в динамической таблице состояния соединений. При прохождении пакета через криптошлюз МЭ определяет, принадлежит ли данный пакет установленному соединению. Если информация о нем есть в таблице состояния соединений – пакет пропускается, минуя правила фильтрации.

Технология контроля состояния соединений повышает производительность МЭ. При включенной функции SPI написание правил фильтрации, разрешающих прохождение трафика в обратном направлении, не требуется. Например, браузер из доверенной сети соединяется с сервером в Интернете, разрешение для прохождения исходящего трафика администратор указывает явно правилом. Запрос от браузера поступает на сервер, МЭ устанавливает соединение, означающее ожидание данных с сервера.

При написании правила, разрешающего прохождение исходящего трафика без SPI, запрос от браузера на сервер поступит, а ответ от него МЭ заблокирует. Вот для чего необходимо включение функции SPI. Таблица состояния соединений поддерживается динамически.

Недостаток МЭ с включенной функцией SPI состоит в том, что он может быть уязвим для DoS-атак. В АПКШ "Континент" МЭ поддерживает технологию защиты от DoS-атак, а также при необходимости есть возможность использовать МЭ без контроля состояния соединений.

На рисунке ниже представлена схема фильтрации IP-пакетов с включенной функцией контроля состояния соединений в АПКШ "Континент".

2. **Для чего предназначена технология "Контроль состояния соединений" в пакетном фильтре, применяемом в АПКШ "Континент"?**

keep state label "P0511" – включен режим "контроль состояния соединений", разрешающий прохождение "обратных" пакетов от получателя к отправителю в рамках данного соединения (технология Statefull inspection);

3. **Что понимается под сетевым объектом в ПУ ЦУС?**

сетевой объект – определяет в правилах трансляции источника и получателя IP-пакетов. Можно задать отдельный хост, сеть, группу пользователей (с привязкой к сетевому объекту). В случае использования в правиле группы пользователей на соответствующих сетевых объектах должно быть установлено ПО "Клиент аутентификации пользователя

4. **В каких целях используется трансляция сетевых адресов?**

Трансляция сетевых адресов

Комплекс поддерживает технологию трансляции IP-адресов – замены (в зависимости от типа трансляции) IP-адресов источника или назначения, что позволяет скрывать внутреннюю структуру локальной сети и предоставлять пользователям с внутренней IP-адресацией доступ к внешним сетям общего пользования, а также обеспечивать доступ извне к внутрисетевым сервисам

Трансляция сетевых адресов (Network Address Translation) в АПКШ "Континент" используется для преобразования IP-адреса транзитных пакетов и решает следующие задачи:

• предоставление пользователям с неуникальными внутрисетевыми адресами доступа к внешним сетям общего пользования;

• обеспечение доступа извне к внутрисетевым сервисам – по определенным портам либо с переопределением портов, либо по всем портам.

В АПКШ "Континент" трансляция адресов может настраиваться в двух направлениях – входящем и исходящем.

Трансляция адресов в исходящем направлении определяет работу с трафиком, исходящим из локальной сети в сеть Интернет. Когда пользователь из локальной сети обращается к внешним ресурсам из сети общего доступа, в передаваемом пакете в качестве отправителя указан его локальный адрес, который недоступен извне. Поэтому КШ транслирует (подменяет) локальный IP-адрес отправителя пакета на свой внешний (видимый из Интернета) IP-адрес и меняет номер порта отправителя (чтобы различать ответные пакеты, адресованные разным локальным компьютерам). Комбинацию, нужную для обратной подстановки (номер порта–локальный адрес отправителя), криптошлюз сохраняет у себя во временной таблице. Через некоторое время после того, как пользователь локальной сети и сервер из сети общего доступа закончат обмениваться пакетами, КШ удалит в таблице запись о данной сессии.

5. **В чем заключается суть** **технологии исходящего транслирования адресов?**

|  |  |
| --- | --- |
| Исходящие | Инициатор соединения – пользователь внутренней сети. В исходящих IP-пакетах внутрисетевой IP-адрес отправителя заменяется на указанный публичный. Имеется возможность динамического выбора из диапазона публичных адресов. Во входящих IP-пакетах, соответствующих данному соединению, публичный адрес получателя заменяется на соответствующий внутрисетевой |

6. **В чем заключается суть технологии входящего транслирования адресов?**

Инициатор соединения – сторонний пользователь, которому известен только публичный IP-адрес получателя. Во входящих IP-пакетах публичный IP-адрес получателя заменяется на указанный внутрисетевой. Порт назначения у входящих IP-пакетов можно также переопределить. В исходящих IP-пакетах, соответствующих данному соединению, внутрисетевой адрес отправителя заменяется на соответствующий публичный

7. **Какие условия необходимо выполнить при создании входящих правил трансляции?**

При создании входящих правил трансляции нельзя в качестве получателя выбрать "Любой"! Порт следует указать обязательно.