Министерство образования и науки Российской Федерации
Филиал Федерального государственного бюджетного образовательного учреждения высшего профессионального образования
«Южно-Уральский государственный университет»
(национальный исследовательский университет)
в г. Нижневартовске

Кафедра «Информатика»

РАБОТА ПРОВЕРЕНА
Рецензент
Начальник АСУ Отдела
/А.С. Волков /
«06» июня 2016г.

ДОПУСТИТЬ К ЗАЩИТЕ
И.о. зав. кафедрой «Информатика»
к.т.н., доцент
/С.Г. Пономарева /
«30» мая 2016 г.

Проектирование беспроводной локальной вычислительной сети на предприятии

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА
К ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ РАБОТЕ
ЮУрГУ- 230100.2016.222.ПЗ ВКР

Консультанты
Экономическая часть
к.э.н., доцент
/ А.В. Прокопьев /
«28» мая 2016 г.

Безопасность жизнедеятельности
к.т.н., доцент
/А.Б. Тряпицын /
«29» мая 2016 г.

Руководитель проекта
к.т.н., доцент
/ И.Л. Кафтанников /
«30» мая 2016г.

Автор проекта
студент группы НвФл-528 гр.
/Н.Е. Ступин /
«30» мая 2016 г.

Нормоконтролер
старший преподаватель
/ Л.Н. Буйлушкина /
«30» мая 2016 г.

Нижневартовск 2016

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФИЛИАЛ ЮЖНО-УРАЛЬСКОГО ГОСУДАРСТВЕННОГО УНИВЕРСИТЕТА
В Г.НИЖНЕВАРТОВСКЕ
КАФЕДРА «ИНФОРМАТИКА»

Направление 230100.62 «Информатика и вычислительная техника»

УТВЕРЖДАЮ
И.о зав. кафедрой «Информатика»
к.т.н., доцент
_____ /С.Г Пономарева /
/личная подпись/
« 05 » февраля 2016 г.

З А Д А Н И Е

на выпускную квалификационную работу студента

Ступина Никиты Евгеньевича

1. Тема работы: Проектирование беспроводной локальной вычислительной сети на предприятии

Утверждена приказом ректора университета от « 15 » апреля 2016 г. № 661

2. Срок сдачи студентом законченной работы « 30 » мая 2016 г.

3. Исходные данные к работе:

Нормативные документы РФ, материалы производственной практики, учебники, справочные данные сети Internet – сайтов

4. Содержание пояснительной записки

1. Теоретические основы построения беспроводных локальных вычислительных сетей

2. Анализ предприятия, его структуры и информационных ресурсов

3. Разработка схемы и организация беспроводной локальной вычислительной сети предприятия

4. Установка и настройка необходимого программного обеспечения

5. Обеспечение информационной безопасности проектируемой сети

6. Технико-экономический раздел

7. Безопасность жизнедеятельности

5. Перечень графического материала

Презентация в MS Power Point: 18 слайдов.

6. Консультанты по работе, с указанием относящихся к ним глав (разделов) работы

Глава (раздел)	Ф.И.О. консультанта	Подпись, дата	
		задание выдал	задание принял
Основная часть	Кафтанников И.Л.	15.01.2016	16.05.2016
Экономическая часть	Прокопьев А.В.	12.01.16	14.05.16
БЖД	Тряпицын А.Б.	12.01.16	15.05.16

7. Дата выдачи задания « 02 » февраля 2016г.

Задание выдал руководитель И.Л. Кафтанников

Задание принял к исполнению студент-дипломник Н.Е. Ступин

КАЛЕНДАРНЫЙ ПЛАН

Наименование этапов выпускной квалификационной работы	Срок выполнения этапа	Отметки о выполнении этапа
Введение	02.02-04.02.2016	выполнено
Теоретические основы построения беспроводных локальных вычислительных сетей	04.03-19.03.2016	выполнено
Анализ предприятия, его структуры и информационных ресурсов	21.03-30.04.2016	выполнено
Разработка схемы и организация беспроводной ЛВС предприятия	01.05-05.05.2016	выполнено
Установка и настройка необходимого программного обеспечения	06.04-09.05.2016	выполнено
Обеспечение информационной безопасности проектируемой сети	10.05-13.05.2016	выполнено
Технико-экономический раздел	13.05-14.05.2016	выполнено
Безопасность жизнедеятельности	14.05-15.05.2016	выполнено
Библиографический список	15.05-16.05.2016	выполнено
Презентация доклада защиты работы	16.05.2016	выполнено
Оформление ВКР	17.05-30.05.2016	выполнено
Защита работы	11.06.2016	

И.о зав. кафедрой _____ /личная подпись/ / С.Г Пономарева /

Руководитель работы _____ /личная подпись/ / И.Л. Кафтанников /

Студент-дипломник _____ /личная подпись/ / Н.Е Ступин /

АННОТАЦИЯ

Ступин Н.Е. Проектирование беспроводной локальной вычислительной сети на предприятии – Нижневартовск: филиал ЮУрГУ, Информатика, НвФл-528: 2016, 116 с., 27 ил., 28 табл., библиогр. список – 22 наим., 6 прил.

Цель: Обеспечить эффективную производственную деятельность предприятия ООО «Инструментстрой» путём разработки и внедрения аппаратно-программного комплекса технических средств связи.

Задачи: Произвести анализ основных технических средств, необходимых для построения беспроводной локальной сети. Проанализировать характеристику исследуемого объекта, состав аппаратных средств компании, информационные потоки, циркулирующие в проектируемой сети и разработать схему организации локальной вычислительной сети компании.

Основной практический результат работы – разработан проект беспроводной сети предприятия, удовлетворяющий всем необходимым требованиям.

					230100.2016.222 ПЗ		
Изм.	Лист	№ докум.	Подпись	Дата			
Разраб.		Ступин Н.Е.			Проектирование беспроводной локальной вычислительной сети на предприятии	Лит.	Лист 6	Листов 116
Проверил		Кафтанников И.Л.				22		
Рецензент		Волков А.С.				Филиал ФГБОУ ВПО «ЮУрГУ» (НВФ) в г. Нижневартовске кафедра «Информатика»		
Н.контр.		Буйлушкина Л.Н.						
Утвердил		Поконечная С.Г.						

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ 10
1 ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПОСТРОЕНИЯ БЕСПРОВОДНЫХ ЛОКАЛЬНЫХ СЕТЕЙ 13
1.1 Преимущества и недостатки беспроводных ЛВС 13
1.2 Основные стандарты беспроводных ЛВС 16
1.3 Топологии беспроводных сетей Wi-Fi 18
1.4 Анализ основных технических средств, необходимых для построения беспроводной ЛВС 21
2 АНАЛИЗ ПРЕДПРИЯТИЯ, ЕГО СТРУКТУРЫ И ИНФОРМАЦИОННЫХ РЕСУРСОВ 27
2.1 Характеристика исследуемого объекта 27
2.2 Состав и структура информационных ресурсов предприятия 31
2.3 Анализ требований и разработка технического задания на проект беспроводной ЛВС предприятия 34
3 РАЗРАБОТКА СХЕМЫ И ОРГАНИЗАЦИЯ БЕСПРОВОДНОЙ ЛВС ПРЕДПРИЯТИЯ 387
3.1 Разработка структуры ЛВС 388
3.2 Выбор необходимого аппаратного и программного обеспечения 399
3.2.1 Выбор точки доступа 399
3.2.2 Выбор коммутатора сети 433
3.2.3 Выбор программного обеспечения 455
3.3 Организация работы беспроводной ЛВС 488
3.3.1 Управление сетью 488
3.3.2 Организация сетевых ресурсов локальной сети 489
4 УСТАНОВКА И НАСТРОЙКА НЕОБХОДИМОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ 511
4.1 Подключение коммутатора 511
4.2 Установка операционной системы сети 522

4.3 Установка и настройка дополнительного программного обеспечения сети… 555
5 ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРОЕКТИРУЕМОЙ СЕТИ 60
5.1 Разработка комплекса программно-аппаратных мер по обеспечению защиты информации компьютерной сети 60
5.1.1 Подсистема защиты от несанкционированного доступа в сеть 60
5.1.2 Средства антивирусной защиты 622
5.1.3 Программно-аппаратные средства межсетевого экранирования 622
5.1.4 Средства криптографической защиты 644
5.1.5 Средства обнаружения вторжений 666
5.1.6 Средства анализа защищенности 677
5.2 Общая структура системы информационной безопасности компьютерной сети 689
5.3 Внедрение предлагаемых средств защиты компьютерной сети 701
6 ТЕХНИКО-ЭКОНОМИЧЕСКИЙ РАЗДЕЛ 80
6.1 Составление календарного плана выполнения работ 800
6.2 Определение сметной стоимости проекта 800
6.2.1 Расчет расходов на оплату труда 810
6.2.2 Страховые взносы с заработной платы 833
6.2.3 Статья «Расходы на материалы» 834
6.2.4 Статья «Прочие расходы» 844
6.2.5 Статья «Административно - хозяйственные расходы» 845
6.2.6. Технико-экономические показатели проекта 855
7 БЕЗОПАСНОСТЬ ЖИЗНЕДЕЯТЕЛЬНОСТИ 877
7.1 Анализ условий труда сист. администратора ЛВС 877
7.1.1 Анализ воздействия ПЭВМ и монитора на сотрудника 877
7.1.2 Анализ источников шума 888
7.1.3 Анализ микроклимата помещений 899

7.2 Пожарная безопасность 90
7.3 Электробезопасность 933
7.4 Расчет необходимого естественного освещения 944
7.5 Анализ экологических особенностей проекта 977
ЗАКЛЮЧЕНИЕ 988
ПЕРЕЧЕНЬ ПРИНЯТЫХ СОКРАЩЕНИЙ……..……...……..…..100
БИБЛИОГРАФИЧЕСКИЙ СПИСОК 1011

ПРИЛОЖЕНИЯ ..... **Ошибка! Закладка не определена.**103
ПРИЛОЖЕНИЕ А. ФАКТОРНЫЙ АНАЛИЗ СРЕДСТВ МЕЖСЕТЕВОГО ЭКРАНИРОВАНИЯ.....103
ПРИЛОЖЕНИЕ Б. ФАКТОРНЫЙ АНАЛИЗ СРЕДСТВ УПРАВЛЕНИЯ СЪЕМНЫМИ НОСИТЕЛЯМИ.....105
ПРИЛОЖЕНИЕ В. ФАКТОРНЫЙ АНАЛИЗ СРЕДСТВ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ.....107
ПРИЛОЖЕНИЕ Г. ФАКТОРНЫЙ АНАЛИЗ СРЕДСТВ АНАЛИЗА ЗАЩИЩЕННОСТИ.....…..110
ПРИЛОЖЕНИЕ Д. ФАКТОРНЫЙ АНАЛИЗ СРЕДСТВ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ.....112
ПРИЛОЖЕНИЕ Е. КОМПАКТ - ДИСК…….....116

ВВЕДЕНИЕ

Вследствие возникновения и дальнейшего развития сетей передачи данных появился эффективный способ взаимодействия между людьми. Первоначально сети использовались в основном для научных исследований, но затем они стали использоваться практически во все областях человеческой деятельности. При этом основная масса сетей существовала независимо друг от друга, решая задачи для определенных групп пользователей [6].

Программное обеспечение, а также терминальные подключения, базы данных, мультимедийные технологии, требующие для своей реализации постоянного и качественного соединения, заставляют обращать особое внимание при подборе оборудования. Это требование актуально как внутри ЛВС, так и при выходе в глобальную сеть.

Актуальность темы рассматриваемой в выпускной квалификационной работе обусловлена следующими факторами:

- масштабное распространение компьютерных сетей во всех сферах человеческой деятельности;

- высокие темпы и уровни развития современных информационных технологий;

- быстрые темпы роста парка персональных компьютеров, применяемых в разнообразных сферах человеческой деятельности из-за увеличения обрабатываемой информации;

- резкое расширение сферы пользователей;

-значительное увеличение объемов информации, накапливаемой, хранимой и обрабатываемой с помощью компьютеров и других средств автоматизации. По оценкам специалистов в настоящее время около 70-90% интеллектуального капитала организации хранится в цифровом виде текстовых файлах, таблицах, базах данных.

Цель выпускной квалификационной работы - оптимальное проектирование беспроводной ЛВС общество с ограниченной ответственностью "Инструментстрой" (далее - ООО «Инструментстрой).

Объект исследования - ООО «Инструментстрой».

Предмет исследования - подходы в области построения, проектирования и внедрения беспроводных ЛВС.

Использование более гибких решений на этапе проектирования ЛВС позволяет с небольшими затратами повысить производительность в пределах исследуемого помещения независимо от количества пользователей и свойств трафика.

Основными требованиями к проектируемой ЛВС являются обеспечение необходимой производительности, оптимизация элементов сети при проектировании.

Исходя из цели выпускной квалификационной работы, определены следующие задачи, которые необходимо решить при проектировании:

1. Выбрать и настроить управляемый коммутатор, который мог бы обеспечить заданные параметры для всех пользователей ЛВС.

2. Подобрать и настроить программный маршрутизатор. При применении маршрутизаторов появляется возможность более гибко регулировать политику безопасности как между сегментами сети, так и при взаимодействии с глобальной сетью Internet.

3. Спроектировать и настроить беспроводную сеть VLAN. Технология виртуальных сетей, взявшая в себя лучшее из современных сетевых технологий, решает много проблем по функционированию сети, в том числе позволяет увеличивать пропускную способность за счёт деления широковещательного домена. Таким образом, появляется возможность создавать независимые элементы сети, куда доступ будет удерживаться на канальном уровне, тем самым гарантируя безопасное пространство рабочих станций и серверов.

Для достижения поставленной в работе цели предполагается произвести анализ коммуникационного оборудования, маршрутизаторов и технологий

организации VLAN, разработать структурную схему построения сети, настроить ОС маршрутизатора, а также дополнительное ПО.

Решение обозначенных выше задач позволит получить систему, обеспечивающую сотрудников предприятия в рамках рассматриваемого технологического цеха связью с высокой скоростью с выходом в глобальные сети с фильтрацией и учетом трафика, а также обеспечить изолированность и, как следствие, безопасность ЛВС.

1 ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПОСТРОЕНИЯ БЕСПРОВОДНЫХ ЛОКАЛЬНЫХ СЕТЕЙ

1.1 Преимущества и недостатки беспроводных ЛВС

Беспроводные ЛВС (Wireless LAN) поддерживают высокоскоростную передачу данных в пределах небольшого пространства (например, университетского городка или небольшого здания), когда пользователи передвигаются с места на место. Беспроводные устройства, которые имеют доступ к этим ЛВС, обычно стационарные или двигаются со скоростью пешехода.

Все стандарты беспроводных ЛВС действуют в нелицензируемом частотном диапазоне. Основные нелицензируемые полосы частот — это диапазоны ISM на 900 МГц, 2,4 ГГц и 5,8 ГГц, а также диапазон нелицензируемой национальной информационной инфраструктуры (U-NII) на 5 ГГц. В диапазонах ISM нелицензируемые пользователи являются вторичными пользователями и поэтому вынуждены справляться с помехами, создаваемыми первичными пользователями в то время, когда они активны. В диапазоне U-NII первичных пользователей нет. Для работы в диапазонах ISM или U-NII лицензии Федеральной комиссии FCC не требуется. Однако это преимущество является палкой о двух концах, так как другие нелицензируемые системы также действуют в этих диапазонах по той же самой причине, что может вызвать очень сильные взаимные помехи между системами. Проблема интерференции уменьшается при установлении для нелицензируемых систем ограничений мощности на единицу частотного диапазона. Беспроводные ЛВС могут иметь либо соединение звездой с пунктами беспроводного доступа или концентраторами. расположенными внутри зоны покрытия, либо архитектуру одноранговой вычислительной сети ЛВС, где беспроводные терминалы автоматически конфигурируются в сеть.

В начале 1990-х годов появились десятки компаний — поставщиков оборудования и услуг беспроводных ЛВС, стремившихся заработать на неудовлетворенном спросе на высокоскоростную беспроводную передачу

данных. Эти беспроводные ЛВС первого поколения базировались на несовместимых пользовательских протоколах. Большинство из них действовало в полосе 26 МГц частотного диапазона ISM 900 МГц, используя расширение спектра прямой последовательностью со скоростью передачи данных порядка 1-2 Мбит/с. Использовались как соединение звездой, так и архитектура одноранговой сети. Отсутствие стандартизации в данной области привело к высокой стоимости разработки, мелкосерийному производству и маленьким рынкам для каждого отдельного вида продукции. Из всей этой оригинальной продукции только небольшое количество было более-менее успешным. Всего лишь одна из беспроводных ЛВС первого поколения — «Альтаир» (Altair) фирмы Motorola — работала вне частотного диапазона 900 МГц. Эта система, работавшая в лицензируемом диапазоне 18 ГГц, имела скорость передачи данных порядка 6 Мбит/с. Однако применение «Альтаира» было затруднено из-за высокой стоимости компонентов и больших потерь в тракте передачи на 18 ГГц, и «Альтаир» был снят с производства через несколько лет после выпуска.

Беспроводные ЛВС второго поколения действуют в полосе шириной 83,5 МГц в диапазоне ISM 2,4 ГГц (Wi-Fi). Стандарт IEEE 802.11b для беспроводных ЛВС этого частотного диапазона был разработан, чтобы избежать некоторых проблем с запатентованными системами первого поколения. Стандарт определяет расширение спектра методом прямой последовательности при скорости передачи данных порядка 1,6 Мбит/с (максимальная физическая скорость передачи данных — 11 Мбит/с) и зоне покрытия около 100 м. Построение сети может быть в виде соединений звездой или архитектуры одноранговой сети, хотя последняя редко используется. Многие компании начали разрабатывать свою продукцию, опираясь на стандарт 802.11b. После медленного первоначального роста популярность беспроводных ЛВС стандарта 802.11b значительно возросла. Появилось много небольших портативных компьютеров со встроенными картами беспроводных ЛВС 802.11b. Компании и университеты установили базовые станции 802.11b на своих территориях, а множество кафе, аэропортов и отелей для повышения своей привлекательности предлагают беспроводный доступ, часто бесплатный.

Для обеспечения более высокой скорости передачи данных, чем в стандарте 802.11b, были разработаны еще два дополнительных стандарта семейства 802.11. Стандарт беспроводной ЛВС IEEE 802.11a занимает полосу шириной 300 МГц в диапазоне U-NII 5 ГГц. Стандарт 802.11a базируется на модуляции нескольких несущих и обеспечивает скорость передачи данных 54 Мбит/с в зоне примерно 30 м. Так как у системы стандарта 802.11a намного шире полоса пропускания и, следовательно, намного больше каналов, чем у 802.11b, она может поддерживать большее число пользователей при большей скорости передачи данных. Сначала были сомнения, не будут ли системы 802.11a значительно дороже, чем системы 802.11b, но в действительности они быстро стали конкурентоспособными по цене. Другой стандарт, 802.llg, имеет ту же самую схему и скорость передачи данных, что и 802.11a, но он работает в диапазоне 2,4 ГГц с зоной около 50 м. Во избежание несовместимости, многие карты бес-проводных ЛВС и приемопередатчики беспроводной сети поддерживают все три стандарта.

В Европе развитие беспроводных ЛВС вращается вокруг стандартов HIPERLAN. Стандарт HIPERLAN/2 похож на стандарт беспроводной ЛВС IEEE 802.11a. В частности, у него аналогичная схема канального уровня, он также действует в полосе частот 5 ГГц, подобно U-NII. Следовательно, у HIPERLAN/2 такая же максимальная скорость передачи данных - около 54 Мбит/с, и та же зона покрытия - приблизительно 30 м, как и у 802.11a. Стандарт HIPERLAN/2 отличается от 802.11a протоколом доступа и встроенной поддержкой «гарантированного качества обслуживания» (QoS).

Беспроводные локальные сети позволят повысить мобильность сотрудников в офисных или производственных помещениях, избавиться от проводов в офисе или дома, вдобавок исключив затраты на монтаж и обслуживание проводной сети.

Беспроводные сети Wi-Fi имеет смысл использовать в компаниях с небольшим количеством рабочих мест или при наличии большого количества беспроводных устройств (ноутбуков, нетбуков, коммуникаторов и т. д.). Чаще

всего используются оба типа сетей одновременно: проводные сети и беспроводные сети Wi-Fi.

Преимущества беспроводных сетей:

- простота и скорость развертывания сети;
- низкая стоимость развертывания;
- отсутствие проводов на рабочем месте.

Скорость передачи делится между всеми устройствами беспроводной сети в пределах обслуживания их одной и той же точкой доступа. Это значит, что если точка доступа предоставляет скорость передачи данных 300 мбит/с и к ней будет одновременно подключено, например 5 ноутбуков, то скорость передачи данных для каждого ноутбука составит 300 / 5 = 60 мбит/с. А в реальности и того меньше, поскольку объем передаваемой служебной информации может достигать 30-40%. В итоге скорость передачи составляет около 36 мбит/с на устройство.

Недостатки беспроводных сетей:

- влияние окружающей среды (деревья, стены зданий);
- сравнительно низкая надежность;
- низкая устойчивость к взлому при неправильной настройке.

Минусы частично можно закрыть более качественным оборудованием и добавлением в состав беспроводной сети большего количества точек доступа.

Беспроводные сети на предприятии следует использовать там, где этого требует специфика бизнеса, например, большие складские площади с небольшим количеством используемого компьютерного оборудования. В любом случае, необходимо тщательно взвесить все за и против перед началом построения локальной сети компании.

1.2 Основные стандарты беспроводных ЛВС

Взаимодействие беспроводных устройств регламентируется целым рядом стандартов.

В этих стандартах беспроводных локальных сетей указывается спектр радиочастотного диапазона, скорость передачи данных, способ передачи данных и прочая информация. Главным разработчиком технических стандартов беспроводной связи является организация IEEE.

Стандарт IEEE 802.11 регламентирует работу устройств в сетях WLAN. С учетом различных характеристик беспроводной связи в стандарт IEEE 802.11 были внесены четыре поправки. На сегодняшний день действуют следующие поправки - 802.11a, 802.11b, 802.11g и 802.11n (поправка 802.11n не ратифицирована на момент написания материала). Все эти технологии отнесены к категории Wi-Fi (Wireless Fidelity).

