

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«ПЕНЗЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Политехнический институт
Факультет приборостроения,
информационных технологий и
электроники

Кафедра
«Информационная безопасность
систем и технологий»

Специальность 100502 –

Специализация -

Информационная безопасность
телекоммуникационных систем
Разработка защищенных
телекоммуникационных систем

ДИПЛОМНАЯ РАБОТА

на тему

ЗАЩИЩЕННАЯ СЕТЬ ПЕРЕДАЧИ ДАННЫХ РАСПРЕДЕЛЕННОЙ
ИНФОРМАЦИОННОЙ СИСТЕМЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

Студент _____ Бербечук Р.А.

Руководитель _____ Мещеряков А.А.

Нормоконтролёр _____ Иванов А.П.

Рецензент главный специалист лаборатории
обнаружения НИКИРЭТ- филиал ФГУП ФНИИЦ

ПО «Старт» им. М.В Проценко _____ Иванов В.Э

Работа допущена к защите (протокол заседания кафедры от _____ № _____)

Заведующий кафедрой _____ С.Л. Зефилов

Работа защищена с отметкой _____ (протокол заседания ГЭК
от _____ № _____)

Секретарь ГЭК _____ А.Г. Фатеев

Пенза 2017

РЕФЕРАТ

Отчет содержит 145 с., 32 рис., 13 табл., 7 источников, 5 прил.

ИНФОРМАЦИОННАЯ СИСТЕМА ПЕРСОНАЛЬНЫХ ДАННЫХ,
МЕЖСЕТЕВОЙ ЭКРАН, ПЕРСОНАЛЬНЫЕ ДАННЫЕ, СЕТЬ ПЕРЕДАЧИ
ДАННЫХ, КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА.

Объектом исследования является сеть передачи данных распределенной информационной системы персональных данных (ИСПДн).

Цель работы – разработка защищенной сети передачи данных распределенной информационной системы персональных данных.

В процессе выполнения работы, была создана сеть передачи данных распределенной ИСПДн, которая состоит из 26 объектов. На каждом из объектов имеются средства криптографической защиты информации (СКЗИ), благодаря которым сохраняется безопасность информации. На каждом объекте есть по два криптошлюза, два межсетевых экрана и на двух объектах, в которых есть выход в интернет, есть средство обнаружения вторжений.

В работе представлены настройки СКЗИ для работы в сети с двумя поставщиками услуг и двадцати шестью объектами:

- настройки коммутатора для работы с двумя криптошлюзами и двумя поставщиками услуг;
- настройка криптошлюзов на шифрование трафика в режиме горячего резервирования;
- настройка межсетевого экрана на работу на определенных портах.

СОДЕРЖАНИЕ

Введение.....	9
1 Требования и состав на создание распределенной информационной системы персональных данных	11
2 Структура сети передачи информации в распределенной информационной системе персональных данных	19
2.1 Структурная схема ИСПДн.....	19
2.2 Информационные потоки распределенной ИСПДн.....	21
3 Расчет требуемой пропускной способности.....	23
3.1 Расчет пропускной способности каналов связи системы СКД.....	23
3.2 Требования к задержке	23
4 Требования к сети передачи данных	24
4.1 Основные требования к сети передачи данных:	24
4.2 Описание услуг.....	25
4.3 Доступ в Интернет	27
4.4 Технические параметры	27
4.5 Сроки предоставления Услуг.....	28
4.6 Зоны ответственности.....	28
4.7 Доступность Услуг.....	29
4.8 Выделение IP-адресов пользователю.....	30
4.9 Требования к службе технической поддержки поставщика услуг	30
4.10 Сертификация.....	31
Полный перечень услуг для каждого объекта приведен в приложении Г...	31
5 Разработка схемы подключения объектов информатизации ИСПДн к сети передачи данных.....	32
5.1 Схема организации СКД	32
5.2 Схема организации сети спортивного объекта.....	37
5.3 Схема организации сети ЦОД и ЦУТП	39
6 Анализ рынка средств защиты информации для обеспечения защищенности сети передачи данных	41

6.1 Системы обнаружения и предотвращения вторжений.	41
6.1.1 Форпост.....	43
6.1.2 ViPNet IDS	44
6.2 Межсетевые экраны.....	46
6.2.1 ССПТ 2.....	48
6.2.2 Cisco ASA	50
6.3 Средство криптографической защиты информации	50
6.3.1 ViPNet.....	52
6.3.2 Континент-АП.....	53
6.4 Результаты анализа	54
7 Межсетевой экран ССПТ-2.....	56
7.1 Общие сведения	56
7.2 Основные функциональные характеристики	58
7.3 Применение правил фильтрации для ССПТ-2 для данной ИСПДн	59
8 Криптошлюз VIPNet Coordinator HW1000.....	68
8.1 Общие сведения	68
8.2 Работа и настройка криптошлюза VIPNet Coordinator HW1000.....	70
9 Коммутатор Cisco 2960	71
9.1 Общие сведения	71
9.2 Работа и настройка коммутатора Cisco 2960	71
10 Разработка организационных требований.....	73
10.1 Организационные требования к СКЗИ	73
10.2 Организационные требования к ИСПДн	79
11 Разработка технических требований.....	81
11.1 Требования к активному сетевому оборудованию.....	81
11.2 Общие требования к структурированной кабельной системе	85
11.3 Требования к элементу структурированной кабельной системе	87
11.4 Подсистема администрирования.....	92
11.5 Подсистема электропитания рабочих мест.....	93
11.6 Тестирование параметров СКС	93

11.7 Требования к документации по проектируемым системам	93
12 Расположение оборудования в стойке	95
13 Руководство администратора ИБ для сети передачи данных	98
13.1 В состав средств защиты информации входят:.....	98
13.2 Функции администратора безопасности информации.....	100
13.3 Применяемые средства защиты информации	103
13.4 Обязательные организационно-технические меры	104
13.5 Управление средствами криптографической защиты информации от НСД в каналах связи	105
13.6 Управление средствами защиты информации от НСД на периметре объектов	106
13.7 Порядок действий администратора безопасности при установке программного обеспечения	107
13.8 Порядок работы с печатными документами и внешними машинными носителями информации	108
13.9 Действия в случае обнаружения угроз безопасности информации....	108
Заключение.....	111
Список использованных источников	112
Приложение А.....	113
Приложение Б	123
Приложение В.....	130
Приложение Г	133
Приложение Д.....	144

ОПРЕДЕЛЕНИЯ

Автоматизированное рабочее место - комплекс программно-технических средств, используемый для подготовки и ввода в систему в электронном виде информации, а также для организации регламентированного доступа пользователей к информации, содержащейся в системе. [1]

Автоматизированная система - система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций[1].

Доступ к информации - возможность получения информации и ее использования. [2]

Защищаемая информация - информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации. [2]

Информационная система персональных данных - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств. [1]

Класс защищенности - определенная совокупность требований по защите от несанкционированного доступа к информации. [5]

Контролируемая зона - пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств. [1]

Система обнаружения вторжений - программное или аппаратное средство, предназначенное для выявления фактов неавторизованного доступа в компьютерную систему или сеть либо несанкционированного управления ими в основном через интернет. [4]

Межсетевой экран — локальное (однокомпонентное) или функционально-распределенное средство (комплекс), реализующее контроль

за информацией, поступающей в АС и/или выходящей из АС, и обеспечивает защиту АС посредством фильтрации информации, т.е. ее анализа по совокупности критериев и принятия решения о ее распространении в (из) АС. [3]

Общедоступные персональные данные - персональные данные доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных либо по его просьбе. [1]

Персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных). [1]

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

FTP – File Transfer Protocol, протокол передачи файлов

VLAN –Virtual Local Area Network — логическая («виртуальная») локальная компьютерная сеть;

VPN – Virtual Private Network, виртуальная частная сеть;

Wi-Fi – Wireless Fidelity, семейство стандартов передачи цифровых потоков данных по радиоканалам;

АРМ – автоматизированное рабочее место;

ИСПДн – информационная система персональных данных;

КПП – контрольно-пропускной пункт;

ЛВС – локальная вычислительная сеть;

МЭ – межсетевой экран;

НСД – несанкционированный доступ;

ПДн – персональные данные;

ПО – программное обеспечение;

ПТС – программно-технические средства;

СКЗИ – средство вычислительной техники;

СЗИ – средство защиты информации;

СОВ – система обнаружения вторжений;

СУБД – система управления базами данных;

ТТЗ – тактико-техническое задание;

ФСТЭК – Федеральная служба по техническому и экспортному контролю;

ЦОД – центр обработки данных;

ЦУТП – центр управления технической поддержки;

ПЭМИН – побочные электромагнитные излучения и наводки.

ВВЕДЕНИЕ

В современном мире огромное количество информации передают по различным сетям, а информация, как известно, представляет собой большую ценность. Особенную ценность имеет конфиденциальная и секретная информация. Для защиты информации необходимо проводить деятельность по предотвращению хищения, модификации, утраты и её утечки. Злоумышленники могут пытаться заполучить важную информацию различными способами для того, чтобы совершить различного рода незаконные действия с выгодой для них. Например, если злоумышленник заполучит информацию, содержащую военную тайну, то он может продать её другой стране, заинтересованной получении этих сведений, при получении информации составляющей коммерческую тайну, злоумышленник может продать конкурентам, при получении ПДн, например номер телефона, по которому и т.д.

На различных спортивных соревнованиях тоже создаются сети передачи данных, в которых передаются и обрабатываются ПДн. Как и конфиденциальные данные, так и ПДн данные необходимо защищать от несанкционированных и непреднамеренных воздействий. Так как спортивные соревнования могут проводиться в разных городах, то нужно разворачивать большую сеть, содержащую ИСПДн.

Для работы сети передачи данных необходимо обеспечить бесперебойную передачу всей информации ко всем объектам сети, а так же обеспечить защиту передаваемой информации, включая ПДн. И для защиты обрабатываемой и передаваемой в ней информации надо использовать определенные средства и меры защиты информации.

Особую опасность представляет собой передачу данных за пределы контролируемой зоны, так как в контролируемой зоне угрозы хищения, модификации, утраты и утечки информации значительно меньше. Для защиты информации за пределами контролируемой зоны нужно использовать особые средства.

Одним из средств защиты ПДн является криптография. Средства криптографии позволяют шифровать проходящий через них трафик по определенным алгоритмам и обеспечить защиту передаваемых данных от одного объекта к другому.

Так же есть и другие средства защиты информации, про которые подробно описано в данной работе, а так же приведены варианты настройки.

1 Требования и состав на создание распределенной информационной системы персональных данных

ИСПДн реализована как территориально распределенная информационная система, включающая в свой состав оборудование точек доступа, автоматизированные рабочие места, серверное оборудование и средства защиты информации. Изделия, входящие в данную систему:

- центральный сервер базы данных (ЦСБД);
- объектовый сервер базы данных (ОСБД);
- сервер связи (СС);
- АРМ объединенного пункта безопасности (АРМ–ОПБ);
- АРМ технического обеспечения (АРМ–ТО);
- АРМ администратора (АРМ-А);
- АРМ бюро пропусков (АРМ–БП);
- блок считывателей управляющий универсальный (БСУУ);
- блок мониторный (БМ);
- стойка мониторная (СМ);
- мобильный терминал (МТ);
- оборудование дистанционного считывания RFID идентификаторов (ОДС);
- система обнаружения вторжения (и/или сетевой датчик);
- сервер безопасности (СБ);
- АРМ администратора безопасности (АРМ-АБ);
- АРМ управления криптосетью (АРМ-УК);
- СЗИ от НСД;
- средства криптографической защиты информации (СКЗИ);
- сетевое оборудование.

В состав системы входят следующие основные объекты информатизации:

- центр обработки данных (ЦОД) ИСПДн;

- центр управления и технической поддержки (ЦУТП);
- спортивные объекты;
- ЦОД внешних систем (шлюз взаимодействия с внешними системами).

Пользователями ИСПДн являются:

- сотрудники объединенного пункта безопасности (ОПБ) спортивного объекта;
- системные администраторы;
- администраторы баз данных;
- администраторы безопасности;
- эксплуатационно-технический персонал.

Функции пользователей обеспечиваются соответствующим набором программно-технических средств (ПТС), объединенных локальными сетями на объектах.

Объектом информатизации ИСПДн является совокупность информационных ресурсов, ПТС и локальной сети, используемых в соответствии с заданной информационной технологией.

Границы ИСПДн и перечень объектов информатизации определяются местами дислокации пользователей, которые расположены на следующих объектах:

- спортивные объекты;
- ЦОД внешних систем;
- ЦОД ИСПДн;
- ЦУТП ИСПДн.

Телекоммуникационное взаимодействие объектов информатизации ИСПДн реализовано через развертываемую защищенную сеть VPN с использованием СКЗИ, функционирующую через мультисервисную сеть связи (МСС) провайдера связи на базе технологии MPLS VPN L3 (топологии «Каждый с каждым»). При этом осуществлено подключение объектов

информатизации ИСПДн к основному и резервному (при наличии) узлам доступа МСС с поддержкой статической и динамической маршрутизации.

В связи с большой территориальной удаленностью спортивных объектов друг от друга и от ЦОД ИСПДн, а также в связи с необходимостью обеспечения автономного функционирования каждого спортивного объекта, на каждом спортивном объекте размещено криптооборудование.

Топология информационной сети радиально-узловая, в ней основными узлами является ЦСБД и резервный ЦСБД, расположенный в ЦУТП, обеспечивающие информационный обмен по каналам связи со всеми ОСБД и внешними системами.

Каждый ОСБД подключается к ЦОД ИСПДн для репликации данных, централизованного управления ИСПДн, принятия внутриведомственных и межведомственных организационных решений, организации мониторинга системы в целом и проведения работ по технической поддержке

Спортивный объект оснащен оборудованием, приведенным в таблице 1. Оборудование каждого объекта должно подразделяться на стационарное (размещаемое в серверных помещениях), дополнительное оборудование (АРМ, коммутационное и каналообразующее оборудование) и периферийное (точки доступа).

Таблица 1 – Оборудование объекта

Наименование составной части	Назначение
Объектовый сервер баз данных	<p>Контроллер домена из состава ОСБД:</p> <p>Внутрисетевое взаимодействие рабочих станций и серверов. Разграничение прав доступа пользователей к АРМ, серверам и БД. Администрирование учетных записей пользователей и машин. Выполнение Обеспечение сервисных функций по управлению ролью отказоустойчивого кластера, систем мониторинга, а также участие в обновлении систем и служб на АРМ и серверах.</p> <p>Кластер БД из состава ОСБД:</p> <p>Хранение и обработка информации поступающей от оконечного оборудования, информации, поступающей из центрального сервера баз данных, обработка поступающих запросов от АРМ спортивного объекта, формирование и отправка ответов на запросы; архивирование и хранение архивов ОСБД, выгрузка данных в систему управления соревнованиями.</p>
Сервер безопасности	Хранение файлов конфигурации и архивов событий, вывод на печать информации о событиях связанных с СЗИ
АРМ–ОПБ	Формирование запросов к объектовому и центральному кластеру БД ИСПДН, обработка полученных ответов.
АРМ–ТО	<p>Обновление файлов периферийного оборудования.</p> <p>Хранение архивных копий СПО. Управление</p> <p>Конфигурирование периферийного оборудования.</p> <p>Отображение информации о состоянии периферийного оборудования в режиме реального времени.</p>

Продолжение таблицы 1

Наименование составной части	Назначение
АРМ Администратора	Обновление систем. Мониторинг состояния и удаленное управление парком серверов, системы хранения данных (СХД). Администрирование домена, VM, DNS, отказоустойчивых кластеров.
АРМ–БП	Учет и выпуск пропускных документов, удовлетворяющих требованиям ИСПДН в период действия режима «Наследие». Контроль пропускных документов, их активация или отмена. Поиск зарегистрированных пропускных документов в базе данных.

Периферийное оборудование предназначено для организации точек доступа следующих типов:

- БСУУ (для считывания идентификаторов, управления исполнительным устройством (турникетами)), БМ (для отображения информации об абоненте) для организации входа и/или выхода сотрудников;

- БСУУ (для идентификаторов, управления исполнительным устройством (турникетами)), БМ (для отображения информации об абоненте) для организации входа и/или выхода зрителей;

- мобильный беспроводной ручной терминал, реализующий функции сканирования идентификаторов и отображение фотографии абонента на дисплее. Мобильный терминал должен обеспечивать обслуживание абонентов на транспортном КПП и у калиток на КПП. Передача данных мобильным терминалом должна осуществляться по стандарту Wi-Fi IEEE 802.11 a/b/g;

- ОДС, обеспечивающее автоматическое сканирование идентификаторов, встроенных в пропускные документы абонентов. ОДС должен использоваться для дистанционного считывания кодов идентификаторов пропускных документов при свободном выходе абонентов

с объекта. ОДС должен подключается к ЛВС спортивного объекта ИСПДн и обеспечивать передачу сообщений о фактах регистрации кодов идентификаторов в базу данных ОСБД как события доступа.

В состав объекта информатизации ЦОД входят:

- ЦСБД;
- сервер связи;
- сервер безопасности;
- СКЗИ (класс защиты не ниже КС2);
- средства обнаружения компьютерных атак/вторжений и/или сетевой датчик (при необходимости);
- сетевое оборудование для организации ЛВС;
- средства бесперебойного питания;
- средства комплексирования (стойка, патч-панели, кабели, переходники, преобразователи и т.п.);
- линии связи между маршрутизатором (коммутатором) и узлами доступа (основным и, при наличии, резервным) МСС провайдера связи на объектах.

В состав объекта информатизации ЦУТП входят:

- ЦСБД (резервирование);
- сервер безопасности;
- АРМ администратора;
- АРМ администратора безопасности;
- АРМ управления криптосетью;
- АРМы технического обеспечения;
- АРМы ОПБ;
- СКЗИ (класс защиты не ниже КС2);
- межсетевые экраны;
- средства обнаружения компьютерных атак/вторжений и/или сетевые датчики (при необходимости);

- сетевое оборудование для организации ЛВС;
- средства бесперебойного питания;
- средства комплексирования (стойка, патч-панели, кабели, переходники, преобразователи и т.п.);
- линии связи между маршрутизатором (коммутатором) и узлами доступа (основным и, при наличии, резервным) МСС провайдера связи на объектах.

В состав типового объекта информатизации – спортивного объекта входят:

- ОСБД;
- сервер безопасности;
- АРМ администратора системы;
- АРМ администратора безопасности;
- АРМы технического обеспечения;
- АРМы ОПБ;
- СКЗИ (класс защиты не ниже КС2);
- сетевое оборудование для организации ЛВС;
- СЗИ;
- средства бесперебойного питания;
- средства комплексирования (стойка, патч-панели, кабели, переходники, преобразователи и т.п.);
- мобильные терминалы;
- БСУУ;
- блоки мониторные;
- ОДС;
- оборудование для организации беспроводного доступа к ЛВС;
- линии связи между маршрутизатором (коммутатором) и узлами доступа (основным и, при наличии, резервным) МСС провайдера связи на объектах.

В состав типового объекта информатизации – шлюза взаимодействия с внешними системами входят:

- СКЗИ (класс защиты не ниже КС2);
- сетевое оборудование для организации ЛВС;
- средства бесперебойного питания;
- средства комплексирования (стойка, патч-панели, кабели, переходники, преобразователи и т.п.);
- линии связи между маршрутизатором (коммутатором) СЕ и узлами доступа (основным и, при наличии, резервным) МСС провайдера связи на объектах.

Криптографическая защита ПДн в ИСПДн при их передаче по каналам связи, не защищенным организационно-техническими мерами, осуществляется с использованием СКЗИ, сертифицированных в системе сертификации РОСС RU.0001.030001 на соответствие требованиям ФСБ России по классу защищенности не ниже КС2.

СКЗИ подключается на объектах ИСПДн в режиме «горячего» резервирования.

2 Структура сети передачи информации в распределенной информационной системе персональных данных

2.1 Структурная схема ИСПДн

В процессе выполнения работы была разработана структурная схема ИСПДн, представленная на рисунке 1.

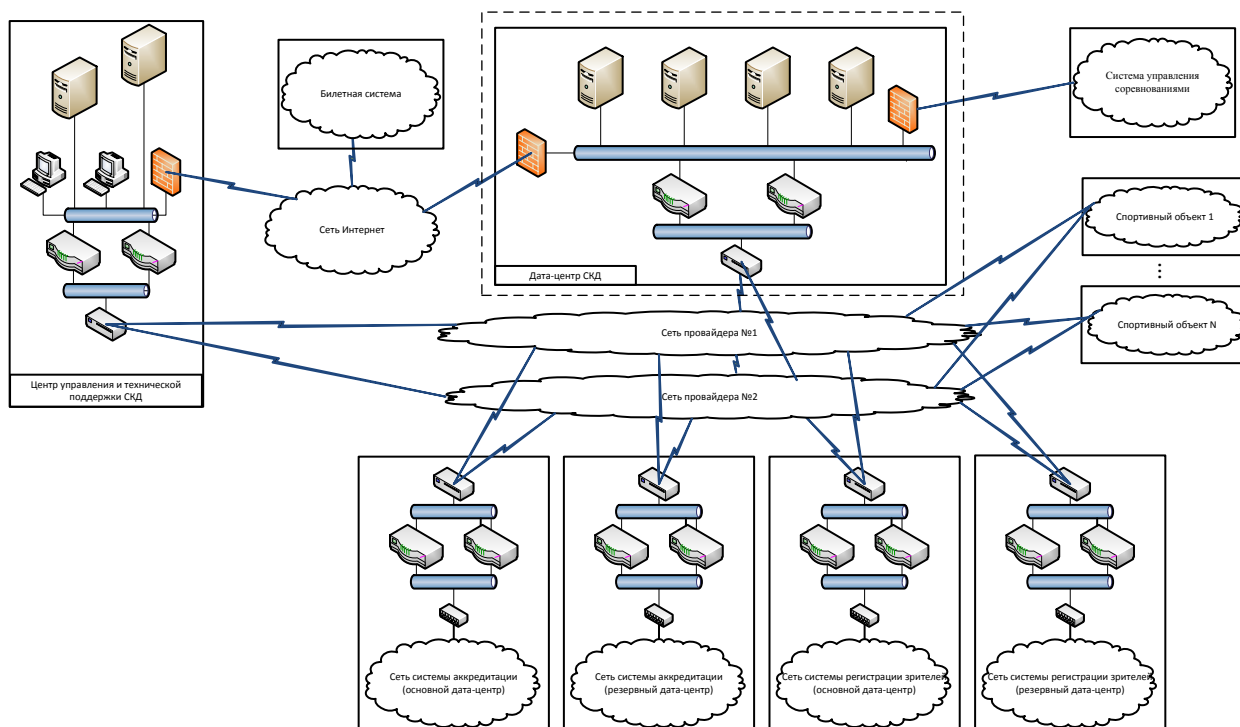


Рисунок 1 – Схема ИСПДн

ИСПДн является распределенной и состоит из следующих структурных единиц:

- дата-центр;
- система управления соревнованиями;
- центр управления и технической поддержки распределенной ИСПДн;

- спортивный объект;
- билетная система;
- сеть системы аккредитации
- система идентификации болельщиков.

В свою очередь дата-центр состоит из:

- ЦСБД;

- сервер связи;
- сервер безопасности;
- резервный сервер.

Центр управления и технической поддержки ИСПДн состоит из:

- ЦСБД (резервирование);
- сервер безопасности;
- сеть системы управления спортивным объектом.

Спортивный объект состоит из:

- помещение СБ;
- помещение ТП;
- серверная спортивного объекта;
- КПП №[1-N].

2.2 Информационные потоки распределенной ИСПДн

Была разработана схема информационных потоков, которая представлена на рисунке 2.

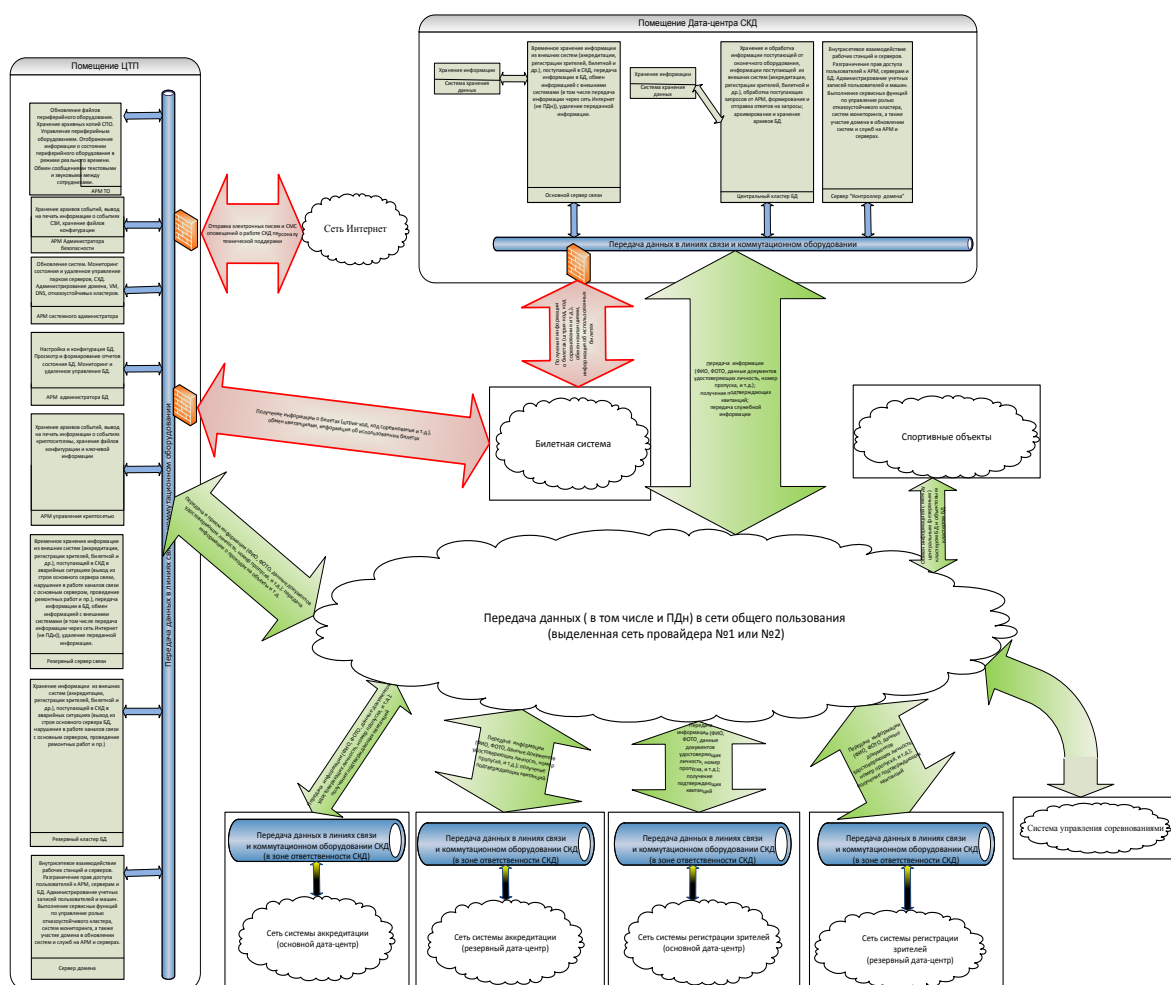


Рисунок 2 – Схема информационных потоков

С учетом того, что ИСПДн представляет собой, построенную территориально на базе распределенных, объединенных в единую логическую сеть, локальных объектов, построенные на базе ЛВС и с учетом циркулирующей информации, относительно сети передачи данных, можно выделить сегменты: локальная сеть передачи данных, доступ в интернет и сети на базе VPN L3, предоставляемыми поставщиками услуг, основным и резервным.

