МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН

Некоммерческое акционерное общество
АЛМАТИНСКИЙ УНИВЕРСИТЕТ ЭНЕРГЕТИКИ И СВЯЗИ

кафедра „Компьютерные технологии"

«Допущен к защите»
Заведующий кафедрой _____
(Ф.И.О., ученая степень, звание)
_____ «_____»_____ **20__ г.**
(подпись)

ДИПЛОМНЫЙ ПРОЕКТ

На тему: „Технологии беспроводных сетей"

Специальность 5В070400 - Вычислительная техника и программное обеспечение

Выполнил (а) Квочкин Н.А. ВТ-10-4
(Фамилия и инициалы) группа

Научный руководитель Тойгожинова А.Ж. ст. препод.
(Фамилия и инициалы, ученая степень, звание)

Консультанты:

по экономической части:
Ергалиева З.Д. сен. преподаватель
(Фамилия и инициалы, ученая степень, звание)
Ергалиева «12» мая 20 14 г.
(подпись)

по безопасности жизнедеятельности:
Трихлеб Н.Г., д.т.н., профессор
(Фамилия и инициалы, ученая степень, звание)
_____ «11» 05 20 14 г.
(подпись)

по применению вычислительной техники:
Тойгожинова А.Ж., ст. препод.
(Фамилия и инициалы, ученая степень, звание)
_____ «15» 05 20 14 г.
(подпись)

_____
(Фамилия и инициалы, ученая степень, звание)
_____ «_____»_____ 20__ г.
(подпись)

Нормоконтролер: Тусупов Д.М.
(Фамилия и инициалы, ученая степень, звание)
_____ «23» мая 20 14 г.
(подпись)

Рецензент: _____
(Фамилия и инициалы, ученая степень, звание)
_____ «_____»_____ 20__ г.
(подпись)

Алматы 2014 г.

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН

Некоммерческое акционерное общество

АЛМАТИНСКИЙ УНИВЕРСИТЕТ ЭНЕРГЕТИКИ И СВЯЗИ

Факультет „Информационных технологий"
Специальность „Вычислительная техника и программное обеспечение"
Кафедра „Компьютерные технологии"

ЗАДАНИЕ

на выполнение дипломного проекта

Студент Квочкин Николай Александрович
(фамилия, имя, отчество)

Тема проекта „Технология беспроводных сетей"

утверждена приказом ректора № 115 от «24» сентября 2013 г.

Срок сдачи законченной работы «7» июня 2014 г.

Исходные данные к проекту требуемые параметры результатов проектирования (исследования) и исходные данные объекта

План здания и схема этажей здания СПбГБУК „СПбГБСС", книги по проектированию и защите локальных сетей, построенных на основе технологии Wi-Fi

Перечень подлежащих разработке дипломного проекта вопросов или краткое содержание дипломного проекта:

1. Виды технологий, применяющихся в беспроводных сетях.
2. Технология Wi-Fi
3. Безопасность в сетях Wi-Fi
4. Проект сети по технологии Wi-Fi для СПбГБУК „СПбГБСС"
5. Сравнение экономической эффективности двух проектов сети.
6. Безопасность жизнедеятельности

Перечень графического материала (с точным указанием обязательных чертежей)

Рекомендуемая основная литература

1. Пол Бедлл. „Сети. Беспроводные технологии"
2. Шаховец И. „Современные технологии беспроводной связи"
3. Семенов А. „Проектирование и расчет структурированных кабельных систем и их компонентов"
4. Ержанова З.Б. „Методические указания к выполнению экономической части дипломных работ для студентов специальности 5В070400"
5. Мотузко Ф.Я. „Охрана труда"

Консультанты по проекту с указанием относящихся к ним разделов

Раздел	Консультант	Сроки	Подпись
Экономика	Ержанова З.Б.	25.04-12.05.14	
БЖД	Приходько Н.Г.	11.04 – 11.05.14	
Основная часть	Тойгожинова А.Ж.	11.04 - 20.05.14	
Нормоконтроль	Гусупов Д.М.	23.05.14г.	

Г Р А Ф И К
подготовки дипломного проекта

№ п/п	Наименование разделов, перечень разрабатываемых вопросов	Сроки представления руководителю	Примечание
1.	Беспроводные технологии. Классификация, история, принципы работы	02.04.2014	
2.	Безопасность Wi-Fi сетей. Прямые и косвенные угрозы.	10.04.2014	
3.	Проект сети для СПбГБУК, СПбГБСС по технологии Wi-Fi. Выбор стандартов беспроводной связи, подбор оборудования.	24.04.2014	
4.	Сравнение экономической эффективности проекта с классической и беспроводной локальными сетями	09.05.2014	
5.	Безопасность жизнедеятельности	11.05.2014	

Дата выдачи задания «3» марта 20 14 г.

Заведующий кафедрой _____ _____
(подпись) (Фамилия и инициалы)

Руководитель _____ Тойгожинова А.Ж.
(подпись) (Фамилия и инициалы)

Задание принял к исполнению
студент _____ Квочкин И.А.
(подпись) (Фамилия и инициалы)

Аннотация

В данном дипломном проекте спроектирована локальная сеть для СПбГБУК «СПбГБСС» на основе технологии беспроводных сетей Wi-Fi. В качестве стандарта связи использован новейший IEEE 802.11ac, позволяющий достичь наибольших скоростей, сопоставимых с проводными локальными сетями. Также реализована задача обеспечения бесшовного Wi-Fi роуминга во всем здании СПбГБУК «СПбГБСС». Произведено сравнение затрат на создание сети по двум вариантам (проводном и на основе Wi-Fi). Рассмотрены аспекты связанные с обеспечение безопасности и оптимальных условий труда на рабочем месте.

Abstract

In this diploma project is designed for LAN SPbGBUK "SPbGBSS" technology-based wireless networks Wi-Fi. As a communication standard used newest IEEE 802.11ac, which achieves the highest speed comparable to wired LANs. Also implemented the task of ensuring seamless Wi-Fi roaming throughout the building SPbGBUK "SPbGBSS". The comparison of the cost of establishing a network in two ways (wired and based on Wi-Fi). The aspects related to security and optimal working conditions in the workplace.

Аңдатпа

Бұл дипломдық жобада Wi-Fi сымсыз желілер технологиясы негізінде «СПбГБСС» СПбГБУК үшін дербес желі жобаланды. Стандарт сапасында дербес сымды желілермен салыстырылатын байланыстың аса жоғары жылдамдықты алуға мүмкіндік беретін ең жаңа IEEE 802 пайдаланылды. Сондай-ақ, «СПбГБСС» СПбГБУК барлық ғимаратында жіксіз Wi-Fi роумингін қамтамасыз ету іске асырылды. Екі нұсқа бойынша (сымды және Wi-Fi негізінде) желіні жасау шығындарының салыстырылуы орындалды. Жұмыс орнында оңтайлы жағдайлар мен қауіпсіздікті қамтамасыз ету үрдісі қарастырылды

Содержание

Введение

Беспроводные технологии – это подкласс информационных технологий, которые предназначены для передачи информации на расстояние между двумя или более точками, не требуя при этом их связи посредством проводов. Для передачи информации может использоваться радиоволны, оптическое, инфракрасное или лазерное излучение.

В настоящее время существует множество беспроводных технологий, наиболее часто известных пользователям по их маркетинговым названиям, например: Wi-Fi, WiMAX, Bluetooth. Каждая технология обладает определёнными характеристиками, которые определяют её область применения.

WiMAX (англ. *Worldwide Interoperability for Microwave Access*) – телекоммуникационная технология, разработанная с целью предоставления универсальной беспроводной связи на больших расстояниях для широкого спектра устройств (от рабочих станций и портативных компьютеров до мобильных телефонов). Основана на стандарте IEEE 802.16, который также имеет название Wireless MAN (WiMAX следует считать жаргонизмом, потому что это не технология, а название форума, на котором Wireless MAN и был принят) [1].

Название «WiMAX» было создано WiMAX Forum – организацией, которая была основана в июне 2001 года с целью продвижения и развития технологии WiMAX. Этот форум так описывает WiMAX: «основанная на стандарте технология, предоставляющая высокоскоростной беспроводной доступ к сети, альтернативный выделенным линиям и DSL». Максимальная скорость составляет около 1 Гбит/сек на ячейку.

Bluetooth – производственная спецификация беспроводных персональных сетей (англ. *Wireless personal area network, WPAN*). Bluetooth обеспечивает обмен информацией между такими устройствами как ПК (настольные, карманные и другие), мобильные телефоны, принтеры, цифровые фотоаппараты, мышки, клавиатуры, наушники, гарнитуры и прочее. Bluetooth позволяет этим устройствам находиться на связи, если они расположены в радиусе до 100 метров друг от друга (дальность связи ощутимо зависит радиопомех и различных преград, мешающих распространению радиоволн).

Данный дипломный проект посвящен проектированию локальной сети по технологии Wi-Fi.

Под аббревиатурой Wi-Fi (от английского словосочетания Wireless Fidelity, дословно – «беспроводное качество» или «беспроводная точность») в настоящее время развивается целое семейство стандартов передачи цифровых потоков данных по радиоканалам. Под этой аббревиатурой скрывается IEEE 802.11 – набор стандартов связи для коммуникации в беспроводной локальной сетевой зоне частотных диапазонов 0,9; 2,4; 3,6 и 5 ГГц. На данный момент существует огромное количество видов стандарта IEEE 802.11 (a/b/g/n/ac и прочее) [2].

Главным преимуществом этой технологии является отсутствие больших количеств проводов и мобильность пользователей. В проекте сети также реализован бесшовный роуминг. Роуминг – процесс автоматического подключения устройства к другой точке доступа одной беспроводной сети при перемещении его в пространстве. При этом клиентское устройство определяет, что уровень сигнала первой точки доступа падает, при нарастании сигнала второй точки доступа и принимает решение о переподключении ко второй точке доступа. Если в процессе такого переподключения потери сигнала не превышают 1-2 пингов, то такой роуминг называется бесшовным. При таком способе осуществления роуминга не наблюдается разрывы при загрузке информации, в работе различных медиа приложений.

1 Беспроводные технологии

1.1 Классификация беспроводных технологий

Существуют различные подходы к классификации беспроводных технологий.

По дальности действия:

- Беспроводные персональные сети (WPAN — Wireless Personal Area Networks). Примеры технологий — Bluetooth.
- Беспроводные локальные сети (WLAN — Wireless Local Area Networks). Примеры технологий — Wi-Fi.
- Беспроводные сети масштаба города (WMAN — Wireless Metropolitan Area Networks). Примеры технологий — WiMAX.
- Беспроводные глобальные сети (WWAN – Wireless Wide Area Network). Примеры технологий – CSD, GPRS, EDGE, EV-DO, HSPA (Рисунок 1.1).

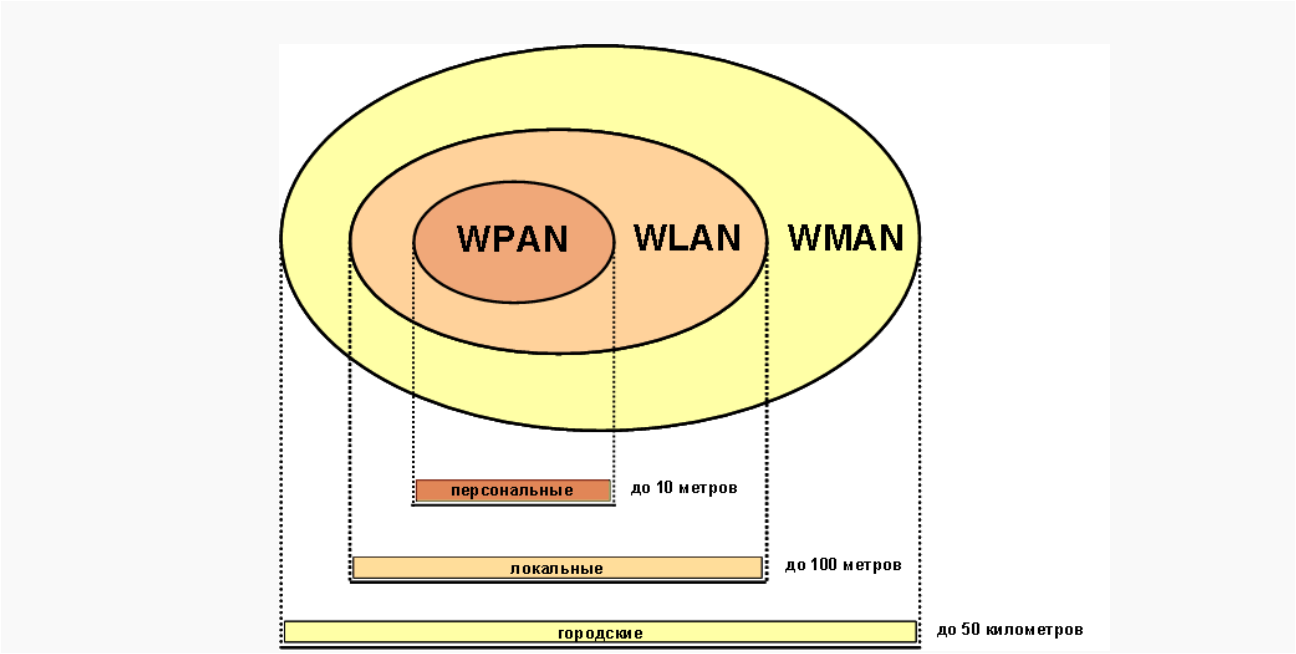

Рисунок 1.1 – Классификация по дальности действия

По топологии:

- Точка-точка.
- Точка-многоточка.

По области применения:

- Корпоративные (ведомственные) беспроводные сети – создаваемые компаниями для собственных нужд.
- Операторские беспроводные сети – создаваемые операторами связи для возмездного оказания услуг.

Кратким, но ёмким способом классификации может служить одновременное отображение двух наиболее существенных характеристик беспроводных технологий на двух осях: максимальная скорость передачи информации и максимальное расстояние (Рисунок 1.2).

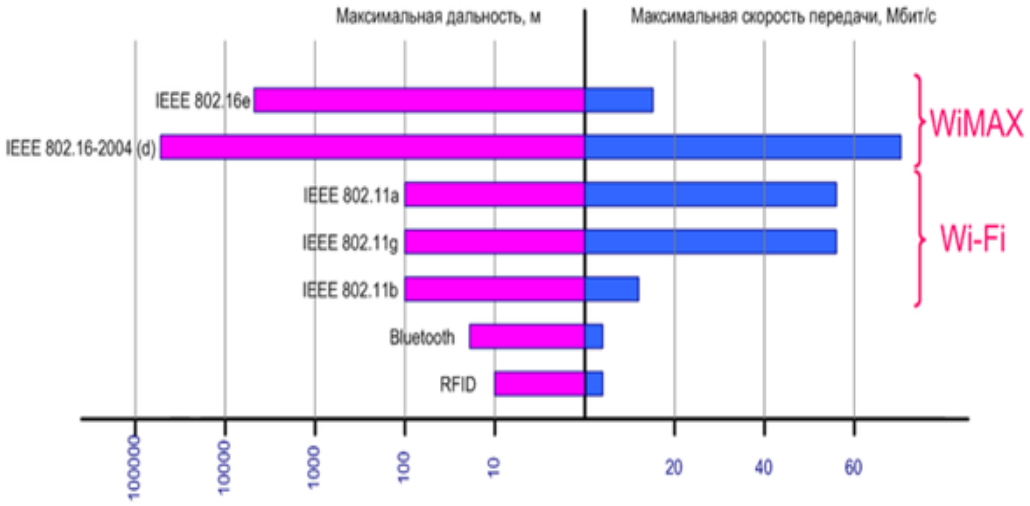

Рисунок 1.2 – Классификация по скорости и расстоянию

1.2 Технология Wi-Fi

Wi-Fi – торговая марка Wi-Fi Alliance для беспроводных сетей на базе стандарта IEEE 802.11. Под аббревиатурой Wi-Fi (от английского словосочетания Wireless Fidelity, которое можно дословно перевести как «беспроводное качество» или «беспроводная точность») в настоящее время развивается целое семейство стандартов передачи цифровых потоков данных по радиоканалам.

Любое оборудование, соответствующее стандарту IEEE 802.11, может быть протестировано в Wi-Fi Alliance и получить соответствующий сертификат и право нанесения логотипа Wi-Fi.

1.2.1 История

Wi-Fi был создан в 1991 году NCR Corporation/AT&T (впоследствии – Lucent Technologies и Agere Systems) в Ньивегейн, Нидерланды. Продукты, предназначавшиеся изначально для систем кассового обслуживания, были выведены на рынок под маркой WaveLAN и обеспечивали скорость передачи данных от 1 до 2 Мбит/с. Создатель Wi-Fi – Вик Хейз (*Vic Hayes*) находился в команде, участвовавшей в разработке таких стандартов, как IEEE 802.11b,IEEE 802.11a и IEEE 802.11g. В 2003 году Вик ушёл из Agere Systems. Agere Systems не смогла конкурировать на равных в тяжёлых рыночных условиях, несмотря

на то что её продукция занимала нишу дешёвых Wi-Fi решений. 802.11abg all-in-one чипсет от Agere (кодовое имя: WARP) плохо продавался, и Agere Systems решила уйти с рынка Wi-Fi в конце 2004 года.

Стандарт IEEE 802.11n был утверждён 11 сентября 2009 года. Его применение позволяет повысить скорость передачи данных практически вчетверо по сравнению с устройствами стандартов 802.11g (максимальная скорость которых равна 54 Мбит/с), при условии использования в режиме 802.11n с другими устройствами 802.11n. Теоретически 802.11n способен обеспечить скорость передачи данных до 600 Мбит/с. С 2011 по 2013 разрабатывался стандарт IEEE 802.11ac, окончательное принятие стандарта запланировано на начало 2014 года. Скорость передачи данных при использовании 802.11ac может достигать нескольких Гбит/с. Большинство ведущих производителей оборудования уже анонсировали устройства поддерживающие данный стандарт.

27 июля 2011 года Институт инженеров электротехники и электроники (IEEE) выпустил официальную версию стандарта IEEE 802.22. Системы и устройства, поддерживающие этот стандарт, позволят передавать данные на скорости до 22 Мбит/с в радиусе 100 км от ближайшего передатчика.

Термин «Wi-Fi» изначально был придуман как игра слов для привлечения внимания потребителя «намёком» на Hi-Fi (англ. *High Fidelity* – высокая точность). Несмотря на то, что поначалу в некоторых пресс-релизах WECA фигурировало словосочетание «Wireless Fidelity» («беспроводная точность»), на данный момент от такой формулировки отказались, и термин «Wi-Fi» никак не расшифровывается [3].

1.2.2 Принцип работы

Обычно схема Wi-Fi сети содержит не менее одной точки доступа и не менее одного клиента. Также возможно подключение двух клиентов в режиме точка-точка (Ad-hoc), когда точка доступа не используется, а клиенты соединяются посредством сетевых адаптеров «напрямую». Точка доступа передаёт свой идентификатор сети (SSID) с помощью специальных сигнальных пакетов на скорости 0,1 Мбит/с каждые 100 мс. Поэтому 0,1 Мбит/с – наименьшая скорость передачи данных для Wi-Fi. Зная SSID сети, клиент может выяснить, возможно ли подключение к данной точке доступа. При попадании в зону действия двух точек доступа с идентичными SSID приёмник может выбирать между ними на основании данных об уровне сигнала. Стандарт Wi-Fi даёт клиенту полную свободу при выборе критериев для соединения. Более подробно принцип работы описан в официальном тексте стандарта.

Однако, стандарт не описывает всех аспектов построения беспроводных локальных сетей Wi-Fi. Поэтому каждый производитель оборудования решает эту задачу по-своему, применяя те подходы, которые он считает наилучшими с той или иной точки зрения. Поэтому возникает необходимость классификации способов построения беспроводных локальных сетей [4].

По способу объединения точек доступа в единую систему можно выделить:

- Автономные точки доступа (называются также самостоятельные, децентрализованные, умные).
- Точки доступа, работающие под управлением контроллера (называются также «легковесные», централизованные).
- Бесконтроллерные, но не автономные (управляемые без контроллера).

По способу организации и управления радиоканалами можно выделить беспроводные локальные сети:

- Со статическими настройками радиоканалов.
- С динамическими (адаптивными) настройками радиоканалов.
- Со «слоистой» или многослойной структурой радиоканалов.

Преимущества Wi-Fi:

- Позволяет развернуть сеть без прокладки кабеля, что может уменьшить стоимость развёртывания и/или расширения сети. Места, где нельзя проложить кабель, например, вне помещений и в зданиях, имеющих историческую ценность, могут обслуживаться беспроводными сетями.
- Позволяет иметь доступ к сети мобильным устройствам.
- Wi-Fi устройства широко распространены на рынке. Гарантируется совместимость оборудования благодаря обязательной сертификации оборудования с логотипом Wi-Fi.
- Мобильность. Вы больше не привязаны к одному месту и можете пользоваться Интернетом в комфортной для вас обстановке.
- В пределах Wi-Fi зоны в сеть Интернет могут выходить несколько пользователей с компьютеров, ноутбуков, телефонов и т. д.
- Излучение от Wi-Fi устройств в момент передачи данных на порядок (в 10 раз) меньше, чем у сотового телефона.

Недостатки Wi-Fi:

- В диапазоне 2,4 GHz работает множество устройств, таких как устройства, поддерживающие Bluetooth, и др, и дажемикроволновые печи, что ухудшает электромагнитную совместимость.
- Производителями оборудования указывается скорость на L1 (OSI), в результате чего создаётся иллюзия, что производитель оборудования завышает скорость, но на самом деле в Wi-Fi весьма высоки служебные «накладные расходы». Получается, что скорость передачи данных на L2 (OSI) в Wi-Fi сети всегда ниже заявленной скорости на L1 (OSI). Реальная скорость зависит от доли служебного трафика, которая зависит уже от наличия между устройствами физических преград (мебель, стены), наличия помех от других беспроводных устройств или электронной аппаратуры, расположения устройств относительно друг друга и т. п.
- Частотный диапазон и эксплуатационные ограничения в различных странах не одинаковы. Во многих европейских странах разрешены два дополнительных канала, которые запрещены в США; В Японии есть ещё один

канал в верхней части диапазона, а другие страны, например, Испания, запрещают использование низкочастотных каналов. Более того, некоторые страны, например, Россия, Белоруссия и Италия, требуют регистрации всех сетей Wi-Fi, работающих вне помещений, или требуют регистрации Wi-Fi-оператора.

- Как было упомянуто выше – в России точки беспроводного доступа, а также адаптеры Wi-Fi с ЭИИМ, превышающей 100 мВт (20 дБм), подлежат обязательной регистрации.
- Стандарт шифрования WEP может быть относительно легко взломан даже при правильной конфигурации (из-за слабой стойкости алгоритма). Новые устройства поддерживают более совершенные протоколы шифрования данных WPA и WPA2. Принятие стандарта IEEE 802.11i (WPA2) в июне 2004 года сделало возможным применение более безопасной схемы связи, которая доступна в новом оборудовании. Обе схемы требуют более стойкий пароль, чем те, которые обычно назначаются пользователями. Многие организации используют дополнительное шифрование (например, VPN) для защиты от вторжения. На данный момент основным методом взлома WPA2 является подбор пароля, поэтому рекомендуется использовать сложные цифробуквенные пароли для того, чтобы максимально усложнить задачу подбора пароля.
- В режиме точка-точка (Ad-hoc) стандарт предписывает лишь реализовать скорость 11 Мбит/сек (802.11b). Шифрование WPA(2) недоступно, только легко взламываемый WEP.

Коммерческое использование Wi-Fi

Коммерческий доступ к сервисам на основе Wi-Fi предоставляется в таких местах, как Интернет-кафе, аэропорты и кафе по всему миру (обычно эти места называют Wi-Fi-кафе), однако их покрытие можно считать точечным по сравнению с сотовыми сетями:

- Ozone и OzoneParis во Франции. В сентябре 2003 года Ozone начала развёртывание сети OzoneParis через The City of Lights. Конечная цель – создание централизованной сети Wi-Fi, полностью покрывающей Париж. Основной принцип Ozone Pervasive Network заключается в том, что это сеть национального масштаба.
- WiSE Technologies предоставляет коммерческий доступ в аэропортах, университетах, и независимых кафе на территории США.
- T-Mobile обеспечивает работу хот-спотов для сети Starbucks в США и Великобритании, а также более 7500 хот-спотов в Германии.
- Pacific Century Cyberworks обеспечивает доступ в магазинах Pacific Coffee в Гонконге.
- Columbia Rural Electric Association пытается развернуть сеть 2.4 ГГц Wi-Fi на территории площадью 9500 км², расположенной между округами Уалла-Уалла и Колумбия в штате Вашингтон и Юматилла, Орегон. В список других крупных сетей в США также входят: Boingo, Wayport и iPass.