Организация "Wi-Fi Alliance" отвечает за тестирование устройств для беспроводных LAN, выпущенных разными производителями. Логотип Wi-Fi на корпусе устройства означает, что это оборудование может взаимодействовать с другими устройствами того же стандарта.

Рассмотрим характеристики основных стандартов современных беспроводных сетей.

Стандарт 802.11a:

- использует РЧ спектр 5 ГГц;
- несовместим со спектром 2,4 ГГц, т.е. устройствами 802.11 b/g/n;
- радиус действия - приблизительно 33% от 802.11 b/g;
- сравнительно дорог в реализации по сравнению с другими технологиями;
- оборудование, отвечающее стандарту 802.11a, становится все более редким.

Стандарт 802.11b:

- первая технология 2,4 ГГц;
- максимальная скорость передачи данных 11 Мбит/с;
- радиус действия - приблизительно 46 м в помещении и 96 м на открытом воздухе.

Стандарт 802.11g:

- семейство технологий 2,4 ГГц;

- максимальная скорость передачи данных повышена до 54 Мбит/с;

- радиус действия - такой же, как у 802.11b;

- имеется обратная совместимость с 802.11b.

Стандарт 802.11n:

- технологии 2,4 ГГц (поддержка 5 ГГц);

- увеличенный радиус действия и пропускная способность;

- обратная совместимость с существующим оборудованием 802.11g и 802.11b (поддержка 802.11a).

1.3 Топологии беспроводных сетей Wi-Fi

Беспроводные сети Wi-Fi могут строиться по любой из следующих топологий:

- независимые базовые зоны обслуживания (Independent Basic Service Sets, IBSSs);

- базовые зоны обслуживания (Basic Service Sets, BSSs);

- расширенные зоны обслуживания (Extended Service Sets, ESSs);

- независимые базовые зоны обслуживания (IBSS).

IBSS представляет собой группу работающих в соответствии со стандартом 802.11 станций, связывающихся непосредственно одна с другой. На рисунке 1.1 показано, как станции, оборудованные беспроводными сетевыми интерфейсными картами (network interface card, NIC) стандарта 802.11, могут формировать IBSS и напрямую связываться одна с другой.

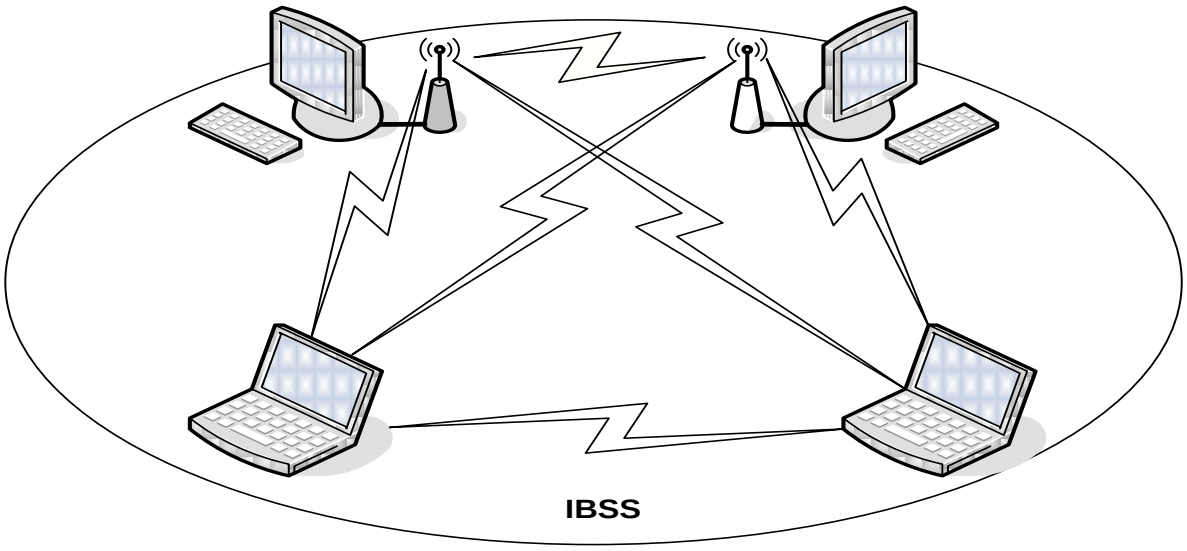


Рисунок 1.1 - Ad-Hoc сеть (IBSS)

Специальная сеть, или независимая базовая зона обслуживания (IBSS), возникает, когда отдельные устройства-клиенты формируют самоподдерживающуюся сеть без использования отдельной точки доступа (AP - Access Point). При создании таких сетей не разрабатывают какие-либо карты места их развертывания и предварительные планы, поэтому они обычно невелики и имеют ограниченную протяженность, достаточную для передачи совместно используемых данных при возникновении такой необходимости.

Поскольку в IBSS отсутствует точка доступа, распределение времени (timing) осуществляется нецентрализованно. Клиент, начинающий передачу в IBSS, задает сигнальный (маячковый) интервал (beacon interval) для создания набора моментов времени передачи маячкового сигнала (set of target beacon transmission time, TBTT). Когда завершается TBTT, каждый клиент IBSS выполняет следующее:

1. Приостанавливает все несработавшие таймеры задержки (backoff timer) из предыдущего TBTT;

2. Определяет новую случайную задержку;

Базовые зоны обслуживания (BSS).

BSS - это группа работающих по стандарту 802.11 станций, связывающихся одна с другой. Технология BSS предполагает наличие особой

станции, которая называется точка доступа AP (Access Point). Точка доступа - это центральный пункт связи для всех станций BSS. Клиентские станции не связываются непосредственно одна с другой. Вместо этого они связываются с точкой доступа, а уже она направляет кадры к станции-адресату. Точка доступа может иметь порт восходящего канала (uplink port), через который BSS подключается к проводной сети (например, восходящий канал Ethernet). Поэтому BSS иногда называют инфраструктурой BSS. На рисунке 1.2 представлена типичная инфраструктура BSS.

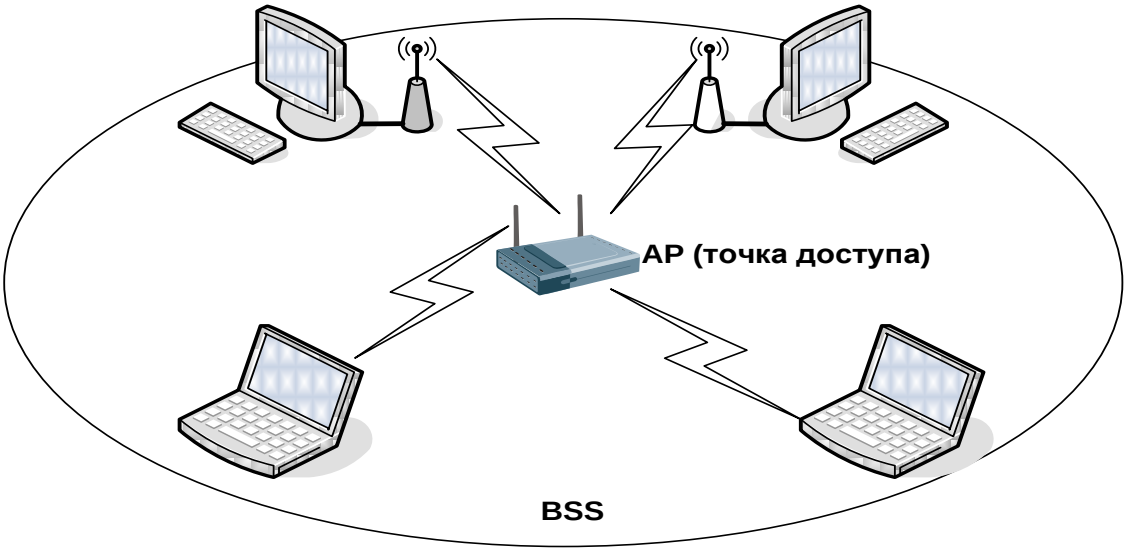


Рисунок 1.2 - Инфраструктура беспроводной ЛВС BSS

Расширенные зоны обслуживания (ESS).

Несколько инфраструктур BSS могут быть соединены через их интерфейсы восходящего канала. Там, где действует стандарт 802.11, интерфейс восходящего канала соединяет BBS с распределительной системой (Distribution System, DS). Несколько BBS, соединённых между собой через распределительную систему, образуют расширенную зону обслуживания (ESS). Восходящий канал к распределительной системе не обязательно должен использовать проводное соединение. На рисунке 1.3 представлен пример практического воплощения ESS. Спецификация стандарта 802.11 оставляет возможность реализации этого канала

в виде беспроводного. Но чаще восходящие каналы к распределительной системе представляют собой каналы проводной технологии Ethernet.

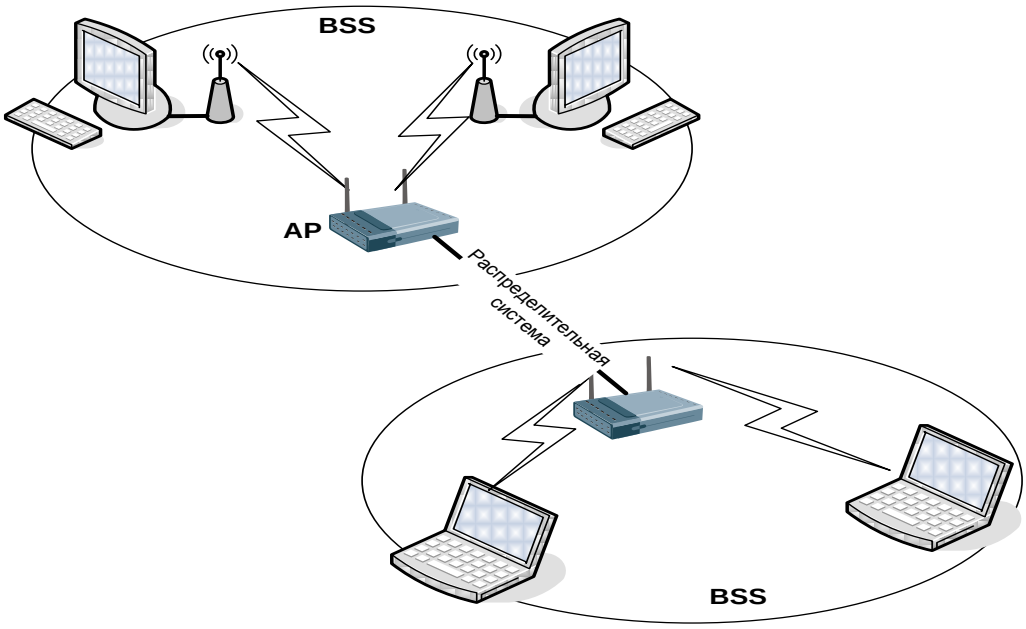


Рисунок 1.3 - Расширенная зона обслуживания ESS беспроводной сети

1.4 Анализ основных технических средств, необходимых для построения беспроводной ЛВС

Одно из главных устройств при организации беспроводных сетей - точка доступа.

Стандарт 802.11 объединяет в одном устройстве функциональность сетевого контроллера и радиотрансиверов.

Задачей сетевого адаптера является подключение к существующей коммуникации. А задача радиотрансивера - обеспечение коммуникаций с распределенными беспроводными устройствами.

Развертывание такой сети является установка точки доступа в свободный порт маршрутизатора или коммутатора.

Для доступа абонентских узлов через сеть Wi-Fi необходимо наличие адаптера беспроводной сети и программного обеспечения.

На установку Wi-Fi требуется разрешение на использование оборудования (мощности более 9 МВт).

Недостаток: отсутствие управляющего элемента, позволяющего манипулировать частотами и распределить передачу данных.

Разброс частоты необходим для предотвращения несанкционированного доступа к данным.

Каждый информационный пакет может отправляться по сети с применением собственной частоты. Выбор частоты распределен по случайному алгоритму.

Проблема распределенного построения сети решается путем использования беспроводных коммутаторов (см. Рисунок 1.4).

Отличием беспроводных коммутаторов от проводных заключается в том, что беспроводные коммутаторы не предоставляют пользователю выделенную полосу пропускания.

При использовании беспроводных коммутаторов также вопросы шифрования и аутентификации переходят от точек доступа к коммутаторам.

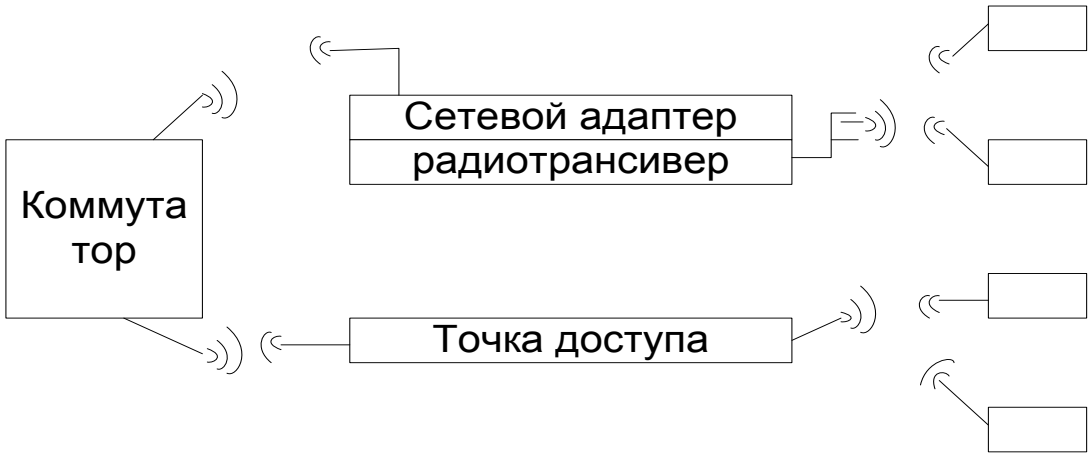


Рисунок 1.4 - Архитектура сети по централизованному принципу

Точка доступа позволяет подключить ограниченное число пользователей в единый общий канал.

Задача беспроводного коммутатора - организовать сеть с механизмом управления пакетами.

Преимуществом использования беспроводного коммутатора является то, что при переходе от одной точки доступа к другой пользователю не требуется дополнительной аутентификации при установлении соединения. Поэтому беспроводной коммутатор является центром беспроводной сети, который позволяет без сеанса связи отслеживать перемещение клиента.

Распространение сигнала между коммутатором и точкой доступа является более мощным, что позволяет на больших расстояниях устанавливать большое количество точек доступа.

Кроме этого, современные беспроводные точки доступа поддерживают режим питания - P0E - питание через информационную среду. Поэтому беспроводной коммутатор способен служить источником питания от точек доступа, а также узлом, который выполняет функции отслеживания указавших участков.

Таким образом, беспроводной коммутатор может компенсировать неисправность участка сети с расширением числа пользователей точек доступа, соседствующих с указанной точкой. Перераспределение происходит алгоритмическим путем. Позволяет разделить нагрузку на соседних 2 абонента при выходе из строя одной из точек доступа и количество абонентов станет по 30. Исходя из информации о количестве пользователей, беспроводной коммутатор эффективно разделяет загрузку каналов, предлагая более широкую полосу пропускания для тех сегментов сети, имеющих большее количество пользователей.

Конфигурация осуществляется с помощью специального программного обеспечения.

Производителями беспроводных коммутаторов являются следующие компании: Symbol Technologies, HP,Proxim, Aruba, Wircless Network, D_link.

В России наиболее распространено оборудование компании Symbol Technologies.

Беспроводной коммутатор представляет собой единую систему, включающую в себя функции обеспечения безопасности, управление мобильности для создания беспроводных Ethernet-сетей корпоративного класса.

Оборудование подразумевает центральное администрирование из центров управления сетями.

Средства безопасности включают межсетевой экран с проверкой состояния связи, полнофункциональный сервер со шлюзами на прикладном уровне, встроенная защищенная База Данных в WEB - аутентификации.

Несколько стандартов: 802.11a, 802.11b, 802.11g. позволяют подключить точку доступа к любым стандартам.

Все точки доступа можно разделить по способу подключения: через USB порт и порт подключения Ethernet - RJ45. Последние пользуются наибольшим успехом, так как наиболее просты в настройке и управлении, а также обладают большей скоростью передачи в локальную сеть. Точки доступа могут быть комнатного (in door) и всепогодного (out door) исполнения. Для создания беспроводной сети внутри помещений используют комнатный вариант прибора. Он обладает меньшей стоимостью и, как правило, большим эстетическим видом. Работают такие точки доступа в пределах одной или нескольких комнат. На открытых участках местности (прямая видимость) возможна работа на расстоянии до 300 метров с использованием стандартных всенаправленных антенн. Точки доступа всепогодного исполнения предназначены для создания радиосети между зданиями. В зависимости от типов антенн такие устройства способны организовывать каналы связи на расстоянии порядка 3-5 км. Максимальная дальность беспроводного канала связи заметно увеличивается при использовании усилителей. В этом случае длина радиоканала достигает 8-10 км. Устройства типа точка доступа представлены на рисунке 1.5.

Большой интерес вызывают беспроводные точки доступа, объединяющие в себе функции других устройств, например, высокоскоростного беспроводного широкополосного маршрутизатора со встроенным коммутатором Fast Ethernet. Маршрутизатор позволяет быстро и легко настроить общий доступ к Интернет

для проводной или беспроводной сети или организовать совместное использование широкополосного канала связи и кабельного/DSL модема дома или в офисе.

а б В Г

Рисунок 1.5 - Виды точек доступа: а, б - внутренние; в, г – внешние

Для подключения к беспроводной сети Wi-Fi достаточно обладать ноутбуком или карманным персональным компьютером (КПК) с подключенным Wi-Fi адаптером.

Любой беспроводной Wi-Fi адаптер должен соответствовать нескольким требованиям:

- необходима совместимость со стандартами;
- работа в диапазоне частот 2,4 ГГц - 2,435 ГГц (или 5 ГГц);
- поддерживать протоколы WEP и желательно WPA;
- поддерживать два типа соединения "точка-точка", и "компьютер сервер";
- поддерживать функцию роуминга.

Существует три основных разновидности Wi-Fi адаптеров, различаемых по типу подключения:

1. Подключаемые к USB порту компьютера. Такие адаптеры компактны, их легко настраивать, а USB интерфейс обеспечивает функцию "горячего подключения".

2. Подключаемые через PCMCIA слот (CardBus) компьютера. Такие устройства располагаются внутри компьютера (ноутбука) и поддерживают любые стандарты, позволяющие передавать информацию со скоростью до 108 Мбит/с.

3. Устройства, интегрированные непосредственно в материнскую плату компьютера. Самый перспективный вариант. Такие адаптеры устанавливаются на ноутбуки серии Intel Centrino. И, в настоящее время используются на подавляющем большинстве мобильных компьютеров. Все виды беспроводных адаптеров представлены на рисунке 1.6.

а б в

Рисунок 1.6 - Беспроводные адаптеры: а - с USB портом, б - формата PCMCIA, в – встраиваемый

Выводы по разделу один:

На сегодня наиболее актуальными технологиями беспроводной связи является Wi-Fi. Эта среда находит повсеместное применение в современном подходе построения систем связи. С широким применением технологий возникает проблема обеспечения информационной безопасности. В решение подобных проблем в технологиях беспроводной связи существуют протоколы безопасности. В каждой из технологий имеющиеся протоколы безопасности содержат ряд недостатков и преимуществ.

2 АНАЛИЗ ПРЕДПРИЯТИЯ, ЕГО СТРУКТУРЫ И ИНФОРМАЦИОННЫХ РЕСУРСОВ

2.1 Характеристика исследуемого объекта

Объект исследования выпускной квалификационной работы - общество с ограниченной ответственностью «Инструментстрой».

Сфера деятельности организации - оптовая и розничная торговля различным инструментом:

- слесарным;
- измерительным;
- столярным;
- крепежным;
- автомобильным;
- садовым;
- режущим;
- строительно-отделочным.

Так же исследуемая компания оказывает услуги в области резки стекла в городе Нижневартовск, уборки и вывоза снега и укладки тротуарной плитки.

Физический адрес компании: г. Нижневартовск, ул. Индустриальная, 79, ст. 3.

Сайт в сети Интернет: http://instrument-nv.ru/.

Рассмотрим информационную структуру исследуемой компании.

Число рабочих компьютеров в организации - 21. Имеются объединения компьютеров в рабочие группы.

В организационную структуру ООО «Инструментстрой» входят:

- директор компании;
- технический отдел;
- секретарь;
- системный администратор;

- отдел бизнес-интеграции;

- отдел по работе с клиентами;

- отдел кадров;

- бухгалтерия.

Все персональные компьютеры офиса организации располагаются в пределах одного этажа административного здания.

План помещений организации ООО «Инструментстрой» представлен на рисунке 2.1 ниже.

Характеристики рабочих ЭВМ, применяющихся в организации - Intel Core I7-3770 3.9 GHz, ОЗУ 8 Gb, HDD 1 Tb. Используемая операционная системы на рабочих компьютерах - Windows 7.

Состав аппаратных средств, используемых в компании, представлен в таблице 2.1.

