КОД безопасности

Аппаратно-программный комплекс шифрования

Континент

Версия 3.9

Руководство администратора

Принципы функционирования комплекса

RU.88338853.501430.022 90 1

Почтовый адрес:	**115127, Россия, Москва, а/я 66 ООО "Код Безопасности"**
Телефон:	**8 495 982-30-20**
E-mail:	**info@securitycode.ru**
Web:	**https://www.securitycode.ru**

Оглавление

Список сокращений

АП	Абонентский пункт
АПКШ	Аппаратно-программный комплекс шифрования
БД	База данных
КА	Клиент аутентификации
КК	Криптографический коммутатор
КШ	Криптографический шлюз
ЛВС	Локальная вычислительная сеть
НСД	Несанкционированный доступ
ОС	Операционная система
ПАК	Программно-аппаратный комплекс
ПО	Программное обеспечение
ПУ	Программа управления
РМ	Рабочее место
СД	Сервер доступа
ЦУС	Центр управления сетью
FTP	File Transfer Protocol
IP	Internet Protocol
NAT	Network Address Translation
PPPoE	Point to Point Protocol over Ethernet
SNMP	Simple Network Management Protocol
SSH	Secure Shell
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
USB	Universal Serial Bus
VoIP	Voice over IP
VPN	Virtual Private Network

Введение

Документ предназначен для администраторов изделия "Аппаратно-программный комплекс шифрования "Континент". Версия 3.9" (далее — комплекс, АПКШ "Континент"). В нем содержатся сведения, необходимые администраторам для ознакомления с назначением, составом и принципами функционирования комплекса.

Сайт в интернете. Информация о продуктах компании "Код Безопасности" представлена на сайте https://www.securitycode.ru.

Служба технической поддержки. Связаться со службой технической поддержки можно по телефону 8 800 505-30-20 или по электронной почте support@securitycode.ru.

Учебные курсы. Освоить аппаратные и программные продукты компании "Код Безопасности" можно в авторизованных учебных центрах. Список учебных центров и условия обучения представлены на сайте компании https://www.securitycode.ru. Связаться с представителем компании по вопросам организации обучения можно по электронной почте education@securitycode.ru.

Версия — 3.9.3 от 03.04.2024.

Глава 1
Назначение комплекса

Технология VPN позволяет объединить локальные вычислительные сети, их сегменты или отдельные компьютеры предприятия в единую защищенную виртуальную сеть на базе общих сетей передачи данных. Переход от распределенной корпоративной сети на базе выделенных каналов к VPN позволяет существенно снизить эксплуатационные расходы. Однако использование общих сетей для организации VPN предъявляет дополнительные требования к обеспечению надежной защиты информационных ресурсов предприятия от несанкционированного доступа.

АПКШ "Континент"предназначен для построения виртуальных частных сетей на основе общих сетей передачи данных, использующих протоколы семейства TCP/IP.

Комплекс реализует следующие основные функции:

- криптографическая защита данных, передаваемых по каналам связи общих сетей передачи данных между составными частями VPN;
- предоставление доступа удаленным пользователям к ресурсам защищаемой сети;
- межсетевое экранирование;
- обнаружение вторжений в информационную систему;
- автоматическая регистрация событий, связанных с функционированием комплекса, в том числе событий НСД;
- централизованное управление 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 IPv6.

Глава 2
Состав комплекса

В состав АПКШ "Континент" входят следующие компоненты:

- криптографический шлюз;
- детектор атак;
- сервер доступа;
- ЦУС;
- программа управления комплексом:
  - программа управления ЦУС;
- клиент аутентификации пользователя.

Компоненты комплекса можно устанавливать как на аппаратных, так и на виртуальных платформах.

Криптографический шлюз

Криптографический шлюз представляет собой программное средство, предварительно устанавливаемое на специализированную аппаратную платформу с архитектурой x64.

Примечание.
Далее в эксплуатационной документации под термином криптографический шлюз понимается как программное обеспечение, устанавливаемое на аппаратную платформу, так и аппаратная платформа с установленным программным обеспечением КШ.

Криптографический шлюз 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 посредством межсетевого экранирования.

КК может быть оснащен специализированной платой — криптоускорителем, который повышает производительность КК при шифровании трафика VPN.

Детектор атак

Детектор атак представляет собой программное средство, предварительно установленное на специализированной аппаратной платформе с архитектурой x64.

Примечание. Далее в эксплуатационной документации под термином детектор атак понимается как программное обеспечение, устанавливаемое на аппаратную платформу, так и аппаратная платформа с установленным программным обеспечением ДА.

Детектор атак обеспечивает анализ сетевого трафика и обнаружение сетевых атак сигнатурным методом.

Детектор атак обеспечивает обнаружение следующих основных угроз безопасности информации:

- преднамеренный несанкционированный доступ или специальные воздействия на информацию (носители информации) со стороны внешних нарушителей, действующих из информационно- телекоммуникационных сетей, в том числе сетей международного информационного обмена;
- преднамеренный несанкционированный доступ или специальные воздействия на информацию (носители информации) со стороны внутренних нарушителей, обладающих правами и полномочиями на доступ к информации в информационной системе.

Сервер доступа

Сервер доступа представляет собой предварительно устанавливаемое на одном из КШ программное средство, обеспечивающее доступ удаленных пользователей к ресурсам сегментов VPN. Сервер доступа может быть установлен на одном КШ вместе с ЦУС.

Сервер доступа обеспечивает:

- защищенное соединение между АП и сетью, защищенной КШ;

- формирование симметричного ключа (ГОСТ 28147-89) для аутентификации администратора и запись ключевой информации на ключевой носитель;
- аутентификацию администратора при установлении защищенного соединения с программой управления;
- взаимодействие с программой управления;
- взаимодействие с сертификатами пользователей "КриптоПро CSP", выпущенными по стандарту ГОСТ Р 34.10-2012;
- смену режимов СД (3.x и 4.x) для взаимодействия с СКЗИ "Континент-АП" версий 3.7.x, 4.0.x и 4.1.x;
- хранение необходимой для работы информации;
- аутентификацию удаленных пользователей посредством технологии сертификатов открытых ключей стандарта x509v3;
- загрузку в фильтр IP-пакетов криптографического шлюза правил фильтрации в соответствии с правами подключившегося пользователя;
- контроль состояния установленных защищенных соединений абонентских пунктов с криптографическим шлюзом и выгрузку сессионной информации при разрыве соединения;
- регистрацию событий, связанных с работой сервера, использованием программы управления и подключением удаленных пользователей.

Центр управления сетью

ЦУС представляет собой предварительно устанавливаемое на одном из КШ программное средство, обеспечивающее централизованное управление работой всех сетевых устройств комплекса.

Примечание. Далее в эксплуатационной документации под термином ЦУС понимается как программное обеспечение, устанавливаемое на одном из КШ, так и КШ с установленным программным обеспечением ЦУС.

Помимо управления сетевыми устройствами ЦУС обеспечивает отслеживание состояния сетевых устройств и VPN-каналов, а также фиксацию и реагирование на инциденты несанкционированного доступа.

Программа управления комплексом

Программа управления комплексом представляет собой программное средство, устанавливаемое на одном или нескольких компьютерах (рабочих местах администратора), которые находятся в той же сети, что и КШ с ЦУС.

Программа управления обеспечивает централизованное управление настройками и оперативный контроль состояния всех компонентов комплекса и соединений удаленных пользователей.

В состав ПУ комплексом входит ПУ ЦУС, предназначенная для управления и мониторинга сетевых устройств.

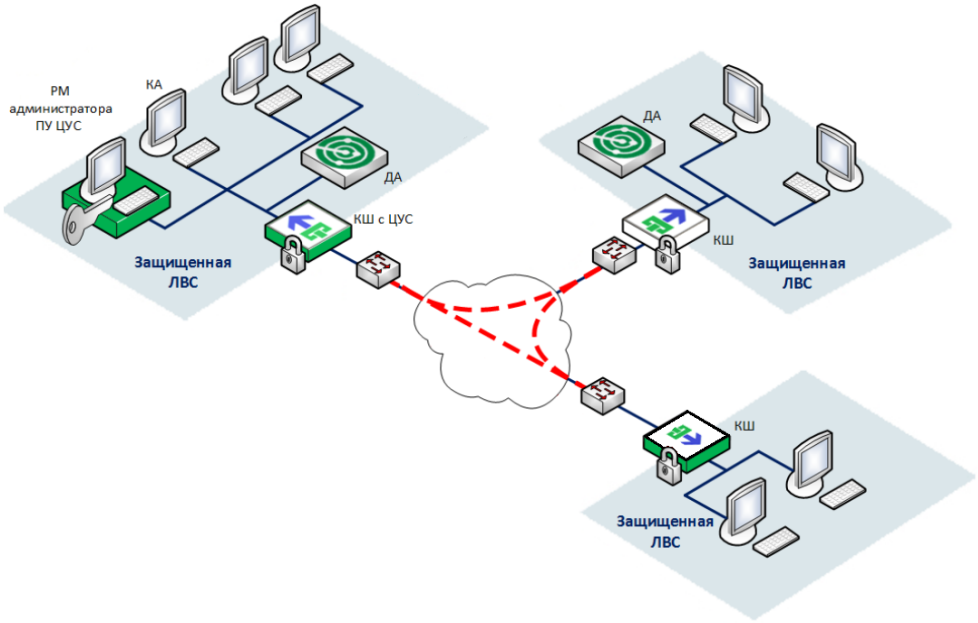
Клиент аутентификации пользователя

КА пользователя представляет собой программное средство, устанавливаемое на компьютерах, находящихся в защищенном сегменте сети, и обеспечивающее идентификацию и аутентификацию пользователей, зарегистрированных в ПУ комплексом.

Глава 3
Принципы функционирования комплекса

Обобщенная функциональная схема защищенной корпоративной сети

На рисунке ниже (см. стр. **10**) представлена обобщенная структура защищенной корпоративной сети, состоящей из нескольких локальных вычислительных сетей.



Связь между ЛВС осуществляется по каналам связи общих сетей передачи данных. К общим сетям каждая ЛВС подключена через криптографический шлюз. Подключение ЛВС через криптографический шлюз обеспечивает скрытие внутренней структуры защищаемого сегмента сети. При этом IP-адреса устройств в защищаемых сегментах должны быть уникальными только в рамках данной корпоративной сети.

КШ может содержать несколько сетевых интерфейсов, к которым можно подключить независимые локальные сети. Физические интерфейсы одного КШ могут быть объединены в один логический для повышения надежности и увеличения пропускной способности канала (агрегация интерфейсов).

При подключении компьютеров к криптографическому шлюзу может осуществляться их аутентификация посредством КА.

