

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования
«Тольяттинский государственный университет»

Институт математики, физики и информационных технологий

(наименование института полностью)

Кафедра «Прикладная математика и информатика»

(наименование кафедры)

09.03.03 Прикладная информатика

(код и наименование направления подготовки, специальности)

Бизнес-информатика

(направленность (профиль)/специализация)

БАКАЛАВРСКАЯ РАБОТА

на тему «Организация защищенного доступа пользователей к объекту
информатизации с использованием
программно-аппаратного комплекса VipNet»

Студент

К.А. Глушак

(И.О. Фамилия)

(личная подпись)

Руководитель

О.М. Гущина

(И.О. Фамилия)

(личная подпись)

Допустить к защите

Заведующий кафедрой к.т.н., доцент, А.В. Очеповский _____

(ученая степень, звание, И.О. Фамилия) (личная подпись)

« _____ » _____ 2019г.

Тольятти 2019



Росдистант
ВЫСШЕЕ ОБРАЗОВАНИЕ ДИСТАНЦИОННО

АННОТАЦИЯ

Название работы: «Организация защищенного доступа пользователей к объекту информатизации с использованием программно-аппаратного комплекса VipNet».

Автор: Глушак К.А., гр. ПИБд-1402а.

Тематика работы: описание процесса разработки компьютерной сети и проверки ее работоспособности на основе использования программно-аппаратного комплекса VipNet. **Объектом исследования** является процесс создания компьютерной сети с использованием структурированной кабельной системы. **Предметом исследования** является процесс организации защищенного доступа с пользователей к объекту информатизации в спроектированной компьютерной сети.

Целью данной работы является разработка методов и организационных мер защиты компьютерных систем от несанкционированного доступа с использованием программно-технического комплекса VipNet.

Работа разбита на 3 главы, описывающие 3 основные этапы разработки компьютерной сети и проверки ее пропускной способности. **Первая глава** посвящена анализу программного оборудования, которое требуется для организации защищенного доступа к объектам информатизации. **Во второй главе** описан сам проект компьютерной сети, включающий как техническое решение, так и разработку интерактивной технологической карты для администратора сети VipNet. **В третьей главе** рассмотрена апробация разработанной компьютерной сети с использованием программно-технического комплекса VipNet. Работа завершается оценкой экономической эффективности спроектированной компьютерной сети.

Общий объем работы составляет 58 страниц, в том числе 30 рисунков, 11 таблиц.

СОДЕРЖАНИЕ

| | |
|--|----|
| ВВЕДЕНИЕ..... | 5 |
| 1 АНАЛИЗ ПРОГРАММНОГО ОБОРУДОВАНИЯ ДЛЯ ОРГАНИЗАЦИИ ЗАЩИЩЕННОГО ДОСТУПА ПОЛЬЗОВАТЕЛЕЙ К ОБЪЕКТУ ИНФОРМАТИЗАЦИИ..... | 7 |
| 1.1 Анализ программных комплексов защиты от несанкционированной доступа | 7 |
| 1.2 Перечень необходимого оборудования для автоматизации разграничения доступа к объекту информатизации..... | 10 |
| 2 ПРОЕКТ КОМПЬЮТЕРНОЙ СЕТИ С ПРИМЕНЕНИЕМ СТРУКТУРИРОВАННОЙ КАБЕЛЬНОЙ СИСТЕМЫ | 15 |
| 2.1 Построение сети с использованием структурированной кабельной системы | 15 |
| 2.2 Описание технического решения при проектировании вычислительной компьютерной сети | 18 |
| 2.3 Описание аппаратно-технической платформы для построения компьютерной сети | 21 |
| 2.4 Разработка интерактивной технологической карты для администратора сети Vip Net по смене ключевой информации | 24 |
| 2.5 Проект резервной беспроводной VPN сети с учетом требований по защите информации от НДС | 26 |
| 2.5.1 В случае НДС, обрыва кабельного сигнала..... | 26 |
| 2.5.2. Выбор пассивного оборудования..... | 34 |
| 3 АПРОБАЦИЯ РАЗРАБОТАННОЙ КОМПЬЮТЕРНОЙ СЕТИ АППАРАТНО- ТЕХНИЧЕСКИМ КОМПЛЕКСОМ ПРИ ОРГАНИЗАЦИИ ЗАЩИЩЕННОГО ДОСТУПА..... | 36 |
| 3.1 Технические мероприятия по защите информации от НДС | 36 |
| 3.2 Тестирование VipNet для организации защищенного доступа к объектам информатизации..... | 40 |

| | |
|---|----|
| 3.3 Экономическая оценка спроектированной СКС с учетом СЗИ от НСД «VIPNET» | 46 |
| ЗАКЛЮЧЕНИЕ | 54 |
| СПИСОК ИСПОЛЬЗУЕМОЙ ЛИТЕРАТУРЫ..... | 56 |

ВВЕДЕНИЕ

В современных информационных и телекоммуникационных системах, на рабочих местах представителей самых различных профессий широко используется компьютерная техника. В компьютерах накапливаются, обрабатываются, хранятся и передаются по каналам связи текстовые документы, банки данных, закодированные изображения, аудио- и видеоматериалы, числовые данные, программы и т.п.

Каждый пользователь компьютера может привести множество примеров, когда по вине каких-то непродуманных действий были стерты или испорчены файлы, нарушена работоспособность операционной системы.

Опасней всего являются вирусные атаки, попытки несанкционированного доступа к ресурсам системы, а также добыча информации из персональных компьютеров путем современного съема информации.

Обеспечение необходимого уровня защиты информации требует создания целостной системы организационных и технических мероприятий и применения специальных средств и методов защиты информации.

Объектом исследования является процесс создания компьютерной сети с использованием структурированной кабельной системы. Предметом исследования является процесс организации защищенного доступа с пользователей к объекту информатизации в спроектированной компьютерной сети.

Целью бакалаврской работы является разработка методов и организационных мер защиты компьютерных систем от несанкционированного доступа с использованием программно-технического комплекса VipNet.

Для реализации цели бакалаврской работы необходимо решить ряд задач:

1. Провести анализ задач, решаемых при организации защищенного доступа пользователей к объекту информатизации.
2. Определить перечень необходимого оборудования для автоматизации разграничения доступа к объекту информатизации с использованием программно-аппаратных средств.

3. Разработать интерактивную технологическую карту для администратора сети VIP Net по смене ключевой информации.
4. Спроектировать резервную беспроводную VPN сеть с учетом требования по защите информации от НДС.
5. Разработать технические мероприятия по защите информации от НДС.
6. Произвести экономическую оценку спроектированной СКС.

Работа разбита на 3 главы, описывающие 3 основные этапы разработки компьютерной сети и проверки ее пропускной способности. **Первая глава** посвящена анализу программного оборудования, которое требуется для организации защищенного доступа к объектам информатизации. **Во второй главе** описан сам проект компьютерной сети, включающий как техническое решение, так и разработку интерактивной технологической карты для администратора сети VipNet. **В третьей главе** рассмотрена апробация разработанной компьютерной сети с использованием программно-технического комплекса VipNet. Работа завершается оценкой экономической эффективности спроектированной компьютерной сети.

Общий объем работы составляет 58 страниц, в том числе 30 рисунков, 11 таблиц.

1 АНАЛИЗ ПРОГРАММНОГО ОБОРУДОВАНИЯ ДЛЯ ОРГАНИЗАЦИИ ЗАЩИЩЕННОГО ДОСТУПА ПОЛЬЗОВАТЕЛЕЙ К ОБЪЕКТУ ИНФОРМАТИЗАЦИИ

1.1 Анализ программных комплексов защиты от несанкционированной доступа

Secret Net используется комплекс традиционных и дополнительных механизмов обеспечения защиты рабочих станций и серверов от НСД. Традиционными механизмами обеспечивается выполнение требований регуляторов по защите персональных данных, конфиденциальной информации и государственной тайны. Дополнительный функционал средств защиты от НСД повышает защищенность обрабатываемой на рабочей станции и серверах информации.

Secret Net является сертифицированным средством защиты информации от несанкционированного доступа и позволяет привести автоматизированные системы в соответствие с требованиями нормативных документов.

Для обеспечения безопасности рабочих станций и серверов сети используются различные механизмы безопасности:

- надежная идентификация и аутентификация;
- авторизованный и выборочный контроль доступа;
- закрытая программная среда;
- криптографическая защита данных;
- другие защитные механизмы.

Администратору безопасности предоставляется единое средство управления всеми защитными механизмами, позволяющее централизованно контролировать и контролировать выполнение требований политики безопасности.

Система **Secret Net** состоит из трех компонентов: клиентской части, сервера безопасности и подсистемы управления (рисунок 1).



Рисунок 1 – Основные компоненты Secret Net

Особенностью системы Secret Net является архитектура клиент-сервер, в которой серверная часть обеспечивает централизованное хранение и обработку данных системы безопасности, а клиентская часть защищает ресурсы рабочей станции или сервера и сохраняет управляющую информацию в своей собственной базе данных.

Клиентская часть системы безопасности (как автономная, так и сетевая) установлена на компьютере, который содержит важную информацию, будь то рабочая станция в сети или любой сервер (включая сервер безопасности).

Основное назначение клиентской части:

- защита компьютерных ресурсов от несанкционированного доступа и разграничение прав зарегистрированных пользователей;
- регистрация событий, происходящих на рабочей станции или сетевом сервере, и передача информации на сервер безопасности;
- осуществление централизованного и децентрализованного контроля действий администратора безопасности.

Клиенты Secret Net оснащены инструментами поддержки оборудования (для идентификации пользователей по электронным идентификаторам и управления загрузками с внешних носителей).

Сервер безопасности устанавливается на выделенном компьютере или контроллере домена и выполняет следующие задачи:

- ведение центральной базы данных (CDB) системы защиты, работающей под управлением СУБД Oracle 8.0 Personal Edition и содержащей информацию, необходимую для работы системы защиты;
- сбор информации о событиях со всех клиентов Secret Net в единый журнал и передача обработанной информации в подсистему управления;
- взаимодействие с подсистемой управления и передача административных команд клиентской части системы безопасности.

Подсистема управления Secret Net устанавливается на рабочем месте администратора безопасности и предоставляет следующие функции:

- аутентификация пользователя.
- обеспечение контроля доступа к защищенной информации и устройствам.
- доверенная информационная среда.
- контроль каналов распространения конфиденциальной информации.
- управление компьютерными устройствами и отчуждаемыми носителями на основе централизованных политик, исключающих утечку конфиденциальной информации.

Схема управления, реализованная в Secret Net, позволяет управлять информационной безопасностью в терминах реального домена и полностью обеспечивать жесткое разделение полномочий между администратором сети и администратором безопасности.

Программно-аппаратный комплекс **VIP Net** представляют собой интегрированные решения на базе нескольких аппаратных платформ и программного обеспечения производства ОАО "Инфотекст", предназначенного для организации сетевой защиты в VPN-сетях. В качестве аппаратной платформы в комплексе может использоваться компактный компьютер или полноценный сервер, устанавливаемый в стандартной стойке.

Программный пакет VIP Net OFFICE- программное обеспечение для организации виртуальных частных защищенных сетей (VPN) типовых конфигураций (защищенных сетей VIP Net). VIP Net OFFICE предназначен для использования в небольших локальных и распределенных IP-сетях и обеспечивает защищенную работу удаленных пользователей с любым типом подключения к Интернету.

Продукты компании «ИнфоТеКС» проходят регулярную сертификацию в ФСТЭК России на соответствие требованиям безопасности для средств защиты конфиденциальной информации, включая персональные данные.

Для решения задачи обеспечения защищенного взаимодействия непосредственно между компьютерами в большой распределенной сети в системе должны присутствовать как минимум три обязательных элемента:

- ПО VIP Net Administrator,
- ПО VIP Net Coordinator,
- ПО VIP Net Client.

Проведя анализ решаемых задач Secret Net и VIP Net можно сделать вывод о том, что VIP Net имеет ряд преимуществ, таких как: FireWall везде, поддержка Wi-Fi, WiMax, EDGE/3G, клиент- клиент, представляет собой как ПО так и ПАК, качественный VPN-клиент.

1.2 Перечень необходимого оборудования для автоматизации разграничения доступа к объекту информатизации

Проанализировав имеющееся и недостающее оборудование, мы можем сделать вывод что нам необходимы:

Аппаратные средства: Системный блок – 13шт, Монитор – 13шт., ПАК HW100 G2 – 2шт., Клавиатура – 13шт., Мышь – 13 шт., USB-ключ eToken PRO(Java) 72Kb/CERT – 1 шт.

Программные средства: ПО Страж – NT, ПО VIP Net OFFICE, ПК VIP Net ADMINISTRATOR, ПАК HW100 G2

Оптимальным решением для нас является ЭВМ, указанная в таблице 1.

Таблица 1 - Системные параметры ЭВМ

| Системные параметры ЭВМ | |
|-------------------------------------|--|
| Системный блок DELL OptiPlex 390 MT | |
| Процессор | G620 Частота CPU, МГц: 2600 |
| Оперативная память | DDR3 Объем ОЗУ, Гб: 2 |
| Система хранения информации | Размер HDD, Гб: 500 |
| Видеоадаптер | Intel 2000 HD |
| Слоты расширения | Один разъем PCIe x16 максимальной высоты Три полнопрофильных разъема PCIe x1 |
| Порты ввода-вывода: | 8 внешних портов External USB 2.0 (2 на передней 6 на задней панели) и 2 внутренних порта USB 2.0 Опциональный переходник PS2 Один порт RJ-45 Один порт VGA 1 разъем HDMI (опциональный переходник DVI) Разъем для микрофона на передней панели Выход для наушников Разъем для микрофона/линейный вход, линейный выход на задней панели Опциональная плата с параллельным/последовательным разъемом PCIe (MT) Опциональная плата с последовательным разъемом PCIe (DT и SFF) Опциональная плата PCIe USB 3.0 |
| Сетевая карта | Gigabit LAN |
| Блок питания | Вт: 265 |
| Оптический привод: | 16xDVD+/-RW |
| Флоппидисковод | ОС: DOS |
| Монитор | |
| LG M2232D-PZ 22" | <ul style="list-style-type: none"> - Тип ЖК-телевизор - Светодиодная (LED) подсветка есть, Edge LED - Диагональ 22" (56 см) - Формат экрана 16:9 - Разрешение 1920x1080 - Поддержка HDTV есть, 1080p (Full HD) - Стереозвук: есть - Частота обновления 50 Гц |

| Системные параметры ЭВМ | |
|------------------------------------|---|
| Клавиатура | |
| Chicony KB-0837 | <ul style="list-style-type: none"> - Назначение настольный компьютер - Интерфейс подключения USB - Цвет черный - Дополнительно - Особенности Volume mute/Vol+/Vol- |
| Мышь | |
| A4Tech X-738K | -Black USB |
| Координатор HW100G2 | |
| Процессор | -Intel Atom N270 с частотой 1.6 ГГц |
| Intel Atom N270 с частотой 1.6 ГГц | -1 ГБ |
| Оперативная память | -Compact Flash 1 ГБ (флэш-диск) |
| Электронный диск | -4 интерфейса Ethe |
| Сетевые интерфейсы | rnet Realtek 8111C 10/100/1000 Мбит/с |
| Графический контроллер | -VGA |
| USB | -USB 2 порта Rev. 2.0 |
| Мощность источника питания | -12 Вт (внешний адаптер 12В ACDC) |

В качестве аппаратной платформы в ПАК VIP Net Coordinator HW100 используются мини-компьютеры с пассивным охлаждением (без вентилятора охлаждения), с низким уровнем тепловыделения и энергопотребления. Компьютеры имеют компактные габаритные размеры и небольшой вес, их применение особенно оправдано в тех местах, где физическое пространство ограничено, а условия окружающей среды неблагоприятны.