- Sify, индийский Интернет-провайдер, установил 120 точек доступа в Бангалоре: в отелях, галереях и правительственных учреждениях.
- Vex имеет большую сеть хот-спотов, расположенную по всей территории Бразилии. Telefónica Speedy WiFi начала предоставлять свои сервисы в новой растущей сети, распространившейся на территорию штата São Paulo.
- BT Openzone владеет многими хот-спотами в Великобритании, работающими в McDonald's, и имеет роуминговое соглашение с T-Mobile UK и ReadyToSurf. Их клиенты также имеют доступ к хот-спотам The Cloud.
- Netstop обеспечивает доступ в Новой Зеландии.
- В Эстонии имеется несколько коммерческих операторов, крупнейший из них Elion, обеспечивает АЗС Statoil по всей Эстонии и крупные торговые центры.
- Компания Вымпелком, под торговой маркой Билайн, купив Golden Telecom, осуществляет поддержку самой большой в мире городской сети Wi-Fi вМоскве. Каналы доступа к проводной сети обеспечивает крупнейший московский провайдер Корбина Телеком. Развернуты сети и в Московских аэропортах Шереметьево и Домодедово.
- Компания EarthLink планировала в третьем квартале 2007 года полностью подключить Филадельфию (США) к сети Интернет через беспроводные каналы связи. Это должен был быть первый город-мегаполис в США, полностью охваченный Wi-Fi. Предполагаемая стоимость должна была составлять 20–22 доллара в месяц при скорости подключения 1 Мбит/сек. Для малоимущих жителей Филадельфии – 12–15 долларов в месяц. В настоящее время центр города и прилегающие к нему районы уже подключены. Подключение остальных районов будет производиться по мере установки передатчиков.
- Укртелеком на Украине предоставляет услуги Wi-Fi («ОГО! Wi-Fi») по всем городам страны. По замыслу покрытие распространяется не только на центры городов, крупные отели, рестораны, кафе, вокзалы аэропорты, но и на библиотеки, отделения «Телекомсервис» и т. д. В действительности система покрывает только примерно 70 % ресторанов быстрого питания McDonalds, и некоторые другие. Половина из существующих точек часто не активны, либо к ним невозможно подключиться, так как установлены обычные роутеры, которые позволяют подключать не более 11 абонентов.
- Компания SevStar на Украине предоставляет услуги доступа в интернет с помощью технологии Wi-Fi (на частоте 2.4ГГц) на улицах и в заведениях города Севастополя. В городе установлено более 100 точек доступа, позволяющих жителям и гостям города выходить в сеть в любом районе города.
- АИСТ в Одесской области предоставляет доступ к сети Интернет посредством Wi-Fi учебным заведениям, фермерским хозяйствам, населению в частном секторе.
- Белтелеком в Республике Беларусь предоставляет доступ к сети Интернет посредством Wi-Fi под торговой маркой «ByFly» с оплатой по

трафику или поминутно. В каждом городе имеется не менее одной точки доступа, как правило — в отделении почты. В крупных городах, областных центрах имеется множество хот-спотов.

- В Армении в Ереване оператор Orange развернул бесплатную Wi-Fi сеть в общественном транспорте (автобусы) и на остановках ожидания транспорта. Проект запущен в 2011 году.
- Megafon предоставил возможность бесплатно получить доступ к интернету посредством Wi-Fi в аэропорту в Сочи.

2 Безопасность Wi-Fi сетей

2.1 Угрозы Wi-Fi сетям

С точки зрения безопасности, следует учитывать не только угрозы, свойственные проводным сетям, но также и среду передачи сигнала. В беспроводных сетях получить доступ к передаваемой информации намного проще, чем в проводных сетях, равно как и повлиять на канал передачи данных. Достаточно поместить соответствующее устройство в зоне действия сети.

Существует два основных варианта устройства беспроводной сети:

- Ad-hoc – передача напрямую между устройствами.
- Hot-spot – передача осуществляется через точку доступа.

В Hot-spot сетях присутствует точка доступа (англ. *Access point*), посредством которой происходит не только взаимодействие внутри сети, но и доступ к внешним сетям. Hot-spot представляет наибольший интерес с точки зрения защиты информации, т.к., взломав точку доступа, злоумышленник может получить информацию не только со станций, размещенных в данной беспроводной сети [5].

Угрозы информационной безопасности, возникающие при использовании Wi-Fi сетей, можно условно разделить на два класса представлено на рисунке 2.1:

- прямые – угрозы информационной безопасности, возникающие при передаче информации по беспроводному интерфейсу IEEE 802.11;
- косвенные – угрозы, связанные с наличием на объекте и рядом с объектом большого количества Wi-Fi-сетей.

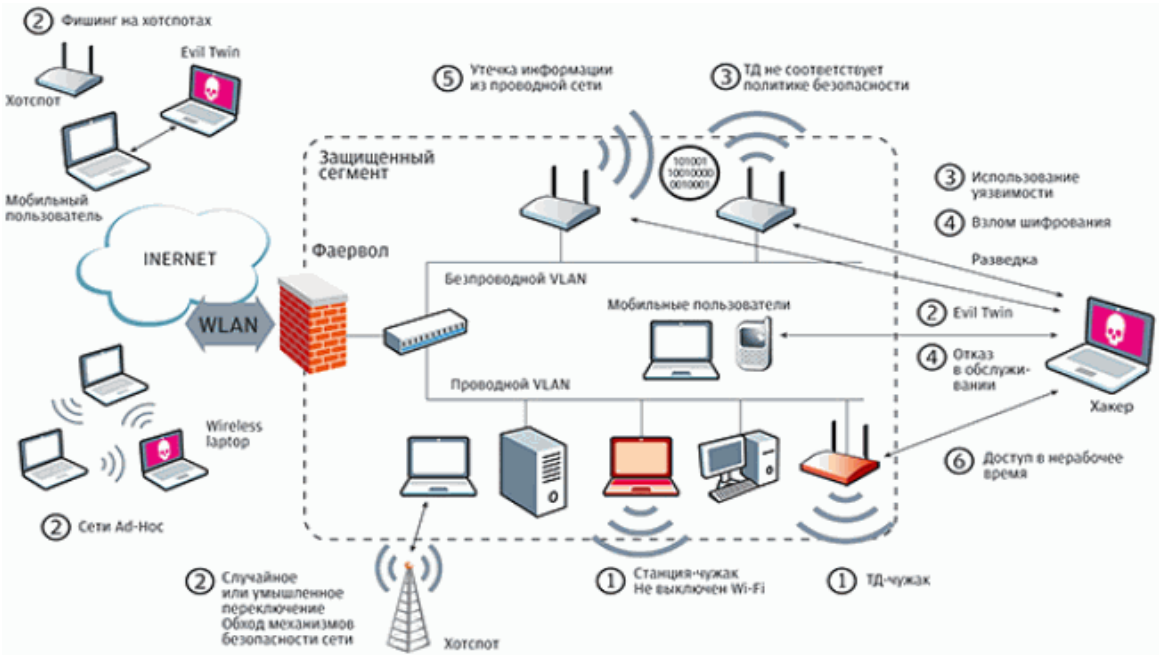

Рисунок 2.1 – Угрозы Wi-Fi сетям

2.2 Прямые угрозы

Радиоканал передачи данных, используемый в Wi-Fi потенциально подвержен вмешательству с целью нарушения конфиденциальности, целостности и доступности информации.

В Wi-Fi предусмотрены как аутентификация, так и шифрование, но эти элементы защиты имеют свои изъяны.

Шифрование значительно снижает скорость передачи данных, и, зачастую, оно осознанно отключается администратором для оптимизации трафика. Первоначальный стандарт шифрования WEP (Wired Equivalent Privacy) был дискредитирован за счёт уязвимостей в алгоритме распределения ключей RC4. Это несколько притормозило развитие Wi-Fi рынка и вызвало создание институтом IEEE рабочей группы 802.11i для разработки нового стандарта, учитывающего уязвимости WEP, обеспечивающего 128-битное AES шифрование и аутентификацию для защиты данных. Wi-Fi Alliance в 2003 представил свой собственный промежуточный вариант этого стандарта - WPA (Wi-Fi Protected Access). WPA использует протокол целостности временных ключей TKIP (Temporal Key Integrity Protocol). Также в нём используется метод контрольной суммы MIC (Message Integrity Code), которая позволяет проверять целостность пакетов. В 2004 Wi-Fi Alliance выпустили стандарт WPA2, который представляет собой улучшенный WPA. Основное различие между WPA и WPA2 заключается в технологии шифрования: TKIP и AES. WPA2 обеспечивает более высокий уровень защиты сети, так как TKIP позволяет создавать ключи длиной до 128 бит, а AES - до 256 бит [6].

Угроза блокирования информации в канале Wi-Fi практически оставлена без внимания при разработке технологии. Само по себе блокирование канала не является опасным, так как обычно Wi-Fi сети являются вспомогательными, однако блокирование может представлять собой лишь подготовительный этап для атаки "человек посередине", когда между клиентом и точкой доступа появляется третье устройство, которое перенаправляет трафик между ними через себя. Такое вмешательство позволяет удалять, искажать или навязывать ложную информацию.

- *Чужаки* – чужаками (RogueDevices, Rogues) называются устройства, предоставляющие возможность неавторизованного доступа к корпоративной сети, обычно в обход механизмов защиты, определенных политикой безопасности. Запрет на использование устройств беспроводной связи не защитит от беспроводных атак, если в сети, умышленно или нет, появится чужак. В роли чужака может выступать всё, у чего есть проводной и беспроводной интерфейсы: точки доступа (включая программные), сканеры, проекторы, ноутбуки с обеими включёнными интерфейсами и т.д.
- *Нефексированная природа связяи* – Беспроводные устройства могут менять точки подключения к сети прямо в процессе работы. Например, могут происходить «случайные ассоциации»,когда ноутбук с Windows XP (доверительно относящейся ко всем беспроводным сетям) или просто

некорректно сконфигурированный беспроводной клиент автоматически ассоциируется и подключает пользователя к ближайшей беспроводной сети. Таким образом нарушитель переключает на себя пользователя для последующего сканирования уязвимостей, фишинга или атак "человек посередине". А если пользователь при этом подключен и к проводной сети, то он становится точной входа - чужаком. К тому же многие пользователи, подключённые к внутренней сети и имеющие Wi-Fi интерфейс, недовольные качеством и политикой работы сети (недостаточная скорость или нельзя выйти ВКонтакт), переключаются на ближайшую доступную точку доступа (или операционная система делает это автоматически при отказе проводной сети). При этом вся защита сети терпит крах.

- *Уязвимость сетей и устройств* – Некорректно сконфигурированные устройства, устройства со слабыми и недостаточно длинными ключами шифрования, использующие уязвимые методы аутентификации - именно такие устройства подвергаются атакам в первую очередь. Согласно отчётам аналитиков, большая часть успешных взломов происходит как раз из-за неправильных настроек точек доступа и программного обеспечения клиента.
- *Некорректно сконфигурированные точки доступа* – Достаточно подключить неправильно настроенную точку доступа к сети для взлома последней. Настройки "по умолчанию" не включают шифрование и аутентификацию, или используют ключи, прописанные в руководстве и поэтому всем известные. Маловероятно, что пользователи достаточно серьёзно озаботятся безопасной конфигурацией устройств. Именно такие привнесённые точки доступа и создают основные угрозы защищённым сетям.
- *Некорректно настроенные устройства пользователей* - угроза опаснее, чем некорректно сконфигурированные точки доступа. Это устройства пользователей, и они не конфигурируются специально в целях безопасности внутренней сети предприятия. К тому же они находятся за периметром контролируемой зоны, так и внутри него, позволяя злоумышленнику проводить всевозможные атаки, как-то распространять вредоносное программное обеспечение или просто обеспечивая удобную точку входа.
- *Взлом шифрования* - О защищённости WEP и речи уже нет. Интернет полон специального и удобного в использовании ПО для взлома этого стандарта, которое собирает статистику трафика до тех пор, пока её не станет достаточно для восстановления ключа шифрования. Стандарты WPA и WPA2 также имеют ряд уязвимостей разной степени опасности, позволяющих их взлом. Пока что нет информации об успешных атаках на WPA2-Enterprise (802.1x).
- *Имперсонация* – Имперсонация авторизованного пользователя – серьезная угроза любой сети, не только беспроводной. Однако в беспроводной сети определить подлинность пользователя сложнее. Конечно, существуют SSID и можно пытаться фильтровать по MAC-адресам, но и то и другое передается в эфире в открытом виде, и их несложно подделать, а подделав – как минимум снизить пропускную способность сети, вставляя неправильные кадры,

а разобравшись в алгоритмах шифрования – устраивать атаки на структуру сети (например, ARP-spoofing). Имперсонация пользователя возможна не только в случае MAC-аутентификации или использования статических ключей. Схемы на основе 802.1x не являются абсолютно безопасными. Некоторые механизмы (LEAP) имеют сложность взлома схожую со взломом WEP. Другие механизмы, EAP-FAST или PEAP-MSCHAPv2 хотя и надёжнее, но не гарантируют устойчивость к комплексной атаке.

- *Отказы в обслуживании* – DoS атаки направлены на нарушение качества функционирования сети или на абсолютное прекращение доступа пользователей. В случае Wi-Fi сети отследить источник, заваливающий сеть "мусорными" пакетами, крайне сложно - его местоположение ограничивается лишь зоной покрытия. К тому же есть аппаратный вариант этой атаки – установка достаточно сильного источника помех в нужном частотном диапазоне.

2.3 Косвенные угрозы

Сигналы Wi-Fi устройств имеют достаточно сложную структуру и широкий спектр, поэтому эти сигналы, а тем более, окружающие устройства Wi-Fi невозможно идентифицировать обычными средствами радиомониторинга. Уверенное обнаружение сигнала WiFi современными комплексами радиомониторинга в широкой полосе частот возможно только по энергетическому признаку при наличии полос параллельного анализа шириной несколько десятков МГц на скорости не менее 400 МГц/с и лишь в ближней зоне. Сигналы точек доступа, находящихся в дальней зоне, оказываются ниже уровня шумов приёмника. Обнаружение Wi-Fi-передатчиков при последовательном сканировании узкополосными приёмниками вообще невозможно.

Исходя из того, что практически каждый объект окружает множество "чужих" Wi-Fi сетей, отличить легальных клиентов своей сети и соседних сетей от нарушителей крайне сложно, что позволяет успешно маскировать несанкционированную передачу информации среди легальных Wi-Fi-каналов.

Wi-Fi-передатчик излучает так называемый «OFDM сигнал». Это означает, что в один момент времени устройство передаёт в одном сигнале, занимающем широкую полосу частот (около 20 МГц) несколько несущих информацию - поднесущих информационных каналов, которые расположены так близко друг от друга, что при приёме их на обычном приёмном устройстве, сигнал выглядит как единый «купол». Выделить в таком «куполе» поднесущие и идентифицировать передающие устройства можно только специальным приёмником.

В крупных городах Wi-Fi сети общего пользования имеют достаточно обширную зону покрытия, чтобы отпала необходимость использовать мобильный пункт приёма информации рядом с объектом - несанкционированное устройство может подключиться к доступной Wi-Fi сети

и использовать её для передачи информации через Интернет в любое требуемое место.

Пропускная способность Wi-Fi сетей позволяет передавать звук и видео в реальном времени. Это упрощает злоумышленнику использовать акустические и оптические каналы утечки информации - достаточно легально купить Wi-Fi-видеокамеру и установить её в качестве устройства негласного получения информации.

Примеры:

1 С Wi-Fi видеокамеры с микрофоном информация передаётся на точку доступа, работающую в режиме ретранслятора. Точка расположена на крыше и имеет направленную антенну — таким образом можно значительно увеличить дальность сигнала — до нескольких километров. Сам сигнал принимается на контрольном пункте.

2 Смартфон сотрудника с помощью вируса записывает окружающий звук и передаёт его злоумышленнику с помощью Wi-Fi. В качестве контрольного пункта используется точка доступа со скрытым именем, чтобы обнаружить её было труднее.

3 Если на объекте ограничен вынос носителей информации и выход в Интернет ограничен, то одним из вариантов скрытой передачи большого объёма информации является Wi-Fi. Нужно подключиться к соседним Wi-Fi сетям, оставаясь незамеченным среди легальных пользователей.

Утечки информации из проводной сети - Как правило беспроводные сети соединяются с проводными. Значит через точку доступа можно атаковать проводную сеть. А если наличествуют ошибки в настройке как проводной, так и беспроводной сети, то открывается целый плацдарм для атак. Пример - точки доступа, работающие в режиме моста (Layer 2 Bridge), подключённые в сеть без маршрутизаторов или в сеть с нарушением сегментации и передающие в радиоэфир широковещательные пакеты из проводной части сети (ARP-запросы, DHCP, кадры STP и д.р.). Эти данные в целом полезны для разведки, и на их основе можно проводить такие атаки, как "человек посередине", атаки отказа в обслуживании, отравление кеша DNS и др.

Другой пример - при наличии нескольких ESSID (Extended Service Set Identifier) на одной точке доступа. Если на такой точке настроена как защищённая сеть, так и публичная, при неправильной конфигурации широковещательные пакеты будут отправляться в обе сети. Это позволит злоумышленнику, например, нарушить работу DHCP или ARP в защищённом сегменте сети. Это можно запретить, организовав привязку ESS к BSS, что поддерживается практически всеми производителями оборудования класса Enterprise (и мало кем из класса Consumer).

Интерференция

Качество работы Wi-Fi сети как радиоэфира зависит от многих факторов. Один из них - интерференция радиосигналов, которая может значительно снизить пропускную способность сети и количество пользователей, вплоть до полной невозможности использования сети. В качестве источника может

выступать любое устройство, излучающее на той же частоте сигнал достаточной мощности. Это могут быть как соседние точки доступа, так и микроволновки. Эту особенность могут также использовать злоумышленники в качестве атаки отказа в обслуживании, или для подготовки атаки "человек посередине", заглушая легитимные точки доступа и оставляя свою с таким же SSID.

Существуют и другие особенности беспроводных сетей помимо интерференции. Неправильно настроенный клиент или сбоящая антенна могут ухудшить качество обслуживания всех остальных пользователей. Или вопрос стабильности связи. Не только сигнал точки доступа должен достичь клиента, но и сигнал клиента должен достичь точки. Обычно точки мощнее, и чтобы добиться симметрии, возможно придётся снизить мощность сигнала. Для 5 ГГц следует помнить, что надежно работают только 4 канала: 36/40/44/48 (для Европы, для США есть еще 5). На остальных включен режим сосуществования с радарами (DFS). В итоге, связь может периодически пропадать.

3 Проектирование сети для СПбГБУК «СПбГБСС».

3.1 Стандарт беспроводной связи

Для коммуникации в беспроводной локальной сетевой зоне частотных диапазонов 0,9; 2,4; 3,6 и 5 ГГц применяется набор стандартов IEEE 802.11.

Изначально стандарт IEEE 802.11 предполагал возможность передачи данных по радиоканалу на скорости не более 1 Мбит/с и, опционально, на скорости 2 Мбит/с. Один из первых высокоскоростных стандартов беспроводных сетей –IEEE 802.11a –определяет скорость передачи уже до 54 Мбит/с брутто. Рабочий диапазон стандарта – 5 ГГц.

Вопреки своему названию, принятый в 1999 году стандарт IEEE 802.11b не является продолжением стандарта 802.11a, поскольку в них используются различные технологии: DSSS (точнее, его улучшенная версия HR-DSSS) в 802.11b против OFDM в 802.11a. Стандарт предусматривает использование нелицензируемого диапазона частот 2,4 ГГц. Скорость передачи до 11 Мбит/с.

Продукты стандарта IEEE 802.11b, поставляемые разными изготовителями, тестируются на совместимость и сертифицируются организацией Wireless Ethernet Compatibility Alliance (WECA), которая в настоящее время больше известна под названием Wi-Fi Alliance. Совместимые беспроводные продукты, прошедшие испытания по программе «Альянса Wi-Fi», могут быть маркированы знаком Wi-Fi [7].

Долгое время IEEE 802.11b был распространённым стандартом, на базе которого было построено большинство беспроводных локальных сетей. Сейчас его место занял стандарт IEEE 802.11g, постепенно вытесняемый высокоскоростным IEEE 802.11n.

Проект стандарта IEEE 802.11g был утверждён в октябре 2002 г. Этот стандарт предусматривает использование диапазона частот 2,4 ГГц, обеспечивая скорость соединения до 54 Мбит/с (брутто) и превосходя, таким образом, стандарт IEEE 802.11b, который обеспечивает скорость соединения до 11 Мбит/с. Кроме того, он гарантирует обратную совместимость со стандартом 802.11b. Обратная совместимость стандарта IEEE 802.11g может быть реализована в режиме модуляции DSSS, и тогда скорость соединения будет ограничена одиннадцатью мегабитами в секунду либо в режиме модуляции OFDM, при котором скорость может достигать 54 Мбит/с. Таким образом, данный стандарт является наиболее приемлемым при построении беспроводных сетей. На рисунке 3.1 можно наглядно проследить эволюцию стандартов 802.11.

Сеть, проектируемая в данном дипломном проекте будет построена на стандарте 802.11ac.

EEE 802.11ac – стандарт беспроводных локальных сетей, работающий на частотах 5–6 ГГц.

Стандарт позволяет существенно расширить пропускную способность сети, начиная от 3000 Мбит/с и до 10 Гбит/с при 8x MU-MIMO-антеннах. Это наиболее существенное нововведение относительно IEEE 802.11n. Кроме того, ожидается снижение энергопотребления, что, в свою очередь, продлит время автономной работы мобильных устройств (Рисунок 3.1).

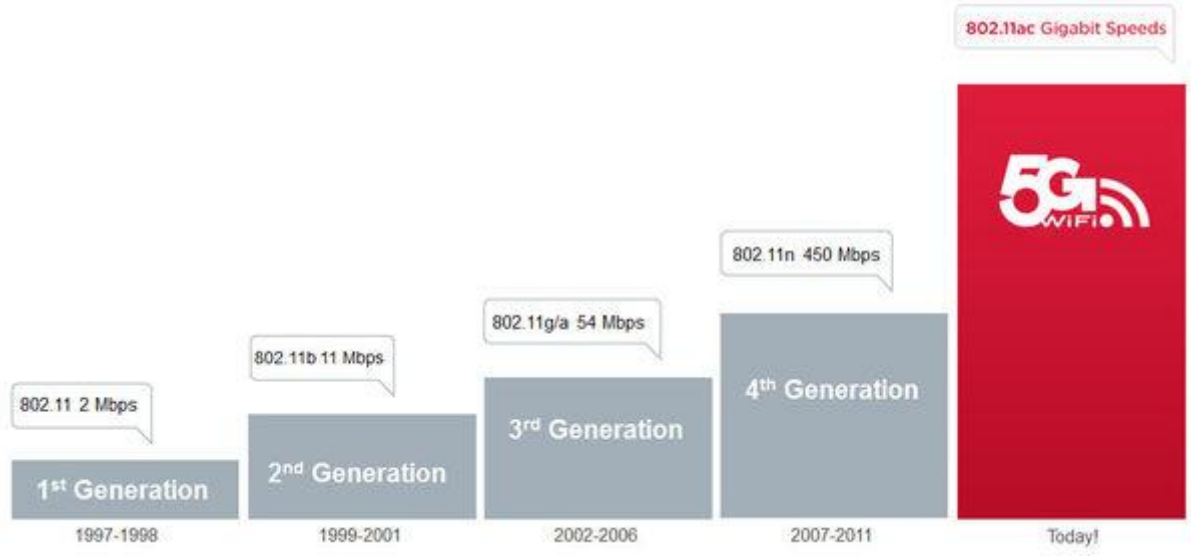

Рисунок 3.1 – Стандарты 802.11

20 января 2011 года была принята первая черновая редакция версии 0.1. 1 февраля 2013 года принята черновая редакция версии 5.0 (завершено на 95 %). 4 апреля 2013 года обновлена черновая редакция версии 5.0 (завершено на 96 %).