В комплексе предусмотрена поддержка виртуальных локальных сетей, организованных в защищенных сегментах сети.

Криптографический шлюз осуществляет маршрутизацию проходящего через него трафика IP-пакетов, поэтому дополнительный маршрутизатор в общем случае не требуется.

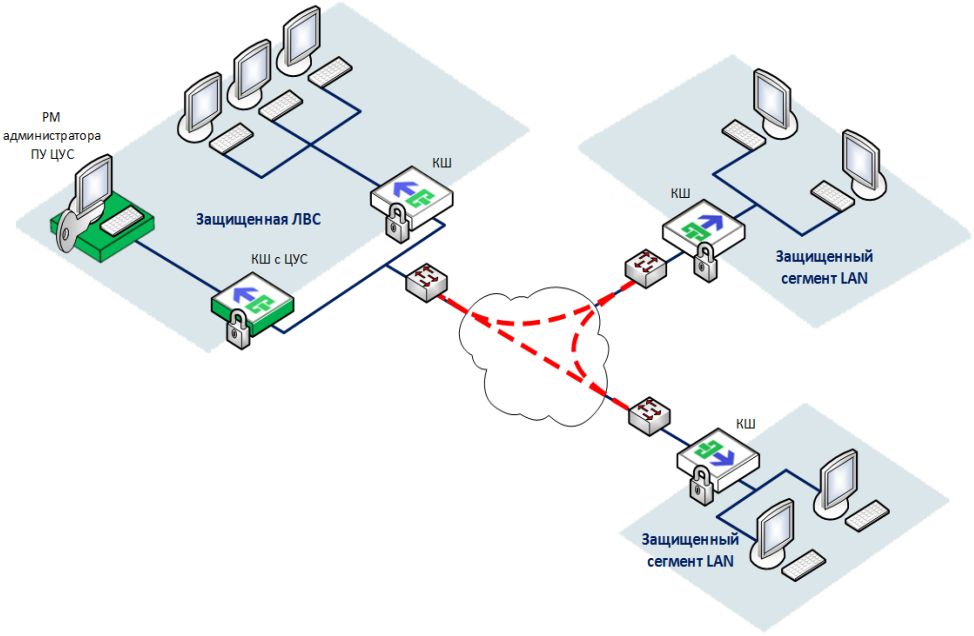
Если необходимо использовать дополнительный маршрутизатор, он может быть размещен как перед КШ (в защищаемом сегменте сети), так и после (вне защищаемого сегмента сети). Если маршрутизатор находится в защищаемом сегменте сети, никаких дополнительных действий по защите маршрутизатора не требуется.

Если маршрутизатор находится вне защищаемого сегмента сети, то предусмотрена возможность защищенного управления маршрутизатором (см. стр. **13**).

Кроме маршрутизации трафика, криптографический шлюз осуществляет обработку входящих и исходящих IP-пакетов — фильтрацию и криптографическое преобразование данных, передаваемых по общим каналам связи. Для организации доступа пользователей корпоративной сети к узлам общей сети используется механизм трансляции сетевых адресов NAT.

Для поддержки функционала СОВ в защищенных сегментах сети используются ДА, подключаемые к SPAN-портам КШ. Выявление компьютерных атак осуществляется на основе анализа полученного таким образом сетевого трафика. Сетевой интерфейс, захватывающий сетевой трафик для анализа, имеет тип "мониторинг".

Представленный выше вариант использования комплекса применим только для небольших сетей (2–5 КШ). При использовании в комплексе более пяти КШ рекомендуется вынести ЦУС и РМ управления сетью КШ в отдельный защищаемый сегмент (см. рисунок ниже). В этом случае ЦУС используется только для управления сетью КШ.



Автоматическое управление сетевыми устройствами осуществляет ЦУС, размещающийся на одном из криптографических шлюзов. Этот КШ можно использовать как любой другой рядовой шлюз в корпоративной сети для приема и передачи IP- пакетов, их фильтрации, маршрутизации и криптографического преобразования.

Основное управление сетевыми устройствами осуществляется через ЦУС с помощью программы управления. Программа управления устанавливается на выделенном компьютере, входящем в состав защищаемого сегмента корпоративной сети (РМ администратора).

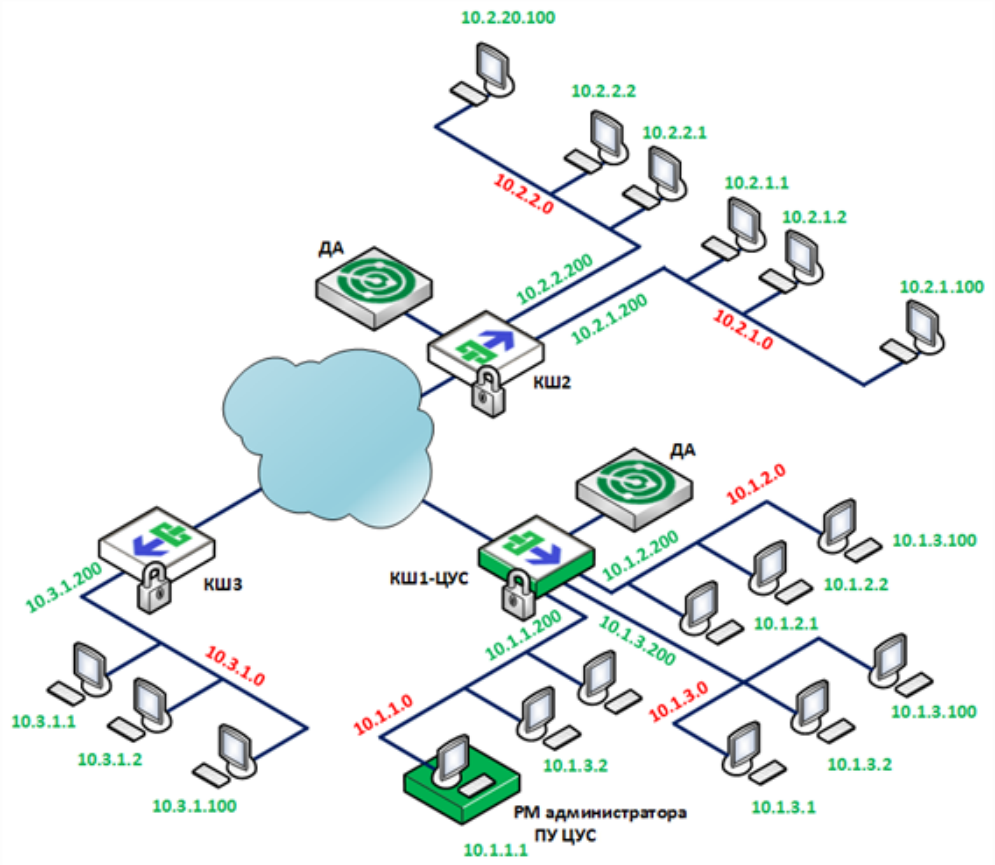
Администратор может управлять сетевыми устройствами локально, путем подключения монитора и клавиатуры непосредственно к устройству. Также имеется возможность удаленного выключения и перезагрузки сетевого устройства по протоколу SSH.

Клиент аутентификации используется при необходимости для идентификации и аутентификации пользователей, зарегистрированных в комплексе.

Если на пути зашифрованного трафика находятся межсетевые экраны или другое оборудование, осуществляющее фильтрацию IP-пакетов, необходимо создать для них правила, разрешающие прохождение служебных пакетов комплекса.

Пример организации защищенной корпоративной сети

Ниже на рисунке представлен пример организации защищенной корпоративной сети, объединяющей локальные сети центрального офиса и двух филиалов. Криптографический шлюз центрального офиса КШ 1 (с ЦУС) защищает три локальные сети, криптографические шлюзы филиалов КШ 2 и КШ 3 — две и одну соответственно.



Взаимодействие с сетевыми устройствами, поддерживающими NAT

АПКШ "Континент"обеспечивает совместную работу криптографических шлюзов с сетевыми устройствами, поддерживающими трансляцию сетевых адресов NAT. При этом имеется ограничение — на пути трафика между двумя КШ не должно быть более одного сетевого устройства с поддержкой динамической трансляции адресов. КШ с ЦУС всегда должен быть доступен для всех сетевых устройств комплекса.

Подключение КШ к нескольким внешним сетям

Криптографический шлюз может быть одновременно подключен к нескольким внешним сетям (например, принадлежащим разным провайдерам) путем использования технологии Multi-WAN. В АПКШ "Континент" поддерживаются следующие режимы Multi-WAN:

- передача трафика в соответствии с таблицей маршрутизации;
- обеспечение отказоустойчивости канала связи;
- балансировка трафика между внешними интерфейсами КШ.

Криптографический шлюз может функционировать только в одном из перечисленных режимов.

Режим "Передача трафика в соответствии с таблицей маршрутизации" предоставляет администратору возможность контролировать внешние каналы связи при использовании статической маршрутизации.

В режиме "Обеспечение отказоустойчивости канала связи" КШ при выходе из строя основного канала связи автоматически переключается на резервный. Статус канала (основной или резервный) определяется назначенным ему приоритетом. Обратное переключение осуществляется после восстановления работоспособности основного канала в соответствии с выбранным алгоритмом:

- немедленно;

- через указанное время;
- после завершения всех активных соединений.

В режиме "Балансировка трафика между внешними интерфейсами КШ" исходящий трафик автоматически распределяется в соответствии с указанными правилами. Одному классу трафика соответствует одно правило.

В системном журнале регистрируются следующие события:

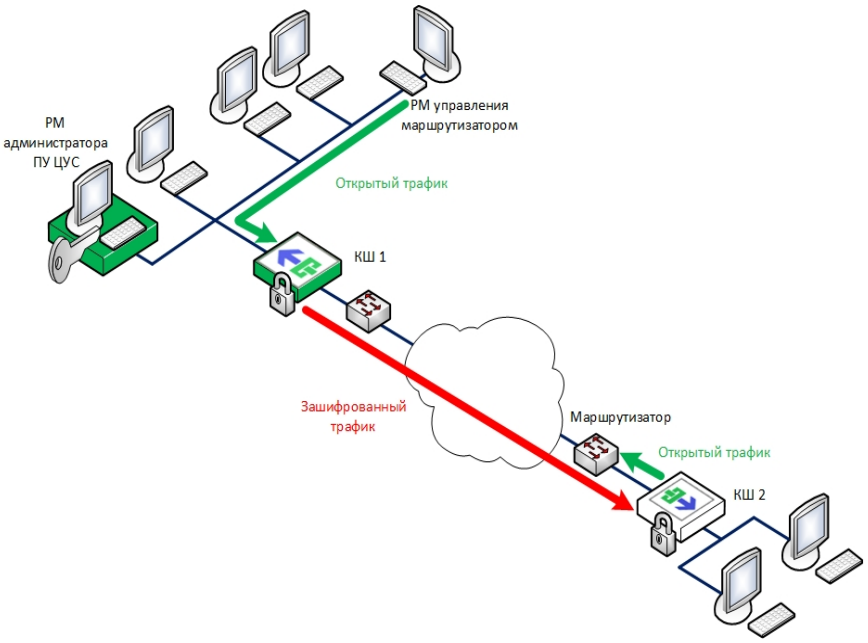
- переключение каналов;
- изменение состояния неактивного канала.

