1. Нормативные документы в области применения средств криптографической защиты информации

1. Федеральный закон № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
2. Федеральный закон № 152-ФЗ «О персональных данных»;
3. Положение об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденное постановлением Правительства Российской Федерации от 17 ноября 2007 года № 781;
4. Порядок проведения классификации информационных систем персональных данных, утвержденный приказом ФСТЭК России, ФСБ России и Мининформсвязи России от 13 февраля 2008 года № 55/86/20;
5. Положение о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005), утвержденное приказом ФСБ России от 9 февраля 2005 года № 66;
6. Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну, в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных (ФСБ России, № 149/6/6-622, 2008);
7. Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации (ФСБ России, № 149/54-144, 2008).
8. Приказ ФСБ РФ от 27 декабря 2011 г. № 796 «Об утверждении Требований к средствам электронной подписи и Требований к средствам удостоверяющего центра».
9. Приказ ФСТЭК от 11 февраля 2013 г. № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».
10. Положение «О сертификации средств защиты информации»: утв. постановлением Правительства Российской Федерации от 26 июня 1995 г. № 608 ».
11. Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных правительством российской федерации требований к защите персональных данных для каждого из уровней защищенности : РД: утв. приказом ФСБ России от 10 июля 2014 г. № 378.

Ср-ва шифрования – аппар., прогр., и апп-прогр средства, сис-мы и ком-сы, реализ. алг-мы криптогр преобр ин-ции и предн-е для ЗИ при прд по кан связи и для защиты от НСД при ее обработке и хранении.

Ср-ва имитозащиты – как ср-ва шифрования только для защиты от навязывания ложной ин-ции

Ср-ва ЭП

2. Классы и виды средств криптографической защиты информации

Шесть уровней КС1, КС2, КС3, КВ1, КВ2, КА1 криптографической защиты информации, не содержащей сведений, составляющих государственную тайну, определенных в порядке возрастания количества и жесткости предъявляемых к криптосредствам требований.

Уровень криптографической защиты информации, не содержащей сведений, составляющих государственную тайну, обеспечиваемой криптосредством, определяется заказчиком этого криптосредства в ТЗ путем отнесения нарушителя, действиям которого должно противостоять криптосредство, к конкретному типу.

При отнесении заказчиком нарушителя к типу Н1 криптосредство должно обеспечить криптографическую защиту по уровню КС1, к типу Н2 – КС2, к типу Н3 – КС3, к типу Н4 – КВ1, к типу Н5 – КВ2, к типу Н6 – КА1.

Шесть классов криптосредств, обозначаемых через КС1, КС2, КС3, КВ1, КВ2, КА1.

Встраивание криптосредств класса КС1 и КС2 осуществляется без контроля со стороны ФСБ России (если этот контроль не предусмотрен техническим заданием на разработку (модернизацию) информационной системы).

Встраивание криптосредств класса КС3, КВ1, КВ2 и КА1 осуществляется только под контролем со стороны ФСБ России.

Н1 - внешний нарушитель из числа лиц категории I, самостоятельно осуществляющий создание способов атак, подготовку и проведение атак;

Н2 - внутренний нарушитель из числа лиц категории II, не имеющий права доступа к средствам вычислительной техники (СВТ), на которых реализованы криптосредства и СФК, самостоятельно осуществляющий создание способов атак, подготовку и проведение атак;

Н3 - внутренний нарушитель из числа лиц категории II, являющийся пользователем СВТ, на которых реализованы криптосредства и СФК, самостоятельно осуществляющий создание способов атак, подготовку и проведение атак;

Н4 - внутренний нарушитель из числа лиц категории II, являющийся пользователем СВТ, на которых реализованы криптосредства и СФК, осуществляющий создание способов и подготовку атак с привлечением специалистов, имеющих опыт разработки и анализа криптосредств (включая специалистов в области анализа сигналов линейной передачи и сигналов ПЭМИН криптосредств);

Н5 - внутренний нарушитель из числа лиц категории II, являющийся пользователем СВТ, на которых реализованы криптосредства и СФК, осуществляющий создание способов и подготовку атак с привлечением специалистов, имеющих опыт разработки и анализа криптосредств (включая специалистов в области использования для реализации атак недокументированных средств прикладного программного обеспечения);

Н6 - внутренний нарушитель из числа лиц категории II, действующий в интересах спецслужбы или организации иностранного государства и являющийся пользователем СВТ, на которых реализованы криптосредства и СФК, осуществляющий создание способов и подготовку атак с привлечением специалистов, имеющих опыт разработки и анализа криптосредств (включая специалистов в области использования для реализации атак недокументированных средств системного программного обеспечения)

3. Назначение и состав комплекса криптографической защиты Континент

АПКШ "Континент" относится к классу средств криптографической защиты информации (СКЗИ) и предназначен для защиты информации при передаче по открытым каналам связи, а также для ее защиты от несанкционированного доступа при ее обработке и хранении.

Состав

– криптографический шлюз: (для КрЗИ при передаче на сетевом уровне – L3 VPN. Он совмещает в себе шифратор трафика, МЭ и маршрутизатор).
– криптографический коммутатор (КрЗИ при передаче на канальном уровне – L2 VPN);
– детектор атак (анализ сетевого трафика и обнаружение угроз безопасности);
– ЦУС: Предназначен для централизованного управления всеми КШ, входящими в состав АПКШ. ЦУС представляет собой КШ на котором установлено специальное ПО ЦУС;
– СД (предназначен для выполнения процедур идентификации и аутентификации удаленных пользователей при подключении абонентских пунктов "Континент-АП" к защищаемой сети;
– абонентский пункт "Континент-АП" (для обеспечения доступа удаленных пользователей в сеть, защищаемую АПКШ "Континент" и КрЗИ АП, является специализированным ПО, которое устанавливается на рабочих местах удаленных пользователей).
– программа управления (ПУ ЦУС) (для централизованного удаленного управления настройками и оперативного контроля состояния всех КШ, входящих в состав комплекса).
– программа агент управления сетью криптографических шлюзов (для получения, обработки и хранения системных событий и событий ИБ АПКШ "Континент");
– программа управления сервером доступа (для управления объектами базы данных сервера доступа и оперативного контроля его состояния.).