Из схемы, представленной на рисунке 2 видно, что информация подлежащая защите циркулирует в управляющем сегменте локальных вычислительных сетях объектов, и информация в сети передачи данных VPN

L3. Так же необходимо обеспечить защиту от вторжений из сети общего доступа, т.е. интернета.

ЛВС управляющего сегмента спортивного объекта территориально расположено в двух помещениях, которые находится на контролируемой зоны и доступ к ним запрещен, а значит, криптографической защиты информации в управляющем сегменте не подлежит. Линии связи, идущие к периферийному оборудованию, разделены МЭ. Для защиты от проникновения используется МЭ и COB.

Доступ в интернет используется для получения информации или отправки сообщения, не подлежащие защите, поэтому необходимо защитить подключение к интернету от вторжений, для этого необходимо установить систему обнаружений вторжений.

Общедоступные сети поставщика услуг, на базе которых организовывается распределенная сеть, используется для передачи и служебной информации и ПДн, как между объектами ЦОД, так и при взаимодействии с внешними системами. Эти сегменты сети подлежат защите меж сетевым экраном от вторжений и КЗИ.

3 Расчет требуемой пропускной способности

3.1 Расчет пропускной способности каналов связи системы СКД

Суммарный трафик сети передачи данных СКД (СПД СКД) на объектах, в момент пиковой нагрузки (МПН), рассчитывается по формуле

$$T_{\text{СКД}} = ((N_{\text{КА}} * V_{\text{КА}}) + (N_{\text{КРЗ}} * V_{\text{КРЗ}})) * X_{\text{КШ}} * N_{\text{П}},$$

где:

$T_{\text{СКД}}$ — суммарный трафик СПД СКД на объекте;

$N_{\text{КА}}$ — количество карт аккредитации, передаваемых в секунду в МПН (до 100);

$V_{\text{КА}}$ — объем сообщения одной карты аккредитации (до 720 Кб);

$N_{\text{КРЗ}}$ — количество карт идентификации болельщиков, передаваемых в секунду в МПН (до 120);

$V_{\text{КРЗ}}$ — объем сообщения одной карты регистрации зрителя (до 640 Кб);

$X_{\text{КШ}}$ — поправочный коэффициент аппаратно-программных средств защиты.

$N_{\text{П}}$ — количество потребителей;

$$T_{\text{СКД}} = ((100 * 720 \text{ Кб}) + (120 * 640 \text{ Кб})) * 2,5 * 12 = 34,875 \text{ Мб/с}$$

3.2 Требования к задержке

Для обеспечения необходимого уровня качества функционирования сервисов СКД, уровень задержки не должен превышать 30 мс.

Требования по полосе пропускания СПД СКД для оснащаемых объектов составляет 60 Мбит/с.

4 Требования к сети передачи данных

4.1 Основные требования к сети передачи данных:

Сеть передачи данных организуется с целью обеспечения производственных процессов и процессов оперативного управления СКД и должны включать в себя:

- услуги по предоставлению виртуальной частной сети третьего уровня - L3 VPN;

- услуги по предоставлению доступа к сети интернет.

Услуги оказываются в местах установки компонентов СКД.

Сеть передачи данных должна обеспечивать:

- доступ в точке нахождения оконечного оборудования поставщиков услуг. При необходимости обеспечивать доступ к сети передачи данных с использованием линий связи, предоставленным объектом;

- при получении доступа в интернет, к выделенным каналам и к услугам передачи данных должны использоваться отдельные линии доступа, проходящие по независимым физическим маршрутам, то есть не имеющие общих точек отказа;

- оборудование, с помощью которого оказываются услуги связи, должно иметь сертификат соответствия для применения на сетях связи Российской Федерации и быть совместимым с оборудованием, используемым на объектах;

- сеть передачи данных должна иметь разрешение в соответствии с законодательством Российской Федерации и нормативными документами органа, регулирующего деятельность в отрасли связи на территории Российской Федерации;

- срок организации связи (подключение) абонентов, отдельного пункта или локальной территории, не более 60 календарных дней, с момента подписания

4.2 Описание услуг

Услуги связи по передаче данных обеспечивают:

- доступ к сети связи;
- соединение по сети передачи данных с использованием оконечного оборудования поставщиков услуг;

Доступ к сети связи может осуществляться с использованием ЛКС и оконечного оборудования, как оборудованию, принадлежащему поставщику услуг, так и собственным оборудованием.

Присоединение к сетям передачи данных, в том числе и других операторов и узлам телематических служб должно осуществляться с использованием шлюзов поставщика услуг. Поставщик услуг принимает все возможные меры для обеспечения надежности и живучести присоединений, необходимого резервирования, достаточной пропускной способности.

Оказание услуги «Виртуальная частная сеть третьего уровня (L3-VPN)» заключается в объединении территориально распределенных локальных сетей и сегментов сетей в единую полносвязанную корпоративную сеть для обмена данными посредством маршрутизации пакетов данных. Услуга организуется на 3-ем уровне модели межсетевого взаимодействия (OSI) на базе пакетной сети передачи данных оператора, построенной по технологии многопротокольной коммутации с использованием меток (Multiprotocol label switching - MPLS).

Виртуальная частная сеть третьего уровня должна представлять собой услугу распределенного маршрутизатора, позволяющего работать друг с другом, используя протокол TCP/IP, при этом обеспечивая логическую связь по схеме «каждый с каждым». Для каждого территориального объекта выделяется своя подсеть IP-адресов, которую необходимо согласовать с поставщиком услуг. Поставщик услуг должен предоставлять возможность подключаться оборудованию НИКИРЭТ к IP VPN, используя статическую или динамическую маршрутизацию. В качестве протоколов динамической маршрутизации на оборудовании поставщика услуг должны поддерживаться

протоколы OSPF и BGP. Любое изменение конфигурации локальных сетей (изменение IP-адресов, настройка статической или динамической маршрутизации) должно согласовываться с поставщиком услуг.

Услуга должна состоять из двух компонентов:

- организация и поддержка виртуальной частной сети третьего уровня;
- организация и поддержка канала доступа к виртуальной частной сети третьего уровня (далее канал доступа к L3 VPN).

Под организацией и поддержкой виртуальной частной сети третьего уровня подразумевается выделение ресурса сети передачи данных поставщика услуг для обеспечения маршрутизации пакетов данных между объектами.

Для каналов доступа к L3 VPN должны использоваться отдельные порты на оконечном оборудовании поставщика услуг. При организации на одном объекте канала доступа к IP VPN совместно с другими услугами передачи данных поставщика услуг (доступ в Интернет) может быть предоставлен один транковый порт Ethernet 802.1Q (с поддержкой VLAN). В этом случае каждой услуге будет соответствовать определенный номер VLAN (VLAN ID) в физическом стыке.

Услуга виртуальных сетей дополнительно определяется совокупностью точек терминирования услуги, скоростями передачи информации и качеством обслуживания в каждой из точек терминирования. В том случае, если по адресу предоставления услуги предоставляется несколько услуг, необходимо предоставить единый транковый порт Ethernet с поддержкой 802.1Q, при этом необходимо согласовать конфигурацию VLAN. При предоставлении услуг L3VPN конфигурирование услуг осуществляется средствами BGP и OSPF. По требованию, поставщик услуг обязан установить оконечное оборудование для обеспечения возможности предоставления услуг по индивидуальным портам.

Услуга виртуального выделенного канала связи должна включать в себя организацию и предоставление основного и резервного канала связи.

Услуга должна обеспечивать возможность пропуска по сети любых типов данных, в том числе и зашифрованных. Поэтому, максимальный размер полезного блока данных одного пакета, который может быть передан протоколом без фрагментации (IP MTU) – не менее 1548 байт.

4.3 Доступ в Интернет

Оказание услуги «Доступ в Интернет» заключается в предоставлении высокоскоростного доступа в глобальную сеть интернет без ограничения объема трафика.

В рамках оказания услуги «Доступ в Интернет» поставщик услуг должен представлять следующий пакет дополнительных услуг:

- выделение и маршрутизация до пяти постоянных IP-адресов (уникальный адрес адресного пространства интернета);
- маршрутизация автономной системы пользователя;
- доступ к серверу статистики и серверу управления услугами.

4.4 Технические параметры

При предоставлении услуги «Виртуальная частная сеть» возможна организация каналов доступа к L3 VPN на скоростях до 100 Мбит/с.

Стандартные скорости каналов и стыки при предоставлении услуг «Виртуальная частная сеть» указаны в таблице 2.

Таблица 2 - Стандартные скорости каналов и стыки

Скорость канала доступа	Стык
10-100 Мбит/с	Ethernet 1000 BaseTX/LX/SX

Параметры качества для различных классов обслуживания приведены в таблице 3.

Требуемый класс качества сообщается поставщику услуг по каждой услуге «Виртуальная частная сеть».

Приведенные параметры качества поддерживаются при загрузке канала доступа к L3 VPN на 100% от установленной полосы пропускания.

Таблица 3 – Параметры качества обслуживания

Класс обслуживания (CoS)	0 (Best Effort, BE)	1 (Business Critical, BC)	2 (MultiMedia, MM)	3 (Real Time, RT)
Время задержки пакетов, не более, мс	250	100	80	50
Вариация времени задержки пакетов, не более, мс	100	50	40	20
Потери пакетов, %, не более	0,10%	0,10%	0,10%	0,10%
Основное применение	Интернет	Критичны е данные	IP TV	VoIP

Услуга «Доступ в Интернет» предоставляется на скоростях до 10 Мбит/с без ограничения объема трафика.

Стандартные скорости доступа и сетевые интерфейсы при предоставлении услуги «Доступ в Интернет» приведены в таблице 4.

Таблица 4 - Стандартные скорости доступа и сетевые интерфейсы

Скорость доступа в Интернет	Интерфейс
до 10 Мбит/с	Ethernet 1000 BaseTX/LX/SX

4.5 Сроки предоставления Услуг

Услуги должны предоставляться в определенный период.

Любая из услуг может быть отключена по официальному запросу.

4.6 Зоны ответственности

При предоставлении услуг разграничение ответственности должны определяется в зависимости от типа «последней мили» в соответствии с разработанными схемами.

В схемах организации связи должны указываться точки разграничения ответственности в зависимости от оборудования и предоставляемых услуг на объекте.

4.7 Доступность Услуг

На сети поставщика услуг, на базе которой оказываются услуги электросвязи, должны быть предусмотрены различные механизмы автоматического резервирования, позволяющие обеспечивать работоспособность услуги электросвязи при аварийных ситуациях на сетевом оборудовании, повреждении линий связи между сетевым оборудованием и других неисправностях сети.

Поставщик услуг должен обеспечивать восстановление работоспособности услуги в течение сроков:

- гарантированный срок восстановления поставщиком услуг услуги электросвязи при устранении неисправностей в своей зоне ответственности, не связанных с повреждением кабеля «последней мили», должен быть не более двух часов с момента обращения в службу технической поддержки поставщика услуг;

- гарантированный срок восстановления услуги электросвязи при устранении неисправностей в своей зоне ответственности, связанных с повреждением волоконно-оптического или медного кабеля «последней мили», должен быть не более 48 (сорока восьми) часов с момента обращения в службу технической поддержки поставщика услуг.

Для подтверждения неисправности, связанной с повреждением волоконно-оптического или медного кабеля «последней мили», поставщик услуг должен предоставить после устранения неисправности следующие документы:

- справку-допуск к месту устранения аварии владельца линейно-кабельных сооружений и/или зданий, где проложена линия, на которой произошла авария;

- паспорт оптической или медной линии связи, подтверждающий задействование линии для организации услуги, по которой открыт паспорт неисправности;

- рефлектограмму измерения оптической линии при возникновении аварии;
- рефлектограмму измерения оптической линии после устранения аварии;
- технический акт на услугу после устранения аварии.

Исполнитель должен обеспечивать коэффициент готовности услуги электросвязи не хуже 0,99997.

4.8 Выделение IP-адресов пользователю

При оказании услуги «Доступ в Интернет» поставщик услуг должен выделить IP-адреса в требуемом пользователю объеме.

4.9 Требования к службе технической поддержки поставщика услуг

Для обработки заявок об ухудшении качества услуг связи у поставщика услуг должна функционировать служба технической поддержки.

Необходимо иметь возможность контролировать ход работ по устранению ухудшения качества по услуге, для чего контактирует со службой технической поддержки.

Служба технической поддержки поставщика услуг должна быть доступна для обращения специалистов службы технической поддержки клиента круглосуточно без перерывов в режиме: двадцать четыре часа в сутки, семь дней в неделю, 365 дней в году в течение всего срока действия договора на услуги связи.

Специалисты службы технической поддержки поставщика услуг должны в любой момент принять информацию по телефону, электронной почте, по факсу.

Организованная поставщиком услуг телефонная линия для обращения специалистов службы технической поддержки пользователя должна быть всегда готова и свободна для входящих звонков.

Поставщик услуг должен проинформировать об актуальных контактных данных (номер телефона, факса и адрес электронной почты) своей службы технической поддержки.

Необходимо, с целью контроля процесса устранения ухудшения качества услуги, должен иметь возможность обращаться по телефону, факсу и по электронной почте в службу технической поддержки с различными запросами.

Специалисты службы технической поддержки поставщика услуг незамедлительно после обращения специалистов службы технической поддержки должны дать развернутый детальный ответ на их запрос.

Если услуга предоставляется с ухудшением качества, он должен действовать в соответствии с согласованным порядком взаимодействия при обнаружении ухудшения качества услуги. Данный порядок должен описывать взаимодействие участников процесса оказания услуг при обнаружении ухудшения качества услуги.

4.10 Сертификация

Оборудование поставщика услуг, с помощью которого оказываются услуги, должно быть сертифицировано на соответствии действующим в РФ правилам и разрешено для использования на территории РФ.

Факт соответствия должен быть подтвержден соответствующим сертификатом соответствия.

Сеть поставщика услуг должна иметь разрешение в соответствии с законодательством РФ и нормативными документами органа, регулирующего деятельность в отрасли связи на территории РФ.

Полный перечень услуг для каждого объекта приведен в приложении Г.

5 Разработка схемы подключения объектов информатизации ИСПДн к сети передачи данных

5.1 Схема организации СКД

Разработана схема организации сети, в которой взаимодействуют 26 объектов с двумя поставщиками услуг доступа в интернет. Все объекты сети находятся в двенадцати городах. Среди этих объектов 12 спортивных, 8 внешних информационных систем, объект размещения оборудования в резервном дата-центре для связи с системой идентификации болельщиков, объект размещения оборудования в основном дата-центре для связи с системой идентификации болельщиков, объект размещения оборудования в основном дата-центре для связи с системой аккредитации, объект размещения оборудования в резервном дата-центре для связи с системой аккредитации, объект центральные сервера базы данных и объект центр управления технической поддержкой. Каждый спортивный объект соединен с билетно-пропускной системой спортивного объекта через МЭ.

Все объекты взаимодействуют через двух поставщиков услуг. Один из них основной, другой резервный. При выходе из строя основного связь будет обеспечиваться резервным поставщиком.

Схема организации сети представлена на рисунке 3. Все объекты на данной схеме и информации о них внесены в таблицу 5.

Таблица 5 – Объекты сети

№ Объекта	Наименование объекта	Место расположение	Узел доступа	Адреса
1	Спортивный объект	Г. N1	OSPF area 65026	20.40.1.1 20.80.1.1
2	Спортивный объект	Г. N2	OSPF area 65026	20.40.2.1 20.80.2.1
3	Спортивный объект	Г. N3	OSPF area 65026	20.40.3.1 20.80.3.1
4	Спортивный объект	Г. N4	OSPF area 65026	20.40.4.1 20.80.4.1
5	Спортивный объект	Г. N5	OSPF area 65026	20.40.5.1 20.80.5.1
6	Спортивный объект	Г. N6	OSPF area 65026	20.40.6.1 20.80.6.1
7	Спортивный объект	Г. N7	OSPF area 65026	20.40.7.1 20.80.7.1
8	Спортивный объект	Г. N8	OSPF area 65026	20.40.8.1 20.80.8.1
9	Спортивный объект	Г. N9	OSPF area 65026	20.40.9.1 20.80.9.1
10	Спортивный объект	Г. N10	OSPF area 65026	20.40.10.1 20.80.10.1
11	Спортивный объект	Г. N12	OSPF area 65026	20.40.11.1 20.80.11.1
12	Спортивный объект	Г. N12	OSPF area 65026	20.40.12.1 20.80.12.1

Продолжение таблицы 5

№ Объекта	Наименование объекта	Место расположение	Узел доступа	Адреса
13	Внешняя информационная система	Г. N12	OSPF area 65026	20.40.13.1 20.80.13.1
14	Внешняя информационная система	Г. N12	OSPF area 65026	20.40.14.1 20.80.14.1
15	Внешняя информационная система	Г. N12	OSPF area 65026	20.40.15.1 20.80.15.1
16	Внешняя информационная система	Г. N11	OSPF area 65026	20.40.16.1 20.80.16.1
17	Внешняя информационная система	Г. N11	OSPF area 65026	20.40.17.1 20.80.17.1
18	Внешняя информационная система	Г. N11	OSPF area 65026	20.40.18.1 20.80.18.1
19	Внешняя информационная система	Г. N11	OSPF area 65026	20.40.19.1 20.80.19.1
20	Внешняя информационная система	Г. N11	OSPF area 65026	20.40.20.1 20.80.20.1

Продолжение таблицы 5

№ Объекта	Наименование объекта	Место расположение	Узел доступа	Адреса
21	размещения оборудования в резервном дата-центре для связи с системой идентификации болельщиков	Г. N12	OSPF area 65026	20.40.21.1 20.80.21.1
22	размещения оборудования в основном дата-центре для связи с системой идентификации болельщиков	Г. N12	OSPF area 65026	20.40.22.1 20.80.22.1
23	объект размещение оборудования в основном дата-центре для связи с системой аккредитации	Г. N12	OSPF area 65026	20.40.23.1 20.80.23.1
24	размещение оборудования в резервном дата-центре для связи с системой аккредитации	Г. N11	OSPF area 65026	20.40.24.1 20.80.24.1
25	центр управления технической поддержкой	Г. N11	OSPF area 65026	20.40.25.1 20.80.25.1
26	центральные сервера базы данных	Г. N11	OSPF area 65026	20.40.26.1 20.80.26.1

5.2 Схема организации сети спортивного объекта

Разработана схема организации сети спортивного объекта, состоящая из двух поставщиков услуг, двух криптошлюзов, двух коммутаторов, сети СКД, МЭ и ЛВС. Данная схема является идентичной схемой для всех двенадцати спортивных объектов.

Связующим узлом между сетью СКД спортивного объекта и выходом в интернет является пограничный коммутатор CISCO 2960, который обеспечивает передачу пакетов данных от криптошлюза в другую подсеть. Данный коммутатор настраивается для работы в двадцати шести подсетях и для двух поставщиков услуг.

Криптографическую защиту подсети обеспечивает два криптошлюза Coordinator HW1000 и МЭ ССПТ-2. Один из криптошлюзов основной, другой резервный. При выходе из строя одного, пакеты данных будут шифровать резервный. МЭ, в свою очередь, фильтрует весь проходящий через него трафик по определенным правилам.

Пакеты данных, проходящие от ЛВС билетно-пропускной системы к сети СКД и обратно, обеспечивает второй коммутатор.

Поставщики услуг обеспечивают связь на базе технологии MPLS VPN L3. При отказе основного канала связи, передача пакетов обеспечивает резервный поставщик.

Схема организации сети спортивного объекта представлена на рисунке 4.

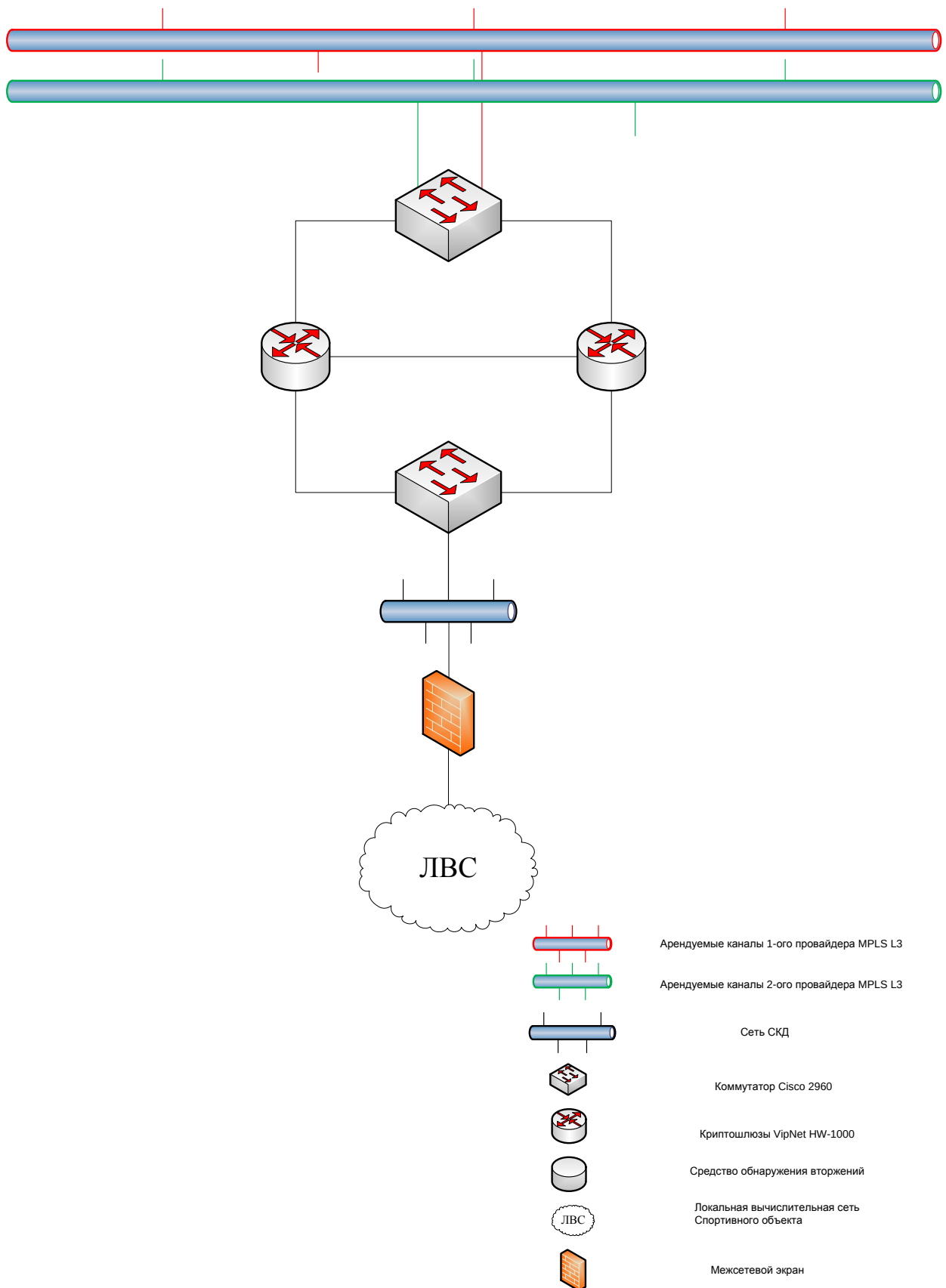


Рисунок 4 – Схема организации сети спортивного объекта

5.3 Схема организации сети ЦОД и ЦУТП

Разработана схема организации сети ЦОД и ЦУТП, состоящая из двух провайдеров, двух коммутаторов, двух маршрутизаторов, МЭ, СОВ и сети СКД.

В данной схеме сеть СКД имеет доступ в интернет, который предоставляет провайдер. Весь трафик через интернет проходит через МЭ и СОВ. В МЭ настраивается механизм трансляции сетевых адресов (NAT) и накладываются определенные правила прохождения для определенных ip-адресов в подсети. СОВ подключается в зеркальный порт, для зеркалирования входящего и исходящего трафика в МЭ. СОВ необходим для анализа проходящего трафика и обнаружения всех атак интернета.

Настройка работы коммутаторов и криптошлюзов такая же, как и на спортивных объектах.

Схема организации сети ЦОД и ЦУТП представлена на рисунке 5.