Примечание. В режиме Multi-WAN в качестве каналов связи между криптошлюзами могут использоваться выделенные каналы, исключающие пересечение между собой и с сетями общего пользования (интернет и др.).

Защищенное управление маршрутизатором

Защищенное управление маршрутизатором, размещенным после криптографического шлюза (вне защищаемого сегмента сети), организуется следующим образом (см. рисунок ниже):

- на криптографическом шлюзе КШ 2 определяют защищенную сеть из одного маршрутизатора;
- на криптографических шлюзах КШ 1 и КШ 2 создают правила фильтрации, разрешающие прохождение управляющего трафика;
- на маршрутизаторе добавляют правило маршрутизации для отсылки IP-пакетов к консоли управления через криптографический шлюз КШ 2.

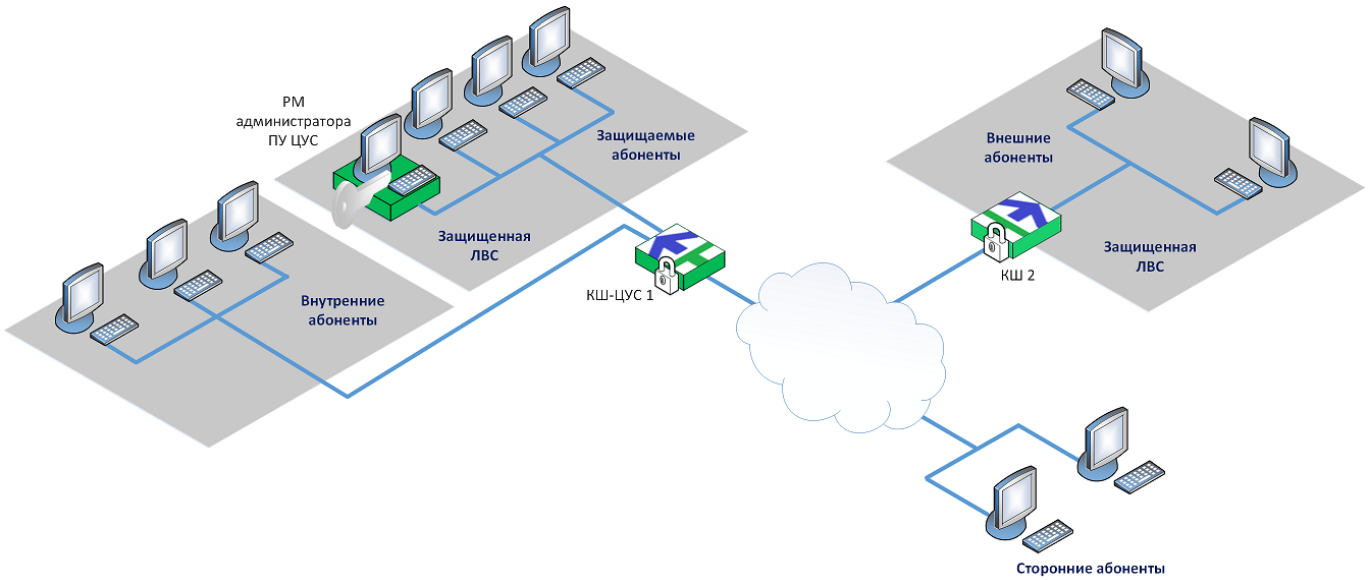


Таким образом, исходный управляющий трафик от консоли управления зашифровывается криптографическим шлюзом КШ 1 и по общей сети передается в зашифрованном виде на КШ 2. Криптографический шлюз КШ 2 расшифровывает трафик и передает его в открытом виде на маршрутизатор. IP-пакеты отсылаются маршрутизатором к консоли управления тем же путем в обратном порядке.

Защищенное управление маршрутизатором возможно только при прямом подключении КШ 2 к общим сетям. Защищенное управление маршрутизатором при подключении КШ 2 через модем не поддерживается.

Обработка IP-пакетов

Обработка IP-пакетов осуществляется криптографическими шлюзами. Режим обработки зависит от статуса абонента сети по отношению к данному криптографическому шлюзу (см. рисунок ниже).



Абонент — любой компьютер, отправляющий и получающий IP- пакеты. Абоненты IP- сети классифицируются следующим образом (на рисунке — по отношению к КШ 1):

- внутренний абонент — входит в состав сегмента сети, защищаемого данным КШ с помощью межсетевого экрана;
- защищаемый абонент — входит в состав сегмента сети, защищаемого данным КШ с помощью межсетевого экрана и VPN;
- внешний абонент — относится к сегменту сети, защищаемому любым другим (отличным от данного) КШ комплекса;
- сторонний абонент — любой абонент IP-сети, не входящий в состав защищаемых сегментов.

Фильтрация IP-пакетов

Все IP-пакеты, проходящие через криптографический шлюз, подвергаются фильтрации. Каждый КШ имеет два фильтра. Фильтрация выполняется дважды, до и после обработки IP- пакетов блоком криптографической защиты.

Фильтрация IP-пакетов осуществляется в соответствии с правилами, сформированными на основе IP-адресов отправителя и получателя, названия протокола, ToS-меток, номеров портов UDP/TCP и имен сетевых интерфейсов. Проверяются также время, факт аутентификации (для защищаемого сегмента), а при фильтрации прикладных протоколов — содержимое пакетов.

Примечание. По умолчанию прохождение любого IP-пакета запрещено, если это не разрешено явно соответствующим правилом фильтрации.

Правила фильтрации IP-пакетов подразделяются на два типа:

- правила, сформированные комплексом автоматически;
- правила, заданные администратором.

Автоматическое формирование правил фильтрации для данного КШ осуществляется при инициализации ЦУС и КШ. Правила этого типа не отображаются на экране и не могут быть удалены или изменены администратором.

Правила, сформированные комплексом автоматически, разрешают соединения между следующими элементами комплекса:

- ЦУС, ПУ ЦУС и агентом ЦУС и СД;
- ЦУС и зарегистрированными сетевыми устройствами;
- основным и резервным КШ.

Для остальных соединений в рамках корпоративной сети правила фильтрации формирует администратор.

Кроме того, администратор может создавать правила фильтрации для разрешения незашифрованных соединений со сторонними абонентами (веб-сайтами, FTP-серверами).

Внимание! При разрешении незашифрованных соединений общий уровень защищенности корпоративной сети снижается, поэтому для обеспечения максимального уровня защиты информации рекомендуется отказаться от разрешения таких соединений.

В КШ предусмотрена функция автоматической оптимизации правил фильтрации. Оптимизация позволяет уменьшить количество правил фильтрации, загружаемых на сетевое устройство.

Оптимизации подлежат однотипные правила, различающиеся только отправителями и получателями. Отправители и получатели, указанные в таких правилах, автоматически объединяются в группы. Для таких групп создается единое правило.

Группы, созданные для оптимизации, отображаются в технологических отчетах под именем ipset<-порядковый номер группы>.

Созданные при оптимизации правила фильтрации отображаются в консоли локального компьютера в списке загруженных. В общем списке правил фильтрации в программе управления такие правила не отображаются.

Примечание. При общем количестве групп более 1000 оптимизацию включать не рекомендуется. Также не рекомендуется включать оптимизацию при наличии групп с количеством элементов более 200000. При превышении указанных значений (групп или элементов в группе) оптимизация автоматически отключается.

Существуют два режима работы фильтра: основной и мягкий. При основном режиме работы фильтра IP-пакеты, прохождение которых запрещено, отбрасываются с регистрацией этого события в журнале НСД. При мягком режиме такие пакеты только регистрируются в журнале НСД, но пропускаются фильтром. Мягкий режим предназначен для настройки криптографического шлюза при вводе его в эксплуатацию.

Если пакет не удовлетворяет установленным правилам фильтрации, он отвергается без уведомления отправителя.

Запрет доступа к ресурсам единого реестра Роскомнадзора

Запрет на доступ к ресурсам, включенным Роскомнадзором в единый реестр, может быть реализован с помощью правил фильтрации. Администратор может создавать дополнительные правила фильтрации.

Сведения, содержащиеся в едином реестре Роскомнадзора, позволяют идентифицировать сайты, содержащие запрещенную к распространению в Российской Федерации информацию.

Информацию о запрещенных ресурсах получают на сайте Роскомнадзора в виде выгрузки из единого реестра, включающей в себя IP-адреса запрещенных сайтов, и затем средствами программы управления ЦУС помещают в БД ЦУС. При этом предусмотрено автоматическое получение выгрузки и запись ее в БД ЦУС с помощью специального агента, входящего в состав подсистемы управления комплексом.

В программе управления ЦУС IP-адреса запрещенных сайтов, хранящиеся в БД ЦУС, отображаются как группа сетевых объектов с именем "Реестр запрещенных ресурсов".

Для установления запрета на доступ к запрещенным ресурсам администратор должен создать правило фильтрации и в качестве адреса получателя (или отправителя) указать группу сетевых объектов "Реестр запрещенных ресурсов". На КШ, для которого было создано данное правило, фильтрация пакетов будет осуществляться только по IP-адресам указанной группы, т. е. по IP-адресам запрещенных сайтов.

Автоматическое обновление списка запрещенных ресурсов поддерживается при наличии агента, обеспечивающего получение выгрузки с сайта Роскомнадзора и ее запись в БД ЦУС.

Блок криптографической защиты

После успешного прохождения фильтров межсетевого экрана IP- пакеты поступают в блок криптографической защиты. Блок криптографической защиты предназначен для обработки поступающих в него IP-пакетов — сжатия, зашифрования/расшифрования и имитозащиты.

IP-пакеты попадают на обработку в блок криптографической защиты, если они удовлетворяют следующим условиям:

- пакет получен от парного КШ и является VPN-пакетом (пакет подлежит расшифрованию в блоке криптографической защиты);
- пакет должен быть отправлен в защищаемую сеть парного КШ (источник пакета не анализируется, а сам пакет подлежит зашифрованию, если не изменена настройка по умолчанию локального меню для "белых" адресов (см. [**5**], "Настройка параметров шифратора").

Для сжатия IP-пакетов используется алгоритм сжатия deflate. Предусмотрена возможность выбора степени сжатия, а также отключения этого режима.