АПКШ "Континент" обеспечивает:

1)шифрование и имитозащиту информации;
2)работу по различным каналам и линиям связи;
3)резервирование гарантированной полосы пропускания;
4)приоритезацию трафика VoIP и ВКС;
5)обнаружение сетевых вторжений;
6)фильтрацию пакетов;
7)маршрутизацию трафика;
8)создание VLAN;
9)скрытие внутренней структуры защищаемых сегментов сети (NAT/PAT);
10)централизованное управление и обновление ПО;
11)аудит и мониторинг событий ИБ;

4. Система управления Континент: ЦУС и программа управления. Назначение и функции криптошлюза Континент

Криптографический шлюз "Континент" предназначен для криптографической защиты информации при ее передаче по открытым каналам связи. Он совмещает в себе шифратор трафика, МЭ и маршрутизатор, кроме этого позволяет выполнить трансляцию IP-адресов внутренней сети и портов с целью сокрытия от злоумышленников их истинных значений.

Обеспечивает:

1)прием и передачу IP-пакетов по протоколам семейства TCP/IP с возможностью приоритезации IP-трафика;
2)сжатие, криптографическое преобразование и имитозащиту IP-пакетов;
3)фильтрацию IP-пакетов в соответствии с заданными правилами фильтрации;
4)трансляцию сетевых адресов и портов в соответствии с заданными правилами трансляции;
5)работу с виртуальными локальными сетями, организованными в защищаемых сегментах сети;
6)скрытие внутренней структуры защищаемого сегмента сети;
7)регистрацию событий аудита и их передачу на центр управления сетью;
8)идентификацию и аутентификацию администратора при запуске и управлении КШ;
9)контроль целостности программного обеспечения КШ; работу в режиме "горячего" резервирования.

Программа Агент управления сетью криптографических шлюзов предназначена для получения, обработки и хранения системных событий и событий информационной безопасности АПКШ "Континент".

Обеспечивает: установление защищенного соединения и обмен данными с ЦУС и Программой управления сетью криптографических шлюзов; получение от ЦУС содержимого журналов аудита в соответствии с установленным расписанием; очистку журналов аудита в соответствии с установленным расписанием; автоматическое создание резервной копии конфигурации ЦУС в соответствии с установленным расписанием.

Центр управления сетью (ЦУС) криптографических шлюзов предназначен для централизованного управления в режиме реального времени всеми криптографическими шлюзами, входящими в состав АПКШ Континент и представляет собой КШ на котором установлено специальное ПО – центр управления сетью.

Дополнительно обеспечивает: аутентификацию КШ, сервера доступа, программ управления и аудита; удаленную настройку КШ (в т.ч. перезагрузку) по защищенному каналу; взаимодействие с Программой управления по критографически защищенному каналу; централизованное управление криптографическими ключами и их рассылку; мониторинг и хранение информации состояния информационной безопасности всех КШ АПКШ; получение и временное хранение системных журналов и журналов НСД КШ. Они могут быть импортированы программой управления на АРМ администратора в виде базы данных MS SQL; оповещение Программы управления о событиях, требующих оперативного вмешательства администратора комплекса в режиме реального времени; восстановление информации о состоянии АПКШ из резервной копии; создание резервной копии конфигурации для реализации холодной замены ЦУС.

5. Виды ключей в АПКШ Континент. Криптопровайдер СКЗИ АПКШ Континент.

Каждый КШ имеет собственный номер.При распределении ключевых данных (КД) между КШ сети, должно быть определено соответствие идентификаторов сетевым адресам КШ. Для задания такого соответствия служат адресные таблицы.У каждого конкретного КШ имеются адреса и ключи только тех КШ сети, с которыми он имеет связь.

Ключевые документы комплекса:

- ключевые блокноты ДС-001, изготавливаемые ЦБС ФСБ;

- ключевой комплект для связи ПУ с ЦУС;

- ключевой комплект для связи ЦУС с КШ.

В комплексе в качестве носителей ключевой информации используются стандартный ГМД 3,5" и USB Flash-накопитель.Ключевой блокнот ЦБС ФСБ представляет собой два ГМД (основной и резервный). Ключевые комплекты для связи с ПУ и с КШ изготавливаются администратором службы безопасности.

Наим ключа	Назначение	Срок	Место хранения
Ключ шифр пакета	Шифрование IP-пакетов	сеанс	ОЗУ КШ
Ключ парной связи	Формирование ключей шифрования пакетов	1 год	жесткий диск КШ
Глав ключ КШ	Шифр-е ключей парной связи для хранения на жестком диске	1 год	жесткий диск ЦУС, энергонезависимая память ПАК "Соболь" КШ
Ключ связи с ЦУС	Шифр ключей ПВС для передачи КШ	1 год	Аналогично выше
Ключ хранения	Шифр главных ключей КШ и ключей связи с ЦУС для хранения на на жестком диске	Неогр	энергонезависимая память ПАК "Соболь" КШ
Адм ключ	Защита соединения ПУ с ЦУС	1 год	идентификатор адм

6. Возможности комплекса криптографической защиты Континент: межсетевое экранирование, шифрование, виды криптотуннелей, приоритезация трафика, QoS, MultiWAN.

MultiWAN:

КШ может быть одновременно подключен к нескольким внешним сетям (например, принадлежащим разным провайдерам). Имеются следующие режимы Multi-WAN:

1)Передача трафика в соответствии с таблицей маршрутизации;

2)Обеспечение отказоустойчивости канала связи;

3)Балансировка трафика между внешними интерфейсами КШ.

Поддержка QoS

Комплекс поддерживает работу следующих механизмов управления QoS:

1.классификация трафика(Классы трафика определяют в специальном справочнике. Максимальное количество классов – 32);

2.маркировка IP-пакетов(Маркировка IP-пакета определяется значением поля ToS в заголовке IP-пакета.

Правила маркировки задают при определении класса.);

3.управление перегрузками с помощью очередей:

Комплекс предоставляет возможности по управлению очередями следующих

типов:

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

4.предупреждение перегрузок

Шифрование:

1.Алгоритм шифрования ГОСТ 28147-89 (гаммирование с ОС)

2.Защита от искажений ГОСТ 28147-89 (иммитовставка)

3.Длина ключа 256 бит

Виды криптотуннелей:

1.Статический

2.Динамический

Криптографический шлюз обладает функциями межсетевого экрана – инспектора состояния (stateful inspection firewall). Правила фильтрации позволяют разграничить доступ по различным параметрам: интерфейсам КШ; IP-адресам отправителя и получателя; номерам портов TCP/UDP; флагам заголовка пакета; времени работы правила фильтрации.

Обнаружение сетевых атак Для обнаружения компьютерных атак к одному из сетевых интерфейсов КШ подключают выделенную ПЭВМ с установленной на ней системой обнаружения атак (СОА), а этот интерфейс определяется как SPAN-порт (Switched Port Analyzer).

7. Назначение и состав комплекса криптографической защиты Дионис.

Об. Назн. - для обеспечения ИБ во внутр. сети организации посредством криптозащиты, МЭ и предоставления информационных услуг пользователям посредством развертывания сервера прикладных инф.служб.