Для решения задачи обеспечения защищенного взаимодействия непосредственно между компьютерами в большой распределенной сети в системе должны присутствовать как минимум 3 обязательных элемента: ПО VIP Net Administrator, ПО VIP Net Coordinator, ПО VIP Net Client:

Базовый программный комплекс VIP Net Administrator предназначен для настройки и управления защищенной сетью, входящих в состав VIP Net CUSTOM.

VIPNet Coordinator — 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:

1. Маршрутизатор VPN-пакетов: маршрутизация зашифрованных IP-пакетов, передаваемых между сегментами защищенной сети.
2. VPN-шлюз: туннелирование (шифрование и имитозащита) открытых IP-пакетов, передаваемых между локальными сегментами сети.
3. Межсетевой экран: анализ, фильтрация и регистрация IP-трафика на границе сегмента сети.
4. Транспортный сервер: маршрутизация передачи защищенных служебных данных в сети VIPNet, почтовых сообщений, передаваемых программой «VIPNet Деловая почта».
5. 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.

Типовое решение состоит из следующих функциональных компонентов (рис.2).

Факторы, влияющие на информацию, обрабатываемую на объекте информатизации. (Изолированность информации (то есть кто с ней может работать), ее уровень секретности (ДСП, секретно или сов. секретно), как циркулирует информация внутри системы).

Управляющий ПО VIP Net разделено на два компонента, отвечающие за разные аспекты его функционирования, в целях повышения безопасности. При

этом ни тот, ни другой компоненты администрации по отдельности не могут оказать существенного влияния на функционирование сети, то есть возможности несанкционированного доступа к информатизации пользователей администратором сведены к минимуму.

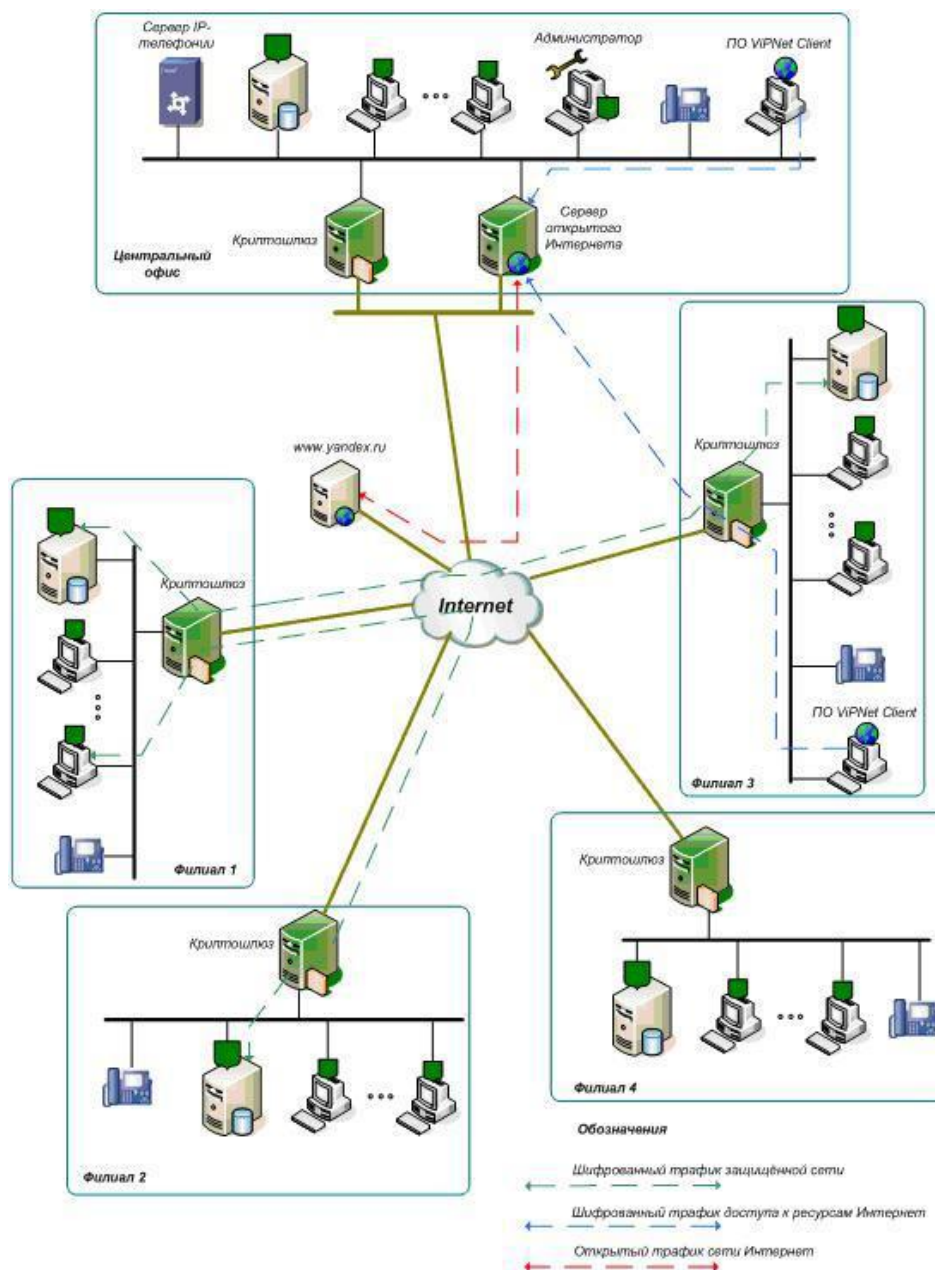


Рисунок 2 – Основные компоненты ViPNet Coordinator

Таким образом, были определены программно-аппаратная платформа и технические требования для реализации технологической карты разработки сети, которая максимально сможет оградить компьютерную систему от несанкционированного доступа.

2 ПРОЕКТ КОМПЬЮТЕРНОЙ СЕТИ С ПРИМЕНЕНИЕМ СТРУКТУРИРОВАННОЙ КАБЕЛЬНОЙ СИСТЕМЫ

2.1 Построение сети с использованием структурированной кабельной системы

Структурированная кабельная система - это набор коммутационных элементов (кабелей, разъемов, коннекторов, кроссовых панелей и шкафов), а также методика их совместного использования, которая позволяет создавать регулярные, легко расширяемые структуры связей в вычислительных сетях.

UTP - кабель медный неэкранированный, независимо от категории выпускается в четырехпарном исполнении. Обычно две пары для передачи данных, и два - для передачи голоса. Категория 5е специально разработана для поддержки высокоскоростных протоколов. На этом кабеле работают протоколы со скоростью передачи 100Мбит/с (FastEthernet), 155Мбит/с (АТМ протокол), 1Гбит/с (Gigabit Ethernet). Характеристики определяются в диапазоне 100 МГц. Улучшенная категория 5е разработана специально для поддержки протокола Gigabit Ethernet и передает данные одновременно по всем четырем парам.

При установке ИР руководствовался правилами:

- При монтаже ИР с использованием короба или по иной схеме, когда корпус розетки занимает вертикальное положение, целесообразным является применение розеточных модулей с угловой установкой как обеспечивающих меньший радиус изгиба шнура в точке подключения;

- При монтаже ИР, корпус которой имеет в рабочем положении горизонтальную ориентацию, используется плоская установка розеточных модулей;

- Схема крепления розеточного модуля должна делать невозможным или, по крайней мере, существенно затруднять его демонтаж без применения специальных инструментов (защита от любопытных); достаточно хорошо этому критерию отвечает схема key-stone.

На рисунке 3 приведена схема расположения зданий, которые непосредственно задействованы для создания ЛВС с программное-аппаратным комплексом VipNet.

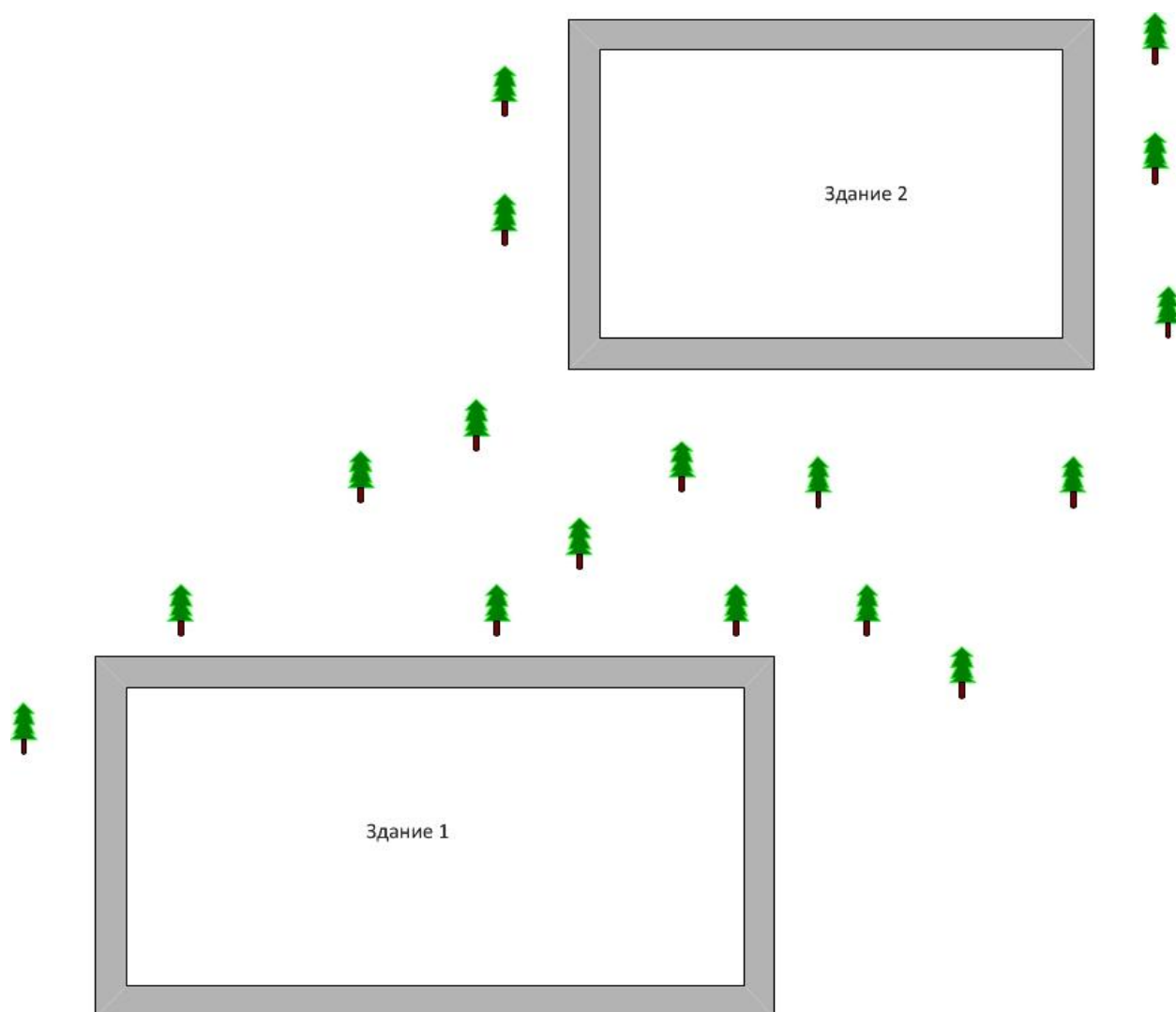


Рисунок 3 – Рисунок расположения помещений

Здание 1 имеет 1 этаж,

Здание 2 имеет 1 этаж.

Количество абонентов проектируемой ЛВС в каждом из задействованных зданий и строений указано в таблице 2.

Таблица 2- Количество абонентов

| Здание 1 | | | |
|---|----------------|---------------------|-----------------------|
| Помещение . (1;2;3;4;5) | Серверная. (1) | Число Абонентов (9) | Секретный Абонент (1) |
| Здание 2 | | | |
| Помещение . (6) | Серверная. (0) | Число Абонентов (4) | Секретный Абонент (0) |
| Общее число абонентов в зданиях:13 | | | |

На рисунке 4 указывается размещение рабочих мест в зданиях и помещений Управления.

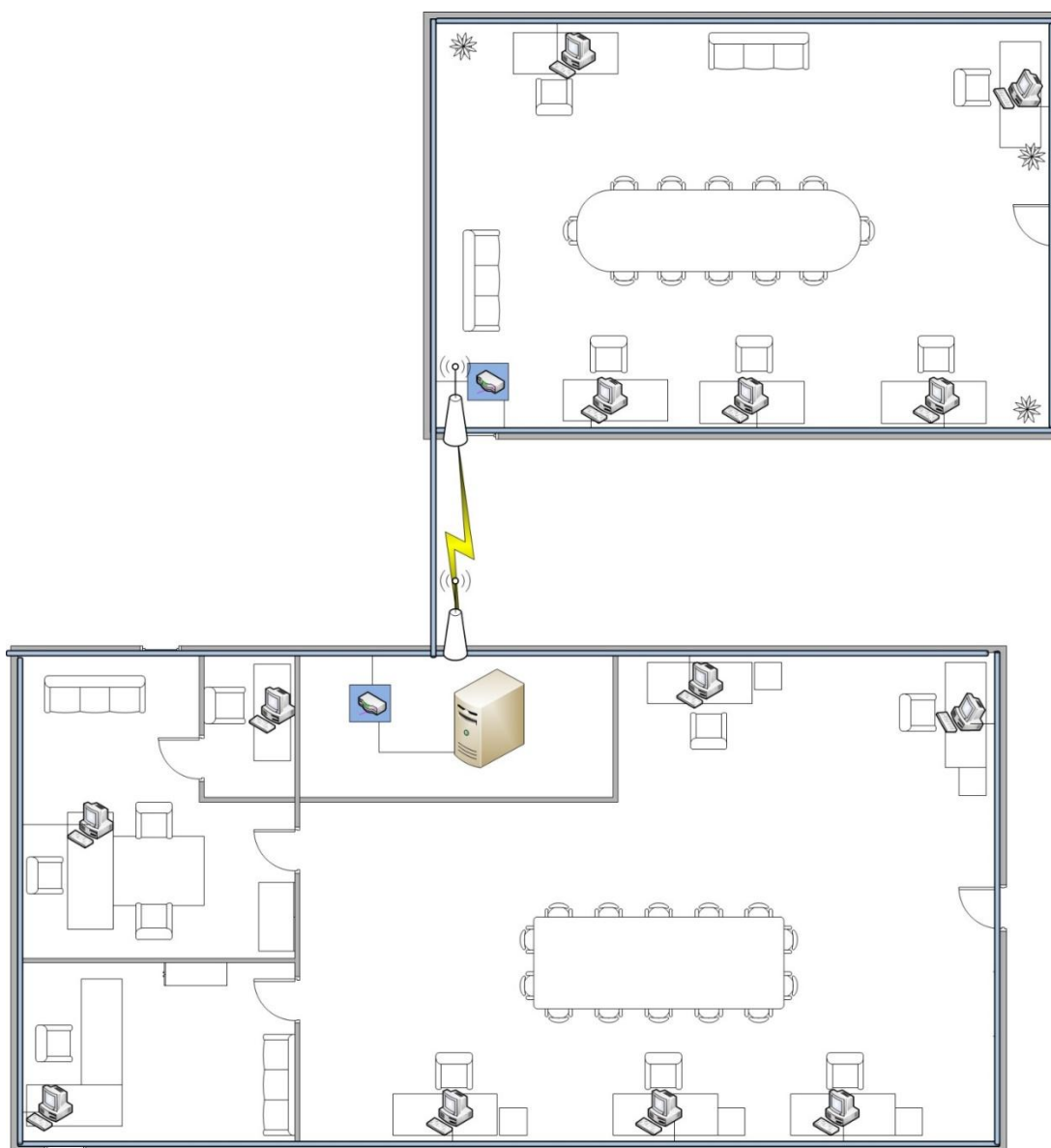


Рисунок 4 - Размещение рабочих мест в зданиях

Наименование помещений показано в таблице 3.