На апрель 2013 года некоторыми производителями (Quantenna, Broadcom, Buffalo, D-Link, Cisco) уже представлены чипы, поддерживающие работу по стандарту IEEE 802.11ac Draft 0.1, а также выпущены на рынок устройства, поддерживающие черновой вариант данного стандарта.

Принятие финальной версии спецификации 802.11ac состоялось в январе 2014 года.

Дебютировал на представленных в 2013 году компьютерах Mac и маршрутизаторах компании Apple. Первым мобильным устройством с поддержкой данного стандарта является Motorola Moto X.

Выбор данного стандарта, для проектировки сети обусловлен множеством причин:

– Возросшая скорость передачи данных (более высокая скорость обеспечивает большее удобство для пользователей).

– Возросшая чувствительность сети (чувствительность у клиентов и точек доступа возросла, а значит, для успешной работы и достижения более высоких скоростей не потребуется увеличивать площадь покрытия сети).

– Возросшая емкость сети (побочный эффект повышенной скорости – для передачи того же объема данных требуется меньшее время).

3.2 Роуминг в сетях Wi-Fi

Роумингом называется процесс переподключения устройства к беспроводной сети при перемещении его в пространстве. Принимаемая мощность радиосигнала ослабевает с расстоянием до передатчика, в результате чего падает эффективная скорость передачи информации, растут канальные ошибки вплоть до обрыва беспроводного соединения. При наличии в радио-сети с одним именем (SSID) более чем одной точки доступа перемещение мобильного абонента из зоны уверенной работы в пределах первой точки доступа в зону, где сигнал от второй точки доступа качественнее (выше мощность, больше отношение сигнал/шум) может произойти такое переподключение.

Решение об осуществлении переподключения **всегда** принимает клиентское устройство (драйвер Wi-Fi адаптера). Точка доступа может только «подсказать» устройству о желательности данного действия. Иногда можно указать в настройках драйвера параметр «агрессивности» принятия решения. Однако при первоначальном подключении абонента централизованно управляемая система может «заставить» абонента подключиться к предпочтительной (с точки зрения загрузки) точке, и на желаемом канале/диапазоне [8].

Бесшовным называют такой механизм роуминга, при котором потери передаваемых данных, возникающие в момент переключения с точки на точку, минимальны либо равны нулю, а стек TCP/IP клиентской операционной системы даже не замечает факт переключения. Такой механизм важен при эксплуатации чувствительных к задержкам и потерям приложений, таких как передача голоса по радиосети (Voice over Wireless), потокового видео, больших объемов данных и вообще всех случаев, где протокол TCP не в состоянии «переварить» временное пропадание канала передачи данных.

Для осуществления роуминга необходимо наличие контроллера беспроводных сетей. Данный контроллер может быть встроен в точку доступа (такое часто практикуют специалисты компании Zyxel) или в коммутатор (решения от Cisco, D-Link и т.д) или же подключен отдельным устройством. Принцип осуществления Wi-Fi роуминга можно понять по рисунку 3.2.

Для реализации роуминга в сети СПбГБУК «СПбГБСС» будет применен способ, когда контроллер беспроводных точек доступа уже встроен в коммутатор. Для этих целей отлично подойдет коммутатор компании D-Link DWS–3024 (Описание его технических характеристик представлено в приложении Б). Вместе с ним будут работать беспроводные точки доступа Asus RT-AC68U (Технические характеристики описаны в приложении В).

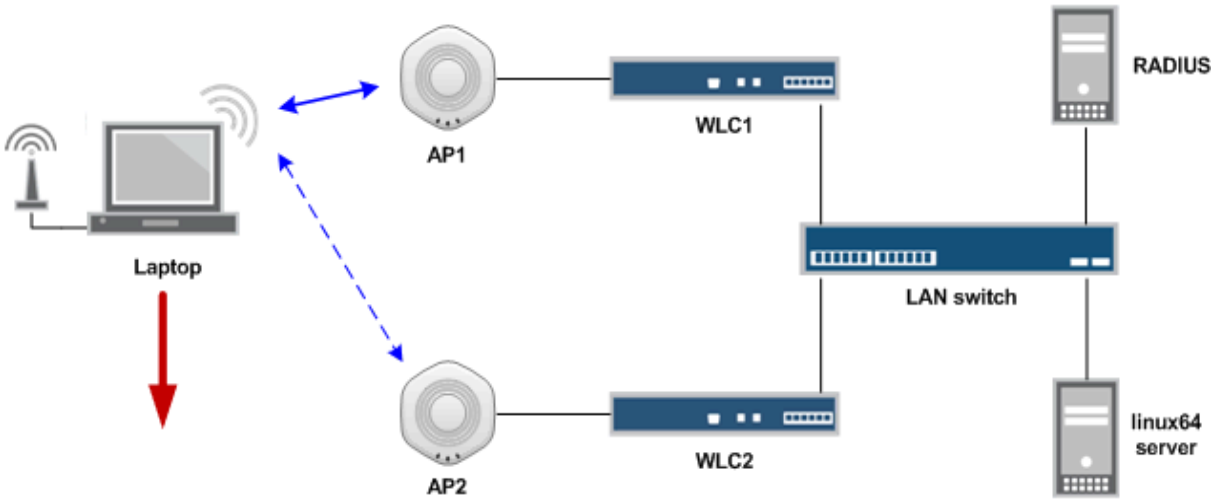

Рисунок 3.2 – Принцип осуществления Wi-Fi роуминга

3.3 Топология сети

В данной сети имеется 4 точки доступа Asus RT-AC68U, 3 из которых работают в режиме точки доступа, а последняя в режиме беспроводного маршрутизатора. Имеется основной маршрутизатор Cisco 1941 коммутатор D-link DWS-3024 со встроенным контроллером беспроводных сетей. С топологией сети можно ознакомиться по рисунку 3.3 (кол-во конечных устройств снижено, чтобы не засорять схему).

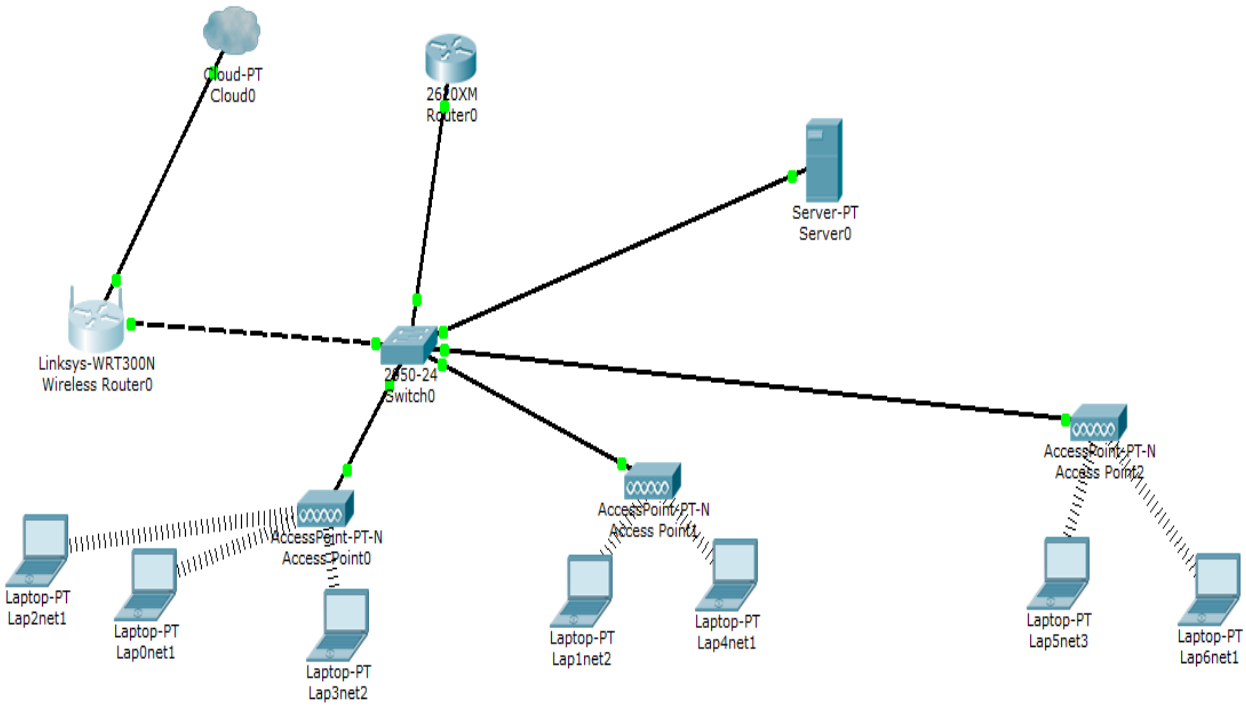

Рисунок 3.3 – Топология сети СПбГБУК «СПбГБСС»

Расчеты по проектированию сети проводились в программе TamoGraph Site Survey. Подробная схема этажей здания представлена в приложении А.

На основании расчетов и исходя из практической целесообразности точки доступа решено разместить на втором этаже здания. Так как точки доступа работают в режиме 5GHz (стандарт IEEE 802.11ac) а в качестве перекрытия использовано дерево, то затухание сигнала при преодолении легкого перекрытия для сигнала 5.0 GHz составляет 23dB, отражение – 7%. На основании данных результатов мы можем получить следующие результаты уровня сигнала (рисунок 3.4 – 3.6).

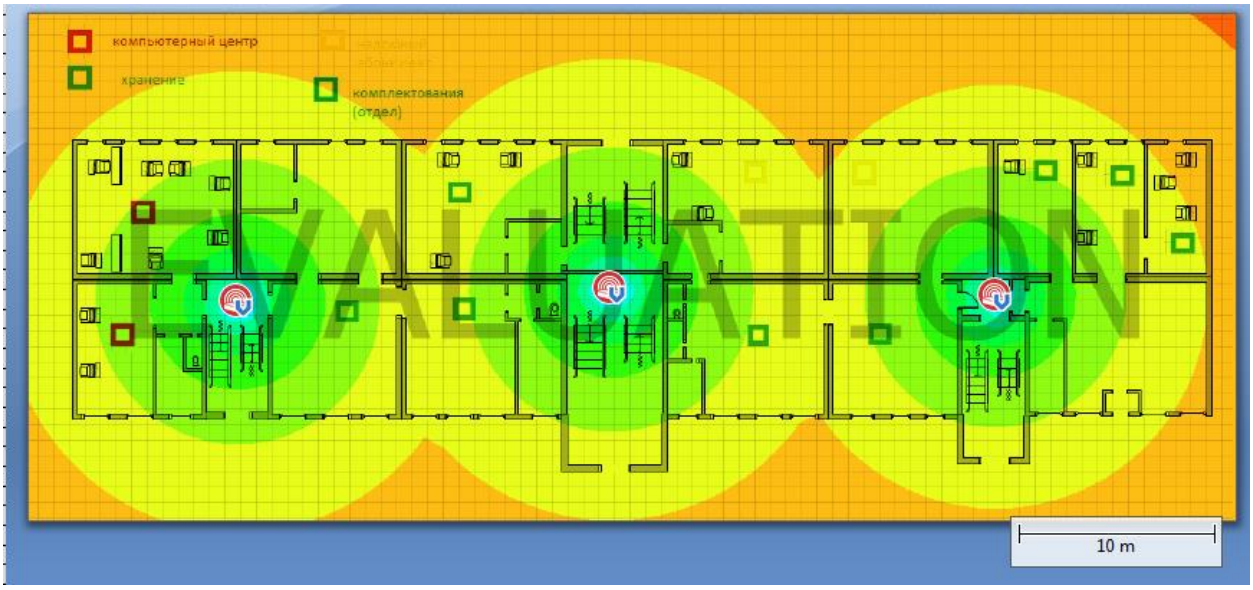

Рисунок 3.4 – Уровень сигнала на первом этаже здания

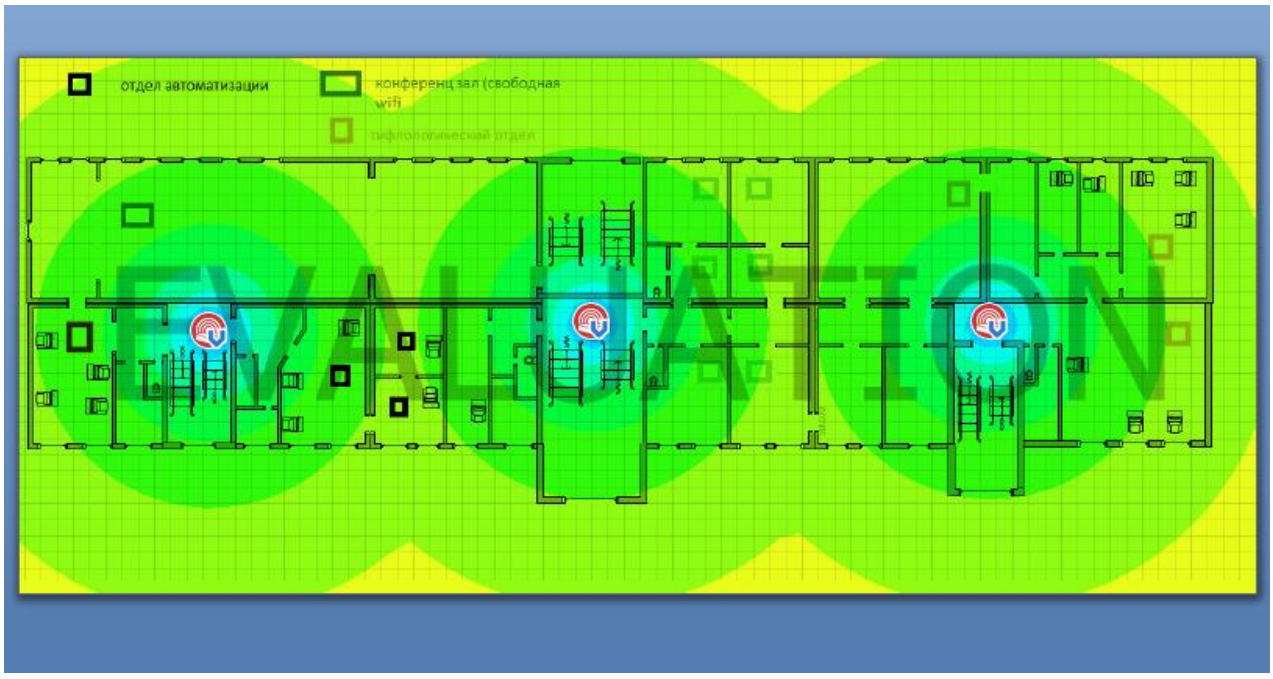

Рисунок 3.5 – Уровень сигнала на втором этаже здания

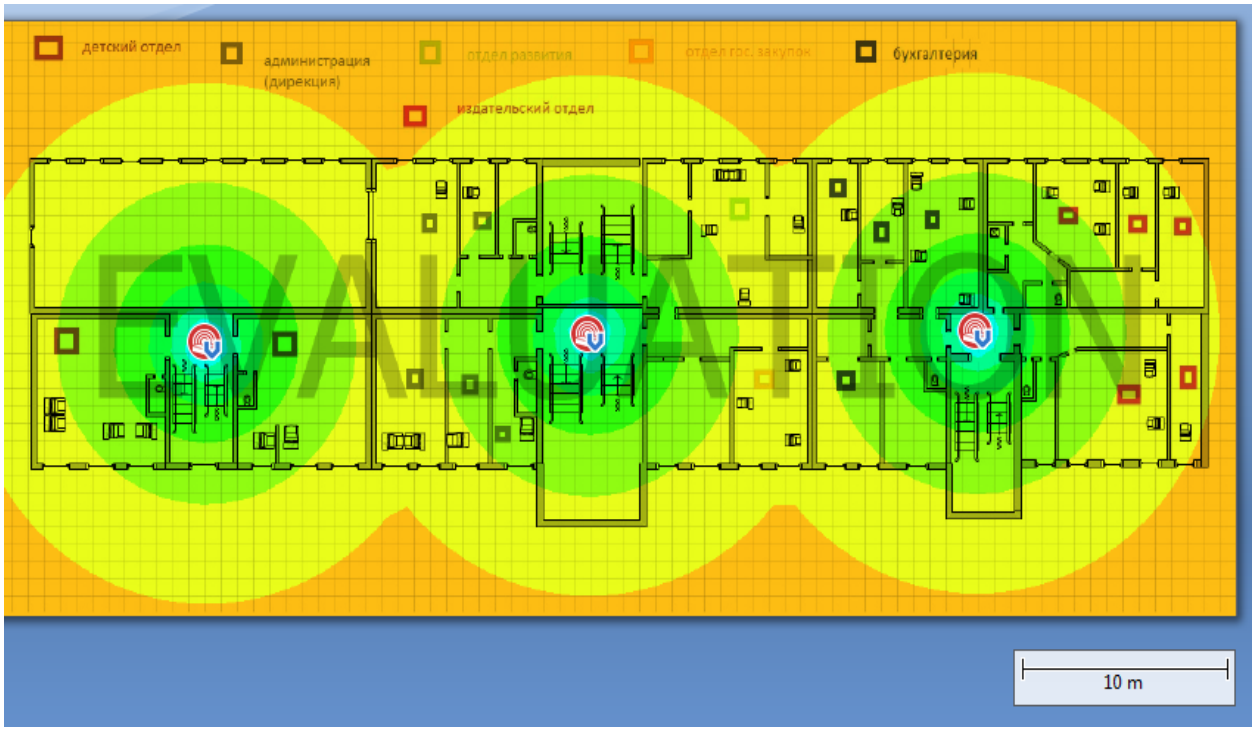

Рисунок 3.6 – Уровень сигнала на третьем этаже здания.

При этом скорости передачи данных можно наглядно увидеть на рисунках 3.7 – 3.9, где скорость изменяется от одного 1Mbps при красном спектре до 600Mbps при синих оттенках.

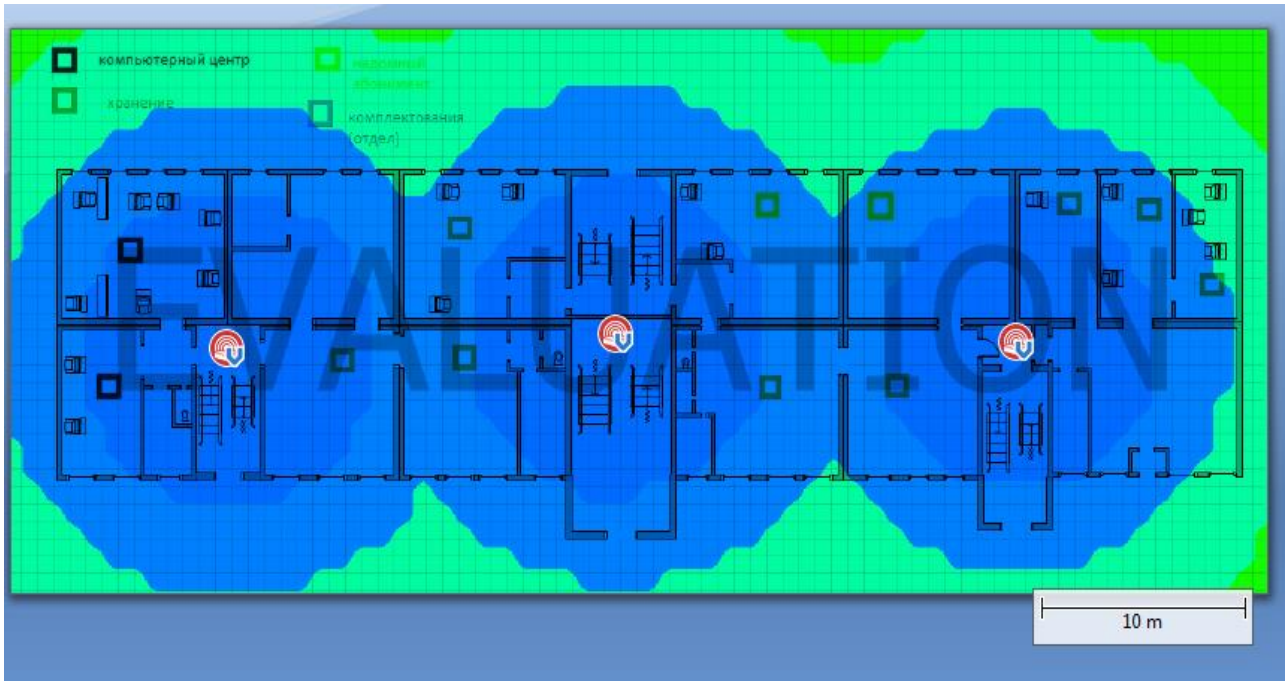

Рисунок 3.7 – Ожидаемая скорость на первом этаже

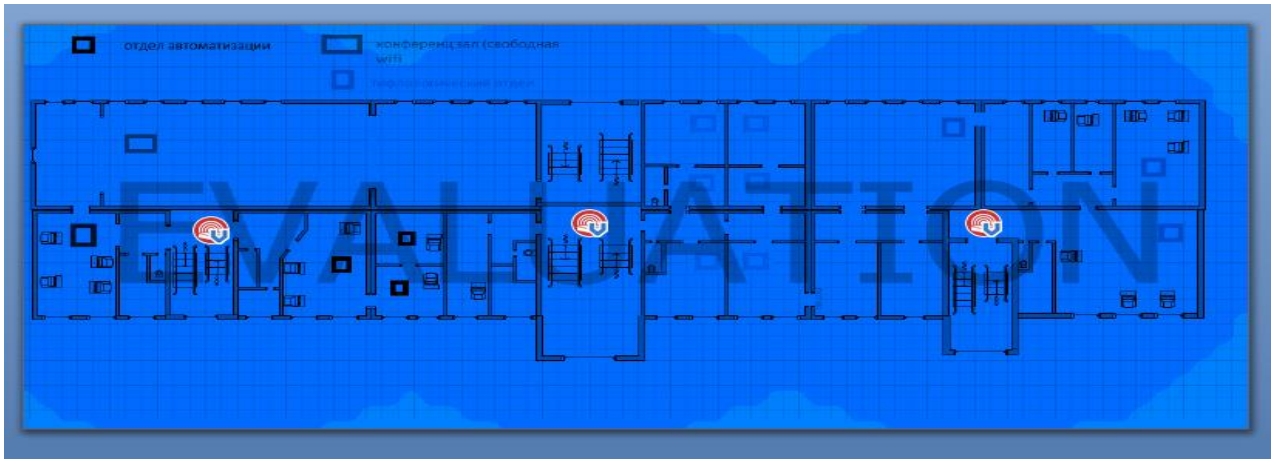

Рисунок 3.8 – Ожидаемая скорость на втором этаже здания

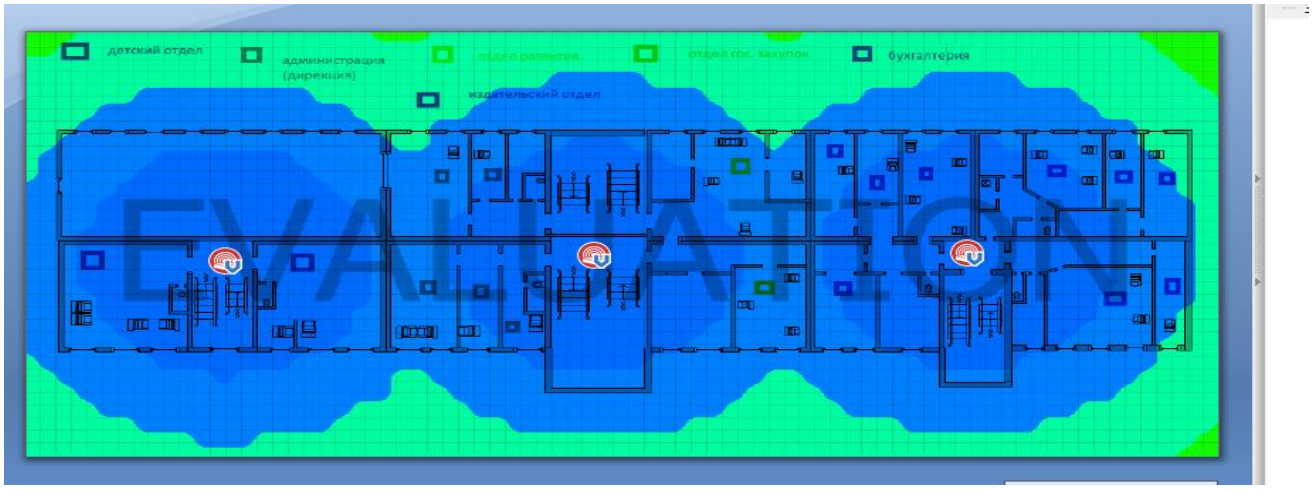

Рисунок 3.9 – Ожидаемая скорость на третьем этаже здания

Отношение сигнала к шуму проиллюстрировано на рисунках 3.10 – 3.12.