Частн. Назн.: (для информации не сост. ГТ)

1) шифрования и вычисления ЭП информации;

2) вычисления ЭП, имитовставки и шифр. областей оперативной памяти;

3) шифрования и имитозащиты IP-трафика;

4) генерации и управления КИ.

Возможности: ГОСТ 28147-89. – шифр.

1. **NAT, Аудит, Туннелирование**
2. **Фильтрация пакетов IP-трафика**
3. **Аутентификация(клиентск.,межузл-я)**
4. **Сжатие данных при туннелировании (LZW)**
5. **Поточное аппаратное/програмное шифр (в режиме гаммирования,имитозащита)**
8. **Симметр/несиметр. Многоуровн. Сист КИ**
9. **Сервер доступа, Контроль целостности**
10. **Расписание доступа для клиентов**
11. **Защищенный сервер почты с возм. Фильтр.**
12. **FTP сервер, Сервер файловых Транз-й, DNS**
13. **Удаленное упр-е,мониторинг, протокол SNMP.**

Состав:

8. Основные типы изделий Дионис. Функционал и программные компоненты изделия Дионис. Система управления Дионис: ЦГУ (ЦУА), Diadm.

ИЗДЕЛИЯ (УЗЛЫ) КОМПЛЕКСА И ИХ ЗАДАЧИ

1.Создание ведомственных интегрированных ССПД (IP-телефония, видеоконференцсвязь, обмен данными), составляющих ГТ, с использованием следующих компонентов:

специализированные Маршрутизаторы серии DioNIS TS 16000R , DPS ;

специализированные Криптомаршрутизаторы серии КМ-07Ф, КМ-МПМ, Dionis-NX;

межсетевой экран DioNIS FW 16000R

2.Создание ведомственных интегрированных сетей и систем передачи конфиденциальной информации (IP-телефония, видеоконференции, обмен данными) с использованием следующих компонентов:

криптомаршрутизаторы серии DIONIS: DioNIS TS/FW 16000/KB2, Dionis-LXM;

межсетевые экраны «DioNIS Firewall»

защищенный сервер электронной почты и файловых транзакций DIONIS

3. Создание для конфиденциальных приложений специализированных сетей и систем гарантированной доставки сообщений (унифицированных транспортных подсистем).

АБОНЕНТСКИЕ СРЕДСТВА КОМПЛЕКСА

Для обесп-ия абонентского шифрования и ЭП могут использоваться защищенные клиентские места (АРМ):

DiPostS.OOC с функциями ЭЦП и шифрования корреспонденции, «DiPostCA» - - автоматизированное рабочее место абонента электронной почты: почтовое клиентское ПО, обладающее функциями шифрования;

DiSec - клиент криптографического сервера доступа, программное средство шифрования абонентского трафика TCP/IP,

DiSign - - абонентский пункт ЭП: обеспечение ЭП документов Microsoft Office. «DiSignCA» - осуществляет формирование и проверку электронной подписи для файлов.

УПРАВЛЕНИЕ КМ "ДИОНИС"

1. Управление с помощью локальной консоли.

2. Управление с помощью удаленной консоли. (ОС DOS, Windows или Linux) На компьютере должна быть установлена программа "DiAdm".

3. Центр группового управления "DionisMC" производства компании "ФАКТОР-ТС". ЦГУ требует для своей работы отдельный компьютер с установленной ОС Windows XP.

4. Использование для удаленного управления другого КМ "ДИОНИС". В этом варианте удаленный управляющий узел "ДИОНИС" фактически выполняет функции ЦГУ "DionisMC".

9. Возможности подсистемы криптографической защиты Дионис (виды криптотуннелей) и подсистемы межсетевого экранирования изделия Dionis. Виды и назначение ключей

Возможности:
Развязка внутреннего и внешнего адресного пространства NAT;
Фильтрация пакетов IP-трафика;
Настраиваемые правила фильтрации;
IP-фильтрация по временному графику;
Фиксация фильтруемого трафика и случаев нарушения правил фильтрации;
Аутентификация: клиентская с ключом 256 битPAP/CHAP межузловая;
Туннелирование, правила отбора и временной график работы туннеля;
Сжатие данных при туннелировании алгоритмами LZW;
Межузловое поточное аппаратное или программное шифрование IP-датаграмм в режиме гаммирования. Имитозащита. Симметричная и несимметричная многоуровневая система ключей.
Возможность работы с ключами на дискетах,Smart Card и Touch Memory;
Индивидуальные для каждого клиента настройки расписания доступа, общего времени работы, даты истечения доступа;
Защищенный SMTP/POP3/IMAP4-сервер почты с возможностью фильтрации и антивирусной проверки почты.
Полная архивация всей корреспонденции;
Защищенный FTP-сервер, Сервер файловых транзакций для реализации клиент-серверных приложений;
Защищенный DNS-сервер;Многоуровневый доступ абонентов к сервису;
Удаленное управление, мониторинг, поддержка протокола SNMP;
Механизм постоянного и динамического контроля целостности данных в памяти и файловой системе;
Ключи: IP-шифрование и Межхостовое шифрование используют ключевую систему с симметричными ключами;
Абонентское шифрование использует ключевую систему с несимметричными ключами.

Состав ключевых дискет: Файлы: GK.DB3 - главный ключ
UZ.DB3 - узел замены
RANDOM.INI - начальное заполнение датчика случайных чисел

Директории: KM_K - ключевая информация для IP-шифратора.
В директории файлы: CKD, KIS_1 HOST - ключевая информация для межхостового шифрования
В директории файлы: nnnnn.KEY - ключ сетевого набора. SYS - сетевой набор

Варианты применения СКЗИ в комплексе ДИОНИС
1. Абонентское шифрование - шифрование и электронная подпись почтовой корреспонденции и файлов на рабочих местах абонентов узлов ДИОНИС и других Internet-узлов.
2. Межхостовое шифрование (Криптопочтамт) -шифрование потоков почтовой корреспонденции и файлов при обмене информацией между узлами ДИОНИС.
3. IP-шифрование - шифрование IP-потоков между узлами ДИОНИС.
4. IP-шифрование (Сервер доступа) - шифрование IP-потоков между узлами ДИОНИС и мобильными абонентами

10. Назначение и возможности комплекса криптографической защиты ViPNet.