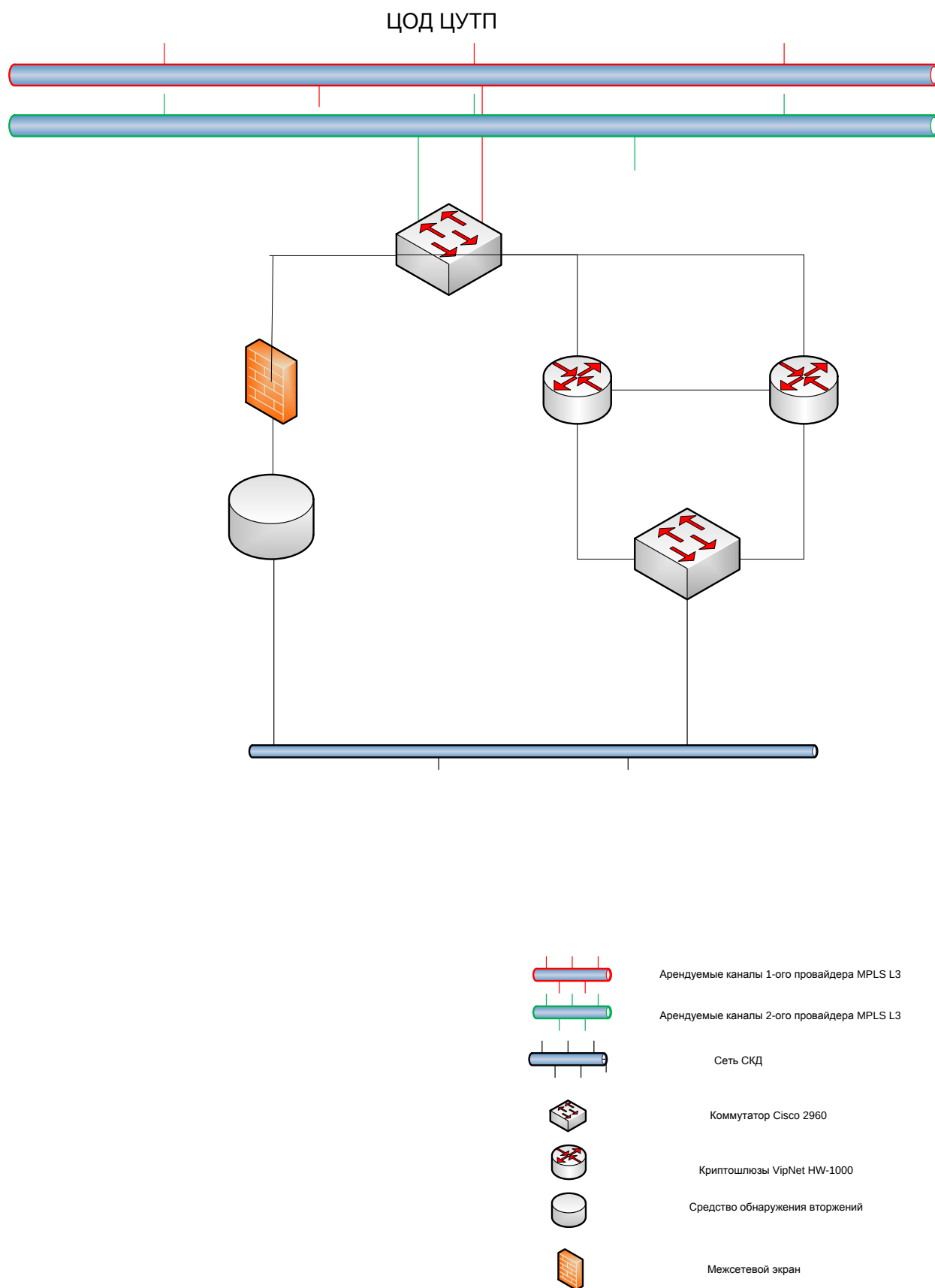


Рисунок 5 – Схема организации сети ЦОД и ЦУТП

6 Анализ рынка средств защиты информации для обеспечения защищенности сети передачи данных

6.1 Системы обнаружения и предотвращения вторжений.

Система обнаружения вторжений (СОВ) - программное или аппаратное средство, предназначенное для выявления фактов неавторизованного доступа в компьютерную систему или сеть либо несанкционированного управления ими в основном через Интернет. Системы обнаружения вторжений обеспечивают дополнительный уровень защиты компьютерных систем.

Системы обнаружения вторжений используются для обнаружения некоторых типов вредоносной активности, которая может нарушить безопасность компьютерной системы. К такой активности относятся сетевые атаки против уязвимых сервисов, атаки, направленные на повышение привилегий, неавторизованный доступ к важным файлам, а также действия вредоносного программного обеспечения (компьютерных вирусов, троянов и червей).

Требования к системам обнаружения вторжений применяются к программным и программно-техническим средствам, используемым в целях обеспечения защиты (не криптографическими методами) информации, содержащей сведения, составляющие государственную тайну, иной информации с ограниченным доступом.

Требования предназначены для организаций, осуществляющих в соответствии с законодательством Российской Федерации работы по созданию средств защиты информации, заявителей на осуществление сертификации продукции, а также для испытательных лабораторий и органов по сертификации, выполняющих работы по сертификации средств защиты информации на соответствие обязательным требованиям по безопасности информации.

Для дифференциации требований к функциям безопасности систем обнаружения вторжений установлено шесть классов защиты систем обнаружения вторжений. Самый низкий класс - шестой, самый высокий - первый.

В данной ИСПДн СОВ должно соответствовать требованиям не ниже четвертого класса защищенности.

Основными компонентами системы обнаружения вторжений (СОВ) являются датчики (сенсоры) и анализаторы.

Решение об обнаружении вторжения СОВ принимают в соответствии с результатами анализа информации, собираемой датчиками СОВ, с применением базы решающих правил СОВ.

В системе обнаружения вторжений должны быть реализованы следующие функции безопасности системы обнаружения вторжений:

- разграничение доступа к управлению системой обнаружения вторжений;
- управление работой системы обнаружения вторжений;
- управление параметрами системы обнаружения вторжений;
- управление установкой обновлений (актуализации) базы решающих правил системы обнаружения вторжений;
- анализ данных системы обнаружения вторжений;
- аудит безопасности системы обнаружения вторжений;
- сбор данных о событиях и активности в контролируемой информационной системе;
- реагирование системы обнаружения вторжений.

В среде, в которой СОВ функционирует, должны быть реализованы следующие функции безопасности среды:

- обеспечение доверенного маршрута;
- обеспечение доверенного канала;
- обеспечение условий безопасного функционирования;
- управление атрибутами безопасности.

Функции безопасности системы обнаружения вторжений должны обладать составом функциональных возможностей, обеспечивающих реализацию этих функций.

Далее изложены следующие виды требований безопасности, предъявляемые к СОВ:

- функциональные требования безопасности;
- требования доверия к безопасности.

Функциональные требования безопасности СОВ включают:

- требования по осуществлению сбора данных СОВ;
- требования к анализу данных СОВ;
- требования к реагированию СОВ;
- требования к средствам обновления базы решающих правил СОВ;
- требования по защите СОВ;
- требования по управлению режимами выполнения функций безопасности (работой СОВ);
- требования по управлению данными функций безопасности (данными СОВ);
- требования по управлению ролями субъектов;
- требования к средствам администрирования СОВ;
- требования к аудиту функционирования СОВ.

Рассмотрим следующие СОВ:

- Форпост;
- ViPNet IDS.

6.1.1 Форпост

Система обнаружения компьютерных атак (IDS - Intrusion detection system, в переводе с англ. русскоязычный термин — СОВ/СОА) «ФОРПОСТ» предназначена для автоматического выявления воздействий на контролируемую данным средством автоматизированную информационную систему, которые могут быть классифицированы как компьютерные атаки или вторжения, и блокирования развития выявленных компьютерных атак. включает в себя следующие компоненты:

- сетевые датчики, предназначенные для защиты объектов сетевых сегментов АС;
- серверные датчики, устанавливаемые на серверы АС и обеспечивающие защиту определенных сетевых сервисов системы;
- центр анализа и координации, обеспечивающий централизованный сбор, хранение и анализ информации, поступающей от серверных и сетевых датчиков;
- консоль администратора, предназначенная для централизованного управления компонентами системы.

Возможности:

- обнаружение и блокирование сетевых атак, направленных на нарушение информационной безопасности АС
- мониторинг трафика АС на сетевом, транспортном и прикладном уровнях
- выявление аномалий сетевого трафика АС
- обнаружение и блокирование сетевых атак в реальном масштабе времени
- оперативное реагирование на выявленные сетевые атаки
- обновление базы данных сигнатур атак в системе

6.1.2 ViPNet IDS

ViPNet IDS – это программно-аппаратный комплекс, выполненный в виде отдельно стоящего сетевого устройства, предназначенный для обнаружения вторжений в информационные системы на основе динамического анализа сетевого трафика стека протоколов TCP/IP для протоколов всех уровней модели взаимодействия открытых систем, начиная с сетевого и заканчивая прикладным. ViPNet IDS может использоваться в органах государственной власти Российской Федерации в автоматизированных информационных системах, обрабатывающих информацию, не содержащую сведений, составляющих государственную тайну.

Особенности:

- обнаружение компьютерных атак (вторжений) на основе динамического анализа сетевого трафика стека протоколов TCP/IP для протоколов всех уровней модели взаимодействия открытых систем, начиная с сетевого и заканчивая прикладным;
- регистрация компьютерных атак (вторжений) в момент времени, близкий к реальному;
- отображение обобщенной статистической информации об атаках;
- журналирование обнаруженных событий и атак для последующего анализа;
- выборочный поиск событий (атак) в соответствии с заданными фильтрами (по временному диапазону, IP-адресу, порту, степени критичности и др.);
- экспорт журнала атак (вторжений) в файл формата CSV для последующего анализа в сторонних приложениях;
- обновление баз решающих правил в автоматизированном режиме с Сервера обновлений при предоставлении новой версии указанной базы производителем;
- механизм, обеспечивающий маскирование ПАК ViPNet IDS в составе контролируемой сети;
- выборочное использование отдельных правил обнаружения или групп правил на усмотрение администратора ViPNet IDS;
- добавление собственных правил для анализа сетевого трафика;
- выборочный контроль ресурсов сети на уровне отдельных объектов;
- регистрация, отображение и экспорт в файл формата PCAP IP-пакетов, соответствующих зарегистрированным событиям (атакам) для последующего анализа в стороннем ПО;
- автоматическая передача обобщенной информации о сетевых атаках (вторжениях) системе централизованного мониторинга ViPNet StateWatcher по протоколу SNMP;

- контроль целостности исполняемых и конфигурационных файлов;
- контроль целостности загружаемых баз правил обнаружения атак.

6.2 Межсетевые экраны

Основной задачей сетевого экрана является защита компьютерных сетей или отдельных узлов от несанкционированного доступа. Также сетевые экраны часто называют фильтрами, так как их основная задача - не пропускать (фильтровать) пакеты, не подходящие под критерии, определённые в конфигурации.

Некоторые сетевые экраны также позволяют осуществлять трансляцию адресов - динамическую замену внутрисетевых (серых) адресов или портов на внешние, используемые за пределами ЛВС.

В данной ИСПДн МЭ считаю необходимым соответствовать требованиям не ниже четвертого класса защищенности.

МЭ должен обеспечивать фильтрацию на сетевом уровне.

Решение по фильтрации может приниматься для каждого сетевого пакета независимо на основе, по крайней мере, сетевых адресов отправителя и получателя или на основе других эквивалентных атрибутов.

Дополнительно МЭ должен обеспечивать:

- фильтрацию пакетов служебных протоколов, служащих для диагностики и управления работой сетевых устройств;
- фильтрацию с учетом входного и выходного сетевого интерфейса как средство проверки подлинности сетевых адресов;
- фильтрацию с учетом любых значимых полей сетевых пакетов.

МЭ должен обеспечивать возможность регистрации и учета фильтруемых пакетов. В параметры регистрации включаются адрес, время и результат фильтрации.

МЭ должен обеспечивать регистрацию входа (выхода) администратора МЭ в систему (из системы) либо загрузки и инициализации системы и ее программного останова. Регистрация выхода из системы не проводится в моменты аппаратного отключения МЭ.

В параметрах регистрации указываются:

- дата, время и код регистрируемого события;
- результат попытки осуществления регистрируемого события - успешная или неуспешная;
- идентификатор администратора МЭ, предъявленный при попытке осуществления регистрируемого события.

МЭ должен обеспечивать регистрацию входа (выхода) администратора МЭ в систему (из системы) либо загрузки и инициализации системы и ее программного останова. Регистрация выхода из системы не проводится в моменты аппаратурного отключения МЭ.

В параметрах регистрации указываются:

- дата, время и код регистрируемого события;
- результат попытки осуществления регистрируемого события - успешная или неуспешная;
- идентификатор администратора МЭ, предъявленный при попытке осуществления регистрируемого события.

Дополнительно МЭ должен обеспечивать регистрацию запуска программ и процессов (заданий, задач).

МЭ должен содержать средства контроля за целостностью своей программной и информационной части.

МЭ должен предусматривать процедуру восстановления после сбоев и отказов оборудования, которые должны обеспечивать восстановление свойств МЭ.

В МЭ должна обеспечиваться возможность регламентного тестирования:

- реализации правил фильтрации);
- процесса регистрации;
- процесса идентификации и аутентификации администратора МЭ;
- процесса регистрации действий администратора МЭ;

- процесса контроля за целостностью программной и информационной части.

Документ руководство администратора МЭ содержит:

- описание контролируемых функций МЭ;
- руководство по настройке и конфигурированию МЭ;
- описание старта МЭ и процедур проверки правильности старта;
- руководство по процедуре восстановления.

Тестовая документация должна содержать описание тестов и испытаний, которым подвергался МЭ и результаты тестирования.

Конструкторская (проектная) документация должна содержать:

- общую схему МЭ;
- общее описание принципов работы МЭ;
- описание правил фильтрации; описание средств и процесса идентификации и аутентификации;
- описание средств и процесса регистрации;
- описание средств и процесса контроля за целостностью программной и информационной части МЭ;
- описание процедуры восстановления свойств МЭ.

Рассмотрим следующие МЭ:

- ССПТ 2;
- Cisco ASA.

6.2.1 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.

ССПТ-2 применяется для разделения сегментов локальной вычислительной сети (ЛВС) с целью обеспечения защиты информации от несанкционированного доступа посредством:

- пакетной фильтрации на основе анализа параметров заголовков пакетов на различных уровнях сетевого взаимодействия – от канального до транспортного уровней включительно;

- управления транспортными соединениями между узлами ЛВС на основе анализа параметров виртуальных соединений и/или запросов на их установление;

- контроля данных прикладного уровня на основе заданных критериев и с учетом направления передачи потока пакетов.

ССПТ-2 может использоваться в ЛВС, построенных на базе технологии Ethernet с пропускной способностью 10/100/1000 Мбит/с.

Возможности:

- многоуровневая скрытая фильтрация пакетов по совокупности критериев;

- контроль транспортных соединений (до 40000 TCP сессий) на основе проверки соответствия каждого пакета контексту выбранной сессии;

- трансляция сетевых адресов (режим NAT) для сокрытия структуры внутренней сети с выделением «демилитаризованной зоны»;

- блокировка компьютерных flood-атак на основе фильтрация аномальной активности сетевых потоков данных;

- «зеркалирование» трафика на заданный интерфейс для анализа и проверки с использованием специальных средств контроля;

- горячее резервирование для создания систем фильтрации высокой готовности и отказоустойчивости;

- выгрузка журналов регистрации по протоколам FTP и SYSlog;

- защита канала управления с использованием алгоритма ГОСТ 28147-89 «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования» [8];

- аутентификация и авторизация администратора с помощью протокола RADIUS;

- контроль доступа к порту управления на основе списка доверенных сетевых адресов

- синхронизация таймера операционной системы по протоколу NTP.

6.2.2 Cisco ASA

Cisco ASA (Adaptive Security Appliance) — серия аппаратных межсетевых экранов, разработанных компанией Cisco Systems.

Возможности:

- межсетевое экранирование с учетом состояния соединений;
- глубокий анализ протоколов прикладного уровня;
- трансляция сетевых адресов;
- IPsec VPN;
- SSL VPN (подключение к сети через веб-интерфейс);
- протоколы динамической маршрутизации (RIP, EIGRP, OSPF).
- ASA не поддерживают протоколы туннелирования (такие, как GRE)

и policy-based routing

6.3 Средство криптографической защиты информации

В соответствии с приказом ФСБ России от 10 июля 2014 г. N 378 "Об утверждении Составы и содержания 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" СКЗИ присвоен второй уровень защищенности.

Для обеспечения 2 уровня защищенности персональных данных при их обработке в информационных системах, необходимо:

- организовать режим обеспечения безопасности помещений, в которых размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;

- обеспечить сохранность носителей персональных данных;
 - утвердить руководителем оператора документа, определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей;
 - использовать средства защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз.
 - назначить должностное лицо (работника), ответственного за обеспечение безопасности персональных данных в информационной системе.
 - чтобы доступ к содержанию электронного журнала сообщений был возможен исключительно для должностных лиц (работников) оператора или уполномоченного лица, которым сведения, содержащиеся в указанном журнале, необходимы для выполнения служебных (трудовых) обязанностей.
- Для выполнения вышеперечисленных требований необходимо:
- утвердить руководителем оператора список лиц, допущенных к содержанию электронного журнала сообщений, и поддержание указанного списка в актуальном состоянии;
 - обеспечить информационную систему автоматизированными средствами, регистрирующими запросы пользователей информационной системы на получение персональных данных, а также факты предоставления персональных данных по этим запросам в электронном журнале сообщений;
 - обеспечить информационную систему автоматизированными средствами, исключающими доступ к содержанию электронного журнала сообщений лиц, не указанных в утвержденном руководителем оператора списке лиц, допущенных к содержанию электронного журнала сообщений;
 - обеспечить периодический контроль работоспособности указанных в вышеперечисленных подпунктах настоящего пункта автоматизированных средств (не реже 1 раза в полгода).

Рассмотрим следующие СКЗИ:

- VipNet;
- Континент-АП.

6.3.1 ViPNet

ViPNet объединяет целый ряд продуктов и сетевых решений, рассчитанных на обработку информации ограниченного доступа, включая персональные данные:

- программные и программно-аппаратные средства организации виртуальных частных сетей (VPN) и инфраструктуры открытых ключей (PKI);
- средства межсетевого экранирования и персональные сетевые экраны;
- средства шифрования данных, хранимых и обрабатываемых на компьютерах и в сети;
- системы централизованного управления и мониторинга СЗИ;
- средства криптографической защиты информации для встраивания в прикладные системы сторонних разработчиков (системы юридически значимого документооборота, порталы и т.п.);
- программно-аппаратные комплексы (или самостоятельные сетевые устройства) обнаружения компьютерных атак ViPNet IDS.

Комплексный подход к обеспечению ИБ:

- многоуровневая защита от сетевых атак;
- конфиденциальность, целостность и доступность информационных ресурсов при использовании любых каналов связи;
- централизованное управление средствами защиты.

Уникальные механизмы сетевой безопасности:

- виртуализация адресного пространства в рамках VPN;
- полное сокрытие структуры защищаемой сети и передаваемой информации;

- низкоуровневый драйвер защиты приложений и операционной системы.

Прозрачная работа в современных сетях связи:

- поддержка всех доступных технологий связи: xDSL, Ethernet, WiFi, WiMAX, GPRS/EDGE/3G;
- полная совместимость с протоколами TCP/IP;
- прозрачная работа через NAT/PAT, поддержка DHCP, DNS;
- корректная обработка мультимедийного трафика и IP-телефонии.

Неограниченная масштабируемость и высокая надежность:

- до десятков тысяч сетевых узлов в одной защищенной сети;
- возможность произвольного связывания защищенных сетей;
- доступные конфигурации серверных продуктов с режимами горячего резервирования и кластеризации.

Развитые прикладные сервисы:

- все необходимые компоненты для развертывания инфраструктуры удостоверяющих центров;
- элементы документооборота и механизмы электронной цифровой подписи;
- защищенные чат и конференция;
- поддержка стандартных интерфейсов для встраивания в прикладное программное обеспечение заказчика.

Соответствие требованиям законодательства и регуляторов рынка:

- регулярная сертификация продуктов Компании на соответствие требованиям ФСБ и ФСТЭК России к средствам защиты конфиденциальной информации, включая персональные данные.

6.3.2 Континент-АП

Континент-АП позволяет обеспечить:

- защищенный доступ в корпоративную сеть с удаленных рабочих станций, персональных компьютеров удаленных сотрудников и мобильных устройств;

- подключение малых филиалов (1-2 АРМ) к виртуальной части сети организации.

Основные возможности Континента-АП:

- шифрование трафика по ГОСТ 28147–89 «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования»[8] с современной ключевой схемой обеспечивает гарантированную криптостойкость защищенного соединения;

- идентификация и аутентификация удаленного пользователя при установке соединения осуществляются на основе сертификатов открытых ключей стандарта X.509;

- персональный межсетевой экран в «Континент-АП» для ОС MS Windows обеспечивает безопасное подключение к сетям общего пользования и разграничение доступа к сетевым ресурсам АРМ;

- все политики доступа удаленных сотрудников настраиваются администратором VPN-сети организации при помощи программы управления ЦУС «Континент».

6.4 Результаты анализа

СОВ решено использовать отечественный продукт Фортпост v2.0. Он имеет сертификат и модульную структуру построения. Это идеальное решения для поставленной задачи.

Решено использовать МЭ ССПТ-2, так как у него большая функциональность и, по сравнению, с его конкурентом Cisco обойдется гораздо дешевле, так ССПТ-2 является разработкой наше отечественной организации. Не смотря на многолетнюю историю бренда Cisco, ССПТ-2 будет оптимальным выбором для данной работы.

В качестве криптографического оборудования будет использоваться комплекс программ VIPNet. Его функциональности достаточно для нашего проекта. В свою очередь Континент-АП обладает рядом преимуществ:

- поддержка широкого спектра ОС семейства MS Windows, Linux и Android;

- доступ по выделенным и коммутируемым каналам связи;
- поддержка работы с динамическими IP-адресами;
- возможность контроля доступа к ресурсам сетей общего пользования.

Но VipNet является разработкой отечественной компании и обойдется дешевле, то в ИСПДн необходимо использовать именно его.

7 Межсетевой экран ССПТ-2

7.1 Общие сведения

FNP типа ССПТ-2 является межсетевым экраном нового поколения (патент РФ 2214623, патент US 7281129), реализующим функции межсетевого экрана, но при этом остающимся «невидимым» для любых протоколов и тестовых воздействий, что достигается за счет отсутствия физических и логических адресов на его фильтрующих интерфейсах.

Скрытность функционирования межсетевого экрана повышает надежность системы защиты в целом и существенно упрощает процедуру установки ССПТ-2 в существующие компьютерные сети и функционирующие на их основе информационные и телематические системы.

На базе ССПТ-2 реализуются высокоэффективные масштабируемые решения по защите информации в компьютерных сетях на базе технологии Ethernet. Устройство FNP используется как:

Основное средство защиты для реализации различных политик информационной безопасности с помощью:

- фильтрации пакетов на канальном, сетевом, транспортном и прикладном уровнях;
- управления транспортными соединениями между отдельными узлами ЛВС или виртуальной ЛВС (VLAN);
- контроля контента данных на прикладном уровне с учетом направления, времени и типа протоколов передачи трафика.

Дополнительное устройство защиты для:

- обеспечения безопасности функционирования ранее установленных в компьютерной сети средств защиты и устройств маршрутизации;
- мониторинга трафика с возможностью анализа данных регистрации пакетов по различным критериям и интеграции с IDS;
- обеспечения функционирования сетевых распределенных телематических приложений и GRID ресурсов.

Функциональные характеристики:

- многоуровневая скрытная фильтрация пакетов по совокупности критериев.
- контроль транспортных соединений (до 40000 TCP сессий) на основе проверки соответствия каждого пакета контексту выбранной TCP сессии.
- трансляция сетевых адресов (режим NAT) в режиме «стелс» для сокрытия структуры внутренней сети с выделением «демилитаризованной зоны».
- блокировка компьютерных flood-атак на основе фильтрации аномальной активности сетевых потоков данных.
- регистрация системных событий и полных заголовков обработанных пакетов на всех уровнях межсетевого взаимодействия.
- ведение журналов регистрации пакетов и их выгрузка по запросам администратора сети с использованием протоколов FTP и SYSlog.
- аутентификация и авторизация администратора с помощью протокола RADIUS.
- контроль доступа к интерфейсу управления на основе списка доверенных сетевых адресов.
- синхронизация системного времени по протоколу NTP.

Межсетевой экран ССПТ-2 работает в режиме скрытной фильтрации и предназначен для защиты автоматизированных систем (АС), в которых обрабатывается информация различных уровней конфиденциальности.

ССПТ-2 применяется для разделения сегментов локальной вычислительной сети (ЛВС) с целью обеспечения защиты информации от несанкционированного доступа посредством:

- пакетной фильтрации на основе анализа параметров заголовков пакетов на различных уровнях сетевого взаимодействия – от канального до транспортного уровня включительно;

- управления транспортными соединениями между узлами ЛВС на основе анализа параметров виртуальных соединений и/или запросов на их установление;

- контроля данных прикладного уровня на основе заданных критериев и с учетом направления передачи потока пакетов.

ССПТ-2 может использоваться в ЛВС, построенных на базе технологии Ethernet с пропускной способностью 10/100/1000 Мбит/с.

7.2 Основные функциональные характеристики

Межсетевой экран ССПТ-2 обладает следующими основными функциональными характеристиками:

- многоуровневая, многопротокольная скрытная пакетная фильтрация по совокупности критериев;

- управление сессиями – контроль транспортных соединений на основе проверки соответствия каждого обрабатываемого пакета контексту сессии;

- трансляция сетевых адресов (режим NAT) с целью сокрытия внутренней сети с выделением “демилитаризованной зоны”;

- возможность аутентификации входящих и исходящих запросов методами, устойчивыми к пассивному и/или активному прослушиванию сети

- аутентификация сетевых пользователей (может быть активизирована только при включенном режиме NAT);

- блокировка сетевых flood-атак на основе выявления и последующей фильтрации аномальной активности сетевых потоков данных;

- выгрузка файлов регистрации событий и пакетов с использованием протоколов FTP и SYSLOG;

- защита канала управления на основе алгоритмов шифрования ГОСТ 28147-89 и ГОСТ Р 34.10-2001;

- контроль доступа к интерфейсам управления ССПТ-2 на основе списка доверенных IP-адресов;

– синхронизация системного времени операционной системы ССПТ-2 по протоколу NTP;

– “зеркалирование” трафика на заданный фильтрующий интерфейс для последующих анализа и проверки с использованием специальных средств контроля;

– горячее резервирование для создания систем фильтрации высокой готовности и отказоустойчивости.

7.3 Применение правил фильтрации для ССПТ-2 для данной ИСПДн

В данной системе межсетевые экраны выступают в качестве пограничных, то есть устанавливаются на разделение сети СКД и ЛВС билетно-пропускной системы спортивного объекта. Они осуществляют фильтрацию трафика между ПДн и не ПДн и устанавливаются на всех спортивных объектах во всех городах. Расположение и количество МЭ в сети представлено в таблице 6.

Таблица 6 - Расположении МЭ

№	Модель МЭ	Объект расположения МЭ	Количество, шт
1	ССПТ-2	Спортивный объект в г. №1	2
2	ССПТ-2	Спортивный объект в г. №2	2
3	ССПТ-2	Спортивный объект в г. №3	2
4	ССПТ-2	Спортивный объект в г. №4	2
5	ССПТ-2	Спортивный объект в г. №5	2
6	ССПТ-2	Спортивный объект в г. №6	2
7	ССПТ-2	Спортивный объект в г. №7	2
8	ССПТ-2	Спортивный объект в г. №8	2
9	ССПТ-2	Спортивный объект в г. №9	2
10	ССПТ-2	Спортивный объект в г. №10	2
11	ССПТ-2	Центр управления технической поддержки №1 в г. №11	2

Продолжение таблицы 6

№	Модель МЭ	Объект расположения МЭ	Кол- во, шт
12	ССПТ-2	Центр управления технической поддержки №2 в г. №11	2
13	ССПТ-2	Спортивный объект №1 в г. №12	2
14	ССПТ-2	Спортивный объект №2 в г. №12	2

Необходимо установить правила VLAN-групп МЭ на каждом спортивном объекте для их работы в данной ИСПДн. Правила настройки VLAN-групп для МЭ представлены в таблице 7.