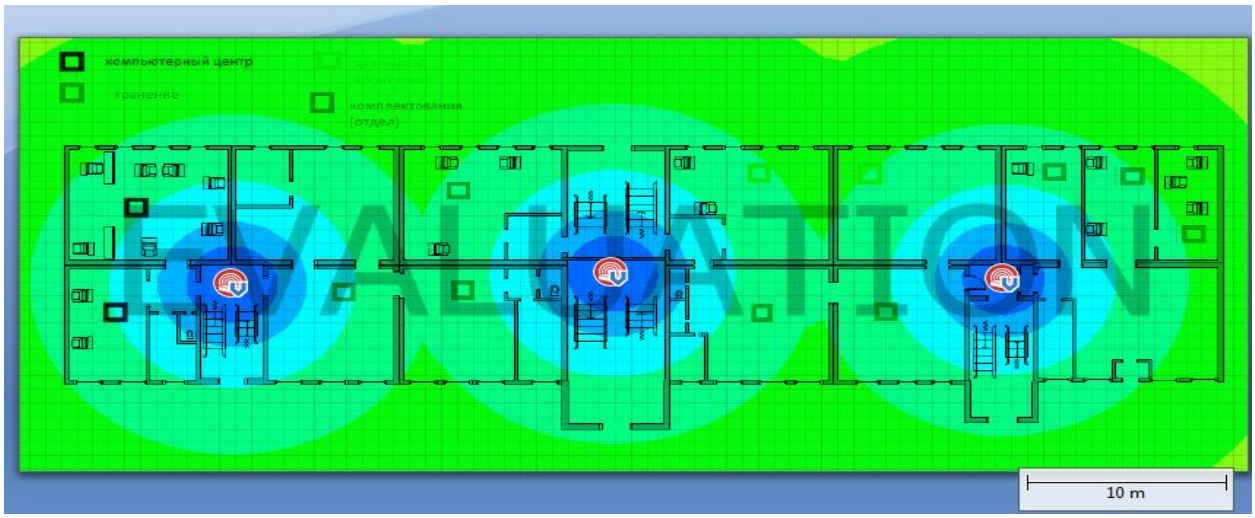

Рисунок 3.10 – Отношение сигнал/шум для первого этажа

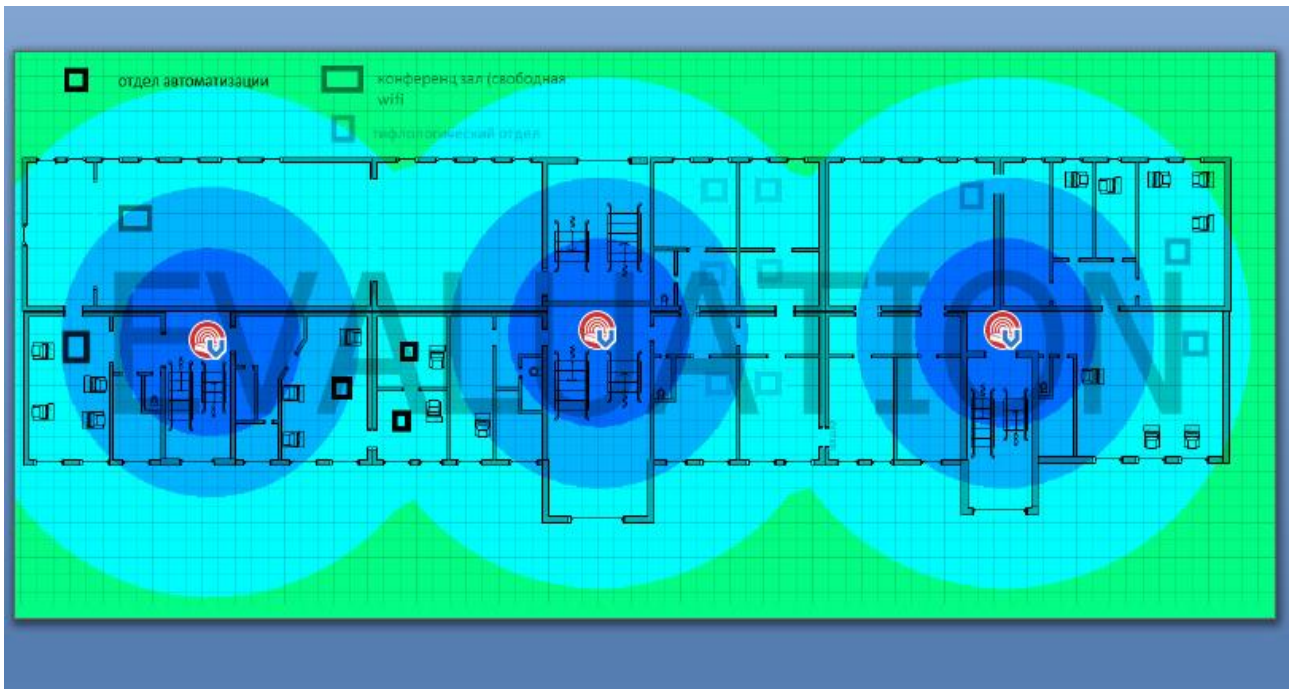

Рисунок 3.11 – Отношение сигнал/шум для второго этажа здания

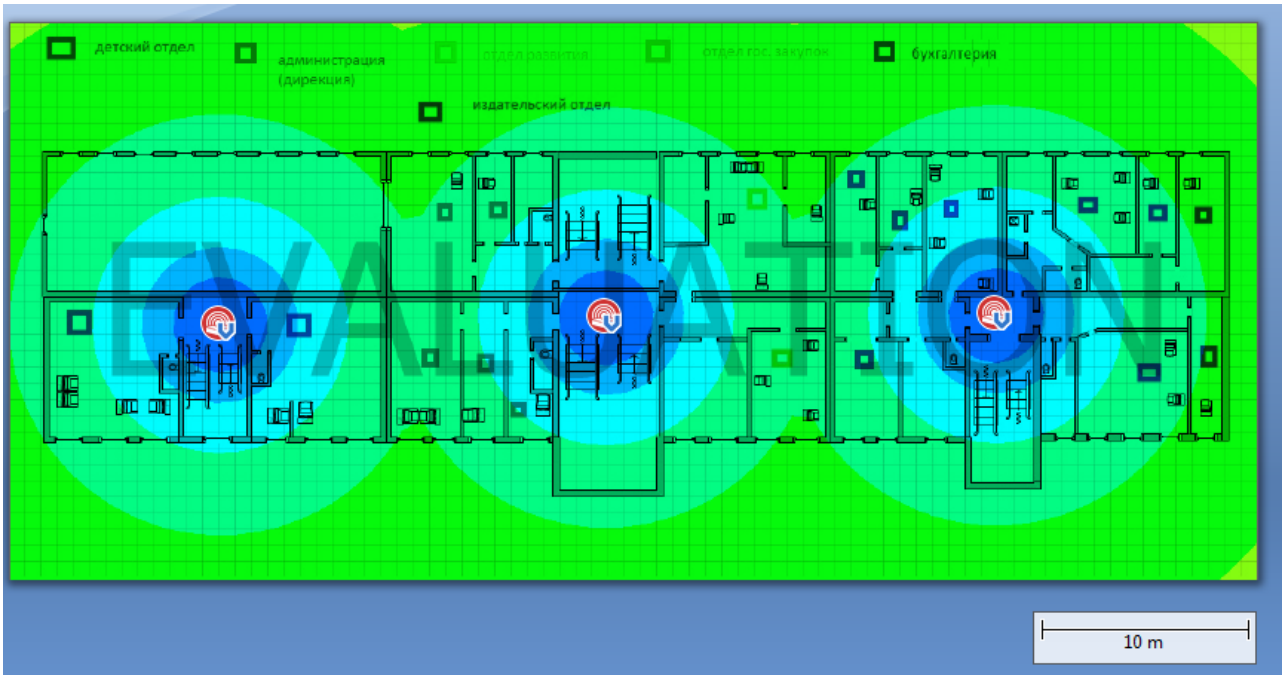

Рисунок 3.12 – Отношение сигнал/шум для третьего этажа здания

Ширина канала для всех этажей будет одинакова и составлять 40 MHz для первой и третьей точки и 80 MHz для второй (рисунок 3.13)

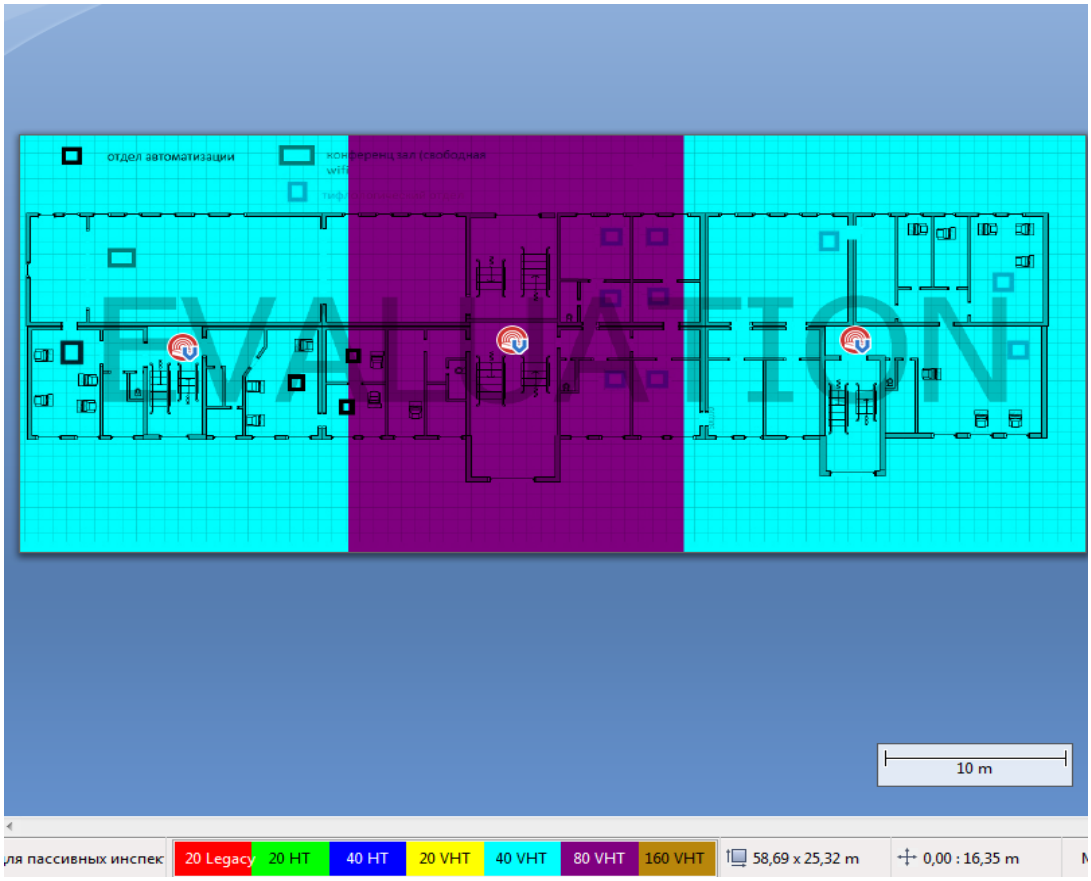

Рисунок 3.13 – Ширина канала связи

3.4 Клиентские адаптеры для подключения к сети

Для подключения к сети конечных пользователей будут использоваться внутренние адаптеры беспроводных сетей Asus PCE-AC68 (рисунок 3.14). Технические характеристики данных адаптеров представлены в приложении Г.

Данный адаптер устанавливается в PCI-Ex1 разъем материнской платы. Материнская плата должна обладать данным типом разъема (PCI-Ex1) или, необходимо воспользоваться переходником с других видов разъемов. Внешние антенны (3x3:3) можно либо напрямую подключить к разъёмам RP-SMA на плате, либо же воспользоваться треугольной подставкой с мощным магнитным основанием. К плате подставка подключается толстым кабелем длиной около метра. Такой тип подключения будет оправдан в местах с наименьшим уровнем сигнала.

Рисунок 3.14 – Адаптер беспроводных сетей Asus PCE-AC68 с внешними антеннами на выносной подставке

3.5 IP адресация в сети СПбГБУК «СПбГБСС»

В данной организации существует 12 отделов, с максимальным числом компьютеров 10 ед. в каждом отделе. Также есть конференц-зал, который является самостоятельным отделом и сетевое оборудование (сервера, маршрутизаторы и прочее) сгруппировано в отдел. В приложении А есть план здания с отмеченными на нем отделами. Диапазон ip адресов представлен в таблице 3.1. Маска подсети во всех случаях 255.255.255.0.

Запрет на получения доступа между компьютерами разных отделов осуществлен на основе ACL списков (пример представлен в приложении Д).

Т а б л и ц а 3.1 – Ip адресация

№ отдела	Название Отдела	Начальный Ip	Конечный Ip	№ точки доступа
1	Администрация	171.71.1.2	171.71.1.10	2
2	Бухгалтерия	171.71.1.11	171.71.1.20	3

Окончание таблицы 3.1

№ отдела	Название Отдела	Начальный Ip	Конечный Ip	№ точки доступа
3	Автоматизации	171.71.1.21	171.71.1.30	1
4	Компьютерный центр	171.71.1.31	171.71.1.50	1
5	Хранения	171.71.1.51	171.71.1.60	1,2,3
6	Надомный абонемент	171.71.1.61	171.71.1.70	2,3
7	Комплектования	171.71.1.71	171.71.1.90	2
8	Тифлологический	171.71.1.91	171.71.1.100	3
9	Детский	171.71.1.101	171.71.1.110	1
10	Развития	171.71.1.111	171.71.1.120	2
11	Гос. закупок	171.71.1.121	171.71.1.130	2
12	Издательский	171.71.1.131	171.71.1.140	3
13	Конференц-зал	171.71.1.141	171.71.1.160	4
14	Сетевое оборудование	171.71.1.201	171.71.1.220	-

3.6 ACL списки

ACL (Access Control List) — это набор текстовых выражений, который позволяет что-либо разрешить или запретить. Чаще всего ACL запрещают Ip пакеты, но они также могут просматривать содержимое этих пакетов, порты и прочее. Также возможно приметь ACL для различных сетевых протоколов и прочего [9].

ACL подразделяются на два типа:

– Стандартный (standard), позволяет проверять только адреса источников.

– Расширенный (Extended), позволяет проверять адреса источников, получателей, типы портов и виды протоколов.

Обозначаются ACL либо номером, либо символьным именем, причем, для стандартных ACL номера можно задавать в диапазоне от 1 до 99, а для расширенных – от 100 до 199 [10].

ACL список создается отдельно, причем порядок строк имеет очень важное значение. Строки, записанные раньше – имеют больший приоритет. Например, если мы запишем так:

```
Router(config-ext-nacl)#  permit  ip  host  171.71.1.11  host
171.71.1.12
Router(config-ext-nacl)#deny ip host 171.71.1.11 any
```

То хост с адресом 171.71.1.11 будет иметь доступ до хоста 171.71.1.12 и больше ни до какого. Если же изменить порядок строк – вот так:

```
Router(config-ext-nacl)#deny ip host 171.71.1.11 any
Router(config-ext-nacl)#permit    ip    host    171.71.1.11    host
171.71.1.12
```

То хост 171.71.1.11 вообще не будет иметь доступа к каким-либо хостам.

В данной сети находится около 100 хостов для примера будет рассмотрен ACL лист для 8 ПК, расположенных в 3х отделах. Это хосты 171.71.1.11, 171.71.1.12, 171.71.1.13, 171.71.1.14 из первого отдела, 171.71.1.21, 171.71.1.22 из второго, 171.71.1.33, 171.71.1.34 из третьего.

Вход в привилегированный режим:

```
Router>en
```

Вход в режим настройки маршрутизатора:

```
Router#conf t
```

Создание ACL списка 112:

```
Router(config)#ip access-list extended 112
```

Разрешения для хоста 171.71.1.11

```
Router(config-ext-nacl)#permit    ip    host    171.71.1.11    host
171.71.1.12
Router(config-ext-nacl)#permit    ip    host    171.71.1.11    host
171.71.1.13
Router(config-ext-nacl)#permit    ip    host    171.71.1.11    host
171.71.1.14
Router(config-ext-nacl)#permit    ip    host    171.71.1.11    host
171.71.1.15
Router(config-ext-nacl)#permit    ip    host    171.71.1.11    host
171.71.1.16
Router(config-ext-nacl)#permit    ip    host    171.71.1.11    host
171.71.1.17
Router(config-ext-nacl)#permit    ip    host    171.71.1.11    host
171.71.1.18
Router(config-ext-nacl)#permit    ip    host    171.71.1.11    host
171.71.1.19
Router(config-ext-nacl)#permit    ip    host    171.71.1.11    host
171.71.1.20
Router(config-ext-nacl)#permit ip host 171.71.1.11 host 171.71.1.1
Router(config-ext-nacl)#permit ip host 171.71.1.11 host 171.71.1.2
Router(config-ext-nacl)#permit ip host 171.71.1.11 host 171.71.1.3
Router(config-ext-nacl)#permit ip host 171.71.1.11 host 171.71.1.4
Router(config-ext-nacl)#permit ip host 171.71.1.11 host 171.71.1.4
Router(config-ext-nacl)#permit ip host 171.71.1.11 host 171.71.1.5
```

```
Router(config-ext-nacl)#permit ip host 171.71.1.11 host 171.71.1.6
Router(config-ext-nacl)#permit ip host 171.71.1.11 host 171.71.1.7
Router(config-ext-nacl)#permit ip host 171.71.1.11 host 171.71.1.8
Router(config-ext-nacl)#permit ip host 171.71.1.11 host 171.71.1.9
Router(config-ext-nacl)#permit    ip    host    171.71.1.11    host
171.71.1.10
Router(config-ext-nacl)#deny ip host 171.71.1.11 any
```

Разрешение для хоста 171.71.1.12

```
Router(config-ext-nacl)#permit    ip    host    171.71.1.12    host
171.71.1.11
Router(config-ext-nacl)#permit    ip    host    171.71.1.12    host
171.71.1.13
Router(config-ext-nacl)#permit    ip    host    171.71.1.12    host
171.71.1.14
Router(config-ext-nacl)#permit    ip    host    171.71.1.12    host
171.71.1.15
Router(config-ext-nacl)#permit    ip    host    171.71.1.12    host
171.71.1.16
Router(config-ext-nacl)#permit    ip    host    171.71.1.12    host
171.71.1.17
Router(config-ext-nacl)#permit    ip    host    171.71.1.12    host
171.71.1.18
Router(config-ext-nacl)#permit    ip    host    171.71.1.12    host
171.71.1.19
Router(config-ext-nacl)#permit    ip    host    171.71.1.12    host
171.71.1.20
Router(config-ext-nacl)#permit ip host 171.71.1.12 host 171.71.1.1
Router(config-ext-nacl)#permit ip host 171.71.1.12 host 171.71.1.2
Router(config-ext-nacl)#permit ip host 171.71.1.12 host 171.71.1.3
Router(config-ext-nacl)#permit ip host 171.71.1.12 host 171.71.1.4
Router(config-ext-nacl)#permit ip host 171.71.1.12 host 171.71.1.5
Router(config-ext-nacl)#permit ip host 171.71.1.12 host 171.71.1.6
Router(config-ext-nacl)#permit ip host 171.71.1.12 host 171.71.1.7
Router(config-ext-nacl)#permit ip host 171.71.1.12 host 171.71.1.8
Router(config-ext-nacl)#permit ip host 171.71.1.12 host 171.71.1.9
Router(config-ext-nacl)#permit    ip    host    171.71.1.12    host
171.71.1.10
Router(config-ext-nacl)#deny ip host 171.71.1.12 any
```

Разрешения для хоста 171.71.1.13

```
Router(config-ext-nacl)#permit    ip    host    171.71.1.13    host
171.71.1.11
Router(config-ext-nacl)#permit    ip    host    171.71.1.13    host
171.71.1.12
Router(config-ext-nacl)#permit    ip    host    171.71.1.13    host
171.71.1.13
Router(config-ext-nacl)#permit    ip    host    171.71.1.13    host
171.71.1.14
```

```
Router(config-ext-nacl)#permit    ip    host    171.71.1.13    host
171.71.1.15
Router(config-ext-nacl)#permit    ip    host    171.71.1.13    host
171.71.1.16
Router(config-ext-nacl)#permit    ip    host    171.71.1.13    host
171.71.1.17
Router(config-ext-nacl)#permit    ip    host    171.71.1.13    host
171.71.1.18
Router(config-ext-nacl)#permit    ip    host    171.71.1.13    host
171.71.1.19
Router(config-ext-nacl)#permit    ip    host    171.71.1.13    host
171.71.1.20
Router(config-ext-nacl)#permit ip host 171.71.1.13 host 171.71.1.1
Router(config-ext-nacl)#permit ip host 171.71.1.13 host 171.71.1.2
Router(config-ext-nacl)#permit ip host 171.71.1.13 host 171.71.1.3
Router(config-ext-nacl)#permit ip host 171.71.1.13 host 171.71.1.4
Router(config-ext-nacl)#permit ip host 171.71.1.13 host 171.71.1.5
Router(config-ext-nacl)#permit ip host 171.71.1.13 host 171.71.1.6
Router(config-ext-nacl)#permit ip host 171.71.1.13 host 171.71.1.7
Router(config-ext-nacl)#permit ip host 171.71.1.13 host 171.71.1.8
Router(config-ext-nacl)#permit ip host 171.71.1.13 host 171.71.1.9
Router(config-ext-nacl)#permit    ip    host    171.71.1.13    host
171.71.1.10
Router(config-ext-nacl)#deny ip host 171.71.1.13 any
```

Разрешения для хоста 171.71.1.14

```
Router(config-ext-nacl)#permit    ip    host    171.71.1.14    host
171.71.1.11
Router(config-ext-nacl)#permit    ip    host    171.71.1.14    host
171.71.1.12
Router(config-ext-nacl)#permit    ip    host    171.71.1.14    host
171.71.1.13
Router(config-ext-nacl)#permit    ip    host    171.71.1.14    host
171.71.1.14
Router(config-ext-nacl)#permit    ip    host    171.71.1.14    host
171.71.1.15
Router(config-ext-nacl)#permit    ip    host    171.71.1.14    host
171.71.1.16
Router(config-ext-nacl)#permit    ip    host    171.71.1.14    host
171.71.1.17
Router(config-ext-nacl)#permit    ip    host    171.71.1.14    host
171.71.1.18
Router(config-ext-nacl)#permit    ip    host    171.71.1.14    host
171.71.1.19
Router(config-ext-nacl)#permit    ip    host    171.71.1.14    host
171.71.1.20
Router(config-ext-nacl)#permit ip host 171.71.1.14 host 171.71.1.1
Router(config-ext-nacl)#permit ip host 171.71.1.14 host 171.71.1.2
Router(config-ext-nacl)#permit ip host 171.71.1.14 host 171.71.1.3
Router(config-ext-nacl)#permit ip host 171.71.1.14 host 171.71.1.4
Router(config-ext-nacl)#permit ip host 171.71.1.14 host 171.71.1.5
```

```
Router(config-ext-nacl)#permit ip host 171.71.1.14 host 171.71.1.6
Router(config-ext-nacl)#permit ip host 171.71.1.14 host 171.71.1.7
Router(config-ext-nacl)#permit ip host 171.71.1.14 host 171.71.1.8
Router(config-ext-nacl)#permit ip host 171.71.1.14 host 171.71.1.9
Router(config-ext-nacl)#permit    ip    host    171.71.1.14    host
171.71.1.10
Router(config-ext-nacl)#deny ip host 171.71.1.14 any
```