Применение сжатия позволяет увеличить скорость передачи IP-пакетов по низкоскоростным каналам связи. Так, при пропускной способности линии 64 Кбит/с скорость передачи IP-пакетов после сжатия возрастает в 1,5 раза. Кроме того, сжатие IP-пакетов обеспечивает дополнительную защиту при попытке их несанкционированного перехвата во время передачи по общим каналам связи.

Сжатые IP-пакеты зашифровываются и инкапсулируются в новый IP-пакет, в котором:

- в качестве IP-адреса источника выступает внешний IP-адрес КШ-отправителя;
- в качестве IP-адреса приемника выступает внешний IP-адрес КШ-получателя.

Список адресов, для которых осуществляется шифрование пакетов, определяется списком связанных КШ и их защищаемых сетей.

Трансляция сетевых адресов

Трансляция сетевых адресов служит для преобразования IP-адреса транзитных пакетов. Характеристики IP-пакетов, для которых используется трансляция адресов, определяют с помощью правил трансляции.

Описание правил трансляции адресов представлено в Табл.1, задачи, решаемые с помощью данного механизма, — в Табл.2.

Табл.1 Правила трансляции адресов

Правило	Описание
Исходящие	Инициатор соединения — абонент защищенной 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
Входящие	Инициатор соединения — сторонний абонент, 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
1:1	Инициатор соединения — любая сторона. В исходящих IP-пакетах внутрисетевой IP-адрес отправителя заменяется на указанный публичный. Во входящих IP-пакетах публичный IP-адрес получателя заменяется на указанный внутрисетевой

Табл.2 Задачи, решаемые с помощью трансляции адресов

Задача	Правило
Скрытие структуры внутренней сети за одним публичным адресом	Исходящие
Предоставление пользователям с неуникальными внутрисетевыми адресами доступа к внешним сетям общего пользования	Исходящие
Обеспечение доступа извне к внутрисетевым сервисам:	
• по определенным портам	Входящие
• с переопределением портов	Входящие
• по всем портам (обычно используют для предоставления доступа к серверам, находящимся в демилитаризованной зоне)	1:1

Трансляция сетевых адресов выполняется перед применением правил фильтрации. При обработке IP-пакетов блоком криптографической защиты трансляция сетевых адресов не применяется.

Защита от DoS-атак

Для правила фильтрации, разрешающего TCP-соединение, можно включить режим защиты от DoS-атак типа SYN-флуд.

При обращении клиента к серверу доступа криптографический шлюз сначала устанавливает TCP-соединение с клиентом от имени сервера, а затем с сервером от имени клиента. После этого клиент с сервером

могут обмениваться сетевыми пакетами. Полуоткрытые соединения с просроченным временем ожидания автоматически удаляются из очереди.

Для настройки режима используют следующие параметры:

- максимальное количество соединений, которое может быть установлено по указанному правилу фильтрации;
- время, по истечении которого неактивное соединение будет автоматически разорвано;
- количество новых соединений, регистрируемых для данного правила, в секунду.

Обнаружение вторжений (атак)

В комплексе поддерживает проверку всего трафика, проходящего через КШ, на наличие попыток неавторизованного доступа (сетевых атак). Для этого к одному из сетевых интерфейсов КШ подключают сетевое устройство "Детектор атак" с установленной на нем системой обнаружения вторжений (атак), и этот интерфейс определяется как SPAN-порт (Switched Port Analyzer). Через этот порт СОВ получает копии всех IP-пакетов, проходящих через КШ, и анализирует их на наличие неавторизованных или подозрительных действий. Копии IP-пакетов, отправляемых или поступивших по защищенному каналу, передаются на SPAN-порт соответственно до их зашифровывания или после расшифровывания.

Детектор атак контролирует следующие данные о сетевом трафике:

- сетевой адрес;
- используемый порт;
- значения полей сетевого пакета;
- идентификаторы протоколов;
- размер полей пакета;
- интенсивность трафика.

Анализ данных с целью обнаружения вторжений осуществляется с использованием сигнатурного и эвристического методов.

Метод сигнатурного анализа основан на применении набора решающих правил, предварительно загруженных в базу данных ЦУС и постоянно обновляемых с заданной периодичностью. При этом обновление решающих правил может выполняться как автоматически по настраиваемому расписанию, так и вручную.

Автоматическое обновление решающих правил осуществляется специальным агентом – агентом обновлений, в функции которого входят проверка наличия новых обновлений, получение обновлений от поставщика и загрузка их в соответствии с расписанием в базу данных ЦУС.

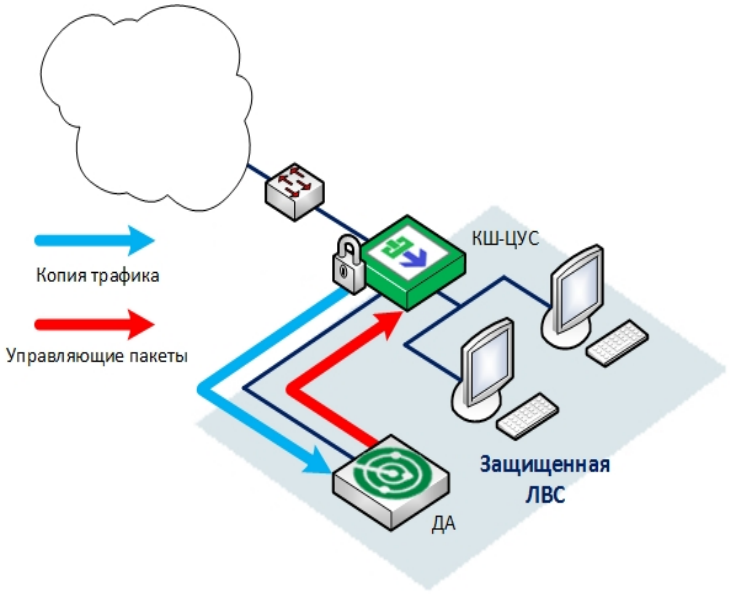
Эвристический анализ выявления аномалий сетевого трафика можно применять в дополнение к сигнатурному анализу. При этом используются настройки эвристического анализатора, заданные по умолчанию.

События, связанные с работой ДА и обнаружением вторжений, регистрируются в его локальных журналах и передаются в базу данных средствами агента ЦУС. Просмотр событий осуществляется в программе просмотра журналов.

В случае обнаружения вторжения или нарушения безопасности, администратору отсылается сообщение по электронной почте, а в программе управления ЦУС появляется визуальное отображение зафиксированного НСД.

В ДА предусмотрены следующие варианты автоматического реагирования на атаки:

- запись детальной информации о факте атаки в журнал центральной базы данных;
- оперативное уведомление администратора о факте вторжения по электронной почте и в ПУ ЦУС.



Передача управляющих пакетов СОВ в контролируемую сеть (сетевой сегмент) осуществляется в обратном порядке через SPAN-порт или через дополнительный сетевой интерфейс системы обнаружения вторжений (атак), настроенный специальным образом.

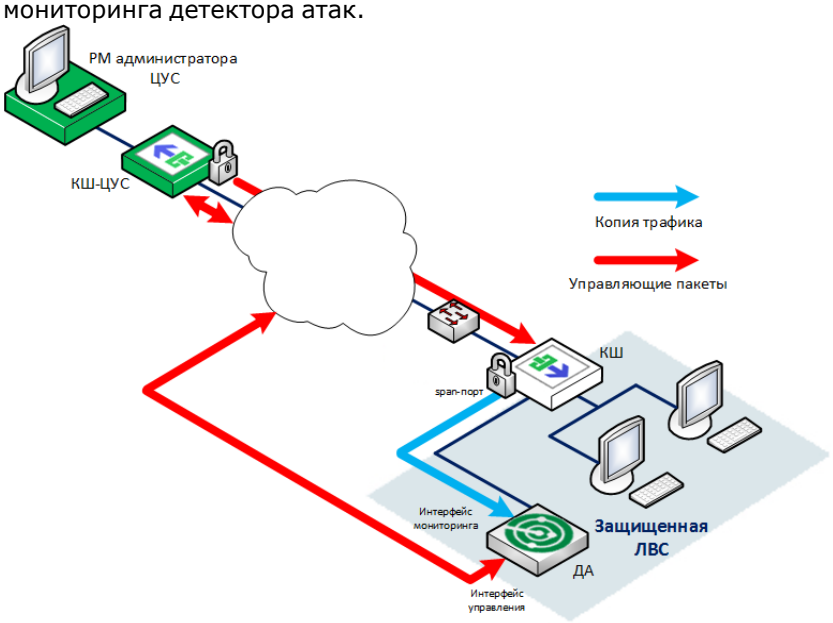
Необходимо учитывать, что интерфейс, определенный как SPAN-порт, должен использоваться только для целей анализа сетевого трафика.

Внимание! Запрещается подключать интерфейс, определенный как SPAN-порт, к любым сетям – это может привести к лавинообразному росту трафика и вывести сети из строя.

Примеры типовых вариантов использования ДА

Подключение детектора атак с одним интерфейсом мониторинга

На рисунке, представленном ниже, защищаемая корпоративная сеть предприятия находится за криптошлюзом АПКШ "Континент". Трафик между защищаемой сетью и сетями общего доступа (например, интернет) зеркалируется на span- порт криптошлюза. Span- порт криптошлюза подключен к интерфейсу мониторинга детектора атак.

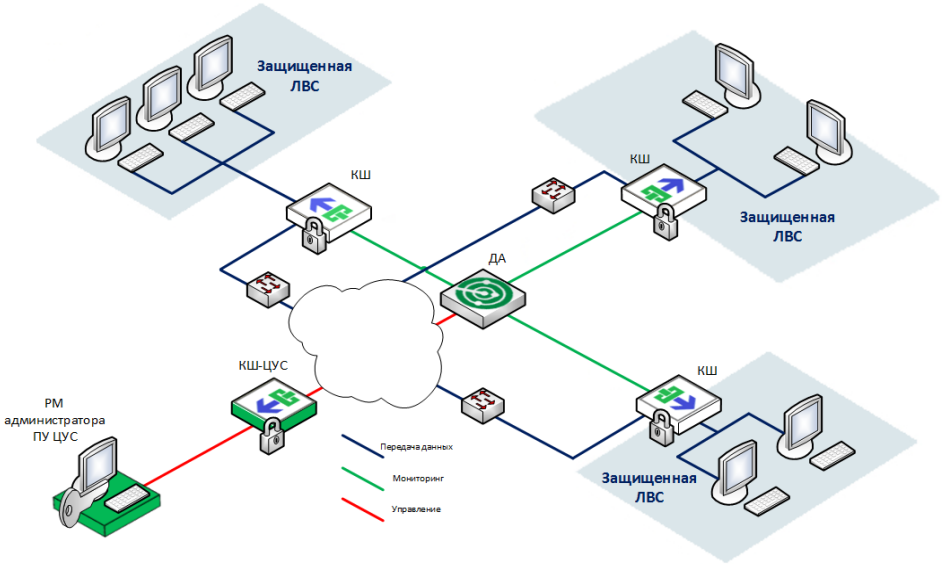


Команды управления от ЦУС поступают на интерфейс управления детектора атак по защищенному каналу.