Таблица 3- Наименование помещений

| № | Наименование | м ² |
|---|--------------------------------|----------------|
| 1 | Помещение серверной | 15 |
| 2 | Кабинет начальника | 20 |
| 3 | Кабинет заместителя начальника | 15 |
| 4 | Секретное помещение | 9 |
| 5 | Класс слушателей | 30 |
| 6 | Класс слушателей | 30 |

2.2 Описание технического решения при проектировании вычислительной компьютерной сети

Для проектирования ЛВС подразделения необходимо: – Прокладка волоконно-оптической линии связи между зданием, в котором располагаются сервера и зданием куда переезжает подразделение. – Установка напольного шкафа на 19 дюймов в здании организации кабельной сети. – Установка в шкафу оптических полок и подвод оптического кабеля. – Размещение автоматизированных рабочих мест в здании переезда (в соответствии с правилами структурированной кабельной системы).

Сетевые технологии будут определяться прокладкой кабеля и используемыми материалами и оборудованием. Организацию сети будем выполнять по одноуровневой схеме:

Первый уровень - это 100 Мбитные ветвящиеся каналы. Здесь используем технологию Ethernet 100Base-TX. В качестве среды передачи данных спецификация 100Base-TX использует кабель UTP категории 5.

Максимальная дальность прохождения сигнала без повторителя - 100 м.

Несложная конструкция и комфортный ремонт, обслуживание при поломке.

Вывод кабеля на наружную стену осуществляется согласно нормам проектирования ВСН 60-89, пункт 2.11.

Помещение серверной находится в отдельном помещении. Это делается в основном исходя из целей безопасности, охлаждения (поддержание

определенной температуры, вентиляции) и чтобы серверная не мешала работать сотрудникам. В сети имеется 15 рабочих мест, предназначенных для размещения пользователей. Согласно нормам площадь аппаратной, обслуживающей сети должна быть не менее 14 кв. м. (Таблица 4).

Таблица 4 – Техническое решение проектируемого помещения.

| Номер помещения | Назначение | Площадь | |
|-----------------|------------|-------------|----------------|
| | | Фактическая | По норме(мин.) |
| Здание 1 | | | |
| 3 | Серверная | 15 кв.м | 14 кв.м |

На рисунке 5 отмечен план размещения оборудования в серверной.

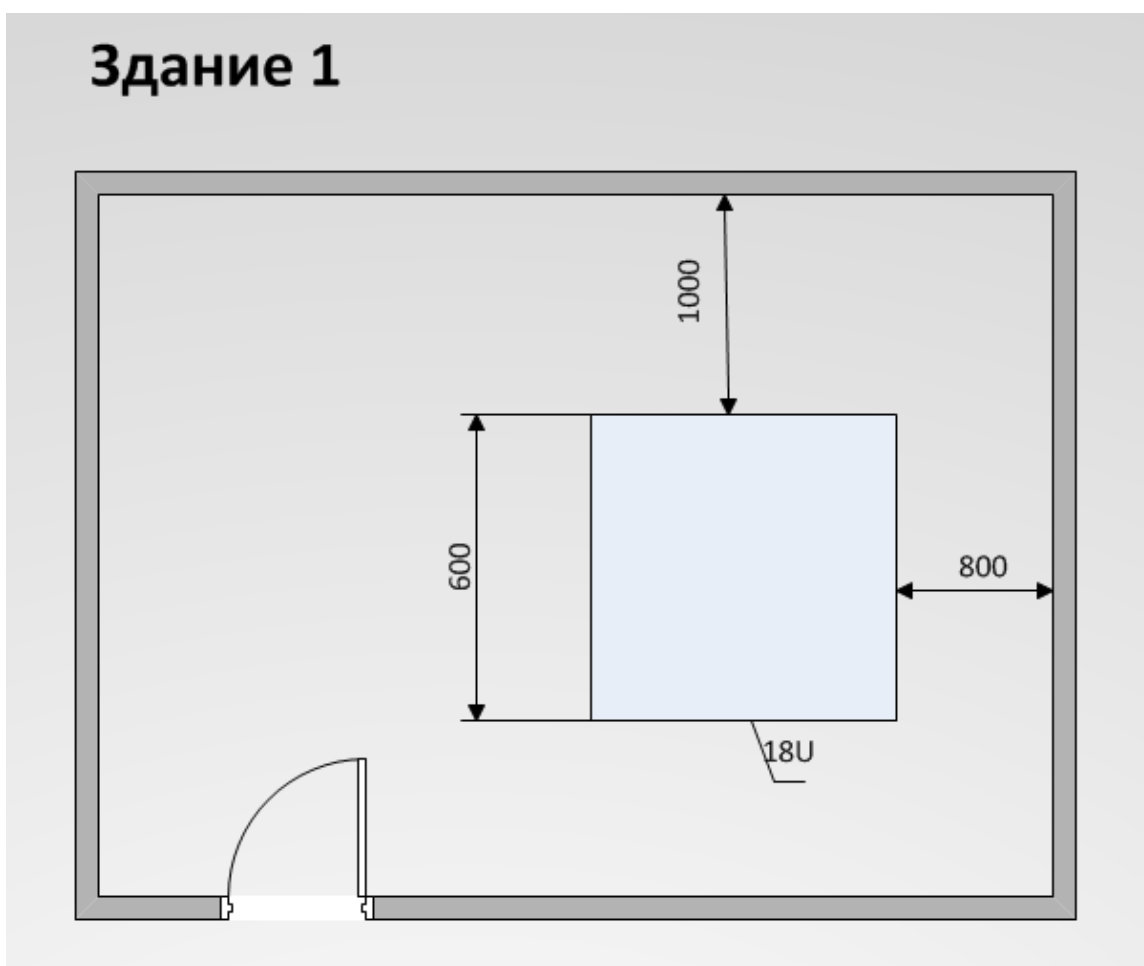


Рисунок 5 - План размещения активного оборудования

В серверном шкафу, который находится в помещении №7 здания, расположено следующее оборудование:

- Sun Fire X4150 Two Quad-Core Intel Xeon E5450-3шт.
- Sun Storage J4200; 2U SAS array; SAS I/O module
- Sun StorEdge[™] LTO 3 tape drive
- Cisco Catalyst 2960 24 10/100/1000, 4 T/SFP LAN Base Image
- Cisco Catalyst 2960 7 10/100/1000 + 1 T/SFP LAN Base
- Cisco GE SFP, LC connector LX/LH transceiver
- 3Com 5 x Ethernet 10/100BaseT • RJ-45 (auto MDI-II/MDI-X port)
- ИБП Smart UPS RT 3000

Для оптимизации пространства в комнате, все оборудование было собрано в единый телекоммуникационный шкаф 42U, представленный на рисунке 6.



Рисунок 6 – Серверный шкаф

2.3 Описание аппаратно-технической платформы для построения компьютерной сети

ViPNet Coordinator - это программный сервер защищенной сети ViPNet, установленный в ОС Linux с ядрами 2.4.2 / 31-2.6.2 / 32 (RedHat, Suse и другие дистрибутивы).

В зависимости от настроек ViPNet Linux Coordinator может выполнять следующие функции, включающие:

- Серверы IP-адресов;
- Безопасное подключение прокси-серверов;
- Туннельный сервер (криптографический шлюз);
- Брандмауэр для открытых, защищенных и туннелируемых ресурсов;
- Защищенные почтовые серверы;
- Отказоустойчивый сервер защищенной сети ViPNet ViPNet Failover настроен.

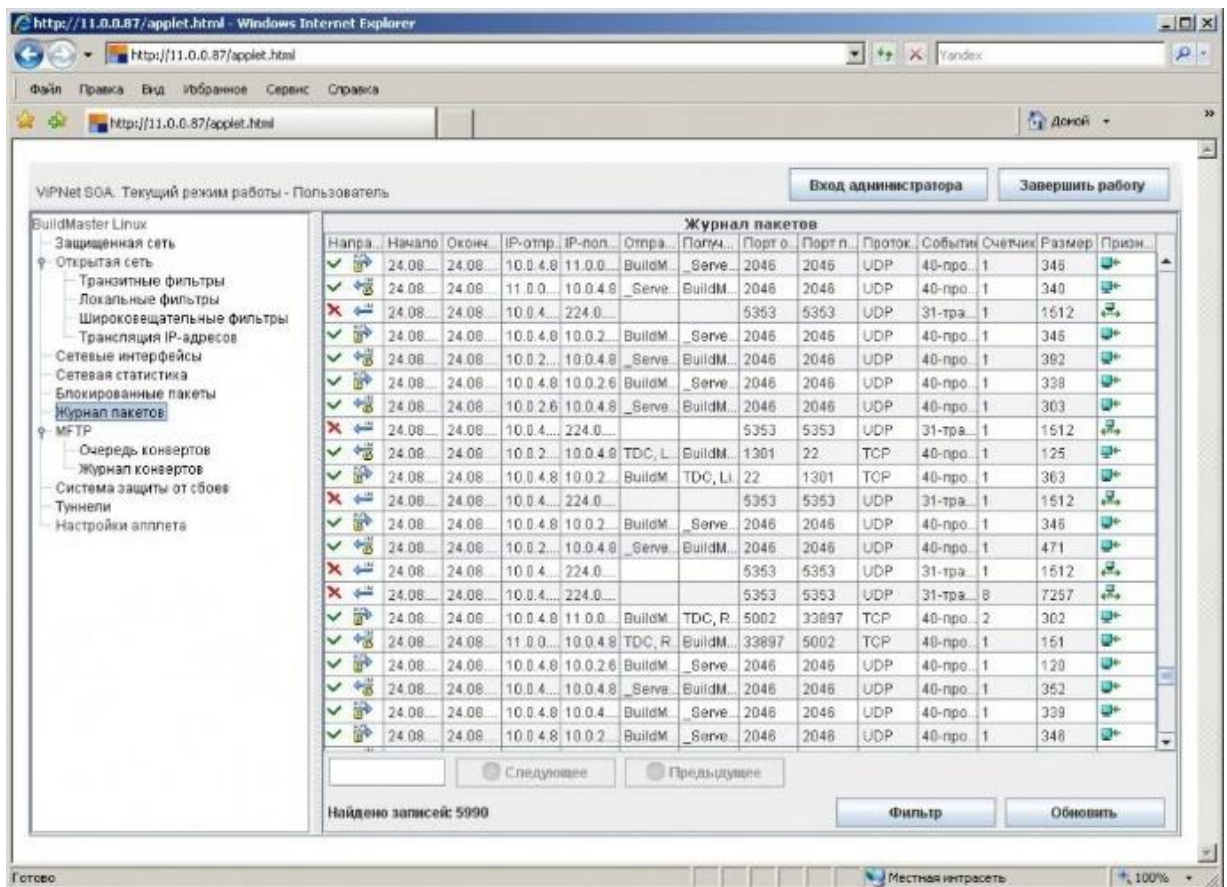


Рисунок 7 – Экранная форма ViPNet Coordinator

Несмотря на шифрование трафика, другой важной функцией программного обеспечения ViPNet Coordinator является захват и фильтрация IP-пакетов, проходящих через каждый сетевой интерфейс координатора. Можно настроить правила противодействия спуфингу для чистого трафика, выбрать систему безопасности для каждого сетевого интерфейса при открытой обработке трафика, правила фильтрации конфигурации для чистого и безопасного трафика.

Еще одной важной функцией является обеспечение открытой трансляции сетевых адресов координатором. Можно настроить статические и динамические правила трансляции для организации соединения для открытия интернет-ресурсов. Координатор также поддерживает преобразование сетевых адресов на прикладном уровне для FTP с целью поддержания клиентов FTP в активном режиме и фильтрацию команд FTP для защиты от неправильного использования значений IP-адресов клиента и сервера.

В таблице 5 представлены основные характеристики действия ViPNet Coordinator.

Таблица 5 – Характеристика ViPNet Coordinator

| Функция | Реализация |
|--------------------------------------|---|
| Туннельные протоколы | По технологии ViPNet (инкапсуляция IP-трафика любого приложения в IP # 241 и UDP) |
| Шифрование и аутентификация | Шифрование по ГОСТ 28147-89 (256 бит). |
| Аутентификация | Аутентификация для каждого зашифрованного IP-пакета на основе симметричной технологии распределения ключей ViPNet и уникального идентификатора. |
| Количество поддерживаемых соединений | Определяется приобретенной лицензией |
| маршрутизация | Статическая маршрутизация Прозрачность для устройств NAT (для безопасного трафика) Поддержка DHCP |

Программное обеспечение включает в себя пару симметричных ключей шифрования, обеспечивающих надежное шифрование. Структура симметричного ключа не требует дополнительных процедур открытой синхронизации для генерации ключа. Это повышает отказоустойчивость системы, устраняет любую остановку при обработке любых сетевых протоколов, обеспечивает немедленную (при получении первого IP-пакета) организацию любых сетевых подключений других участников VPN.

Информация о симметричном ключе распространяется автоматически в случае появления новых пользователей в сети, установки новых ссылок или удаления существующих в центре управления сетью, компрометации ключей или рабочих процедур изменения ключевой информации.

Несмотря на туннелирование трафика между локальными сетями и сетями с удаленной инфраструктурой, можно использовать программное обеспечение ViPNet Coordinator в качестве сервера доступа для удаленных VPN-клиентов (узлов с установленным программным обеспечением ViPNet Client).

Конфигурация и управление:

- Удаленная / локальная настройка с использованием системной консоли. Удаленное конфигурирование и управление возможны при использовании протокола SSH;
- Удаленная настройка основных параметров с помощью программного обеспечения ViPNet Administrator;
- Поддержка SNMP-ловушек для удаленного создания отчетов о событиях;
- Удаленный запрос журнала IP-пакетов (через такие продукты Windows, как ViPNet Coordinator и Client);
- Java-апплет ViPNet SGA v.3 мониторинга текущего состояния;
- Ведение системного журнала на удаленном компьютере.

Вывод: таким образом, на момент проведения проектных работ основным стандартом построения ЛВС являлся Ethernet в различных вариантах. Для

реализации горизонтальной подсистемы использовалась элементная база категории 5е, которая обеспечивает передачу по трактам СКС сигналов всех широко распространенных на практике разновидностей этого сетевого интерфейса. Для достижения задачи применялись все требующиеся меры защиты информации от несанкционированного доступа в соответствии с руководящими документами.