Таблица 7 – правила VLAN-групп МЭ для спортивных объектов

Объект расположения МЭ	Правило фильтрации	Передача пакетов из интерфейса	Получения пакета на интерфейс	Протокол передачи	Порт
Спортивный объект в г. №1	Разрешение передачи пакетов	Eth0	Eth1	ICMP	161,162
				UDP	80
Спортивный объект в г. №2	Разрешение передачи пакетов	Eth0	Eth1	ICMP	161,162
				UDP	80
Спортивный объект в г. №3	Разрешение передачи пакетов	Eth0	Eth1	ICMP	161,162
				UDP	80
Спортивный объект в г. №4	Разрешение передачи пакетов	Eth0	Eth1	ICMP	161,162
				UDP	80
Спортивный объект в г. №5	Разрешение передачи пакетов	Eth0	Eth1	ICMP	161,162
				UDP	80

Продолжение таблицы 7

Объект расположения МЭ	Правило фильтрации	Передача пакетов из интерфейса	Получения пакета на интерфейс	Протокол передачи	Порт
Спортивный объект в г. №6	Разрешение передачи пакетов	Eth0	Eth1	ICMP	161,162
				UDP	80
Спортивный объект в г. №7	Разрешение передачи пакетов	Eth0	Eth1	ICMP	161,162
				UDP	80
Спортивный объект в г. №8	Разрешение передачи пакетов	Eth0	Eth1	ICMP	161,162
				UDP	80
Спортивный объект в г. №9	Разрешение передачи пакетов	Eth0	Eth1	ICMP	161,162
				UDP	80
Спортивный объект в г. №10	Разрешение передачи пакетов	Eth0	Eth1	ICMP	161,162
				UDP	80
Спортивный объект №1 в г. №12	Разрешение передачи пакетов	Eth0	Eth1	ICMP	161,162
				UDP	80
Спортивный объект №2 в г. №12	Разрешение передачи пакетов	Eth0	Eth1	ICMP	161,162
				UDP	80

На все остальные интерфейсы, протоколы и порты по умолчанию накладывается правило о запрете передаче пакетов по ним для VLAN-групп.

Также необходимо установить правила фильтрации по ip-адресам МЭ на каждом спортивном объекте для их работы в данной ИСПДн. Правила настройки ip-адресов для МЭ представлены в таблице 8.

Таблица 8 – Правила по ip-адресам

Объект расположения МЭ	Правило фильтрации	Передача пакетов из интерфейса	Получения пакета на интерфейс	Протокол передачи	Порт	Разрешенные ip-адреса
Спортивный объект в г. №1	Разрешение передачи пакетов	Eth0	Eth1	ICMP	161,162	192.168.1.0/23
				UDP	80	192.168.234.0/21
Спортивный объект в г. №2	Разрешение передачи пакетов	Eth0	Eth1	ICMP	161,162	192.168.32.0/23
				UDP	80	192.168.124.0/21
Спортивный объект в г. №3	Разрешение передачи пакетов	Eth0	Eth1	ICMP	161,162	192.168.4.0/23
				UDP	80	192.168.246.0/21
Спортивный объект в г. №4	Разрешение передачи пакетов	Eth0	Eth1	ICMP	161,162	192.168.6.0/23
				UDP	80	192.168.220.0/21
Спортивный объект в г. №5	Разрешение передачи пакетов	Eth0	Eth1	ICMP	161,162	192.168.8..0/23
				UDP	80	192.168.188.0/21

Продолжение таблицы 8

Объект расположения МЭ	Правило фильтрации	Передача пакетов из интерфейса	Получения пакета на интерфейс	Протокол передачи	Порт	Разрешенные ip-адреса
Спортивный объект в г. №6	Разрешение передачи пакетов	Eth0	Eth1	ICMP	161,162	192.168.10.0/23
				UDP	80	192.168.128.0/21
Спортивный объект в г. №7	Разрешение передачи пакетов	Eth0	Eth1	ICMP	161,162	192.168.12.0/23
				UDP	80	192.168.138.0/21
Спортивный объект в г. №8	Разрешение передачи пакетов	Eth0	Eth1	ICMP	161,162	192.168.14.0/23
				UDP	80	192.168.136.0/21
Спортивный объект в г. №9	Разрешение передачи пакетов	Eth0	Eth1	ICMP	161,162	192.168.16.0/23
				UDP	80	192.168.134.0/21
Спортивный объект в г. №10	Разрешение передачи пакетов	Eth0	Eth1	ICMP	161,162	192.168.18.0/23
				UDP	80	192.168.178.0/21

Продолжение таблицы 8

Объект расположения МЭ	Правило фильтрации	Передача пакетов из интерфейса	Получения пакета на интерфейс	Протокол передачи	Порт	Разрешенные ip-адреса
Спортивный объект №1 в г. №12	Разрешение передачи пакетов	Eth0	Eth1	ICMP	161,162	192.168.30.0/23
				UDP	80	192.168.90.0/21
Спортивный объект №2 в г. №12	Разрешение передачи пакетов	Eth0	Eth1	ICMP	161,162	192.168.32.0/23
				UDP	80	192.168.100.0/21

На все остальные интерфейсы, протоколы, порты и ip-адреса по умолчанию накладывается правило о запрете передаче пакетов по ним.

Также необходимо настройки подсистемы трансляции сетевых адресов NAT МЭ на каждом спортивном объекте для их работы в данной ИСПДн.

Настройки подсистемы трансляции сетевых адресов NAT для МЭ представлены в таблице 9.

Таблица 9 – Параметры настройки сетевых адресов NAT

Объект расположения МЭ	Правило фильтрации	Передача пакетов из интерфейса	Получения пакета на интерфейс	Протокол передачи	Порт	IP-адрес узла	MAC-адрес сетевого адаптера узла
Спортивный объект в г. №1	Разрешение передачи пакетов	Eth0	Eth1	ICMP	161,162	192.168.1.0/23	00:04:23:bd:0b:d1
				UDP	80	192.168.234.0/21	
Спортивный объект в г. №2	Разрешение передачи пакетов	Eth0	Eth1	ICMP	161,162	192.168.32.0/23	00:04:32:bd:0b:d2
				UDP	80	192.168.124.0/21	
Спортивный объект в г. №3	Разрешение передачи пакетов	Eth0	Eth1	ICMP	161,162	192.168.4.0/23	00:04:22:bd:0b:d3
				UDP	80	192.168.246.0/21	
Спортивный объект в г. №4	Разрешение передачи пакетов	Eth0	Eth1	ICMP	161,162	192.168.6.0/23	00:04:06:bd:0b:d4
				UDP	80	192.168.220.0/21	

Продолжение таблицы 9

Объект расположения МЭ	Правило фильтрации	Передача пакетов из интерфейса	Получения пакета на интерфейс	Протокол передачи	Порт	IP-адрес узла	MAC-адрес сетевого адаптера узла
Спортивный объект в г. №5	Разрешение передачи пакетов	Eth0	Eth1	ICMP	161,162	192.168.8..0/23	00:04:08:bd:0b:d5
				UDP	80	192.168.188.0/21	
Спортивный объект в г. №6	Разрешение передачи пакетов	Eth0	Eth1	ICMP	161,162	192.168.10.0/23	00:04:10:bd:0b:d6
				UDP	80	192.168.128.0/21	
Спортивный объект в г. №7	Разрешение передачи пакетов	Eth0	Eth1	ICMP	161,162	192.168.12.0/23	00:04:12:bd:0b:d7
				UDP	80	192.168.138.0/21	
Спортивный объект в г. №8	Разрешение передачи пакетов	Eth0	Eth1	ICMP	161,162	192.168.14.0/23	00:04:214:bd:0b:d8
				UDP	80	192.168.136.0/21	
Спортивный объект в г. №9	Разрешение передачи пакетов	Eth0	Eth1	ICMP	161,162	192.168.16.0/23	00:04:16:bd:0b:d1
				UDP	80	192.168.134.0/21	

Продолжение таблицы 9

Объект расположения МЭ	Правило фильтрации	Передача пакетов из интерфейса	Получения пакета на интерфейс	Протокол передачи	Порт	IP-адрес узла	MAC-адрес сетевого адаптера узла
Спортивный объект в г. №10	Разрешение передачи пакетов	Eth0	Eth1	ICMP	161,162	192.168.18.0/23	00:04:18:bd:0b:d2
				UDP	80	192.168.178.0/21	
Спортивный объект №1 в г. №12	Разрешение передачи пакетов	Eth0	Eth1	ICMP	161,162	192.168.30.0/23	00:04:30:bd:0b:d3
				UDP	80	192.168.90.0/21	
Спортивный объект №2 в г. №12	Разрешение передачи пакетов	Eth0	Eth1	ICMP	161,162	192.168.32.0/23	00:04:32:bd:0b:d4
				UDP	80	192.168.100.0/21	

На каждом спортивном объекте устанавливаются два МЭ. Один основной, другой резервный. Для их совместной работы необходимо их синхронизировать и настроить на работу в режиме «зеркалирования». Пример настройки МЭ ССПТ-2 представлен в приложении А.

8 Кристошлюз ViPNet Coordinator HW1000

8.1 Общие сведения

ViPNet Coordinator (Сертификат соответствия ФСБ России № СФ/124-2981 от 14.11.2016 на соответствие изделия «Программно-аппаратный комплекс ViPNet Coordinator HW 4» требованиям ГОСТ 28147-89 и требованиям ФСБ России к средствам криптографической защиты класса КСЗ)— семейство шлюзов безопасности, входящих в состав продуктовой линейки ViPNet Network Security. В зависимости от настроек ViPNet Coordinator может выполнять следующие функции в защищенной сети ViPNet:

- маршрутизатор VPN-пакетов: маршрутизация зашифрованных IP-пакетов, передаваемых между сегментами защищенной сети.
- VPN-шлюз: туннелирование (шифрование и имитозащита) открытых IP-пакетов, передаваемых между локальными сегментами сети.
- межсетевой экран: анализ, фильтрация и регистрация IP-трафика на границе сегмента сети.
- транспортный сервер: маршрутизация передачи защищенных служебных данных в сети ViPNet, почтовых сообщений, передаваемых программой «ViPNet Деловая почта».
- сервер IP-адресов, сервер соединений: обеспечивает регистрацию и доступ в реальном времени к информации о состоянии объектов защищенной сети и о текущем значении их сетевых настроек (IP-адресов и т.п.).

Продукты ViPNet Coordinator адаптированы для использования в различных отраслях и сценариях применения. Семейство шлюзов безопасности ViPNet Coordinator подразделяется на решения, в зависимости от особенностей их исполнения, в том числе аппаратной платформы продукта, набора дополнительных сетевых сервисов, производительности, сетевых интерфейсов и др.

ViPNet Coordinator HW1000 — шлюз безопасности для защиты компьютерных сетей масштаба предприятия. ViPNet Coordinator HW1000

позволяет организовать защищенный доступ как в ЦОДы, так и в корпоративную облачную инфраструктуру, и поддерживает защиту скоростных каналов связи до 1 Гбит/сек. ПАК ViPNet Coordinator HW1000, исполненный в форм-факторе 1U, потребляет низкое количество электроэнергии, обладает невысоким уровнем тепловыделения и не требует каких-либо особых условий для размещения и эксплуатации, представляя собой высокоэффективное средство сетевой защиты.

Сертификат соответствия ФСБ России № СФ/124-2981 от 14.11.2016 на соответствие изделия «Программно-аппаратный комплекс ViPNet Coordinator HW 4» требованиям ГОСТ 28147-89 и требованиям ФСБ России к средствам криптографической защиты класса КСЗ.

Примущества ViPNet Coordinator HW1000:

- VPN без установления соединения обеспечивает повышенную надежность и устойчивость соединений через шлюз безопасности ViPNet Coordinator HW1000;
- поддержка работы в современных мультисервисных сетях связи без ограничений по совместимости со службами DHCP, WINS, DNS, с динамическим преобразованием адресов (NAT, PAT), с использованием мультимедийных протоколов (SIP, H323, SCCP и другие);
- использование ПО ViPNet Administrator в качестве центра генерации ключей шифрования.
- специальная архитектура файловой системы предотвращает возможность порчи образа операционной системы и ПО ViPNet при сбоях питания.
- возможность повышения надежности координатора за счет его развертывания в составе кластера горячего резервирования.

8.2 Работа и настройка криптошлюза VIPNet Coordinator HW1000

В данной сети криптошлюз должен выполнять функцию координатора, т.е. должен выполнять шифрование трафика «все со всеми» и отправлять пакет данных по заданному маршруту. То есть если компьютер, находящиеся в одной подсети, хочет обратиться к компьютеру, находящиеся в другой подсети, он отправит пакет на внутренний порт криптошлюза. Тот получит пакет, зашифрует и отправит в подсеть, тому адресату, которому положено. Для этого необходимо прописать конфигурацию всей сети. Все настройки проходят в приложении «VIPNet Administrator центр управления сетью».

Для работы криптошлюза необходимо:

- прописать все криптошлюзы;
- сгенерировать все возможные маршруты;
- прописать в криптошлюзе адрес подсети;
- назначить криптошлюзам задачу по шифрованию трафика;
- назначить пользователей к каждому криптошлюзу;
- обеспечить режим резервирования.

Все настройки осуществлялись в соответствии с регистрационным файлом, который предоставляется производителем. В нем записано количество узлов, которые могут быть в данной сети, определенной количество мобильных устройств, количество АРМ и количество возможных криптошлюзов для работы в режиме резервирования.

Настройка криптошлюза VIPNet Coordinator HW1000 для данной сети, представлена в приложении Б.

9 Коммутатор Cisco 2960

9.1 Общие сведения

Коммутатор Cisco 2960 предназначен для применения в качестве оборудования коммутации пакетов информации, для использования в сети связи общего пользования и технологических сетях связи в случае их присоединения к сети общего пользования.

Коммутаторы Cisco Catalyst серии 2960 предоставляют следующие возможности:

- спаренные порты каскадирования для обеспечения гибкости каскадных соединений коммутаторов Gigabit Ethernet, которые позволяют использовать подключение по медным или оптоволоконным кабелям; каждый спаренный порт каскадирования состоит из одного порта Ethernet 10/100/1000 Мбит/с и одного порта GbE для подключения SFP, при этом активен может быть только один из двух портов;
- возможность подключения настольных компьютеров к 24 или 48 портам Fast Ethernet;
- конфигурации PoE с мощностью до 15,4 Вт на один порт;
- широкий набор программных средств, обеспечивающих простоту эксплуатации, защиту бизнес-процессов,
- устойчивость и работу в "сетях без границ";
- ограниченная гарантия на оборудование в течение его жизненного цикла.

9.2 Работа и настройка коммутатора Cisco 2960

В данном разделе рассматривается пограничный коммутатор, который находится на границе КЗ. Он используется для коммутации нашего оборудования, находящегося в КЗ, с оборудованием основного и резервного провайдеров. Конкретно коммутатор получает зашифрованный пакет данных от криптошлюза и отправляет его на оборудования провайдера, который, в свою очередь, отправляет его по определенному адресу.

Для выполнения данной задачи необходимо настроить коммутатор для работы с несколькими портами и двумя провайдерами. Текст настройки представлен в приложении В.

10 Разработка организационных требований

10.1 Организационные требования к СКЗИ

Организационные меры обеспечения безопасности обработки с использованием криптографических средств персональных данных:

- разработку для каждой информационной системы персональных данных модели угроз безопасности персональных данных при их обработке;
- разработку на основе модели угроз системы безопасности персональных данных, обеспечивающей нейтрализацию всех перечисленных в модели угроз;
- определение необходимости использования криптосредств для обеспечения безопасности персональных данных и, в случае положительного решения, определение на основе модели угроз цели использования криптосредств для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных и (или) иных неправомерных действий при их обработке;
- установку и ввод в эксплуатацию криптосредств в соответствии с эксплуатационной и технической документацией к этим средствам;
- проверку готовности криптосредств к использованию с составлением заключений о возможности их эксплуатации;
- обучение лиц, использующих криптосредства, работе с ними;
- поэкземплярный учет используемых криптосредств, эксплуатационной и технической документации к ним, носителей персональных данных;
- учет лиц, допущенных к работе с криптосредствами, предназначенными для обеспечения безопасности персональных данных в информационной системе (пользователи криптосредств);
- контроль за соблюдением условий использования криптосредств, предусмотренных эксплуатационной и технической документацией к ним;

– разбирательство и составление заключений по фактам нарушения условий хранения носителей персональных данных, использования криптосредств, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений;

– описание организационных и технических мер, которые оператор обязуется осуществлять при обеспечении безопасности персональных данных с использованием криптосредств при их обработке в информационных системах, с указанием в частности:

– индекса, условного наименования и регистрационных номеров используемых криптосредств;

– соответствия размещения и монтажа аппаратуры и оборудования, входящего в состав криптосредств, требованиям нормативной документации и правилам пользования криптосредствами;

– соответствия помещений, в котором размещены криптосредства и хранится ключевая документация к ним, настоящим Требованиям с описанием основных средств защиты;

– выполнения требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных.

Описание принятых мер должно быть включено в уведомление.

Криптографическая защита ПДн в ИСПДн при их передаче по каналам связи, не защищенным организационно-техническими мерами, осуществляется с использованием СКЗИ, сертифицированных в системе сертификации РОСС RU.0001.030001 на соответствие требованиям ФСБ России по классу защищенности не ниже КС2.

СКЗИ класса КС2 применяются для нейтрализации атак, при создании способов, подготовке и проведении которых используются возможности из числа следующих дополнительных возможностей:

а) создание способов, подготовка и проведение атак без привлечения специалистов в области разработки и анализа СКЗИ;

б) создание способов, подготовка и проведение атак на различных этапах жизненного цикла СКЗИ;

в) проведение атаки, находясь вне пространства, в пределах которого осуществляется контроль за пребыванием и действиями лиц и (или) транспортных средств;

г) проведение на этапах разработки (модернизации), производства, хранения, транспортировки СКЗИ и этапе ввода в эксплуатацию СКЗИ (пусконаладочные работы) следующих атак:

- внесение несанкционированных изменений в СКЗИ и (или) в компоненты аппаратных и программных средств, совместно с которыми штатно функционируют СКЗИ и в совокупности представляющие среду функционирования СКЗИ (далее - СФ), которые способны повлиять на выполнение предъявляемых к СКЗИ требований, в том числе с использованием вредоносных программ;

- внесение несанкционированных изменений в документацию на СКЗИ и компоненты СФ;

д) проведение атак на этапе эксплуатации СКЗИ на:

- персональные данные;
- ключевую, аутентифицирующую и парольную информацию СКЗИ;
- программные компоненты СКЗИ;
- аппаратные компоненты СКЗИ;
- программные компоненты СФ, включая программное обеспечение BIOS;

- аппаратные компоненты СФ;
- данные, передаваемые по каналам связи;
- иные объекты, которые установлены при формировании совокупности предложений о возможностях, которые могут использоваться при создании способов, подготовке и проведении атак с учетом применяемых в информационной системе информационных технологий, аппаратных средств (далее - АС) и программного обеспечения (далее - ПО);

е) получение из находящихся в свободном доступе источников (включая информационно-телекоммуникационные сети, доступ к которым не ограничен определенным кругом лиц, в том числе информационно-телекоммуникационную сеть "Интернет") информации об информационной системе, в которой используется СКЗИ. При этом может быть получена следующая информация:

- общие сведения об информационной системе, в которой используется СКЗИ (назначение, состав, оператор, объекты, в которых размещены ресурсы информационной системы);

- сведения об информационных технологиях, базах данных, АС, ПО, используемых в информационной системе совместно с СКЗИ, за исключением сведений, содержащихся только в конструкторской документации на информационные технологии, базы данных, АС, ПО, используемые в информационной системе совместно с СКЗИ;

- содержание конструкторской документации на СКЗИ;
- содержание находящейся в свободном доступе документации на аппаратные и программные компоненты СКЗИ и СФ;

- общие сведения о защищаемой информации, используемой в процессе эксплуатации СКЗИ;

- сведения о каналах связи, по которым передаются защищаемые СКЗИ персональные данные (далее - канал связи);

- все возможные данные, передаваемые в открытом виде по каналам связи, не защищенным от несанкционированного доступа к информации организационными и техническими мерами;

- сведения обо всех проявляющихся в каналах связи, не защищенных от несанкционированного доступа к информации организационными и техническими мерами, нарушениях правил эксплуатации СКЗИ и СФ;

- сведения обо всех проявляющихся в каналах связи, не защищенных от несанкционированного доступа к информации организационными и техническими мерами, неисправностях и сбоях аппаратных компонентов СКЗИ и СФ;

- сведения, получаемые в результате анализа любых сигналов от аппаратных компонентов СКЗИ и СФ;

ж) применение:

- находящихся в свободном доступе или используемых за пределами контролируемой зоны АС и ПО, включая аппаратные и программные компоненты СКЗИ и СФ;

- специально разработанных АС и ПО;

з) использование на этапе эксплуатации в качестве среды переноса от субъекта к объекту (от объекта к субъекту) атаки действий, осуществляемых при подготовке и (или) проведении атаки:

- каналов связи, не защищенных от несанкционированного доступа к информации организационными и техническими мерами;

- каналов распространения сигналов, сопровождающих функционирование СКЗИ и СФ;

и) проведение на этапе эксплуатации атаки из информационно-телекоммуникационных сетей, доступ к которым не ограничен определенным кругом лиц, если информационные системы, в которых используются СКЗИ, имеют выход в эти сети;

к) использование на этапе эксплуатации находящихся за пределами контролируемой зоны АС и ПО из состава средств информационной системы, применяемых на местах эксплуатации СКЗИ (далее - штатные средства).

л) проведение атаки при нахождении в пределах контролируемой зоны;

м) проведение атак на этапе эксплуатации СКЗИ на документацию на СКЗИ и компоненты СФ, помещения, в которых находится совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем (далее - СВТ), на которых реализованы СКЗИ и СФ;

н) получение в рамках предоставленных полномочий, а также в результате наблюдений следующей информации:

- сведений о физических мерах защиты объектов, в которых размещены ресурсы информационной системы;

- сведений о мерах по обеспечению контролируемой зоны объектов, в которых размещены ресурсы информационной системы;

- сведений о мерах по разграничению доступа в Помещения, в которых находятся СВТ, на которых реализованы СКЗИ и СФ;

о) использование штатных средств, ограниченное мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий.

п) создание способов, подготовка и проведение атак с привлечением специалистов в области анализа сигналов, сопровождающих функционирование СКЗИ и СФ, и в области использования для реализации атак недокументированных (не декларированных) возможностей прикладного ПО;

р) проведение лабораторных исследований СКЗИ, используемых вне контролируемой зоны, ограниченное мерами, реализованными в

информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий;

с) проведение работ по созданию способов и средств атак в научно-исследовательских центрах, специализирующихся в области разработки и анализа СКЗИ и СФ, в том числе с использованием исходных текстов входящего в СФ прикладного ПО, непосредственно использующего вызовы программных функций СКЗИ.

10.2 Организационные требования к ИСПДн

Для обеспечения 2 уровня защищенности персональных данных при их обработке в информационных системах, необходимо:

- организовать режим обеспечения безопасности помещений, в которых размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;

- обеспечить сохранность носителей персональных данных;

- утвердить руководителем оператора документа, определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей;

- использовать средства защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз.

- назначить должностное лицо (работника), ответственного за обеспечение безопасности персональных данных в информационной системе.

- чтобы доступ к содержанию электронного журнала сообщений был возможен исключительно для должностных лиц (работников) оператора или уполномоченного лица, которым сведения, содержащиеся в указанном журнале, необходимы для выполнения служебных (трудовых) обязанностей.

Для выполнения вышеперечисленных требований необходимо:

- утвердить руководителем оператора список лиц, допущенных к содержанию электронного журнала сообщений, и поддержание указанного списка в актуальном состоянии;
- обеспечить информационную систему автоматизированными средствами, регистрирующими запросы пользователей информационной системы на получение персональных данных, а также факты предоставления персональных данных по этим запросам в электронном журнале сообщений;
- обеспечить информационную систему автоматизированными средствами, исключающими доступ к содержанию электронного журнала сообщений лиц, не указанных в утвержденном руководителем оператора списке лиц, допущенных к содержанию электронного журнала сообщений;
- обеспечить периодический контроль работоспособности указанных в вышеперечисленных подпунктах настоящего пункта автоматизированных средств (не реже 1 раза в полгода).

11 Разработка технических требований

11.1 Требования к активному сетевому оборудованию

Активное сетевое оборудование должно обеспечить объединение и подключение АРМ, объектовых серверов и устройств контроля доступа к централизованным вычислительным ресурсам на основе современных и перспективных сетевых технологий – Fast Ethernet, Gigabit Ethernet.

Активное сетевое оборудование и серверы объекта должны быть размещены в отдельном помещении. Сетевое оборудование контроля доступа должно быть размещено в защищенных коммутационных шкафах.

Оборудование должно иметь возможность установки в стандартные 19” стойки или шкафы.

Поддержка современных стандартов передачи данных:

- стандарт IEEE 802.3. Спецификация параметров и требований технологии передачи "Ethernet" (Local Area Networks): Carrier Sense Multiple Access with Collision Detection (CSMA/CD) - ETHERNET;

- стандарт IEEE 802.3u. Спецификация параметров и требований технологии передачи "Fast Ethernet" (Local and Metropolitan Area Networks-Supplement - Media Access Control (MAC) Parameters, Physical Layer, Medium Attachment Units and Repeater for 100 Mb/s Operation, Type 100BASE-T);

- стандарт IEEE 802.3z. Спецификация параметров и требований технологии передачи "Gigabit Ethernet" (Media Access Control Parameters, Physical Layers, Repeater and Management Parameters for 1,000 Mb/s Operation, Supplement to Information Technology - Local and Metropolitan Area Networks - Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications);

- стандарт IEEE 802.1p. Спецификация параметров и требований технологии классификации трафика и динамической широковещательной фильтрации (Standard for Local and Metropolitan Area Networks&Supplement to Media Access Control (MAC) Bridges: Traffic Class Expediting and Dynamic Multicast Filtering);

– стандарт IEEE 802.1D-2004. Спецификация параметров и требований протокола STP и его модификаций RSTP и MSTP (Media Access Control (MAC) Bridges).