Назначение: защита видеоконференций и IP-телефонии; доступ к распределенным информационным ресурсам объединенной сети; организация систем информационных киосков и банкоматов, функционирующих в необслуживаемом режиме; безопасное использование каналов связи сетей общего доступа для объединения удаленных офисов; безопасное защищенное подключение удаленных пользователей к ресурсам локальных сетей; устранение конфликтов пересечения IP-адресации в локальных сетях; идентификация и аутентификация трафика в защищенной сети в режиме «точка-точка»; идентификация и авторизация пользователей средств VPN; контроль и управление распределенной сетью; создание структуры PKI и многое другое.

Состав и возможности комплекса:

VipNet Administrator(выполняет функции создания, настройки, модификации и управления защищенной VPN-сетью), включающий в себя:
ViPNet NCC (ЦУС) — ПО, предназначенное для конфигурирования и управления виртуальной защищенной сетью ViPNet (Формирование и хранение первичной ключевой информации);
Формирование ключей шифрования для узлов защищенной сети и ключей шифрования между пользователями защищенной сети (двухуровневая схема);
Выполнение процедур смены мастер-ключей и компрометации ключей шифрования;
Выработка персональных ключей защиты пользователей и криптографически надежных парольных фраз (паролей);
Запись персональных ключей пользователей на аппаратные носители ключей — электронные идентификаторы
ViPNet KC & CA (УЦ и КЦ) — ПО, которое выполняет функции центра формирования ключей шифрования и персональных ключей пользователей —Ключевого Центра, а также функции Удостоверяющего Центра.
Остальные элементы комлпекса:

ViPNet StateWatcher (Центр мониторинга, ЦМ) — программный комплекс, который реализован по клиент-серверной технологии и предназначен для централизованного мониторинга состояния узлов защищенной сети ViPNet. Криптопровайдер ViPNet CSP — ViPNet Client содержит встроенный криптопровайдер, реализующий стандартный для разработчиков прикладных систем для ОС Windows интерфейс Microsoft CryptoAPI 2.0. Программа ViPNet Publication Service (Сервис Публикации) предназначена для автоматизации процессов публикации выпущенных в УЦ ViPNet сертификатов и списков отозванных сертификатов.
Программный комплекс ViPNet Registration Point (Пункт Регистрации) предназначен для создания защищенного АРМ регистрации пользователей, хранения регистрационных данных, создания запросов на выпуск сертификатов и их обслуживание в УКЦ, а также запросов на формирование ключевых дистрибутивов пользователей сети ViPNet в УКЦ.
VipNet Coordinator(VPN-сервер, выполняет работу NAT, явл-ся защи-ым почт-ым сер-ом для соед-ия незащищ-ых комп-ов). VipNet Client(обеспе-ет защи-ое соеди-ие по TCP/IP с другими поль-ми.

11. Система управления ViPNet. Назначение и функции ViPNet Administrator. Криптопровайдер СКЗИ ViPNet.

ViPNet Administrator предназначен для:

1.Создания VPN-сети на основе технологии ViPNet администрирования VPN-сети (добавление, удаление, изменение объектов сети, настройка параметров работы, контроль работоспособности и др.)

2.Обновления ПО ViPNet, установленного на узлах защищенной сети

Состав:

Серверное приложения ЦУС

Клиентское приложения ЦУС

База данных SQL

Удостоверяющий и ключевой центры

VipNet-ЦУС выполняет следующие функции:

Создание и модификация структуры сети ViPNet;

Разграничение уровней полномочий пользователей сети ViPNet;

Отправка ключевой и справочной информации, обновлений ПО ViPNet на сетевые узлы;

УЦ и КЦ выполняют следующие функции:

Формирование и управление ключевой структурой сети

Издание и управление сертификатами пользователей

ViPNetCSP - криптопровайдер, обеспечивающий вызов криптографических функций из различных приложений, использующих интерфейс CryptoAPI 2.0.
Предназначен для реализации криптографических функций
Устанавливается как отдельная программа
Может быть установлен как из отдельного установочного файла, так и вместе с программами ViPNet Client, ViPNet Coordinator, ViPNet CryptoService
Назначение ViPNet CSP
создание ключей электронной подписи
вычисление и проверка электронной подписи
Хэширование данных
шифрование и имитозащита данных
генерация случайных и псевдослучайных чисел, ключей шифрования
аутентификация и выработка ключа при передаче данных по протоколам SSL/TLS
хранение сертификатов открытых ключей непосредственно в контейнерах ключей
поддержка различных устройств хранения электронных ключей

12. Состав и функции программно-аппаратных и программных средств ViPNetCoordinator.

VipnetCoordinator-многофункц.ПО.

ViPNet Coordinator предназначен для:

1.Защиты сегментов IP-сетей

2.Защиты трафика, передаваемого по открытым каналам связи

3.Координации работы узлов защищенной сети

Функции ViPNet Coordinator

Выполняет функции персонального и межсетевого экрана

Создает туннели для организации защищенных соединений с открытыми узлами

Осуществляет трансляцию адресов (NAT) для проходящего через координатор открытого трафика

Позволяет разделить доступ защищенных узлов в Интернет и к ресурсам локальной сети

Позволяет исключить любые атаки в реальном времени на компьютеры локальной сети

Обеспечивает обмен служебными и прикладными транспортными конвертами между узлами сети ViPNet.

Сообщает защищенным узлам информацию об IP-адресах и параметрах доступа других узлов

Обеспечивает маршрутизацию транзитного VPN-трафика, проходящего через координатор на другие защищенные узлы

Аппаратные реализации: ViPNet Coordinator HW1000 (криптошлюз и межсетевой экран, построенный на аппаратной платформе телекоммуникационных серверов компании «Аквариус» и выполняющий функции криптошлюза и межсетевого экрана; интегрируется в существующую инфраструктуру, защищает передаваемую информацию от НСД и подмены); - ViPNet Coordinator HW-VPNM (модуль расширения для шлюзов безопасности USG2000 компании Huawei Symantec); - ViPNet Coordinator NME-RVPN (модуль расширения для аппаратных решений Cisco Systems); - ViPNet Coordinator HW 100 — это компактный криптошлюз и межсетевой экран.

Для установки ViPNet Coordinator необходимо иметь: - Соответствующий инсталляционный комплект, - Набор ключей (ключевой дистрибутив) и парольную информацию для пользователя координатора, предоставляемые админом УКЦ. Ключевой дистрибутив содержит: всю ключевую информацию, справочники и регистрационный файл.

13. Предназначение, основные элементы и структура ТСКП (иерархическое представление зон ТСКП).

Трансп сеть с комм пакетов- это распределенная организационно-техническая система, предназначенная передачи и коммутации оцифрованной информации в виде частей небольшого размера — так называемых пакетов, которые передаются по сети в общем случае независимо друг от друга (дейтаграммы), либо последовательно друг за другом по виртуальным соединениям.