2.4 Разработка интерактивной технологической карты для администратора сети Vip Net по смене ключевой информации

Данная интерактивная карта выполнена на примере одного из классов здания. Она показывает технологию выполнения операций по защите информации и разграничению доступа, по которой вновь прибывший сотрудник (техник) с легкостью может ознакомиться со структурой защиты информации с использованием СЗИ от НСД VipNet. На ней показана: информация об аппаратной части ПК, информацию о VipNe, информацию о работе системы.

На рисунке 8 показана главная страница.

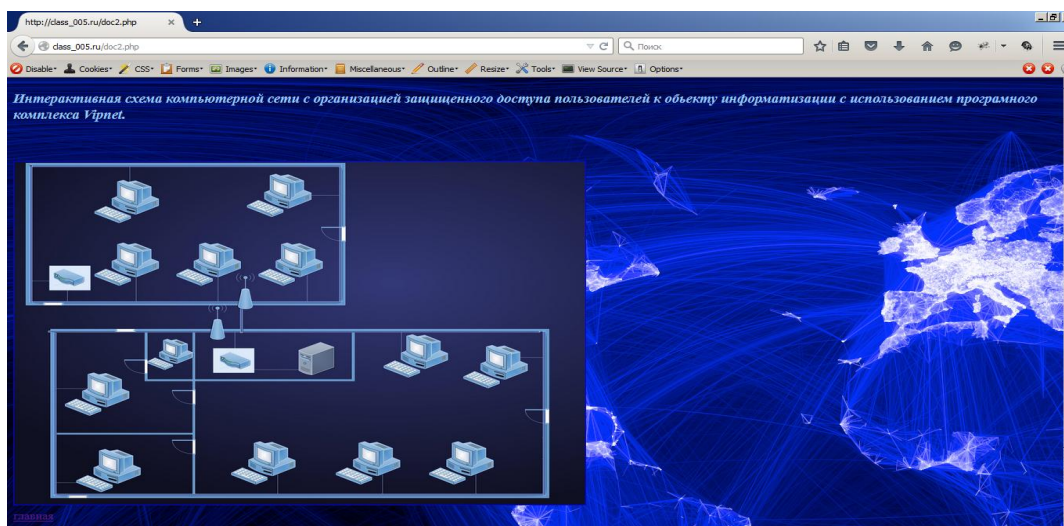


Рисунок 8 - Главная страница

После перехода на главную страницу мы видим схему защищенной сети, при наведении курсора мыши на любую из иконок (ПК) высвечивается частичная информация: разграничения прав доступа, пользователь, имя оператора. Это представлено на рисунке 9.

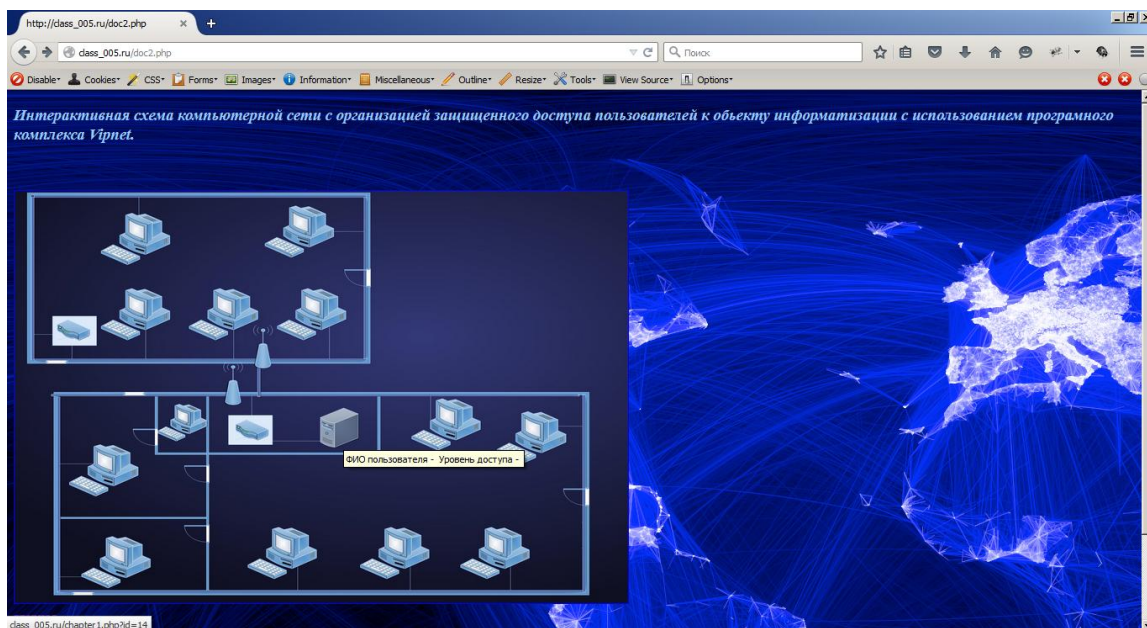


Рисунок 9 - Схема защищенной сети

Далее при нажатии на иконку (ПК) выводится информация об аппаратной части, это показано на рисунках 10-11, в которую входит: данные рабочих станций(Кому разрешен доступ, дата производства ПК, Серийный номер (ID)), информация о работе системы(Варианты доступа, Время работы, Период работы).

Информация об АРМ

| Данные пользователя | | |
|----------------------------|----------------------------|-----------------------|
| ФИО | Уровень доступа | Дата производства АРМ |
| Патченко Максим Дмитриевич | для служебного пользования | 01.12.2013 |
| Характеристики АРМов: | | |
| Состав комплекта АРМов: | Производитель | Серийный номер (ID) |
| Системный блок | AOC E950Swn | T-0029782 |
| Монитор | Microsoft Wired 200 | 6/н |
| Клавиатура | Microsoft L2 200 | 6/н |
| Мышь | Microsoft L2 200 | 6/н |
| Состав ЭВМ | | |

Рисунок 10 - Схема защищенной сети

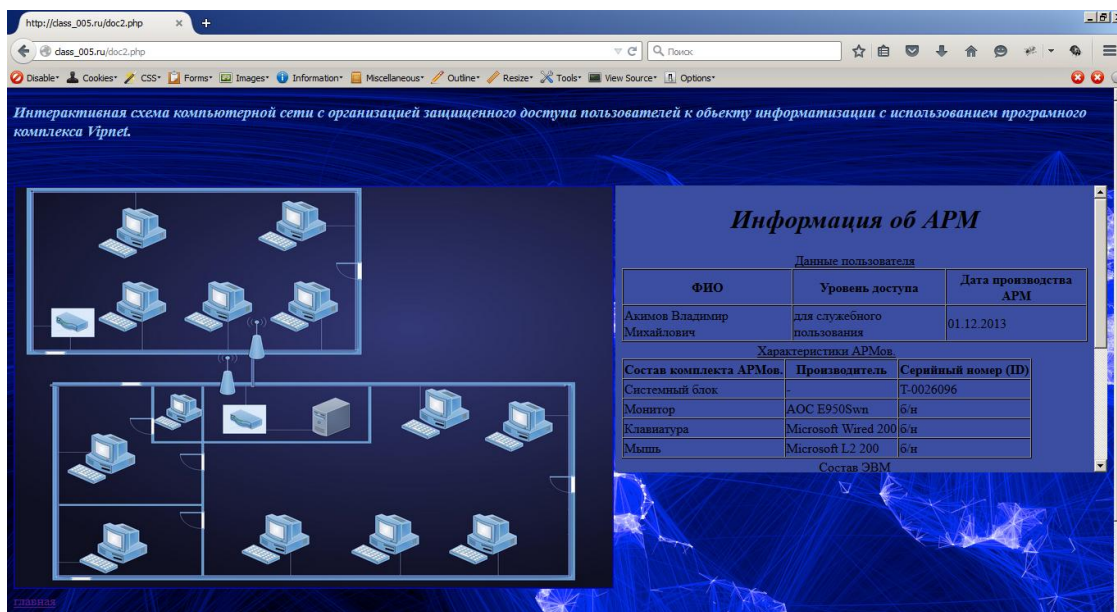


Рисунок 11 - Схема защищенной сети

Вывод: технологическая карта выполнения операций по защите информации в помещении будет служить как инструкция для администратора, так и один из основных документов по созданию руководства пользователя. Например, если выйдет из строя какой-либо АРМ, то системный Администратор при помощи интерактивной технологической карты с легкостью сможет узнать все настройки.

2.5 Проект резервной беспроводной VPN сети с учетом требований по защите информации от НДС

2.5.1 В случае НДС, обрыва кабельного сигнала.

В реализации БС активным оборудованием будет являться беспроводной маршрутизатор D-Link 6600 AP, характеристики которого по стандарту 802.11n представлены в таблице 6.

Исходя из параметров маршрутизатора следует вывод, что заявленная скорость передачи данных в обычном режиме составляет до 130Мбит/с при использовании стандарта 802.11n. Так же, данный маршрутизатор поддерживает технологию WDS, необходимую для реализации БС. При частоте 5 GHz коэффициент усиления антенн равен 6 dBi. Маршрутизатор поддерживает все

необходимые методы безопасности, питание может происходить как от электрической сети 220В, так и при помощи PoE, то есть через отдельный кабель “витой пары”. Настройка маршрутизатора происходит через web-интерфейс или командную строку. Через web-интерфейс удобнее за счет того, что все проводится в графической форме.

Таблица 6 - Характеристики беспроводного маршрутизатора D-Link 6600AP 802.11n

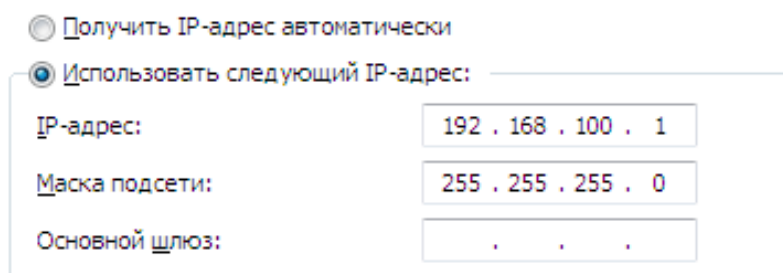
| № | Параметр | Значение |
|----|--------------------------------------|--|
| 1 | Беспроводной интерфейс | 802.11a/b/g/n (2,4/5 ГГц) |
| 2 | Интерфейс | LAN: 10/100/1000 Gigabit Ethernet |
| 3 | Коэффициент усиления антенн: | 5 dBi для 2.4 ГГц и 6 dBi для 5 ГГц |
| 4 | Частота 802.11n: | 2,4 ГГц – 2,497 ГГц и 4,9 ГГц – 5,85 ГГц |
| 5 | Скорость передачи данных: 802.11n | 6,5 Мбит/с – 130 Мбит/с (20 Мбит/с) 6,5 Мбит/с – 300 Мбит/с (40 Мбит/с) |
| 6 | Режимы работы | Точка доступа; WDS; WDS + AP; |
| 7 | Безопасность | SSID: Изоляция станции Безопасность: WEP, Dynamic WEP, WPA Personal/ Enterprise, WPA2 Personal/ Enterprise Аутентификация: Фильтрация по MAC-адресам, 802.1x |
| 8 | Системное управление | Web-интерфейс пользователя: HTTP/HTTPS Командная строка: SNMP, SSH, Telnet |
| 9 | Питание | Адаптер питания: 12В/ 1А Power over Ethernet: 48 В постоянного тока +/- 10% |
| 10 | Рабочая температура | От 0° до 40° С |
| 11 | Рабочая влажность | От 10% до 90% без конденсата |

Настройка маршрутизатора происходит в 5 этапов:

1. Настройка Ethernet-адаптера на необходимую сеть;
2. Настройка частоты и канала передачи данных;
3. Создание точки доступа;

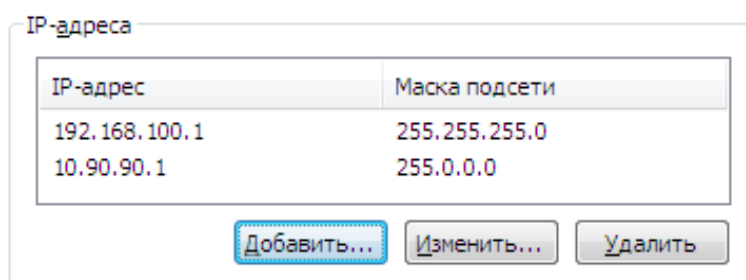
4. Организация безопасности;
5. Создание WDS.

Первый этап подразумевает изменение стандартных параметров маршрутизатора на настраиваемую сеть. Это необходимо для организации контроля доступа к настройкам маршрутизатора и работе в определенной сети. Перед началом работы необходимо сбросить параметры маршрутизатора к заводским путем нажатия и удержания на кнопку “Reset” на маршрутизаторе. После этого установится ip-адрес сетевого адаптера маршрутизатора 10.90.90.91 с маской сети 255.0.0.0. Далее настраивается ip-адрес сетевого адаптера компьютера в этой сети. IP-адрес из сети с маршрутизатором устанавливается альтернативным (рисунок 13), а основным устанавливается ip-адрес, входящий в настраиваемую сеть (рисунок 12).



The screenshot shows a network configuration dialog box with two radio buttons at the top. The first is "Получить IP-адрес автоматически" (unselected). The second is "Использовать следующий IP-адрес:" (selected). Below this are three input fields: "IP-адрес:" with the value "192 . 168 . 100 . 1", "Маска подсети:" with the value "255 . 255 . 255 . 0", and "Основной шлюз:" with the value ". . .".

Рисунок 12 – Настройка основного ip-адреса сетевого адаптера компьютера



The screenshot shows a table titled "IP-адреса" with two columns: "IP-адрес" and "Маска подсети". The table contains two rows of data. Below the table are three buttons: "Добавить...", "Изменить...", and "Удалить". The "Добавить..." button is highlighted with a blue dashed border.

| IP-адрес | Маска подсети |
|---------------|---------------|
| 192.168.100.1 | 255.255.255.0 |
| 10.90.90.1 | 255.0.0.0 |

Рисунок 13 – Авторизация при входе в web-интерфейс маршрутизатора.

На рисунке 14 показан web-интерфейс, через который происходит настройка беспроводного маршрутизатора.