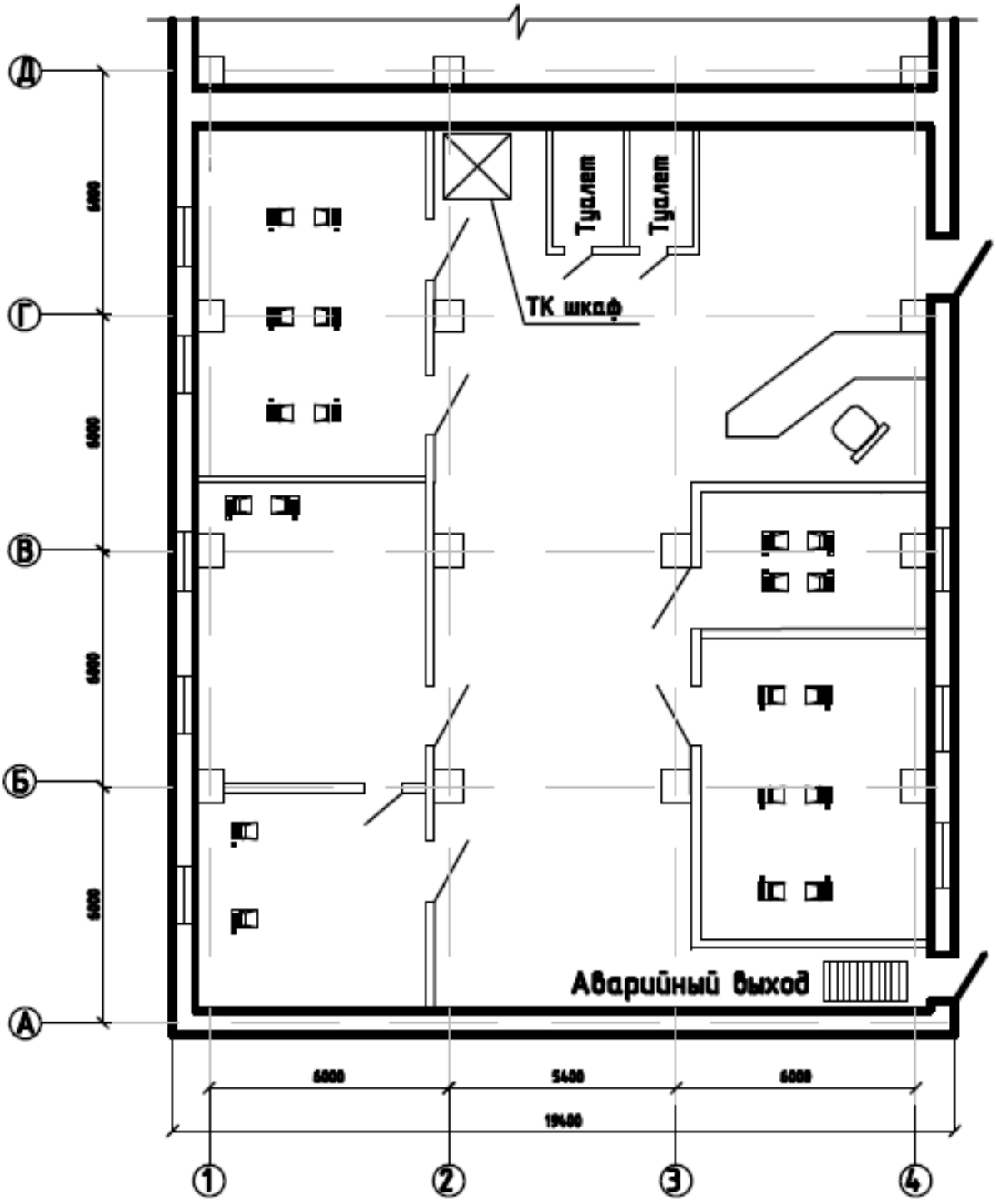


Рисунок 2.1 - План помещений организации ООО «Инструментстрой»

Таблица 2.1 - Состав аппаратных средств компании

Наименование оборудования	Описание оборудования	Кол.
ЭВМ	Intel Core I7-3770 3.9 GHz, JPE 8 Gb, HDD 1 Tb	21
Принтер	Canon LaserShot LBP-1120	5
Плоттер	HP Designjet 130	2

В компании функционирует информационная система "1С: Торговля и склад". Данная ИС предназначена для учета основных видов торговых операций. Благодаря гибкости и настраиваемости система способна выполнять все необходимые предприятию функции учета - от ведения справочников и ввода первичных документов до получения различных ведомостей и аналитических отчетов.

"1С: Торговля и склад" автоматизирует работу на всех этапах деятельности компании и позволяет:

- вести раздельный управленческий и финансовый учет;
- вести учет товарного запаса с возможностью выбора метода списания себестоимости;
- вести раздельный учет собственных товаров и товаров, взятых на реализацию;
- оформлять закупку и продажу товаров;
- производить автоматическое начальное заполнение документов на основе ранее введенных данных;
- вести учет взаиморасчетов с покупателями и поставщиками, детализировать взаиморасчеты по отдельным договорам;
- выполнять резервирование товаров и контроль оплаты;
- вести учет денежных средств на расчетных счетах и в кассе;
- вести учет товарных кредитов и контроль их погашения;
- вести учет переданных на реализацию товаров, их возврат и оплату;

Доступ к ИС имеется исключительно у работников компании. Сотрудники имеют доступ только к ограниченному числу файлов рассматриваемой системы, которые необходимы в ходе их трудовой деятельности.

2.2 Состав и структура информационных ресурсов предприятия

В ИС ООО «Инструментстрой» происходит обработка информации, содержащей персональные данные сотрудников и клиентов организации. С помощью вышеуказанной системы происходят следующие внутренние процессы компании:

- формирование штатного расписания - регистрация подразделений и должностей, формирование штата организации;
- прием сотрудников на работу, назначение на должность;
- учет личных сведений сотрудников;
- ведение журналов по отпускам и больничным листам;
- учет сведений по всем исполняемым сотрудником должностям;
- учет кадровых перемещений - перевод на другую должность;
- ведение архива уволенных сотрудников;
- формирование отчетных документов, приказов по штатному расписанию и персоналу.

Так же по средствам данной системы происходят следующие внешние процессы компании:

- формирование заявок на оформление заказов клиентов;
- оформление карт постоянных покупателей для постоянных клиентов компании. При оформлении данных карт используются персональные данные клиентов - фамилия, имя, отчество, паспортные данные, мобильный телефон. При оформлении карт клиент дает свое согласие на обработку персональных данных в соответствии с действующим законодательством.

На данном предприятии имеется объединение компьютеров в локальную сеть только сотрудников бухгалтерии, работа которых связана с информационной

средой "1С: Торговля и склад". Отсутствие единой ЛВС в рассматриваемой организации в значительной степени осложняет функционирование компании. Создание общей, беспроводной ЛВС организации позволит обеспечить автоматизацию большинства рабочих процессов, облегчить работу сотрудников и повысить производительность их труда и эффективность работы ООО «Инструментстрой».

На первых стадиях выпускной квалификационной работы необходимо проанализировать информационные потоки, циркулирующие в исследуемой информационной системе организации. По результатам анализа следует составить перечень информационных ресурсов, обрабатываемых организацией. Результатом вышеуказанного анализа должен быть список, содержащий факты получения/обработки/хранения информации. По каждому факту обработки информации необходимо дать следующие описания:

- цель получения данных;
- механизм получения данных;
- перечень получаемых данных;
- механизм обработки информации;

В результате проведённого анализа ИС организации были выявлено виды обработки информации, представленные ниже в таблице 2.2.

Таблица 2.2 - Виды обработки информации в ООО «Инструментстрой»

№ п/п	Наименование подразделения	Вид данных	Место обработки/хранения
1	Технический отдел	Техническая информация о заказах клиентов	Данные технического отдела
2	Отдел по работе с клиентами	ФИО, паспортные данные клиентов компании	Электронная документация отдела по работе с клиентами
3	Отдел бизнес-интеграции	Информация о планах развития компании, политика функционирования компании	Данные бизнес-приложения

Продолжение таблицы 2.2

№ п/п	Наименование подразделения	Вид данных	Место обработки/хранения
4	Бухгалтерия	ФИО, паспортные данные, дата рождения, сведения о работе (должность, место работы), сведения о доходах сотрудников компании	1С: Бухгалтерия, 1С: Торговля и склад
5	Отдел кадров	ФИО, паспортные данные, сведения о работе сотрудников	Электронная документация отдела кадров

В итоге, обработка информации в ИС организации осуществляется в том или ином виде в пяти подразделениях.

Функционально в ИС компании можно выделить три основные категории:

1) категория ПО «1С: Торговля и склад»;

2) базы данных подразделений;

3) файловые ресурсы.

Рассмотрим каждую категорию отдельно.

Обработка информации первой категории производится сотрудниками департамента кадровой политики и сотрудниками технического отдела и отдела по работе с клиентами. Режим обработки данных - многопользовательский, имеет место разграничение прав доступа.

Обработка информации в Базах данных отделов осуществляется сотрудниками всех подразделений компании. Режим обработки данных - многопользовательский, имеет место разграничение прав доступа.

В категории «хранение данных» на файловых ресурсах обработка информации производится так же работниками всех подразделений. Режим обработки информации - многопользовательский, имеет место разграничение прав доступа.

В ИС организации происходит обработка персональных данных сотрудников и клиентов ООО «Инструментстрой», поэтому при проектировании ЛВС организации необходимо применение средств защиты информации, имеющих сертификаты ФСТЭК и ФСБ.

2.3 Анализ требований и разработка технического задания на проект беспроводной ЛВС предприятия

В ходе совместной работы с системным администратором ООО «Инструментстрой», были разработаны основные базовые требования, предъявляемые к проектируемой сети.

Данные требования сформированы с учетом рабочих потребностей и нагрузок на проектируемую компьютерную сеть.

Основные требования представлены ниже.

Общее количество точек - 21.

Тип соединения - WLAN для работы пользователей по WI-FI (802.11g).

Локальная вычислительная сеть в целом должна соответствовать категории не ниже 5E, все комплектующие должны соответствовать категории не ниже 5e.

Для создания беспроводной ЛВС необходимо использовать только высококачественные компоненты, которые прошли стопроцентное тестирование в соответствии с требованиями ISO 9001.

Оборудование ЛВС и схемы его соединений должны обеспечивать двойное резервирование каналов передачи данных.

Следует отметить, что вышеперечисленные требования являются базовыми и необходимыми.

Для конкретизации необходимых требований в ходе выпускной квалификационной работы разработано техническое задание на выполнение работ по проектированию беспроводной ЛВС ООО «Инструментстрой». В данном техническом задании определены необходимые требования к проекту.

Техническое задание на выполнение работ по проектированию беспроводной ЛВС ООО «Инструментстрой» приведено ниже.

1. Общие сведения о проекте.

Проектирование беспроводной ЛВС должно производиться на основе следующие документов:

- настоящее согласованное с руководством компании Техническое Задание на проект беспроводной ЛВС ООО «Инструментстрой»;

- договор на проект сети;

- стандарт локальной сети ISO 9001.

Информация по срокам и этапам выполнения работ по разработке сети закрепляется в договоре на выполняемые работы.

2. Цели создания беспроводной ЛВС ООО «Инструментстрой».

Локальная вычислительная сеть должна выполнять функции организации передачи данных компании. Определенные техническим заданием требования используются в качестве базы в процессе проектирования ЛВС.

3. Общие требования к проектируемой беспроводной ЛВС.

3.1. Требования к сети в целом.

Общее число точек сети - 21.

Проектируемая ЛВС должна удовлетворять условиям соответствия категории 5E, все комплектующие, входящие в состав сети, должны удовлетворять условиям соответствия категории не 5e.

При проектировании ЛВС следует пользоваться комплектующими, прошедшими тестирование и соответствующими требованиям стандарта ISO 9001.

3.2. Основные требования к активному сетевому оборудованию.

1) Активное сетевое оборудование ЛВС должно исправно функционировать без перебоев 24 часа в сутки, 7 дней в неделю, не учитывая время, необходимое на проведение технико-регламентных работ.

2) Маршрутизатор необходимо выполнить на базе с установленной ОС Linux, так как данная ОС обладает низкой себестоимостью и, при этом, качественными эксплуатационными характеристиками. Ядро системы - не ниже 2.6, должна присутствовать функция биллинга.

3) Количество портов активного сетевого оборудования должно обеспечивать возможность бесперебойного функционирования всех рабочих помещений, а так же иметь запас в 10%.

3.3. Основные требования к системе электропитания и заземления.

Электропитание рабочих мест проектируемой компьютерной сети должно осуществляться по выделенной распределительной электрической сети 380/220В, 50Гц, которая должна подключается к общему электроснабжению здания.

3.4 Основные требования к надежности проектируемой сети.

Совокупность оборудования из состава проектируемой ЛВС должна обеспечивать стабильные физические характеристики канала между портами активного сетевого оборудования и абонентами сети независимо от состояния трассы коммутации.

В случае, если какой-либо из каналов вышел из строя, должен автоматически обеспечиваться переход на использование резервных каналов.

3.8. Требования к безопасности проектируемой ЛВС.

Оборудование и материалы, используемые при проектировании ЛВС, не должны допускать вреда здоровью или поражения сотрудников электрическим током, электромагнитным излучением, при условии соблюдений правил эксплуатации ЛВС.

3.9. Требования однородности.

При проектировании ЛВС требуется применять унифицированные типы кабельных систем рабочих мест, независимо от подключаемого технического оборудования и активного сетевого оборудования.

3.10. Требования расширяемости.

В процессе проектирования необходимо обеспечить при необходимости возможность увеличить абонентскую емкость проектируемой ЛВС на 10% за счет подключения дополнительной линии.

Разработанное Техническое задание учитывает все основные и специальные требования, предъявляемые руководством компании к проектируемой сети.

Выводы по разделу два:

Для расчета, построения и последующего внедрения беспроводной ЛВС, с системным администратором ООО «Инструментстрой» были согласованы ряд необходимых требований, была рассмотрена информационная структура компании, посчитана и учтена вся компьютерная техника, все отделы, составлен перечень информационных ресурсов, обрабатываемых организацией, произведен анализ требований и разработано техническое задание на проект беспроводной ЛВС предприятия.

3 РАЗРАБОТКА СХЕМЫ И ОРГАНИЗАЦИЯ БЕСПРОВОДНОЙ ЛВС ПРЕДПРИЯТИЯ

3.1 Разработка структуры ЛВС

Беспроводная сеть, которую планируется реализовать, будет основана на стандарте IEEE 802.11n.

Сеть будет управляться сервером с помощью беспроводного коммутатора. Так как беспроводной коммутатор и точки доступа распространяют сигнал сферически, планируется установить три точки доступа по всей площади офиса, а беспроводной коммутатор - в центре офиса, для охвата каждой точки доступа. Схема беспроводной сети представлена на рисунке 3.1.

Организация сети доступа:

- Организовать сеть беспроводного доступа, для чего приобрести и установить три точки доступа.

- Беспроводной коммутатор разместить в рабочем помещении на третьем этаже.

- Настроить беспроводной коммутатор, определить точки доступа. Обеспечить мониторинг и защиту сети.

- Организация подключения к сети Internet. Доступ к сети Internet организовать через широкополосный /DSL модем.

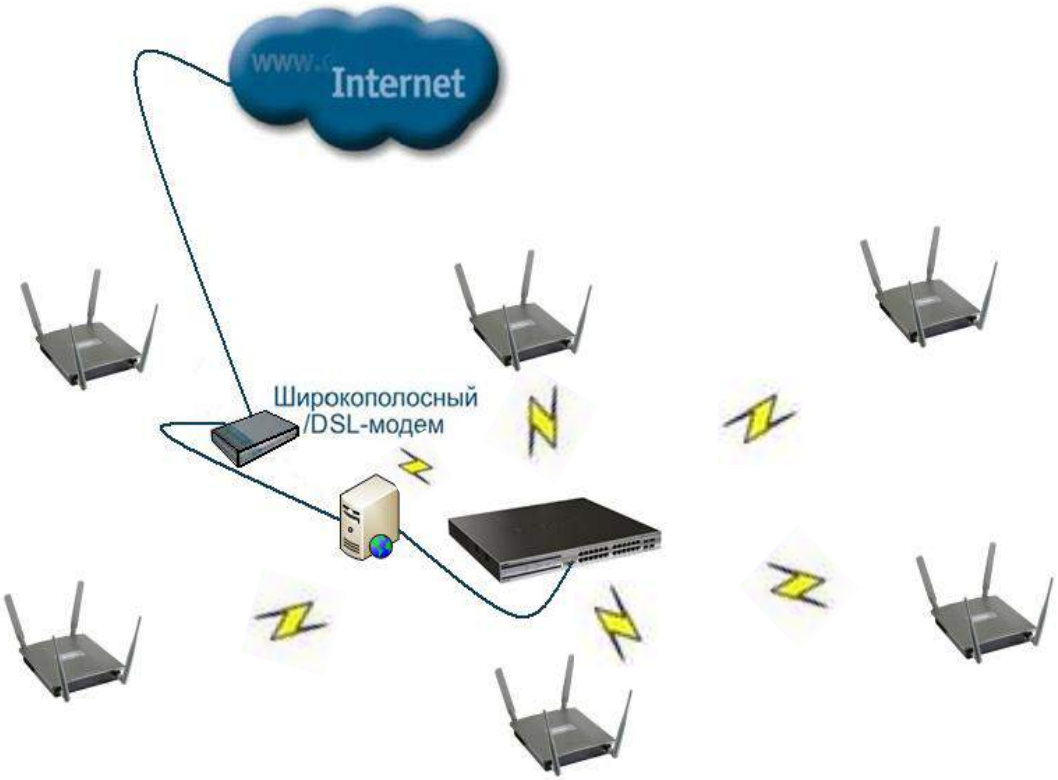


Рисунок 3.1 - Схема беспроводной сети

3.2 Выбор необходимого аппаратного и программного обеспечения

3.2.1 Выбор точки доступа

Используемая точка доступа - D-Link DWL-8600AP.

D-Link DWL-8600AP - унифицированная беспроводная точка доступа, соответствующая стандарту IEEE 802.11n. Гибкая в управлении и мощная, данная точка доступа предназначена для развертывания сетей в режиме автономной беспроводной точки доступа или в режиме управляемой точки доступа, управление которой осуществляется при подключении к беспроводному коммутатору. Предприятия могут начать работу с организации сети с помощью одной интеллектуальной точки доступа DWL-8600AP, предоставляющей ряд расширенных функций LAN, а затем в любое время перейти к централизованной

системе управления после подключения аналогичной точки доступа DWL-8600AP к унифицированному проводному/беспроводному коммутатору D-Link.

Стандарт 802.11n увеличивает пропускную способность в 6 раз больше по сравнению с сетями стандарта 802.11a/g. Точка доступа DWL-8600AP является обратно совместимой с устройствами стандарта 802.1a/b/g и позволяет настройку 2x2:2* в обоих направлениях Tx/Rx. Технология Multiple In Multiple Out (MIMO) и каналы с увеличенной пропускной способностью увеличивают физическую скорость передачи данных при использовании стандарта 802.11n. MIMO обеспечивает одновременную передачу нескольких сигналов с помощью нескольких антенн вместо одной.

DWL-8600AP поддерживает функцию APSD (Автоматический переход в режим сохранения энергии) по расписанию и вне расписания. Выполняемая вне расписания функция APSD (U-APSD) является более эффективным методом управления питанием по сравнению с функцией Power Save Polling 802.11. Основным преимуществом функции U-APSD является возможность синхронизации передачи и получения голосовых фреймов с точкой доступа, таким образом, устройство может переходить в режим сохранения энергии в случае, когда не выполняется отправка или прием пакетов. DWL-8600AP является полностью совместимой с устройствами стандарта 802.3af даже в режиме максимально потребляемой мощности. В отличие от точки доступа стандарта 802.11n других производителей, которым требуется PoE или 802.3at при работе обеих частот, DWL-8600AP обеспечивает непрерывную поддержку энергосберегающей технологии D-Link Green. Вид DWL-8600AP представлен на рисунке 3.2.

Рисунок 3.2 - Беспроводная точка доступа DWL-8600AP

Коммутаторы DWS-4026 автоматически настраивают каждую подключенную точку доступа DWL-8600AP, таким образом, во время установки не требуется настройка. При замене DWL-8600AP выполняется автоматическая настройка точки доступа с теми же параметрами, что и у предыдущего устройства, что значительно упрощает процесс замены.

DWL-8600AP поддерживает набор встроенных функций, позволяющий администраторам организовать защищенную сеть и подключиться к любому коммутатору и маршрутизатору, совместимому с устройствами Ethernet. Расширенные функции беспроводной сети, поддерживаемые точкой доступа, включают: WEP-шифрование данных, безопасность WPA/WPA2, фильтрация MAC-адресов, балансировка нагрузки между точками доступа, QoS/WMM (Wireless Media) и обнаружение несанкционированных точек доступа. DWL-8600AP поддерживает возможность локального хранения настроек безопасности. Можно расширить беспроводные подключения путем добавления нескольких точек доступа DWL-8600AP к другим точкам доступа с поддержкой стандарта 802.11a/g/n. Благодаря функции AP Clustering можно объединить до 8 точек доступа для удобства управления и настройки всех точек доступа. Предприятия, не требующие сложной сетевой инфраструктуры, могут использовать DWL-

8600AP для установки беспроводной сети без дополнительного аппаратного обеспечения.

В качестве альтернативного варианта DWL-8600AP может работать совместно с унифицированным проводным/беспроводным коммутатором. В данном режиме несколько точек доступа DWL-8600AP могут быть подключены непосредственно или опосредованно к одному из данных коммутаторов для обеспечения высокого уровня безопасности и беспроводной мобильности. При подключении к этим коммутаторам каждая точка доступа DWL-8600AP автоматически настраивается на оптимальный радиочастотный канал и выходную мощность передатчика, обеспечивая беспроводных клиентов сигналом наилучшего качества как в полосе 2,4ГГц, так и в полосе 5ГГц, предоставляя непрерывное беспроводное соединение.

DWL-8600AP обеспечивает максимальную скорость беспроводного соединения для каждого из частотных диапазонов. При одновременной работе в двух диапазонах частот можно создать две сети, использующие полную полосу пропускания беспроводного канала, что позволит повысить общую производительность беспроводной сети. Кроме того, DWL-8600AP остается полностью обратно совместимой с оборудованием стандарта 802.11b, работающим на частоте 2,4ГГц.