Подключение детектора атак с несколькими интерфейсами мониторинга

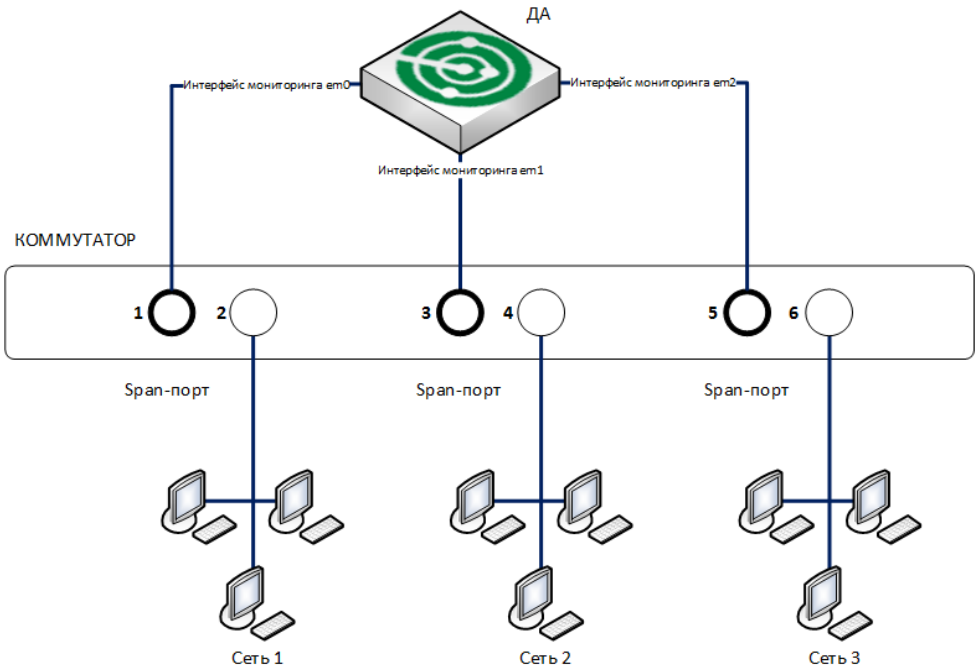
В зависимости от используемой аппаратной платформы в ДА может быть настроено от одного до трех интерфейсов мониторинга. Это дает возможность одновременно контролировать и анализировать трафики, приходящие на каждый из таких интерфейсов.

На рисунке ниже показано подключение к детектору атак трех КШ АПКШ "Континент", каждый из которых зеркалирует трафик на свой span-порт.



Подключение детектора атак к коммутационному оборудованию сторонних производителей

Детектор атак может быть подключен к коммутационному оборудованию (маршрутизатору, коммутатору и пр.), имеющему в своем составе span-порт. На рисунке ниже показано подключение детектора атак к коммутатору с тремя span-портами (порты 1, 3, 5), на которые зеркалируются трафики с портов 2, 4, 6.



Обеспечение доступа удаленных пользователей

Для организации доступа удаленных пользователей к ресурсам защищаемой сети в комплексе используется следующее программное обеспечение:

- сервер доступа;
- программа управления сервером доступа;
- абонентский пункт.

Сервер доступа

Сервер доступа представляет собой предварительно устанавливаемое на одном из КШ программное средство, обеспечивающее доступ удаленных пользователей к ресурсам сегментов VPN (см. стр. 7).

Программа управления сервером доступа

Программа управления сервером доступа предназначена для управления объектами базы данных сервера и оперативного контроля его состояния. Программа устанавливается на одном или нескольких компьютерах защищаемого сегмента сети — РМ администратора.

В состав программы управления входят криптопровайдер "Код Безопасности CSP" и программа управления сгенерированными им ключами.

Программа управления обеспечивает:

- установление защищенного соединения и обмен данными с сервером доступа;
- мониторинг состояния сервера доступа и оперативное управление сервером;
- получение от сервера доступа и отображение информации о состоянии базы данных сервера;
- добавление, удаление и модификацию объектов базы данных сервера доступа;
- резервное копирование и восстановление базы данных сервера доступа;
- управление сертификатами открытых ключей;
- получение от сервера доступа журнала событий, его отображение и управление записями журнала.

Абонентский пункт

Абонентский пункт представляет собой специализированное программное обеспечение, устанавливаемое на рабочих местах удаленных пользователей для организации их доступа к ресурсам защищаемой сети.

В состав абонентского пункта входят следующие компоненты:

- криптопровайдер "Код Безопасности CSP";

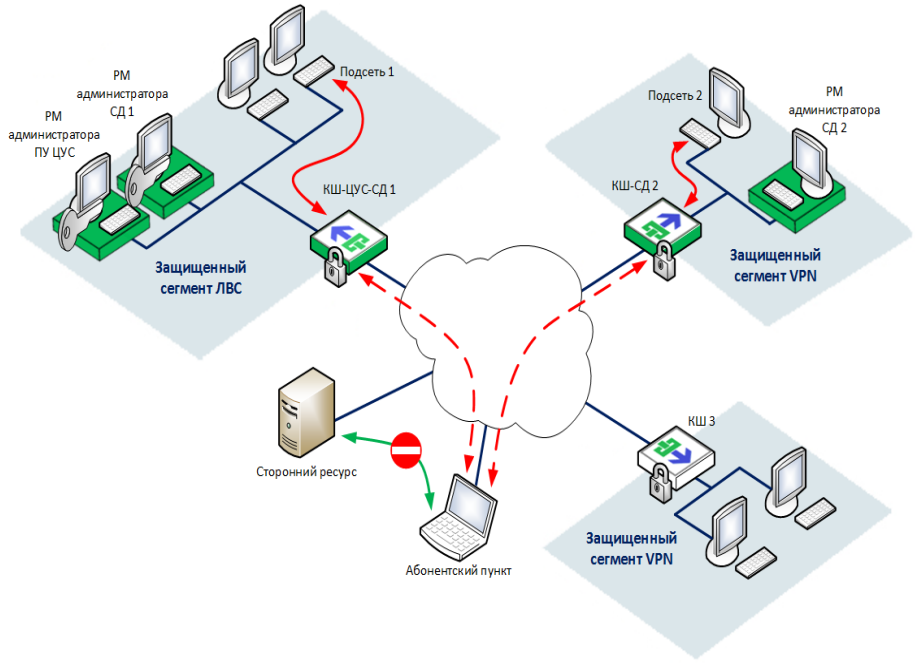
- программа управления сгенерированными ключами;
- программа управления абонентским пунктом и межсетевым экраном.

Абонентский пункт обеспечивает:

- установление защищенного соединения и обмен данными с сервером доступа;
- обоюдную аутентификацию с сервером доступа в процессе установления защищенного соединения посредством технологии сертификатов открытых ключей стандарта x509v3;
- защищенное соединение с сервером доступа по протоколу UDP и TCP;
- доступ к ресурсам VPN при установлении соединения с СД;
- необходимый функционал для работы с сертификатами открытых ключей;
- протоколирование подключений к серверу доступа в журнале соединений;
- отображение записей журнала соединений и управление ими;
- фильтрацию всего входящего и исходящего IP-трафика средствами встроенного МСЭ.

Абонентский пункт поставляется на оптическом носителе.

Доступ удаленных пользователей к ресурсам защищенной сети



Для организации доступа удаленного пользователя к корпоративным ресурсам криптографический шлюз комплектуется сервером доступа, а на компьютере удаленного пользователя устанавливается абонентский пункт. Один сервер доступа обслуживает защищенные сети только того КШ, на котором он установлен.

Удаленный пользователь, зарегистрированный на нескольких серверах доступа, может подключаться к любому из этих серверов с одного и того же абонентского пункта. Связь удаленного пользователя с внутренними абонентами защищенной сети осуществляется по каналам связи общих сетей передачи данных. Одновременное подключение с одного абонентского пункта к нескольким серверам доступа невозможно.

Инициатором соединения абонентского пункта с сервером доступа может быть только удаленный пользователь. Разорвать соединение может как пользователь, так и администратор сервера доступа. В некоторых случаях разрыв соединения может автоматически выполняться самим сервером доступа.

Защищенное (с зашифрованным трафиком) соединение между абонентским пунктом и сервером доступа устанавливается только после их успешной взаимной аутентификации, которая осуществляется на основе сертификатов открытых ключей стандарта x509v3.

Для повышения устойчивости к сетевым атакам вида "отказ в обслуживании" (DoS-атакам) администратор может вводить ограничения на количество одновременно подключенных к серверу доступа абонентских пунктов, а также редактировать параметры таких соединений.

После установления соединения сервер доступа осуществляет загрузку правил фильтрации IP-пакетов из индивидуального списка правил данного пользователя в фильтр IP-пакетов криптографического шлюза. Кроме того, список доступных пользователю защищаемых подсетей передается на абонентский пункт.

Далее обмен данными между абонентским пунктом и абонентами защищенной сети осуществляется через сервер доступа. При этом весь трафик, передаваемый между абонентским пунктом и защищенной сетью, шифруется с использованием алгоритма ГОСТ 28147–89.

Для упрощения настройки маршрутизации трафика между абонентским пунктом и абонентами защищенной сети абонентскому пункту назначается внутрисетевой IP-адрес. Трафик от абонента защищенной сети поступает на этот внутрисетевой IP-адрес абонентского пункта, а сервер доступа перенаправляет трафик непосредственно на абонентский пункт. При назначении абонентским пунктам внутрисетевых адресов может использоваться как динамическая, так и статическая адресация.

Резервирование IP-адресов из выделенного диапазона X.X.X.1 — X.X.X.N:

- X.X.X.1 — IP-адрес сервера доступа;
- X.X.X.2 — IP-адрес только для статической адресации;
- X.X.X.N — широковещательный IP-адрес (broadcast).

Остальные IP-адреса диапазона можно использовать как для статической, так и динамической адресации.

Назначение абонентскому пункту статического адреса предоставляет возможность устанавливать связь абонентских пунктов между собой. Для установления такой связи необходимо дополнительно создать правила фильтрации.

Предусмотрен режим работы абонентского пункта, который запрещает все незащищенные соединения со сторонними абонентами (например, с веб-узлами или FTP-серверами) во время связи с абонентами защищенной сети.