Активное сетевое оборудование должно обеспечивать:

- круглосуточный режим работы;
- высокую надежность и отказоустойчивость оборудования;
- возможность гибкого наращивания конфигурации ЛВС;
- возможность подключения централизованных ресурсов непосредственно к высокоскоростной магистрали сети;
- возможность масштабирования пропускной способности сети;
- повышенную пропускную способность на участках с наиболее интенсивным трафиком;
- минимизацию задержек при обращении к серверам;
- малое время восстановления оборудования после отказов в сети;
- возможность самодиагностирования сетевого оборудования и простоту локализации неисправностей;
- работу оборудования в диапазоне рабочих температур от +5 до +40 С.;
- единообразие применяемого оборудования (например, все активное оборудование ЛВС от одного производителя).
- подключение оборудования по технологии Ethernet с автоматическим определением скорости подключения;
- технологию объединения портов для создания единого логического соединения на портах Fast Ethernet;
- возможность информационного взаимодействия через систему телекоммуникаций на базе протокола IP;
- возможность использования, как для высокоскоростной передачи данных, так и низкоскоростных аналоговых голосовых приложений;
- производительность на системной шине не менее 30 Гбит/с;

- возможность установления приоритетов трафика на уровне портов;
- соединение периферийного активного сетевого оборудования и центрального активного сетевого оборудования по технологии Gigabit Ethernet;
- технологию локальных виртуальных сетей "VLAN" (стандарт 802.1Q);
- протокол быстрого восстановления сетевой топологии IEEE 802.1D-2004 RSTP (Rapid Spanning Tree Protocol) для резервирования соединений и предотвращения колец в логической топологии сети;
- информационную безопасность (идентификация пользователей, блокирование портов, списки доступа);
- поддержку протоколов резервирования основных компонентов, позволяющих обойтись без переконфигурирования сетевых устройств для обеспечения безотказной работы магистрали и межсетевого взаимодействия;
- возможность дистанционного управления и настройки оборудования с помощью встроенного программного обеспечения.
- возможность дистанционного мониторинга группы с помощью специального ПО.
- на стадии проектирования необходимо предусмотреть подключение активного сетевого оборудования к источникам бесперебойного питания.

Требования к техническим характеристиками сетевого оборудования представлены в таблице №10.

Таблица 10 - Требования к техническим характеристикам активного оборудования ЛВС

Тип коммутатора	Управляемый коммутатор 2 уровня (или эквивалент)
Порты	22 порта 1000BaseX SFP 2 комбо-порта 10/100/1000BASE-T или 1000BaseX SFP
Стандарты и функции	IEEE 802.3 10BASE-T/802.3u 100BASE-TX IEEE 802.3ab 1000BASE-T/802.3z 1000BASE-SX/LX ANSI/IEEE 802.3 NWay автосогласование IEEE 802.3x управление потоком Автоматическое определение полярности MDI/MDIX Зеркалирование портов
VLAN	IEEE 802.1Q Tagged VLAN VLAN на базе портов GARP/GVRP Максимальное количество VLAN на устройство: 255
Агрегирование портов	Максимальное количество портов в транковой группе: 8 Максимальное количество транковых групп на устройство: 6 Рабочий режим: распределение нагрузки Статические и динамические режимы Link Aggregation (LACP), совместимые с 802.3ad
Безопасность доступа	Функция Port security (макс. 20 MAC-адресов) Управление доступом 802.1x на базе портов Управление доступом 802.1x на базе MAC-адресов SSH v.1, v.2; SSL Сегментация трафика (без или с тегами VLAN) IP-MAC binding: 512 записей

Продолжение таблицы 10

Тип коммутатора	Управляемый коммутатор 2 уровня (или эквивалент)
Spanning Tree Protocol	Совместимость с 802.1D Spanning Tree 802.1w Rapid Spanning Tree 802.1s Multiple Spanning Tree Фильтрация BPDU для каждого порта
Рабочая температура	от +5 до 40 C
Температура хранения	-25 до 55 C
Влажность	От 5% до 95% без образования конденсата
Размеры	441 x 309 x 44 мм 19" - для установки в шкаф, 1 U высота

11.2 Общие требования к структурированной кабельной системе

Создаваемая структурированная кабельная система должна соответствовать стандартам TIA/EIA-568B и ISO 11801 и отвечать требованиям, предъявляемым к кабельным системам категории 5Е.

Оборудование в составе СКС должно обеспечивать постоянство физических характеристик канала между портом активного оборудования СКС и абонентским оборудованием вне зависимости от трассы коммутации на панелях переключения распределительных узлов.

Постоянство физических параметров канала должно обеспечиваться при последующих перекроссировках вне зависимости от их числа (но не более определенного производителем оборудования СКС).

Разрыв любого канала СКС возможен только при коммутации на панелях переключения распределительных узлов.

Используемые в СКС оборудование и материалы не должны допускать изменений физико-химических параметров в результате воздействия окружающей среды в течение всего гарантийного срока эксплуатации ЛВС

(не менее 20 лет) при условии соблюдения заданных производителем СКС условий эксплуатации.

В случае выхода из строя любого из каналов СКС должна обеспечиваться возможность перехода на использование альтернативного канала из числа резервных при помощи изменения соединений на панелях переключения распределительных узлов.

Должен быть ограничен доступ персонала объекта к оборудованию распределительных узлов.

Используемое оборудование и материалы не должны допускать возможности нанесения вреда здоровью или поражения персонала электрическим током, или электромагнитными излучениями при условии соблюдения правил эксплуатации оборудования.

На объекте должна обеспечиваться совместимость архитектурных, дизайнерских, технических и технологических решений, применяемых в рамках построения СКС.

Для реализации СКС на всех этапах должно применяться кабельное и коммутационное оборудование одного производителя для возможности сертификации СКС и постановки ее на долгосрочное гарантийное обеспечение (не менее 20 лет).

Применить унифицированные типы кабелей и разъемов в рамках рабочих мест, горизонтальной подсистемы, подсистем внутренних магистралей, а также распределительных узлов, вне зависимости от типов подключаемого абонентского оборудования и активного оборудования различных подсистем.

Обеспечить возможность увеличения абонентской емкости СКС за счет включения дополнительных линий горизонтальной подсистемы, без необходимости прокладки новых кабельных трасс, кабельных каналов, нарушения интерьера рабочих помещений, а также без остановки работы персонала объекта.

11.3 Требования к элементу структурированной кабельной системе

Структурированная кабельная система должна включать в себя объектовый распределительный узел.

Объектовый распределительный узел должен быть логическим центром СКС объекта и должен обеспечивать установку кроссового оборудования подсистем внутренних магистралей, активного оборудования, серверов и источников бесперебойного питания.

Объектовый распределительный узел должен размещаться в специализированном помещении с ограниченным доступом. Требования к объектному распределительному узлу приведены в таблице 11.

Таблица 11 - Требования к объектовому распределительному узлу

Шкаф напольный (или эквивалент)	
Количество (шт.)	1
Технические характеристики	
Высота (U)	42U (1U=4,445 см)
Горизонтальный установочный размер (дюйм)	19"
Высота (мм)	2 033
Ширина (мм)	800
Глубина (мм)	1 000
Передняя система замков	ригельный
Смотровое стекло	тонированное закаленное
Стенки	съёмные на защёлках и почтовых замках
Исполнение	напольный
Масса (кг)	171
Материал	сталь СТ08
Максимальная нагрузка (кг)	500
Уровень защиты	IP30
Дополнительное оборудование (или эквивалент)	
Полка	
Высота (мм)	25
Глубина (мм)	750
Горизонтальный установочный размер (дюйм)	19"

Продолжение таблицы 11

Дополнительное оборудование (или эквивалент)	
Метод крепления	к четырем направляющим шкафа
Грузоподъемность (кг)	100
Блок розеток (или эквивалент)	
Количество розеток (шт.)	8
Высота (U)	1U (1U=4,445 см)
Электропитание (В)	220
Тип розеток	с заземлением
Горизонтальный установочный размер (дюйм)	19"
Метод крепления	к двум направляющим шкафа
Дополнительные функции	возможность подключения к источнику бесперебойного питания
Пассивное оборудование СКС (или эквивалент)	
Коммутационная панель UTP (или эквивалент)	
Количество портов (шт.)	24, 48
Высота (U)	1U (1U=4,445 см)
Горизонтальный установочный размер (дюйм)	19"
Категория	5е
Тип	неэкранированный
Метод крепления	к двум направляющим шкафа
Поддерживаемые приложения	10BASE-T Ethernet 100BASE-TX Fast Ethernet 1000BASE-T Gigabit Ethernet
Соответствие стандартам	ANSI/TIA/EIA-568-B.2 ISO/IEC 11801 2 редакция, класс D и категория 5
Оптический кросс (или эквивалент)	
Количество портов (шт.)	32
Высота (U)	1U (1U=4,445 см)
Горизонтальный установочный размер (дюйм)	19"
Кабель	одномодовый

Распределительный узел входной группы должен представлять собой совокупность коммутационного оборудования, необходимого для функционирования рабочего места входной группы и турникетов.

Распределительный узел входной группы должен размещаться в запирающемся шкафу.

Коммутационные шнуры от коммутатора входной группы до турникетов изготавливаются по месту из экранированной фольгированной витой пары. Требования к распределительным узлам входной группы представлены в таблице 12.

Таблица 12 – Требования к распределительным узлам входной группы

Шкаф напольный	
Количество (шт.)	1
Технические характеристики	
Высота (U)	27U (1U=4,445 см)
Горизонтальный установочный размер (дюйм)	19"
Высота (мм)	1 365
Ширина (мм)	600
Глубина (мм)	800
Передняя система замков	ригельный
Смотровое стекло	тонированное закаленное
Стенки	съемные на защелках и почтовых замках
Исполнение	напольный
Масса (кг)	78
Материал	сталь СТ08
Максимальная нагрузка (кг)	350
Уровень защиты	IP30

Продолжение таблицы 12

Дополнительное оборудование	
Блок розеток	
Количество розеток (шт.)	8
Высота (U)	1U (1U=4,445 см)
Электропитание (В)	220
Тип розеток	с заземлением
Горизонтальный установочный размер (дюйм)	19"
Метод крепления	к двум направляющим шкафа
Дополнительные функции	возможность подключения к источнику бесперебойного питания
Пассивное оборудование	
Коммутационная панель UTP	
Количество портов (шт.)	24, 48
Высота (U)	1U (1U=4,445 см)
Горизонтальный установочный размер (дюйм)	19"
Категория	5е
Тип	неэкранированный
Тип разъема	RJ45
Поддерживаемые приложения	10BASE-T Ethernet 100BASE-TX Fast Ethernet 1000BASE-T Gigabit Ethernet
Соответствие стандартам	ANSI/TIA/EIA-568-B.2 ISO/IEC 11801 2 редакция, класс D и категория 5

Продолжение таблицы 12

Оптический кросс	
Количество портов (шт.)	4
Высота (U)	1U (1U=4,445 см)
Горизонтальный установочный размер (дюйм)	19"
Кабель	одномодовый
Тип розетки	SC
Ввод кабеля	вдоль задней стенки
Метод крепления	к двум направляющим шкафа
Поддерживаемые приложения	100BASE-FX Fast Ethernet 1000BASE-LX Gigabit Ethernet
Соответствие стандартам	TIA/EIA-942, TIA/EIA-604-5; IEC 61754-7, IEC 61300-4, Telcordia GR-326-CORE
Органайзер металлический (или эквивалент)	
Глубина колец (мм)	40
Высота (U)	1U (1U=4,445 см)
Горизонтальный установочный размер (дюйм)	19"
Метод крепления	к двум направляющим шкафа
Коммутационные шнуры	
Длины	зависит от дальности турникета
Категория	5e
Тип кабеля	SFTP экранированный фольгированный
Материал наружной оболочки	PVC
Количество пар	4

Продолжение таблицы 12

Тип разъема	RJ45/RJ45
Поддерживаемые приложения	10BASE-T Ethernet 100BASE-TX Fast Ethernet 1000BASE-T Gigabit Ethernet
Соответствие стандартам	ISO/IEC 11801, ANSI/TIA/EIA-568-B.2, ISO/IEC 11801 2 редакция, класс D и категория 5
Оптические коммутационные шнуры	
Длины	1,5м, 3м
Тип кабеля	Одномодовый
Тип разъема	SC-SC
Количество волокон	2
Поддерживаемые приложения	100BASE-FX Fast Ethernet 1000BASE-LX Gigabit Ethernet
Соответствие стандартам	IEC 60874-7 TIA/EIA-604-3A Telcordia GR-326-CORE

В шкафах должен обеспечиваться необходимый (не менее 50%) запас по свободному месту для установки дополнительного оборудования при увеличении числа рабочих мест.

Количество коммутационных шнуров для подключения рабочих мест к портам активного сетевого должно соответствовать количеству рабочих мест в зоне обслуживания распределительного узла.

11.4 Подсистема администрирования

Подсистема администрирования должна быть спроектирована таким образом, чтобы была точная маркировка (идентификация) всех компонентов, составляющих кабельную систему, а также кабельных трасс, телекоммуникационных шкафов и других частей структурированной кабельной системы.

Каждая метка должна быть долгоживущей, доступной и читаемой.

11.5 Подсистема электропитания рабочих мест

Подсистема электропитания должна обеспечивать рабочие места «чистым» электропитанием, независимым от основной электропроводки (освещение, бытовое оборудование, и т.д.).

Заземление розеток электропитания и оборудования ЛВС произвести по требованиям ПУЭ и международных стандартов.

Коммутационное оборудование электрических щитов и сами щиты системы электропитания должны быть промышленного назначения.

11.6 Тестирование параметров СКС

После проведения работ по монтажу СКС все кабели из неэкранированной витой пары проверяются на соответствие характеристикам, установленным для кабельных сетей категории 5е. Тестированию подвергаются все параметры, входящие в требования стандарта EIA/TIA 568B на характеристики каналов передачи данных выполненных кабелем неэкранированная витая пара для внутриофисных помещений.

Тестирование производится для каждого канала передачи данных. Канал передачи данных включает в себя: пассивное оборудование от абонентской розетки на рабочем месте, до порта на коммутационной панели в соответствующем кроссовом центре.

Результаты тестирования сохраняются до окончания работ и выдаются в печатном и электронном виде в форме развернутой таблицы.

11.7 Требования к документации по проектируемым системам

Документация должна включать в себя:

- эскизный проект по предложенным системам;
- пояснительную записку;
- планы размещения рабочих мест и кабельных трасс;
- структурные схемы СКС объектов;
- схемы размещения оборудования в телекоммуникационных шкафах;

- схемы маркировки коммутационных панелей;
- однолинейные схемы электропитания рабочих мест;
- схему топологии ЛВС.

12 Расположение оборудования в стойке

Размещение оборудования в стойке определяется на основе следующих правил:

- самые тяжелые вещи, такие как источник бесперебойного питания, размещаются на нижних полках;
- вентиляционные панели размещаются на верху стойки, либо где то ещё, если необходимо;
- консоли размещаются удобней с точки зрения эргономики;
- розеточные блоки размещаются с задней стороны;
- коммутационное оборудования, легкое, ставится наверх;
- самое теплое и тяжелое ставиться вниз.

Консоли размещаются, приблизительно, на расстоянии чуть больше метра от пола, чтобы специалисту удобно было выполнять настройки. Теплое оборудования устанавливается внизу стойки, так как теплый воздух поднимается вверх, соответственно холодное вверху стойки, так как холодный воздух опускается вниз.

Схема размещения оборудования в стойке представлена на рисунке 6.

Схема расположения стоек на объектах представлена на рисунке 7 и 8.

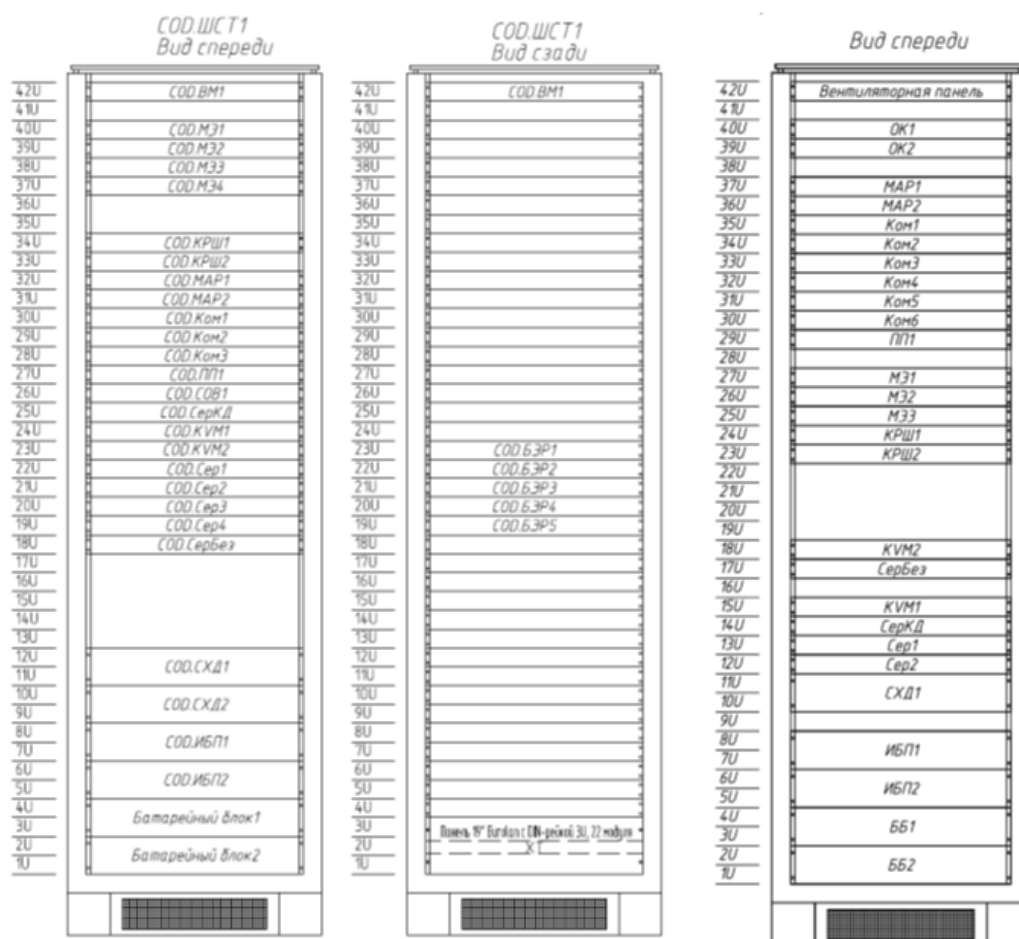


Рисунок 6 – Схема расположения оборудования в стойке

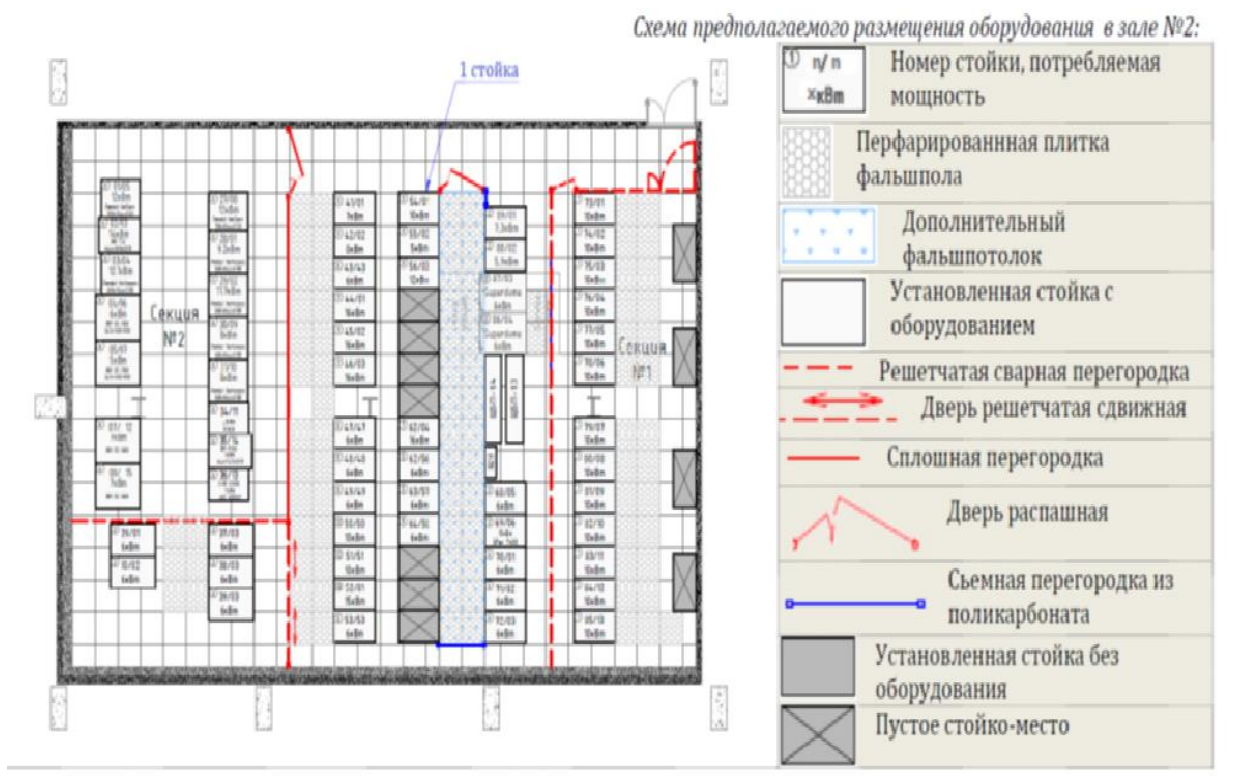


Рисунок 7 - Схема расположения стоек на объекте ЦСБД

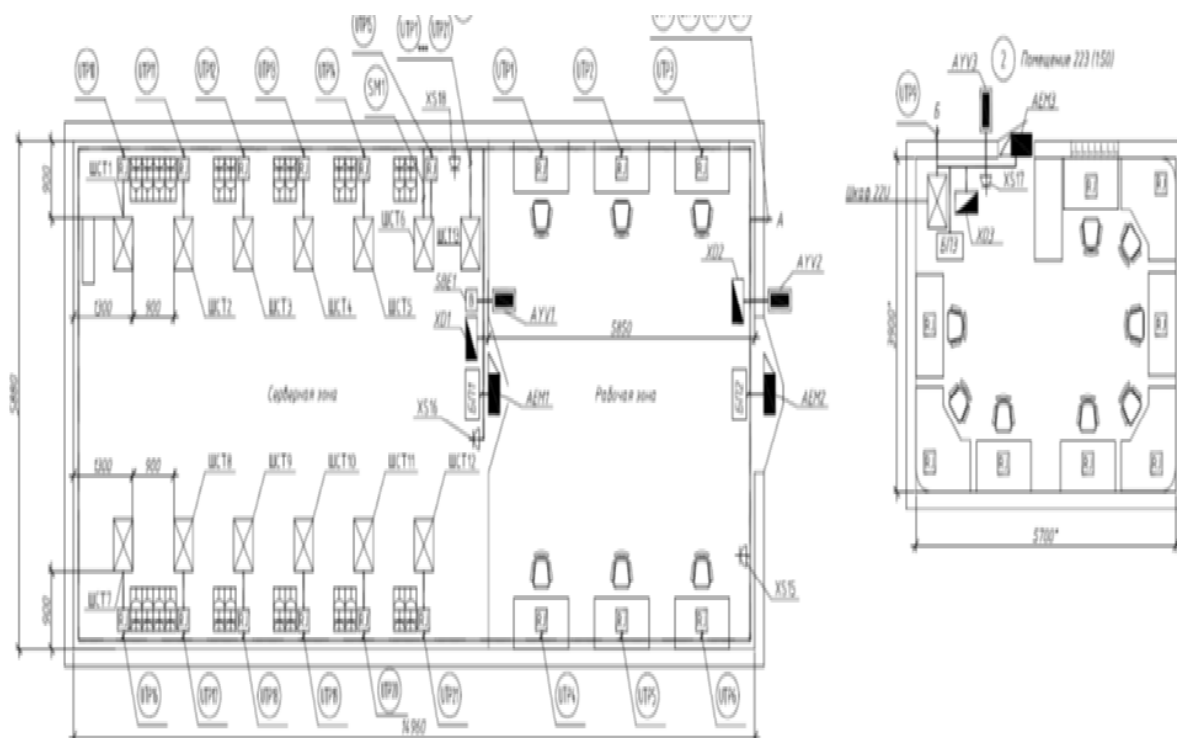


Рисунок 8 - Схема расположения стоек на объекте ЦУТП

13 Руководство администратора ИБ для сети передачи данных

13.1 В состав средств защиты информации входят:

1) средства криптографической защиты информации от НСД в каналах связи представляют собой комплекс СКЗИ, предназначенных для защиты информации в каналах связи, выходящих за пределы контролируемой зоны объектов размещения СКД. Комплекс включает:

- средство криптографической защиты информации программно-аппаратный комплекс «ViPNet Coordinator HW1000». Сертификат соответствия ФСБ России № СФ/515-1999, действует до 24.10.2017 г.;

- средство криптографической защиты информации программный комплекс «ViPNet Administrator 3.2». Сертификат соответствия ФСБ России № - СФ / 124-2861 действителен до 31.03.2018г.

2) средства защиты информации от НСД на периметре объектов обеспечивают контроль и фильтрацию потоков информации и обнаружение компьютерных атак на границах сетевой инфраструктуры объектов размещения СКД, а также сегментирование ЛВС объектов для обеспечения безопасного выхода в сеть Интернет. К ним относятся:

- межсетевой экран программно-аппаратный комплекс «ViPNet Coordinator HW1000». Сертификат соответствия ФСТЭК России № 2353, действует до 26.05.2017 г.;

- межсетевой экран ССПТ-2 версия 1.3. Сертификат соответствия ФСТЭК России в данный момент проходит сертификацию;

- система обнаружения компьютерных атак «Форпост» версия 2.0 (далее – СОКА «Форпост»). Сертификат соответствия ФСТЭК России № 2845, действует до 18.03.2019 г.;

На каждое АРМ (включая видеотерминалы) СКД заводится паспорт, который ведется администратором безопасности и содержит следующие сведения:

- о системном и специальном программном обеспечении (наименование ПО, версия);
- о составе технических средств (наименование, учетные номера блоков и устройств);
- о проводимом техническом обслуживании (ТО) (дата проведения очередного ТО, подпись исполнителя);
- о проводимых ремонтно-восстановительных и профилактических работах (наименование работы, дата выполнения, подписи исполнителей, администратора безопасности и принявшего восстановленное (прошедшее профилактику) изделие);
- о восстановлении работоспособности ПО, его обновлении и отладке;
- о вскрытии печатей и опечатывании оборудования АРМ (дата вскрытия (опечатывания), причина вскрытия, подпись администратора безопасности);
- о результатах выполнения регламентных работ по управлению ключевой системой (первоначальная установка и плановая смена ключей, действия при компрометации ключей).

Необходимый уровень безопасности информации в СКД обеспечивается:

- выполнением требований предписания на эксплуатацию СКД;
- выполнением требований предписаний на эксплуатацию технических средств СКД;
- применением комплекса программно-аппаратных средств защиты информации от несанкционированного доступа;
- выполнением настоящего Руководства администратором безопасности;
- выполнением требований нормативных документов ведомства.