DWL-8600AP непрерывно сканирует оба диапазона частот и связанные с ними каналы для обнаружения несанкционированных подключений, обеспечивая при этом соединение для мобильных клиентов. Если обнаружено несанкционированное подключение, точка доступа отправляет отчет коммутатору DWS-4026, который ей управляет. Используя управляющую консоль, администратор может определить несанкционированную точку доступа и предпринять соответствующие действия. DWL-8600AP поддерживает такие функции как 64/128/152-битное WEP-шифрование данных, WPA/WPA2 и Multiple SSID для каждого радиочастотного канала. При подключении к коммутатору DWS-4026 эти функции наряду с фильтрацией MAC-адресов и запретом широковещания SSID могут использоваться для настройки параметров

безопасности и ограничения доступа во внутреннюю сеть извне. DWL-8600AP поддерживает 802.1Q VLAN Tagging и WMM (Wi-Fi Multimedia) для передачи данных таких приложений как VoIP и потоковое аудио/видео с заданным приоритетом.

3.2.2 Выбор коммутатора сети

Решено применять коммутатор серии DWS-4026.

Данная серия включает унифицированные проводные/беспроводные коммутаторы, которые поддерживают расширенные функции и стандарты 802.11n. Данные коммутаторы имеют возможность управления до 64 беспроводными точками доступа DWL-8600AP и до 256 точками доступа DWL-8600AP. DWS-4026 - это полнофункциональное и экономичное решение для среднего и крупного бизнеса, а так же провайдеров услуг. Коммутатор DWS-4026 способен поддерживать функции управления и применяется, как беспроводной контроллер в беспроводной сети или в качестве гигабитного коммутатора второго уровня с поддержкой PoE. По средствам настройки управления WLAN, а так же функций управления, используемый коммутатор дает возможность администраторам легко контролировать работу сети.

Большая часть из имеющихся на данный момент на рынке контроллеров сети осуществляют процесс централизованной обработки трафика. Данный процесс в большинстве случаев вызывает значительную задержку трафика. Коммутатор DWS-4026 предоставляет пользователям дополнительный функционал. Беспроводной трафик возможно направлять обратно к коммутатору с целью обеспечения безопасности либо локально перенаправлять к точке доступа для обеспечения оптимальной производительности. Коммутатор данной серии предоставляет администраторам сети гибкость по средствам наличия опций туннелирования трафика к коммутатору с целью управления безопасностью и перераспределения трафика для оптимальной производительности.

DWS-4026 так же имеет возможность поддержки функции Wireless Intrusion Detection System (WIDS), предназначенной для обнаружения несанкционированных точек доступа и нарушителей, обнаружения угроз безопасности беспроводной ЛВС. По средствам функции WIDS системные администраторы имеют возможность обнаруживать разнообразные угрозы безопасности, а так же использовать сканирование каналов с целью обзора сети и предотвращения потенциальных угроз. Другие функции безопасности - это WPA/WPA2 Enterprise, адаптивный портал, а так же аутентификация, которая основывается на применении MAC-адресов.

Беспроводные клиенты имеют возможность использовать преимущества гибкого роуминга между точками доступа, которые управляются коммутатором DWS-4026и даже в том случае, если они находятся в разных подсетях. DWS-4026 оперирует различными механизмами, такими как аутентификация, а так же кэширование ключей, поэтому беспроводные клиенты сети имеют возможность перемещаться в зоне действия беспроводной сети не прибегая к процедуре повторной аутентификации. Быстрый роуминг производится без разрыва соединений, что обеспечивает устойчивую работу соединений мобильных приложений. DWS-4026 поддерживает функции туннелирования точек доступа. Данная функция применяется с целью поддержки роуминга без перенаправления данных трафика. Это значительно оптимизирует сетевой трафик и сохраняет полосу пропускания.

DWS-4026 имеет возможность поддержки функцию формирования трафика. Данная функция упорядочивает трафик с течением времени, благодаря чему, скорость передачи данных ограничивается.

DWS-4026 так же имеет возможность поддерживать функцию «самовосстановления» сети, которая увеличивает отказоустойчивость проектируемой беспроводной сети. С целью восполнения недостаточной зоны покрытия из-за поломки точки доступа (к примеру, из-за сбоя питания), коммутатор в автоматическом режиме наращивает выходную мощность передатчиков других точек доступа, с целью увеличить зону покрытия. Что бы

обеспечить непрерывное подключение клиентов, коммутатор осуществляет балансировку нагрузки точек доступа. Так же коммутатор блокирует подключения новых пользователей к точке доступа с целью исключения перегрузки полос пропускания. Функция самовосстановления сети, а так же балансировки нагрузки точек доступа, коммутатор DWS-4026 позволяет эффективно регулировать полосу пропускания, трафик WLAN, а так же обеспечить зону наилучшего покрытия.

Кроме функционирования в виде управляющего устройства, коммутатор DWS-4026 имеет возможность использоваться в качестве стандартного проводного коммутатор второго уровня с расширенным функционалом.

3.2.3 Выбор программного обеспечения

Имеется два базовых варианта операционных систем: система на базе ядра LINUX и система на базе ядра WINDOWS. Недостатками серверов на базе операционных систем Windows является завышение требований к ресурсам, уязвимость для DoS-атак, нестабильная работа в сети. Учитывая требования технического задания, использоваться будет операционная система на базе ядра LINUX.

Проектируемая сеть должна давать для пользователей возможность выхода в глобальную сеть Интернет. Данная возможность реализуется при помощи сервера-шлюза, базирующегося на операционной системе LINUX.

Главные задачи, которые должен решать сервер-шлюз - это обеспечение пользователям сети доступа в Интернет, учеты трафика за каждым пользователем, а так же защита локальной сети от внешних атак [12].

Разделение и учет трафика можно организовать двумя способами: настройкой маршрутизации вместе с биллинговой системой или с применением прокси-сервера. Обе схемы имеют равное значение и применимы очень широко.

Общий принцип применения прокси-сервера выражен в том, что пользователь ЛВС прописывает в браузере IP и порт прокси-сервера, а затем все

запросы браузер переводит на определенный порт LINUX сервера. Итак, можно сделать выводы, что учет производится по всем протоколам и портам, не понижает производительность сервера при динамической работе пользователей в интернете.

Сравним два вида интернет-шлюзов: на базе платформы Microsoft Windows и на базе платформы Linux.

На рынке имеется множество продукции на базе данных платформ. Рассмотрим самые популярные.

1. KERIO CONTROL (WINDOWS).

Возможности данного программного обеспечения включают:

- возможность управления полосой пропускания;
- надежную защиту от хакерских атак;
- DHCP, DNS серверы;
- кеширующие PROXY сервера;
- мощный инструмент управления доступом в сеть Интернет;
- антивирусное ядро;
- авторизацию пользователей;
- гибкую настройку и удобное управление.

После изучения характеристик данного программного обеспечения, делаем выводы, что эта модель удобна в настройке, может создавать временные зоны пользователей. Стоимость на 25 человек составляет 60 000 рублей без учета стоимости операционной системы WINDOWS.

2.TRAFFIC INSPECTOR (WINDOWS).

Преимущества данного программного обеспечения заключаются в:

- наличии лицензии ФСТЭК на осуществление деятельности по разработке, производству систем защиты информации;
- многоуровневой защите трафика: в составе Traffic Inspector имеется система блокирования высокой активности, защищающая от неизвестных вирусных программ;

- простоте установки и функционирования программного обеспечения, которое работает на ОС Microsoft Windows, при этом не требуя специфических настроек;

- наличие маршрутизации трафика нескольких провайдеров.

Сделаем выводы, что данная модель удобна при настройке, которая осуществляется через административную панель. Стоимость на 25 человек - 14 000 рублей без учета цены операционной системы WINDOWS.

3. TRAFFPRO OFFICE (LINUX PACKAGE).

С помощью данного программного обеспечение решаются вопросы:

- защиты сети от внешних угроз;

- использования резервирования каналов;

- использования одновременно более двух провайдеров;

- ограничения доступа пользователей сети к развлекательным ресурсам;

- балансирования трафика между пользователями сети для увеличения качества использования каналов;

- блокирования вирусной активности [20].

Сделаем выводы по данному программному обеспечению.

Данная программа имеет возможность установки с помощью исходников на установленную систему LINUX (FEDORA, UBUNTU) через запуск автоматических скриптов установки. Все необходимые программы установки скачиваются в автоматическом режиме. Пользователь имеет возможность в процессе установки указывать сетевые интерфейсы. Программное обеспечение TRAFFPRO требует от пользователя базовых знаний операционной системы LINUX. Рассматриваемая программа не перегружена большим количеством служб и способна функционировать на слабых конфигурациях ПК. Цена на 40 человек составляет 12 000 рублей.

3.3 Организация работы беспроводной ЛВС

3.3.1 Управление сетью

В организации имеется 38 рабочих станций пользователей. Для защиты корпоративной информации от несанкционированного доступа пользователей к настройкам программного обеспечения было решено использовать доменную сеть в ЛВС.

Домен представляет собой единый и целостный управляемый объект. Домен имеет как минимум один сервер, осуществляющий функцию контроллера домена. Контроллер домена позволяет централизованно осуществлять контроль над сетью, конфигурировать компьютеры, подключенные к домену. Доменная система позволяет в значительной степени повысить безопасность сети, управляя разрешениями, политиками безопасности. Это значит, что без ведома администратора домена, никто не может легально, самостоятельно подключиться к сети и получить доступ ко всей информации в сети. Компьютеры - члены домена подконтрольны контроллеру домена. Для того, что бы обновить программное обеспечение, изменить настройки и тому подобное, нет необходимости обходить каждый компьютер в доменной сети и все делать вручную. Все можно сделать через контроллер домена.

Из этого делаем выводы, что такая организация ЛВС экономит значительное количество времени и имеет много плюсов.

3.3.2 Организация сетевых ресурсов локальной сети

На предприятии с таким количеством рабочих станций, невозможно представить работу без организации сетевых ресурсов. Для этого необходимо использовать файловый сервер (он же резервный контроллер домена). Схема общих ресурсов представлена в таблице 3.1. Есть общие папки, к которым открыт общий доступ на основаниях требования политики безопасности.

Таблица 3.1 - Схема общих ресурсов

Название ресурса	Назначение	Права
Личные папки	Используются для обмена информацией между пользователями организации	Полный доступ для всех пользователей сети
Базы данных компании	Резервное копирование информационных ресурсов отделов	Свободный доступ пользователей ограничен
Резервные копии информационной системы компании	Сохранение информационных ресурсов компании	Свободный доступ пользователей ограничен
Отдел кадров	Используется для хранения данных отдела кадров	Отдел кадров - полный доступ, корреспонденты - только чтение и т.д.
Отдел по работе с клиентами	Используется для хранения персональных данных клиентов.	Сотрудники отдела по работе с клиентами - полный доступ. Остальные - только чтение
Бухгалтерия	Используется для хранения служебной информации бухгалтеров	Бухгалтерия - полный доступ. Остальные - только чтение.

К некоторым рабочим станциям подключены принтеры через интерфейс USB. На данной рабочей станции делается общий доступ к принтеру (если такой доступ необходим) и далее возможно подключение данного устройства для печати на любой компьютер предприятия.

Очевидный минус такого способа, заключается в том, что в то время, когда компьютер выключен или отключен от ЛВС - печать на принтере будет невозможна. Однако часть принтеров организации имеет сетевой интерфейс RJ-45.

Такие принтеры подключаются в любой ближайший коммутатор (предварительно на принтере должен быть настроен IP-адрес), на любой компьютер сети (рисунок 3.3). Тут и до конца страницы у меня не читается

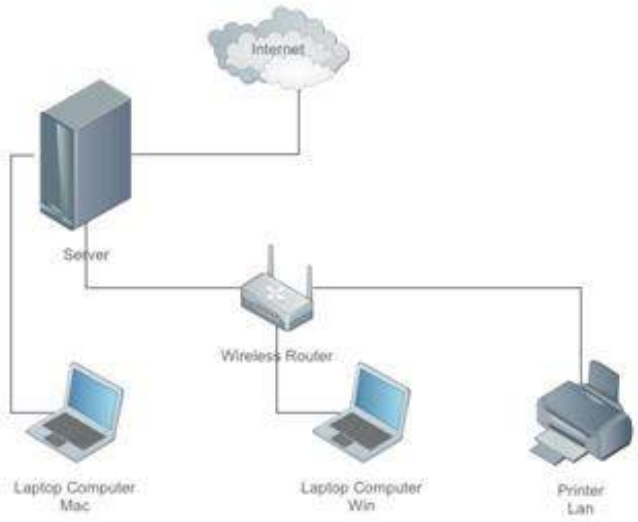


Рисунок 3.3 - Организация подключения сетевого принтера

Плюсом данной схемы подключения является круглосуточный доступ к принтеру.

Выводы по разделу три:

В процессе разработки схемы и организации беспроводной ЛВС предприятия были выбраны три точки доступа D-Link DWL-8600AP, т.к. они обладают достаточной мощностью и охватывают большую часть покрытия, один коммутатор серии DWS-4026, который автоматически умеет настраивать эти точки при подключении к нему (экономия времени) и выбран стандарт связи 802.11n, т.к. он увеличивает пропускную способность в 6 раз больше по сравнению с сетями стандарта 802.11a/g.

4 УСТАНОВКА И НАСТРОЙКА НЕОБХОДИМОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

4.1 Подключение коммутатора

Необходимо осуществить подключение и настройку выбранного коммутатора DWS-4026.

Коммутатор располагает 48 портами на скорости 10/100 Мбит/с и 4 портами на скорости 100/1000 Мбит/с. Число рабочих помещений - 10. Гигабитные порты 51-52 из резерва примем тегируемыми. Через них будет реализовываться функция подключения сетевых карт от маршрутизатора.

Порты 49-50 задействованы для подключения 2 двух каналов провайдера интернета (основной и резервный).

Порты с 1 по 12 задействованы в подключении рабочих помещений.

Настройка на маршрутизаторе:

- на интерфейсе №1 (eth0) маршрутизатора будут настроены два сабинтерфейса vlan100 и vlan101. На них будут реализованы настройки провайдеров интернета;

- на интерфейсе №2 (eth1) маршрутизатора будут настроены 42 сабинтерфейса vlan2-vlan43 с настройкой IP параметров.

Настройка на коммутаторе:

- формируются виртуальные сети vlan2-vlan13, порты с 1 по 12 поочередно добавляются в VLAN;

- на портах 49 и 50 создаются vlan100 и vlan101. Данные порты будут принимать Интернет-каналы от различных провайдеров;

- порт 51 соединен со вторым интерфейсом маршрутизатора. Его сделаем тегируемым и добавим данный порт в vlan100 и vlan101. С помощью этого мы сможем использовать одну физическую линию и вместить в неё два канала [19];

- порт 52 коммутатора будет соединен со вторым интерфейсом маршрутизатора. Его необходимо сделать тегируемым, а так же добавить его в vlan2-vlan43.

Настройки сети на коммутаторе сформированы по умолчанию. Они имеют адрес 192.168.1.100/24. Изначально порты включены в vlan1. Поэтому конфигурировать telnet-ом можно с помощью любого порта [18].

Для исключения возможности потери управления над коммутатором в процессе удаления портов из vlan1, подключим коммутатор к порту 48. Далее выполним команды удаления портов со 2 по 13.

Включим в каждый vlan порт 52. Гигабитный порт 52 соединяем с сетевой картой шлюза, на котором будут настроены VLAN порты.

Коммутацию входных интернет-каналов будет осуществлять коммутатор. Каждому каналу будет сформирован отдельный VLAN. Будет осуществляться привязка к порту. Создадим VLAN на 49 и 50 портах.

Добавим гигабитные порты в VLAN.

Добавим тегированный порт - гигабитный порт в VLAN.

Для получения хорошей производительности коммутации и маршрутизации между VLAN следует воспользоваться сетевой картой с поддержкой VLAN 802.1Q. Последняя облегчит работу процессора сервера за счет добавки тега в кадр, а так же пересчёта контрольных суммы. Процессор будет работать только над маршрутизацией интерфейсов, сервисов и служб.

4.2 Установка операционной системы сети

Произведем установку операционной системы с ядром LINUX на маршрутизатор. Серверным вариантом является установка одного ядра системы вместе с необходимыми программами, среди которых C++ компилятор, текстовый редактор, ssh сервер, командные оболочки BASH и SH. Серверный вариант не содержит графическую оболочку рабочего стола, поскольку серверу она не требуется.

Сегодня возможность серверной установки имеется у дистрибутивов, основанных на версии ОС RedHat Enterprise Linux. Один из таких дистрибутивов - бесплатный Russian Fedora Linux, располагаемых в свободном доступе.

На рисунке 4.1 представлено окно установщика.

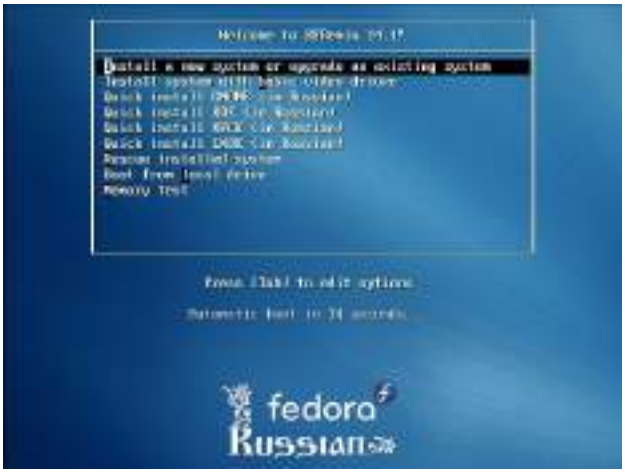


Рисунок 4.1 - Окно приветствия установщика

При установке Linux установщик дает возможность проверить носитель на ошибки (рисунок 4.2).

Рисунок 4.2 - Окно теста носителя

Затем установщик предлагает вариант разбиения диска (рисунок 4.3).

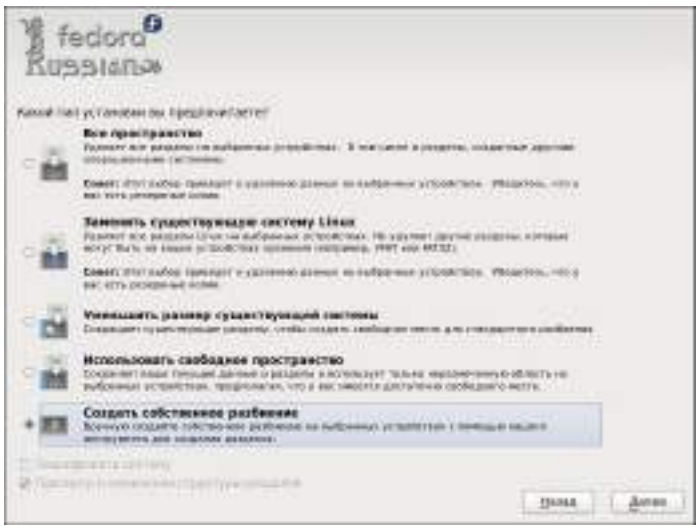


Рисунок 4.3 - Выбор ручного разбиения диска на разделы

Необходимо разбить диск так, чтобы под каждый раздел имелось собственное разбиение. Исходный объем жесткого диска - 1 Тб, данного объема вполне достаточно для реализации необходимых функций.

В следующем окне необходимо отметить наименьшую конфигурацию (рисунок 4.4) и выбрать лишь те пакеты, которые будут требоваться для работы.

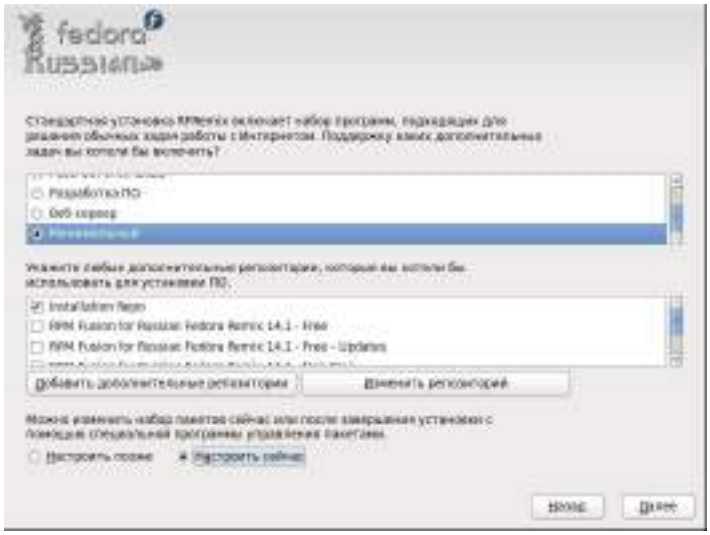


Рисунок 4.4 - Выбор типа установки

Завершающий этап установки состоит в том, что система инсталлирует все требуемые пакеты (рисунок 4.5) и предлагает перезагрузить компьютер. Установка завершена.

Рисунок 4.5 - Завершение установки

4.3 Установка и настройка дополнительного программного обеспечения сети

Настройка операционной системы подразделяется на следующие этапы:

- конфигурирование сети;
- добавление VLAN интерфейсов;
- установка DHCP, DNS серверов.

1. Конфигурирование сети.

Конфигурирование сети в Linux осуществляется посредством следующих команд:

ifconfigethx 292.168.5.x netmask 455.755.258.1 up,

где, ethx - оператор, определяющий имя сетевого интерфейса.

Заблаговременно необходимо определить список сетевых плат. Для этого нужно выполнить команду ifconfig.

Данная команда сформирует на экране список сетевых карт, имеющихся в системе [13].

Определять физические интерфейсы eth0 и eth1 и присваивать им IP адреса не нужно, так как в этом нет необходимости. IP адреса нужны только VLAN интерфейсам, потому что вся маршрутизация проходит на них.

Перед тем как выполнять настройку vlan, для повышения стабильности установим последний драйвер для карты INTEL. Драйвера следует скомпилировать по исходникам. Для этого используется компилятор C++.

Выполним автоматическую компиляцию с помощью команды:

rpmbuild -tb e1000e-1.10.6.tar.gz.

Данная команда распаковывает архив, компилирует драйвер, создает установочные пакеты e1000e-1.10.6-1.x86_64.rpm удобные для установки. Для того, что бы установить драйвера из распакованного установочного пакета, выполняем команду:

rpm -Uvh e1000e-1.10.6-1.x86_64.rpm.