Достоинства: Эффективность использования пропускной способности, При перегрузке сети никого не «выбрасывает» с сообщением «сеть занята», сеть просто снижает всем или нескольким абонентам скорость передачи,Абонент, использующий свой канал не полностью, фактически отдаёт пропускную способность сети остальным

Недостатки: Пропускная способность расходуется на передачу технических данных (служебной информации), Задержки доставки, в том числе переменные, из-за того, что при занятости исходящего канала пакет может ждать своей очереди в коммутаторе.

Структура пакета: адрес источника, адрес назначения, номер последовательности.

Перед передачей каждое сообщение разбивается на пакеты, фиксированного пути нет, пакеты маршрутизируются в соответствии с наилучшим возможным маршрутом на текущий момент, когда пакеты достигают назначения, они мб собраны в исх сообщ, используя номера последовательности.

<u>Характеристики сети:</u> пакет содержит адресную, управляющую, информационную и контрольную части, т.е. в его заголовке имеются флаг, адреса отправителя и получателя, тип кадра (служебный или информационный), номер кадра (используется для правильной сборки сообщения из пакетов); на канальном уровне применено оконное управление, размер окна задает число кадров, которые можно передать до получения подтверждения; передача данных по виртуальным (логическим) каналам, т.е. это сети с установлением соединения; узлы на маршруте, обнаружив ошибку, ликвидируют ошиюочный пакет и запрашивает повторную передачу пакета.

Состав: Станция данных(ООД) ->пункт обмена пакетами -> станция данных (ООД)

15. Предназначение и состав системы защиты ТСКП. Краткая характеристика ПАСЗИ в ТСКП

Средства защиты информации - это совокупность инженерно-технических, электрических, электронных, оптических и других устройств и приспособлений, приборов и технических систем, а также иных вещных элементов, используемых для решения различных задач по защите информации, в том числе предупреждения утечки и обеспечения безопасности защищаемой информации.

Аппаратные – различные по типу устройства, которые аппаратными средствами решают задачи защиты информации. Программные - включают программы для идентификации пользователей, контроля доступа, шифрования информации, удаления остаточной (рабочей) информации типа временных файлов, тестового контроля системы защиты и др. Примеры аппаратных ср-в: eToken.

Программные ср-ва функционируют в составе ПО, например: антивирусные программы, ср-ва управления доступом, криптографические средства. Аппаратно-программные ср-ва: системы идентификации и аутентификации, системы шифрования дисковых данных, управления ключевой информацией

16. Требования безопасности МПО ТСКП. Требования по защите системы управления МП-оборудованием от КА

Трансп сеть с комм пакет - это распределенная организационно-техническая система, предназначенная передачи и коммутации оцифрованной информации в виде частей небольшого размера — так называемых пакетов, которые передаются по сети в общем случае независимо друг от друга (дейтаграммы), либо последовательно друг за другом по виртуальным соединениям. Мультипротокольное оборудование ТСКП – может включать крипто- маршр,комм; серв упр; модемы. КМ предназначен для КЗИ при ее передаче по открытым каналам связи, пред соб спец ап-прог ср, вып ф-ии шиф-ра трафика и МЭ, кроме этого позволяет выполнить преобразование IP-адресов (NAT) внутр сети и портов (PAT) с целью сокрытия от злоумышленников их истинных значений. Треб: прм и прд IP-пак по прот TCP/IP; КЗИ IP-пак; NAT/PAT; созд и раб с защ VLAN; скр структ внутр сети; обесп фильтр; обесп резервир; оптимальность выбора маршрута; простота реализации алг марш; устойчивость к отк оборуд; содерж только стат марш. КК предн для соединения нескольких узлов внутр сети защищ поср КМ в пределах одного или нескольких сегментов сети. Треб организ VLAN; поддерж QoS; агрегир; зеркалир; сегмент траф м/д портами; контр трафика на обн петель, огр кол-ва изучаемых mac-адресов, огр входящей/исходящей скорости на портах, ф-ии списков доступа. СУ это АПК, предн для упр рес ТСКП (техн средст, ТК рес), усл ТСКП и процессами прим, техн экспл и разв ТСКП. Треб: аутентиф и удал настр оборуд; взаим по защ каналу; монитор и хран инф о сост ТСКП; получ и врем хран журн; восст инф о сост ТСКП, созд резерв копий.

17. Назначение и основные возможности системы управления ТСКП.

Система управления ТСКП - это распределенная организационно- техническая система, предназначенная для управления, в том числе автоматизированного, ресурсами ТСКП (техническими средствами, телекоммуникационными ресурсами), услугами ТСКП и процессами применения, технической эксплуатации и развития ТСКП.
Основными функциями системы управления ТСКП являются:
планирование, оперативно-техническое управление, контроль, учет и координация.
Система управления состоит из ОРГАНИЗАЦИОННОЙ и ЭКСПЛУАТАЦИОННОЙ подсистем.
Организационная подсистема управления предназначена для планирования, контроля, учета и координации, включая:
управление развитием;
координацию деятельности эксплуатирующих подразделений;
управление услугами;
планирование, распределение и учет ресурсов.
Эксплуатационная подсистема управления СКП предназначена для оперативно-технического управления СКП:
Управление функционированием технических средств, телекоммуникационных ресурсов и технологических процессов в соответствии с указаниями (распоряжениями), поступающими из организационной подсистемы управления;
управление отказами (сбоями) ТС, ТР и ТП;
контроль, сбор и обработку информации о состоянии ТС, ТР и ТП и услуг, учет их использования;
управление средствами информационной безопасности; передачу информации о функционировании в организационную подсистему управления.

18. Назначение, состав и принципы функционирования МЭ ССПТ-2

Межсетевой экран ССПТ-2 работает в режиме скрытной фильтрации и предназначен для защиты автоматизированных систем (АС), в которых обрабатывается информация различных уровней конфиденциальности. Он применяется для разделения сегментов ЛВС с целью обеспечения ЗИ от НСД посредством: 1) пакетной фильтрации на основе анализа параметров заголовков пакетов на различных уровнях ЭМВОС; 2) управления транспортными соединениями между узлами ЛВС на основе анализа параметров виртуальных соединений и запросов на их установление; 3) контроля данных прикладного уровня на основе заданных критериев и с учетом направления передачи потока пакетов.