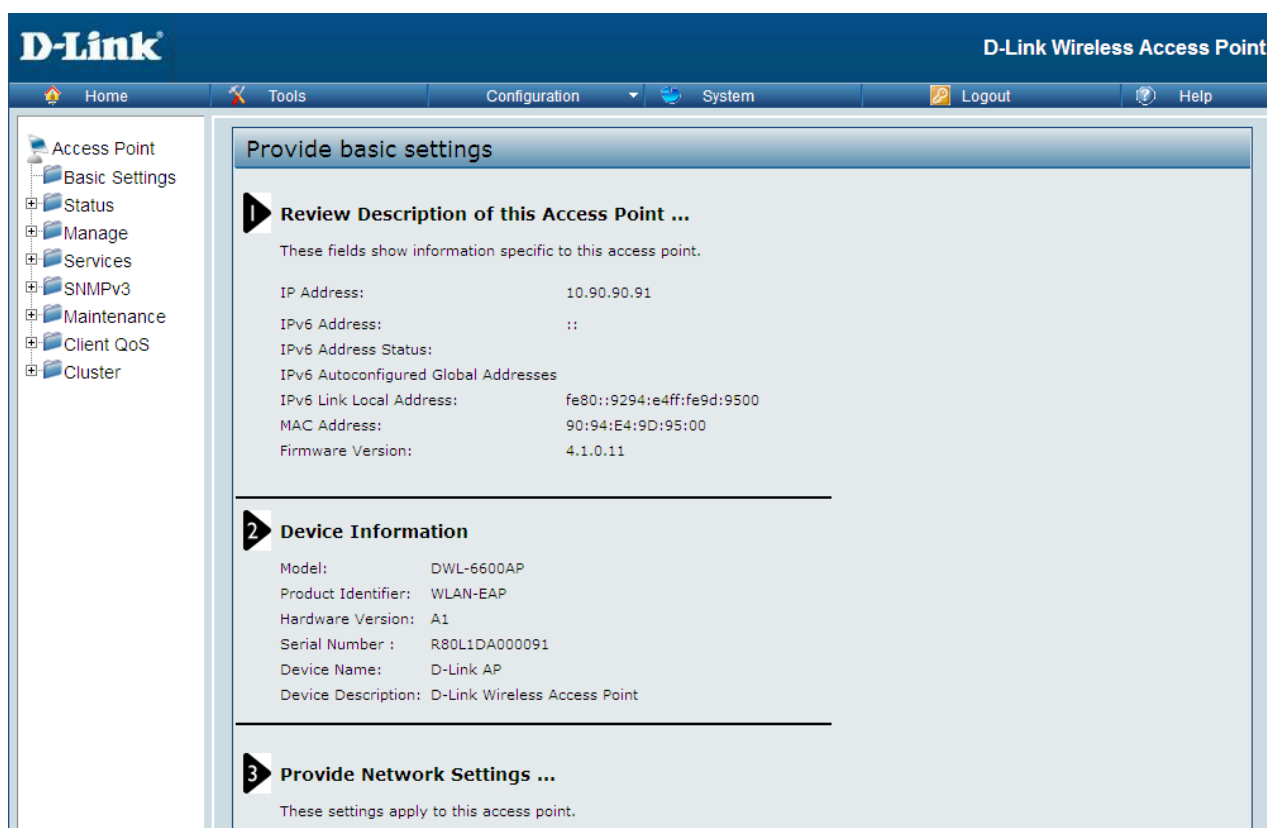


Рисунок 14 – Web-интерфейс маршрутизатора.

Следующим шагом следует настроить сетевой адаптер маршрутизатора. Для этого во вкладке “Manage” выбирается меню “Ethernet Settings”. Если в сети работает служба DHCP, необходимо исключить от раздачи ip-адресов для маршрутизаторов. В выпадающем списке строки “Connection Type” выбирается параметр “Static IP” для настройки статического ip-адреса. В поля строки “Static IP Address” вводится ip-адрес необходимой сети, задается соответствующая маска этой сети в строке “Subnet Mask”. В поля строки “Default Gateway” проставляются нули, так как связи с другими сетями не будет (рисунок 15).

После проведенных действий нажав кнопку “Apply” осуществляется переход через адресную строку вводом нового ip-адреса маршрутизатора.

Второй этап включает в себя выбор частоты и канала передачи данных для работы маршрутизатора. Это происходит во вкладке Wireless Settings, рисунок.

| | | | |
|---|---|-------|-------------|
| Hostname | DLINK-WLAN-AP | | |
| Internal Interface Settings | | | |
| MAC Address | 90:94:E4:9D:95:00 | | |
| Management VLAN ID | 1 | | |
| Untagged VLAN | <input checked="" type="radio"/> Enabled <input type="radio"/> Disabled | | |
| Untagged VLAN ID | 1 | | |
| Connection Type | Static IP ▾ | | |
| Static IP Address | 192 | . 168 | . 100 . 201 |
| Subnet Mask | 255 | . 255 | . 255 . 0 |
| Default Gateway | 0 | . 0 | . 0 . 0 |
| DNS Nameservers | <input type="radio"/> Dynamic <input checked="" type="radio"/> Manual | | |
| | | . | |
| | | . | |
| IPv6 Admin Mode | <input checked="" type="radio"/> Enabled <input type="radio"/> Disabled | | |
| IPv6 Auto Config Admin Mode | <input checked="" type="radio"/> Enabled <input type="radio"/> Disabled | | |
| Static IPv6 Address | :: | | |
| Static IPv6 Address Prefix Length | 0 | | |
| Static IPv6 Address Status | | | |
| IPv6 Autoconfigured Global Addresses | | | |
| IPv6 Link Local Address | fe80::9294:e4ff:fe9d:9500 | | |
| Default IPv6 Gateway | :: | | |
| Click "Apply" to save the new settings. | | | |
| <input type="button" value="Apply"/> | | | |

Рисунок 15 – Настройка сетевого адаптера маршрутизатора.

Параметр RI (Radio Interface) означает использование частоты 5 ГГц, RI2 работает на частоте 2,4 ГГц. Так как в предложении по организации сети выбрана частота 5 ГГц, то настраивается RI. Напротив выбирается пункт “On”, в выпадающем списке “Mode” необходимо выбрать стандарт “5 GHz IEEE 802.11n”. Каналы, доступные для выбора при настройке маршрутизатора: 36, 44, 52, 60, 149, 157. Оптимально выбирать высший канал, так как высокие частоты поддерживают не все антенны и беспроводные устройства, а нижние настраиваются по умолчанию в иных случаях. Выбирается канал 157 с частотой 5,785 ГГц (рисунок 16).

The image shows a configuration window with the following settings:

- TSPEC Violation Interval:** 300 (Sec, Range: 0 - 900, 0 Disables)
- Radio Interface:**
 - On/Off: On (selected)
 - MAC Address: 90:94:E4:9D:95:00
 - Mode: 5 GHz IEEE 802.11n
 - Channel: 157
 - Station Isolation:
- Radio Interface 2:**
 - On/Off: Off (selected)
 - MAC Address: 90:94:E4:9D:95:10
 - Mode: IEEE 802.11b/g/n
 - Channel: Auto
 - Station Isolation:
- AeroScout™ Engine Protocol Support:** Disabled

Click "Apply" to save the new settings.

Рисунок 16 – Выбор частоты и канала передачи данных.

После выбора частоты и канала передачи данных следует третий этап, создание точки доступа. Для выполнения этого этапа осуществляется переход во вкладку VAP (Virtual Access Point). На открывшейся web-странице выбирается настраиваемая частота, параметр "Radio". Выбирается первый пункт в выпадающем списке, так как настраивается канал на частоте 5 GHz. Ниже заполняются поля для создания точки доступа. Значение SSID является идентификатором беспроводной сети. Для скрытия SSID необходимо убрать выделенный пункт "Broadcast SSID". В таком случае выполняется метод защиты беспроводной сети "скрытие SSID", указанный ранее в работе. Пункт "Security" включает в себя способ и ключ шифрования данных. Как указано ранее, для защиты сети необходимо выбрать тип шифрования WPA2 и записать ключ максимальной длины (32 символа) используя цифры, знаки пунктуации, регистр, разные языки. Следующий пункт "Mac Auth Type" выполняет метод защиты "фильтрация по MAC-адресу". В выпадающем списке необходимо выбрать значение "Local", так как список будет храниться на самих

маршрутизаторах, то есть локально. После настройки основных пунктов необходимо их сохранить нажатием на кнопку “Apply” (рисунок 17).

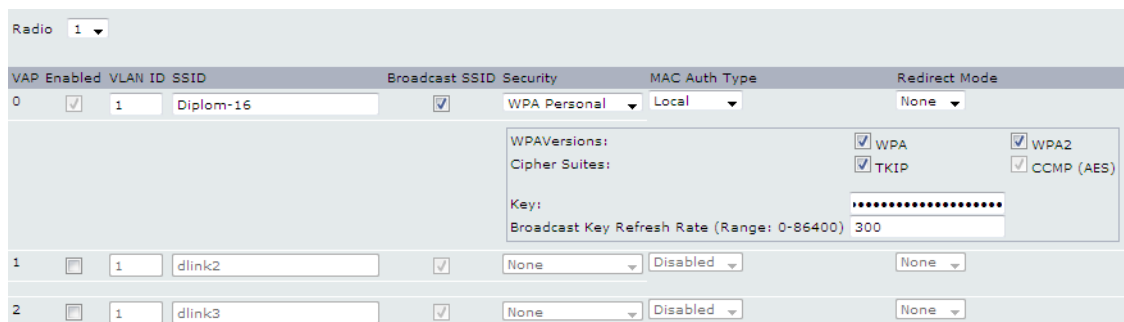


Рисунок 17 – Настройка точки доступа.

После настройки точки доступа заполняется список MAC-адресов для фильтрации подключаемых устройств. Для этого, при переходе во вкладку “MAC-auth” выбирается способ фильтрации “Filter”. Первый способ означает подключение только тех устройств, MAC-адреса которых указаны в списке, а второй способ наоборот, блокировка подключения тех устройств, MAC-адреса которых указаны в списке. В данном методе защиты сети будет использоваться ситуация, когда в разрешающем списке будет находиться только 1 случайный MAC-адрес, который не известен никому (рисунок 18).

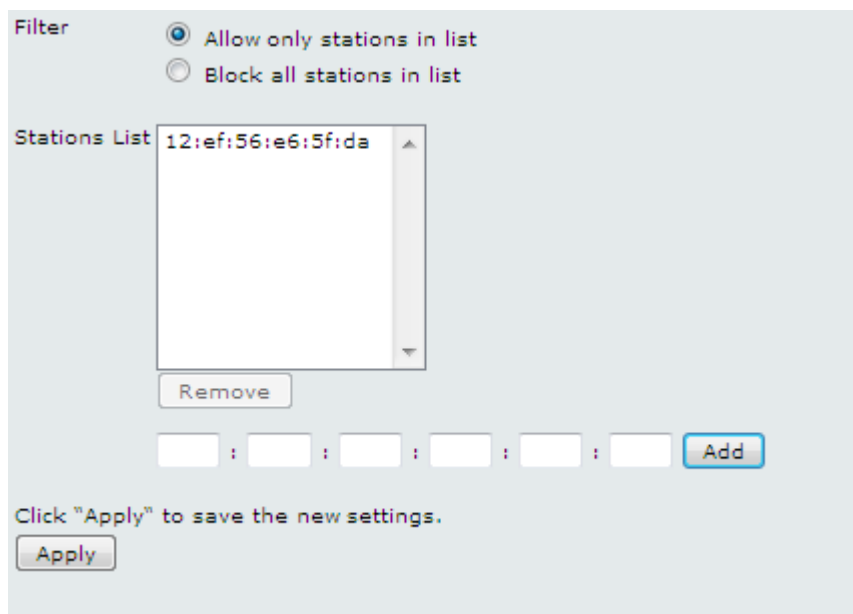


Рисунок 18 – Настройка MAC-аутентификации.

Далее запускается маршрутизатор в режиме кластера, для создания соединения типа WDS между маршрутизаторами. В меню при выборе пункта “Cluster” открывается web-страница с кнопкой запуска кластера (рисунок 19).

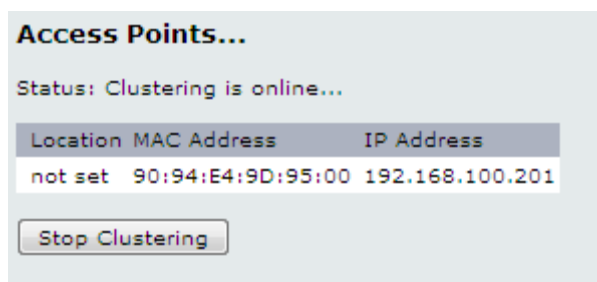


Рисунок 19 – Старт режима кластера.

Для продолжения настройки, данные мероприятия должны быть выполнены на всех маршрутизаторах. После этого, поочередно продолжая настраивать сеть, необходимо на маршрутизаторах открыть вкладку “WDS”, в строке “Spanning Tree Mode” выбрать значение “Enabled”, параметр “Radio” должен иметь значение “1”. В строке “Local Address” указан MAC-адрес данного маршрутизатора.

Этот MAC-адрес необходим для связи с соседними маршрутизаторами, он должен вводиться в строку “Remote Address” (рисунок 20).

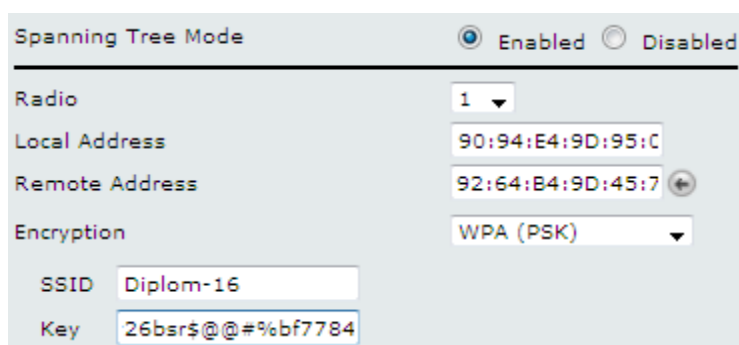


Рисунок 20 – Настройка WDS.

На маршрутизаторах, которые имеют 2 соединения, настройка WDS происходит к каждому соединению отдельно. После проведенных действий маршрутизаторы автоматически производят подключение и создание общей БС. Проверяется правильность настройки и создания сети путем подключения компьютера к крайнему маршрутизатору и проверкой соединения утилитой

PING к каждому маршрутизатору. Изначально, пакеты могут не доходить до адресата и требуется время ожидания. Для удобства используется атрибут “-t” при запуске утилиты PING. Команда выглядит следующим образом “ping <ip-адрес> -t”. Таким образом, утилита не ограничивает количество отправок пакетов данным адресату, а осуществляет запросы до того момента, пока пользователь сам не прекратит работу утилиты.

2.5.2. Выбор пассивного оборудования

К пассивному оборудованию относятся элементы сети, которые не получают питание от электрической сети или других источников, и выполняют функцию распределения или снижения уровня сигналов. К такому оборудованию относятся:

1. Кабельная система: кабель (коаксиальный, оптоволоконный, витая пара).
2. Вилка/розетка.
3. Патч-панель.
4. Оборудование трассы для кабелей (кабельные лотки, монтажные шкафы, стойки и телекоммуникационные шкафы).

Для данной работы потребуются следующие элементы оборудования:

1. Антенны для маршрутизаторов.
2. Соединительный кабель для подключения антенны к маршрутизатору.
3. Кронштейн для антенны.
4. Кабель “витая пара” для подключения маршрутизатора на объекте.

Антенна для маршрутизатора выбирается из следующих параметров:

- направление сигнала (всенаправленное, направленное, узконаправленное);
- дальность распространения сигнала;
- частота работы (2,4 ГГц или 5 ГГц).

Исходя из необходимых значений распространения сигнала, выбрана направленная антенна Wivat AT-5.8/Patch (таблица 7).