После этого можно приступать к настройке VLAN.

2. Создание VLAN.

Работа VLAN требует от операционной системы его поддержки. Для этого необходимо загрузить модуль 8021q непосредственно в ядро следующей командой:

modprobe 8021q.

По завершении настройки Linux для каждого отдельно VLANa будет сформировано отдельное устройство. Необходимо определить формат обозначения устройств из четырех возможных вариантов. Формат выбирается по средствам следующей команды:

vconfig set_name_type [name-type]

где, name-type принимает следующие значения:

VLAN_PLUS_VID имя устройства выглядит так: vlan0002.

VLAN_PLUS_VID_NO_PAD имя устройства выглядит так: vlan2.

DEV_PLUS_VID имя устройства выглядит так: eth0.0002.

DEV_PLUS_VID_NO_PAD имя устройства выглядит так: eth0.2

Для того, что бы исключить случаи несовместимости, выбираем второй вариант:

vconfig set_name_type VLAN_PLUS_VID_NO_PAD.

Теперь необходимо вновь вернуться к настройке ОС.

Определим VLAN'ы, используемые на данном интерфейсе. Каждый VLAN добавим на необходимый интерфейс.

Создаем сабинтерфейсы провайдеров: vlan100 и vlan101:

vconfig add eth0 100,

vconfig add eth0 101.

Для того, что бы интерфейсы были сохранены после перезагрузки, создаём два конфигурационных файла в папке /etc/sysconfig/network-scripts. Имена файлов ifcfg-vlan100 и ifcfg-vlan101 со следующим текстом:

VLAN=yes

VLAN_NAME_TYPE=VLAN_PLUS_VID_NO_PAD

PHYSDEV=eth0

NAME="vlan100" (“vlan101”)

BOOTPROTO=none

DEVICE=vlan100 (“vlan101”)

IPADDR=112.152.65.165 (312.122.63.5)

NETMASK=235.235.235.250 (235.235.235.0)

GATEWAY=213.153.63.131 (222.132.63.3)

IPV6INIT=no

USERCTL=no

ONBOOT=yes.

Необходимые параметры:

VLAN=yes - в противном случае интерфейс не будет сформирован после перезагрузки системы.

Последние параметры отвечают за имя сабинтерфейса vlan и ассоциацию с физическими интерфейсами eth0:

VLAN_NAME_TYPE=VLAN_PLUS_VID_NO_PAD

PHYSDEV=eth0.

Создание VLAN интерфейсов требует создания аналогичных файлов конфигурации на интерфейсах eth1 с собственными настройками.

3. DHCP и DNS серверы.

Служба DHCP решает проблемы, которые связаны с окружением сетей, проблемы с назначениями IP адресов [12].Серверы DHCP гарантируют уникальность всех IP адресов. Сервису необходимо вмешательство пользователя для того, что бы назначить и обслужить IP адреса. Администраторы имеют возможности по написанию файлов конфигурации и перепоручения оставшихся заданий серверу DHCP. Этот сервер контролирует пулы IP адресов и освобождает администратора от данной задачи.

Вышеописанный процесс выстраивается из четырех шагов: запрос клиентом DHCP IP-адресов; предложение DHCP-сервером адреса; принятие клиентом предложения и запрос адресов; официальное назначение адреса сервером. Для того, что бы исключить простои сервера, сервер DHCP определяет его на определенный срок. Данная процедура - арендный договор (lease). Когда истекает половина срока арендного договора, клиент DHCP повторно запрашивает его возобновление, в свою очередь, сервер DHCP определяет следующий арендный договор. Это значит, что когда компьютер не использует назначенный IP-адрес, арендный договор завершается, а адрес переходит в пул с целью повторного использования.

В выпускной квалификационной работе будет использован DHCP сервер, потому что последний способен поддерживать неограниченное число выделяемых пулов. Это незаменимо при использовании DHCP сервера с целью раздачи адресов в VLAN. Настроечным файлом выступает файл /etc/dhcpd.conf. Выделяемые пулы формируются блоками для каждого сабинтерфейса отдельно.

DNS - (DomainNameSystem) - это доменная система, которая преобразовывает доменные имена в IP-адреса или наоборот. DNS-сервер - сервер, обслуживающий запросы клиентов. Этот сервер при обращении кеширует процессы преобразования имени узла в IP, а при следующих обращениях пользуется преобразованиями из КЭШа. Данная процедура в значительной степени ускоряет запрос. Величина скорости разрешения DNS-имени возрастает до 30 раз.

Выводы по разделу четыре:

Результат данного этапа работы - этапа проектирования - схема рабочих помещений с расположением оборудования. Точка отсчёта системы - серверная комната. Максимальная длина одного сегмента сети не превышает 90 метров. Каждое рабочее помещение имеет сетевые розетки.

Следующий этап - настройка оборудования. На выбранном коммутаторе сформированы VLAN с привязкой к порту из расчёта один VLAN - на один порт - на одно помещение. Каналы от провайдеров заводятся в гигабитные порты коммутатора. Каждый порт добавляется в VLAN провайдера, передача данных на маршрутизатор осуществляется через тегированные порты.

Завершающий этап - установка и настройка ОС, выполненная в серверном варианте. При этом использовался необходимый минимум программ. С целью повышения удобства администрирования сети установлены и настроены DHCP и DNS серверы.

5 ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРОЕКТИРУЕМОЙ СЕТИ

5.1 Разработка комплекса программно-аппаратных мер по обеспечению защиты информации компьютерной сети

Систему информационной безопасности проектируемой беспроводной ЛВС предполагается реализовать на базе нескольких подсистем. Данные подсистемы подробно рассмотрены ниже.

5.1.1 Подсистема защиты от несанкционированного доступа в сеть

Подсистему защиты от НСД в компьютерную сеть предполагается реализовать с помощью средств управления съемными носителями (СУСН), а так же средствами обеспечения усиленной аутентификации.

Выбор СУСН основывается на анализе производителей и их продуктов, удовлетворяющих требованиям к системе защиты. Вышеуказанные программные продукты указаны в таблице 5.1.

Таблица 5.1 - Анализируемые СУСН

Наименование средства защиты информации	Сертиф. ФСТЭК	Сертиф. ФСБ	Другие	Примечание
Security Studio (Информзащита).	1	0	0	4 НДВ 4, 5 СВТ.
Device Lock (Смарт Лайн Инк).	1	0	0	4 НДВ, ЗБ.
Lumension Device Control (Lumension).	0	0	0	
McAfee Device Control (McAfee).	0	0	0	
Cisco Security Agent (Cisco Systems).	1	0	1	ТУ, EAL2.
Symantec Endpoint Protection 11.0 (Symantec Corporation).	1	0	1	ТУ, 4 НВД.

Проведем анализ функциональных и системных возможностей продуктов, которые связаны с управлением, мониторингом, характеристик, связанных с доверием, стоимостью продуктов. Факторный анализ продуктов приведен в приложении Б.

В процессе сравнения стоимости СЗИ используются данные, которые указаны в таблице 5.2.

Таблица 5.2 - Стоимость средств управления съемными носителями

Информация для сравнения	Security Studio	Device Lock	Lumention Device Control	McAfee Device Conrol	Cisco Security Agent	Symantec endpoint Protection
Стоимость для 50 АРМ, рублей.	12740,00	7070,0	16920,00	5632,00	33498,00	8615,18
Стоимость сертификации, рублей.	0,00	4747,0	30000,00	160000,00	160000,00	1600,00

Результат сравнения представлен на рисунке 5.1.

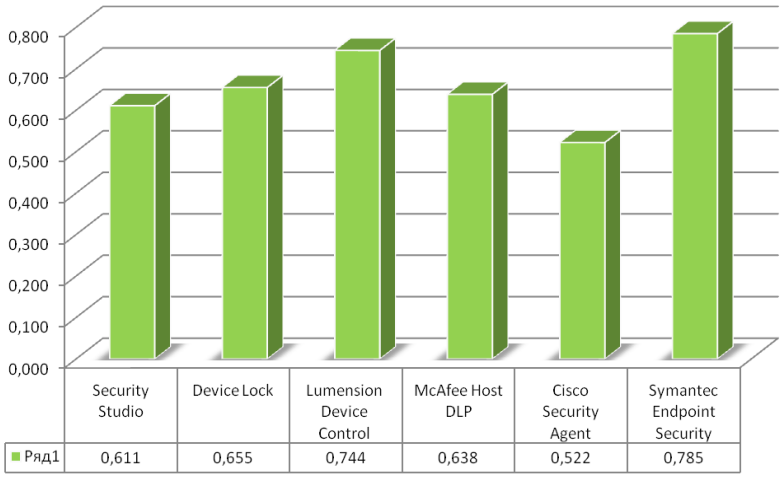


Рисунок 5.1 - Сравнение рейтингов СУСН

По результатам анализа выбрано программное обеспечение Symantec Endpoint Protection. Компания-производитель Symantec. Это комплексное

средство, которое реализует несколько функций и имеет максимальные показатели эффективности.

5.1.2 Средства антивирусной защиты

В качестве САВЗ информационной системы будут использоваться средства Symantec Endpoint Protection. Производство данного программного обеспечения ведет компания Symantec. Данное средство защиты является комплексным средством реализации функции нескольких подсистем, а так же имеет высокий показатель эффективности.

5.1.3 Программно-аппаратные средства межсетевого экранирования

Одними из наиболее оптимальных программно-аппаратных средств межсетевого экранирования являются следующие:

- Cisco ASA5510-K8;
- Cisco ASA5540-K8;
- Cisco ASA5580-20-BUN-K8.

Cisco ASA 5500 Series обеспечивает наиболее качественный класс защиты сетей, отличается хорошим показателем надежности и высокой функциональности. Выбор модели определяется активной нагрузкой на межсетевой экран, необходимым количеством сетевых интерфейсов, возможностью встраивания модулей обнаружения вторжений, а так же других уникальных возможностей модели.

Программно-аппаратные экраны дополняются ПМЭ, которые применяются в процессе взаимодействия рабочих машин пользователей информационной системы со смежными системами в локальных вычислительных сетях.

В процессе выбора ПМЭ рассматриваются производители, которые удовлетворяют требованиям к системам защиты, указанные в таблице 5.3.

Был проведен сравнительный анализ основных возможностей продуктов, а так же возможностей, которые связаны с управлением и мониторингом.

Факторный анализ продуктов приведен в приложении А.

Таблица 5.3 - Анализируемые средства ПМЭ

Наименование средства защиты информации	Сертиф. ФСТЭК	Сертиф. ФСБ	Другие	Примечание
СЗИ, основанные на встроенных механизмах защиты,существующих ОС семейства Windows (Microsoft).	1	0	0	По ЗБ.
McAfee Total Protection for Endpoint (McAfee).	0	0	0	
Symantec Endpoint Protection (Symantec Corporation).	1	0	0	ТУ, НДВ4.
Cisco Security Agent (Cisco Systems).	0,5	0	1	ТУ, EAL2.

Произведено сравнение стоимости ПМЭ. Результаты сравнения представлены в таблице 5.4.

Результаты сравнения средств ПМЭ приведены на рисунке 5.2.

В качестве ПМЭ используется продукт Symantec Endpoint Protection. Фирма-производитель - Symantec. Данный программный продукт является комплексным средством защиты информации, которое реализует функции нескольких подсистем и имеет высокие показатели эффективности.

Таблица 5.4 - Стоимость средств ПМЭ

Информация для сравнения	Windows Firewall	McAfee Total Protection for Endpoint	Symantec Endpoint Protection	Cisco Security Agent
Стоимость решения для защиты 20 пользователей, руб.	0,00	2 473 600,0	1 356 644,5	3 380 000,0
Стоимость сертификации, рублей.	3 125 670,0	1 600 000,0	0,00	1 600 000,0

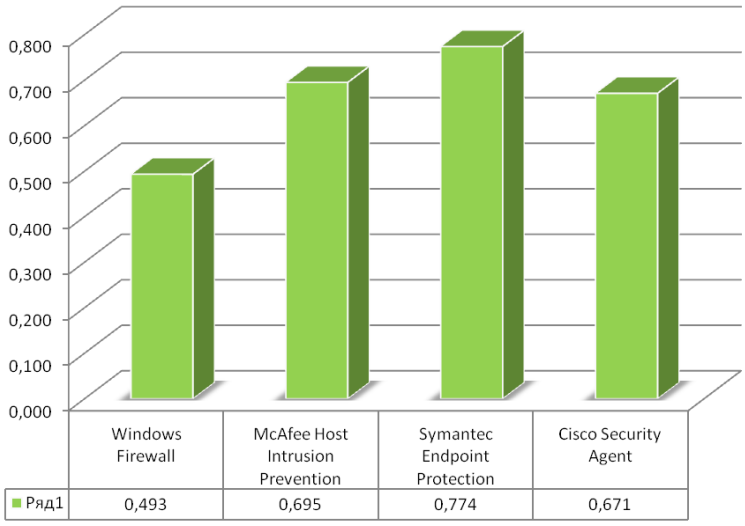


Рисунок 5.2 - Сравнение средств ПМЭ

5.1.4 Средства криптографической защиты

Выбор средств криптографической защиты основывался на анализе производителей и продуктов, которые удовлетворяют требованиям к системе защиты, указанных в таблице 5.5.

Проведено сравнение функциональных и системных возможностей программных продуктов, возможностей, которые связаны с управлением, характеристик, связанных с качеством и стоимостью продуктов.

Таблица 5.5 - Анализируемые средства криптографической защиты

Наименование средства защиты информации	Сертиф. ФСТЭК	Сертиф. ФСБ	Другие	Примечание (сертификация)
Континент (Информзащита).	1	1		КС1, КС2, МЭ2.
Check Point VPN-1 (Check Point).	1			КС1, КС2, МЭ3.
S-Terra CSP VPN Gate (С-Терра СиЭсПи)	1			КС1, КС2, соответствие ЗБ.
StoneGate VPN (StoneSoft).	1			КС1, КС2, МЭ3.

Сравнение стоимости средств защиты приведено в таблице 5.6.

Таблица 5.6 - Стоимость средств криптографической защиты

Информация для сравнения	Континент	Check Point VPN-1	S-Terra CSP VPN Gate	StoneGate VPN
Стоимость 2-х VPN шлюзов с пропускной способностью не меньше 100 Мбит/с, руб.	269 000,00	998 088,00	1 037 800	1 156 320,00
Поддержка на год, рублей.	80 700,00	179 655,84	43 680,00	196 627,20

Факторный анализ продуктов приведен в приложении Д.

Результат сравнения средств криптографической защиты представлен на рисунке 5.3.

Средством построения VPN используется продукт S-Terra CSP VPN. Производство данного программного продукта осуществляет компания «С-Терра СиЭсПи». На компьютерах пользователей информационной системы применяются клиентские части продукта CSP VPN Client.

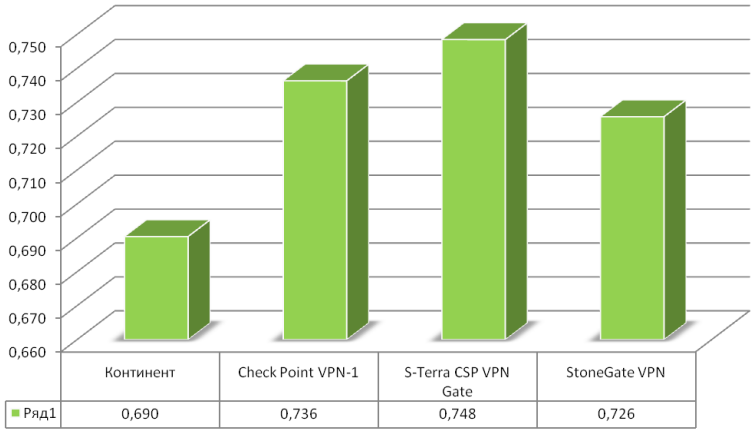


Рисунок 5.3 - Сравнение средств криптографической защиты

5.1.5 Средства обнаружения вторжений

Выбор средств обнаружения вторжений должен удовлетворять требованиям, указанным в таблице 5.7

Таблица 5.7 - Средства обнаружения вторжений

Наименование средства защиты информации	Сертиф. ФСТЭК	Сертиф. ФСБ	Другие	Примечание
Stonegate IPS (Stonesoft).	1	0	0	ТУ, НДВ 4.
IBM ISS Proventia (IBM).	1	0	0	ТУ.
Аргус	0	1	0	Соответствует классу Г

После проведения сравнения функциональных и системных возможностей продуктов, а так же возможностей, которые связаны с управлением, доверием и стоимостью средств обнаружения вторжений получены необходимые результаты.

Результаты сравнения стоимости средств защиты представлены в таблице 5.8

Таблица 5.8 - Стоимость средств обнаружения вторжений

Информация для сравнения	Stonegate IPS	IBM ISS Proventia (IBM)	Аргус
Стоимость СОВ с 4-мя сетевыми интерфейсами	261 144,00	515 678,80	255 000,00
Стоимость сертификации.	90 000,00	28 362,33	0,00

Результат сравнения средств обнаружения вторжений представлен на рисунке 5.4.

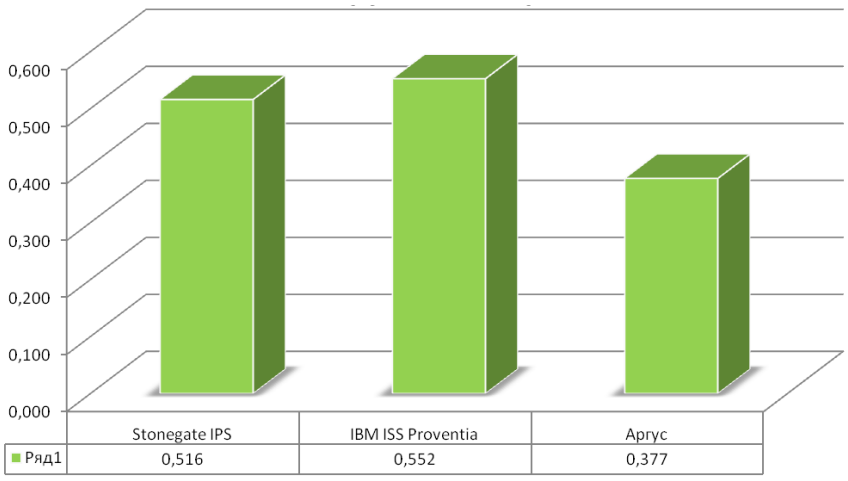


Рисунок 5.4 - Сравнение средств обнаружения вторжений

Средством обнаружения вторжения принят продукт семейства IBM Proventia IPS. Производством данного программного занимается компания IBM. Данное средство обладает максимальными показателями. Следует отметить, что необходима сертификация СЗИ.

5.1.6 Средства анализа защищенности

Сравнение средств анализа защищенности приведено в таблице 5.9.

В процессе выбора средств анализа защищенности анализировались производители и их продукты, которые удовлетворяют требованиям к системе защиты.

Таблица 5.9 - Стоимость средств анализа защищенности

Информация для сравнения	XSpider	IBM Internet Scanner	MaxPatrol
Стоимость сертифицированного варианта САЗ на 200 АРМ или 20 сущностей СУБД.	1 036 800,00	1 764 334,00	4 600 000,00
Стоимость обновления средства анализа защищенности (в год), рублей.	97 128,00	352 866,80	1 840 000,00

Результаты сравнения средств анализа защищенности представлены на рисунке 5.5

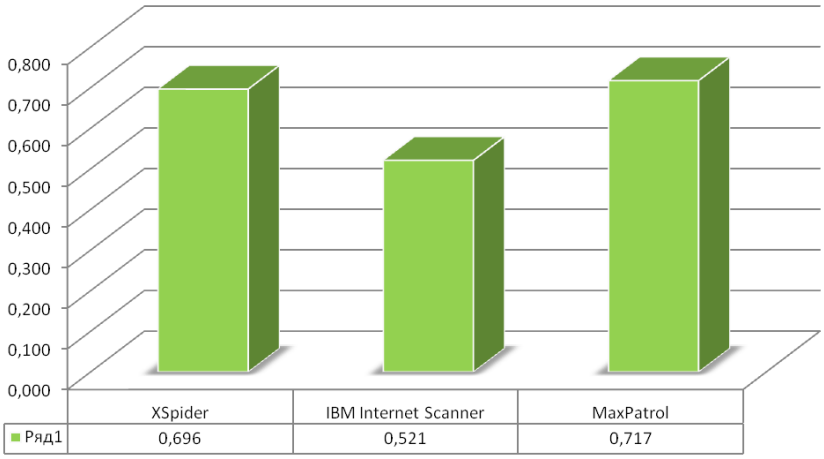


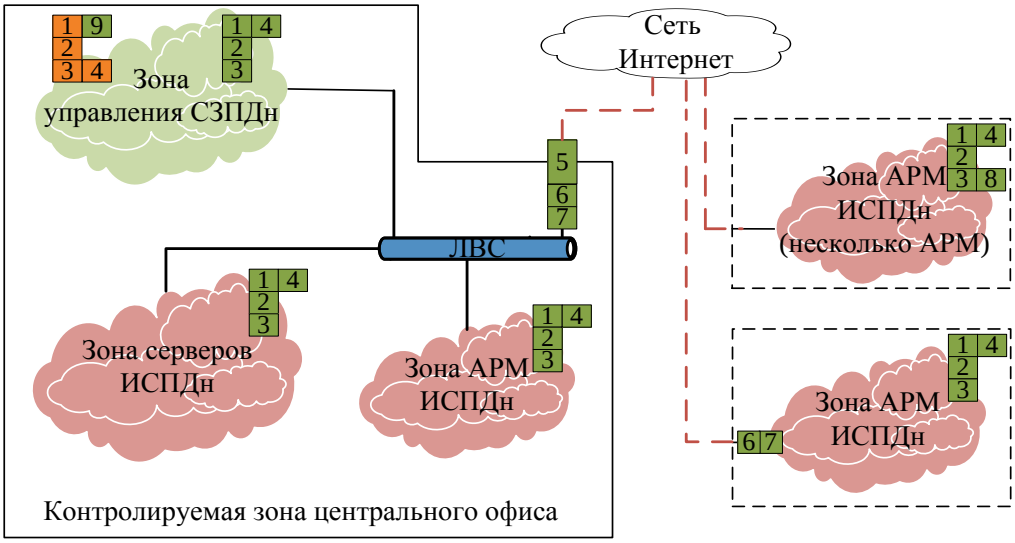
Рисунок 5.5 - Сравнение рейтингов средств анализа защищенности

Факторный анализ средств обнаружения вторжений представлен в приложении В.