Внимание! Если на пути трафика, передаваемого между абонентским пунктом и сервером доступа или между программой управления и сервером доступа, находятся межсетевые экраны или другое оборудование, осуществляющее фильтрацию IP-пакетов, необходимо создать на этих устройствах правила фильтрации, разрешающие прохождение служебных пакетов комплекса.

Аутентификация удаленного пользователя

Аутентификация удаленного пользователя при установлении соединения между абонентским пунктом и сервером доступа осуществляется на основе сертификатов открытых ключей стандарта X.509v3.

Сертификат содержит имя владельца сертификата и его открытый ключ, а также дополнительную системную информацию. Достоверность этой информации подтверждается подписью доверенного центра сертификации.

Используются следующие сертификаты:

- корневой сертификат;
- сертификат сервера доступа;
- сертификат пользователя.

Возможны два варианта организации работы с сертификатами:

- Доверенным центром является внешний центр сертификации. Центр сертификации предоставляет корневой сертификат, сертификат сервера доступа, а также все сертификаты пользователей. Сертификат сервера доступа издается по запросу, сформированному администратором средствами программы управления. Сертификаты пользователей издаются по запросам, сформированным средствами абонентского пункта. Администратор не имеет доступа к закрытому ключу центра сертификации и закрытым ключам пользователей. Полученные сертификаты регистрируются на сервере доступа и передаются пользователям.
- Доверенным центром сертификации является программа управления сервером доступа. Администратор средствами программы управления и криптопровайдера, совместно с которым работает программа, издает корневой сертификат, сертификат сервера доступа, а также все сертификаты пользователей. Сертификат сервера доступа и сертификаты пользователей подписываются закрытым ключом центра сертификации — программы управления сервером доступа.

Имеется возможность издания сертификатов пользователей по запросам, сформированным средствами абонентского пункта. В этом случае администратор не имеет доступа к закрытым ключам пользователей.

Программа управления сервером доступа и абонентские пункты имеют свой встроенный криптопровайдер и поддерживают работу с криптопровайдером "КриптоПро CSP".

При использовании сертификатов внешнего центра сертификации наличие криптопровайдера "КриптоПро CSP" необходимо на компьютере с программой управления сервером доступа и на компьютерах с установленным абонентским пунктом.

При использовании корневого сертификата, созданного средствами программы управления сервером доступа с помощью криптопровайдера "КриптоПро CSP", этот криптопровайдер должен быть установлен и на компьютерах с абонентским пунктом.

Предусмотрена возможность одновременного использования в системе нескольких корневых сертификатов и нескольких сертификатов сервера доступа. Каждому пользователю также может быть выдано несколько сертификатов. При этом разные сертификаты пользователя могут быть заверены закрытыми ключами разных удостоверяющих центров, а могут — закрытым ключом одного и того же удостоверяющего центра. При плановой смене сертификатов такая возможность позволяет зарегистрировать новые сертификаты до истечения сроков действия заменяемых. Рекомендуется также регистрировать в системе резервные сертификаты на случай внеплановой смены действующих сертификатов, например, при компрометации закрытого ключа удостоверяющего центра.

При смене сертификатов работа пользователей, уже подключенных к серверу доступа, продолжается вплоть до завершения текущего сеанса работы. Если обновление сертификатов вызвано потерей доверия к существующим сертификатам, то, выполнив процедуру обновления, необходимо принудительно отключить всех пользователей от сервера доступа.

Защита от DoS-атак

Для повышения устойчивости СД к сетевым атакам вида "отказ в обслуживании" (DoS-атакам) администратор может вводить ограничения на следующие параметры:

- количество абонентских пунктов, стоящих в очереди на подключение;
- число одновременно подключенных к серверу доступа абонентских пунктов;
- длина цепочки связанных сертификатов в сертификате пользователя;
- время, по истечении которого следует разорвать связь сервера доступа с неактивным абонентским пунктом.

Управление сервером доступа

Администратор управляет сервером доступа с помощью программы управления, которая устанавливается на одном или нескольких компьютерах защищенного сегмента сети — РМ администратора.

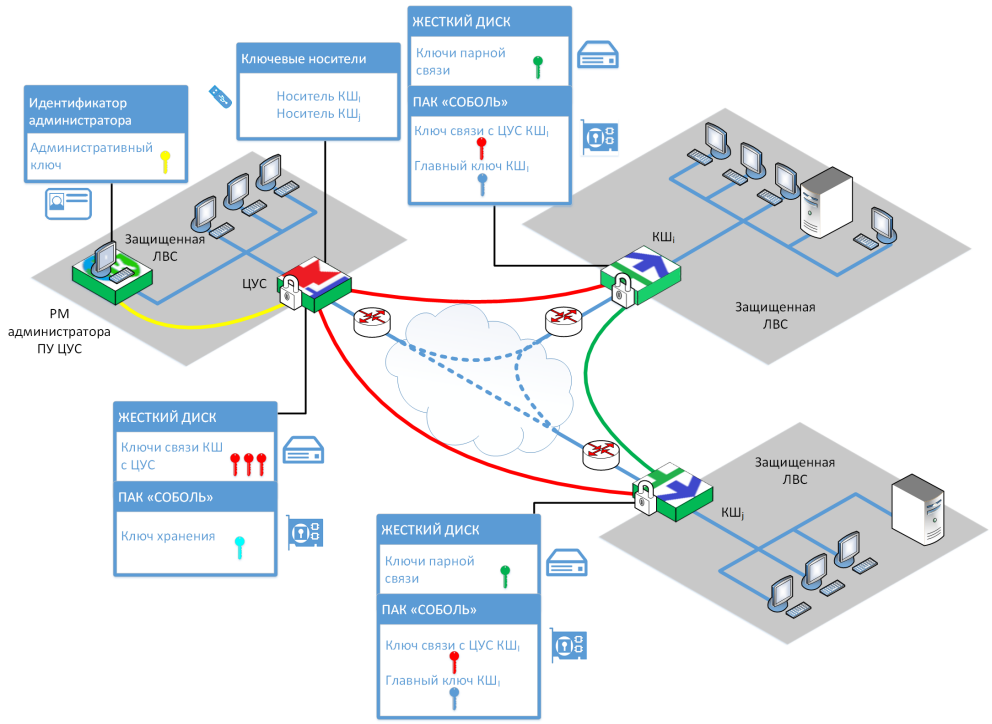
Примечание. При одновременном управлении СД с нескольких РМ возможны сбои в работе программы управления, поэтому рекомендуется их поочередное использование.

Соединение программы управления с сервером доступа устанавливается только после предъявления администратором персонального идентификатора. Этот идентификатор создается средствами локального управления сервером доступа и содержит уникальную ключевую информацию. Соединение программы управления с сервером доступа осуществляется по защищенному каналу.

Администратор осуществляет оперативный контроль состояния сервера доступа и управляет базой данных сервера.

Управление криптографическими ключами

Схема обмена информацией по защищенным каналам связи в корпоративной сети, обслуживаемой комплексом, представлена ниже.



При работе комплекса используется симметричная криптографическая система. Криптографическое соединение между двумя КШ в сети осуществляется на ключах парной связи. Шифрование каждого IP-пакета производится на индивидуальном ключе — ключе шифрования пакета, который формируется из ключа парной связи. Для шифрования данных используется алгоритм ГОСТ 28147-89 в режиме гаммирования с обратной связью. Имитозащита данных осуществляется с использованием алгоритма ГОСТ 28147-89 в режиме выработки имитовставки. Список ключей, используемых комплексом, представлен в Табл.3.

Управление криптографическими ключами осуществляется централизованно из ЦУС. Средствами ЦУС для каждого КШ выполняются следующие операции:

- генерация главных ключей КШ, ключей связи с ЦУС и ключей парной связи;
- передача ключей на КШ;
- смена главных ключей, ключа связи с ЦУС и ключей парной связи;
- формирование ключевых носителей КШ.

Передача ключей парной связи с ЦУС на КШ производится по защищенному каналу связи на ключе связи с ЦУС. Ключи парной связи, зашифрованные на главном ключе КШ, хранятся на жестком диске КШ.

Главный ключ КШ и ключ связи с ЦУС хранятся в энергонезависимой памяти ПАК "Соболь" КШ, а также на жестком диске ЦУС. Ключ хранения ЦУС находится в энергонезависимой памяти ПАК "Соболь", установленного на ЦУС, и предназначен для безопасного хранения БД ЦУС на жестком диске КШ с ЦУС. Ключ хранения КШ/КК находится в энергонезависимой памяти КШ/КК и предназначен для безопасного хранения БД КШ/КК на жестком диске.

Главные ключи, ключи связи с ЦУС и ключи парной связи генерирует ЦУС из исходного ключевого материала ("исходная ключевая информация"). В качестве источника исходной ключевой информации может быть использован ПАК "Соболь" или ключевые блокноты РДП-006 и (или) РДП-А.

Примечание. Комплекты ключевых блокнотов РДП-006 и РДП-А необходимо заказать в установленном порядке в ЦБС ФСБ России.

Для защиты соединения между программой управления и ЦУС используется специальный административный ключ. Этот ключ хранится на идентификаторе администратора комплекса и в БД ЦУС. Ключ администратора зашифровывается с использованием пароля по ГОСТ 28147-89 в режиме гаммирования с обратной связью. Каждому зарегистрированному администратору присваивается уникальный ключ.

Смена ключей шифрования осуществляется периодически в соответствии с принятым планом смены ключей, а также в случае компрометации ключей. Смену ключей на ЦУС выполняют средствами локального управления, смену ключей на КШ — с помощью программы управления или средствами локального управления.

Имеется возможность средствами программы управления создать резервный ключевой материал. При необходимости на основе этого ключевого материала можно сгенерировать ключ связи с ЦУС для любого КШ.

Табл.3 Список ключей, используемых комплексом

Наименование ключа	Назначение	Место хранения
Ключ парной связи (K_{ij})	Шифрование данных, передаваемых между $КШ_i$ и $КШ_j$	Жесткий диск КШ (в зашифрованном виде)
Главный ключ КШ	Шифрование ключей парной связи для хранения на КШ	БД ЦУС, энергонезависимая память ПАК "Соболь" КШ, USB-флеш-накопитель
Ключ связи КШ с ЦУС	Шифрование данных, передаваемых между КШ и ЦУС	БД ЦУС, энергонезависимая память ПАК "Соболь" КШ, USB-флеш-накопитель
Ключ хранения	Шифрование БД ЦУС	Энергонезависимая память ПАК "Соболь" ЦУС
Административный ключ	Защита соединения программы управления с ЦУС	Идентификатор администратора

Аутентификация пользователей

Идентификация и аутентификация пользователей, работающих на компьютерах в защищенной сети КШ, выполняются с помощью специальной программы "Континент. Аутентификация пользователя", установленной на компьютер пользователя.