Разрешения для хоста 171.71.1.21

```
Router(config-ext-nacl)#permit    ip    host    171.71.1.21    host
171.71.1.22
Router(config-ext-nacl)#permit    ip    host    171.71.1.21    host
171.71.1.23
Router(config-ext-nacl)#permit    ip    host    171.71.1.21    host
171.71.1.24
Router(config-ext-nacl)#permit    ip    host    171.71.1.21    host
171.71.1.25
Router(config-ext-nacl)#permit    ip    host    171.71.1.21    host
171.71.1.26
Router(config-ext-nacl)#permit    ip    host    171.71.1.21    host
171.71.1.27
Router(config-ext-nacl)#permit    ip    host    171.71.1.21    host
171.71.1.28
Router(config-ext-nacl)#permit    ip    host    171.71.1.21    host
171.71.1.29
Router(config-ext-nacl)#permit    ip    host    171.71.1.21    host
171.71.1.30
Router(config-ext-nacl)#permit ip host 171.71.1.21 host 171.71.1.1
Router(config-ext-nacl)#permit ip host 171.71.1.21 host 171.71.1.2
Router(config-ext-nacl)#permit ip host 171.71.1.21 host 171.71.1.3
Router(config-ext-nacl)#permit ip host 171.71.1.21 host 171.71.1.4
Router(config-ext-nacl)#permit ip host 171.71.1.21 host 171.71.1.5
Router(config-ext-nacl)#permit ip host 171.71.1.21 host 171.71.1.6
Router(config-ext-nacl)#permit ip host 171.71.1.21 host 171.71.1.7
Router(config-ext-nacl)#permit ip host 171.71.1.21 host 171.71.1.8
Router(config-ext-nacl)#permit ip host 171.71.1.21 host 171.71.1.9
Router(config-ext-nacl)#permit    ip    host    171.71.1.21    host
171.71.1.10
Router(config-ext-nacl)#deny ip host 171.71.1.21 any
```

Разрешения для хоста 171.71.1.22

```
Router(config-ext-nacl)#permit    ip    host    171.71.1.22    host
171.71.1.22
Router(config-ext-nacl)#permit    ip    host    171.71.1.22    host
171.71.1.23
Router(config-ext-nacl)#permit    ip    host    171.71.1.22    host
171.71.1.24
Router(config-ext-nacl)#permit    ip    host    171.71.1.22    host
171.71.1.25
```

```
Router(config-ext-nacl)#permit    ip    host    171.71.1.22    host
171.71.1.26
Router(config-ext-nacl)#permit    ip    host    171.71.1.22    host
171.71.1.27
Router(config-ext-nacl)#permit    ip    host    171.71.1.22    host
171.71.1.28
Router(config-ext-nacl)#permit    ip    host    171.71.1.22    host
171.71.1.29
Router(config-ext-nacl)#permit    ip    host    171.71.1.22    host
171.71.1.30
Router(config-ext-nacl)#permit ip host 171.71.1.22 host 171.71.1.1
Router(config-ext-nacl)#permit ip host 171.71.1.22 host 171.71.1.2
Router(config-ext-nacl)#permit ip host 171.71.1.22 host 171.71.1.3
Router(config-ext-nacl)#permit ip host 171.71.1.22 host 171.71.1.4
Router(config-ext-nacl)#permit    ip    host    171.71.1.22    host
171.71.1.5
Router(config-ext-nacl)#permit ip host 171.71.1.22 host 171.71.1.6
Router(config-ext-nacl)#permit ip host 171.71.1.22 host 171.71.1.7
Router(config-ext-nacl)#permit ip host 171.71.1.22 host 171.71.1.8
Router(config-ext-nacl)#permit ip host 171.71.1.22 host 171.71.1.9
Router(config-ext-nacl)#permit    ip    host    171.71.1.22    host
171.71.1.10
Router(config-ext-nacl)#deny ip host 171.71.1.22 any
```

Разрешения для хоста 171.71.1.33

```
Router(config-ext-nacl)#permit    ip    host    171.71.1.33    host
171.71.1.31
Router(config-ext-nacl)#permit    ip    host    171.71.1.33    host
171.71.1.32
Router(config-ext-nacl)#permit    ip    host    171.71.1.33    host
171.71.1.34
Router(config-ext-nacl)#permit    ip    host    171.71.1.33    host
171.71.1.35
Router(config-ext-nacl)#permit    ip    host    171.71.1.33    host
171.71.1.36
Router(config-ext-nacl)#permit    ip    host    171.71.1.33    host
171.71.1.37
Router(config-ext-nacl)#permit    ip    host    171.71.1.33    host
171.71.1.38
Router(config-ext-nacl)#permit    ip    host    171.71.1.33    host
171.71.1.39
Router(config-ext-nacl)#permit    ip    host    171.71.1.33    host
171.71.1.40
Router(config-ext-nacl)#permit ip host 171.71.1.33 host 171.71.1.1
Router(config-ext-nacl)#permit ip host 171.71.1.33 host 171.71.1.2
Router(config-ext-nacl)#permit ip host 171.71.1.33 host 171.71.1.3
Router(config-ext-nacl)#permit ip host 171.71.1.33 host 171.71.1.4
Router(config-ext-nacl)#permit ip host 171.71.1.33 host 171.71.1.5
Router(config-ext-nacl)#permit ip host 171.71.1.33 host 171.71.1.6
Router(config-ext-nacl)#permit ip host 171.71.1.33 host 171.71.1.7
Router(config-ext-nacl)#permit ip host 171.71.1.33 host 171.71.1.8
```

```
Router(config-ext-nacl)#permit ip host 171.71.1.33 host 171.71.1.9
Router(config-ext-nacl)#permit    ip    host    171.71.1.33    host
171.71.1.10
Router(config-ext-nacl)#deny ip host 171.71.1.33 any
```

Разрешения для хоста 171.71.1.34

```
Router(config-ext-nacl)#permit    ip    host    171.71.1.34    host
171.71.1.31
Router(config-ext-nacl)#permit    ip    host    171.71.1.34    host
171.71.1.32
Router(config-ext-nacl)#permit    ip    host    171.71.1.34    host
171.71.1.34
Router(config-ext-nacl)#permit    ip    host    171.71.1.34    host
171.71.1.35
Router(config-ext-nacl)#permit    ip    host    171.71.1.34    host
171.71.1.36
Router(config-ext-nacl)#permit    ip    host    171.71.1.34    host
171.71.1.37
Router(config-ext-nacl)#permit    ip    host    171.71.1.34    host
171.71.1.38
Router(config-ext-nacl)#permit    ip    host    171.71.1.34    host
171.71.1.39
Router(config-ext-nacl)#permit    ip    host    171.71.1.34    host
171.71.1.40
Router(config-ext-nacl)#permit ip host 171.71.1.34 host 171.71.1.1
Router(config-ext-nacl)#permit ip host 171.71.1.34 host 171.71.1.2
Router(config-ext-nacl)#permit ip host 171.71.1.34 host 171.71.1.3
Router(config-ext-nacl)#permit ip host 171.71.1.34 host 171.71.1.4
Router(config-ext-nacl)#permit ip host 171.71.1.34 host 171.71.1.5
Router(config-ext-nacl)#permit ip host 171.71.1.34 host 171.71.1.6
Router(config-ext-nacl)#permit ip host 171.71.1.34 host 171.71.1.7
Router(config-ext-nacl)#permit ip host 171.71.1.34 host 171.71.1.8
Router(config-ext-nacl)#permit ip host 171.71.1.34 host 171.71.1.9
Router(config-ext-nacl)#permit    ip    host    171.71.1.34    host
171.71.1.10
Router(config-ext-nacl)#deny ip host 171.71.1.34 any
```

После того, как ACL список был создан, его необходимо применить на маршрутизаторе. При имеющейся схеме сети ACL список нужно установить на фильтрацию входящего траффика:

– Вход в режим настройки интерфейса:

```
Router(config)#int fa 0/0
```

– Применение ACL списка:

```
Router(config-if)#ip acc
Router(config-if)#ip access-group 112 out
```

```
Router(config-if)#end
```

3.7 Настройка подключения к интеренету Asus RT-AC68U

Данный маршрутизатор, как и все модели компании Asus, выпускаемые с 2011 года имеет очень удобный web интерфейс, для получения доступа к которому необходимо воспользоваться любым браузером. В адресной строке браузера необходимо ввести 192.168.1.1 или 192.168.0.1(зависит от прошивки модели, можно посмотреть на обратной стороне маршрутизатора) , после чего в качестве пары логин\пароль указать: admin\admin (рисунок 3.15).

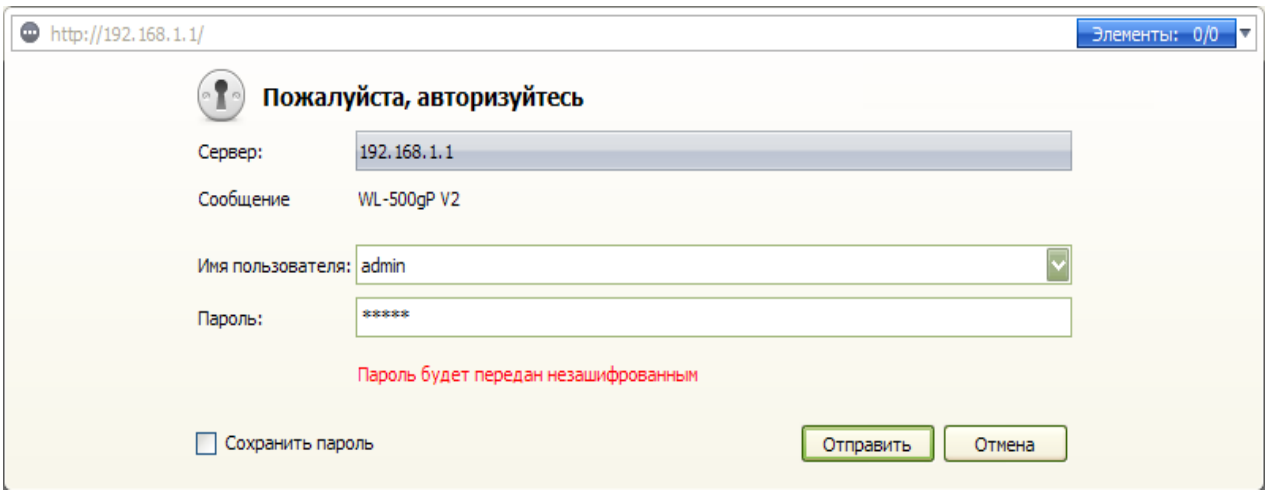

Рисунок 3.15 – Авторизация в web интерфейсе маршрутизатора Asus RT-AC68U

Одной из вкладок меню настройки данного маршрутизатора является карта сети, где в графическом виде отображено состояние роутера, клиентов и других внешних устройств.(рисунок 3.16).

Рисунок 3.16 – Карта сети маршрутизатора Asus RT-AC68U

Так как роутер имеет два независимых друг от друга радиоблока, то он может работать одновременно в диапазоне 2.4ГГц и 5ГГц. Большая часть настроек точек доступа дублируется. Среди дополнительных опций существует возможность задать расписание работы – одно для рабочих дней и другое для выходных.

Также маршрутизатор может организовывать гостевые сети, в количестве 3 на каждый из диапазонов. При этом, среди настраевымых параметров есть имя, защита, время работы. Имеется возможность разрешить доступ не только к интернету но и к другим частям сети (рисунок 3.17).

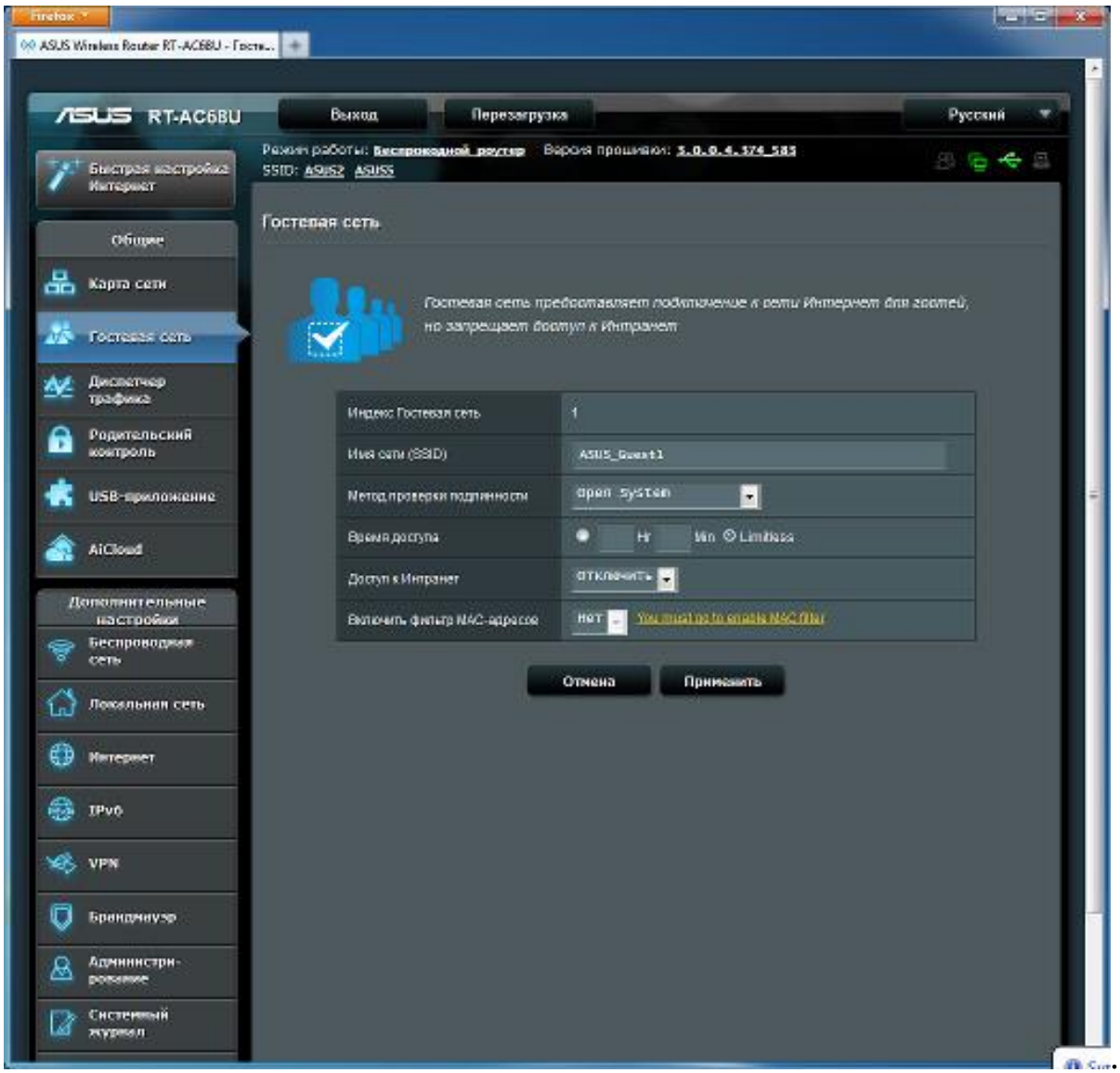

Рисунок 3.17 – Настройка гостевой сети на маршрутизаторе Asus RT-AC68U

Кроме ведения стандратного системного журнала, маршрутизатор может предоставить и другую информацию по состоянию роутера: параметры точек доступа и списки их клиентов, таблицы маршрутизации и прочее).

Имеется возможность настройки администрирования (изменение прошивки, настройка конфигурации, режим работы устройства). Существует возможность установления разрешния на доступ к консоли через telnet.

3.8 Дополнительные возможности Asus RT-AC68U в качестве маршрутизатора.

Одной из удобных возможностей Asus RT-AC68U является мониторинг трафика в режиме роутера (рисунок 3.18).

Рисунок 3.18 – Диспетчер трафика на Asus RT-AC68U

Еще одной интересной особенностью данного устройства является возможность одновременного подключения к двум интернет провайдерам (рисунок 3.19). Второй провайдер может быть активен одновременно с основным, или использоваться в качестве резервного. При использовании двух провайдеров необходимо задействовать кроме основного WAN-порта один из портов LAN или использовать подключение через 3G модем.

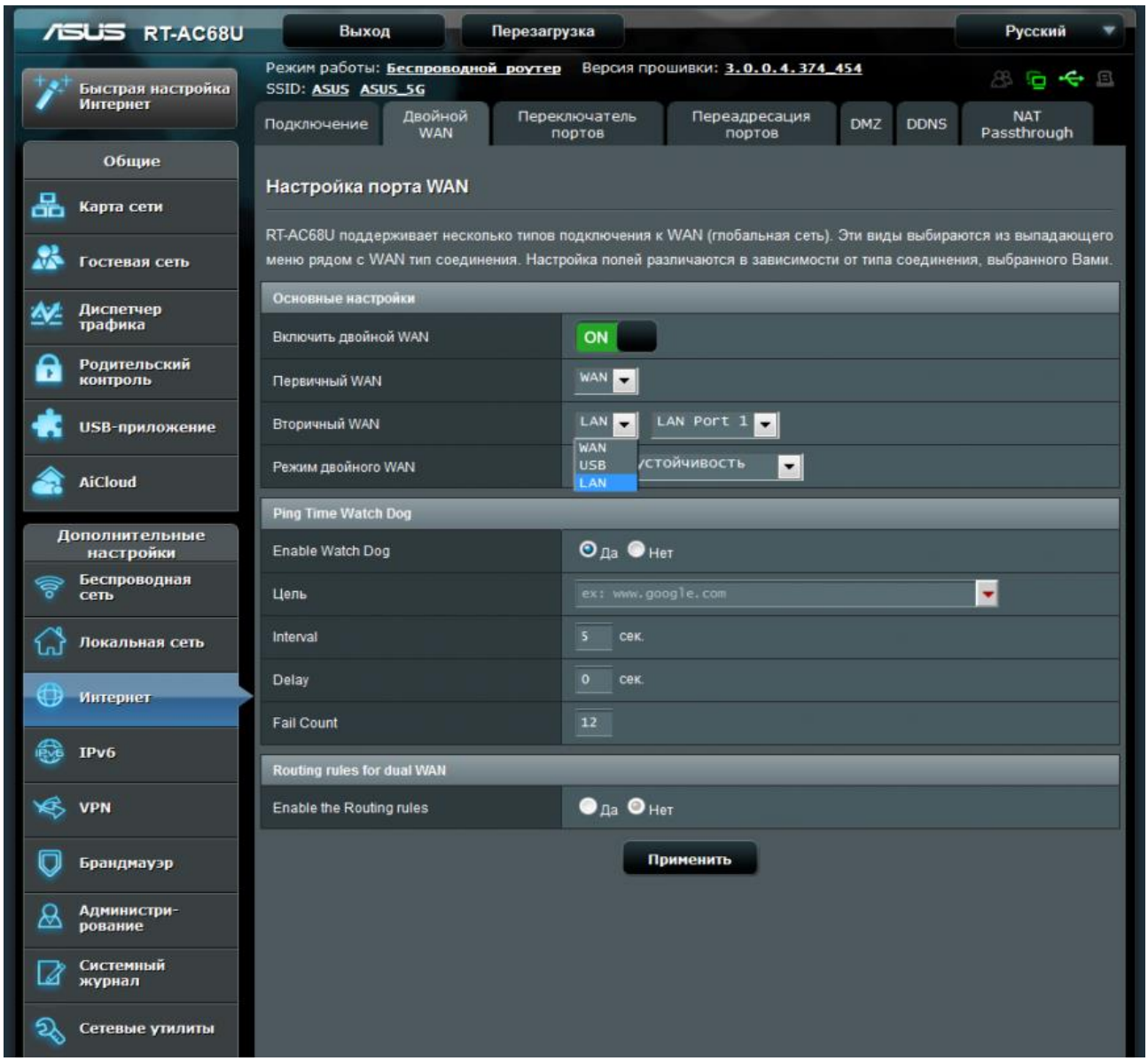

Рисунок 3.19 – Двойной WAN на Asus RT-AC68U

Данный маршрутизатор имеет функцию VPN-сервера (рисунок 3.20), позволяющую подключаться к сети из любого места. При этом, маршрутизатор использует алгоритмы шифрования MPPE-128 или MPPE-40.

VPN (англ. *Virtual Private Network* – виртуальная частная сеть) – обобщённое название технологий, позволяющих обеспечить одно или несколько сетевых соединений (логическую сеть) поверх другой сети (например, Интернет). Несмотря на то, что коммуникации осуществляются по сетям с меньшим или неизвестным уровнем доверия (например, по публичным сетям), уровень доверия к построенной логической сети не зависит от уровня доверия к базовым сетям благодаря использованию средств криптографии (шифрования, аутентификации, инфраструктуры открытых ключей, средств для защиты от повторов и изменений, передаваемых по логической сети

сообщений). В зависимости от применяемых протоколов и назначения, VPN может обеспечивать соединения трёх видов: *узел-узел*, *узел-сеть* и *сеть-сеть*.

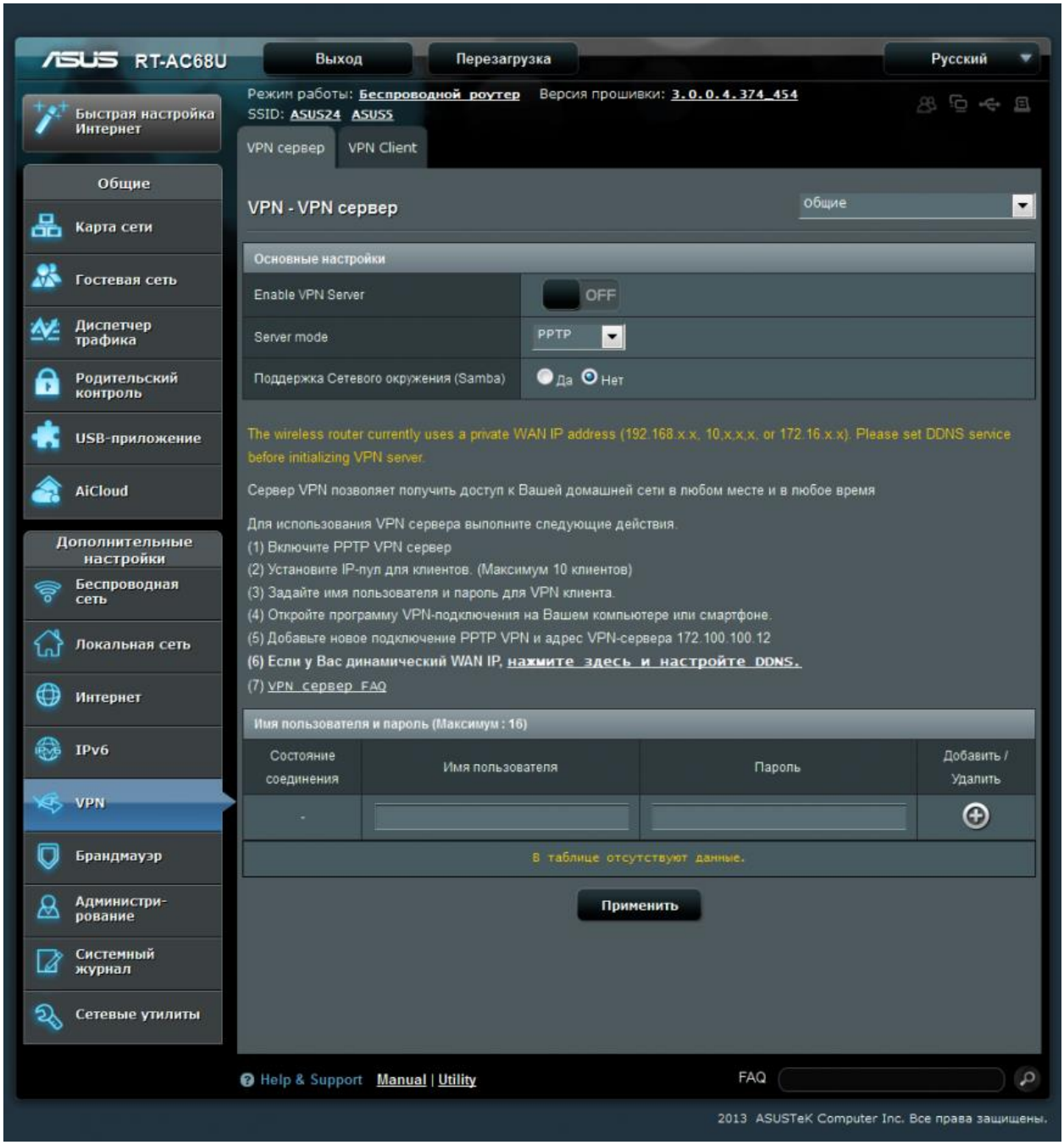

Рисунок 3.20 – Порядок действий для настройки VPN-сервера на Asus RT-AC68U.