Таблица 7 – Характеристики направленной антенны Wivat AT-5.8/Patch(7)

| № | Параметр | Значение |
|---|----------------------|-----------------|
| 1 | Тип | Направленная |
| 2 | Рабочие частоты | 5.8 GHz |
| 3 | Разъем | RP-SMA |
| 4 | Коэффициент усиления | 7 dBi |
| 5 | Габариты | 85 x 90 x 12 мм |
| 6 | Рабочие температуры | До -20С до +40С |

Из представленных параметров антенны делается вывод, что она способна реализовать распространение сигнала в любое время года на необходимое расстояние, а также, обеспечивается быстрое размещение данной антенны на зданиях при развертывании всей сети.

Таким образом выбранное оборудование в полной мере соответствует заявленным требованиям при организации БС, а сама БС соответствует требованиям в организации защищенной связи между объектами пограничных органов. Все методы защиты БС соблюдены и организованны. Анализ БС показал, что зона покрытия сигнала не выходит за пределы контролируемой территории. Скорость передачи информации между крайними объектами способна организовать видео-поток данных без каких-либо проблем.

3 АПРОБАЦИЯ РАЗРАБОТАННОЙ КОМПЬЮТЕРНОЙ СЕТИ АППАРАТНО-ТЕХНИЧЕСКИМ КОМПЛЕКСОМ ПРИ ОРГАНИЗАЦИИ ЗАЩИЩЕННОГО ДОСТУПА

3.1 Технические мероприятия по защите информации от НСД

Организация независимого питания оборудования; Используются Источники бесперебойного питания (ИБП)- автоматическое электронное устройство с аккумуляторной батареей предназначенное для бесперебойного кратковременного снабжения электрической энергии компьютера и его компонентов с целью корректного завершения работы и сохранения данных в случае резкого падения или отсутствия входного питающего напряжения системы. Массовое использование ИБП связано с обеспечением бесперебойной работы компьютеров, позволяющее подключенному к ИБП оборудованию при пропадании электрического тока или при выходе его параметров за допустимое нормы, некоторое непродолжительное (как правило – до 10-15 минут) время продолжить работу:

- Экранирование помещений обработки данных (использование трехкамерных стекол; использование пластмассовых труб, а не железных; увеличение ширины стен помещения, в котором находится объект информатизации)

- Введение на объект информатизации системы охраны помещений (сигнализация, датчики движения, видеокамеры и т.д.)

- Организация пропускного и внутриобъектового режима –Это комплекс мер по недопущению бесконтрольного перемещения лиц по предприятию, между охраняемыми зонами.

- Магнитные карты, ID-карты, Электронные карты, Оптические карты.

- Программно-аппаратная защита информации (Принцип обоснованности доступа, принцип достаточной глубины контроля доступа, принцип обоснованности доступа, принцип персональной ответственности)

- Защита информационно-программного обеспечения на уровне операционных систем.

Технические мероприятия по защите информации от НСД представлены на рисунке 21.

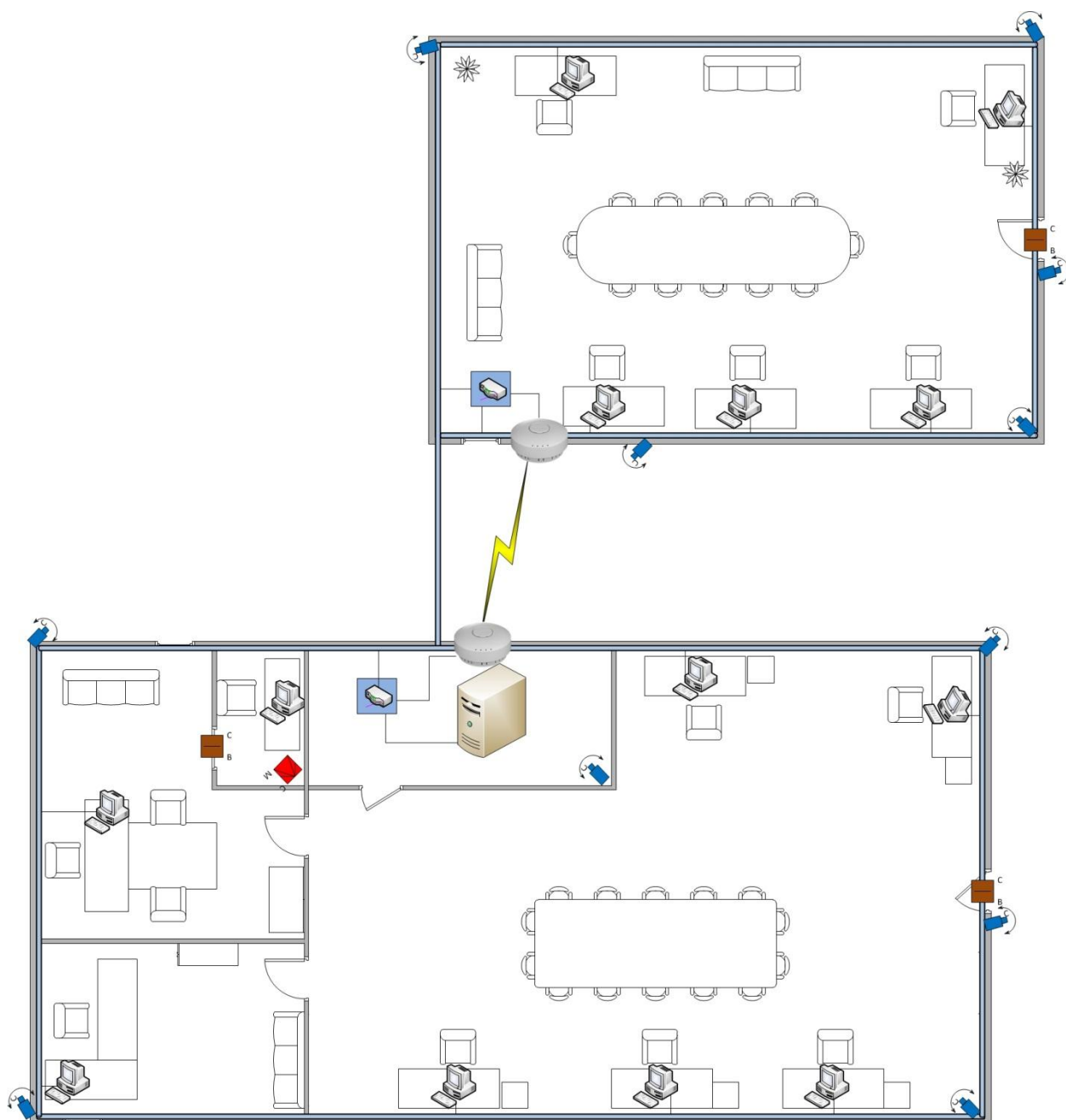


Рисунок 21 - Технические мероприятия по защите информации от НСД

Настройка сервера маршрутизатора WH-100: оператору HW-100 необходимо получить дистрибутив ключей от оператора VIP Net ЦУС-УКЦ и начать настройку PC-100.

Запустите WH-100. После загрузки, система предложит ввести имя пользователя: **VIP Net** и пароль: **vipnet**.

Последовательность первичной инициализации:

- Выберите full screen interface – 2 пункт меню.

```
Vipnet Coordinator HW100-3.0(201) tty1
hw100 login: vipnet
Password:

1) command line interface
2) full-screen interface
Please select setup wizard operating mode : 2_
```

Рисунок 22 – Выбор режима инициализации

- В открывшемся окне нажмите «Далее», выберите USB-Flash.

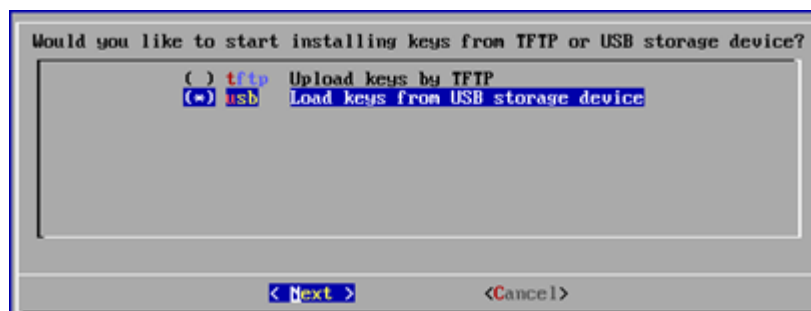


Рисунок 23 – Выбор места хранения дистрибутива ключей

Система начнёт поиск дистрибутивов ключей на USB накопителе. Выберите из списка найденных дистрибутивов тот, который предназначен для HW-100, введите пароль к дистрибутиву. Начнется процесс установки адресных справочников и ключей узлов.

Настройка сетевых адаптеров eth0 и eth1. Необходимо настроить два сетевых адаптера, первый – eth0 является шлюзом для внутренней сети, второй – eth1 является шлюзом для внешней сети (192.168.0.0). настройте их согласно схеме на рисунке № 21.

Далее укажите шлюз – 192.168.0.254. После проведения первичной инициализации система вновь потребует ввести логин и пароль.

Для окончательной настройки HW-100 следует ввести последовательность команд: **enable** – переход в привилегированный режим. После ввода команды необходимо ввести пароль администратора защищённой сети.

Данный пароль задаётся на этапе создания дистрибутивов ключей в УКЦ (Рисунок 24).

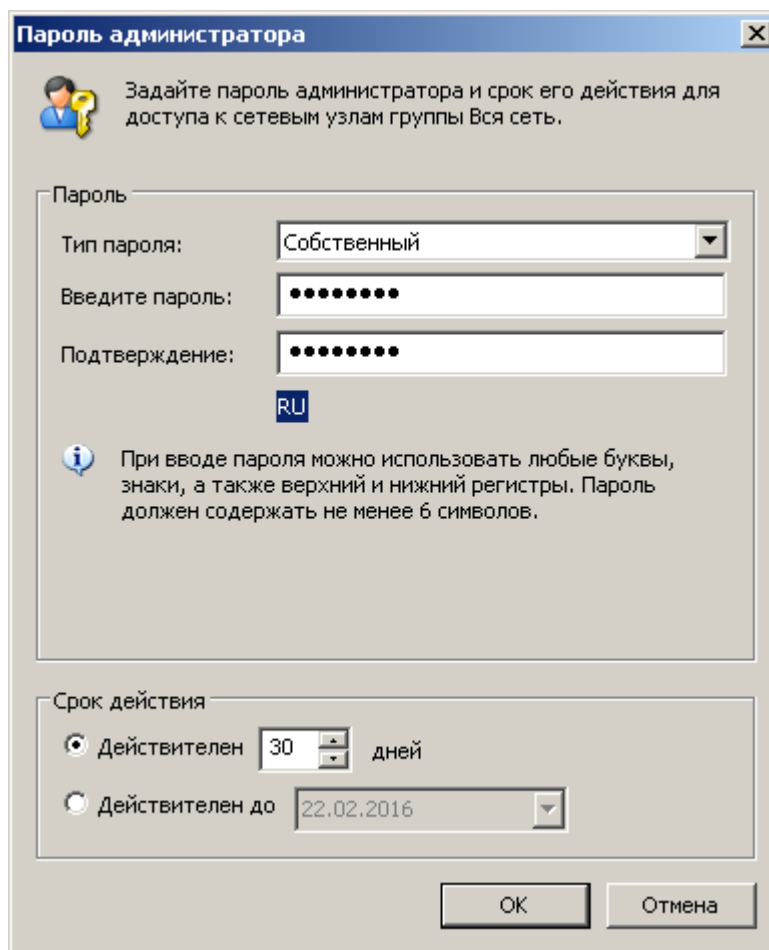


Рисунок 24 – Установка пароля администратора

- mftp start
- iplir start
- inet add route 192.168.x.0 gw 192.168.0.x netmask 255.255.255.0
- inet show routing

Вывод: технологическая карта выполнения операций по защите информации в помещении будет служить как инструкция для администратора, так и один из основных документов по созданию руководства пользователя. Например, если выйдет из строя какой-либо АРМ, то системный Администратор при помощи интерактивной технологической карты с легкостью сможет узнать все настройки.

3.2 Тестирование ViPNet для организации защищенного доступа к объектам информатизации

На момент тестирования решения не было данных об измерении производительности версии программного обеспечения ViPNet Custom для различных конфигураций. Было интересно сравнить результаты программной реализации ViPNet Custom с аппаратной реализацией ViPNet Coordinator HW1000 / HW2000, производительность которой известна и задокументирована производителем.

Самые мощные конфигурации платформы HW имеет следующие характеристики (таблица 8).

Таблица 8 – Характеристика платформы

| Тип | Платформа | ЦПУ | Пропускная способность |
|-----------|--------------------|-----------------------|------------------------|
| HW1000 Q2 | AquaServer T40 S44 | Intel Core i5-750 | До 280 Мб / с |
| HW2000 Q3 | AquaServer T50 D14 | Intel Xeon E5-2620 v2 | До 2,7 Гбит / с |

Изначально мы получили доступ к оборудованию со следующими характеристиками:

- 1) IBM system x3550 M4 2 x E5-2960v2 10 ядер 64 ГБ ОЗУ;
- 2) Fujitsu TX140 S1 E3-1230v2 4 ядра 16 ГБ оперативной памяти.

В IBM мы организовали 2 виртуальных сервера с виртуальным 10-гигабитным коммутатором на основе платформы ESX 6.0u1b, а затем мы оценили общую производительность двух виртуальных машин.

Описание стенда:

1. Сервер IBM system x3550 M4 2 x E5-2960v2 10 ядер 64 ГБ ОЗУ, ESXi 6.0u1.
2. Для каждой виртуальной машины (VM) выделяется один физический процессор с 10 ядрами.
3. VM1: Windows 2012 R2 (ViPNet Coordinator 4.3_ (1.33043)):
 - а. 1 процессор 10 ядер;

- б. 8 ГБ ОЗУ.
- 4. VM2: Windows 8.1 (ViPNet Client 4.3_ (1.33043)):
 - а. 1 процессор 10 ядер;
 - б. 8 ГБ ОЗУ.
- 5. Виртуальные машины подключены к виртуальному коммутатору 10 Гбит / с, установлен MTU 9000.
- 6. Fujitsu TX140 S1 E3-1230v2 4-ядерный сервер, 16 ГБ ОЗУ, Windows 2012 R2, ViPNet Client 4.3_ (1.33043).

Физические серверы IBM и Fujitsu соединены гигабитной сетью с MTU 9000. Hyper Threading отключена на обоих серверах. Iperf3 использовался в качестве загрузочного программного обеспечения.

Компоновка стенда показана на рисунке 25.