Регистрация пользователя выполняется средствами централизованного управления комплексом. При регистрации пользователю присваивается имя и пароль. Эти имя и пароль пользователь указывает при аутентификации на своем компьютере.

Доступ предоставляется группам пользователей с помощью правил фильтрации IP-пакетов и правил трансляции сетевых адресов. Группа пользователей связана с определенным сетевым объектом. Доступ, предоставляемый этой группе, действует только на компьютерах, относящихся к этому сетевому объекту.

Информация о зарегистрированных пользователях и группах хранится в базе данных ЦУС, информация о пользователях, прошедших аутентификацию, — на КШ.

Для выполнения идентификации и аутентификации пользователей необходимо включение на КШ режима "Аутентификация пользователей" (см. [**8**]).

Возможна аутентификация только на тех компьютерах, которые подключены к внутренним интерфейсам КШ. Аутентификация пользователя на компьютерах, подключенных к внешнему интерфейсу КШ, не выполняется.

Аутентификация пользователей при подключении к межсетевому экрану на КШ выполняется по идентификатору и паролю, некриптографическим способом.

Обмен данными между КШ и подключаемым компьютером осуществляется по протоколу TCP.

Установка и настройка программы "Континент. Аутентификации пользователя" представлены в [**8**].

Обеспечение отказоустойчивости комплекса

Резервное копирование и восстановление базы данных ЦУС

Резервное копирование и восстановление базы данных ЦУС предназначены для быстрого восстановления работы сети в случае выхода из строя штатного ЦУС.

Резервное копирование базы данных ЦУС выполняется автоматически по заданному расписанию. Рекомендуется после каждого изменения настроек комплекса сохранять резервную копию вручную.

В случае выхода ЦУС из строя осуществляется замена КШ, на котором функционирует ЦУС, на работоспособный. После этого администратор запускает процедуру восстановления базы данных ЦУС из ранее сохраненной резервной копии. Сохранение резервной копии и восстановление базы данных осуществляются администратором с помощью программы управления.

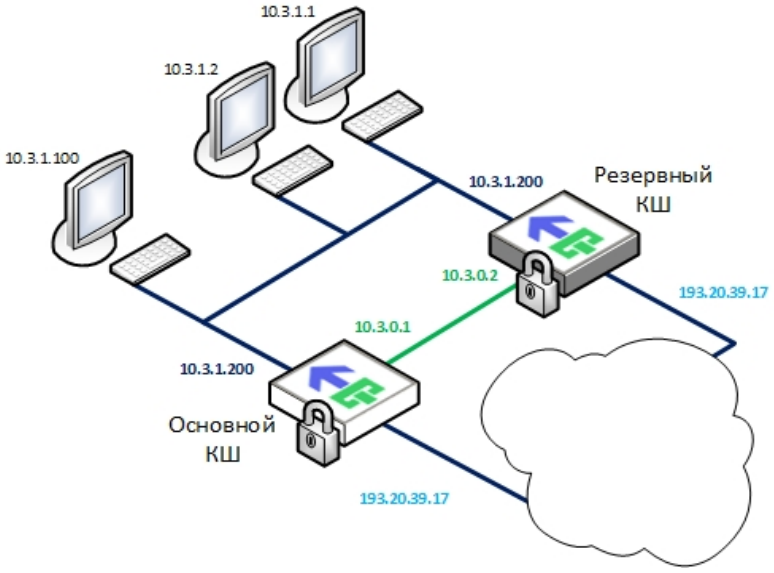
Аппаратное резервирование

Аппаратное резервирование предназначено для обеспечения бесперебойной работы комплекса в случае выхода из строя какого-либо КШ или КК.

Примечание. Возможность аппаратного резервирования отсутствует у КШ, подключенных к телефонным линиям с помощью модема.

Аппаратное резервирование осуществляется путем подключения к основному криптографическому шлюзу (или криптокоммутатору) резервного устройства — создается кластер. Любое из устройств такого кластера может быть как основным, так и резервным. IP- и MAC-адреса внешнего и внутренних интерфейсов у основного и резервного устройств совпадают. При подключении сетевого оборудования к данным интерфейсам необходимо выполнить его настройку, исключающую обнаружение "петель".

Для обмена служебными данными между основным и резервным КШ используются специально выделенные интерфейсы (таких интерфейсов резервирования у КШ может быть несколько). Прием и передача шифруемых данных или обмен данными с ЦУС через эти интерфейсы невозможны. IP-адреса интерфейсов резервирования должны быть уникальными для данной корпоративной сети и различаться для основного и резервного КШ. На рисунке ниже представлен пример использования резервного КШ в корпоративной сети.



Если оба КШ расположены в одной серверной стойке, для их соединения используется сетевой кросс-кабель. В остальных случаях соединение криптографических шлюзов осуществляется через IP-сеть.

В штатном режиме работы основной КШ обрабатывает проходящие через него IP-пакеты и осуществляет связь с ЦУС. Кроме этого он периодически передает на резервный КШ текущие значения счетчиков пакетов. Изменения в конфигурационной информации, полученной от ЦУС, передаются на резервный КШ по мере поступления.

Резервный КШ принимает только данные синхронизации от основного КШ. Его внутренние и внешний интерфейсы отключены, обработка IP-пакетов не производится. Отсутствие сигнала от основного КШ воспринимается как его отключение, и резервный КШ автоматически переходит в активный режим. Время перехода резервного КШ в активный режим составляет около 30 секунд после переключения. При этом в основном окне программы управления ЦУС изменится вид пиктограммы, отображающей вышедший из строя КШ.

Обратное переключение канала связи с резервного КШ на основной может осуществляться как вручную администратором из программы управления, так и автоматически. В автоматическом режиме резервный КШ (который в данный момент является активным) отслеживает наличие сообщений от основного КШ и при их поступлении в течение установленного времени осуществляет обратное переключение. Настройка автоматического режима осуществляется с помощью программы управления.

Автоматическое переключение криптографических шлюзов в кластере осуществляется также при потере соединения на каком-либо из используемых сетевых интерфейсов. Переключение выполняется по следующему алгоритму:

- Проверяются внешние интерфейсы. Активным становится КШ, у которого большее количество работоспособных внешних интерфейсов.

- При одинаковом состоянии внешних интерфейсов проверяется количество функционирующих внутренних интерфейсов. Активным становится КШ, у которого количество работоспособных внутренних интерфейсов больше.
- При одинаковом состоянии внешних интерфейсов и при одинаковом количестве работоспособных внутренних интерфейсов:
  - при включенном автоматическом режиме активным становится основной КШ;
  - при выключенном автоматическом режиме переключения не происходит.

Механизм работы нескольких интерфейсов резервирования следующий. Для обмена трафиком между основным и резервным КШ всегда используется только один интерфейс. При выходе этого интерфейса из строя выполняется автоматическое переключение на следующий интерфейс. Сбой на отдельном интерфейсе в системе не отображается. Регистрируется в журнале и отображается в программе управления только выход из строя всех интерфейсов резервирования.

Централизованное управление сетевыми устройствами

Управление сетью осуществляется с помощью программы управления, установленной на одном или нескольких компьютерах защищенного сегмента сети (РМ администратора). Ограничение на количество РМ администратора отсутствует.

Эти компьютеры должны входить в защищенную сеть, к которой подключен один из интерфейсов ЦУС. Обычное местоположение РМ администратора — в сети, защищаемой таким КШ.

Программа управления устанавливает защищенное соединение с ЦУС и позволяет контролировать все сетевые устройства комплекса через ЦУС в диалоговом режиме.

Внимание! Запуск программы управления возможен только при предъявлении идентификатора администратора комплекса.

Связь между КШ, управляемыми разными ЦУС

Имеется возможность организации защищенного соединения между КШ, принадлежащими разным криптографическим сетям и управляемыми разными ЦУС.

Для этого администраторы этих сетей регистрируют каждый в своей программе управления внешнюю криптографическую сеть и обмениваются конфигурационными файлами со списком разрешенных к доступу ресурсов. Перед отправкой конфигурационный файл снабжается электронной подписью и зашифровывается. При получении файла выполняется проверка электронной подписи и целостности, а также расшифрование его содержимого.

Информационный обмен между КШ, принадлежащими разным сетям, регулируется с помощью правил фильтрации. Ключи парной связи КШ генерируются на основе специального межсетевого ключа.

Для генерации межсетевого ключа, формирования электронной подписи и зашифровывания конфигурационных файлов в комплексе используется собственная инфраструктура открытых ключей. Генерацию ключевой пары и издание сертификата открытого ключа для своей сети выполняет ЦУС. Администраторы обмениваются этими сертификатами до начала процедуры организации связи между сетями.

Контроль сетевых устройств по протоколу SNMP

В комплексе можно контролировать работу сетевых устройств с помощью средств управления объектами сети по протоколу SNMP. Таким образом можно контролировать следующие параметры:

- время работы сетевого устройства с момента включения;
- количество полученных/переданных пакетов;
- состояние интерфейсов (Up/Down) и пр.

Реализовано обслуживание запросов "на чтение" к сетевому устройству. Имеется возможность рассылки служебных сообщений (traps). Эти сообщения рассылаются при возникновении следующих событий:

- "холодный запуск" (coldStart);
- физическое нарушение связи на интерфейсе (linkDown);
- восстановление связи на интерфейсе (linkUp).

Подробное описание модуля приводится в [**10**].

Централизованное управление параметрами SNMP

Централизованное управление параметрами взаимодействия по протоколу SNMP осуществляется в ПУ ЦУС.

Функциональные возможности централизованного управления обеспечивают:

- доступ к мониторингу сетевого устройства или нескольких сетевых устройств;
- возможность изменения параметров подключения системы мониторинга по протоколу SNMP;
- настройку генерации SNMP trap-сообщений.

Подробное описание принципов централизованного управления представлено в [**2**].

Multicast-вещание

Комплекс поддерживает следующие методы рассылки пакетов:

- Unicast — однонаправленная передача данных (сетевой пакет направляется одному адресату);
- Multicast — групповая передача данных (сетевой пакет одновременно направляется определенной группе адресатов).

Метод рассылки определяется типом сетевого объекта (см. [**2**]).

Multicast- вещание используют для организации мультимедиатрансляций, видеоконференций, видеонаблюдения и т. п.

Для групповой рассылки используется специально выделенный диапазон сетевых адресов от 224.0.0.0 до 239.255.255.255.

Автоматическая настройка сетевых параметров

Криптографический шлюз можно использовать в качестве DHCP-сервера или DHCP-ретранслятора. Это позволяет компьютерам автоматически получать IP-адрес и другие параметры, необходимые для работы в сети TCP/IP при загрузке.