Основной принцип функционирования заключается в применении скрытной фильтрации, позволяющий скрывать для средств удаленного сетевого мониторинга место расположения ССПТ-2. Он не изменяет параметров проходящих через него пакетов и не требует при своей установке настройки других сетевых устройств, не подвержен воздействию комп. атак, может исп. для реализ. ПБ на основе комбинации правил фильтрации, позволяет выявлять аномальные или неавторизованные воздействия. Правила фильтрации создаются для различных уровней ЭМВОС и в соответствии с правилами над пакетами могут осуществляться следующие действия: 1) «отбросить»(drop) пакет не будет передан ни на один из интерфейсов; 2) «пропустить»(accept) пакет будет передан на следующий уровень фильтрации, либо передан на фильтрующие интерфейсы в соответствии с маской выходных интерфейсов; 3) «передать»(pass) фильтрация будет завершена и пакет будет передан на фильтрующие интерфейсы в соответствии с маской;

Состав ССПТ-2: 1) подсистема администрирования (средство для настройки и управления механизмами МЭ; 2) фильтрации (осущ фильтрац трафика в соотв с правилами); 3) аутентификации (обесп идентиф и аутентиф админа при входе); 4) оповещения и аудита (для управления регистрацией в журнале безопасности событий, связанных с работой МЭ); 5) собственной защиты осуществл слежение за неизменностью контролируемых объектов с целью защиты от модификации);

19. Назначение, состав и возможности программно-аппаратного комплекса обнаружения и предупреждения КА «Форпост».

Сист. Обнаруж. Комп. атак (СОА) "Форпост" предн. для авт. выявления возд. на контр-ую данным средством автоматизир. Инф. Сист. (АИС), которые м.б. классифицированы как комп. атаки. В основе функционирования – сигнатурный метод обн-я КА(по шаблонам), обладает подсистемой собственной без-ти, позвол. шифровать передаваемую м-ду компонентами инф-ю с исп. отеч. СКЗИ, осущ. контроль целостности собств. ресурсов и ресурсов защищ. АИС и включает следующие механизмы собственной защиты:

- идентиф. и аутентиф. адм. СОА при запуске консоли адм. по имени польз-ля и паролю;
- в процессе работы осущ. контроль целостности компонентов и конфигураций СОА;
- имеется функция сигнализации адм. СОА о неверных попытках аутентификации при доступе к консоли адм., в частности, сигнализ. о 3 подряд неверных попытках аут-ии путём записи соотв. события в сист.журнал и отсылки сообщения по ЭП;

"Форпост" обеспечивает:

- обнар. КА, направленных на сервера телематических служб (WEB, FTP, электронная почта, СУБД и пр.) и рабочие станции, размещённые в контр. сегментах АИС;
- предотвр. развития сетевых КА путём блокирования ист. атак посредством отправки сетевому оборудованию (межсетевому экрану, коммутатору, маршрутизатору) по протоколам RS-232, telnet соотв. посл-ти команд на основе шаблонов;
- оповещение адм. безопасности об обнар. КА путём вывода соотв-го сообщ. на консоль адм. СОА, записи сообщения в спец. журнал, путём отправки сообщений по ЭП;
- контроль целостности собственных ресурсов СОА и ресурсов защищаемой АИС, отслеживает действия наруш-й по отношению к контролируемым ресурсам в скомпрометированной системе
- *ведение* журнала системных сообщ., содержащего служебную инф-ю, формируемую компонентами СОА, журнала сообщений от сетевого оборудования, поступающих по протоколам SNMP и syslog;
- *удалённое* упр-е сетевым обор. по защищённому, с исп. отечеств. СКЗИ, каналу;
- генерацию отчётов на основе содержимого журналов СОА;

Основные структурные элементы :1) координационный центр – обесп. перед. инф. м-ду модулями сист. и вып-ет ф-ции контроля работоспос-ти компонентов; 2) инф. фонд – предст. собой БД "IDS", работающую под управлением СУБД MS SQL 2005 и выше для хранения событий системы, хранения шаблонов датчиков и базы сигнатур СОА, вспомогательных таблиц;

САМ ФОРПОСТ ВКЛ В СЕБЯ: 1.Модули агенты – для упр-я датч., а также обеспеч. перед. инф. м-ду датч. и коорд. центром; 2.Сетевые датч. (сенсоры) – для анализа поступ. трафика на наличие компьютерных атак, используя сигнатур-й метод; 3.Серверные датчики – для сбора инфы о трафике, поступающем на сервера ИС, для блк пакетов, кот. нарушают ПБ

4.Консоль адм-ра – для управления датчиками и подключённым сетевым оборудованием и отображения информации об обнаруж. атаках. 4.Инф-й фонд - для хран-я рез-тов работы СОА и конфигурац-й инфы.

4.Модуль коорд-ции потоков инф.- для прд инф м-ду Агентами, Инф Фондом, Консолью Адм-ра, Модулем Анализа д-х

5.Модуль Анализа д-х – для обр-ки д-х, собранных сетевым датчиком для обн-я распределенных КА

20. Система обнаружения КА СОПКА и ГОССОПКА. Ведомственный центр мониторинга компьютерных атак

Указ Президента Российской Федерации от 15 января 2013 г. №31с
«О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации».

Система обнаружения компьютерных атак – это спец-ное программное или программно-аппаратное средство, выявляющее КА на ресурсы АИС посредством сбора и анализа данных о событиях, регистрируемых в системе.

НАЗНАЧЕНИЕ СИСТЕМ СОПКА - для мониторинга и ид-ции известных нарушений по доступу к инф-но-ткционным ресурсам комп.сети, и аудита (оценки безопасности) подозрительных действий, которые происходят в компьютерной системе/сети и реагирования на них.

СОСТАВ1. *Подсистема (модуль) сбора данных* предназначен для регистрации событий в системе и передачи их остальным модулям СОА. 2. *Подсистема (модуль) анализа* обрабатывает информацию полученную от модуля сбора данных. – основа методы обнаружения атак и идентифицирует факт нарушения безопасности. 3. *Подсистема (модуль) реакции* осуществляет реагирование на обнаруженные атаки и иные контролируемые события. 4. *Подсистема (модуль) хранения* данных обеспечивает хранение данных, собранных в процессе функционирования СОА/СПА.5. *Подсистема (модуль) управления* реализует политику безопасности для различных подсистем СОПКА (например, модулей сбора), получает информацию от этих комп-тов.

ВОЗМОЖНОСТИ1) С целью повышения защищенности распределенных компьютерных сетей и систем необходимо планировать комплексное использование как сетевых так и системных (хостовых) СОПКА и использование централизованного контроля.2) Сигнатурные методы более точны в определении КА имея точные данные об атаке, но пропускают неизвестные. 3) Эвристические механизмы позволяют обнаруживать неизвестные КА, но имеют некоторый уровень ошибок ложного срабатывания.4) Для положительной динамики в области обнаружения компьютерных атак необходимо правильно определить и выбрать соответствующую СОПКА на контролируемом сегменте сети.