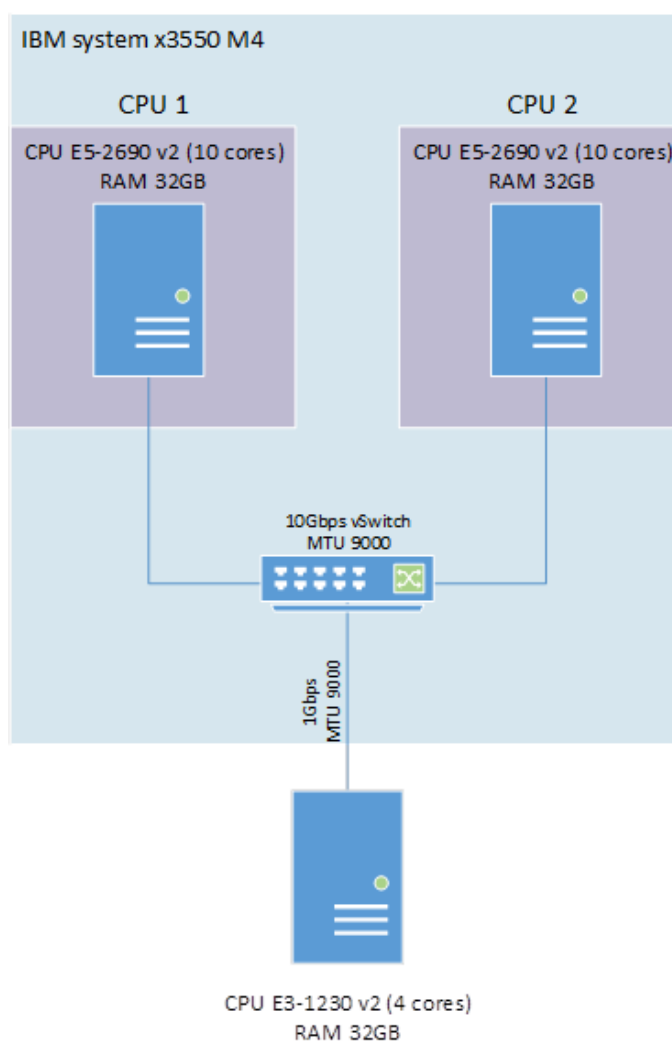


Рисунок 25 - Схема организации испытательного стенда

На VM1 сторона, Iperf3 работает в режиме сервера. Серверная VM2 Iperf3 запущен с параметрами Iperf.exe -с IP_server -P10 -t 100, где параметр -P10 указывает количество потоков на сервере, равное количеству ядер.

Результаты показаны в таблице 9 и на рисунках 26-27.

Таблица 9 - Результат теста

| хозяин | Загрузка процессора | Достигнутая нагрузка | канал |
|--|---------------------|----------------------|-------------|
| VM1 Windows 2012 R2 (Координатор ViPNet 4.3) | 100% | 2,47 Гбит / с | 10 Гбит / с |
| VM2 Windows 8.1 (ViPNet Client 4.3) | 100% | 2,47 Гбит / с | 10 Гбит / с |

```

[ 51] 310.00-311.00 sec 31.8 MBytes 267 Mbits/sec
[ 71] 310.00-311.00 sec 33.5 MBytes 281 Mbits/sec
[ 91] 310.00-311.00 sec 31.8 MBytes 266 Mbits/sec
[ 11] 310.00-311.00 sec 31.3 MBytes 263 Mbits/sec
[ 13] 310.00-311.00 sec 31.1 MBytes 261 Mbits/sec
[ 15] 310.00-311.00 sec 30.8 MBytes 259 Mbits/sec
[ 17] 310.00-311.00 sec 27.9 MBytes 234 Mbits/sec
[ 19] 310.00-311.00 sec 25.9 MBytes 217 Mbits/sec
[ 21] 310.00-311.00 sec 24.7 MBytes 207 Mbits/sec
[ 23] 310.00-311.00 sec 25.5 MBytes 214 Mbits/sec
[SUM] 310.00-311.00 sec 294 MBytes 2.47 Gbits/sec

[ 51] 311.00-312.00 sec 34.0 MBytes 285 Mbits/sec
[ 71] 311.00-312.00 sec 32.9 MBytes 276 Mbits/sec
[ 91] 311.00-312.00 sec 30.4 MBytes 255 Mbits/sec
[ 11] 311.00-312.00 sec 29.2 MBytes 245 Mbits/sec
[ 13] 311.00-312.00 sec 30.6 MBytes 257 Mbits/sec
[ 15] 311.00-312.00 sec 29.9 MBytes 251 Mbits/sec
[ 17] 311.00-312.00 sec 27.9 MBytes 234 Mbits/sec
[ 19] 311.00-312.00 sec 27.6 MBytes 232 Mbits/sec
[ 21] 311.00-312.00 sec 26.5 MBytes 223 Mbits/sec
[ 23] 311.00-312.00 sec 24.3 MBytes 204 Mbits/sec
[SUM] 311.00-312.00 sec 293 MBytes 2.46 Gbits/sec

```

Рисунок 26 - Вывод iPerf3 на VM1 Windows 2012 R2 (ViPNet Coordinator 4.3)

```

[ 41] 310.00-311.00 sec 31.9 MBytes 267 Mbits/sec
[ 61] 310.00-311.01 sec 33.6 MBytes 281 Mbits/sec
[ 81] 310.00-311.01 sec 31.8 MBytes 265 Mbits/sec
[ 10] 310.00-311.01 sec 31.5 MBytes 263 Mbits/sec
[ 12] 310.00-311.01 sec 31.2 MBytes 261 Mbits/sec
[ 14] 310.00-311.01 sec 31.0 MBytes 259 Mbits/sec
[ 16] 310.00-311.01 sec 28.0 MBytes 234 Mbits/sec
[ 18] 310.00-311.01 sec 26.0 MBytes 217 Mbits/sec
[ 20] 310.00-311.01 sec 24.8 MBytes 207 Mbits/sec
[ 22] 310.00-311.01 sec 25.5 MBytes 213 Mbits/sec
[SUM] 310.00-311.00 sec 295 MBytes 2.47 Gbits/sec

[ 41] 311.00-312.01 sec 33.6 MBytes 281 Mbits/sec
[ 61] 311.01-312.01 sec 33.1 MBytes 277 Mbits/sec
[ 81] 311.01-312.01 sec 30.8 MBytes 257 Mbits/sec
[ 10] 311.01-312.01 sec 29.0 MBytes 243 Mbits/sec
[ 12] 311.01-312.01 sec 31.0 MBytes 260 Mbits/sec
[ 14] 311.01-312.01 sec 30.2 MBytes 253 Mbits/sec
[ 16] 311.01-312.01 sec 28.0 MBytes 234 Mbits/sec
[ 18] 311.01-312.01 sec 27.8 MBytes 232 Mbits/sec
[ 20] 311.01-312.01 sec 26.8 MBytes 224 Mbits/sec
[ 22] 311.01-312.01 sec 24.5 MBytes 205 Mbits/sec
[SUM] 311.00-312.01 sec 295 MBytes 2.46 Gbits/sec

```

Рисунок 27 - Вывод iPerf3 на VM2 Windows 8.1 (ViPNet Client 4.3)

На основании полученных результатов были сделаны следующие выводы:

- 1) изменения позволили добиться максимальной производительности шифрования при полном использовании процессора;
- 2) суммарную производительность при использовании двух Xeon E5-2960v2 можно считать равной 5 Гбит / с;
- 3) с учетом общей производительности двух процессоров результирующая производительность шифрования удваивает официальные результаты ViPNet Coordinator HW2000.

Во время тестирования не было разницы в пропускной способности между ViPNet Client и ViPNet Coordinator.

Для дальнейшего исследования производительности программной части программного обеспечения ViPNet мы получили доступ к двум отдельным блейд-серверам со следующими характеристиками:

- ЦП 2 x E5-2690v2 10 ядер;
- ESXi 6.0u1.

Каждая виртуальная машина расположена на своем отдельном «блейде».

1. VM1: Windows 2012 R2 (ViPNet Client 4.3_ (1.33043)):

- 2 процессора 20 ядер;
- 32 ГБ ОЗУ.

2. VM2: Windows 2012 R2 (ViPNet Client 4.3_ (1.33043)):

- 2 процессора 20 ядер;
- 32 ГБ ОЗУ.

Сетевое соединение между виртуальными машинами осуществляется через блейд-сервер с пропускной способностью 10 Гбит / с с MTU 9000. Nuperg Threading отключена на обоих серверах.

Для моделирования нагрузки использовалось программное обеспечение iPerf3 и, кроме того, Ntttcr со следующими основными параметрами:

- 1) на принимающей стороне:
 - a. Iperf.exe -s;

2) на стороне передачи:

а. Iperf.exe -cserver_ip -P20 -t100;

3) на принимающей стороне:

а. NTttcp.exe -r -wu 5 -cd 5 -m 20, *, self_ip -l 64k -t 60 -sb 128k -rb 128k;

4) на стороне передачи:

а. NTttcp.exe -s -wu 5 -cd 5 -m 20, *, server_ip -l 64k -t 60 -sb 128k -rb 128k.

Организация стенда показана на рисунке 28.



Рисунок 28 - Схема организации стенда

Для начала давайте проверим пропускную способность сети без шифрования. Программное обеспечение ViPNet не установлено.

Тест проводился трижды. Результаты показаны в таблице 10 и на рисунках 29-30.

Таблица 10 - Результат теста

| хозяин | Загрузка процессора | Достигнутая нагрузка | канал |
|--------|---------------------|----------------------|-------------|
| NTttcp | 2,5% | 8,5 Гбит / с | 10 Гбит / с |
| Iperf | четыре% | 9,3 Гбит / с | 10 Гбит / с |

```
##### Totals: #####

Bytes(MEG)      realtime(s)  Avg Frame Size  Throughput(MB/s)
=====
65538.250000    60.000      8659.662        1092.304

Throughput(Buffers/s)  Cycles/Byte      Buffers
=====
8738.433              1.286            524306.000

DPCs(count/s)  Pkts(num/DPC)      Intr(count/s)  Pkts(num/intr)
=====
17612.350      2.884              24298.150      2.091

Packets Sent  Packets Received  Retransmits  Errors  Avg. CPU %
=====
7935857       3048096           916          0       2.454

c:\>
```

Рисунок 29 - Результат теста Ntttcp без шифрования

```
[ 27] 0.00-100.01 sec 5.42 GBytes 465 Mbits/sec receiver
[ 29] 0.00-100.01 sec 0.00 Bytes 0.00 bits/sec sender
[ 29] 0.00-100.01 sec 5.40 GBytes 464 Mbits/sec receiver
[ 31] 0.00-100.01 sec 0.00 Bytes 0.00 bits/sec sender
[ 31] 0.00-100.01 sec 5.39 GBytes 463 Mbits/sec receiver
[ 33] 0.00-100.01 sec 0.00 Bytes 0.00 bits/sec sender
[ 33] 0.00-100.01 sec 5.37 GBytes 461 Mbits/sec receiver
[ 35] 0.00-100.01 sec 0.00 Bytes 0.00 bits/sec sender
[ 35] 0.00-100.01 sec 5.36 GBytes 460 Mbits/sec receiver
[ 37] 0.00-100.01 sec 0.00 Bytes 0.00 bits/sec sender
[ 37] 0.00-100.01 sec 5.34 GBytes 459 Mbits/sec receiver
[ 39] 0.00-100.01 sec 0.00 Bytes 0.00 bits/sec sender
[ 39] 0.00-100.01 sec 5.32 GBytes 457 Mbits/sec receiver
[ 41] 0.00-100.01 sec 0.00 Bytes 0.00 bits/sec sender
[ 41] 0.00-100.01 sec 5.31 GBytes 456 Mbits/sec receiver
[ 43] 0.00-100.01 sec 0.00 Bytes 0.00 bits/sec sender
[ 43] 0.00-100.01 sec 5.29 GBytes 454 Mbits/sec receiver
[ 45] 0.00-100.01 sec 0.00 Bytes 0.00 bits/sec sender
[ 45] 0.00-100.01 sec 5.27 GBytes 453 Mbits/sec receiver
[SUM] 0.00-100.01 sec 0.00 Bytes 0.00 bits/sec sender
[SUM] 0.00-100.01 sec 109 GBytes 9.32 Gbits/sec receiver
```

Рисунок 30 - Результат теста Iperf без шифрования

На основании результатов были сделаны следующие выводы:

- 1) достигнута пропускная способность сети 10 Гбит / с;

2) есть разница в результатах программного обеспечения для тестирования. Кроме того, для надежности результаты будут опубликованы как для Iperf, так и для Ntttcp.

Таким образом, тестирование показало результативность применения аппаратной платформы при работе спроектированной компьютерной вычислительной сети.

3.3 Экономическая оценка спроектированной СКС с учетом СЗИ от НСД «VIPNET»

При разработке проекта СКС была спроектирована компьютерная сеть с применением структурированной кабельной системы на основе витой пары и оптоволокна.

Были применены следующие стандарты СКС:

– ГОСТ Р 53245-2008 - Информационные технологии. Системы кабельные структурированные. Монтаж основных узлов системы. Методы испытания;

– ГОСТ Р 53246-2008 - Информационные технологии. Системы кабельные структурированные. Проектирование основных узлов системы. Общие требования;

– Международный стандарт ISO/IEC 11801 Generic Cabling for Customer Premises;

– Европейский стандарт EN 50173 Information technology– Generic cabling systems;

Для реализации горизонтальной подсистемы была использована элементная база категории 5е, которая обеспечивает передачу по трактам СКС сигналов всех широко распространенных на практике разновидностей этого сетевого интерфейса ЛВС. Данная сеть позволяет подключить 16 рабочих места (с возможностью расширения). Обеспечивается передача данных со скоростью 100 Мбит/с.

Спроектированная компьютерная сеть отвечает всем требованиям руководящих документов по защите информации от несанкционированного доступа.

Экономическая оценка разработанных мероприятий от НСД включает комплекс мероприятий по определению ряда затрат, а именно:

- Затраты на оборудование;
- Затраты на лицензированное программное обеспечение;

Сотрудники пограничных, таможенных и других контрольных органов обеспечены автоматизированными рабочими местами. В них предусмотрено наличие необходимой операционной системы. И других необходимых программ для установки и функционирования программы.

Исходя из этого, можно сделать вывод о том, что имеется достаточное количество АРМ и лицензионное программное обеспечение для обеспечения функционирования программы. Экономическая оценка рассчитывалась исходя из стоимости затрат компьютерного времени и затрат на приобретение ПО, которая вычисляется по формуле 1:

$$K_3 = Z_1 + V \quad (1)$$

где

V - стоимость лицензионного ПО

Z₁ - затраты компьютерного времени, руб.;

Затраты компьютерного времени вычисляются по формуле 2:

$$Z_1 = C_k * F_k + C_{ТО}, \quad (2)$$

где

C_k - стоимость компьютерного часа, руб.

C_{ТО} - затраты на техобслуживание, руб.

F_k - затраты компьютерного времени на разработку программы

Стоимость компьютерного времени исчисляется по формуле 3:

$$C_k = C_A + C_3, \quad (3)$$

Где

C_A - амортизационные отчисления, руб.

C_3 - затраты на электроэнергию, руб.

Амортизация за 1 час работы, определяются по формуле 4:

$$C_A = N_{Ai} / F_i, \quad (4)$$

где

N_{Ai} - годовая норма амортизации i -го оборудования, руб;

F_i - годовой фонд времени работы i -го оборудования, час.

Для установки программного обеспечения использовалась ПЭВМ. Балансовая стоимость данного ПЭВМ на момент приобретения в октябрь 2010 года составляла 15000 рублей.

Приказ Министерства Финансов РФ № 157-н от 12 октября 2012 года устанавливает нормы амортизации. На объекты основных средств, стоимостью свыше 40000 рублей, амортизация начисляется в соответствии с рассчитанными в установленном порядке нормами. Расчет годовой суммы начисления амортизации основных средств и нематериальных активов проводится линейным способом исходя из балансовой стоимости объектов и нормы амортизации, исчисленной исходя из срока полезного использования этих объектов.