3.9 Настройка работы адаптера беспроводных сетей Asus PCE-AC68

После установки адаптера в ПК необходимо установить драйвер устройства и фирменное ПО, поставляемое в комплекте с адаптером на диске. Интерфейс программы интуитивно понятен и не требует специальных знаний для его использования. Единственной проблемой является несовершенство

некоторых версий программы, в которых русские слова не вмещаются целиком на клавиши, но это можно обойти изменив язык программы. Интерфейс ПО представлен на рисунках 3.21 – 3.23.

Рисунок 3.21 – Главное меню программы

Рисунок 3.22 – Раздел «Конфигурация»

Рисунок 3.23 – Раздел «Дополнительно»

В разделе «дополнительно» есть возможность включения Turbo QAM, при условии, что данная технология поддерживается точкой доступа\маршрутизатором.

На закладке «состояние» кроме информации о состоянии адаптера можно узнать информацию об узле и другие параметры Ipv4.

4 Экономическая часть

4.1 Обоснование выбора и состава оборудования

На сегодняшний день рынок оборудования представлен большим разнообразием производителей. Выбор того или иного производителя должен проводится с учетом множества факторов, основные из них это: годность оборудования для реализации данного проекта, используемая технология, совместимость с другим оборудованием, стоимость оборудования.

Будет произведено сравнение проекта сети с использованием технологии Wi-Fi и классической проводной локальной сети.

Проект будет финансироваться из собственных средств организации. В случае реализации сети на основе технологии Wi-Fi монтаж оборудования и его настройка может осуществляться местными специалистами. Для монтажа классической сети нужно привлечь специалиста по монтажу СКС.

Для реализации данного проекта потребуется использовать различное оборудование. Перечень и краткое описание применения оборудования с соответствующими стоимостными показателями приведены ниже.

4.2 Расчет капитальных вложений (вариант 1)

Затраты по капитальным вложениям на реализацию проекта включают в себя затраты на приобретение основного оборудования, монтаж оборудования, транспортные расходы и проектирование, и рассчитывается по формуле

$$K_{\Sigma} = K_{O} + K_{M} + K_{TP} + K_{ПР} \quad (4.1)$$

где $К_О$ – капитальные вложения на приобретение основного оборудования;

$К_{М.}$ – расходы по монтажу оборудования;

$К_{ТР}$ – транспортные расходы;

$К_{ПР}$ – затраты на проектирование [11].

Общий перечень необходимого основного оборудования и его стоимость приведены в таблице 4.1.

Т а б л и ц а 4.1 – Смета затрат на приобретение основного оборудования для реализации проекта.

Наименование	Количество, шт.	Цена за ед., тенге	Сумма, тенге (без НДС)
Коммутатор D-Link DWS-3024, шт.	4	562500	2250752

Окончание таблицы 4.1

Наименование	Количество, шт.	Цена за ед., тенге	Сумма, тенге (без НДС)
Маршрутизатор - Cisco 1941 w/2 GE,2 EHWIC slots,256MB CF,512MB DRAM, IP Base, шт.	2	284 400	568800
Кабель сетевой ParLan U/UTP4 4x2x0,52 мм cat 5e нг (A) -HF 100941 (Паритет Подольск), м.	2000	95	190000
Кабель-канал 60x40x2000мм (белый) **Россия,двойной замок, м.**	2000	325	650000
ASUS RT-AC68UWi-Fi-точка доступа (роутер) стандарт Wi-Fi: 802.11a/b/g/n/ac, шт.	1	38400	38400
Прочие материалы			250500
ИТОГО:			**3948452**

Транспортные расходы, составляют 3% от стоимости всего оборудования и рассчитываются по формуле

$$Ктр = 0{,}03 \cdot Ко = 0{,}03 \cdot 3948452 = 118454 \text{ тенге}$$

Монтаж оборудования, пуско-наладка производится инженерами-монтажниками, расходы составляют 1% от стоимости всего оборудования и рассчитываются по формуле

$$Км = 0{,}01 \cdot Ко = 0{,}01 \cdot 3948452 = 39485 \text{ тенге}$$

Расходы по проектированию и разработке проекта составляют 0,5% от стоимости всего оборудования и рассчитываются по формуле

$$Кпр = 0{,}005 \cdot Ко = 0{,}005 \cdot 3948452 = 19742 \text{ тенге}$$

Общая сумма капитальных вложений по реализации проекта составляет

$$K_{\Sigma} = 3948452 + 118454 + 39485 + 19742 = 4126133 \text{ тенге}$$

4.3 Эксплуатационные расходы (вариант 1)

Текущие затраты на эксплуатацию определяются по формуле

$$Э_Р = ФОТ + О_С + А_О + Э + Н \quad (4.2)$$

где ФОТ – фонд оплаты труда;

$О_С$ – отчисления на соц. нужды;

ОАО – амортизационные отчисления;

Э – электроэнергия для производственных нужд;

Н – накладные затраты.

Фонд оплаты труда

В штате состоят 2 инженера-техника, 1 – осуществляющий монтаж оборудования, 1 – обслуживающий и настраивающий систему. Месячная зарплата у инженера-техника составляет 110 000 тенге. Заработная плата сотрудников приведена в таблице 4.2.

Т а б л и ц а 4.2 – Заработная плата сотрудников

Должность	Количество	Месячная заработная плата, тенге	Годовая заработная плата, тенге
Инженер-техник	2	110 000	2 640 000

Затраты по оплате труда состоят из основной и дополнительной заработных плат и рассчитываются по формуле

$$ФОТ = Зосн + Здоп \quad (4.3)$$

где Зосн – основная заработная плата,

Здоп – дополнительная заработная плата.

Основная заработная плата в год составляет

Зосн =2 640 000 тенге

Дополнительная заработная плата составляет 10% от основной заработной платы и рассчитывается по формуле

$$З_{ДОП} = 0{,}1 \cdot З_{ОСН} \quad (4.4)$$

$З_{ДОП} = 0{,}1 \cdot 2640000 = 264000$ тенге

Общий фонд оплаты труда за год составит

ФОТ=2640000 + 264 000 =2 904 000 тенге

Расчет затрат по социальному налогу

В соответствии со статьей 385 Налогового кодекса РК социальный налог составляет 11% от начисленных доходов и рассчитывается по формуле

$$Oc = 0{,}11 \cdot (ФОТ - ПО) \tag{4.5}$$

где ПО – отчисления в пенсионный фонд.

ФОТ – фонд оплаты труда

0,11 – ставка на социальные нужды

Отчисления в пенсионный фонд составляют 10% от ФОТ, социальным налогом не облагаются и рассчитываются по формуле:

$$ПО = 0{,}1 \cdot ФОТ \tag{4.6}$$

$ПО = 0{,}1 \cdot 2904000 = 290400$ тенге

Тогда социальный налог будет равен

$Oc = 0{,}11 \cdot (2904000 - 290400) = 287496$ тенге

Расчет затрат на амортизацию

Амортизационные отчисления берутся исходя из того, что норма амортизации на оборудование связи составляет 25% и вычисляются по следующей формуле

$$A_0 = H_A \cdot \sum K \tag{4.7}$$

где $Н_А$ – норма амортизации;

∑К – стоимость оборудования.

Тогда амортизационные отчисления составляют

$A_0 = H_A \cdot \sum K = 0.25 \cdot 4126133 = 1031533$ тенге

Расчет затрат на электроэнергию

Затраты на электроэнергию для производственных нужд в течение года, включают в себя расходы электроэнергии на оборудование и дополнительные нужды и рассчитываются по формуле

$$Э = З_{ЭЛ.ОБОР.} + З_{ДОП.НУЖ.} \tag{4.8}$$

где $З_{ЭЛ.ОБОР.}$ – затраты на электроэнергию для оборудования;

$З_{ДОП.НУЖ.}$ – затраты на дополнительные нужды.

Затраты электроэнергии на оборудование рассчитывается по формуле

$$З_{ЭЛ.ОБОР.} = W \cdot T \cdot S \quad (4.9)$$

где W – потребляемая мощность, W=7кВт;

T – время работы (на 2014 календарный год время работы для 40 часовой пяти дневной рабочей недели составляют 1960 час.);

S – Тариф, равный 1 кВтч=14,65 тг.

$$З_{ЭЛ.ОБОР.} = 7 \cdot 14{,}65 \cdot 1960 = 200\,998 \text{ тенге}$$

Затраты на дополнительные нужды составляют 5% от затрат на электроэнергию оборудования и рассчитываются по формуле

$$З_{ДОП.НУЖ.} = 0{,}05 \cdot З_{ЭЛ.ОБОР.} \quad (4.10)$$

где $З_{ЭЛ.ОБОР}$ – затраты на электроэнергию для оборудования.

Затраты на электроэнергию для дополнительных нужд

$$З_{ДОП.НУЖ.} = 0{,}05 \cdot 200998 = 10050 \text{ тенге}$$

Тогда суммарные затраты на электроэнергию будут равны

$$Э = 200\,998 + 10050 = 211048 \text{ тенге}$$

Расчет накладных затрат

Накладные расходы составляют 75% от всех затрат и рассчитываются по формуле

$$Н = 0{,}75 \cdot (ФОТ + О_с + А_о + З_{эл.обор}) \quad (4.11)$$

где ФОТ – фонд оплаты труда.

Тогда накладные затраты составят

$$Н = 0{,}75 \cdot (2904000 + 287496 + 1031533 + 211048) = 3325558 \text{ тенге}$$

Результаты расчета годовых эксплуатационных расходов представлены в таблице 4.3.

Т а б л и ц а 4.3 – Годовые эксплуатационные расходы (вариант 1)

Показатель	**Сумма тенге**
ФОТ	2 904 000
Отчисления на социальные нужды (Ос)	287 496
Амортизационные отчисления ($А_0$)	1031533
Затраты на электроэнергию (Э)	211048
Накладные расходы (Н)	3325558
ИТОГО	**7 759 635**

4.4 Расчет капитальных вложений (вариант 2)

Затраты по капитальным вложениям на реализацию проекта включают в себя затраты на приобретение основного оборудования, монтаж оборудования, транспортные расходы и проектирование, и рассчитывается по формуле

$$K_{\Sigma} = K_{O} + K_{M} + K_{TP} + K_{ПР} \quad (4.12)$$

где $К_О$ – капитальные вложения на приобретение основного оборудования;

$К_{М.}$ – расходы по монтажу оборудования;

$К_{ТР}$ – транспортные расходы;

$К_{ПР}$ – затраты на проектирование.

Общий перечень необходимого основного оборудования и его стоимость приведены в таблице 4.4.

Т а б л и ц а 4.4 – Смета затрат на приобретение основного оборудования для реализации проекта.

Наименование	Количество, шт.	Цена за ед., тенге	Сумма, тенге (без НДС)
Маршрутизатор - Cisco 1941 w/2 GE,2 EHWIC slots,256MB CF,512MB DRAM, IP Base, шт	1	284 400	284400
Коммутатор D-Link DWS-3024, шт	1	562500	562500
Кабель сетевой ParLan U/UTP4 4x2x0,52 мм cat 5e нг (А) -HF 100941 (Паритет Подольск), м	100	95	9500
Кабель-канал 60x40x2000мм (белый) Россия,двойной замок, м	100	325	32500
ASUS RT-AC68UWi-Fi-точка доступа (роутер) стандарт Wi-Fi: 802.11a/b/g/n/ac, шт	4	38400	153600

Окончание таблицы 4.4

Pci-e WiFi адаптер asus PCE-AC68, м	15896	75	1267200
Прочие материалы			250500
ИТОГО:			**2294740**

Транспортные расходы, составляют 3% от стоимости всего оборудования и рассчитываются по формуле

$$Ктр = 0{,}03 \cdot Ко = 0{,}03 \cdot 2294740 = 68842 \text{ тенге}$$

Монтаж оборудования, пуско-наладка производится инженерами-монтажниками, расходы составляют 1% от стоимости всего оборудования и рассчитываются по формуле

$$Км = 0{,}01 \cdot Ко = 0{,}01 \cdot 2294740 = 22947 \text{ тенге}$$

Расходы по проектированию и разработке проекта составляют 0,5% от стоимости всего оборудования и рассчитываются по формуле

$$Кпр = 0{,}005 \cdot Ко = 0{,}005 \cdot 2294740 = 11474 \text{ тенге}$$

Общая сумма капитальных вложений по реализации проекта составляет

$$K_{\Sigma} = 2294740 + 68842 + 22947 + 11474 = 2398003 \text{ тенге}$$

4.5 Эксплуатационные расходы (вариант 2)

Текущие затраты на эксплуатацию определяются по формуле

$$Э_{Р} = ФОТ + О_{С} + А_{О} + Э + Н \qquad (4.13)$$

где ФОТ – фонд оплаты труда;
$О_С$ – отчисления на соц. нужды;
ОАО – амортизационные отчисления;
Э – электроэнергия для производственных нужд;
Н – накладные затраты.

Фонд оплаты труда

Из-за более удобного в эксплуатации оборудования, штат можно сократить до 1 инженера–техника. Месячная зарплата у инженера-техника составляет – 110 000 тенге. Заработная плата приведена в таблице 4.5.

Т а б л и ц а 4.5 – Заработная плата сотрудников

Должность	Количество	Месячная заработная плата, тенге	Годовая заработная плата, тенге
Инженер-техник	1	110 000	1 320 000

Затраты по оплате труда состоят из основной и дополнительной заработных плат и рассчитываются по формуле

$$ФОТ = Зосн + Здоп \quad (4.14)$$

где Зосн – основная заработная плата,
Здоп – дополнительная заработная плата.

Основная заработная плата в год составляет

Зосн = 1 320 000 тенге

Дополнительная заработная плата составляет 10% от основной заработной платы и рассчитывается по формуле

$$З_{ДОП} = 0{,}1 \cdot З_{ОСН} \quad (4.15)$$

$З_{ДОП}$=0,1*1320000=132000 тенге

Общий фонд оплаты труда за год составит

ФОТ=1320000 + 132 000 =1 452 000 тенге

В соответствии со статьей 385 Налогового кодекса РК социальный налог составляет 11% от начисленных доходов и рассчитывается по формуле

$$Ос = 0{,}11 \cdot (ФОТ - ПО) \quad (4.16)$$

где ПО – отчисления в пенсионный фонд;
ФОТ – фонд оплаты труда;
0,11 – ставка на социальные нужды.

Отчисления в пенсионный фонд составляют 10% от ФОТ, социальным налогом не облагаются и рассчитываются по формуле

$$ПО = 0{,}1 \cdot ФОТ \quad (4.17)$$

$ПО = 0{,}1 \cdot 1452000 = 145200$ тенге

Тогда социальный налог будет равен

$Ос = 0{,}11 \cdot (1452000 - 145200) = 143748$ тенге

Амортизационные отчисления берутся исходя из того, что норма амортизации на оборудование связи составляет 25% и вычисляются по следующей формуле

$$A_0 = H_A \cdot \sum K \quad (4.18)$$

где $Н_А$ – норма амортизации;

$\sum$К – стоимость оборудования.

Тогда амортизационные отчисления составляют:

$A_0 = H_A \cdot \sum K = 0.25 \cdot 2398003 = 599501$ тенге

Затраты на электроэнергию для производственных нужд в течение года, включают в себя расходы электроэнергии на оборудование и дополнительные нужды и рассчитываются по формуле

$$Э = З_{ЭЛ.ОБОР.} + З_{ДОП.НУЖ.} \quad (4.19)$$

где $З_{ЭЛ.ОБОР.}$ – затраты на электроэнергию для оборудования;

$З_{ДОП.НУЖ.}$ – затраты на дополнительные нужды.

Затраты электроэнергии на оборудование рассчитывается по формуле

$$З_{ЭЛ.ОБОР.} = W \cdot T \cdot S \quad (4.20)$$

где W – потребляемая мощность, W=7кВт;

T – время работы;

S – тариф, равный 1 кВтч=14,65 тг;

T – время работы (на 2014 календарный год время работы для 40 часовой пяти дневной рабочей недели составляют 1960 час.).

$$З_{ЭЛ.ОБОР.} = 7 \cdot 14{,}65 \cdot 1960 = 200998 \text{ тенге}$$

Затраты на дополнительные нужды составляют 5% от затрат на электроэнергию оборудования и рассчитываются по формуле

$$З_{ДОП.НУЖ.} = 0{,}05 \cdot З_{ЭЛ.ОБОР.} \quad (4.21)$$

где $З_{ЭЛ.ОБОР}$ – затраты на электроэнергию для оборудования.

Затраты на электроэнергию для дополнительных нужд

$$З_{ДОП.НУЖ.} = 0{,}05 \cdot 200998 = 10050 \text{ тенге}$$

Тогда суммарные затраты на электроэнергию будут равны

$$Э = 200\,998 + 10050 = 211048 \text{ тенге}$$

Накладные расходы составляют 75% от всех затрат и рассчитываются по формуле

$$Н = 0{,}75 \cdot (ФОТ + О_с + А_о + З_{эл.обор}) \quad (4.22)$$

где ФОТ – фонд оплаты труда.

Тогда накладные затраты составят

$$Н = 0{,}75 \cdot (1452000 + 143748 + 599501 + 211048) = 1730481 \text{ тенге}$$

Результаты расчета годовых эксплуатационных расходов представлены в таблице 4.6.

Т а б л и ц а 4.6 – Годовые эксплуатационные расходы (вариант 2)

Показатель	**Сумма тенге**
ФОТ	1 452 000
Отчисления на социальные нужды (Ос)	143 748
Амортизационные отчисления ($А_0$)	599501
Затраты на электроэнергию (Э)	211048
Накладные расходы (Н)	1730481
ИТОГО	**4136778**

4.6 Оценка сравнительной эффективности от реализации проекта

Сравнительная экономическая эффективность капитальных вложений применяется для выбора наилучшего из возможных плановых и проектных вариантов капитальных вложений. Для этого сопоставляются по сравниваемым вариантам капитальные вложения и текущие затраты. Выбирается вариант, дающий их оптимальное соотношение.

Сравнительная эффективность капитальных вложений определяется на основе минимума приведенных затрат. Приведенные затраты по каждому варианту представляют собой сумму текущих затрат (себестоимости) и капитальных вложений, приведенных к одинаковой размерности в соответствии с нормативом эффективности:

$$Зi = Ci + ЕнКi \rightarrow min \qquad (4.23)$$

где Ci – текущие затраты (себестоимость) по каждому варианту;

Кi – капитальные вложения по тому же варианту;

Е – норма дисконта.

По первому варианту реализации проекта приведенные затраты составят

$З_1 = 7759635+0,25*4126133 = 8791168$ тенге

По второму варианту реализации

$З_2 = 4136778+0,25*2398003 = 4736279$ тенге

$З_2 < З_1$

Показатели Ci и Кi могут применяться как в полной сумме капитальных вложений и себестоимости годовой продукции, так и в виде удельных капитальных вложений на единицу продукции и себестоимости единицы продукции [12].

Сравнительная эффективность капитальных вложений определяется на основе минимума приведенных затрат.

Т а б л и ц а 4.7 – Результаты расчета эффективности по вариантам

Показатели	Вариант 1, тг	Вариант 2, тг
Капитальные вложения ($К_i$)	4126133	2398003
Издержки ($С_i$)	7 759 635	4136778
Приведенные затраты ($З_i$)	8791168	4736279

На основании полученных данных можно заключить, реализация проекта по варианту №2 выгоднее, чем реализация проекта по варианту №1, т.к. приведенные затраты меньше на 4054890 тенге.

5 Безопасность жизнедеятельности

5.1 Анализ условий труда обслуживающего персонала при эксплуатации ПК

Главной целью данного проекта является создание беспроводной локальной сети в здании СПбГБУК «СПбГБСС». Так же нужно предусмотреть безопасность работы с ПК в серверном помещении.

В список опасных и вредных факторов при работе за компьютером входят:

1 повышенная напряженность электрического поля;
2 токсические вещества;
3 повышенный уровень шума на рабочем месте;
4 пониженная контрастность;
5 повышенная напряженность магнитного поля;
6 недостаточная освещенность рабочей зоны;
7 повышенный уровень статистического электричества.

Касательно здоровья сотрудников, можно выделить несколько факторов риска, которым сопровождается влияние компьютера на организм человека:

1 проблемы, обусловленные наличием электромагнитного излучения;
2 проблемы зрения;
3 проблемы, связанные с мышцами и суставами;
4 стресс, депрессия и другие нервные расстройства, которые обуславливаются влиянием компьютера на психику человека;
5 малоподвижный образ жизни;
6 переработка (более 9 часов в сутки);
7 стрессы;
8 работа в ночное время суток, и как следствие нарушение выработки гормона мелатонина [13].

Магнитное поле

Компьютер при работе создает вокруг себя электромагнитное поле, которое обладает способностью биологического, специфического и теплового воздействия на организм человека. За счет влияния электромагнитного поля на клетки и ткани человека происходят нарушения условно-рефлекторной деятельности, снижение активности мозга. Все это проявляется в головной боли, утомляемости, ухудшении самочувствия, гипотонии.

За счет теплового воздействия электромагнитного поля повышается температура тела, идет нагрев тканей и органов. Больше всего подвержены тепловому облучению такие органы как печень, поджелудочная железа, мочевой пузырь, желудок. Все это может вызвать язвы, кровотечения и перфорации [3].

Шум

На рабочем месте сотрудников источниками шума, как правило, являются разговаривающие люди, внешний шум и отчасти – компьютер, принтер. Они издают довольно незначительный шум, поэтому в помещении достаточно использовать звукопоглощение.

Из строительно-акустических методов защиты от шума выбран метод для помещения, представленного на рисунке 1 – план рабочего помещения звукопоглощающие конструкции и экраны.

Для выбранного помещения выбрано звукопоглощающие облицовка, состоящая из матов, из супертонкого стекловолокна с оболочкой из стеклоткани, которую нужно разместить на потолке и верхних частях стен. Максимальное звукопоглощение будет достигнуто при облицовке не менее 60 % общей площади ограждающих поверхностей помещения.

Электростатическое поле, вредные вещества в воздухе

При работе компьютер образует вокруг себя электростатическое поле, которое деионизирует окружающую среду, а при нагревании платы и корпус монитора испускают в воздух вредные вещества. Всё это делает воздух очень сухим, слабо ионизированным, со специфическим запахом и в общем "тяжёлым" для дыхания. Естественно, такой воздух не может быть полезен для организма и может привести к заболеваниям аллергического характера, болезням органов дыхания и другим расстройствам.

Технический персонал состоит из двух сотрудников: главный технический специалист и оператор работающий непосредственно на ПК. Технический специалист работает 3 раза в неделю по 6 часов. Оператор работает каждый день.

Работа сотрудников непосредственно связана с компьютером, а соответственно с вредным дополнительным воздействием целой группы факторов, что существенно снижает производительность их труда.

К таким факторам можно отнести:

1) неправильную освещенность;
2) эргономические нарушения к требованиям рабочего места;
3) наличие напряжения.

Согласно ГОСТ 12.1.005-88 «ССБТ. Оптимальные и допустимые нормы микроклимата, в зависимости от категории работ», работа людей в помещение относится к работе лёгкой тяжести (1а) [14].

В помещениях при работе с ПК должны соблюдаться следующие климатические условия:

Холодный период года

1) Температура в помещении:
   а) оптимальная температура 24 С˚, допустимая температура 26 С˚;
   б) относительная влажность 55 %, допустимая влажность 70%;
   в) скорость движение воздуха относительная и допустимая 0,1 м/с.
2) Температура в серверной:
   а) оптимальная температура 15 С˚, допустимая температура 20 С˚;

б) относительная влажность 50 %, допустимая влажность 65%;

в) скорость движение воздуха относительная и допустимая 0,1 м/с.