20. Система обнаружения КА СОПКА и ГОССОПКА. Ведомственный центр мониторинга компьютерных атак

Центры мониторинга - основная организационно-техническая составляющая системы ГосСопка.

В соответствии с Концепцией Центры мониторинга являются ядром ГосСОПКА, без создания и развёртывания которых указанная система не состоится. Выписка из Концепции ГосСОПКА: «Также ведомственные центры могут создаваться и эксплуатироваться в интересах органов государственной власти организациями, осуществляющими лицензируемую деятельность в области защиты информации». Создание ЦМ и ГосСОПКА в целом предполагает активное участие предприятий промышленности, работающих в области ИБ (лицензиаты ФСБ России). Основная техническая задача: обеспечение взаимоувязанной работы СЗИ различного назначения и создание единой консоли анализа и управления для них, как ключевого элемента центра мониторинга.

Проведение мероприятий по оценке Основные задачи Центров мониторинга:

Обнаружение, предупреждение и ликвидация последствий компьютерных атак, направленных на контролируемые информационные защищенности контролируемых информационных ресурсов;

Проведение мероприятий по установлению причин компьютерных инцидентов, вызванных компьютерными атаками на контролируемые информационные ресурсы;

Сбор и анализ данных о состоянии информационной безопасности в контролируемых информационных ресурсах

Осуществление взаимодействия между Центрами

Информирование заинтересованных лиц и субъектов Системы по вопросам обнаружения, предупреждения и ликвидации последствий компьютерных атак

Функции центра ГосСопка: Инвентаризация информационных ресурсов, Выявление уязвимостей

Анализ угроз, Повышение осведомленности персонала и пользователей, Прием сообщений о возможных инцидентах, Обнаружение компьютерных атак, Анализ данных о событиях безопасности, Регистрация инцидентов, Реагирование на инциденты и ликвидация их последствий, Расследование инцидентов, Анализ результатов устранения последствий инцидентов,

ЦУ СОА: Централизованное хранение, Централизованное удалённое управление, Табличное представление зарегистрированных событий с гибкой системой фильтрации, Генерация отчетов о зарегистрированных событиях, Почтовые уведомления о зарегистрированных событиях.

В соответствии с концепцией территориальная структура ГосСОПКА имеет вид:

Российская Федерация[(Главный центр)-(Ведомственный центр 1)-(Корпоративный центр 1)]

Федеральный округ [(Региональный центр)-(Ведомственный центр 2)-(Корпоративный центр 2)]

Субъект РФ[(Территориальный центр)-(Ведомственный центр 3)-(Корпоративный центр 3)]

И все центры связаны между собой по горизонтали и по вертикали в низ!

21 Назначение, функции и особенности применения ПАК обнаружения и предупреждения КА Форпост. Варианты аппаратной основы ПАК и варианты операционных систем в ПАК для установки и функционирования программного средства Форпост.

Система обнаружения компьютерных атак «ФОРПОСТ» разработана компанией «Российские наукоемкие технологии» «РНТ» и **предназначена** для автоматического выявления воздействий на контролируемую данным средством автоматизированную информационную систему, которые идентифицируются как компьютерные атаки или вторжения, и их блокирование.

Функциональные возможности СОА «ФОРПОСТ»: обнаружение компьютерных атак; защита информационного обмена с помощью СКЗИ; предотвращение развития сетевых компьютерных атак путем блокирования источников атак; генерация отчетов на основе содержимого журналов СОА; Анализ сетевого трафика на 2-7 уровнях сетевой модели; Оповещение об обнаруженных атаках

Система обнаружения компьютерных атак «ФОРПОСТ» имеет сертификаты: ФСБ, ФСТЭК

В основу функционирования системы положен сигнатурный метод выявления атак «ФОРПОСТ» производит их анализ на соответствие указанным шаблонам атак, имеющихся в базе данных. В случае обнаружения сигнатуры в исходных данных система регистрирует факт обнаружения атаки, оповещает администратора безопасности и блокирует источник атаки

Особенности применения СОА Форпост Автоматизированные системы по классификации ФСТЭК России; Обеспечение безопасности персональных данных при их обработке в информационных системах; Защита информации в автоматизированных системах на критически важных объектах; Защита информации, не составляющей государственную тайну

ПАК имеет следующие виды исполнений:

Базовое, в котором все необходимые программные компоненты установлены в одном устройстве. Виды представлены на сайте разработчика примеры: (Форпост 20 до 100Мбит/с, Форпост 200 низкий уровень шума до 1 Гб/с, Форпост 400 высок. производит. до 7Гб/с, Фор. 2000 повышенная отказоустойчивость, производительность до 2Гб/с, Ф. 2400 повышенная отказоустойчивость, производительность до 4Гб/с Модульное, состоящее из сетевых датчиков, предназначенных для анализа трафика; центра управления, в который поступают данные с сетевых датчиков; опционального АРМ администратора

СОА «Форпост» **работает под управлением ОС** Windows XP/7, Server 2003/2008 и обладает подсистемой собственной безопасности, которая позволяет шифровать передаваемую информацию с использованием СКЗИ

22. Предназначение и структура сети RSNet. Информационные услуги сети RSNet.

Сегмент сети Интернет для ФОГВ и ОГВ субъектов РФ - совокупность территориально распределенных сетей и систем информационного обеспечения, принадлежащих организациям, имеющим гос. статус и взаимодействующих с сетью «Интернет» через узлы сети RSNET.

Назначение: предоставление эффективной информационной поддержки должностных лиц при решения задач оперативного гос. управления.

Задачи решаемые при функционировании сети RSNET:

1.обеспечение доступа пользователей сети RSNET к отечественным и зарубежным инф-м ресурсам;

2.предоставление возможности опубликования в сети Интернет информации о работе ФОГВ и органов гос. власти субъектов РФ;

3.обеспечение почтового информационного обмена пользователей сети RSNET между собой и с внешними абонентами;

4.обеспечение авторизации предоставляемой информации с использованием Удостоверяющих центров цифровых сертификатов;

Структура:

Верхний уровень (Главным узлом (8 отдел УИТО СССИ) сети RSNet и Центральным региональным узлом (УШДС СССИ) сети RSNet, которые размещены в г. Москва . Взаимодействие между этими двумя узлами осуществляется по выделенному ВОЛС)

Второй ур. (узлы в центрах федеральных округов РФ, которые подключаются к Центральному региональному узлу сети RSNet)

Третий ур. (узлы в субъектах РФ, подключаемые к соответствующим узлам в центрах федеральных округов РФ)