13.2 Функции администратора безопасности информации

Деятельность пользователей АРМ СКД в части обеспечения безопасности информации осуществляется под руководством специально уполномоченного сотрудника - администратора информационной безопасности (администратор ИБ).

Администратором ИБ назначается сотрудник подразделения, обслуживающего СКД, изучивший данное Руководство и прошедший обучение по эксплуатации, управлению (администрированию) применяемых в СКД средств защиты информации):

- в объеме знаний пользователя АРМ СКД;
- в объеме знаний администратора средств межсетевого экранирования – МЭ ССПТ-2;
- в объеме знаний администратора ПАК ViPNet Coordinator HW 1000;
- в объеме знаний администратора системы обнаружения компьютерных атак «Форпост»;

Администратор ИБ должен быть назначен приказом по ОИ.

Администратор ИБ выполняет свои обязанности, руководствуясь настоящим Руководством и документами:

Эксплуатационной документацией на отдельные средства защиты информации:

- руководство администратора МЭ ССПТ-2 54323649.501410.00009-0134 РА;
- документация на изделие «Система обнаружения компьютерных атак «Форпост», версия 2.0 (включая, Программное обеспечение система обнаружения атак «ФОРПОСТ» Версия 2.0 Руководство по установке РМАГ.00026-20 91 01, Руководство по администрированию РМАГ.00026-20 92 01);
- руководство администратора средств криптографической защиты «ViPNet Coordinator HW1000»;

– руководство по использованию программных средств «ViPNet Administrator 3.2».

С целью непрерывности процесса работ по обеспечению безопасности информации целесообразно назначать администраторами ИБ нескольких сотрудников подразделения, эксплуатирующих ПЗИ на объектах.

Администратор ИБ выполняет следующие функции:

– производит настройку средств защиты информации;

– разрабатывает и реализует (устанавливает с помощью программно - аппаратных средств защиты) атрибуты контроля доступа на основе утвержденного порядка доступа пользователей СКД к техническим средствам СКД;

– обеспечивает внесение изменений в эксплуатационные документы по вопросам обеспечения безопасности информации (технические паспорта, отдельные инструкции, разрабатываемые в дополнение к настоящему Руководству) установленным порядком и доводит эти изменения до пользователей АРМ СКД;

– организует (в пределах своих полномочий) мероприятия по расследованию выявленных угроз безопасности информации в следующих случаях:

1) обнаружения атак на информационные ресурсы АРМ (сервера) СКД;

2) нарушения целостности ОС, ПО и файловой системы, заключающиеся в умышленной или неумышленной несанкционированной модификации состава и/или содержимого данных и/или программ, используемых на АРМ и серверах;

3) отказа системы защиты информации, в результате несанкционированных действий нарушителя в результате которых, нарушается свойство доступности некоторых информационных ресурсов (либо ресурсам в целом) СКД;

4) повреждения печати (гарантийной голографической наклейки) на системном блоке какого-либо АРМ или сервера, на печатаемых технических средствах и кабелеводах ЛВС;

- осуществляет общий контроль над выполнением требований предписаний на размещение, монтаж и эксплуатацию технических средств ПЗИ и нормативных документов по защите информации;

- создает новые, вносит изменения в существующие и удаляет неиспользуемые учетные записи пользователей;

- обеспечивает и контролирует соответствие состава программных средств АРМ комплектности, приведенной в паспорте АРМ, и их целостность;

- хранит и поддерживает в актуальном состоянии паспорта АРМ;

- ведет реестр выданных персональных идентификаторов пользователей;

- анализирует регистрационные протоколы работы средств защиты и операционной системы и в случае необходимости (при обнаружении фактов НСД) производит расследование;

- осуществляет периодический (рекомендуется не реже одного раза в неделю) анализ журнала событий безопасности СЗИ;

- осуществляет периодическое (рекомендуется не реже одного раза в две недели) тестирование средств защиты информации;

- при выявлении сбоев тестирования и неисправностей средств защиты информации администратор безопасности обязан выполнить действия по восстановлению их работоспособности в соответствии с эксплуатационной документацией разработчика СЗИ и настоящим Руководством;

- осуществляет плановую (с периодом 30 дней) и, при необходимости, экстренную смену действующих паролей пользователей;

- осуществляет, при необходимости, смену пароля отдельных пользователей;
- осуществляет первоначальную активизацию в полном объеме подсистемы контроля доступа;
- обеспечивает и отвечает за общую безопасность информации на объекте информатизации.

13.3 Применяемые средства защиты информации

В составе системы защиты информации применяются:

- средства криптографической защиты информации от НСД в каналах связи.
- средства защиты информации от НСД на периметре объектов.

В СКД для защиты каналов связи, которые незащищены от НСД к информации организационно-техническими мерами, используются изделия программно-аппаратный комплекс (ПАК) ViPNet Coordinator HW1000.

Изделие ПАК ViPNet Coordinator HW 1000 соответствует требованиям ФСБ России к СКЗИ класса KB2 и может использоваться для защиты информации, не содержащей сведений, составляющих государственную тайну (ФСБ России № СФ/515-1999, действует до 24.10.2017 г).

Для администрирования СКЗИ используется средства управления:

- программный комплекс ViPNet Administrator 3.2;
- криптошлюза гарантированной доставки обновлений (в т.ч. ключевой информации) на базе ПАК ViPNet Coordinator HW1000;

Средства защиты информации на периметре объектов обеспечивают контроль и фильтрацию потоков информации, обнаружение компьютерных атак на границах сетевой инфраструктуры объектов размещения СКД, а также сегментирование ЛВС объектов для обеспечения безопасного выхода в сеть Интернет. К ним относятся:

- межсетевой экран ССПТ-2 версия 1.3, соответствует требованиям ФСБ России к устройствам типа межсетевые экраны по 3 классу

защищенности и может использоваться для защиты информации от несанкционированного доступа в информационных и телекоммуникационных системах. Сертификат соответствия ФСТЭК России в данный момент проходит сертификацию;

- система обнаружения компьютерных атак «Форпост» версия 2.0 (СОКА «Форпост»). Сертификат соответствия ФСТЭК России № 2845, действует до 18.03.2019 г.;

13.4 Обязательные организационно-технические меры

Ограничение доступа абонентов, не являющихся пользователями СКЗИ, к каналам связи СКД проходящим внутри контролируемой зоны необходимо реализовать следующие меры:

- осуществлять прокладку кабелей в коробах;
- сформировать перечень лиц допущенных до работ с каналом связи;
- в случае возникновения технических неполадок (обрыв связи, ухудшение скорости передачи данных), необходимо осуществить контроль целостности.

Для предотвращения несанкционированного доступа в серверные помещения с размещенными СЗИ (МЭ, СОВ, СКЗИ) и непосредственно к оборудованию необходимо реализовать следующие меры:

- оснащение помещений системой контроля доступа (СКУД);
- в случае отсутствия данной системы устройством оборудование помещений предусмотреть опечатывающим;
- формирование списка лиц допущенных к оборудованию в соответствии с их обязанностями;
- опломбирование оборудования установленного в помещении;
- контроль выдачи ключей от помещения;
- доступ в помещение осуществляется в присутствии сотрудников СКЗИ;
- разработка матрицы прав доступа;
- разработка инструкций пользователей.

13.5 Управление средствами криптографической защиты информации от НСД в каналах связи

Средства криптографической защиты информации от НСД в каналах связи представляют собой комплекс СКЗИ, предназначенных для защиты информации в каналах связи, выходящих за пределы контролируемой зоны объектов размещения СКД. Комплекс включает:

- средство криптографической защиты информации программно-аппаратный комплекс ViPNet Coordinator HW1000;
- средство криптографической защиты информации программный комплекс ViPNet Administrator 3.2.

Функции, выполняемые Администратором ИБ в части управления средствами криптографической защиты информации изложены в п. 2.5 раздела 2.1 данного Руководства.

Администратор ИБ реализует функции по управлению средствами обеспечения защиты информации от НСД в каналах связи, руководствуясь положениями следующих эксплуатационных документов:

- Руководство администратора ПАК средство криптографической защиты ViPNet Coordinator HW1000;
- Руководство администратора.

Настройка криптографических средств защиты информации в каналах связи осуществляется в соответствии с эксплуатационной документацией на эти СЗИ.

13.6 Управление средствами защиты информации от НСД на периметре объектов

Средства защиты информации от НСД на периметре объектов обеспечивают контроль и фильтрацию потоков информации, и обнаружение компьютерных атак на границах сетевой инфраструктуры объектов размещения СКД, а также сегментирование ЛВС объектов для обеспечения безопасного выхода в сеть Интернет. К ним относятся:

- межсетевой экран программно-аппаратный комплекс ViPNet Coordinator HW1000;

- межсетевой экран ССПТ-2 версия 1.3;

- система обнаружения компьютерных атак «Форпост» версия 2.0;

Функции, выполняемые Администратором ИБ в части управления СЗИ от НСД на периметре объектов изложены в п. 2.5 раздела 2.1 данного Руководства.

Администратор ИБ реализует функции по управлению средствами ЗИ от НСД на периметре, руководствуясь положениями следующих эксплуатационных документов:

- руководство администратора ПАК средство криптографической защиты ViPNet Coordinator HW1000;

- документация на изделие «Система обнаружения компьютерных атак «Форпост», версия 2.0 (включая, Программное обеспечение система обнаружения атак «ФОРПОСТ» Версия 2.0 Руководство по установке РМАГ.00026-20 91 01, Руководство по администрированию РМАГ.00026-20 92 01);

- «Межсетевой экран ССПТ-2. Руководство администратора»;

Настройка СЗИ от НСД на периметре объектов осуществляется в соответствии с эксплуатационной документацией на эти СЗИ.

13.7 Порядок действий администратора безопасности при установке программного обеспечения

Программное обеспечение, установленное на средства вычислительной техники АРМ СКД, является фиксированным и должно строго соответствовать составу ПО, приведенному в рабочей документации на АРМ, паспорту на АРМ и предписанию на эксплуатацию СКД, выданному по результатам аттестационных испытаний.

Запрещено:

- самостоятельно вносить изменения в состав ПО (как общесистемного, так и специального);
- устанавливать ПО, которое не указано в паспорте на АРМ.

В случае необходимости восстановления работоспособности и отладки программного обеспечения (после ремонта технических средств либо сбоев, вызвавших отказ ПО) допускается его переустановка только с дистрибутивов, хранящихся у администратора ИБ.

При проведении работ, связанных с установкой и наладкой программных средств, входящих в состав АРМ СКД, запрещается использование внешних МНИ, позволяющие осуществлять запись информации (USB, CD/DVD-RW и т.д.). Установка программного обеспечения должна осуществляться только с носителей типа CD/DVD-R.

При необходимости изменения состава программного обеспечения, администратором безопасности организуется обращение в Центр по лицензированию, сертификации и защите государственной тайны ФСБ России для проведения соответствующих исследований и/или получения разрешения на пополнение/изменение ПО в СКД.

О всех производимых разрешенных изменениях программного обеспечения администратор безопасности делает запись в паспорте соответствующего АРМ.

В случае выявления факта несанкционированного изменения или установки ПО, не соответствующего паспортным данным на АРМ, администратор безопасности инициирует служебное расследование.

13.8 Порядок работы с печатными документами и внешними машинными носителями информации

Выдача информации на печать производится с АРМ пользователей и используется для работы с «твердыми» копиями документов.

Максимальный гриф, присваиваемый документам, обрабатываемым в КСОБ и хранящимся на бумажных носителях – «для служебного пользования».

Порядок учета и работы с печатными документами определяется на ОИ.

В качестве внешних МНИ, для проведения работ пользователями, используются выдаваемые (под роспись) на ОИ МНИ типа CD-R или DVD-R, а также flash-накопители.

Хранение и использование МНИ на объектах должно осуществляться в условиях, исключающих несанкционированное копирование информации, их хищение, изменение или уничтожение содержащейся на них информации. Доступ к индивидуальным внешним МНИ лиц, не являющихся пользователями СКД, должен быть исключен.

13.9 Действия в случае обнаружения угроз безопасности информации

В случае обнаружения угроз безопасности информации работа на АРМ СКД должна быть прекращена, далее проводятся мероприятия по оценке влияния выявленных нарушений на безопасность информации, обрабатываемой на АРМ и АС в целом.

По факту обнаруженной угрозы информационной безопасности, установленным порядком, назначается комиссия для проведения служебного расследования.

Председателем комиссии в зависимости от степени угрозы информационной безопасности СКД распоряжением руководителя объекта

информатизации назначается ответственное должностное лицо или администратор безопасности.

В ходе служебного расследования организуются работы по выявлению в АРМ и серверах СКД вредоносных программных средств скрытого воздействия на программные и информационные среды.

Работа комиссии может проводиться с привлечением (при необходимости) уполномоченных представителей организаций-разработчиков СКД и организаций, ведущих сопровождение работоспособности оборудования, системного и специального ПО.

Служебное расследование завершается актом (протоколом), в котором указываются проведенные работы, выявленные нарушения, причины, которые привели к реализации угрозы, нанесенный информационный ущерб и меры, принятые по устранению данной угрозы и информационного ущерба.

Акт подписывается председателем и членами комиссии, а затем утверждается руководителем объекта информатизации Ведомства.

Решение о возобновлении работы на АРМ СКД принимает ответственное должностное лицо объекта информатизации Ведомства на основе результатов работы комиссии по расследованию и устранению причин угрозы информационной безопасности. Копии акта расследования и распоряжения ответственного должностного лица объекта информатизации Ведомства о возобновлении работы на АРМ СКД.

Запрещается в процессе эксплуатации ПЗИ СКД:

- осуществлять несанкционированный доступ и модификацию учетной базы программных средств защиты информации;
- подключать к сетевым розеткам ЛВС технические средства, не входящие в состав технических средств СКД;
- подключать к ПЭВМ дополнительные устройства без соответствующего предписания на возможность их эксплуатации в составе СКД;

- работать на АРМ, если во время начальной загрузки не проходят встроенные тесты, предусмотренные средствами ЗИ, в том числе защиты от НСД;
- оставлять без контроля во включенном состоянии АРМ без активации штатной функции блокировки ОС и выключения питания монитора;
- осуществлять нештатное вскрытие системных блоков ПЭВМ;
- производить модификацию состава программного обеспечения АРМ СКД с нарушением установленного порядка;
- использовать не имеющее разрешения на эксплуатацию ПО;
- работать на АРМ при обнаружении нарушений целостности печатей, несанкционированного изменения конфигурации АРМ, неисправности технических средств АРМ;
- работать на АРМ лицам, не отданных приказом как пользователей АРМ, не прошедших инструктаж перед началом работ и не принявших АРМ по описи;
- использовать неучтенные МНИ и учтенные МНИ, не прошедшие антивирусную проверку.

ЗАКЛЮЧЕНИЕ

В результате выполнения дипломной работы была разработана защищенная сеть передачи данных распределенной ИСПДн.

В процессе дипломного проектирования были выполнены следующие этапы:

- определение способов организации сети;
- расчет требуемой пропускной способности;
- разработка требований к сети передачи данных;
- разработка схем подключения объектов информатизации ИСПДн к сети передачи данных;
- анализ рынка средств защиты информации для обеспечения защищенности сети передачи данных;
- настройка работы оборудования сети передачи данных распределенной ИСПДн;
- разработка организационных требований;
- разработка технических требований;
- расположение оборудования в стойке и на объекте;
- руководство администратора ИБ для данной сети.

Требования технического задания на дипломное проектирование выполнено в полном объеме.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 Федеральный закон от 27.07.2006 N 152-ФЗ (ред.от 05.04.2013) «О персональных данных».

2 Федеральный закон от 27.07.2006 N 149-ФЗ (ред. от 06.04.2011) «Об информации, информационных технологиях и о защите информации».

3 Постановление Правительства РФ от 01.11.2012 N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

4 Приказ ФСТЭК России от 18 февраля 2013 г. N 21 «Об утверждении Составы и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

5 Приказ ФСТЭК России от 11.02.2013 N 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» (Зарегистрировано в Минюсте России 31.05.2013 N 28608).

6 Межсетевой экран ССПТ-2. Руководство администратора. (54323649.501410.00009-0134 РА).

7 ViPNet Administrator Центр управления сетью. Руководство администратора. (ФРКЕ.00006-05 32 01).

ПРИЛОЖЕНИЕ А

(обязательно)

Настройка МЭ для спортивных объектов ССПТ-2

Для настройки необходимо подключиться к ССПТ-2 через системную консоль. Для этого необходимо подключить VGA-монитор и клавиатуру к разъемам ССПТ-2 и включить питание. После загрузки операционной системы на ССПТ-2 на экран выведется информация о состоянии ССПТ-2 и приглашение на вход пользователя (рисунок 9).

```
Оперативная память: 1062797312 байт (1013M)
Всего интерфейсов: 6
  Фильтрующих интерфейсов: 5: eth0,eth1,eth2,eth3,eth4
  Управляющий интерфейс:  включен,192.168.23.10/255.255.255.0
Версия ПО ССПТ-2: 1.3 (FNP2_RELEASE_1_3)
Пакетный фильтр:  запущен
Сервер авторизации:  запущен
Сервер проверки контрольных сумм:  запущен
Сервер высокой готовности:  запущен
Сервер регистрации:  запущен
Командный сервер:  запущен
Сервер терминального доступа:  запущен
WEB интерфейс:  остановлен
Starting cron.
Local package initialization:.
Starting background file system checks in 60 seconds.

Thu Nov 24 09:23:24 GMT 2016

FreeBSD/i386 (fnp2) (ttyv0)
```

Рисунок 9 – Информация о состоянии ССПТ-2

Далее нужно пройти два уровня авторизации пользователя и получить доступ к командному интерфейсу администратора. Пример авторизации пользователя в командном интерфейсе администратора ССПТ-2 с системной консоли приведен на рисунке 10. Ввод паролей на терминале не отображается.

```

Nov 24 09:23:53 fnp2 kernel: arp: 28:bb:c8:06:2e:c8 is using my IP address 192.
68.23.10 on em0!
fnpsh
Password:
Last login: Fri Nov 18 11:18:12 on ttyv0
Copyright (c) 1992-2009 The FreeBSD Project.
Copyright (c) 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994
The Regents of the University of California. All rights reserved.

Межсетевой экран ССПТ-2
(с) ЗАО "НПО РТК", 2006-2011

Межсетевой экран ССПТ-2
Командный интерфейс, версия 1.3
(с) ЗАО "НПО РТК", 2000-2010. Все права защищены

Имя пользователя: Nov 24 09:24:24 fnp2 last message repeated 33 times
admin
Пароль:

FNPSH-I-3001-Успешная авторизация пользователя
fnpsh>

```

Рисунок 10 – Авторизация пользователя с системной консоли ССПТ-2

Следующим этапом настройки является добавление в список доступа к ССПТ-2 диапазон IP-адресов 192.168.23.1 – 192.168.23.15 входящих в подсеть. Пример добавления в список доступа диапазон IP-адресов представлен на рисунке 11.

```

fnpsh> interface control acl show
Список доступа:
Всего записей: 0 Свободных позиций: 16
fnpsh> interface control acl add 192.168.23.1-192.168.23.15
FNPSH-I-302F-Новая запись добавлена в список доступа
fnpsh> interface control acl show
Список доступа:
1 192.168.23.1-192.168.23.15
Всего записей: 1 Свободных позиций: 15
fnpsh>

```

Рисунок 11 – Добавление списка доступа к ССПТ-2

Адрес подключенного ССПТ-2 определен как 192.168.23.9.

Так же необходимо установить скорость передачи управляемого интерфейса в автоматический режим. Результаты предварительной настройки представлены на рисунке 12.

```

Настроено :
Состояние:      включено
Адрес:          192.168.23.9
Маска:          255.255.255.0
Скорость:       autoselect
Список доступа: 192.168.23.1-192.168.23.15

Определено :
Состояние:      включено
Адрес:          192.168.23.9
Маска:          255.255.255.0
Скорость:       100baseTX/full-duplex
Несущая:        активна
fnpsh>

```

Рисунок 12 – Предварительные настройки

Далее нужно включить все фильтрующие элементы, имеющие в ССПТ-2. Установить автоматическую скорость передачи фильтрующего элемента. Пример работы фильтров представлен на рисунке 13. Из рисунка 13 видно, что ССПТ-2 использует первые два интерфейса Eth0 и Eth1.

```

fnpsh> interface control enable
FNPSH-I-3054-Управляющий интерфейс включен
fnpsh> interface filter enable Eth0
FNPSH-E-1024-Фильтрующий интерфейс с заданным именем не найден (enable)
fnpsh> interface filter Eth0 enable
FNPSH-E-1024-Фильтрующий интерфейс с заданным именем не найден (Eth0)
fnpsh> interface filter eth0 enable
FNPSH-I-3027-Фильтрующий интерфейс включен (eth0)
fnpsh> interface filter show
FNPSH-E-1024-Фильтрующий интерфейс с заданным именем не найден (show)
fnpsh> interface filter all show

```

Интерфейс	Настроено			Определено		
	Сост.	Скорость	Зеркалиро.	Сост.	Скорость	Несуща
0:eth0	вкл.	auto	откл.	вкл.	1000baseTX full-dup.	да
1:eth1	вкл.	auto	откл.	вкл.	100baseTX full-dupl.	да
2:eth2	вкл.	auto	откл.	вкл.		нет
3:eth3	вкл.	auto	откл.	вкл.		нет
4:eth4	вкл.	auto	откл.	вкл.		нет

```

fnpsh>

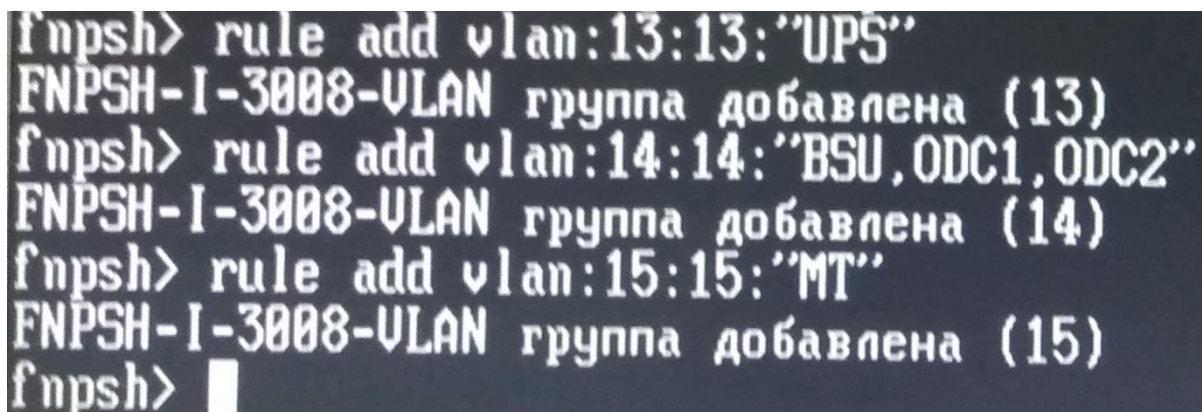
```

Рисунок 13 – Работа фильтров ССПТ-2

Для запрета или разрешения фильтрации VLAN-группы или ip-адреса необходимо создать ряд правил. Для начало нужно создать три VLAN-группы:

- группа №13 состоящая из УПС;
- группа №14 состоящая из БСУ и ОДЦ;
- группа №15 состоящая из МТ.