Тёплый период года

1) Температура в помещении:

а) оптимальная температура 24 С˚, допустимая температура 25 С˚;

б) относительная влажность 53 %, допустимая влажность 65%;

в) скорость движение воздуха относительная и допустимая 0,1 м/с.

2) Температура в серверной:

а) оптимальная температура 15 С˚, допустимая температура 20 С˚;

б) относительная влажность 40 %, допустимая влажность 55%;

в) скорость движение воздуха относительная и допустимая 0,05 м/с [15].

Помещение имеет 2комнаты. Размеры серверной: длина (L) = 2,8 метра, ширина (В) = 2,2 метра, высота (Н) = 3 метра. Размер помещения, содержащего сервер: длина (L) = 7,9 метра, ширина (В) = 6,4 метра, высота (Н) = 3 метра. Помещение находится в здании на 3-м этаже, рассчитано на 2 рабочих места.

План помещения выбранного для размещения оборудования и технического персонала изображен на рисунке 5.1.

Рисунок 5.1 – План рабочего помещения

Рабочее место состоит из следующих компонентов:

- два стола;
- два стула;
- два персональных компьютера;
- в серверной находиться: сам сервер и его комплектующие.

5.2 Эргономические требования к рабочему месту

Проектирование рабочих мест, снабженных видеотерминалами, относится к числу важных проблем эргономического проектирования в области вычислительной техники.

Рабочее место и взаимное расположение всех его элементов должно соответствовать антропометрическим, физическим и психологическим требованиям. Большое значение имеет также характер работы. В частности, при организации рабочего места программиста должны быть соблюдены следующие основные условия: оптимальное размещение оборудования, входящего в состав рабочего места и достаточное рабочее пространство, позволяющее осуществлять все необходимые движения и перемещения.

Эргономическими аспектами проектирования видеотерминальных рабочих мест, в частности, являются: высота рабочей поверхности, размеры пространства для ног, требования к расположению документов на рабочем месте (наличие и размеры подставки для документов, возможность различного размещения документов, расстояние от глаз пользователя до экрана, документа, клавиатуры и т.д.), характеристики рабочего кресла, требования к поверхности рабочего стола, регулируемость элементов рабочего места.

Главными элементами рабочего места программиста являются стол и кресло. Основным рабочим положением является положение сидя.

Рабочая поза сидя вызывает минимальное утомление программиста. Рациональная планировка рабочего места предусматривает четкий порядок и постоянство размещения предметов, средств труда и документации. То, что требуется для выполнения работ чаще, расположено в зоне легкой досягаемости рабочего пространства.

Моторное поле – пространство рабочего места, в котором могут осуществляться двигательные действия человека.

Максимальная зона досягаемости рук – это часть моторного поля рабочего места, ограниченного дугами, описываемыми максимально вытянутыми руками при движении их в плечевом суставе.

Оптимальная зона – часть моторного поля рабочего места, ограниченного дугами, описываемыми предплечьями при движении в локтевых суставах с опорой в точке локтя и с относительно неподвижным плечом [16].

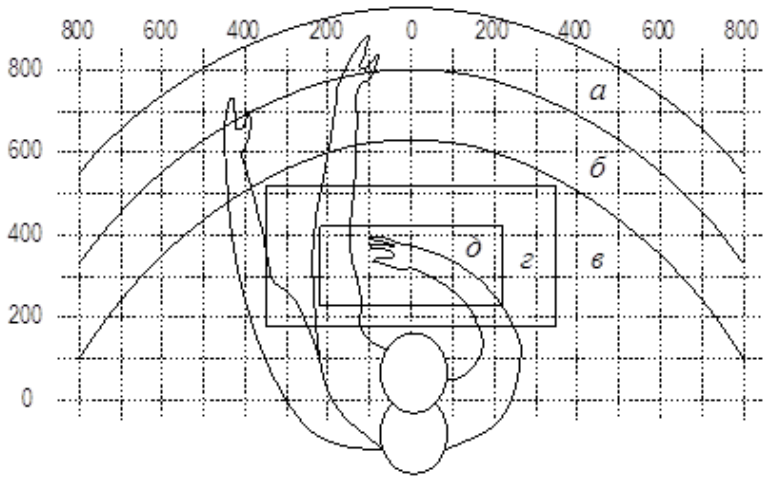

Рисунок 5.2 – Зоны досягаемости рук в горизонтальной плоскости.

а – зона максимальной досягаемости; б – зона досягаемости пальцев при вытянутой руке; в – зона легкой досягаемости ладони; г – оптимальное пространство для грубой ручной работы; д – оптимальное пространство для тонкой ручной работы.

Оптимальное размещение предметов труда и документации в зонах досягаемости:

- дисплей размещается в зоне а (в центре);
- системный блок размещается в предусмотренной нише стола;
- клавиатура – в зоне г/д;
- «мышь» – в зоне в справа;
- сканер в зоне а/б (слева);
- принтер находится в зоне а (справа).

Документация, необходимая при работе – в зоне легкой досягаемости ладони, а в выдвижных ящиках стола – литература, неиспользуемая постоянно.

На рисунке 5.3 показан пример размещения основных и периферийных составляющих ПК на рабочем столе программиста.

1 – сканер, 2 – монитор, 3 – принтер, 4 – поверхность рабочего стола, 5 – клавиатура, 6 – манипулятор типа «мышь».

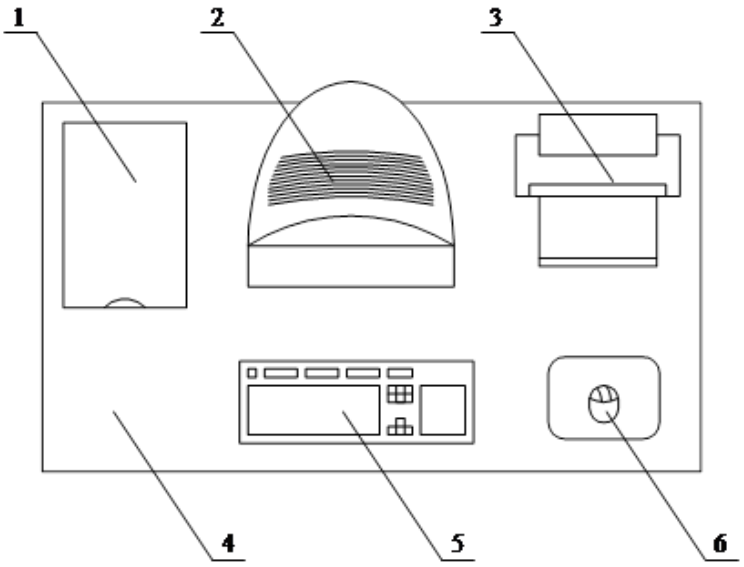

Рисунок 5.3 – Размещение основных и периферийных составляющих ПК.

Для комфортной работы стол должен удовлетворять следующим условиям

– высота стола должна быть выбрана с учетом возможности сидеть свободно, в удобной позе, при необходимости опираясь на подлокотники;

– нижняя часть стола должна быть сконструирована так, чтобы программист мог удобно сидеть, не был вынужден поджимать ноги;

– поверхность стола должна обладать свойствами, исключающими появление бликов в поле зрения программиста;

– конструкция стола должна предусматривает наличие 4 выдвижных ящиков;

– высота рабочей составляет: 700 мм. Высота поверхности, на которую устанавливается клавиатура, должна быть около 650 мм.

Большое значение придается характеристикам рабочего кресла. Так, рекомендуемая высота сиденья над уровнем пола составляет 500 мм. Поверхность сиденья мягкая, передний край закругленный, а угол наклона спинки – регулируемый.

Необходимо предусматривать при проектировании возможность различного размещения документов: сбоку от видеотерминала, между монитором и клавиатурой и т.п. Кроме того, в случаях, когда видеотерминал имеет низкое качество изображения, например, заметны мелькания, расстояние от глаз до экрана равно 700мм, расстояние от глаза до документа 350. Вообще при высоком качестве изображения на видеотерминале расстояние от глаз пользователя до экрана, документа и клавиатуры может быть равным.

Положение экрана определяется:

– расстоянием считывания 0,6 м;

– углом считывания, направлением взгляда на 20° ниже горизонтали к центру экрана, причем экран перпендикулярен этому направлению.

Должна также предусматриваться возможность регулирования экрана:

– по высоте +3 см;

– по наклону от -10° до +20° относительно вертикали;

– в левом и правом направлениях.

Большое значение также придается правильной рабочей позе пользователя. При неудобной рабочей позе могут появиться боли в мышцах, суставах и сухожилиях. Требования к рабочей позе пользователя видеотерминала следующие:

– голова не должна быть наклонена более чем на 20°;

– плечи должны быть расслаблены;

– локти - под углом 80°…100°;

– предплечья и кисти рук - в горизонтальном положении.

Причина неправильной позы пользователей обусловлена следующими факторами: нет хорошей подставки для документов, клавиатура находится слишком высоко, а документы – низко, некуда положить руки и кисти, недостаточно пространство для ног.

В целях преодоления указанных недостатков даются общие рекомендации: лучше передвижная клавиатура; так же предусмотрены специальные приспособления для регулирования высоты стола, клавиатуры и экрана, а также подставка для рук.

Существенное значение для производительной и качественной работы на компьютере имеют размеры знаков, плотность их размещения, контраст и соотношение яркостей символов и фона экрана. Расстояние от глаз оператора до экрана дисплея составляет 60 см, то высота знака должна быть не менее 3мм, оптимальное соотношение ширины и высоты знака составляет 3:4, а расстояние между знаками – 15% их высоты. Соотношение яркости фона экрана и символов – от 1:3.

Во время пользования компьютером медики советуют устанавливать монитор на расстоянии 50-60 см от глаз. С учетом высказывании специалистов также учитывается, что верхняя часть видеодисплея должна быть на уровне глаз или чуть ниже. Когда человек смотрит прямо перед собой, его глаза открываются шире, чем, когда он смотрит вниз. За счет этого площадь обзора значительно увеличивается, вызывая обезвоживание глаз. К тому же если экран установлен высоко, а глаза широко открыты, нарушается функция моргания. Это значит, что глаза не закрываются полностью, не омываются слезной жидкостью, не получают достаточного увлажнения, что приводит к их быстрой утомляемости.

Создание благоприятных условий труда и правильное эстетическое оформление рабочих мест на производстве имеет большое значение как для облегчения труда, так и для повышения его привлекательности, положительно влияющей на производительность труда.

5.3. Расчет системы искусственного освещения помещения

Помещение зала имеет естественное освещение через 3 боковых окна, и искусственное освещение, которое позволяет вести работы в темное время суток и днем в местах, где показатель КЕО не соответствует нормативам.

Поэтому рассчитаем общее освещение помещения аппаратного зала длиной А = 7,9 м., шириной В = 6,4 м., высотой Н = 3 м. Так как ориентация окон в предложенном плане помещения (Рисунок 1) в основном северо-западная, то стены будут окрашены в белый цвет, пол будет оранжево-красный. Так как работа будет связана с компьютерами то коэффициент отражения будет составлять:

1 для потолка: 62%;
2 для стен: 43%;
3 для пола: 28%;
4 для других поверхностей и рабочей мебели: 36%.

Разряд зрительной работы – III высокой точности. Нормируемая освещенность – 300 лк. Для помещения используем люминесцентную лампу ЛБ (белого цвета), мощностью 40 Вт., световым потоком 3120 лм., диаметром 40 мм. и длиной со штырьками 1213,6 мм [17].

Высота светильника h_c = 4-r, где r- высота лампочки.

h_c = 3- 3,2 = 0,2 м

Высота рабочей поверхности

h_P = 1,8 м.

Определим необходимое расстояние между светильниками

$$L = \lambda \cdot h \tag{5.1}$$

где $\lambda = 1.2 \div 1.4$.

Высота светильника над освещаемой поверхностью

$h = 3 - 1{,}8 - 0{,}2 = 1$ м.

По этим данным находим, что необходимое расстояние между светильниками равно

$$L = \lambda \cdot h \tag{5.2}$$

$L = 1{,}2 \cdot 1 = 1{,}2$

Определим индекс помещения I [1]

$$I = \frac{A \cdot B}{h \cdot (A + B)} \quad (5.3)$$

$$\text{I} = \frac{7{,}9 \cdot 6{,}4}{2 \cdot (7{,}9 + 6{,}4)} = 1{,}767$$

Определим коэффициент использования η [5].

$$\eta = 0{,}73$$

В качестве светильника возьмем ЛСП02 рассчитанный на две лампы мощностью 40 Вт, диаметром 40 мм и длиной со штырьками 1213,6 мм. Длина светильника 1234 мм, ширина 276 мм. Световой поток лампы ЛБ 40 Фл составляет 3230 лм., световой поток, излучаемый светильником Фсв равен:

$$\Phi_{СВ} = \Phi_{Л} \cdot 2 = 3230 \cdot 2 = 6460 \text{ лм.}$$

Определим число светильников

$$N = \frac{E \cdot K_З \cdot S \cdot Z}{n \cdot \Phi_{Л} \cdot \eta} \quad (5.4)$$

где S – площадь помещения, S=50,5 $м^2$.;
КЗ – коэффициент запаса, КЗ=1,5[1];
Е – заданная минимальная освещенность, Е=400 лк. [1];
Z – коэффициент неравномерности освещения, Z=1,2 [1];
n – количество ламп в светильнике, n=2;
Фл – световой поток выбранной лампы, Фл=3230 лм.;
η – коэффициент использования, η=0,73[1].

$$N = \frac{400*1{,}5*50{,}5*1{,}2}{2*3230*0{,}73} = 7{,}71 \approx 8 \text{ светильников}$$

Расположение светильников показано на рисунке 5.4.

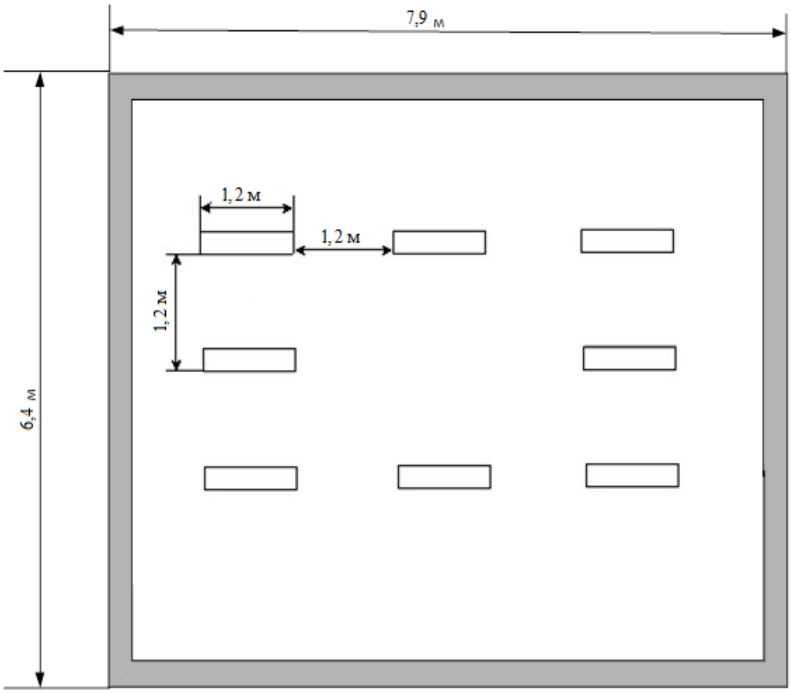

Рисунок 5.4 – Расположение светильников в помещении

Итого, для создания нормированной освещенности нам понадобится 8 ламп, в двух рядах по 3 светильника и в одном - 2 светильника, в каждом светильнике по две лампы.

5.4 Итоги угроз безопасности жизнедеятельности

В данном разделе был произведён анализ условий труда в рабочем помещении для двух человек. Уровень условий труда признан допустимым, и данные, полученные из расчетов полностью удовлетворяют требованиям стандартов безопасности жизнедеятельности.

Были проанализированы основные требования по эргономике рабочего места. Учитывались все факторы касающиеся зрения, положения сидящего, комфортабельности рабочего места и расположения всех необходимых предметов на рабочем столе.

Так как в помещении есть три окна и естественным освещением, то можно использовать лампы мощностью 40 Вт., со световым потоком 3120 лм., диаметром 40 мм. и длиной со штырьками 1213,6 мм. При чем так как каждый светильник состоит из 2 ламп, то можно использовать в каждом светильнике только по одной лампе, но это при дневном свете. Во время работы в вечернее время суток или ночью необходимо включать весь необходимый свет для более оптимальной работы.

Заключение

В этом дипломном проекте были рассмотрены такие технологии беспроводных сетей, как Wi-Fi, WiMAX, Bluetooth. Была спроектирована беспроводная локальная сеть для СПбГБУК «СПбГБСС» по технологии Wi-Fi стандарта 802.11ac. Стандарт 802.11ac на сегодняшний день является одним из ведущих стандартов в мире для проектирования локальных сетей небольших размеров. А по максимально достижимой скорости передачи данных этот стандарт находится на первом месте.

Были рассмотрены угрозы для Wi-Fi сетей, методы их предотвращения.

В экономической части дипломного проекта было осуществлено сравнение двух проектов сетей: классического кабельного варианта и варианта на основе беспроводной технологии. Стоимость создания сети по беспроводному варианту почти в два раза ниже, чем стоимость создания классической кабельной сети.

Также был проведен обзор вредных факторов, влияющих на безопасности жизнедеятельности сотрудников IT-отдела СПбГБУК «СПбГБСС». Был произведен расчет необходимого освещения в помещении серверной.

Список используемой литературы

1 Сайт http://ru.wikipedia.org/wiki/Беспроводные_технологии
2 Сайт http://ru.wikipedia.org/wiki/Wi-Fi
3 Сайт http://ru.wikipedia.org/wiki/
4 Щербаков А.К. Wi-Fi: Все что Вы хотели знать, но боялись спросить. – М.: Бук-Пресс, 2005. – 239с.
5 Пол Беделл. Сети. Беспроводные технологии. – М.: НТ Пресс, 2008. – 448с.
6 Шахнович И. Современные технологии беспроводной связи. – М.: Техносфера, 2006. – 288с.
7 Семенов А. Проектирование и расчет структурированных кабельных систем и их компонентов. – М.: ДМК Пресс, 2008.
8 Ватаманюк А. И. Беспроводная сеть своими руками. – М.: Техносфера, 2006. – 192с.
9 Сайт http://ru.wikipedia.org/wiki/ACL
10 Сайт http://habrahabr.ru/post/121806/
11 Методические указания к выполнению экономической части дипломных работ для студентов специальности 5В070400 – Вычислительная техника и программное обеспечение Еркешева З.Д, Боканова Г.Ш.
12 Титов В.И. Экономика предприятия. – М.: Эксмо, 2008. – 354 с.
13 Мотузко Ф.Я. Охрана труда. – М.: Высшая школа, 1989. – 336с.
14 ГОСТ 12.0.003-72.4. Опасные и вредные производственные факторы. Классификация. – М.: Издательство стандартов, 1975.
15 Безопасность жизнедеятельности /Под ред. Н.А. Белова. – М.: Знание, 2000. – 364с.
16 Зинченко В.П. Основы эргономики. – М.: МГУ, 1979. – 179с.
17 Самгин Э.Б. Освещение рабочих мест. – М.: МИРЭА, 1989. – 186с.
18 Олифер. Н.А. Протоколы и оборудование сетевого уровня / Н.А. Олифер – М.: Центр информационных технологий. 1996. – 176 с.
19 Айвенс К. Компьютерные сети. Хитрости. – М.: НТ Пресс, 2006. – 298с.
20 Ватаманюк А. И. Беспроводная сеть своими руками. – М.: Техносфера, 2006. – 192с.
21 Поляк-Брагинский А. В. Локальные сети. Модернизация и поиск неисправностей. – М.: Техносфера, 2006. – 640с.
22 Столлингс В. Современные компьютерные сети. 2-е издание. – М.: НТ Пресс, 2003, – 783с.
23 Колисниченко Д. Н. Сделай сам компьютерную сеть. Монтаж, настройка, обслуживание. – М.: Техносфера, 2004. – 400с.
24 Крук Б. И., Попантонопуло В. Н., Шувалов В. П. Телекоммуникационные системы и сети: Учебное пособие. В 3 томах. Том 1 - Современные технологии. – М.: ДМК Пресс, 2003. – 643с.
25 Таненбаун Э. Компьютерные сети. – М.: НТ Пресс, 2003. – 992с.

26 Рошан, Педжман, Лиэри, Джонатан. Основы построения беспроводных локальных сетей стандарта 802.11. – М.: НТ Пресс, 2004. – 304с.
27 Уэнстром М. Организация защиты сетей cisco. – М.: НТ Пресс, 2006. – 776с.
28 Пролетарский А. В., Баскаков И. В., Чирков Д. Н. Беспроводные сети Wi-Fi. – М.: БИНОМ. Лаборатория знаний, 2007. – 178 с.