Пользователи: Президент; Администрация; Аппарат Правительства; Конституционный суд; ФСБ, СВР, Минобороны. Официальные домены: GOV.RU, KREMLIN.RU Почтовые серверы: mail.gov.ru Физическая структура: блока публичных IP сетей класса “C”; IP сетей класса “A”, “B” и “C”, выделенных для организации приватных сетей (более 16 млн. IP адресов) из блока немаршрутизируемых в Интернет IP сетей. Информационные услуги: Электронная почта (qmail - агент пересылки почты Интернет для UNIX-like операционных систем); Сервис обработки нежелательных почтовых сообщений (SPAM) (Сервис реализован с помощью ПО Mailscanner. MailScanner - это почтовый вирусный сканер, защитная программа и маркировщик спама); Сканирование на вирусы почты (Qmail-Scanner, средство для сканирования содержимого сообщений для qmail); WEB-хостинг (Для предоставления сервиса виртуального хостинга используется web-сервер Apache); Сервис хранения информации (FTP) (Сервис хранения и доступа к информации базируется на протоколе FTP, позволяющем организовать обмен файлами между пользователями системы используя общий системный ресурс – сервер FTP); Сервис аутентификации и авторизации пользователей (AAA) (Сервис AAA реализуется на базе протоколов RADIUS. AAA-сервер предназначен для обработки запросов на аутентификацию удаленных пользователей, администраторов и операторов изделия, а также ведения базы данных пользователей); Сервер NTP (сетевой протокол задания времени служит для осуществления синхронизации работы различных процессов в серверах и программах клиента); Сервис DNS (DNS сервис реализуется ПО Bind. BIND - пакет программного обеспечения для поддержки DNS)

23. Предназначение и состав центральных узлов. Предназначение и состав узлов 1 и 2. Предназначение абонентских узлов.

Сеть RSNet имеет иерархическую структуру, соответствующую административно-территориальному делению Российской Федерации, состоящую из трех уровней:

Верхний уровень иерархии реализуется двумя центрами управления: Главный центр управления сетью (Главный узел сети RSNET, эксплуатируется 8 отдел УИТО СССИ ФСО России) и Центральный узел регионального сегмента (Центральный региональный узел сети RSNET, эксплуатируется УШДС СССИ ФСО России). Взаимодействие между узлами сети RSNet осуществляется в основном на базе инфраструктуры виртуальных сетей и каналов связи, арендуемой у национальных операторов связи.

Второй уровень образуют узлы в центрах федеральных округов Российской Федерации, которые подключаются к Центральному региональному узлу сети RSNet.

Третий уровень образуют узлы в субъектах Российской Федерации, подключаемые к соответствующим узлам в центрах федеральных округов Российской Федерации.

Оборудование узлов представлено тремя группами: Телекоммуникационное оборудование на базе маршрутизаторов Cisco 7600, по схеме двойного резервирования; Сервера и рабочие станции. В качестве серверов используются оборудование (ETegro Therascale, DEPO, HP, KraftWay); Система безопасности.

Приказ ФСО России от 06.10.2006 № 458/дсп. «Инструкция об организации, эксплуатации и обеспечении информационной безопасности абонентских пунктов сети "Интернет" в подразделениях федеральных органов государственной охраны». Инструкция определяет порядок организации абонентских пунктов (АП) при включении их в состав средств международного информационного обмена, в подразделениях органов государственной охраны и основные требования по обеспечению информационной безопасности при их эксплуатации.

Защищённый абонентский пункт «Обруч-АП-2» Назначение для подключения к информационно-телекоммуникационным сетям, позволяющим осуществлять передачу информации через государственную границу Российской Федерации, в том числе к международной компьютерной сети «Интернет». Защита сведений, составляющих государственную тайну, служебной информации ограниченного распространения, конфиденциальной информации, персональных данных.

Изделие «Узел» предназначено для организ-и эффект. и безопасного информа-о-коммуник-го взаимодействия пользователей с информац-и ресурсами сообщества сетей Интернет и сетью RSNET, предостав-я перспективных информац-ых и телекоммуникац-х услуг, а также публикации в сети Интернет официальных материалов органов государственной власти Российской Федерации.

23. Предназначение и состав центральных узлов. Предназначение и состав узлов 1 и 2. Предназначение абонентских узлов(продолж)

Регион-ый сегмент сети RSNET, строится на базе Изделий «Узел-1» и «Узел-2». К каждому Изделию «Узел-1» присоед-ся не менее 10 Изделий «Программно-технический комплекс узла сети RSNET второго типа» («Узел-2»).

Взаимодействие узлов осуществляется по выделенным арендованным, либо собственным каналам связи, или путем использования услуги IP VPN предоставляемой операторами дальней связи.

Оборудование узлов представлено тремя группами:

1. **Телекоммуникационное оборудование;**
2. **Сервера и рабочие станции.;**
3. **Система безопасности.**

Назначение и состав подсистем:

1. **Телекоммуникационная подсистема-обесп-е передачи данных и межсетевое взаим-ие конечных устр.**
2. **Подсистема информационной безопасности- мониторинг системных и сетевых ресурсов, анализ полученной информации и своевременное уведомление администраторов об обнаружении попыток несанкционированного сетевого доступа и активности**
3. **Подсистема служебных сервисов- решение вспомогат.ельных сетевых функций, оптимизация сетевых процессов и ведение базы данных абонентов.**
4. **Подсистема телематических служб- обеспечить основу для построения безопасного, информационно-сервисного портала ОГВ, возможность размещения не менее 10 виртуальных Web-серверов**
5. **Подсистема управления- контроль состояния оборудования и сетевых приложений, производительности и использования ресурсов.**

24. Структура подсистемы безопасности. Средства защиты узлов RSNet. Краткая характеристика программно-аппаратных СЗИ в RSNet.

Оборудование узлов представлено тремя группами:

1.Телекоммуникационное оборудование на базе маршрутизаторов Cisco, по схеме двойного резерв-я;

Cisco 7600 — семейство шасси для организации ядра сети. Устройство модульное, может быть дополнено различными платами расширения.

2.Сервера и рабочие станции. В качестве серверов используются оборудование (ETegro Therascale, DEPO, HP, KraftWay);

3.Система безопасности.

Информационная безопасность :

-МЭ(Check Point Power-1, StoneGate Firewall);
-средств анти- DDoS (Аппаратно-программный комплекс «Периметр»);
-систем обнаруж и предотвр. компьютерных атак;
-антивирусных средств;
-систем сбора, анализа и корреляции событий ИБ;
-защита сайтов с помощью Trustwave Web Application Firewall ;
-задействования встроенных механизмов защиты сетевого оборудования и серверных операционных систем;
-применения безопасных профилей конфигурации оборудования;
-использования организационных мер

Структура подсистемы безопасности