Средство анализа защищенности представлено продуктом MaxPatrol. Производством данного продукта занимается компания Positive Technologies. Данное средство обладает высокими показателями качества.

5.2 Общая структура системы информационной безопасности компьютерной сети

Структура системы защиты информации ЛВС ООО «Инструментстрой» представлена на рисунке 5.6.



№	Компонент СЗПДн
1.	Средство защиты от НСД «eToken»
2.	СУСН «McAfee Device Control»
3.	САВЗ «McAfee Total Protection for Endpoint»
4.	ПМЭ «McAfee Total Protection for Endpoint»
5.	МЭ Cisco ASA
6.	Proventia IPS
7.	CSP VPN Gate
8.	CSP VPN Client
9.	Сканер MaxPatrol

Компоненты связанные с управлением СЗПДн

№	Компонент СЗПДн
1.	Сервер управления «McAfee ePolicy Orcestrator»
2.	Консоль управления «McAfee ePolicy Orcestrator»
3.	eToken TMS 2
4.	Сервер MaxPatrol

Рисунок 5.6 - Структура разрабатываемой системы защиты информации беспроводной сети

Программное обеспечение «Symantec Endpoint Protection» сформировано из нижеприведенных компонентов:

- «Symantec Endpoint Protection Client» - САВЗ, СУСН, ПМЭ;
- «Symantec Endpoint Protection Manage» - сервера управления;
- «Symantec Endpoint Protection Manager Console».

Система антивирусной защиты «Symantec Endpoint Protection Client» обеспечивает защиту персональных компьютеров пользователей от вредоносных программ и защиту серверов на базе операционной системы Microsoft Windows.

СУСН «Symantec Endpoint Protection Client» управляет подключениями периферийных устройств, а так режимами их функционирования.

ПМЭ «Symantec Endpoint Protection Client» является собой персональным межсетевым экраном, который обеспечивает персональную защиту компьютеров и серверов на базе операционной системы Microsoft Windows.

Для осуществления качественного межсетевого экранирования следует разделить все узлы информационной системы и системы защиты на защищенные зоны, обеспечивающиеся организацией виртуальных сетей. Запрещение взаимодействия между узлами защищенных зон в обход средств МСЭ Cisco ASA 5500 Series. Cisco ASA 5500 Series выполняются:

- маршрутизацией сетевого трафика защищаемых зон;
- фильтрацией трафика между защищаемыми зонами на базе параметров протоколов 3 и 4 уровня сетевой модели OSI;
- регистрацией и учетом фильтруемых пакетов данных.

Система криптографической защиты, в состав которой входят программные продукты «S-terra CSP VPN Gate» и «CSP VPN Client», обеспечивает шифрование защищаемых данных при их передаче по неконтролируемому каналу связи, а так же управление криптографическими ключами.

Средство обнаружения вторжений представлено программным продуктом «IBM Proventia Prevention Appliance», который дает возможность обнаружения трафика сетевой атаки, которая запрещена политикой безопасности, автоматически реагировать на обнаруженное вторжение.

САЗ «MaxPatrol» дает возможность выявлять уязвимости программного обеспечения информационной системы и системы защиты, тестирования эффективности системы защиты информации.

5.3 Внедрение предлагаемых средств защиты компьютерной сети

Рассмотрим вопрос о внедрении и размещении каждого из компонентов системы защиты компьютерной сети.

Защита от НСД в сеть реализована на следующих компонентах:

- драйверы Symantec Client;
- программное обеспечение Endpoint Protection;
- USB-ключ;

Размещение компонентов защиты от НСД представлено в таблице 5.10.

Таблица 5.10 - Размещение компонент подсистемы защиты от НСД

Компонент	Расположение
Драйверы Symantec Client	Программное обеспечение на серверах и АРМ ЛВС.
USB-ключи	Пользователи ЛВС
Программное обеспечение Endpoint Protection	Программное обеспечение на серверах и АРМ ЛВС

Компоненты подсистемы защиты от НСД работают в режимах, которые указаны в таблице 5.11.

Таблица 5.11 - Режимы функционирования компонент средств защиты от НСД

Компонент	Режим функционирования
Набор драйверов Symantec Client	В рабочие часы пользователей.
ПО Endpoint Protection	В рабочие часы пользователей.
USB-ключи	В рабочие часы пользователей.
Центр Сертификации «КриптоПро УЦ».	Круглосуточно и ежедневно.
Центр Регистрации «КриптоПро УЦ».	Круглосуточно и ежедневно.
АРМ администратора Центра Регистрации.	В рабочие часы администраторов.
АРМ разбора конфликтных ситуаций.	В рабочие часы администраторов.

Средство защиты от несанкционированного доступа производства компании Symantec обеспечивают:

- сохранение хранимых ключей в памяти аппаратного идентификатора;
- идентификацию и двухфакторную аутентификацию пользователя ЛВС в процессе входа/выхода в ОС или приложения;
- принудительное выключение пользователя в том случае, если отсоединен аппаратный идентификатор пользователя.

Решение защиты узлов «Symantec Endpoint Protection» производства фирмы Symantec является средством антивирусной защиты, средством межсетевого экранирования и средством управления носителями.

«Symantec Endpoint Protection» имеет возможность обеспечивать комплексную защиту от вредоносных программ на базе технологий Symantec Antivirus с полной защищенностью в масштабе реального времени и автоматически локализоваться выявленные угрозы.

Решение «Symantec Endpoint Protection» объединяет в себе следующие составляющие:

- средство антивирусной защиты, средства управления носителями, средства межсетевого экранирования «Symantec Endpoint Protection Client»;
- сервер «Symantec Endpoint Protection Manage» и консоль управления;

Размещение системы «Symantec Endpoint Protection» обозначено в таблице 5.12. Взаимодействие между компонентами «Symantec Endpoint Protection» приведено на рисунке 5.8.

Таблица 5.12 - Размещение компонент «Symantec Endpoint Protection»

Компонент	Расположение
«Symantec Endpoint Protection Client».	В виде ПО на АРМ пользователей ЛВС.
«Symantec Endpoint Protection Manage».	В виде ПО на создаваемом сервере, который размещается в зоне управления СЗ
«Symantec Endpoint Protection Manager Console».	В виде ПО на существующем АРМ администратора САВЗ.

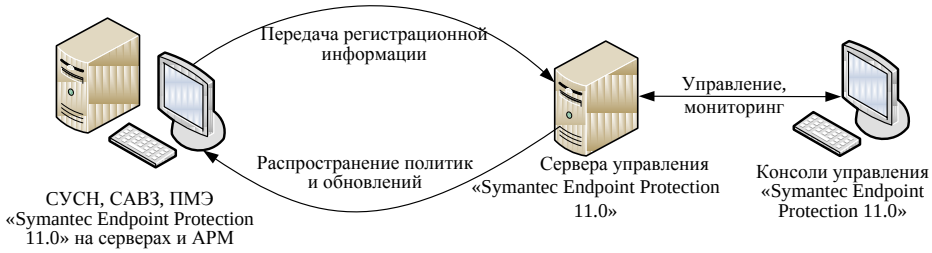


Рисунок 5.8 - Принцип функционирования и размещения компонентов «Symantec Endpoint Protection»

Составляющие системы «Symantec Endpoint Protection» работают в соответствии с режимами, которые приведены в таблице 5.13.

Таблица 5.13 - Режимы функционирования средств «Symantec Endpoint Protection»

Компонент	Режим функционирования
СУСН «Symantec Endpoint Protection Client».	В рабочие часы пользователей.
САВЗ «Symantec Endpoint Protection Client».	В рабочие часы пользователей.
ПМЭ «Symantec Endpoint Protection Client».	В рабочие часы пользователей.
Сервер «Symantec Endpoint Protection Manage».	Круглосуточно и ежедневно.
Консоль управления «Symantec Endpoint Protection Manager Console».	В рабочие часы администраторов.

Программное обеспечение антивирусной защиты «Symantec Endpoint Protection Client» дают возможность:

- автоматической проверки определения присутствия вредоносных программ по определенным шаблонам;
- автоматической проверки определения других вирусов с помощью специального алгоритма анализа;
- автоматической блокировки обнаруженных вирусов и возможность удаления вредоносной программой;
- выполнять проверку по расписанию;

- выполнять антивирусную проверку файлов непосредственно в момент запуска;

- контролировать выполнение макросов в документах Microsoft Office и блокировать опасные макрокоманды;

- антивирусной проверки исполняемых скриптов;

- исключить из списка проверки «чистых» приложений.

- получать информацию о состоянии программ, используя при этом разные варианты отчета с разными уровнями детализации.

- периодического обновления шаблона вредоносных программ;

- регистрации событий в процессе обнаружения, блокирования, удаления вируса.

«Symantec Endpoint Protection Client» дает возможность управления подключением периферийных устройств и режимами их работы.

ПМЭ «Symantec Endpoint Protection Client» является персональным межсетевым экраном, который обеспечивает защиту ЭВМ и сервера.

Средства межсетевого экранирования выполняются в виде межсетевых экранов (МСЭ) Cisco ASA 5500 Series и ПМЭ «Symantec Endpoint Protection». Помимо этого, в защите межсетевых взаимодействий участвуют существующие в организации средства сети, обеспечивающие виртуальные локальные сети с фильтрацией трафика, который проходит между VLAN, сертифицированными межсетевыми экранами.

Взаимодействие защищаемых зон информационной системы имеет место исключительно при наличии средств МСЭ. Взаимодействие реализуется путём:

- ПМЭ (Symantec Endpoint Protection);

МСЭ Cisco 5500 Series. На рисунке 5.9 обозначен принцип размещения компонентов межсетевого экранирования.

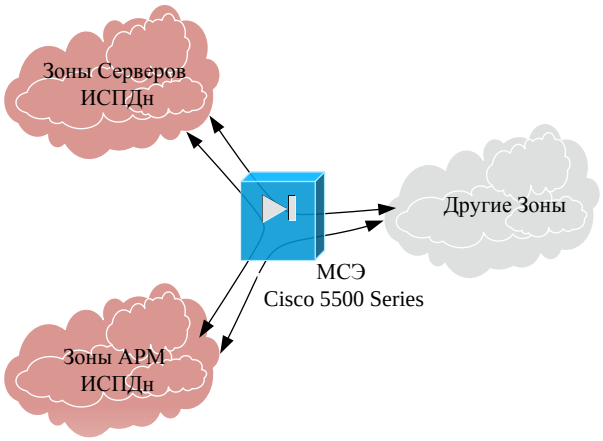


Рисунок 5.9 - Принцип размещения межсетевого экранирования

Составляющие подсистемы МСЭ функционируют в режимах, которые приведены в таблице 5.14.

Таблица 5.14 - Режимы функционирования средств межсетевого экранирования

Компонент	Режим функционирования
МСЭ «Cisco ASA 5500 Series».	Круглосуточно и ежедневно.
Консоль управлений.	В рабочие часы администраторов безопасности.

Подсистема обеспечения защиты межсетевых взаимодействий дает возможность:

- раздела всех узлов баз данных на зоны, обеспеченные организацией локальных сетей;
- запрещать взаимодействия узлов защищаемых зон в обход средств МСЭ;
- маршрутизации сетевого трафика защищаемых зон;
- фильтрации сетевого трафика между защищенными зонами, за основу которых взят параметр протоколов 3 и 4 уровней сетевой модели OSI;
- регистрации и учета фильтруемых пакетов данных.
- параметры регистрации включают адрес, время, результат процесса фильтрации;
- регистрации запусков внутренних программ;
- регистрации входа и выхода администратора МСЭ в систему или из

системы, или загрузки системы и ее программной остановки.

Состав средств криптографической защиты следующий:

- криптошлюз «S-terra CSP VPN Gate»;

- S-terra VPN клиент «CSP VPN Client».

Размещение составляющих подсистемы приведено в таблице 5.15.

Таблица 5.15 - Размещение средств криптографической защиты

Компонент	Расположение
Криптошлюз «S-terra CSP VPN Gate».	В виде ПАК, который размещается на границе зоны серверов ЛВС.
S-terra VPN клиент «CSP VPN Client».	В виде ПО установленного на АРМ удаленного пользователя ЛВС.

Взаимодействие между компонентами подсистемы приведено на рисунке 5.10.

Составляющие подсистемы криптографической защиты работают в режимах, которые приведены в таблице 5.16

Таблица 5.16 - Режимы функционирования средств криптографической защиты

Компонент	Режим функционирования
Криптошлюз «S-terra CSP VPN Gate».	Круглосуточно и ежедневно.
S-terra VPN клиент «CSP VPN Client».	В рабочие часы пользователей.

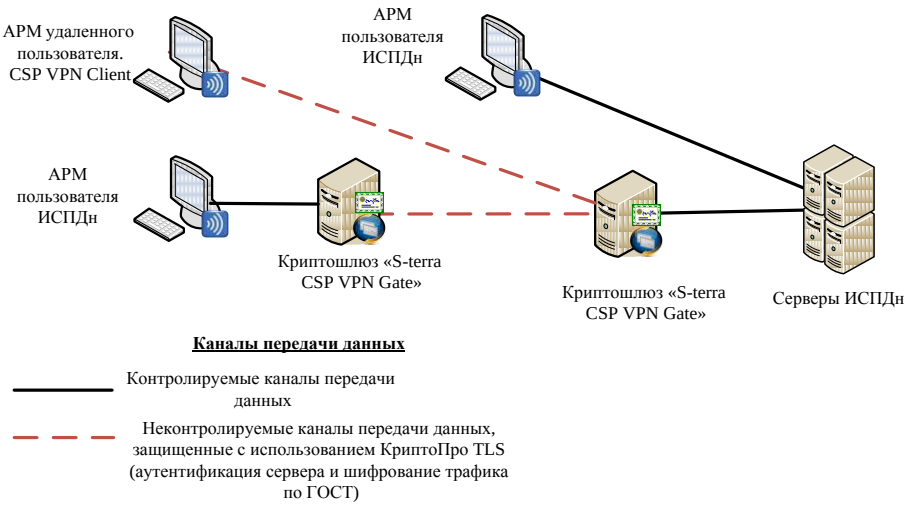


Рисунок 5.10 - Принцип размещения компонентов криптографической защиты

Подсистема криптографической защиты дает возможность:

- шифрования защищаемых данных в момент их передачи по неконтролируемому каналу связи;
- зашифровки команды управления при её передаче по неконтролируемому каналу связи;
- управления криптографическим ключом;
- изготовления списка отозванных сертификатов ключа подписи;
- регистрации событий, связанных с безопасностью информационной системы.

Средства обнаружения вторжений приведены программно-аппаратным продуктом IBM - «Proventia Intrusion Prevention Appliance».

Размещение составляющих данной системы приведено в таблице 5.17.

Таблица 5.17 - Размещение компонент средств обнаружения вторжений

Компонент	Расположение
«IBM Proventia Prevention Appliance».	Программно-аппаратное средство, которое размещается в зоне подключения к сети Интернет.
Консоль управления.	В рабочие часы администратора безопасности.

Средства обнаружения вторжений «IBM Proventia IPS» дают возможность:

- обнаружения трафика известных сетевых атак из потока информации;
- обнаружения запрещенных политикой безопасности сетевых атак;
- автоматически реагировать на обнаруженное вторжение;
- периодически обновлять обнаруживаемые сигнатуры атак;
- регистрации событий, которые связаны с безопасностью информационной системы.

Средствами анализа защищенности выступает компонент производства компании «MaxPatrol».

Размещение компонентов подсистемы представлено в таблице 5.18.

Таблица 5.18 - Размещение компонент подсистемы обнаружения вторжений

Компонент	Расположение
MaxPatrol Server Audit.	В виде ПО на создаваемом АРМ аудитора ИБ, который может подключаться во все зоны.

Взаимодействие средств анализа защищённости с компонентами информационной системы представлено на рисунке 5.11.

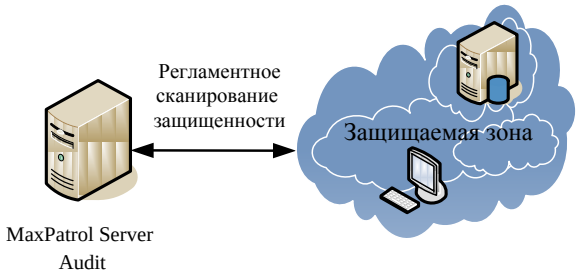


Рисунок 5.11 - Принцип функционирования и размещения компонентов подсистемы анализа защищенности

Обобщим полученные результаты.

Нейтрализация и снижение вероятности появления тех или иных осуществляется по средствам использования комплекса мер защиты: организационно-технических, инженерно-технических и программно-аппаратных.

Система защиты состоит из подсистем:

- защиты от НСД;
- антивирусной защиты;
- межсетевого экранирования;
- криптографической защиты;
- обнаружения вторжений;
- анализа защищенности;
- подсистемы контроля и управления доступом.

Факторный анализ показал, что наилучшими характеристиками обладают следующие средства защиты информации:

- программное обеспечение Symantec Endpoint Protection;
- программное обеспечение eToken Network Logon, которое используется совместно с eToken PRO (Java)/72K/CERT-1883;
- Cisco ASA 5500 Series;
- S-Terra CSP VPN;
- IBM Proventia IPS;
- MaxPatrol.

Вышеуказанные средства защиты обладают необходимыми сертификатами ФСБ и ФСТЭК России, образуют систему защиты конфиденциальной информации, которая обеспечивает соблюдение требований законодательства.

Выводы по разделу пять:

Систему информационной безопасности проектируемой беспроводной ЛВС реализовали на базе нескольких подсистем.

Были рассмотрены и тщательно проанализированы различные продукты САВЗ, ПМЭ, НСД, СУСН и выбраны оптимальные по надёжности/цене.

6 ТЕХНИКО-ЭКОНОМИЧЕСКИЙ РАЗДЕЛ

6.1 Составление календарного плана выполнения работ

Календарный план обеспечивает возможность контроля над ходом выполнения работ и его регулирования на всех этапах работ.

План выполнения работ по данному проекту составлен в виде таблицы (таблица 6.1).

По итогам таблицы 6.1 дата окончания выполнения проекта 17 мая 2016 года. Календарный план не учитывает выходные и праздничные дни в году. Поэтому следует предположить, что продолжительность разработки проекта увеличится.

Таблица 6.1 - Календарный план разработки и реализации проекта

Наименование этапов	Период выполнения		Продолжитель-ность этапов, дн
	дата начала	дата окончания	
1. Подготовительный этап	16.04.2016	03.05.2016	14
2. Этап проектирования	04.04.2016	07.05.2016	5
3. Основной этап проведения работ	09.04.2016	12.05.2016	4
4. Заключительный этап	13.04.2016	17.05.2016	5
Итого			28

6.2 Определение сметной стоимости проекта

Целью планирования сметной стоимости работ является экономически обоснованное определение величины затрат на выполнение проекта.

6.2.1 Расчет расходов на оплату труда

Расчет расходов на оплату труда включает расчет по тарифу и расчет дополнительных расходов.

В расчете расходов на оплату труда по тарифу учитываются выплаты по заработной плате за выполненную работу, рассчитанные на основании тарифных ставок и должностных окладов в соответствии с принятой в организации системе оплаты труда. Данные сведены в таблицу 6.2.

Таблица 6.2 - Расходы на оплату труда по тарифу

Персонал	Общая трудоемкость, $Т_{ОБЩ}$, час	Оклад исполнителя, О, руб./мес.	Часовая тарифная ставка, ЧТС, руб./час	Расходы на оплату труда, $Р_{ОТ}$, руб.
Руководитель проекта	55	50 000,0	284,1	15625,5
Системный администратор	169	30 000,0	170,5	28806,9
Итого				44432,4

Формулы, по которым велся расчёт, приведены ниже:

$$ЧТС_i = О_i / F_{ПЛ, Мес}, \quad (6.1)$$

$$F_{Пл., Мес.} = Д*Ч_{ДН, Мес}, \quad (6.2)$$

где Д - длительность рабочего дня - 8 часов;

$Ч_{Дн., Мес.}$ - количество рабочих дней месяца - 22 дня.

$$Р_{ОТ\ i} = ЧТС_i * Т_{Общ\ i}, \quad (6.3)$$

Данные по $Т_{Общ\ i}$ берутся из таблицы 3.1.

$$Р_{ОТ}^{\text{тариф}} = \sum Р_{ОТ\,i}, \quad (6.4)$$

Данные для расчета дополнительных расходов используются из таблицы 6.3.

Расчет производится исходя из следующих формул:

$$Р_{ОТ}^{1.1} = Р_{ОТ}^{\text{тариф}}, \quad (6.5)$$

$$Р_{ОТ}^{1.2} = 0{,}14 * Р_{ОТ}^{1.1}, \quad (6.6)$$

$$Р_{ОТ}^{1.3} = 0{,}5 * Р_{ОТ}^{1.1}, \quad (6{,}7)$$

$$Р_{ОТ}^{1.4} = 0{,}15 * (Р_{ОТ}^{1.1} + Р_{ОТ}^{1.2} + Р_{ОТ}^{1.3}), \quad (6.8)$$

$$Р_{ОТ}^{1} = Р_{ОТ}^{1.1} + Р_{ОТ}^{1.2} + Р_{ОТ}^{1.3} + Р_{ОТ}^{1.4}, \quad (6.9)$$

Подставив данные из таблицы 6.4, получим:

$Р_{ОТ}^{1.1} = 44432{,}4$ руб.

$Р_{ОТ}^{1.2} = 0{,}14 * 44432{,}4 = 6220{,}6$ руб.