Результат представлен на рисунке 14.



```
fnpsh> rule add vlan:13:13:"UPS"
FNPSH-I-3008-VLAN группа добавлена (13)
fnpsh> rule add vlan:14:14:"BSU,ODC1,ODC2"
FNPSH-I-3008-VLAN группа добавлена (14)
fnpsh> rule add vlan:15:15:"MT"
FNPSH-I-3008-VLAN группа добавлена (15)
fnpsh>
```

Рисунок 14 – Добавление VLAN-групп

Необходимо создать правила для VLAN-групп, в соответствии с таблицей 8, такие, что разрешали передачу пакетов через защищенные интерфейсы Eth0 и Eth1 всем, из приведенных выше, группам VLAN по протокол ICMP и UDP через порты 161, 162 и 80 соответственно (рисунок 15).

```

fnpsh> rule add ip:1 action=accept in=eth0 VLAN=13 protocol=icmp
FNPSH-I-300B-IP правило добавлено (1)
fnpsh> rule add ip:2 action=accept in=eth0 VLAN=14 protocol=icmp
FNPSH-I-300B-IP правило добавлено (2)
fnpsh> rule add ip:3 action=accept in=eth0 VLAN=15 protocol=icmp
FNPSH-I-300B-IP правило добавлено (3)
fnpsh> rule add ip:3 action=accept in=eth0 VLAN=15 protocol=icmp
FNPSH-E-1055-IP правило уже существует
fnpsh> rule add ip:4 action=accept in=eth0 VLAN=13 dastport=80
FNPLIB-E-1000-Недопустимые параметры (dastport)
fnpsh> rule add ip:4 action=accept in=eth0 VLAN=13 dstport=80
FNPSH-I-300B-IP правило добавлено (4)
fnpsh> rule add ip:5 action=accept in=eth0 VLAN=14 dstport=80
FNPSH-I-300B-IP правило добавлено (5)
fnpsh> rule add ip:6 action=accept in=eth0 VLAN=15 dstport=80
FNPSH-I-300B-IP правило добавлено (6)
fnpsh>

```

Рисунок 15 – Добавление правил для VLAN-групп

Следующим шагом нужно установить правила для разрешения передачи пакетов по ip-адресам для каждого периферийного устройства. Условия разрешения передачи пакетов устанавливается в соответствии с таблицей 9. Текст настройки и результат написания всех правил представлены на рисунке 16,17,18,19.

```

fnpsh> rule add ip:8 action=accept in=eth0 srcip=192.168.135.1 protocol=icmp
FNPSH-I-300B-IP правило добавлено (8)
fnpsh> rule add ip:9 action=accept in=eth0 srcip=192.168.135.2 protocol=icmp
FNPSH-I-300B-IP правило добавлено (9)
fnpsh> rule add ip:10 action=accept in=eth0 srcip=192.168.135.2 dstport=80
FNPSH-I-300B-IP правило добавлено (10)
fnpsh> rule add ip:11 action=accept in=eth0 srcip=192.168.132.1 dstport=80
FNPSH-I-300B-IP правило добавлено (11)
fnpsh> rule add ip:11 action=accept in=eth0 srcip=192.168.132.1 protocol=icmp
FNPSH-E-1055-IP правило уже существует
fnpsh> rule add ip:12 action=accept in=eth0 srcip=192.168.132.1 protocol=icmp
FNPSH-I-300B-IP правило добавлено (12)
fnpsh> rule add ip:13 action=accept in=eth0 srcip=192.168.130.1 protocol=icmp
FNPSH-I-300B-IP правило добавлено (13)
fnpsh> rule add ip:13 action=accept in=eth0 srcip=192.168.130.1 dstport=80
FNPSH-E-1055-IP правило уже существует
fnpsh> rule add ip:14 action=accept in=eth0 srcip=192.168.130.1 dstport=80
FNPSH-I-300B-IP правило добавлено (14)
fnpsh> rule add ip:15 action=accept in=eth0 srcip=192.168.130.2 dstport=80
FNPSH-I-300B-IP правило добавлено (15)
fnpsh> rule add ip:15 action=accept in=eth0 srcip=192.168.130.2 protocol=icmp
FNPSH-E-1055-IP правило уже существует
fnpsh> rule add ip:16 action=accept in=eth0 srcip=192.168.130.2 protocol=icmp
FNPSH-I-300B-IP правило добавлено (16)
fnpsh> █

```

Рисунок 16 – Добавления правил для ip адресов

```

fnpsh> rule add ip:14 action=accept in=eth0 srcip=192.168.130.1 dstport=80
FNPSH-I-300B-IP правило добавлено (14)
fnpsh> rule add ip:15 action=accept in=eth0 srcip=192.168.130.2 dstport=80
FNPSH-I-300B-IP правило добавлено (15)
fnpsh> rule add ip:15 action=accept in=eth0 srcip=192.168.130.2 protocol=icmp
FNPSH-E-1055-IP правило уже существует
fnpsh> rule add ip:16 action=accept in=eth0 srcip=192.168.130.2 protocol=icmp
FNPSH-I-300B-IP правило добавлено (16)
fnpsh> rule add ip:17 action=accept in=eth0 srcip=192.168.129.100 protocol=icmp
FNPSH-I-300B-IP правило добавлено (17)
fnpsh> rule add ip:18 action=accept in=eth0 srcip=192.168.129.100 dstport=80
FNPSH-I-300B-IP правило добавлено (18)
fnpsh> rule add ip:19 action=accept in=eth0 srcip=192.168.129.101 dstport=80
FNPSH-I-300B-IP правило добавлено (19)
fnpsh> rule add ip:19 action=accept in=eth0 srcip=192.168.129.101 protocol=icmp
FNPSH-E-1055-IP правило уже существует
fnpsh> rule add ip:20 action=accept in=eth0 srcip=192.168.129.101 protocol=icmp
FNPSH-E-1055-IP правило уже существует
fnpsh> rule add ip:20 action=accept in=eth0 srcip=192.168.129.101 protocol=icmp
FNPSH-I-300B-IP правило добавлено (20)
fnpsh> █

```

Рисунок 17 – Добавления правил для ip-адресов

```

vlan:13:13:"UPS"
vlan:14:14:"BSU,ODC1,ODC2"
vlan:15:15:"MT"
mac:0:accept:nolog
arp:0:accept:nolog
ip:0:drop:nolog
ip:1:accept:nolog:0:1:0:icmp:any:any:any:161,162:any:any:any:any:any:active:
ip:2:accept:nolog:0:1:0:icmp:any:any:any:161,162:any:any:any:any:any:active:
ip:3:accept:nolog:0:1:0:icmp:any:any:any:161,162:any:any:any:any:any:active:
ip:4:accept:nolog:0:1:0:any:any:any:any:80:any:any:any:any:any:active::13:de
ip:5:accept:nolog:0:1:0:any:any:any:any:80:any:any:any:any:any:active::14:de
ip:6:accept:nolog:0:1:0:any:any:any:any:80:any:any:any:any:any:active::15:de
ip:7:accept:nolog:0:1:0:any:192.168.135.1:any:any:80:any:any:any:any:any:act
ip:8:accept:nolog:0:1:0:icmp:192.168.135.1:any:any:161,162:any:any:any:any:a
ip:9:accept:nolog:0:1:0:icmp:192.168.135.2:any:any:161,162:any:any:any:any:a
ip:10:accept:nolog:0:1:0:any:192.168.135.2:any:any:80:any:any:any:any:any:ac
ip:11:accept:nolog:0:1:0:any:192.168.132.1:any:any:80:any:any:any:any:any:ac
ip:12:accept:nolog:0:1:0:icmp:192.168.132.1:any:any:161,162:any:any:any:any:
ip:13:accept:nolog:0:1:0:icmp:192.168.130.1:any:any:161,162:any:any:any:any:
ip:14:accept:nolog:0:1:0:any:192.168.130.1:any:any:80:any:any:any:any:any:ac
ip:15:accept:nolog:0:1:0:any:192.168.130.2:any:any:80:any:any:any:any:any:ac
ip:16:accept:nolog:0:1:0:icmp:192.168.130.2:any:any:161,162:any:any:any:any:
ip:17:accept:nolog:0:1:0:icmp:192.168.129.100:any:any:161,162:any:any:any:an

```

Строки: 1-23 из 27 Столбцы: 1-80 H - справка Q, F10 - выход

Рисунок 18 – Результат установленных правил

```

ip:0:drop:nolog
ip:1:accept:nolog:0:1:0:icmp:any:any:any:161,162:any:any:any:any:any:active
ip:2:accept:nolog:0:1:0:icmp:any:any:any:161,162:any:any:any:any:any:active
ip:3:accept:nolog:0:1:0:icmp:any:any:any:161,162:any:any:any:any:any:active
ip:4:accept:nolog:0:1:0:any:any:any:any:80:any:any:any:any:any:active::13:de
ip:5:accept:nolog:0:1:0:any:any:any:any:80:any:any:any:any:any:active::14:de
ip:6:accept:nolog:0:1:0:any:any:any:any:80:any:any:any:any:any:active::15:de
ip:7:accept:nolog:0:1:0:any:192.168.135.1:any:any:80:any:any:any:any:any:act
ip:8:accept:nolog:0:1:0:icmp:192.168.135.1:any:any:161,162:any:any:any:any:a
ip:9:accept:nolog:0:1:0:icmp:192.168.135.2:any:any:161,162:any:any:any:any:a
ip:10:accept:nolog:0:1:0:any:192.168.135.2:any:any:80:any:any:any:any:any:ac
ip:11:accept:nolog:0:1:0:any:192.168.132.1:any:any:80:any:any:any:any:any:ac
ip:12:accept:nolog:0:1:0:icmp:192.168.132.1:any:any:161,162:any:any:any:any:
ip:13:accept:nolog:0:1:0:icmp:192.168.130.1:any:any:161,162:any:any:any:any:
ip:14:accept:nolog:0:1:0:any:192.168.130.1:any:any:80:any:any:any:any:any:ac
ip:15:accept:nolog:0:1:0:any:192.168.130.2:any:any:80:any:any:any:any:any:ac
ip:16:accept:nolog:0:1:0:icmp:192.168.130.2:any:any:161,162:any:any:any:any:
ip:17:accept:nolog:0:1:0:icmp:192.168.129.100:any:any:161,162:any:any:any:an
ip:18:accept:nolog:0:1:0:any:192.168.129.100:any:any:80:any:any:any:any:any:
ip:19:accept:nolog:0:1:0:any:192.168.129.101:any:any:80:any:any:any:any:any:
ip:20:accept:nolog:0:1:0:icmp:192.168.129.101:any:any:161,162:any:any:any:an
ipx:0:drop:nolog

```

Рисунок 19 – Результат установленных правил

Для всех остальных соединений установить запрет на передачу пакетов.

Для работы двух ССПТ-2 одновременно с одинаковыми настройками необходимо их синхронизировать. Для этого нужно выставить одинаковую скорость на обоих межсетевых экранах и коммутаторах, для каждого ССПТ-2 был установлен ip-адрес смежного ССПТ-2 и для одного из них бы установлен режим “master”- режим основного устройства, а для другого “slave” – режим резервного устройства. Результаты настройки представлены на рисунках 20, 21, 22, 23.

```
fnpsh> reserv neighbour 192.168.23.9
FNPSH-I-3081-IP-адрес смежного устройство изменен
fnpsh> reserv mode master
FNPSH-I-307E-Режим резервирования изменен
fnpsh> reserv enable
FNPSH-I-307F-Резервирование включено
fnpsh> █
```

Рисунок 20 – Настройка резервного ССПТ-2

```
fnpsh> reserv neighbour 192.168.23.10
FNPSH-I-3081-IP-адрес смежного устройство изменен
fnpsh> reserv mode slave
FNPSH-I-307E-Режим резервирования изменен
fnpsh> reserv enable
FNPSH-I-307F-Резервирование включено
fnpsh> █
```

Рисунок 21 – Настройка основного ССПТ-2

```

fnpsh> reserv show
Резервирование:                включено
Режим:                          MASTER (активный)
Смежное устройство:
    IP-адрес:                    192.168.23.9
    Режим:                      Аппаратный отказ (недоступно)
Интерфейсы в активном состоянии: 100baseTX / full-duplex
Интерфейсы в заблокированном состоянии: 10baseT/UTP / half-duplex
fnpsh>

```

Рисунок 22 – Результат настройки резервирования основного ССПТ-2

```

fnpsh> reserv show
Резервирование:                включено
Режим:                          SLAVE (резервный)
Смежное устройство:
    IP-адрес:                    192.168.23.10
    Режим:                      master (активный)
Интерфейсы в активном состоянии: 100baseTX / full-duplex
Интерфейсы в заблокированном состоянии: 10baseT/UTP / full-duplex
fnpsh>

```

Рисунок 23 – Результат настройки резервирования резервного ССПТ-2

ПРИЛОЖЕНИЕ Б

(обязательно)

Настройка работы криптошлюза VIPNet Coordinator HW1000

Настройка криптошлюза осуществляется при помощи приложения VIPNet Administrator Центр управления сетью.

Первым шагом в настройке необходимо внести все имеющиеся данные. Наша сеть имеет 26 подсетей, в каждой подсети по 2 криптошлюза, т.е. в сети всего 52 криптошлюза. Абонентских пунктов (АП) в сети нет. Это указывается в разделе генерации подсистем, представленном на рисунке 24.

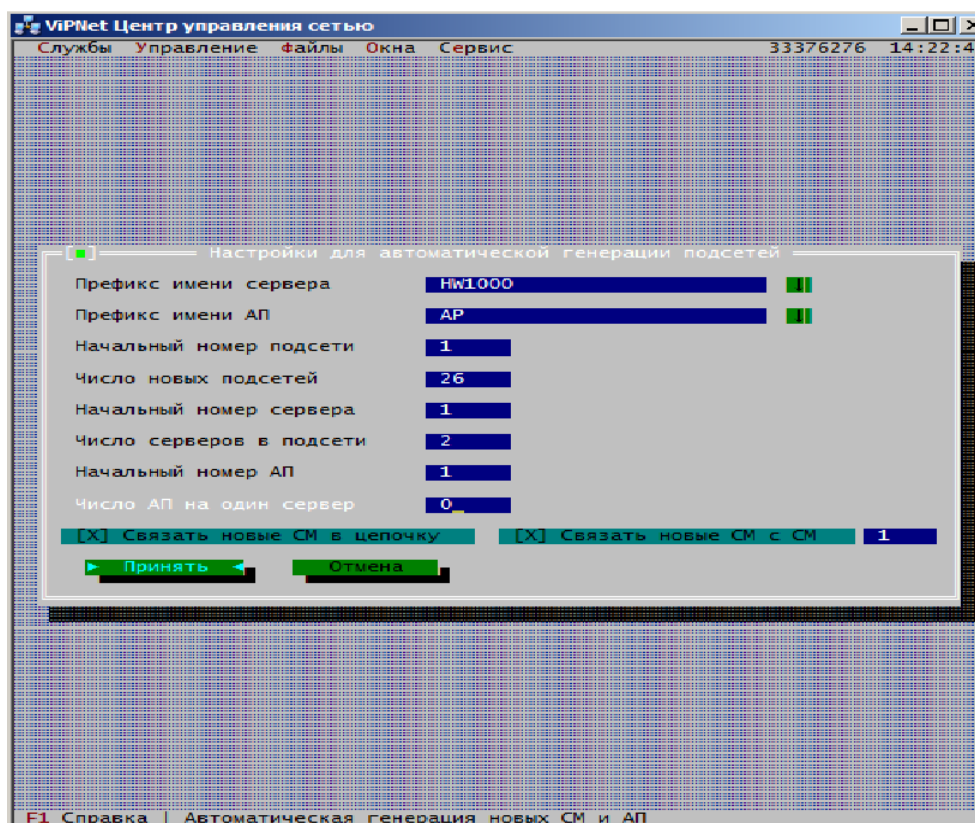


Рисунок 24 – Генерация подсистем

Далее нужно пройти в раздел структуры сети VIPNet. В этом разделе нам предоставляют информацию о существующих серверах, АП, серверо – маршрутизаторных каналов и групп. При прохождении в раздел «серверы-маршрутизаторы» на экран выведется информация о существующих серверах-маршрутизаторов, а конкретно: их имена, номер, кол-во АП на этом сервере-маршрутизаторе, идентификатор и их состоянии, включены они или отключены. Окно «серверы и маршрутизаторы» представлено на рисунке 25.

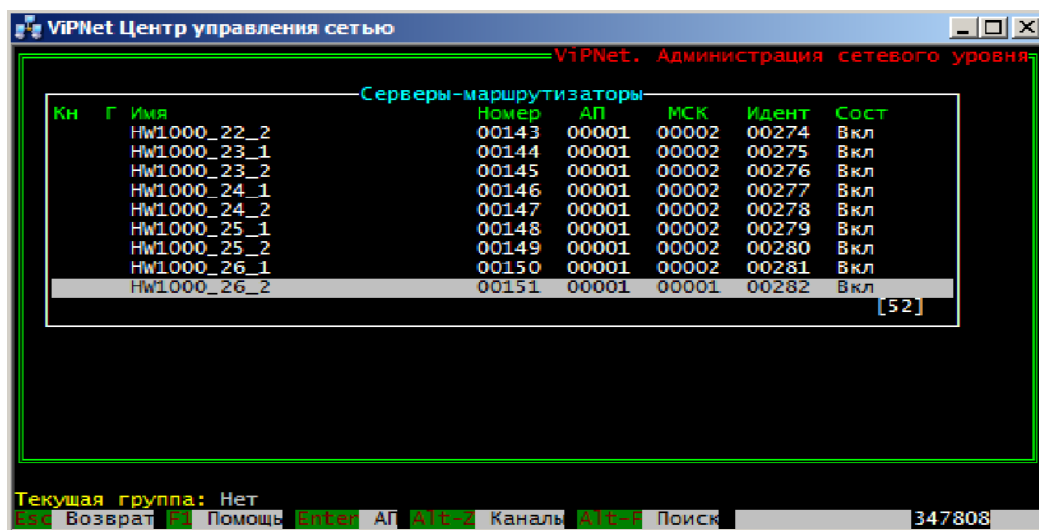


Рисунок 25 – Серверы и маршрутизаторы

Следующим шагом нужно создать межсерверные каналы между всеми криптошлюзами. Для этого нужно пройти во вкладку межсерверные каналы и создать каналы связи между всеми имеющимися криптошлюзами. Результат создания межсерверных каналов представлен на рисунке 26. После этих действий структура сети выглядит так, как показано на рисунке 27.

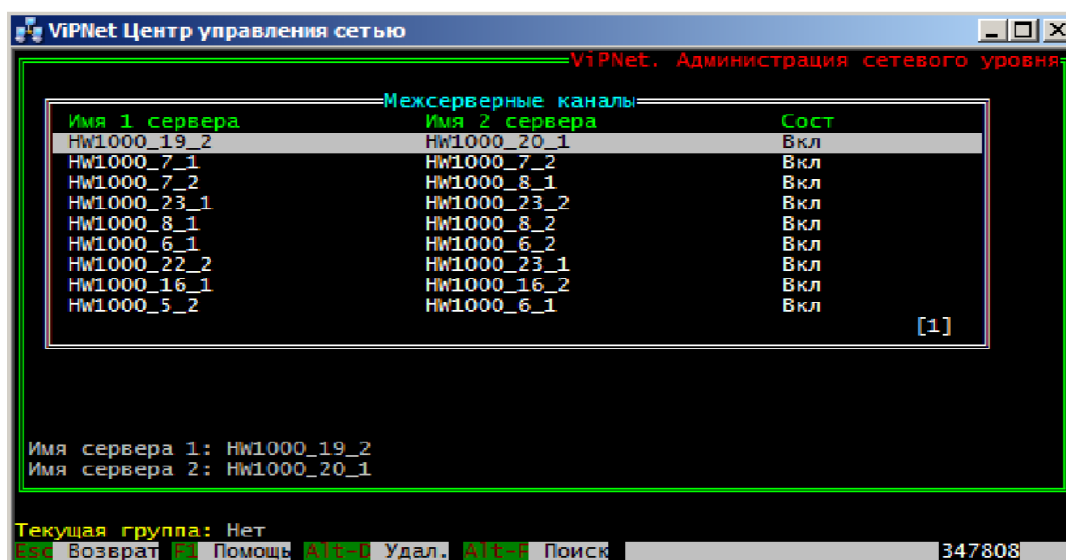


Рисунок 26 – Межсерверные каналы

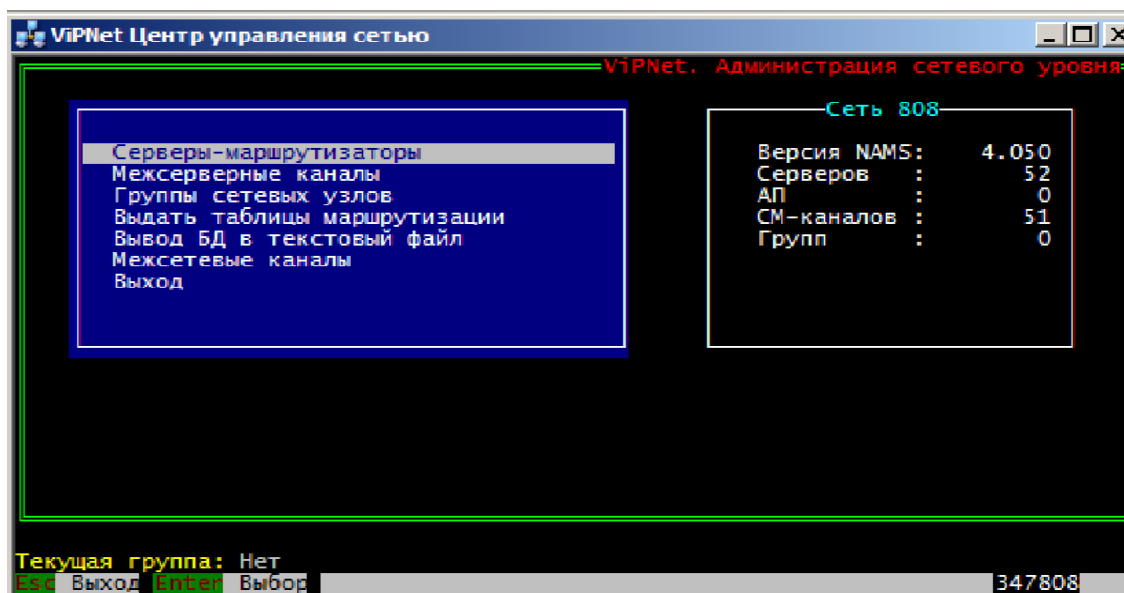


Рисунок 27 – Структура сети

Далее нужно каждому криптошлюзу назначить свой ip-адрес во внешней сети. Для этого во вкладки «управления внешними адресами» указываем для каждого криптошлюза ip-адрес. Результат выполнения данных действий приведен на рисунках 28.

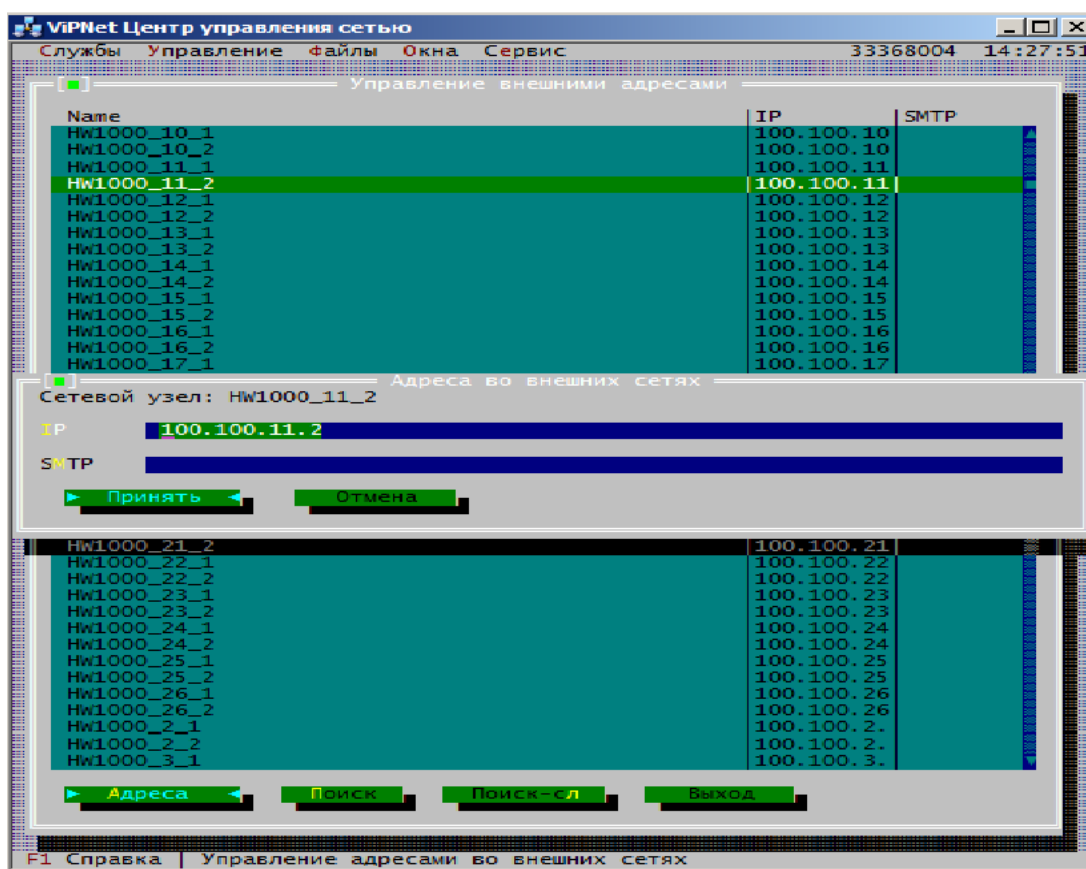


Рисунок 28 – Назначения адреса во внешней сети

Затем нужно зарегистрировать все сетевые узлы в прикладных задачах. В нашем случае, нам нужно назначить для 26-и криптошлюзов работать в режиме Coordinator HW1000 и остальные 26 в режиме Failover, т.е. в режиме резервирования. Для этого мы зашли во вкладку «регистрация сетевых узлов в прикладных задачах» и каждому узлу назначили свою задачу, результат представлен на рисунке 29.

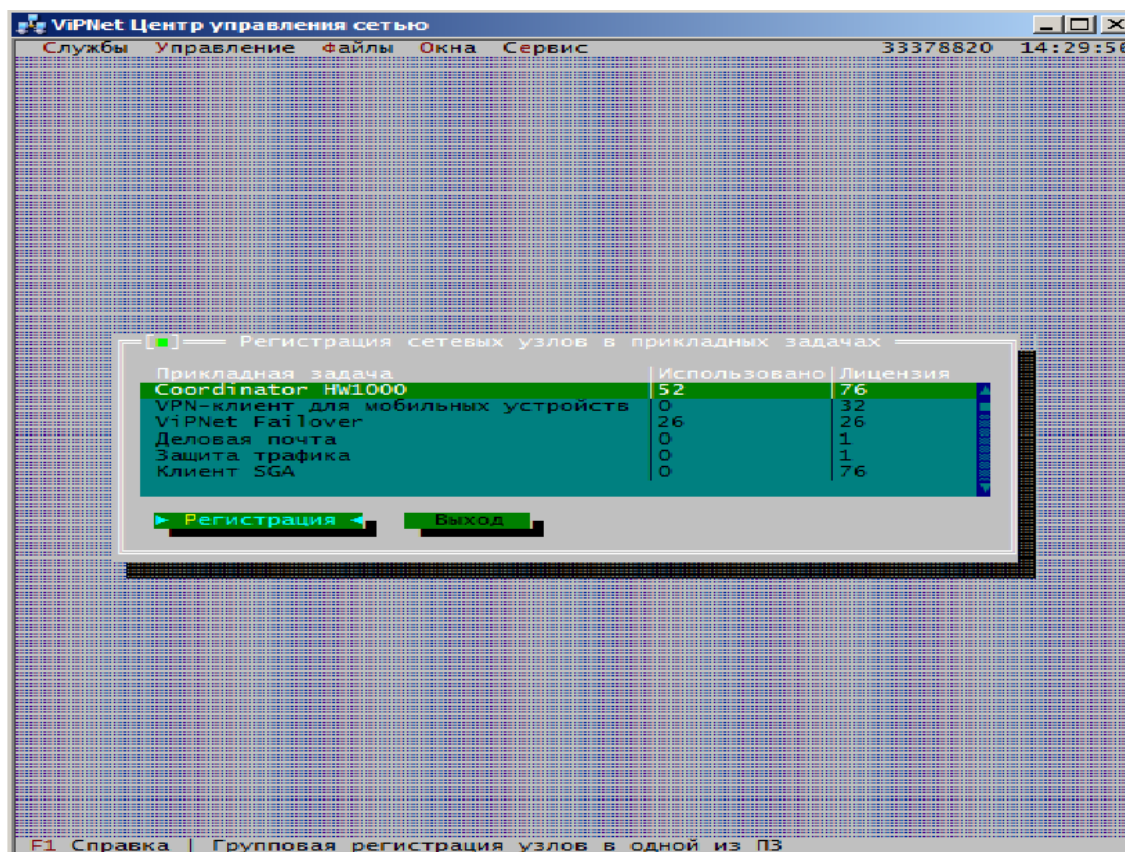


Рисунок 29 – Регистрация сетевых узлов в прикладных задачах

Следующим шагом нужно назначить внутренние ip-адреса для каждого криптошлюза. Для этого во вкладке «регистрация задачи» нужно войти во вкладку «IP-адрес» и там ввести внутренний ip-адрес каждому криптошлюзу. При чем внутренний ip-адрес вводится вместе с маской подсети. Результат назначения внутреннего ip-адреса криптошлюза представлен на рисунке 30.