Сервис DHCP доступен только для компьютеров, расположенных в защищенных (внутренних) сегментах КШ. При этом за одним внутренним интерфейсом КШ может располагаться только один домен.

Сервис DHCP на КШ может быть отключен или работать в одном из двух режимов:

- сервер;
- ретранслятор.

Режим ретранслятора используется в случаях, когда компьютер не может подключиться к DHCP-серверу напрямую. DHCP- ретранслятор обрабатывает стандартный широковещательный DHCP- запрос и перенаправляет его на DHCP-сервер в виде целенаправленного (unicast) пакета, а полученный от DHCP-сервера ответ, в свою очередь, перенаправляет DHCP-клиенту.

По умолчанию сервис DHCP на КШ отключен.

Управление сервисом DHCP осуществляется удаленно средствами ПУ ЦУС.

Поддержка QoS

Комплекс поддерживает работу следующих механизмов управления QoS:

- классификация трафика;
- маркировка IP-пакетов;
- управление перегрузками с помощью очередей;
- предупреждение перегрузок.

Классификация трафика

Классы трафика определяют в специальном справочнике. Максимальное количество классов — 32. Принадлежность конкретных IP-пакетов классу указывается в правилах фильтрации и трансляции.

Маркировка IP-пакетов

Маркировка IP-пакета определяется значением поля ToS в заголовке IP-пакета. Правила маркировки устанавливаются при определении класса (см. [**5**]). Имеются следующие возможности автоматической обработки поля ToS:

- сохранение имеющегося значения;
- заполнение классификатором DSCP;
- заполнение классификатором IPP.

Управление перегрузками с помощью очередей (распределение по очередям)

Комплекс предоставляет возможности по управлению очередями следующих типов:

- очередь на обработку IP-пакетов блоком криптографической защиты;
- очередь на отправку IP-пакетов сетевым интерфейсом.

Обработка IP-пакетов блоком криптографической защиты выполняется в соответствии с приоритетом, указанным для данного класса трафика. Приоритет указывается в свойствах класса. Возможные значения 0—31. Большему значению соответствует более высокий приоритет.

Методы обработки очередей (планировщики) на отправку IP-пакетов сетевыми интерфейсами представлены в Табл.4. На сетевом интерфейсе можно организовать очереди только с одинаковым методом обработки. Максимальное количество очередей – 16 для PRIQ и 8 для CBQ и HFSC. IP-пакеты, для которых очередь не определена явным образом, поступают в очередь по умолчанию.

Табл.4 Методы обработки очередей

Метод	Описание
PRIQ	Priority Queuing. Последовательная обработка очередей в соответствии с их приоритетами. Возможна монополизация канала высокоприоритетными очередями
CBQ	Class Based Queuing. Обработка очередей в соответствии с выделенной на очередь долей общей полосы пропускания. Имеется возможность учитывать приоритеты очередей, а также включать для очереди механизм заимствования общей полосы пропускания в случае неиспользования ее другими очередями (borrow)
HFSC	Hierarchical Fair Service Curve. Дополнительно к возможностям CBQ предлагается два типа управления очередью: realtime и linkshare (см. Табл.5). Параметры Service Curve в данной версии не поддерживаются

Табл.5 Дополнительные параметры HFSC

Метод	Описание
realtime	Полоса пропускания, гарантируемая для данной очереди независимо от потребностей других очередей. При необходимости указанное значение может быть превышено, если определено значение параметра upperlimit
linkshare	Доля общей полосы пропускания, выделенная для данной очереди. При необходимости указанное значение может быть превышено, если определено значение параметра upperlimit
upperlimit	Максимальная полоса пропускания, устанавливаемая для данной очереди. Значение параметра должно быть больше или равно значению, указанному для параметра realtime или linkshare. Необязательный параметр

Предупреждение перегрузок

Поддерживаемые комплексом механизмы защиты от перегрузок представлены в Табл.6. Включение нужного механизма выполняется при настройке очереди на сетевом интерфейсе.

Табл.6 Механизмы управления переполнением очередей

Механизм	Описание
RED	Random Early Detection. Предупреждение перегрузок путем отбрасывания пакетов из случайно выбранных сессий. При использовании RED невозможно разделение по классам QoS
RIO	RED In/Out. Разновидность алгоритма RED, позволяющая использовать классы QoS
ECN	Explicit Congestion Notification. Предупреждение перегрузок путем уведомления отправителя посредством ECN-сессии

Поддержка IPv6

Комплекс поддерживает работу с каналами связи общих сетей передачи данных, использующих протоколы IPv6. При этом действуют приведенные ниже правила и ограничения:

- Протокол IPv6 поддерживается только внешними интерфейсами КШ/ДА и используется только для зашифрованного трафика.
- Связь между двумя КШ может быть установлена только при совпадении версий IP на их внешних интерфейсах.
- В защищенных подсетях комплекса используется адресное пространство IPv4.
- Управляющий трафик ЦУС–КШ может осуществляться как по протоколу IPv6, так и по протоколу IPv4 (в зависимости от версии IP на внешних интерфейсах КШ).
- Рабочие станции защищаемой криптошлюзом подсети не могут обращаться к ресурсам IPv6 в открытой сети и наоборот — запрещен доступ из открытой сети с адреса IPv6 к ресурсам подсети, защищенной криптошлюзом.
- Не поддерживается динамическое назначение IPv6-адресов.
- Для PPP-интерфейсов адресация IPv6 не используется.

Сбор данных для SIEM-систем

В АПКШ "Континент" предусмотрена возможность сбора данных для SIEM-систем. Сбор данных в комплексе осуществляется с помощью программы SIEM Connector. SIEM Connector собирает журналы из ПУ ЦУС и формирует из них файл с расширением .xml, который хранится на жестком диске компьютера.
Сбор журналов осуществляется в соответствии с заданным в программе расписанием. Подробное описание программы представлено в [**6**].

Универсальный коннектор

В АПКШ "Континент" предусмотрен программный модуль — коннектор "Континент. Универсальный коннектор" (далее — коннектор) для выгрузки конфигурации СУ комплекса, формирования XML-файлов для анализа системой Skybox Security, Efros Config Inspector и экспорта в КБ "Континент". Версия 4".

Выгрузка и отправка конфигурации осуществляется в соответствии с заданным расписанием или по команде администратора.

Коннектор может экспортировать конфигурации для всех сетевых устройств комплекса версии 3.9.0 и выше.

Интеграция с SkyBox

Конфигурации КШ сохраняются в XML-файлы, каждый XML-файл содержит конфигурацию КШ. По умолчанию название XML-файла содержит ID КШ, обозна-чение системы Skybox, тип КШ и имя КШ. С помощью настроек профиля можно включить добавление даты и времени экспорта к имени файла.

Интеграция с Efros Config Inspector

Конфигурации СУ сохраняются в XML- файлы, каждый XML-файл содержит конфигурацию одного устройства. По умолчанию название XML-файла содержит ID СУ, обозначение системы Efros, тип СУ и имя СУ. С помощью настроек профиля можно включить добавление даты и времени экспорта к имени файла.

Экспорт конфигураций СУ в КБ "Континент" версии 4

Конфигурации КШ сохраняются в единый XML-файл, для именования файлаиспользуются данные ЦУС, с которого выполняется экспорт. С помощью настроек профиля можно включить добавление даты и времени экспорта к имени файла. В конфигурацию для анализа включаются сведения об объектах в выбранном ЦУС.

Защитные механизмы

В состав программного обеспечения комплекса входят защитные механизмы, позволяющие реализовать следующие функции:

- создание для пользователей ограниченной замкнутой среды программного обеспечения компьютера (замкнутой программной среды);

- разграничение доступа пользователей к ресурсам файловой системы и устройствам компьютера;
- контроль целостности защищаемых ресурсов;
- регистрация событий безопасности.

Настройка и управление защитными механизмами может выполняться средствами системы Secret Net Studio, устанавливаемой в составе программного обеспечения комплекса. Описание настройки и управления защитными механизмами приведено в эксплуатационной документации Secret Net Studio.

Лицензирование

Имеется ряд ограничений на использование комплекса, связанных с политикой лицензирования данного продукта.

Ограничение на параметры ЦУС:

- максимальное количество сетевых устройств, имеющих статус "Введен в эксплуатацию".

Ограничения на использование комплекса определяются приобретенными лицензиями на использование данного продукта.

Лицензии разделяются по типам. Предусмотрены следующие типы лицензий:

Тип лицензии	Описание
Ввод в эксплуатацию	Используется при создании сети ЦУС и вводе сетевого устройства в эксплуатацию
Обновление	Используется при локальном и дистанционном обновлении ПО сетевого устройства, а также при централизованном управлении локально обновленным КШ. При обновлении ПО КШ проверяется наименование аппаратной платформы КШ и его соответствие наименованию, указанному в лицензии. При отсутствии в базе ЦУС лицензии на обновление для аппаратной платформы локально обновленного КШ такой КШ обслуживаться не будет и будет отображаться в ПУ ЦУС как отключенный
Обновление базы решающих правил	Используется при загрузке базы решающих правил с сервера обновлений. При отсутствии лицензии ручная загрузка файла обновлений базы решающих правил в ЦУС запрещена

Лицензии на максимальное количество введенных в эксплуатацию сетевых устройств являются накопительными. Общее количество разрешенных к использованию объектов определяется суммой объектов, указанных в каждой лицензии.

Первоначальная регистрация лицензий для ЦУС выполняется при первом запуске программы управления ЦУС.

Документация

1. Аппаратно-программный комплекс шифрования "Континент". Версия 3.9. Руководство администратора. Ввод в эксплуатацию.
2. Аппаратно-программный комплекс шифрования "Континент". Версия 3.9. Руководство администратора. Управление комплексом.
3. Аппаратно-программный комплекс шифрования "Континент". Версия 3.9. Руководство администратора. Межсетевое экранирование.
4. Аппаратно-программный комплекс шифрования "Континент". Версия 3.9. Руководство администратора. Сетевые функции.
5. Аппаратно-программный комплекс шифрования "Континент". Версия 3.9. Руководство администратора. Настройка VPN.
6. Аппаратно-программный комплекс шифрования "Континент". Версия 3.9. Руководство администратора. Аудит.
7. Аппаратно-программный комплекс шифрования "Континент". Версия 3.9. Руководство администратора. Сервер доступа.
8. Аппаратно-программный комплекс шифрования "Континент". Версия 3.9. Руководство администратора. Клиент аутентификации пользователя.
9. Аппаратно-программный комплекс шифрования "Континент". Версия 3.9. Руководство администратора. Обнаружение вторжений.
10. Аппаратно-программный комплекс шифрования "Континент". Версия 3.9. Руководство администратора. Настройки и использование SNMP.