$Р_{ОТ}^{1.3} = 0{,}5 * 44432{,}4 = 22216{,}2$ руб.

$Р_{ОТ}^{1.4} = 0{,}15 * (44432{,}4 + 6220{,}6 + 22216{,}2) = 10930{,}38$ руб.

$Р_{ОТ}^{1} = 44432{,}4 + 6220{,}6 + 22216{,}2 + 10930{,}38 = 83799{,}58$ руб.

Результаты расчетов сведены в таблицу 6.3.

Таблица 6.3 - Дополнительные расходы на оплату труда

Наименование статей расходов	Сумма, руб.
Расходы на оплату труда по тарифу ($Р_{ОТ}^{1.1}$)	44432,4000
Резервирование средств на оплату отпусков и другие выплаты по законодательству ($Р_{ОТ}^{1.2}$)	6220,6000
Премиальные выплаты ($Р_{ОТ}^{1.3}$)	22216,2000
Зональный коэффициент ($Р_{ОТ}^{1.4}$)	10930,3800
Итого: Расходы на оплату труда ($Р_{ОТ}^{1}$)	83799,5800

6.2.2 Страховые взносы с заработной платы

Эта статья учитывает перечисления организации во внебюджетные государственные фонды, т.е. выплаты по единому социальному налогу (далее - ЕСН).

Данная статья рассчитывается по следующей формуле:

$$ECH = P_{OT}{}^{1} * C_{ECH} / 100, \quad (6.10)$$

где C_{ECH} - ставка ЕСН (30%).

Расчеты:

ЕСН = 83799,5800* 30/ 100 = 25139,874 руб.

6.2.3 Статья «Расходы на материалы»

В данную статью включается стоимость материалов, расходуемых при составлении планов помещений, схем технических коммуникаций, связи, организации охраны, доступа и пр., а так же стоимость материалов, необходимых для оформления документации.

Расчеты затрат на материалы сведены в таблицу 6.4.

Таблица 6.4 - Расходы на материалы

Наименование материала	Количество единиц	Цена за ед., руб.	Сумма, руб.
Бумага формата А4 (500 листов)	1	120	120
Ручка, шт.	6	10	60
Карандаш, шт.	10	8	80

Продолжение таблицы 6.4

Наименование материала	Количество единиц	Цена за ед., руб.	Сумма, руб.
Папка со скоросшивателем, шт.	3	50	150
Дырокол, шт.	1	50	50
Стиплер	1	70	70
Итого			530

6.2.4 Статья «Прочие расходы»

Эта статья предусматривает расходы, не учтенные в других статьях затрат. Расчет расходов определяется по формуле:

$$Р_{ПР}= Р_{ОТ}^{1.1} * К_{ПР}, \quad (6.11)$$

где $К_{ПР}$ - коэффициент прочих расходов (равен 0,2).

Расчеты:

$Р_{Пр} = 0,2 * 44432,4= 8886,48$ руб.

6.2.5 Статья «Административно - хозяйственные расходы»

В этой статье учитываются затраты организации-разработчика на содержание аппарата управления, обслуживающего персонала, содержание зданий и сооружений, текущий ремонт, расходы на отопление и освещение и другие общехозяйственные расходы:

$$P_{A-X} = P_{OT}^{1.1} * K_{A-X}, \quad (6.12)$$

где $К_{А-Х}$ - коэффициент административно - хозяйственных расходов (равен 0,5).

Расчеты: P_{A-X} = 44432,4* 0,5 = 22216,2 руб.

Таблица 6.5 - Смета расходов на разработку проекта

Наименование статей расходов	Сумма, руб.	Удельный вес статей, %
1 Расходы на оплату труда	83799,5800	59,6
2 Единый социальный налог (ЕСН)	25139,874	17,9
3 Расходы на материалы	530,0000	0,3
4 Прочие расходы	8886,4800	6,4
5 Административно - хозяйственные расходы	22216,2000	15,8
Итого:	140572,134	100

6.2.6. Технико-экономические показатели проекта

Ниже на рисунке 6.1 изображена диаграмма, которая отражает технико-экономические показатели проекта.

Рисунок 6.1 - Технико-экономические показатели проекта

Как видно из диаграммы, основные затраты при разработке системы - это затраты на оплату труда.

Выводы по разделу шесть:

В технико-экономическом разделе мы посчитали все планируемые затраты при разработке системы, определили сметную стоимость работы, также составили календарный план выполнения работ. Согласно диаграмме (рисунок 6.1) очевидно, что основные затраты при разработке системы – это затраты на оплату труда.

7 БЕЗОПАСНОСТЬ ЖИЗНЕДЕЯТЕЛЬНОСТИ

7.1 Анализ условий труда системного администратора ЛВС

Изучение и решение проблем, связанных с обеспечением здоровых и безопасных условий, в которых протекает труд человека - одна из наиболее важных задач в разработке новых технологий и систем проектирования. Изучение и выявление возможных причин производственных несчастных случаев, профессиональных заболеваний, аварий, взрывов, пожаров, и разработка мероприятий и требований, направленных на устранение этих причин позволяют создать безопасные и благоприятные условия для труда человека.

Работа системного администратора непосредственно связана компьютером, а соответственно с дополнительным вредным воздействием целой группы факторов, что существенно снижает производительность их труда. К таким факторам можно отнести:

1) воздействие вредных излучений от монитора;

2) неправильная освещенность;

3) не нормированный уровень шума;

4) нарушение микроклимата;

5) наличие напряжения и др.

Проанализируем некоторые факторы, влияющие на условия труда системного администратора сети.

7.1.1 Анализ воздействия ПЭВМ и монитора на сотрудника

Визуальные эргономические параметры монитора являются параметрами безопасности, и их неправильный выбор приводит к ухудшению здоровья пользователя. Все мониторы должны иметь гигиенический сертификат, включающий в том числе оценку визуальных параметров.

Конструкция монитора должна обеспечивать возможность фронтального наблюдения экрана путем поворота корпуса в горизонтальной плоскости вокруг вертикальной оси в пределах плюс-минус 30 градусов и в вертикальной плоскости вокруг горизонтальной оси в пределах плюс-минус 30 градусов с фиксацией в заданном положении.

Для обеспечения надежности считывания информации при соответствующей степени комфортности ее восприятия должны быть определены оптимальные и допустимые диапазоны визуальных эргономических параметров

При проектировании и разработке рабочего места сочетания визуальных эргономических параметров мониторов и их значения, соответствующие оптимальным и допустимым диапазонам, полученные в результате испытаний в специализированных лабораториях, аккредитованных в установленном порядке, и подтвержденные соответствующими протоколами, должны быть внесены в техническую документацию на монитор.

Так же, конструкция монитора и ПЭВМ должна обеспечивать мощность экспозиционной дозы рентгеновского излучения в любой точке на расстоянии 0,05 м от экрана и корпуса монитора при любых положениях регулировочных устройств, которая не должна превышать 7,7·10 А/кг, что соответствует эквивалентной дозе, равной 0,1 мБэр/час (100 мкР/час).

При анализе вредных воздействий от ПЭВМ и мониторов на системного администратора выявлено, что уровень воздействий соответствует требуемым нормам, в организации используются современные мониторы и ПЭВМ, не оказывающие недопустимых вредных воздействий на персонал организации.

7.1.2 Анализ источников шума

Источниками шума на рабочих местах являются сами вычислительные машины (встроенные в стойки ЭВМ вентиляторы, принтеры и т.д.), центральная система вентиляции и кондиционирования воздуха.

В рабочем помещении предприятия уровень шума на рабочих местах не превышает значений, установленных для данных видов работ Санитарными нормами допустимых уровней шума на рабочих местах, и составляет примерно 30 дБА.

В помещении, где работает инженерно-технический персонал, осуществляющий аналитический или измерительный контроль, уровень шума не превышает 60 дБА, что так же соответствует нормативным документам.

На рабочих местах в помещениях, где размещены шумные агрегаты вычислительных машин (факсы, принтеры и т.п.), уровень шума согласно СанПиН 2.2.2/2.4.1340-03 «Гигиенические требования к персональным электронно-вычислительным машинам и организации работы» не должен превышать 75 дБА. После анализа уровня шума в данных помещениях получен уровень в 45 дБА. Данное значение удовлетворяет СанПиН 2.2.2/2.4.1340-03.

Шумящее оборудование, уровни шума которого превышают нормированные, согласно нормативной безе, должно находиться вне помещения, в котором организуются рабочие места. Однако такого рода помещения на предприятии отсутствуют.

7.1.3 Анализ микроклимата помещений

Согласно СанПиН 2.2.2/2.4.1340-03, под метеорологическим условиям производственной среды понимают сочетания температуры, относительной влажности, скорости движения и запыленности воздуха. Температура воздуха является одним из основных параметров, характеризующих тепловое состояние микроклимата. Скорость движения воздуха - это вектор усредненной скорости перемещения воздушных потоков под действием различных побуждающих сил.

Для характеристики содержания влаги в воздухе используют понятия - абсолютная, максимальная и относительная влажность.

Параметры микроклимата на рабочем месте приведены в таблице 7.1.

Таблица 7.1 - Параметры микроклимата на рабочем месте

Категория работ	Энергозатраты, Вт	Периоды года, температура (°С)	
		Холодный	теплый
легкая	до 139	22-24	23-35
средней тяжести	175-232	18-20	21-23
тяжелая	более 290	16-18	18-20

При пониженном давлении воздуха ухудшается отвод тепла от элементов ПЭВМ. Рекомендуется создавать небольшое избыточное атмосферное давление, препятствующее подносу пыли.

Для обеспечения установленных норм в рабочем помещении применяют вентиляцию, что позволяет также обеспечить чистоту воздуха. Система вентиляции выполняется в соответствии с требованиями СНиП 41-01-2003 «Отопление, вентиляция и кондиционирование».

Проведённый анализ системы вентиляция ООО «Инструментстрой» позволяет утверждать, что имеющаяся вентиляция соответствует СНиП 41-01-2003.

7.2 Пожарная безопасность

Пожары на территории предприятия представляют особую опасность, так как сопряжены с большими материальными потерями и угрозами жизни персоналу.

Характерная особенность рассматриваемого предприятия относительно пожаробезопасности - небольшая площадь помещений.

Определим категорию помещений ООО «Инструментстрой» по НПБ 105-03.

Помещение размещается на первом этаже здания. Помещение имеет следующие характеристики:

-площадь помещения - 324 м^2;

-высота помещения до нижнего пояса ферм - 3,02 м;

Так как в помещении отсутствуют горючие газы, легковоспламеняющиеся и горючие жидкости, а также нет источников появления горючей пыли, то данное помещение не будет относиться к категории А или Б.

В помещении пожарная нагрузка представлена в виде бумажной продукции, пластика, деревянной мебели. Помещение предприятия включает двенадцать комнат. План помещений предприятия представлен на рисунке 1.1.

Рассмотрим следующий расчетный случай: в двух рядом стоящих шкафах хранится бумажная документация с высотой складирования 40 см на каждом из 3-х уровней. Шкаф имеет основание 1,91 х 1,56 м; Площадь складирования для 2-х шкафов составляет менее 10 м^2, по этому в соответствие с примечанием в НПБ 105-03 п.25 расчетную площадь принимаем равной 10 м^2.

На шкафах пожарная нагрузка представлена плитами ДСП (оделены уровни стеллажей), и бумажной документацией.

Определим объем плит ДСП:

$V = 1{,}91 \cdot 1{,}56 \cdot 0{,}02 \cdot 3 \cdot 2 = 0{,}35$ м^3

Определим массу, пожарной нагрузки по ДСП (плотность ДСП принимаем равной 820 кг/м^3 по ГОСТ 10632-2014 "Плиты древестно-стружечные"):

$G = 0{,}35 \cdot 820 = 287$ кг

Пожарная нагрузка будет составлять ($Q_Н$ =18,4 МДж·кг$^{-1}$):

$Q = 287 \cdot 18{,}4 = 5280$ МДж

Объем хранимой бумажной документации:

$V = 1{,}91 \cdot 1{,}56 \cdot 0{,}4 \cdot 3 \cdot 2 = 7{,}15$ м^3

Определим массу, пожарной нагрузки по бумажной документации (плотность текстильных изделий принимаем равной 80 кг/м^2):

$G = 7{,}15 \cdot 80 = 572$ кг

Пожарная нагрузка будет составлять ($Q_Н$ =16,7 МДж·кг$^{-1}$):

$Q = 572 \cdot 16{,}7 = 9552$ МДж

Удельная пожарная нагрузка, приходящаяся на 1 м^2 составит:

$$g = \frac{Q_{дсн} + Q_{масса}}{S} = \frac{5280+9552}{10} = 1483 \text{ МДЖ} \cdot \text{м}^{-2}$$

В соответствии с табл.4 НПБ 105-03 это значение соответствует категории В2. Однако помещение может быть отнесено к категории В1 при условии, что способ размещения пожарной нагрузки удовлетворяет необходимым требованиям, изложенным в п.25 НПБ 105-03.

В данном помещении минимальное расстояние от поверхности пожарной нагрузки до нижнего пояса ферм (Н) составляет 0,62 м (принимаем расстояние от верхнего уровня шкафа до нижнего пояса ферм).

Определим, выполняется ли условие:

$Q > 0{,}64 \cdot g_т \cdot H^2$.

После подстановки численных значений получим:

$0{,}64 \cdot g_т \cdot H^2 = 0{,}64 \cdot 2200 \cdot 0{,}62^2 = 541$ МДж,

где $g_т$ =2200 МДж . м^2, т.к. значение g находится в области от 1401 МДж · м^2 до 2200 МДж · м^2.

Так как Q = 14 832 МДж и условие Q > 541 МДж выполняется, помещение следует отнести к категории В1.

Для отвода теплоты от ЭВМ в помещениях постоянно действует система кондиционирования воздуха, что обеспечивает доступ кислорода как окислителя процессов горения.

Для основного помещения предприятия площадью более 100 кв. м требуются следующие первичные средства пожаротушения, которые в организации на момент осмотра отсутствуют:

- семь углекислотный огнетушитель типа ОУ-5 или ОУ-8, с помощью которого можно тушить загорания различных материалов и установок напряжением до 1000 В;

- пять химпенный огнетушитель (ОХП-10), с помощью которого можно тушить твердые материалы и горючие жидкости; войлок, асбест.

Помещения должны быть оборудованы пожарными извещателями. Для осуществления тушения загорания водой в системе автоматического пожаротушения используются устройства спринклеры и дренчеры.

В помещении необходимо наличие плана эвакуации в случае пожара.

После анализа пожаробезопасности и проверки ее на соответствие СНиП 21-01-97 «Пожарная безопасность зданий и сооружений», можно утверждать, что пожарная безопасность будет соответствовать нормативной документации после устранения вышеуказанных замечаний.

7.3 Электробезопасность

Электрический ток, воздействуя на организм человека, может вызвать поражения. Степень таких поражений зависит от рода и силы тока, времени действия, пути прохождения в теле.

Человек начинает ощущать воздействие проходящего через него переменного тока промышленной частоты 50 Гц силой 0,6-1,5 мА и постоянного тока 5-7 мА. При увеличении тока, проходящего через тело человека, его воздействие усиливается и при значении переменного тока промышленной частоты 10 мА (60-80 мА постоянного тока) происходит непроизвольное сокращение мышц (судороги) рук, в результате чего человек не может разжать руку, в которой зажата токоведущая часть, то есть он не в состоянии самостоятельно нарушить контакт с токоведущей частью. При больших значениях тока руки парализуются, затрудняется дыхание. Чем больше ток, тем скорее нарушается работа легких и сердца. При токе промышленной частоты 100 мА и более прекращается работа легких и сердца, причем поражение сердца наступает через 2-3 секунды с начала воздействия тока.

ГОСТ 12.1.038-82 «Система стандартов безопасности труда. Электробезопасность. Предельно допустимые значения напряжений прикосновения и токов».

Предельно допустимые значения напряжений прикосновения и токов» установлены предельно допустимые уровни напряжений прикосновения и силы токов, протекающих через тело человека и возникающих в электроустановках произвольного и бытового назначения постоянного и переменного тока частотой 50 и 400 Гц при времени нахождения под напряжением 10 мин.

На территории предприятия используется сеть промышленной частоты 50 Гц напряжением 220 В, которая питает ПЭВМ центра и другую оргтехнику.

Технические мероприятия, проводимые на предприятии для защиты от поражения электрическим током, проводятся в соответствии с действующими «Правилами технической эксплуатации электроустановок потребителей и правила техники безопасности при эксплуатации электроустановок потребителей» (ПТЭ и ПТБ потребителей) и «Правилами устройства электроустановок» (далее - ПУЭ).

К организационным мероприятиям по электробезопасности, действующим на предприятии относят периодический инструктаж персонала.

К техническим мероприятиям относят:

- использование автоматов защитного отключения;
- использование заземления.

Защитное заземление представляет собой преднамеренное соединение с землей или ее эквивалентом металлических нетоковедущих частей, которые могут оказаться под напряжением. В соответствии с ПУЭ сопротивление системы защитного заземления в любое время года для установок с напряжением до 1000 В не должно превышать 4 Ом.

Заземление техники центра осуществляется при помощи трубчатых заземлителей, вмонтированных в здание, в котором расположена организация.

7.4 Расчет необходимого естественного освещения

Правильно спроектированное и выполненное освещение в организации обеспечивает возможность нормальной производительной деятельности. Сохранность зрения человека, состояние его центральной нервной системы и

безопасность оператора в значительной мере зависит от условий освещения. От освещения зависят также работоспособность и производительность труда.

Естественное освещение характеризуется тем, что создаваемая освещенность изменяется в чрезвычайно широких пределах. Эти изменения обуславливаются временем дня, года и метеорологическими факторами: характером облачности и отражающими свойствами земного покрова. Поэтому, естественное освещение нельзя количественно задавать величиной освещенности. Для правильной расстановки оборудования и распределения рабочих мест с различной степенью зрительного напряжения необходимо аналитически определить коэффициент естественной освещенности (далее - КЕО) в производственном помещении. Нормированное значение КЕО для зданий расположенных в III поясе светового климата для проектных залов равно 2%. Световой поток, падающий в расчетную точку производственного помещения, складывается из прямого диффузного света небосвода, видимого через светопроем, и света, отраженного от внутренних поверхностей помещения и противостоящих зданий.

При боковом освещении КЕО определяется по формуле:

$$E_{бок} = (E_б \cdot q + E_{зд} \cdot R) \cdot r \cdot t_0 / K_з, \qquad (7.1)$$

где $E_б$ и $E_{зд}$ - геометрические коэффициенты естественной освещенности в расчетных точках при боковом освещении, учитывающие соответственно свет от небосвода и отраженный от противостоящего здания;

q - коэффициент, учитывающий неравномерную яркость облачного неба, 0,52;

R - коэффициент, определяющий относительную яркость противостоящего здания, 0,18;

t_0 - общий коэффициент светопропускания;

r - коэффициент, учитывающий повышение КЕО за счет отраженного света от потолка и стен помещения, 5,7;

$К_3$ - коэффициент запаса, 1,2.

Геометрический КЕО в расчетной точке при боковом освещении, учитывающий прямой свет неба, определяется по формуле:

$$К_{гео} = 0.01 \cdot (n_1 * n_2), \quad (7.2)$$

где n_1 - количество лучей от неба через световые проемы в расчетную точку на поперечном разрезе помещения, рассчитываемый по специальным таблицам;

n_2 - аналогично n_1, но на плане помещения (n_1, n_2= 13).

В этом случае:

$К_{гео} = 0.01 \cdot (13 \cdot 13) = 1.69$

Геометрический КЕО: в расчетной точке при боковом освещении, учитывает свет, отраженный от противоположного здания, определяемый по формуле:

$$К_{гео} = 0.01 \cdot (n_3 \cdot n_4), \quad (7.3)$$

где n_3, n_4 - лучи, проходящие от противоположного здания через световой проем в расчетную точку соответственно на поперечном разрезе помещения и на плане помещения, рассчитываемые по специальным таблицам. Они равны 4.

Тогда:

$К_{гео} = 0.01 \cdot (4 \cdot 4) = 0.16$

Коэффициент светопропускания определяется по формуле:

$$t_0 = t_1 \cdot t_2 \cdot t_3 \cdot t_4 \cdot t_5, \quad (7.4)$$

где t_1 - коэффициент светопропускающего материала, равный 0,8;

t_2 - коэффициент, учитывающий потери света в переплетах светопроема, равный 0,7;

t_3 - коэффициент, учитывающий потери света в несущих конструкциях, равный 1;

t_4- коэффициент, учитывающий потери света в солнцезащитных устройствах, равный 1;

t_5 - коэффициент, учитывающий потери света в защитном стекле, установленном под фонарем, равный 0,9.

Найдем значение $E_{бок}$:

$E_{Бок} = (1,69 \cdot 0,52+0,16 \cdot 0,18) \cdot 5,7 \cdot 0,504/1,2=2,15\%$.

Получили значение расчетного КЕО при боковом освещении производственного помещения ($К_{кео} = 2,15$ %) соответствует норме.

7.5 Анализ экологических особенностей проекта

При создании разрабатываемой в выпускной квалификационной работе ЛВС негативных воздействий на экологию и окружающую среду осуществлено не будет. Имеются вторичные отходные материалы, такие как использованная бумага, кабели и так далее, которые утилизируются в соответствии с установленными нормами специализированными организациями. Поэтому разрабатываемая система является экологически безвредной.

Выводы по разделу семь:

В данной главе выпускной квалификационной работы проделано следующее:

- проведен анализ неблагоприятных факторов, воздействующих на пользователя;
- даны характеристики рабочего места оператора, параметры микроклимата в помещении, а так же характеристики уровня освещенности и шума в помещении, где находится рабочее место оператора;
- проведена оценка уровня шума ЭВМ администратора ЛВС.

Прямого вредного воздействия от работы ЛВС на окружающую среду и администратора нет. В связи с этим проект можно считать полностью экологически безопасным.