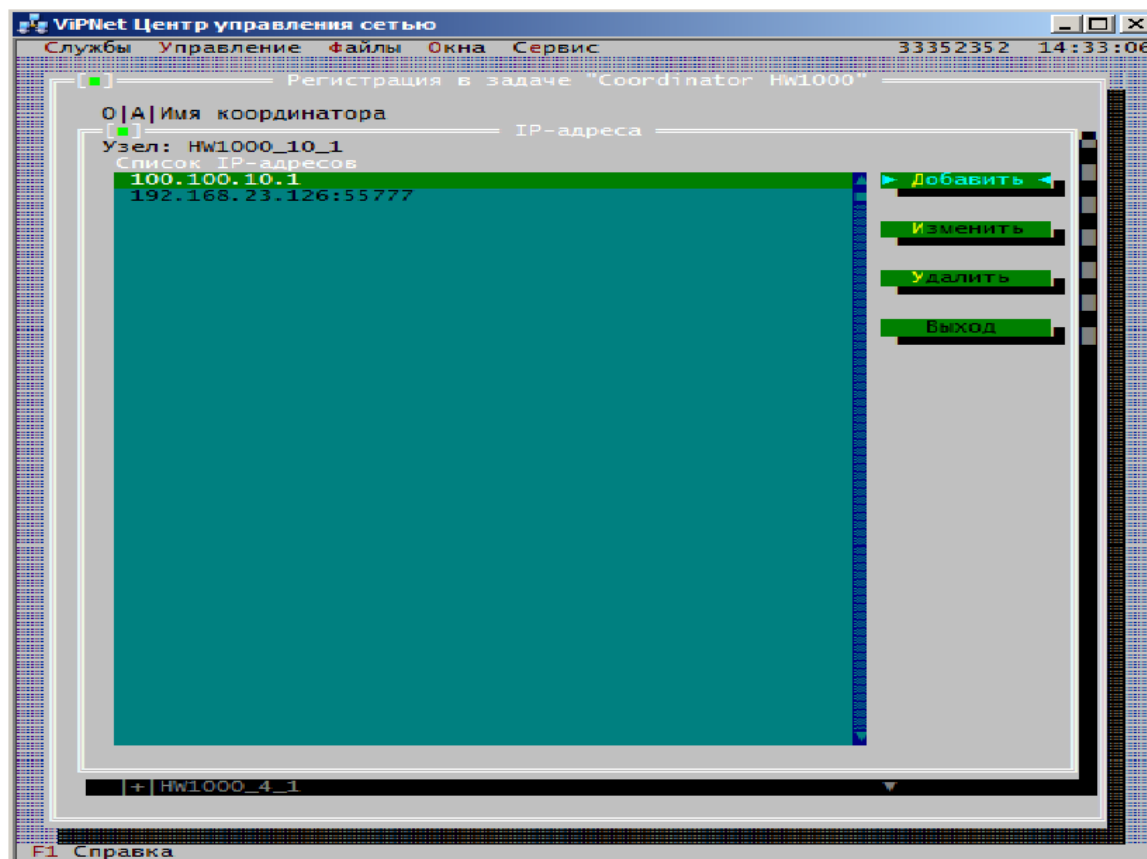


Рисунок 30 – Назначение внутреннего ip-адреса криптошлюза

Финальным шагом настройки является присвоение пользователей каждому криптошлюзу. Для этого во вкладке «каталог пользователей» нужно создать 26 пользователей, по два криптошлюза на одного пользователя, и присвоить каждому пользователю по два криптошлюза. Результаты этих действий представлены на рисунке 31 и 32.

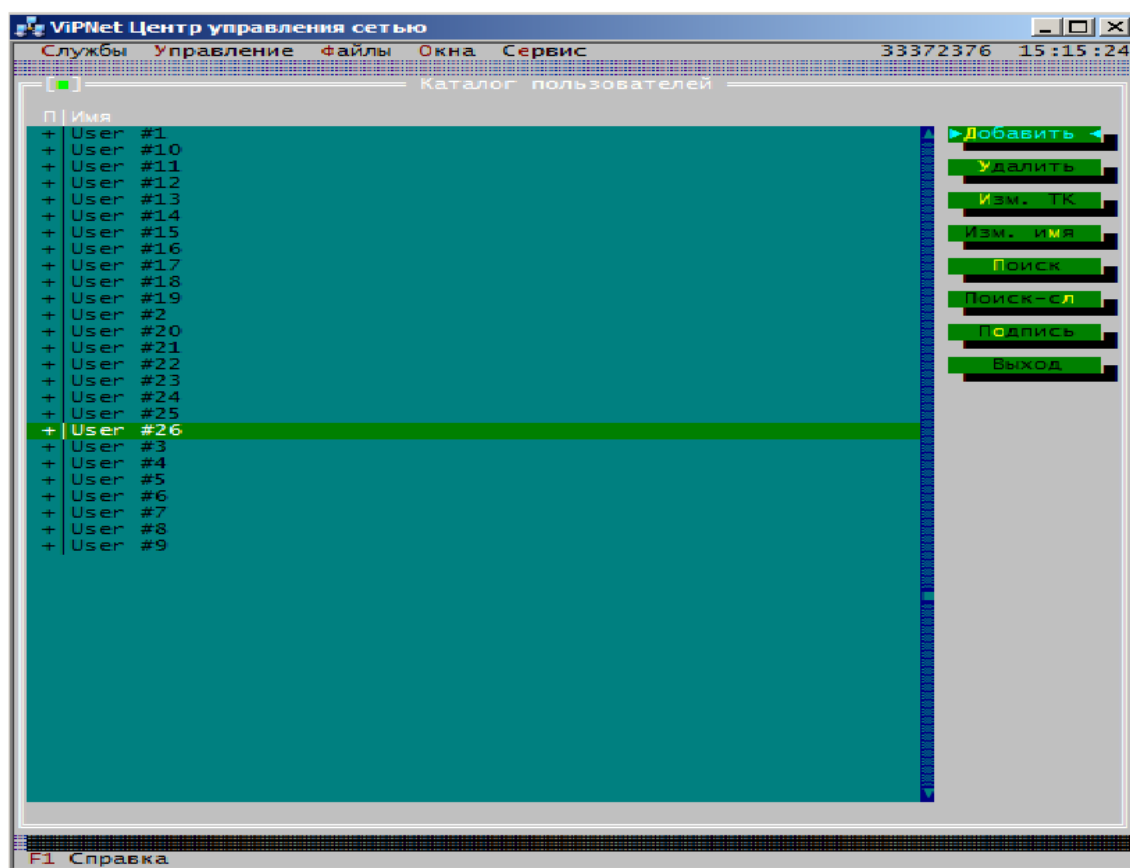


Рисунок 31 – Пользователи криптошлюзов

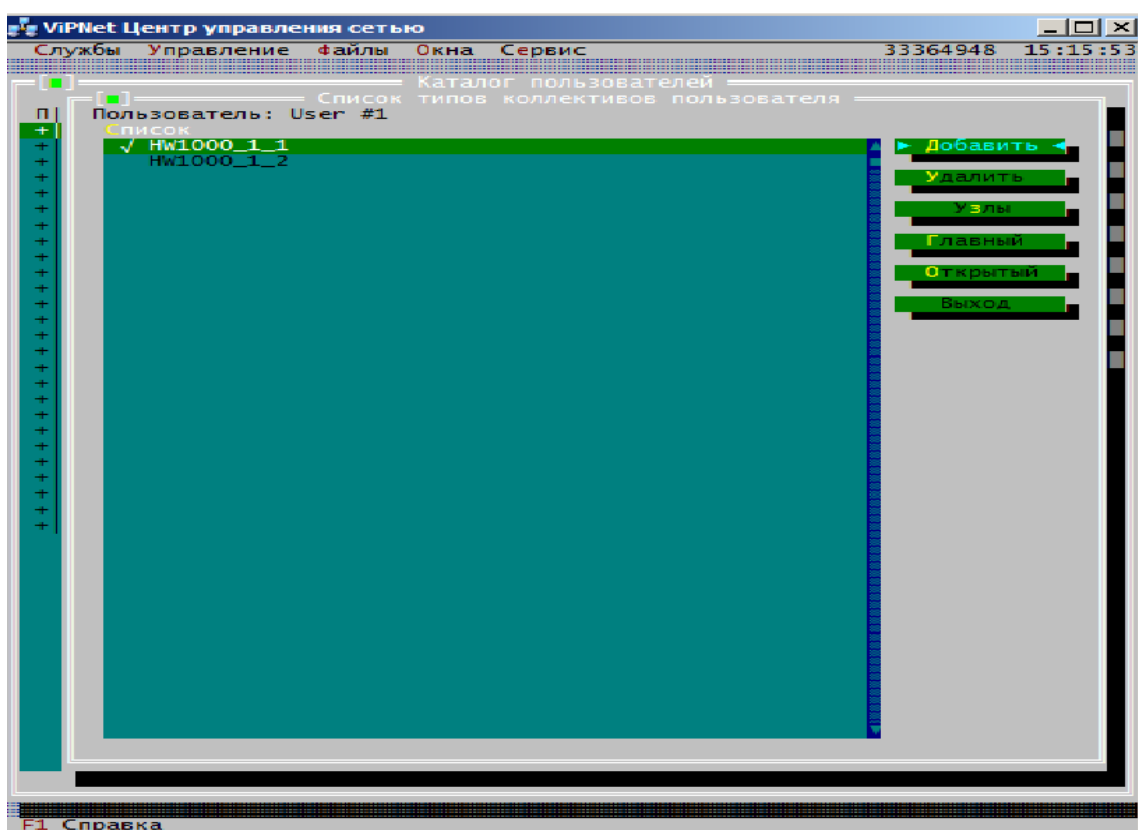


Рисунок 32 – Назначение пользователю криптошлюзов

ПРИЛОЖЕНИЕ В
(обязательно)
Настройка коммутатора Cisco 2960

Для настройки работы коммутатор в сети передачи данных нужно:

- установить интерфейсы работы;
- назначить адреса этим интерфейсам;
- назначить маску подсети;
- установить скорости передачи;
- установить тип соединения;
- назначить адреса всех подсетей;
- указать узлы доступа;
- обозначить приоритеты между поставщиками услуг.

Текст настройки коммутатора представлен ниже.

```
hostname Router

no ip cef

no ipv6 cef

spanning-tree mode pvst

interface FastEthernet0/0

ip address 10.10.15.1 255.255.255.0

ip ospf priority 100

duplex auto

speed auto

interface FastEthernet0/1

no ip address

duplex auto

speed auto

shutdown

interface FastEthernet1/0

ip address 20.40.30.1 255.255.255.0

interface Vlan1

no ip address

shutdown
```

```
router ospf 1
router-id 1.1.15.2
log-adjacency-changes
network 20.20.30.0 0.0.0.255 area 65015
network 20.40.30.0 0.0.0.255 area 0
ip classless
ip flow-export version 9
line con 0
line aux 0
line vty 0 4
login
end
```

ПРИЛОЖЕНИЕ Г

(обязательно)

Перечень услуг приведен в таблице 13

Таблица 13 - Перечень услуг

№ п/ п	Пользователь	Точки терминирования услуги			Ответственное лицо объекта				Тип услуги	Скорость потока данных, Мбит/с	Класс качества	Период оказания услуг			Примечание
		Наименование объекта	Адрес объекта	Стык	ФИО	Должность	Контактный тел.	Адрес эл. почты				Общее кол-во месяцев	Дата начала использования	Дата	
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	НИКИРЭТ – филиал ФГУП ФНПЦ «ПО «Старт» им. М.В. Проценко»	Спортивный объект №1	Г. N1	Ethernet 1000 BaseTX/LX/SX	Сорокин Дмитри	Специалист по ИБ	89635858956	Sorokin@mail.ru	L3 VPN	100		7	ДД.ММ.ГГГГ	ДД.ММ.ГГГГ	
2	НИКИРЭТ – филиал ФГУП ФНПЦ «ПО «Старт» им. М.В. Проценко»	Спортивный объект №2	Г. N2	Ethernet 1000 BaseTX/LX/SX	Давыдов Станислав	Специалист по ИБ	89604785172	davidov@mail.ru	L3 VPN	100		7	ДД.ММ.ГГГГ	ДД.ММ.ГГГГ	

Продолжение таблицы 13

№ п/ п	Пользователь	Точки терминирования услуги			Ответственное лицо объекта				Тип услуги	Скорость потока данных, Мбит/с	Класс качества	Период оказание услуг			Примечание
		Наименование объекта	Адрес объекта	Стык	ФИО	Должность	Контактный тел.	Адрес эл. почты				Дата начала оказания услуг	Дата окончания оказания услуг	Общее кол-во месяцев	
3	НИКИРЭТ – филиал ФГУП ФНПЦ «ПО «Старт» им. М.В. Проценко»	Спортивный объект №3	Г. N3	Ethernet 1000 BaseTX/LX/SX	Белик Андрей	Специалист по ИБ	89872541659	belik@mail.ru	L3 VPN	100		ДД.ММ.ГГГГ	ДД.ММ.ГГГГ	7	
4	НИКИРЭТ – филиал ФГУП ФНПЦ «ПО «Старт» им. М.В. Проценко»	Спортивный объект №4	Г. N4	Ethernet 1000 BaseTX/LX/SX	Самсонов Максим	Специалист по ИБ	89027515749	Samsonov@mail.ru	L3 VPN	100		ДД.ММ.ГГГГ	ДД.ММ.ГГГГ	7	

Продолжение таблицы 13

№ п/ п	Пользователь	Точки терминирования услуги			Ответственное лицо объекта				Тип услуги	Скорость потока данных, Мбит/с	Класс качества	Период оказание услуг			Примечание
		Наименование объекта	Адрес объекта	Стык	ФИО	Должность	Контактный телефон	Адрес эл. почты				Дата прекращения	Дата начала	Общее кол-во месяцев	
5	НИКИРЭТ – филиал ФГУП ФНПЦ «ПО «Старт» им. М.В. Проценко»	Спортивный объект №5	Г. N5	Ethernet 1000 BaseTX/LX/SX	Кузнецов Алексей	Специалист по ИБ	89068529453	kuzuza@mail.ru	L3 VPN	100		ДД.ММ.ГГГГ	ДД.ММ.ГГГГ	7	
6	НИКИРЭТ – филиал ФГУП ФНПЦ «ПО «Старт» им. М.В. Проценко»	Спортивный объект №6	Г. N6	Ethernet 1000 BaseTX/LX/SX	Шишкин Денис	Специалист по ИБ	896036217463	shishas@mail.ru	L3 VPN	100		ДД.ММ.ГГГГ	ДД.ММ.ГГГГ	7	
7	НИКИРЭТ – филиал ФГУП ФНПЦ «ПО «Старт» им. М.В. Проценко»	Спортивный объект №7	Г. N7	Ethernet 1000 Base TX/LX/S	Тонкошкурров Михаил	Специалист по ИБ	89138347891	tonk@mail.ru	L3 VPN	100		ДД.ММ.ГГГГ	ДД.ММ.ГГГГ	7	

Продолжение таблицы 13

№ п/ п	Пользователь	Точки терминирования услуги			Ответственное лицо объекта				Тип услуги	Скорость потока данных, Мбит/с	Класс качества	Период оказание услуг			Примечание
		Наименование объекта	Адрес объекта	Стык	ФИО	Должность	Контактный телефон	Адрес эл. почты				Дата прекращения	Дата начала	Общее кол-во месяцев	
8	НИКИРЭТ – филиал ФГУП ФНПЦ «ПО «Старт» им. М.В. Проценко»	Спортивный объект №8	Г. N8	Ethernet 1000 BaseTX/LX/S	Березин Сергей	Специалист по ИБ	8987726864	berez@mail.ru	L3 VPN	100		ДД.ММ.ГГГГ	ДД.ММ.ГГГГ	7	
9	НИКИРЭТ – филиал ФГУП ФНПЦ «ПО «Старт» им. М.В. Проценко»	Спортивный объект №9	Г. N9	Ethernet 1000 BaseTX/LX/SX	Сабуров Никита	Специалист по ИБ	89647512483	saburov@mail.ru	L3 VPN	100		ДД.ММ.ГГГГ	ДД.ММ.ГГГГ	7	
10	НИКИРЭТ – филиал ФГУП ФНПЦ «ПО «Старт» им. М.В. Проценко»	Спортивный объект №10	Г. N10	Ethernet 1000 BaseTX/LX/S	Ближнин Артем	Специалист по ИБ	89647564802	blj@mail.ru	L3 VPN	100		ДД.ММ.ГГГГ	ДД.ММ.ГГГГ	7	

Продолжение таблицы 13

№ п/ п	Пользователь	Точки терминирования услуги			Ответственное лицо объекта				Тип услуги	Скорость потока данных, Мбит/с	Класс качества	Период оказание услуг			Примечание
		Наименование объекта	Адрес объекта	Стык	ФИО	Должность	Контактный телефон	Адрес эл. почты				Дата прекращения	Дата начала	Общее кол-во месяцев	
11	НИКИРЭТ – филиал ФГУП ФНПЦ «ПО «Старт» им. М.В. Проценко»	Центральный сервера базы данных	Г. N11	Ethernet 1000 BaseTX/LX/S	Корытцев Никита	Специалист по ИБ	89758801697	kotni@mail.ru	L3 VPN	100		ДД.ММ.ГГГГ	ДД.ММ.ГГГГ	7	
12	НИКИРЭТ – филиал ФГУП ФНПЦ «ПО «Старт» им. М.В. Проценко»	Центр управления технической поддержки	Г. N11	Ethernet 1000 BaseTX/LX/SX	Анчуткин Роман	Специалист по ИБ	89025560476	anchut@mail.ru	L3 VPN	100		ДД.ММ.ГГГГ	ДД.ММ.ГГГГ	7	
13	НИКИРЭТ – филиал ФГУП ФНПЦ «ПО «Старт» им. М.В. Проценко»	Спортивный объект №12.1	Г. N12	Ethernet 1000 BaseTX/LX/S	Палин Сергей	Специалист по ИБ	89602577410	ralin@mail.ru	L3 VPN	100		ДД.ММ.ГГГГ	ДД.ММ.ГГГГ	7	

Продолжение таблицы 13

№ п/ п	Пользователь	Точки терминирования услуги			Ответственное лицо				Тип услуги	Скорость потока Мбит/с	Класс качества	Период оказания услуг			Примечание
		Наименование объекта	Адрес объекта	Стык	ФИО	Должность	Контактный	Адрес эл. почты				Общее кол-во месяцев	Дата начала	Дата прекращения	
14	НИКИРЭТ – филиал ФГУП ФНПЦ «ПО «Старт» им. М.В. Проценко»	Спортивный объект №12.2	Г. N12	Ethernet 1000 BaseTX/LX/SX	Маслов Илья	Специалист по ИБ	89372564882	maslov@mail.ru	L3 VPN	100		7	ДД.ММ.ГГГГ	ДД.ММ.ГГГГ	
15	НИКИРЭТ – филиал ФГУП ФНПЦ «ПО «Старт» им. М.В. Проценко»	Внешняя информационная система №1	Г. N12	Ethernet 1000 BaseTX/LX/SX	Суслов Станислав	Специалист по ИБ	89377374220	suslov@mail.ru	L3 VPN	100		7	ДД.ММ.ГГГГ	ДД.ММ.ГГГГ	
16	НИКИРЭТ – филиал ФГУП ФНПЦ «ПО «Старт» им. М.В. Проценко»	Внешняя информационная система №2	Г. N12	Ethernet 1000 BaseTX/LX/S	Малахов Константин	Специалист по ИБ	89872563418	malah@mail.ru	L3 VPN	100		7	ДД.ММ.ГГГГ	ДД.ММ.ГГГГ	

Продолжение таблицы 13

№ п/ п	Пользователь	Точки терминирования услуги			Ответственное лицо объекта				Тип услуги	Скорость поток Mbps/s	Класс качества	Период оказание услуг			Примечание
		Наименование объекта	Адрес объекта	Стык	ФИО	Должность	Контактный телефон	Адрес эл.				Общее кол-во месяцев	Дата прекращения	Дата начала	
17	НИКИРЭТ – филиал ФГУП ФНПЦ «ПО «Старт» им. М.В. Проценко»	Внешняя информационн ая система №3	Г. N12	Ethernet 1000 BaseTX/LX/SX	Маковский Ильядар	Специалист по ИБ	89022458040	makovskij@mail.ru	L3 VPN	100		7	ДД.ММ.ГГГГ	ДД.ММ.ГГГГ	
18	НИКИРЭТ – филиал ФГУП ФНПЦ «ПО «Старт» им. М.В. Проценко»	Размещение оборудования в резервном дата-центре для связи с системой идентификации болельщиков	Г. N12	Ethernet 1000 BaseTX/LX/SX	Коренков Дмитрий	Специалист по ИБ	89873685417	koronkov@mail.ru	L3 VPN	100		7	ДД.ММ.ГГГГ	ДД.ММ.ГГГГ	

Продолжение таблицы 13

№ п/ п	Пользователь	Точки терминирования услуги			Ответственное лицо объекта				Тип услуги	Скорость потока данных, Мбит/с	Класс качества	Период оказание услуг			Примечание
		Наименование объекта	Адрес объекта	Стык	ФИО	Должность	Контактный телефон	Адрес эл. почты				Общее кол-во месяцев	Дата начала	Дата прекращения	
19	НИКИРЭТ – филиал ФГУП ФНПЦ «ПО «Старт» им. М.В. Проценко»	Размещение оборудования в основном дата- центре для связи с системой идентификации болельщиков	Г. N12	Ethernet 1000 BaseTX/LX/SX	Иванов Иван	Специалист по ИБ	89648937481	ivonov@mail.ru	L3 VPN	100		7	ДД.ММ.ГГГГ	ДД.ММ.ГГГГ	
20	НИКИРЭТ – филиал ФГУП ФНПЦ «ПО «Старт» им. М.В. Проценко»	Размещение оборудования в основном дата- центре для связи с системой аккредитации	Г. N12	Ethernet 1000 BaseTX/LX/SX	Макаровский Антон	Специалист по ИБ	89024579830	makarski@mail.ru	L3 VPN	100		7	ДД.ММ.ГГГГ	ДД.ММ.ГГГГ	

Продолжение таблицы 13

№ п/ п	Пользователь	Точки терминирования услуги			Ответственное лицо объекта				Тип услуги	Скорость потока Мбит/с	Класс качества	Период оказание услуг			Примечание
		Наименование объекта	Адрес объекта	Стык	ФИО	Должность	Контактный телефон	Адрес эл. почты				Общее кол-во месяцев	Дата начала	Дата прекращения	
21	НИКИРЭТ – филиал ФГУП ФНПЦ «ПО «Старт» им. М.В. Проценко»	Размещение оборудования в резервном дата-центре для связи с системой аккредитации	Г. N11	Ethernet 1000 BaseTX/LX/SX	Алексакин Павел	Специалист по ИБ	89024837840	aleksakin@mail.ru	L3 VPN	100		7	ДД.ММ.ГГГГ	ДД.ММ.ГГГГ	
22	НИКИРЭТ – филиал ФГУП ФНПЦ «ПО «Старт» им. М.В. Проценко»	Внешняя информационн ая система №1	Г. N11	Ethernet 1000 BaseTX/LX/SX	Кузьминов Андрей	Специалист по ИБ	89578623540	kuzmin@mail.ru	L3 VPN	100		7	ДД.ММ.ГГГГ	ДД.ММ.ГГГГ	
23	НИКИРЭТ – филиал ФГУП ФНПЦ «ПО «Старт» им. М.В. Проценко»	Внешняя информационная система №2	Г. N11	Ethernet 1000 BaseTX/LX/S	Аникин Ренат	Специалист по ИБ	89647582003	anik@mail.ru	L3 VPN	100		7	ДД.ММ.ГГГГ	ДД.ММ.ГГГГ	

Продолжение таблицы 13

№ п/ п	Пользователь	Точки терминирования услуги			Ответственное лицо объекта				Тип услуги	Скорость потока данных, Мбит/с	Класс качества	Период оказание услуг			Примечание
		Наименование объекта	Адрес объекта	Стык	ФИО	Должность	Контактный телефон	Адрес эл. почты				Общее кол-во месяцев	Дата начала	Дата прекращения	
24	НИКИРЭТ – филиал ФГУП ФНПЦ «ПО «Старт» им. М.В. Проценко»	Внешняя информационн ая система №3	Г. N11	Ethernet 1000 BaseTX/LX/S	Синяев Павел	Специалист ИБ	89874120360	sineev@mail.ru	L3 VPN	100		7	ДД.ММ.ГГГГ	ДД.ММ.ГГГГ	
25	НИКИРЭТ – филиал ФГУП ФНПЦ «ПО «Старт» им. М.В. Проценко»	Внешняя информационн ая система №4	Г. N11	Ethernet 1000 BaseTX/LX/S	Петров Николай	Специалист по ИБ	89654897420	retov@mail.ru	L3 VPN	100		7	ДД.ММ.ГГГГ	ДД.ММ.ГГГГ	
26	НИКИРЭТ – филиал ФГУП ФНПЦ «ПО «Старт» им. М.В. Проценко»	Внешняя информационн ая система №5	Г. N11	Ethernet 1000 BaseTX/LX/S	Сидоров Николай	Специалист по ИБ	89751103552	sidiv@mail.ru	L3 VPN	100		7	ДД.ММ.ГГГГ	ДД.ММ.ГГГГ	

ПРИЛОЖЕНИЕ Д

(обязательно)

Результат проверки в системе антиплагиат

ПРОТОКОЛ

проверки ВКР на оригинальность в системе «Антиплагиат» выпускной квалификационной работы на тему «Защищенная сеть передачи данных распределенной информационной системы персональных данных» студента 6 курса Р. А. Бербечука направления подготовки 100502 «Информационная безопасность телекоммуникационных систем». Специализация – разработка защищённых телекоммуникационных систем.

Результаты прохождения ВКР в системе «Антиплагиат» представлен на рисунке А1.

Руководитель ВКР: начальник отдела защиты информации НИКИРЭТ – филиал ФГУП ФНПЦ ПО «Старт» им. М.В Проценко Мещеряков А.А

Информация о документе:

Имя исходного файла: ВКР_11ПТ1_Бербечук_Р_А.docx
Имя компании: Пензенский гос. Университет
Тип документа: Прочее
Имя документа: Группа 11ПТ1 ВКР Бербечук РА
Дата проверки: 16.01.2017 22:25
Модули поиска: Интернет (Антиплагиат), Кольцо вузов, Диссертации и авторефераты РГБ, Модуль поиска ЭБС БиблиоРоссика, Университетская библиотека онлайн, Модуль поиска ЭБС "Лань", Цитирования, Пензенский гос. Университет, Научные статьи Elibray

Текстовые статистики:

Индекс читаемости: сложный
Неизвестные слова: в пределах нормы
Макс. длина слова: в пределах нормы
Большие слова: в пределах нормы

Оригинальные блоки: 74,79%
Заимствованные блоки: 24,81%
Заимствование из "белых" источников: 0,4%
Итоговая оценка оригинальности: 75,19%

Рисунок А1 – Результаты прохождения ВКР в системе «Антиплагиат»

«16» января 2017г.



А. А. Мещеряков