Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
АМУРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
(ФГБОУ ВО «АмГУ»)

Факультет математики и информатики
Кафедра информационных и управляющих систем
Направление подготовки 09.03.02 – Информационные системы и технологии
Направленность (профиль) образовательной программы Безопасность информационных систем

ДОПУСТИТЬ К ЗАЩИТЕ

Зав. кафедрой

_____ А.В. Бушманов
«____» _____2019 г.

БАКАЛАВРСКАЯ РАБОТА

на тему: Проектирование беспроводной сети на основе технологии Wi-Fi

Исполнитель
студент группы 555-об _____М.В. Литовский
(подпись, дата)

Руководитель
доцент, канд. техн. наук _____С.Г. Самохвалова
(подпись, дата)

Консультант
по безопасности и экологичности
доцент, канд. техн. наук _____ А.Б. Булгаков
(подпись, дата)

Нормоконтроль
инженер кафедры _____ В.Н. Адаменко
(подпись, дата)

Благовещенск 2019

Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего профессионального образования
АМУРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
(ФГБОУ ВПО «АмГУ»)

Факультет математики и информатики
Кафедра информационных и управляющих систем

УТВЕРЖДАЮ
Зав. кафедрой
_____ А.В. Бушманов
«____» _____

З А Д А Н И Е

К выпускной квалификационной работе студента Литовского Матвея Вадимовича

1. Тема дипломной работы: Проектирование беспроводной сети на основе технологии Wi-Fi.

(утверждена приказом от 15.04.2019 №847-уч)

2. Срок сдачи студентом законченной работы: 25.06.2019 г.

3. Исходные данные к выпускной квалификационной работе: отчет о прохождении преддипломной практики, нормативная документация, специальная литература.

4. Содержание выпускной квалификационной работы (перечень подлежащих разработке вопросов): Обоснование проектирования и формирование вариантов реализации, проектирование беспроводной сети, включающее в себя выбор сетевого оборудования, создание плана организации сети, проектирование и разработка программы, выбор реализации программы, разработка руководства, Описание методов защиты информации Wi-Fi сетей.

6. Консультанты по дипломной работе:

по безопасности и экологичности – Булгаков А.Б., доцент, кандидат технических наук.

7. Дата выдачи задания: 16.04.2019 г.

Руководитель дипломной работы: Самохвалова С.Г., доцент, кандидат технических наук.

Задание принял к исполнению: _____

РЕФЕРАТ

Бакалаврская работа содержит 101 с., 39 рисунков, 11 таблиц, 25 источников.

WI-FI, 802.11, БЕСПРОВОДНОЙ, СТАНДАРТ, ТОЧКА ДОСТУПА, КОММУТАТОР, WEP, WPA, ПАКЕТ, ДАННЫЕ, ИНФОРМАЦИЯ

В работе выполнено проектирование беспроводной сети на основе технологии Wi-Fi, осуществлен выбор варианта проектирования, создан программный продукт для мониторинга полосы пропускания и анализа трафика.

Цель бакалаврской работы: проектирование беспроводной сети на основе технологии Wi-Fi.

Выполнение работы включает основные этапы:

– обоснование проектирования и формирование вариантов реализации;

– проектирование беспроводной сети, включающее в себя выбор сетевого оборудования, создание плана организации сети, проектирование и разработку программного продукта, выбор наилучшей реализации программы, разработка руководства пользователя;

– описание методов защиты информации Wi-Fi сетей;

– обоснование безопасности и экологичности продукта.

Результатом бакалаврской работы является разработанный проект создания беспроводной сети.

СОДЕРЖАНИЕ

НОРМАТИВНЫЕ ССЫЛКИ

В настоящей бакалаврской работе были использованы ссылки на следующие стандарты и нормативные документы:

ГОСТ 2.103-68 ЕСКД Стадии разработки;

ГОСТ 2.104-68 ЕСКД Основные надписи;

ГОСТ 2.105-95 ЕСКД Общие требования к текстовым документам;

ГОСТ 2.111–2013 ЕСКД. Нормоконтроль;

ГОСТ 7.1-2003 СИБИД. Библиографическая запись. Библиографическое описание. Общие требования и правила составления;

ГОСТ 8.417-2002 Государственная система обеспечения единства измерений (ГСИ). Единицы величин (с Поправками);

ГОСТ Р 12.2.143-2009 Система стандартов безопасности труда (ССБТ). Системы фотолюминесцентные эвакуационные. Требования и методы контроля (с Изменением N 1);

ГОСТ 12.4.026-2015 Система стандартов безопасности труда (ССБТ). Цвета сигнальные, знаки безопасности и разметка сигнальная. Назначение и правила применения. Общие технические требования и характеристики. Методы испытаний (с Поправками);

ГОСТ 34.603-92 Информационная технология. Виды испытаний автоматизированных систем;

ГОСТ Р ИСО 14915-1-2010 Эргономика мультимедийных пользовательских интерфейсов. Часть 1. Принципы проектирования и структура;

ГОСТ Р 50922-2006 Защита информации. Основные термины и определения.

ОПРЕДЕЛЕНИЯ, ОБОЗНАЧЕНИЯ, СОКРАЩЕНИЯ

ГГц – гигагерц;

ГОСТ - государственный общероссийский стандарт;

М – метр;

Мб – мегабайт;

Мбит/с – мегабит в секунду;

ОС – операционная система;

ПЭВМ – персональная электронно-вычислительная машина;

СУБД – система управление базами данных;

ЭВМ – электронно-вычислительная машина;

AES – (Advanced Encryption Standard) усовершенствованный стандарт шифрования;

LINQ – (Language Integrated Query) язык интегрированных запросов;

MIMO – (Multiple Input Multiple Output) метод пространственного кодирования сигнала;

MS – Microsoft;

SQL – (Structured Query Language) структурированный язык запросов;

WEP – (Wired Equivalent Privacy) стандарт обеспечения безопасности сетей Wi-Fi;

Wi-Fi – (Wireless Fidelity) технология беспроводной локальной сети;

WLAN – (Wireless Local Area Network) беспроводная локальная сеть;

WPA и WPA2 – (Wi-Fi Protected Access) более современные стандарты обеспечения безопасности сетей Wi-Fi.