Список сокращений

1 ARP – Address Resolution Protocol (англ. Протокол разрешения адреса)
2 CSD – Circuit Switched Data (англ. Технология передачи данных)
3 CDMA – Code Division Multiple Access (англ. Множественный доступ с кодовым разделением)
4 DNS – Domain Name Service (англ. Служба доменных имен)
5 DSL – Digital Subscriber Line (англ. Цифровая абонентская линия)
6 DSSS – Direct Sequence Spread Spectrum (англ. Широкополосная модуляция с прямым расширением спектра)
7 EDGE – Enhanced Data Rates for GSM Evolution (англ. Цифровая технология беспроводной передачи данных для мобильной связи, которая функционирует как надстройка над 2G и 2.5G)
8 EV-DO – Evolution – Data Only (англ. Технология передачи данных, используемая в сетях сотовой связи стандарта CDMA)
9 GPRS – General Packet Radio Service (англ. Пакетная радиосвязь общего пользования)
10 GSM – Global System for Mobile communications (англ. Глобальный стандарт цифровой мобильной сотовой связи)
11 HSPA – High Speed Packet Access (англ. Высокоскоростная пакетная передача данных)
12 IT – Information Technologies (англ. Информационные технологии)
13 IP – Internet Protocol (англ.Интернет протокол)
14 LAN – Local Area Network (англ. Локальная сеть)
15 MAC – Media Access Control (англ. Уникальный идентификатор, присваемый каждой единице активного оборудования компьютерной сети)
16 OFDM – Orthogonal Frequency-Division Multiplexing (англ. Ортогональное частотное разделение каналов с мультиплексированием)
17 OSI – Open Systems Interconnection (англ. Проект по созданию сетевых стандартов для обеспечения совместимости сетевой инфроструктуры от разных поставщиков.)
18 PoE – Power over Ethernet (англ. Питание через интернет кабель)
19 RADIUS – Remote Authentication in Dial–In User Service (англ. протокол для реализации аутентификации, авторизации и сбора сведений об использованных ресурсах)
20 SSID – Service Set Identifier (англ. Идентификатор беспроводной сети)
21 UDP – User Datagram Protocol (англ. Протокол пользовательский дейтаграмм)
22 VPN – Virtual Private Network (англ. Виртуальная частная сеть)
23 VTP – VLAN Trunking Protocol протокол ЛВС, служащий для обмена информацией во VLAN)
24 WAN – Wide Area Network (англ. Глобальная компьютерная сеть)
25 КЕО – Коэффициент Естественной Освещенности

26 ПК – Персональный Компьютер
27 ПП – Программный Продукт
28 ПО – Программное Обеспечение
29 РК – Республика Казахстан
30 СКС – структурированная кабельная сеть;
31 СПбГБУК – Санкт-Петербургское Государственное Бюджетное Учреждение Культуры
32 СПбГБСС – Санкт-Петербугская Государственная Библиотека для Слепых и Слабовидящих
33 ЭИИМ – эффективная изотропно излучаемая мощность

Приложение А

На рисунках А1-А3 представлены рисунки помещения этажей

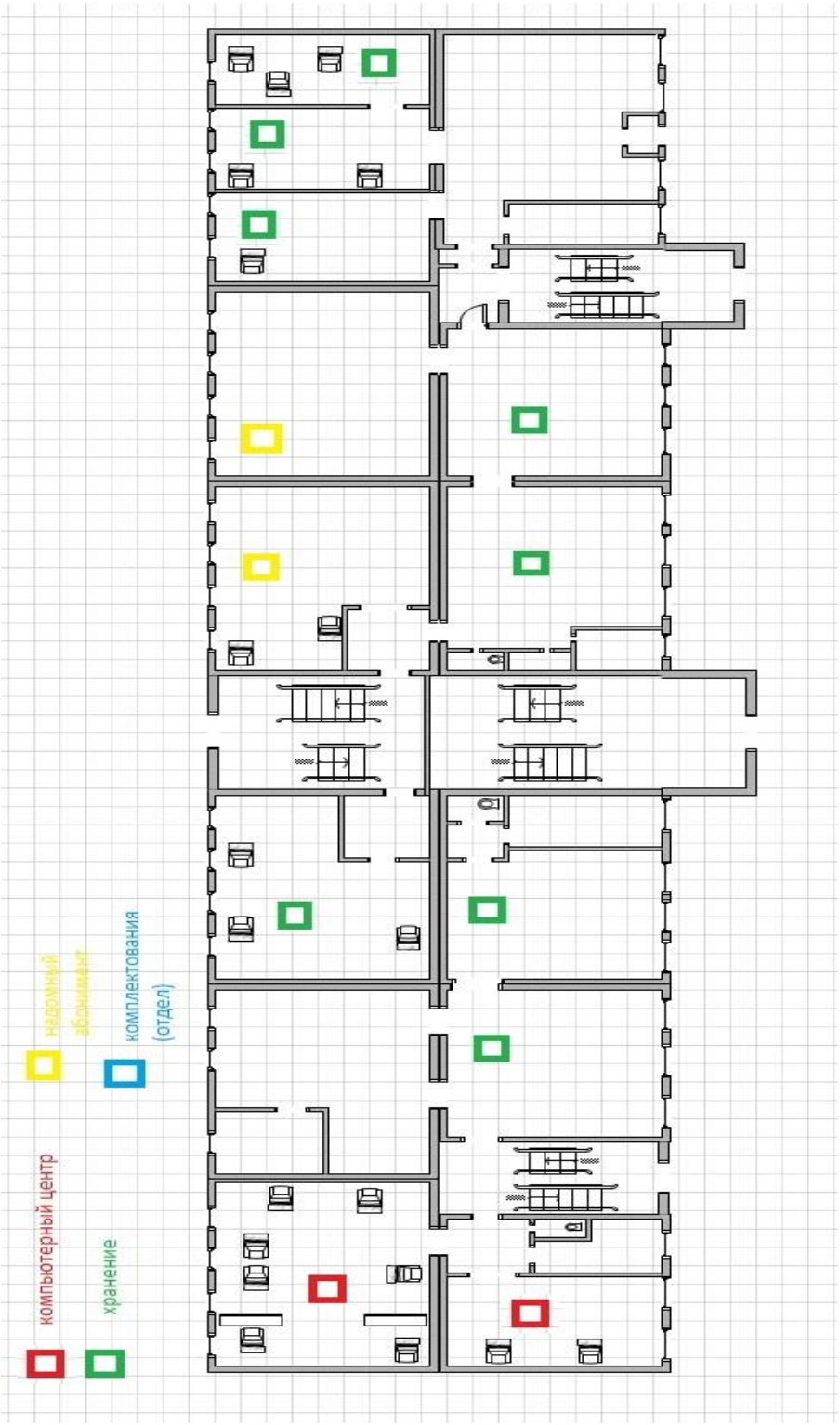

Рисунок А.1 – Схема первого этажа

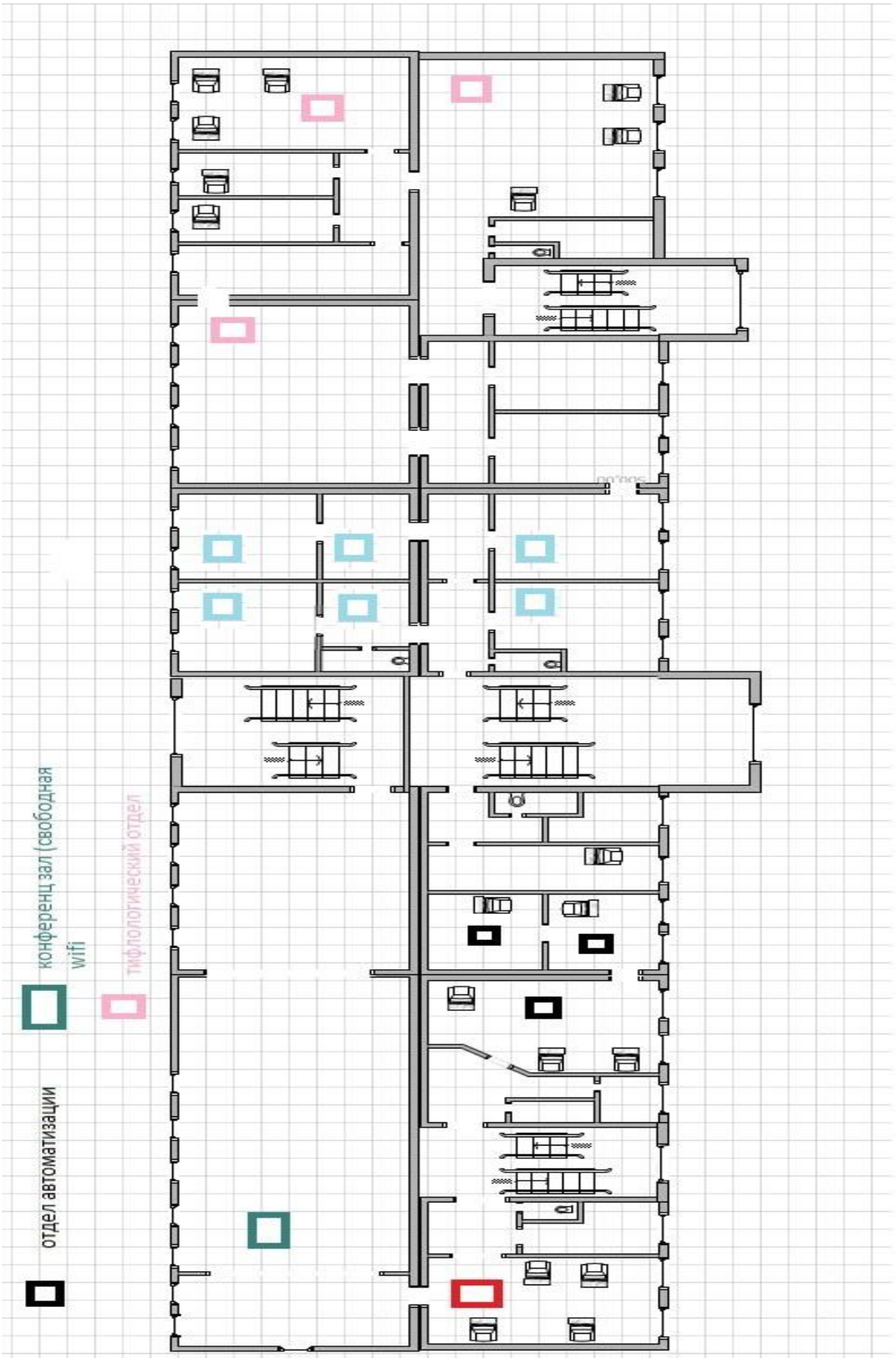

Рисунок А.2 – Схема второго этажа

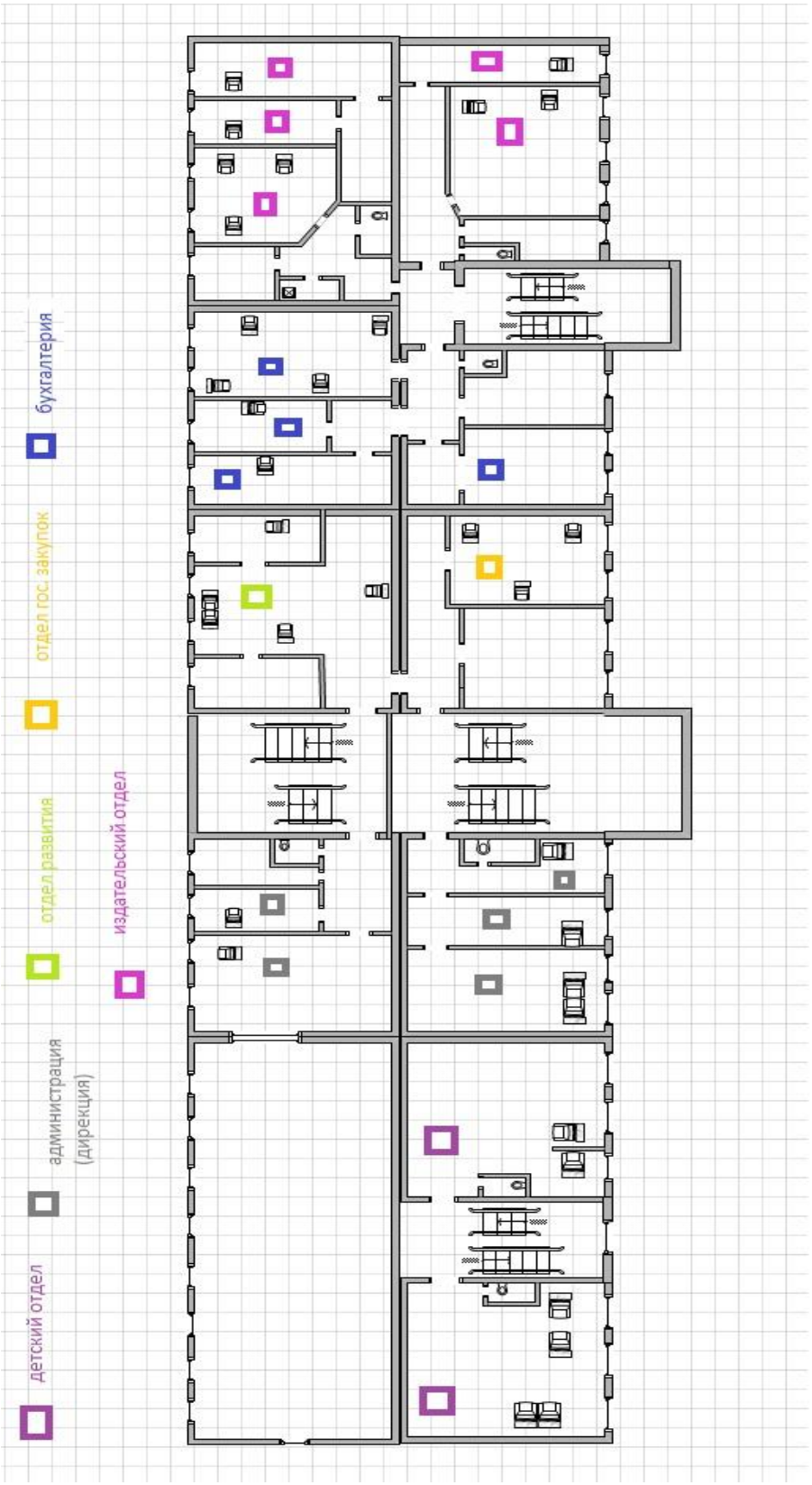

Рисунок А.3 – Схема третьего этажа

Приложение Б

Технические характеристики коммутатора D-link DWS-3024
Внешний вид устройства представлен на рисунке Б1

Рисунок Б1 – Внешний вид DWS-3024

Интерфейсы устройства:

– 24 порта 10/100/1000BASE-T с поддержкой PoE 802.3af;
– 4 комбо-порта SFP+;
– консольный порт RS-232.

Резервный источник питания:

– коннектор для подключения источника питания DPS-600.

Power over Ethernet:

– стандарт: 802.3af;
– выходная мощность на каждом порту: 15,4Вт;
– общая выходная мощность: 370 Вт;
– автоотключение порта при значении тока выше 350мА.

Производительность:

– коммутационная матрица: 48 Гбит/с;
– макс. скорость передачи пакетов: 35,71 Mpps;
– метод коммутации: Store and Forward;
– размер буфера пакетов: 750 КБ.

Управление потоком:

– управление потоком 802.3x в режиме полного дуплекса;
– метод «обратного давления» в полудуплексном режиме.

Дополнительные трансиверы SFP:

– DEM-310GT Трансивер SFP 1000BASE-LX, SMF, макс. расстояние до 10 км,3.3В;
– DEM-311GT Трансивер SFP 1000BASE-SX, MMF, макс. расстояние до 550 м, 3.3В;
– DEM-312GT2 Трансивер SFP 1000BASE-SX, MMF, макс. расстояние до 2 км, 3.3В;
– DEM-314GT Трансивер SFP 1000BASE-LH, SMF, макс. расстояние до 50 км, 3.3В;
– DEM-315GT Трансивер SFP 1000BASE-ZX, SMF, макс. расстояние до 80 км, 3.3В;

– DEM-330T Трансивер SFP 1000BASE-LX, SMF, макс. расстояние до 10 км, 3.3В, WDM (Tx: 1550 nm, Rx: 1310 nm);

– DEM-330R Трансивер SFP 1000BASE-LX, SMF, макс. расстояние до 10 км, 3.3В, WDM (Tx: 1310 nm, Rx:1550 nm);

– DEM-331T Трансивер SFP 1000BASE-LX, SMF, макс. расстояние до 40 км, 3.3В, WDM (Tx: 1550 nm, Rx: 1310 nm);

– DEM-331R Трансивер SFP 1000BASE-LX, SMF, макс. расстояние до 40 км, 3.3В, WDM (Tx: 1310 nm, Rx:1550 nm).

Функции управления WLAN:

– до 48 точек доступа (Непосредственное подключение или через коммутатор LAN);

– до 2048 беспроводных пользователей (1024 пользователей при использовании туннелирования, 2048 пользователей, если туннелирование не используется).

Роуминг:

– быстрый роуминг;

– роуминг между коммутаторами и точками доступа, подключенными к одному коммутатору;

– внутри и межсетевой роуминг.

Управление доступом и полосой пропускания:

– до 16 SSID на точку доступа (8 SSID на радиочастотный диапазон);

– балансировка нагрузки между точками доступа на основе количества пользователей или использования точки доступа.

Управление точками доступа:

– автоматическое обнаружение точек доступа;

– удаленная перезагрузка точек доступа;

– мониторинг точек доступа: список управляемых точек доступа, несанкционированных и не прошедших аутентификацию точек доступа;

– мониторинг клиентов: список клиентов ассоциированных с каждой управляемой точкой доступа;

– мониторинг клиентов Ad-hoc;

– аутентификация точек доступа с помощью локальной базы данных или внешнего сервера RADIUS;

– централизованное управление каналами/политиками безопасности;

– автоматическая настройка каналов точек доступа;

– автоматическая настройка выходной мощности передачи точек доступа.

Функции безопасности WLAN:

– WPA Personal/Enterprise;

– WPA2 Personal/Enterprise;

Продолжение приложения Б

– 64/128/152-битное WEP-шифрование;

– классификация беспроводных станций и точек доступа на основе канала, MAC-адреса, SSID, времени;

– классификация несанкционированных и действительных точек доступа на основе MAC-адреса;

– типы шифрования: WEP, WPA, Dynamic WEP, TKIP, AES-CCMP, EAP-TLS, EAP-TTLS, EAP-MD5, PEAP-GTG, PEAP-MS-CHAPv2, PEAP-TLS;

– адаптивный портал;

– аутентификация на основе MAC-адресов;

– изоляция станции.

Функции 2 уровня:

– размер таблицы MAC-адресов: 8K записей;

– IGMP Snooping: 1K многоадресных групп;

– Spanning Tree:
  - 8021.D Spanning Tree;
  - 802.1w Rapid Spanning Tree;
  - 802.1s Multiple Spanning Tree.

– Агрегирование каналов 802.3ad:
  - до 32 групп;
  - до 8 портов в группе.

– 802.1ab LLDP;

– зеркалирование портов:
  – One-to-One;
  – Many to One.

– Размер Jumbo-фреймов: до 9Кб;

– VLAN:
  – 802.1Q VLAN Tagging;
  – 802.1V+ VLAN на основе MAC-адресов;
  – Double VLAN;
  – группы VLAN Groups: до 3965;
  – VLAN на основе подсетей GVRP.

Функции 3 уровня:

– статическая маршрутизация IPv4;

– плавающие статические маршруты;

– proxy ARP;

– размер таблицы маршрутизации: до 128 статических маршрутов;

– VRRP;

– QoS (Качество обслуживания):
  – очереди приоритетов 802.1p (до 8 очередей на порт);
  – CoS на основе: порта коммутатора, VLAN, DSCP, номера порта TCP/UDP, TOS, MAC-адреса источника/приемника, IP - адреса источника/приемника.
– Минимальная гарантия по полосе пропускания на очередь;
– Формирование трафика на порт.

Списки управления доступом (ACL):

– ACL на основе: порта коммутатора, MAC-адреса, очередей приоритетов 802.1p, VLAN, Ethertype, DSCP, IP-адреса, типа протокола, номера порта TCP/UDP.

Функции безопасности LAN:

– аутентификация RADIUS;
– аутентификация TACACS;
– SSH v1, v2;
– SSL v3;
– функция Port Security:
  – 20 MAC-адресов на порт;
  – Уведомления в случае срабатывания функции.
– Фильтрация MAC-адресов;
– Управление доступом 802.1x на основе портов и Guest VLAN;
– Защита от атак DoS;
– Управление широковещательным штормом в диапазоне от 0 до 255Kpps защищенный порт;
– DHCP-фильтрация.

Методы управления:

– Web-интерфейс;
– сервер Telnet: до 5 сессий;
– клиент TFTP;
– несколько файлов конфигурации;
– клиент BOOTP/DHCP;
– SNTP;
– Поддержка двух копий ПО (Dual Images);
– CLI;
– клиент Telnet;
– SNMP v1, v2c, v3;
– RMON v1: 4 группы (Statistics, History, Alarms, Events);
– Сервер DHCP;
– SYSLOG.

– на устройство: Power, Console, RPS;
– для порта 10/100/1000BASE-T: Link/Activity/Speed, PoE;
– для слота SFP: Link/Activity.

Физические параметры:

– питание: 100-240 В переменного тока, 50/60 Гц, внутренний универсальный источник питания с активной системой PFC;
– потребляемая мощность: 450 Вт (макс., при функционировании всех портов PoE);
– тепловыделение: 1535.49 BTU/час;
– вентиляция: 4 вентилятора 40 x 40 мм.

Размеры:

– 440 (Ш) x 389 (Г) x 44 (В) мм;
– установка в 19” стойку, высота 1U;
– вес 6кг.

Температура:

– рабочая температура: от 0° до 40° С;
– температура хранения: от -10° до 70° С.

Влажность:

– рабочая влажность: от 10% до 90% без образования конденсата;
– влажность хранения: от 5% до 90% без образования конденсата.

Электромагнитная совместимость:

– FCC Class A;
– VCCI;
– C-Tick;
– ICES-003;
– CE;
– EN 60601-1-2.

Безопасность:

– UL;
– CB.

Приложение В

Технические характеристики Asus RT-AC68U

Внешний вид устройства представлен на рисунке В1.

Рисунок В1 – Asus RT-AC68U

Общие характеристики:
– тип – Wi-Fi точка доступа.
Стандарт беспроводной связи:
– 802.11a/b/g/n/ac.
Частота:
– 2.4ГГц;
– 5ГГц;
– возможность одновременной работы.
Макс. скорость беспроводного соединения – 1900 Мбит/с.
Защита информации:
– WEP;
– WPA;
– WPA2;
– 802.1x.
Опции точки доступа/моста:
– коммутатор – 4xLAN;
– скорость портов – 1000 Мбит/сек;
– режим моста;

– режим репитера (повторителя);
– количество разъемов USB 2.0 Type A – 1;
– количество разъемов USB 3.0 Type A – 1.

Расширенные функции:
– скачивание файлов;
– файловый сервер;
– FTP-сервер;
– UPnP;
– AV-сервер.

Гостевая сеть.

Поддержка IPv6.

Маршрутизатор:
– межсетевой экран (FireWall);
– NAT;
– SPI;
– DHCP-сервер;
– поддержка Dynamic DNS;
– демилитаризованная зона (DMZ);
– статическая маршрутизация;
– протоколы динамической маршрутизации IGMP v1, IGMP v2;
– VPN;
– поддержка VPN pass through;
– поддержка VPN-туннелей.

Антенна:
– количество внешних антенн – 3;
– тип внешней антенны – съемная;
– мониторинг и конфигурирование;
– Web-интерфейс.

Память:
– объем оперативной памяти – 256 Мб;
– объем флеш-памяти – 128 Мб.

Дополнительно:
– возможность подключения 3G-модема;
– возможность подключения LTE-модема;
– интерфейс встроенного принт-сервера – USB;
– флэш-память;
– размеры (ШхВхГ) – 220х160х83 мм;
– вес –640 г;
– режим WDS;
– поддержка IPTV.

Приложение Г

Технические характеристики адаптера беспроводной связи Asus PCE AC68.

Внешний вид адаптера представлен на рисунке Г1.

Рисунок Г1 – Asus PCE AC68.

Общие характеристики:
– тип Wi-Fi адаптер;
– стандарт беспроводной связи 802.11a/b/g/n/ac.
Частота:
– 2.4 ГГц;
– 5 ГГц;
– возможность одновременной работы.
Макс. скорость беспроводного соединения – 1900 Мбит/с.
Интерфейс подключения – PCI-E.
Защита информации:
– WEP;
– WPA;
– WPA2.
Антенна:
– количество внешних антенн – 3;
– тип внешней антенны – съемная.
Дополнительно:
– размеры (ШхВхГ) – 103x21x69 мм;
– вес – 125 г.

Приложение Д

Технические характеристики маршрутизатора Cisco 1941
Внешний вид устройства представлен на рисунке Д1

Рисунок Д1 – внешний вид маршрутизатора cisco 1941

Производитель – Cisco.
Модель – CISCO1941/K9.
Память:
– RAM – Установлено 512 МБ. Возможно расширение до 2,5 ГБ;
– Флеш память – Установлено 256 МБ. Возможно расширение до 4 ГБ.
Сеть:
– Технология соединения – проводная;
– Протокол передачи данных Ethernet, Fast Ethernet, Gigabit Ethernet;
– Протокол сети IPSec.
Удаленное управление – RMON, SNMP.
Протоколы маршрутизации:
– BGP;
– GRE;
– OSPF;
– DVMRP;
– EIGRP;
– IS-IS;
– IGMPv3;
– PIM-SM;
– PIM-SSM;
– статическая IPv4 и IPv6 маршрутизация.
Поддерживает:
– VPN;
– DMVPN;
– IPv6;
– MPLS;
– Syslog.
Установлены:

– фаервол;
– функция фильтрации контента;
– DMVPN;
– WRED;
– CBWFQ.

Соответствие стандартам – IEEE 802.1ag, IEEE 802.1ah.

Слоты расширения:

– 2 слота для EHWIC;
– 1 слот Double-Wide EHWIC.

Интерфейсы:

– 2 порта Ethernet 10Base-T/100Base-TX/1000Base-T, разъем RJ-45;
– 1 консольный порт управления, разъем RJ-45;
– 1 консольный порт управления, коннектор Mini-USB тип B;
– 1 последовательный вспомогательный порт, разъем RJ-45;
– 2 порта USB тип A.

Алгоритм шифрования – SSL.

Соответствие стандартам – UL 60950-1, CAN/CSA C22.2 No. 60950-1, EN 60950-1, AS/NZS 60950-1, IEC 60950-1, 47 CFR, Часть t 15, ICES-003 Класс A, EN55022 Класс A, CISPR22 Класс A, AS/NZS 3548 Класс A, VCCI V-3, CNS 13438, EN 300-386, EN 61000 (иммунитет), EN 55024, CISPR 24, EN50082-1.

ОС – Cisco IP Base.

Физические характеристики:

– Питание – Внутренний блок питания. 100-240 В переменного тока. PoE опционально;
– Габариты 89 x 343 x 292 мм;
– Вес : 5.44 кг (с источником питания, без модулей);
– 5.80 кг (с PoE, без модулей);
– 6.35 кг (типичный вес в полной конфигурации).
– Форм-фактор – Внешний. Занимает 2 юнита.
– Монтаж – в комплекте поставки есть монтажный набор на 19 дюймов.

Температура:

– Рабочая: от 0° до 40° C;
– Хранение: от 40° до 70°C;
– Влажность От 5 до 85% (без конденсата).