ЗАКЛЮЧЕНИЕ

Локальные вычислительные сети и глобальная сеть Интернет глубоко проникли во все без исключения сферы человеческой жизни. Обработка баз данных, удалённая работа, поиск необходимых данных заставляют современного человека искать более качественные и быстрые варианты доступа в локальные и глобальные компьютерные сети. Иногда для полной работы компании необходимо обеспечить сетевую безопасность с помощью внедрения виртуальных сетей VPN, устанавливать взаимосвязи с филиалами, которые расположены на огромном расстоянии друг от друга. Учитывая такие сложные и масштабные требования, фирмы, которые занимаются построением локальных вычислительных сетей, отмечают особо важную роль возможных технических решений, способных данные требования удовлетворить.

По завершению выпускной квалификационной работы получены нижеуказанные результаты:

1. Разработана беспроводная локальная вычислительная сеть, которая способна обеспечить качественным доступом пользователей компании ООО «Инструментстрой», обеспечить защищённость сетевого окружения и трафика сети через:

- внедрение не требовательных к ресурсам программных продуктов, позволяющих качественно управлять входящими каналами, предотвращать нецелесообразное использование рабочих ресурсов;
- использование программного маршрутизатора, который позволяет масштабировать локальную сеть по периметру офисных помещений, причем с минимальным задействованием ресурсов для этого;
- использование активного технического коммутационного оборудования, которое способно изолировать сегменты сети на логическом уровне, предотвращая этим самым несанкционированный доступ в сеть из вне;
- увеличение пропускной способности ЛВС через уменьшение широковещательного домена;

- использование ОС на базе Linux, которая способна маршрутизировать трафик на уровне дорогих аппаратных маршрутизаторов.

2. В результате выполнения выпускной квалификационной работы получена значительная экономическая выгода через:

- экономию на ОС и выбор свободно распространяемого программного обеспечения;
- выбор активного оборудования, не имеющего лишних, не требующихся опций;
- приобретение относительно дешёвой серверной платформы с параметрами, которые удовлетворяют требованиям операционной системы маршрутизатора;
- использование программного обеспечения, которое необходимо для эффективного функционирования сети и находящегося в более низкой ценовой категории относительно конкурентов.

Разработанные в процессе выполнения выпускной квалификационной работы технические решения в полном объёме применены для создания ЛВС компании ООО «Инструментстрой».

ПЕРЕЧЕНЬ ПРИНЯТЫХ СОКРАЩЕНИЙ

АВС - антивирусные средства;

АРМ - автоматизированное рабочее место;

ВПр - вредоносная программа;

ВТСС - вспомогательные технические средства и системы;

ИБП - источник бесперебойного питания;

ИС - информационная система;

ИСПДн - информационная система персональных данных;

КЕО - коэффициент естественной освещенности;

ЛВС - локально-вычислительная сеть;

МЭ - межсетевой экран;

НСД - несанкционированный доступ;

ОС - операционная система;

ОЗУ – оперативное запоминающее устройство;

ПО - программное обеспечение;

ПК - персональный компьютер;

ПМЭ - персональный межсетевой экран;

ПЭМИН - побочные электромагнитные излучения и наводки;

РМ - рабочее место;

САВЗ - средства антивирусной защиты;

САЗ - система анализа защищенности;

СЗИ - средство защиты информации;

СКС - структурированная кабельная система;

СПД - сеть передачи данных;

СУСН - средства управления съемными носителями

ТЗ - техническое задание;

ФСТЭК - Федеральная служба по техническому и экспортному контролю;

ЭВМ - электронно-вычислительная машина;

VLAN - виртуальная локальная сеть.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Максимов, Н.В. Архитектура ЭВМ и вычислительных систем: учебник / Н.В. Максимов, Т.Л. Партыка, И.И. Попов. - М.: Форум, 2015 - 512 с.

2. Жук, А.П. Защита информации: учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин. М.: НИЦ ИНФРА-М, 2012. - 392 с.

3. Гришина, Н.В. Информационная безопасность предприятия: учебное пособие / Н.В. Гришина. - Москва: Изд-во Форум: 2015. - 240 с.

4. Вдовенко, Л.А. Информационная система предприятия: учебное пособие/Л.А. Вдовенко - Москва: Изд-во НИЦ ИНФРА-М, 2011. - 304 с.

5. Федотова, Е.Л. Информационные технологии в профессиональной деятельности: учебное пособие / Е.Л. Федотова. - Москва: Изд-во Форум: 2013. - 368 с.

6. Даранова, Е.К. Моделирование системы защиты информации: учебное пособие / Е.К.Баранова, А.В.Бабаш. - Москва: Изд-во: НИЦ ИНФРА, 2011 - 120 с.

7. Ищейнов, В.Я. Основные положения информационной безопасности: учебное пособие/В.Я.Ищейнов, М.В.Мецатунян - Москва: Изд-во Форум: 2010. - 208 с.

8. Хорев, П.Б. Программно-аппаратная защита информации: учебное пособие / П.Б. Хорев. - 2-е изд., испр. и доп. - Москва: Изд-во: Форум: НИЦ ИНФРА-М, 2009. - 352 с.

9. Каратунова, Н. Г. Защита информации. Курс лекций: Учебное пособие / Н. Г. Каратунова. - Краснодар: КСЭИ, 2014. - 188 с. - http://znanium.com/catalog.php?bookinfo=503511.

10. Поляк-Брагинский А.В. Администрирование сети на примерах: учебное пособие / А.В. Поляк-Брагинский - СПб.: Изд-во: БХВ-Петербург, 2005. - 320 с.

11. Олифер, В.Г. Компьютерные сети. Принципы, технологии, протоколы: учебное пособие/ В. Г. Олифер, Н. А. Олифер. - СПб.: Изд-во Питер, 2006. - 958 с.

12. Айвенс, К. Компьютерные сети. Хитрости. К. Айвенс - СПб.: Изд-во Питер, 2006. - 298 с.

13. Галатенко, В.А. Основы информационной безопасности: учебное пособие / В.А. Галатенко - Москва: Изд-во ИНТУИТ.РУ, 2006. - 208 с.

16. Новиков, Ю.В. Основы локальных сетей: курс лекций: учеб. пособие / Ю.В.Новиков, С.В.Кондратенко - Москва: Изд-во Интернет, 2005. - 360 с.

14. Олифер, В.Г. Основы сетей передачи данных: учебное пособие / В.Г. Олифер - Москва: Изд-во ИНТУИТ.РУ, 2005. - 176 с.

15. Каймин, В.А. Информатика: учебник / В.А. Каймин. - Москва: Издво ИНФРА-М, 2006. - 285 с.

16. Галатенко, В.А. Стандарты информационной безопасности: учебное пособие / В.А. - Москва: Изд-во ИНТУИТ.РУ, 2006. - 264 с.

17. Яшин, В.М. Информатика: аппаратные средства персонального компьютера: учебное пособие / В.М. Яшин. - Москва: Изд-во ИНФРА-М, 2008. - 254 с.

18. СНиП 41-01-2003 «Отопление, вентиляция и кондиционирование». - М.: Изд-во стандартов, 2004 - 17 с.

19. СНиП 21-01-97 «Пожарная безопасность зданий и сооружений». - М.: Изд-во стандартов, 1997 - 24 с.

20. ГОСТ 10632-2014 «Плиты древестно-стружечные». - М.: Изд-во стандартов, 2014 – 16 с.

21. ГОСТ 12.1.038-82 ССБТ. «Электробезопасность. Предельно допустимые значения напряжений прикосновения и токов» (с Изменением №1). – М.: Изд-во стандартов, 2001 – 31 с.

22. СТО ЮУрГУ 04–2008 Стандарт организации. Курсовое и дипломное проектирование. Общие требования к содержанию и оформлению / составители: Т.И. Парубочая, Н.В. Сырейщикова, В.И. Гузеев, Л.В. Винокурова. – Челябинск: Изд-во ЮУрГУ, 2008. – 56 с.

ПРИЛОЖЕНИЕ А. ФАКТОРНЫЙ АНАЛИЗ СРЕДСТВ МЕЖСЕТЕВОГО ЭКРАНИРОВАНИЯ

Таблица А.1 - Факторный анализ средств межсетевого экранирования

Параметр средства ЗИ	Весовой коэф.	Symantec Endpoint	Windows Firewall	Cisco Security Agent	McAfee Host Intrusion Prevention
Возможности СЗИ:					
Применение различных параметров фильтрации	1	1	0	1	1
Фильтрация сетевых информационных потоков	1	1	1	1	1
Возможность поддержки протокола IPSec	0,5	0	0	0	0
Фильтрация входящих потоков информации	0,5	1	0	1	1
Возможность применения временных политик или политик по расписанию	0,5	0,8	0	0	1
Возможность контроля за активностью приложений	0,5	1	0	1	1
Возможности системы:					
Возможность масштабирования по числу пользователей системы	0,5	1	1	0,5	1
Возможность интеграции в устройстве комплексов защиты	0	1	1	0	1
Возможность упрощенной массовой установки	1	1	1	1	1
Поддержка операционных систем Windows XP, Vista, 2003, Windows 7	1	1	1	1	1
Объединение в едином средстве защиты на уровне хоста	0	0	0	0	0
Удаленное управление	1	1	1	1	1
Управление и мониторинг:					
Интеграция управления LDAP	1	1	1	1	1

Параметр средства ЗИ	Весовой коэф.	Symantec Endpoint	Windows Firewall	Cisco Security Agent	McAfee Host Intrusion Prevention
Возможность локального управления средствами ЗИ	1	1	1	1	1
Параметр средства ЗИ	Весовой коэф.	Symantec Endpoint	Windows Firewall	Cisco Security Agent	McAfee Host Intrusion Prevention
Удаленное обновление программным обеспечением	1	1	1	1	1
Использование иерархии администратора и оператора	0,8	1	1	0,8	1
Интеграция систем управления с различными серверами	1	1	0	1	1
Наличие консоли оповещения сотрудника службы безопасности	0,5	1	1	0,5	1
Объединение с центральной системой управления инцидентами	0,5	1	1	0,5	1
Наличие средств анализа происшествий	0	1	1	0	1
Объединение с центральной системой управления инцидентами	0	1	0,5	0	0,5
Характеристики доверенности:					
Наличие учебного курса по работе с системой	1	0,5	1	1	1
Услуги и техническая поддержка производителя	1	1	1	1	1
Цена:					
Сертификации	5	0,0	0,0	0,5	0,5
Средств ЗИ	5	0,4	1,0	0,0	0,9
Показатель эффективности исследуемого средства ЗИ		0,774	0,493	0,671	0,731

ПРИЛОЖЕНИЕ Б. АНАЛИЗ СРЕДСТВ УПРАВЛЕНИЯ СЪЕМНЫМИ НОСИТЕЛЯМИ

Таблица Б.1 - Анализ средств управления съемными носителями

Параметр средства ЗИ	Вес. коэфиц.	Lumension Device	Security Studio	Device Lock	Cisco Security Agent	McAfee Device	Symantec Endpoint Security
Возможности СЗИ:							
Возможность разграничения доступа к съемным носителям для пользователей	1	1	1	1	0,5	1	1
Использование списка допустимых носителей	1	1	0,5	1	0,5	1	1
Возможность разграничения доступа к съемным носителям для ЭВМ	0	1	1	1	1	1	1
Назначение права копирования носителей	1	1	0	0	0	1	0
Возможность временного или разового доступа к носителям	0,5	1	0	1	0	0	0
Полный охват подключаемых устройств	1	1	0,8	0,8	0,8	0.8	1
Возможность разграничения доступа по составленному расписанию	0,5	1	0	1	1	0	0
Назначение доступа для различных подключений	0,5	1	0	0	0,5	0	0
Возможность регистрации фактов доступа к носителям	1	1	0,5	1	1	0.5	1
Теневое копирование	0,5	1	0	1	0	0	0
Работа с распределенными инфраструктурами	1	1	1	1	1	1	1
Возможности системы:							

Параметр средства ЗИ	Вес. коэфиц	Lumension Device	Security Studio	Device Lock	Cisco Security Agent	McAfee Device	Symantec Endpoint Security
Объединение в едином средстве защиты на уровне хоста	0,5	0,5	0,5	0,3	1	1	1
Возможность масштабирования по числу пользователей системы	0,5	1	0,8	1	1	1	1
Возможность поддержки операционных систем Windows Mobile	0,5	0,5	0	0	1	0	1
Управление и мониторинг:							
Возможность удаленного управления	0,5	1	1	1	1	1	1
Объединение с центральной системой управления инцидентами	0,5	0,5	0,5	0	0,5	1	1
Интеграция систем управления AD	1	1	1	1	1	1	1
Наличие консоли оповещения сотрудника службы безопасности	1	0,5	1	0,3	0,8	1	1
Интеграция управления LDAP	1	1	0	0	1	0	1
Использование иерархии администратора и оператора	1	1	1	1	1	1	1
Объединение с центральной системой управления инцидентами	0	0	0	0	1	1	1
Наличие средств анализа происшествий	0,5	1	1	0,5	1	1	1
Характеристики доверенности:							
Наличие учебного курса по работе с системой	0,5	0	1	0	1	0,8	1
Услуги и техническая поддержка производителя	1	1	1	0,5	1	1	1
Цена:							
Сертификации	2	0,5	1,0	1,0	0,0	0,5	0,0
Средств ЗИ	5	0,5	0,6	0,8	0,0	0,8	0,7
Показатель эффективности исследуемого средства ЗИ		0,74	0,611	0,655	0,522	0,63	0,785

ПРИЛОЖЕНИЕ В. ФАКТОРНЫЙ АНАЛИЗ СРЕДСТВ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ

Таблица В.1 - Факторный анализ средств обнаружения вторжений

Параметр средства ЗИ	Весовой коэф.	IBM ISS Proventia	Stonegate IPS	Аргус
Возможности СЗИ:				
Возможность обнаружения статистической аномалии	1	1	1	1
Применение сигнатурных методов обнаружения	1	1	1	1
Возможность обнаружения статистической аномалии типа «отказы в обслуживании»	0,2	1	1	1
Возможность обнаружения аномалии при работе протоколов	1	1	1	1
Возможность обслуживания неправильно сформированных пакетов данных	0,2	1	1	1
Возможность распознавания протоколов обработки данных	1	0,5	0,5	0
Использование методов защиты от атаки «обход СОВ»	0,5	1	0,5	0
Возможность обнаружения комбинированных атак	0,5	0	0,5	0
Обнаружение и предотвращение неизвестных атак	0,2	1	1	0

Параметр средства ЗИ	Весовой коэф.	IBM ISS Proventia	Stonegate IPS	Аргус
Возможность поддержки виртуального сенсора	1	0	1	0
Параметр средства ЗИ	Весовой коэф.	IBM ISS Proventia	Stonegate IPS	Аргус
Возможность обнаружения атак на имеющиеся протоколы	0,2	1	0,5	0
Учет важности файловых ресурсов	0,5	0,5	0,5	0
Возможности системы:				
Поддержка операционных систем семейства Windows	0	1	0	0
Наличие различных программных решений	0,5	1	1	0
Поддержка операционных систем семейства Linux	0	0	0	1
Наличие различных аппаратно-программных решений	0,5	1	1	1
Возможность поддержки VLAN	1	1	1	0
Масштабирование производительности	2	1	1	0,2
Балансировка нагрузок	1	1	1	0
Управление и мониторинг:				
Интеграция с центральным управление	1	1	1	0,5
Возможность удаленного управления	1	1	0	1

Параметр средства ЗИ	Весовой коэф.	IBM ISS Proventia	Stonegate IPS	Аргус	
Наличие консоли оповещения сотрудника службы безопасности	1	0,5	1	0,2	
Работа удаленно с помощью консоли (SSH)	1	0	0	0	
Параметр средства ЗИ	Весовой коэф.	IBM ISS Proventia	Stonegate IPS	Аргус	
Наличие средств анализа происшествий	1	0,5	1	0,2	
Объединение с центральной системой управления инцидентами	1	0,8	0,8	0,2	
Характеристики доверенности:					
Наличие учебного курса по работе с системой	1	1	0,8	0	
Услуги и техническая поддержка производителя	1	1	1	0,2	
Цена:					
Сертификации	5	0,7	0	1	
Средств ЗИ	5	0	0,3	0,5	
Показатель эффективности исследуемого средства ЗИ			0,552	0,516	0,377

ПРИЛОЖЕНИЕ Г. ФАКТОРНЫЙ АНАЛИЗ СРЕДСТВ АНАЛИЗА ЗАЩИЩЕННОСТИ

Таблица Г.1 - Факторный анализ средств анализа защищенности

Параметр средства ЗИ	Весовой коэф.	XSpider	MaxPatrol	IBM Internet Scanner
Возможности СЗИ:				
Возможность обнаружения и идентификации устройств в сети	1	1	1	0,8
Возможность локального обнаружения уязвимостей	1	1	1	1
Возможность обнаружения и идентификации работающих сервисов	1	1	1	0,8
Тестирование уязвимостей	1	1	1	1
Возможность Удаленного обнаружения уязвимостей	1	1	1	1
Различные варианты обнаружения уязвимостей	0,5	1	1	0,5
Расширенный анализ баз данных	1	0,8	1	0
Полный охват базы уязвимости	1	1	1	0,5
Расширенный анализ сервисов и приложений	1	1	1	0,2
Различные типы устранения уязвимостей	0,5	1	1	1
Сравнение результатов проверок	0,5	0,8	1	1
Контроль стандартизации	0,5	0	1	0
Возможности системы:				
Наличие различных программных решений	0	1	1	1
Поддержка операционных систем семейства Linux	0,5	0	0	0
Наличие различных аппаратно-программных решений	1	0	0	0
Распределенная архитектура	0,5	1	1	1

Параметр средства ЗИ	Весовой коэф.	XSpider	MaxPatrol	IBM Internet Scanner
Поддержка операционных систем семейства Windows	1	1	1	1
Сохранение результатов в стандартных базах данных	0,5	0	0	1
Возможность управления через графический интерфейс	0,2	1	1	1
Возможность масштабирования производительности	1	1	1	1
Установка и настройка	1	1	1	0,4
Интеграция с центральным управлением	0,5	0,2	0,2	1
Возможность управления с помощью командной строки	0,2	0	0	1
Проверки по расписанию	0,5	0	0,5	1
Использование иерархии администратора и оператора	0,5	0	0	1
Характеристики доверенности:				
Наличие учебного курса по работе с системой	1	1	0,5	1
Услуги и техническая поддержка производителя	1	1	0,5	1
Цена:				
Сертификации	1	0,9	1	0,7
Средств ЗИ	5	0,8	0,0	0,3
Показатель эффективности исследуемого средства ЗИ		0,696	0,717	0,521

ПРИЛОЖЕНИЕ Д. ФАКТОРНЫЙ АНАЛИЗ СРЕДСТВ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ

Таблица Д.1 - Факторный анализ средств криптографической защиты

Параметр средства ЗИ	Весовой коэф	S-Terra CSP VPN Gate	Континент	StoneGate VPN	Check Point VPN-1
Возможности СЗИ:					
Применение разной политики к различному трафику	1	1	1	1	1
Защита информационного трафика	1	1	1	1	1
Возможность поддержки ключевых схем шифрования	1	1	1	1	1
Защита передаваемого трафика	1	1	1	1	1
Возможность поддержки протоколов IPSec	1	1	0	1	1
Передача трафика по NAT-шлюзам	1	1	1	1	1
Применение многоуровневых топологий	1	1	1	1	1
Возможность поддержки ключевых схем PKI	1	1	1	1	1
Взаимодействие со средствами VPN соединений	0,5	1	0	1	1
Возможности системы:					

Параметр средства ЗИ	Весовой коэф	S-Terra CSP VPN Gate	Континент	StoneGate VPN	Check Point VPN-1
Возможность поддержки операционных систем семейства Windows	0	1	0	0	1
Параметр средства ЗИ	Весовой коэф	S-Terra CSP VPN Gate	Континент	StoneGate VPN	Check Point VPN-1
Возможность поддержки операционных систем семейства Linux	0	1	0	0	1
Наличие разнообразных аппаратно-программных решений	0,5	1	1	1	1
Совмещение различных функций шлюзов	0,5	0,5	0,5	0,8	1
Возможность поддержки операционных систем типа VMWare ESX	0,5	0	0	1	1
Балансировка нагрузки	1	1	0	1	1
Возможность масштабирования системы	3	1	0,5	1	0,8
Возможность поддержки приоритетов трафика	0,5	1	1	1	1
Быстрое резервирование	1	1	1	1	1
Возможность поддержки VLAN	1	1	1	1	1
Управление и мониторинг:					

Параметр средства ЗИ	Весовой коэф	S-Terra CSP VPN Gate	Континент	StoneGate VPN	Check Point VPN-1
Интеграция с центральным управление системы ЗИ	1	1	0,5	1	1
Возможность удаленного управления	0,5	0,5	1	1	1
Возможность использования иерархии администратора	1	0,5	0,8	1	1
Параметр средства ЗИ	Весовой коэф	S-Terra CSP VPN Gate	Континент	StoneGate VPN	Check Point VPN-1
Возможность удаленного управления	0,5	1	0	0	1
Обеспечение безопасности управляющих данных	0,5	0,5	1	1	1
Наличие средств анализа событий	0,5	0,5	1	1	1
Наличие консоли оповещения сотрудника службы безопасности	1	0	1	1	1
Объединение с центральной системой управления инцидентами	1	1	0,5	1	1
Характеристики доверенности:					
Услуги и техническая поддержка производителя	1	1	1	1	1
Наличие учебного курса по работе с системой	0,5	1	1	1	0

Параметр средства ЗИ	Весовой коэф	S-Terra CSP VPN Gate	Континент	StoneGate VPN	Check Point VPN-1
Наличие авторизованного учебного курса от производителя	0,5	1	1	1	1
Наличие сертификата по системе классификации ЗИ	0,2	1	1	0	0
Цена:					
Цена технической поддержки	1	0,8	0,6	0	0,1
Цена средств ЗИ	5	0,7	0,7	0	0,1
Показатель эффективности исследуемого средства ЗИ		0,748	0,690	0,726	0,736

ПРИЛОЖЕНИЕ Е. КОМПАКТ – ДИСК

Содержание:

1. Пояснительная записка
2. Презентация