В соответствии с документацией, срок службы ПЭВМ составляет 8 лет.

Соответственно, годовая норма амортизации N_{Ai} рассчитывается следующим образом, указанным в формуле 5:

$$N_{Ai} = C_i / S_i, \quad (5)$$

где

S_i - срок службы i -оборудования, год;

C_i - балансовая стоимость i -го оборудования, которое использовалось для создания программного обеспечения, руб:

$$N_{Ai} = 15000 / 8 = 1875 \text{ руб. /год}$$

Исходя из данных формуляра, годовой фонд времени работы ПЭВМ составил 2000 часов.

Расчет амортизационных отчислений за 1 час работы был найден по формуле 6:

$$C_A = 1875 / 2000 = 0.94 \text{ руб. /час} \quad (6)$$

Затраты на электроэнергию за один час рассчитываются по формуле 7:

$$C_э = P_э * C_{кВт}, \quad (7)$$

где

$P_э$ - расход электроэнергии, потребляемой компьютером, кВт/ч;

$C_{кВт}$ - стоимость 1 кВт/ч электроэнергии, руб.

Исходя из характеристик данного компьютера, потребление электроэнергии составляет 0,4 кВт/ч. Тариф на электроэнергию установлен Правительством Калининградской области на уровне 2,47 руб. за 1 кВт. Тогда размер затрат на электроэнергию рассчитывается по формуле 8:

$$C_э = 0.4 * 2.47 = 0.988 \text{ руб. /час} \quad (8)$$

Затраты на техобслуживание определяются по формуле 9:

$$C_{ТО} = r_{ТО} * \tau, \quad (9)$$

где

$r_{ТО}$ – денежное довольствие инженера, руб.;

τ – периодичность обслуживания, час.

В подразделении пограничного контроля техническое обслуживание ПЭВМ проводится инженером один раз в месяц. Денежное довольствие инженера составляет 55000 рублей в месяц. Техническое обслуживание занимает не более одного часа.

Рабочее время инженера составляет 40 часов в неделю. Исходя из этого, можно сделать вывод о количестве часов его служебной деятельности в месяц – 160 часов.

Были произведены затраты государства на денежное довольствие инженера в час, и соответственно на техническое обслуживание ПЭВМ:

$$C_{ТО} = 55000 / 160 = 343.75 \text{ руб. /час}$$

Себестоимость компьютерного часа:

$$C_k = 0.94 + 0.988 = 1.928 \text{ руб. /час}$$

Таким образом, затраты компьютерного времени получились следующими:

$$З_1 = 1,928 * 180 + 343,75 = 690,79 \text{ руб.}$$

Стоимость лицензионного программного обеспечения составляет 8000 рублей. Общая стоимость согласно формуле 1 будет следующей:

$$K_3 = 690,79 \text{ руб.} + 8000 \text{ руб.}$$

Таким образом, из произведенных расчетов можно сделать вывод о том, что полная стоимость мероприятий по защите от НДС составит 8690,79 рублей.

Определение экономической оценки заключалось в калькуляции расчетов ценовой категории на необходимое оборудование, которое указано в таблице 11 и его количества.

Таблица 11 – Калькуляция затрат на оборудование

| № п/п | Наименование и техническая характеристика | Код оборудования изделия | Цена за единицу | Единица измерения | Количество | Цена (руб.) | Примечание |
|---|---|--------------------------|-----------------|-------------------|------------|-------------|------------|
| Сервер | | | | | | | |
| 1 | Sun Fire X4150 Two Quad-Core Intel Xeon E5450 | | 8281 | шт. | 3 | 24843 | |
| 2 | Sun Storage J4200 | 4252K4G | 37270 | шт. | 1 | 37270 | |
| Источники бесперебойного питания | | | | | | | |
| 1 | ИБП Smart UPS RT 3000 | | 110786 | шт. | 1 | 110786 | |
| 2 | APC BACK UPS ES 700 | | 5800 | Шт. | 13 | 75400 | |
| Активное оборудование ЛВС (с учетом ЗИП) | | | | | | | |
| 1 | Cisco Catalyst 2960 24 10/100/1000 | | 106127 | Шт. | 3 | 318381 | |
| 2 | Cisco Catalyst | | | шт. | | | |

| | | | | | | | | |
|-------------------------------|---|-----|-------------------------|---------|-----|-----|---------|--|
| | 2960 10/100/1000 | 7 | | 28207 | | 2 | 56414 | |
| 3 | Cisco GE SFP | | | 21970 | шт. | 6 | 131820 | |
| 4 | 3Com Ethernet 10/100BaseT | 5 х | | 24598 | | 10 | 245980 | |
| 5 | Кабель FTP NEOMAX пары одножильный неэкранированн ый витая пара Кат 5E (бухта 305 м) | 4 | 09Z684- 5P | 6477 | шт. | 2 | 12955 | |
| 6 | Коннектор разъем вилка RJ-45 под UTP кабель витая пара Кат 5 6m" gold | | 09Z6KI- H3 | 4,59 | шт. | 100 | 405,72 | |
| 7 | Розетка внешняя настенная STP ,2 порта RJ- 45 | | 09ZAA43 4 | 284,00 | шт. | 21 | 5974 | |
| 8 | Блок розеток 8розеток 1U 19"х2 | | | 550,00 | шт. | 3 | 1550,00 | |
| 9 | Маршрутизатор D-Link 6600-AP | | 6600-AP | 9494,00 | шт. | 2 | 18988 | |
| Пассивное оборудование | | | | | | | | |
| 1 | Направленная антенна Wivat AT-5-8/Patch(7) | | AT- 5.8/Patch(7) | 795,00 | шт. | 2 | 1590 | |

| | | | | | | | |
|--------------------------------|--------------------------------------|----------------|---------|-----|----|---------|--|
| 2 | Соединительный кабель RP-SMA | Link TL-ANT-PT | 97,00 | м. | 4 | 388 | |
| 3 | Кронштейн | КРП-20 | 43,00 | шт. | 4 | 172 | |
| 4 | Соединительный кабель "Витая пара" | Cat 5e | 25,00 | м | 25 | 625 | |
| 9 | Полка монитора, перфорированная 19" | | 484,00 | шт. | 1 | 484,00 | |
| 10 | Полка выдвижная под клавиатуру 19" | | 1768,00 | шт. | 1 | 1768,00 | |
| 11 | Заглушка 4Ux4шт | | 219,00 | шт. | 7 | 1533,00 | |
| Мониторы | | | | | | | |
| 1 | Монитор 22" ЖК | | 3351 | шт. | 14 | 46914 | |
| Периферийные устройства | | | | | | | |
| 1 | Клавиатура Chicony KB-0837 проводная | | 900 | шт. | 14 | 12600 | |
| 2 | Мышь A4Tech X-738K | | 515 | шт. | 14 | 7210 | |
| Системный блок | | | | | | | |
| 1 | DELL OptiPlex 390 MT | | 15580 | шт. | 13 | 201657 | |
| Оборудование СИБ | | | | | | | |
| 1 | ПАК VIP Net HW100 | | 106800 | шт. | 2 | 213400 | |
| 2 | ПО | | 85000 | шт. | 1 | 85000 | |

| | | | | | | | |
|------------------------------------|--|--|---------|-----|---------------|---------|--|
| | VIP Net Administrator | | | | | | |
| 3 | ПО VIP Net Cordinator | | 50000 | Шт. | 2 | 100000 | |
| 4 | ПО VIP Net Client | | 9500 | Шт. | 12 | 114000 | |
| Электронный замок для двери | | | | | | | |
| 1 | Электронный замок для двери с питанием от батареек Модель: Z-7 ЕНТ | | 8000 | Шт. | 2 | 16000 | |
| Шкафы | | | | | | | |
| | Серверный шкаф 42" Sun Rack 1000-42 | | 17795.7 | Шт. | 1 | 17795.7 | |
| | | | | | Итого: | 1861932 | |

Вывод: затраты на оборудование составили: 1861932 (один миллион восемьсот шестьдесят одна тысяча девятьсот тридцать два)

- спроектированная СКС : 1349532руб.
- СИБ с учетом СЗИ VipNet: 512400руб.

Большая сумма получилась из-за того, что ИБП: Smart UPS RT 3000 и APC BACK UPS ES 700 будут установлены на всех оборудованях сети, что обеспечит автономную работы всей сети на 15 минут в случае отключения электроэнергии. Этого времени будет достаточно, чтобы успеть сохранить необходимую информацию на файловый сервер.

ЗАКЛЮЧЕНИЕ

В соответствии с руководящими документами по защите информации, структурированная кабельная сеть отвечает всем требованиям. Проведенный анализ существующих требований по защите компьютерных сетей, показал, что организационных мер защиты информации от НСД недостаточно, чтобы организовать полноценную защиту компьютерной сети. При разработке проекта компьютерной сети была применена структурированная кабельная система на основе витой пары. Для реализации горизонтальной подсистемы была использована элементная база категории 5е, которая обеспечивает передачу по трактам СКС сигналов всех широко распространенных на практике разновидностей этого сетевого интерфейса ЛВС. Это решение обеспечивает резерв пропускной способности горизонтальных трактов СКС, дает достаточную поддержку функционирования всех известных и перспективных видов приложений, то есть обеспечивает надежную защиту инвестиций заказчика, сделанных им в СКС. Данная сеть позволяет подключить 12 рабочее место (с возможностью расширения). Обеспечивает передача данных со скоростью 100 Мбит/с. является достаточной для выполнения сотрудниками поставленных задач на своем служебном оборудовании.

Была разработана интерактивная технологическая карта выполнения операций по защите информации, она будет служить как инструкция для администратора, так и один из основных документов по созданию руководства пользователя.

Были составлены методы и организационные меры защиты информации, в ходе анализа которых можно сделать вывод о том, что принятые меры отвечают всем требованиям нормативно-правовой базы. Так же можно отметить, что устанавливаемая система защиты «VipNet» не требует привлечения большого штата сотрудников для ее развертывания. Она является современным средством защиты информации, имеет ряд преимуществ, такие как надежность и стабильность работы, простота реализации в подразделении. «VipNet» имеет возможность удаленной установки, а также позволяет

подключать электронные ключи, осуществлять постоянный контроль над пользователями, которые осуществляют служебную деятельность на ЭВМ. Также эта система наряду с серверными средствами администрирования имеет возможность осуществлять аналогичные действия, без обращения к серверу.

СПИСОК ИСПОЛЬЗУЕМОЙ ЛИТЕРАТУРЫ

1. Основы защиты информации. Иванов В. А., Кузнецов А. В. Учебное пособие для радиотехнических специальностей ВУЗов.
2. П.Н. Девянин. Модели безопасности компьютерных систем. Управление доступом и информационными потоками. Учебное пособие для вузов. Москва: Горячая линия – Телеком, 2011 г. – 320 с., ил.
3. Духан Е.И., Синадский Н.И., Хорьков Д.А. Применение программно-аппаратных средств защиты компьютерной информации.
4. Семенов А.Б. Проектирование и расчет структурированных кабельных систем и компонентов. – М.: ДМК Пресс; М.: Компания АйТи, 2003 г.
5. Квалификационная работа. Е.В. Сулямов, А.Н. Мезенцев, А.М. Дубовик.
6. Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля не декларированных возможностей (Гостехкомиссия России, 1999).
7. Приказ ФСТЭК России № 17 от 11 февраля 2013. Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах.
8. Приказ ФСТЭК России № 21 от 18 февраля 2013. Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах.
9. Федеральный закон от 27 июля 2006 г. №149-ФЗ. Об информации, информационных технологиях и о защите информации.
10. Система защиты информации VIP Net 2014 года. Н.В Кубакова, А.О.Чефранова, А.В Уривский, Ю.Ф.Алабина.
11. Зайцев А.П., Голубятников И.В., Мещеряков Р.В., Шелупанов А.А. Программно-аппаратные средства обеспечения информационной безопасности:

Учебное пособие. Издание 2-е изд. и добавить. - М.: Машиностроение-1, 2006. - 260 с.

12. Вайнштейн Ю.В., Демин С.Л., Кирко И.Н. и другие. Учебник по дисциплинам «Основы информационной безопасности», «Информационная безопасность и защита информации». - Красноярск, 2007. - 303 с.

13. Варлатая С.К., Шаханова М.В. Аппаратно-программные средства и методы защиты информации: Учебное пособие. - Владивосток: Издательство ФЕДТУ, 2007. - 318 с.

14. 2) Лагутин М.Г. научная статья[электронный ресурс]: вопросы межведомственного информационного взаимодействия в электронном виде. URL:<https://e.mail.ru/attachment/14769551900000000228/0;1>(дата обращения 10.10.2016) 3)Руководство пользователя ViPNet[электронный ресурс].URL: https://files.infotecs.ru/_dl/sess/vipnet_csp/docs/ViPNet_CSP_User_Guide_Ru.pdf (дата обращения 20.12.2016) 4)Бедердинова О.И., Коряковская Н.В. Алгоритм разработки системы защиты информации [электронный ресурс]. URL=<http://cyberleninka.ru/article/n/algorithm-razrabotki-sistemy-zaschityinformatsii> (дата обращения 15.10.2016)

15. Прудников Антон Игоревич, Шахов Владимир Григорьевич Особенности использования технологии ViPNet для защиты информации в корпоративных сетях // ОНВ. 2012. №2 (110). URL: <https://cyberleninka.ru/article/n/osobennosti-ispolzovaniya-tehnologii-vipnet-dlya-zaschity-informatsii-v-korporativnyh-setyah> (дата обращения: 19.06.2019).

16. Наумов Родион Владимирович Технология vpn ViPNet // Научный журнал. 2016. №8 (9). URL: <https://cyberleninka.ru/article/n/tehnologiya-vpn-vipnet> (дата обращения: 19.06.2019).

17. Gross, J. and M.B. Rosson. Looking for Trouble: Understanding End-User Security Management. in Computer Human Interaction for the Management of Information Technology (CHIMIT) 2007.

18. Kumaraguru, P., et al., Teaching Johnny not to fall for phish. ACM Trans. Internet Technol., 2010. 10(2): p. 1-31.

19. Craig, J.S., The human element: training, awareness, and human resources implications of health information security policy under the Health Insurance Portability and Accountability Act (HIPAA), in 2009 Information Security Curriculum Development Conference. 2009, ACM: Kennesaw, Georgia. p. 95-99.

20. Johnson, M., et al., Optimizing a policy authoring framework for security and privacy policies, in Proceedings of the Sixth Symposium on Usable Privacy and Security. 2010, ACM: Redmond, Washington. p. 1-9.

21. Kvedar, D., M. Nettis, and S.P. Fulton, The use of formal social engineering techniques to identify weaknesses during a computer vulnerability competition. *J. Comput. Small Coll.*, 2010. 26(2): p. 80- 87.

22. Jackson, C. (2010). *Network security auditing*. Indianapolis, IN: Cisco Press, pp. 8-9.

23. Jungck, Kathleen and Rahman, Syed (2011); " Cloud Computing Avoids Downfall of Application Service Providers";*International Journal of Information Technology Convergence and services (IJITCS)*, ISSN : 2231 - 153X (Online) ; 2231 – 1939

24. Anderson, C. L. and R. Agarwal (2010). "Practicing safe computing: a multimethod empirical examination of home computer user security behavioral intentions." *MIS Quarterly* 34(3): 613-643.