ВВЕДЕНИЕ

Технология Wi-Fi является одной из лидирующей по передаче информации по радиоканалам на рынке и в современном мире используется почти повсеместно. Сети, построенные на основе Wi-Fi, стали уже неотъемлемой частью нашей жизни в цифровой эпохе. В любом общественном месте сейчас располагаются точки доступа десятков различных сетей. Во многих квартирах жилых домов есть свои точки доступа для выхода в интернет.

Заинтересованность в сетях Wi-Fi особо распространена и среди корпоративного сектора у работодателей. В первую очередь они стремятся оптимизировать рабочий процесс и повысить производительность сотрудников, через развертывание беспроводной сети на предприятии, которая во многих случаях предпочтительнее проводной Ethernet сети и позволяет создать условия удобства при эксплуатации, а также обеспечивает сотрудникам свободу и независимость от рабочего места. Кроме того, сеть, построенная на основе технологии Wi-Fi, просто развернуть с минимальными затратами по времени, она обладает гибкостью и легкой расширяемостью. Поэтому все больше предприятий переходят на беспроводные сети, основанные на технологии Wi-Fi.

В любой сети существует поток трафика, это вся информация, которая проходит по сети и доступна всем пользователям, подключенным к ней. В правильно организованной беспроводной сети трафик строго регулируется и анализируется в режиме реального времени. Таким образом можно обнаруживать ошибки и обрывы в сетях, выявлять подозрительную активность, проверять загруженность трафика.

Для анализа потока данных существуют специальные программы. Они применяются администраторами сети для вышеописанных целей и представляют собой анализаторы трафика.

При создании такого продукта ставят целью создание легкой, не нагруженной программы, способной сканировать поток данных в заданной сети с

выявлением характеристик, таких как протокол передачи, скорость передачи, тип подключения, ip адрес и т.д.

Целью данной выпускной квалификационной работы является проектирование беспроводной сети на основе технологии Wi-Fi для Управления Федеральной службы государственной регистрации, кадастра и картографии по Амурской области с созданием современных возможностей связи.

1 АНАЛИЗ ПРЕДПРИЯТИЯ «УПРАВЛЕНИЕ РОСРЕЕСТРА»

Управление Федеральной службы государственной регистрации, кадастра и картографии по Амурской области (далее – Управление) является территориальным органом федерального органа исполнительной власти, реализующим на территории Амурской области полномочия Росреестра.

Управление в соответствии с Положением, утвержденным приказом Росреестра от 30.05.2016 №П/0263 (в редакции приказа Росреестра от 23.01.2017 №П/0027), осуществляет следующие функции [14]:

− оказание услуг в сфере государственной регистрации прав и государственного кадастрового учета на недвижимое имущество;

− проведение землеустройства, государственного мониторинга земель, геодезии и картографии, а также функции в сфере наименований географических объектов;

− осуществление государственного земельного надзора;

− функции по государственной кадастровой оценке объектов недвижимости;

− надзор за деятельностью саморегулируемых организаций оценщиков, арбитражных управляющих, кадастровых инженеров.

В соответствии с приказом Управления «О распределении полномочий в Управлении Росреестра по Амурской области» деятельность структурных подразделений, осуществляющих вышеперечисленные функции, курируют и координируют руководитель Управления и его заместители.

Наглядно это отображено в организационной структуре Управления, построенной в соответствии с распределением полномочий и ответственности должностных лиц.

Организационная структура представляет собой совокупность подразделений организации и их взаимосвязей, в рамках которой между подразделениями и должностными лицами распределяются управленческие задачи с учетом их компетенции.

Организационная структура предприятия является линейной структурой управления и подразумевает наличие начальника-руководителя, имеющего определенные полномочия и единолично руководящего деятельностью подчиненных работников, для каждого структурного подразделения.

На рисунке 1 представлена организационная структура предприятия Управления.

Линейное управление построено таким образом, что каждая ячейка и сотрудник имеют лишь одного руководителя, через него единовременно по каналу проходят команды управления. При такой организации управленческие ячейки несут ответственность за деятельность управляемых объектов и за ее результаты. Руководители назначаются по ячейкам, каждый выполняет определенный вид работ, разрабатывает и принимает решения, характерные для управления подчиненным объектом [4].

Линейная структура управления формирует своего рода иерархию руководителей, где руководитель нижнего уровня подчиняется руководителю более высокого. Распоряжения поступают с верхнего уровня на нижние по цепочке. В данной структуре реализован принцип единоначалия, который означает, что подчиненные сотрудники выполняют распоряжения и поручения только своего непосредственного начальника. А вышестоящие органы управления лишены права контролировать деятельность исполнителей, обходя их назначенного начальника.

Управление возглавляет руководитель, назначенный на должность и так же освобождаемый от нее Министром экономического развития Российской Федерации в установленном порядке. Руководитель несет ответственность за исполнение обязанностей и полномочий, возложенных на Управление и осуществляет руководство его деятельностью. У руководителя имеется до пяти заместителей, назначаемых и снимаемых с должности им самим. Необходимое количество заместителей также определяется руководителем [9].

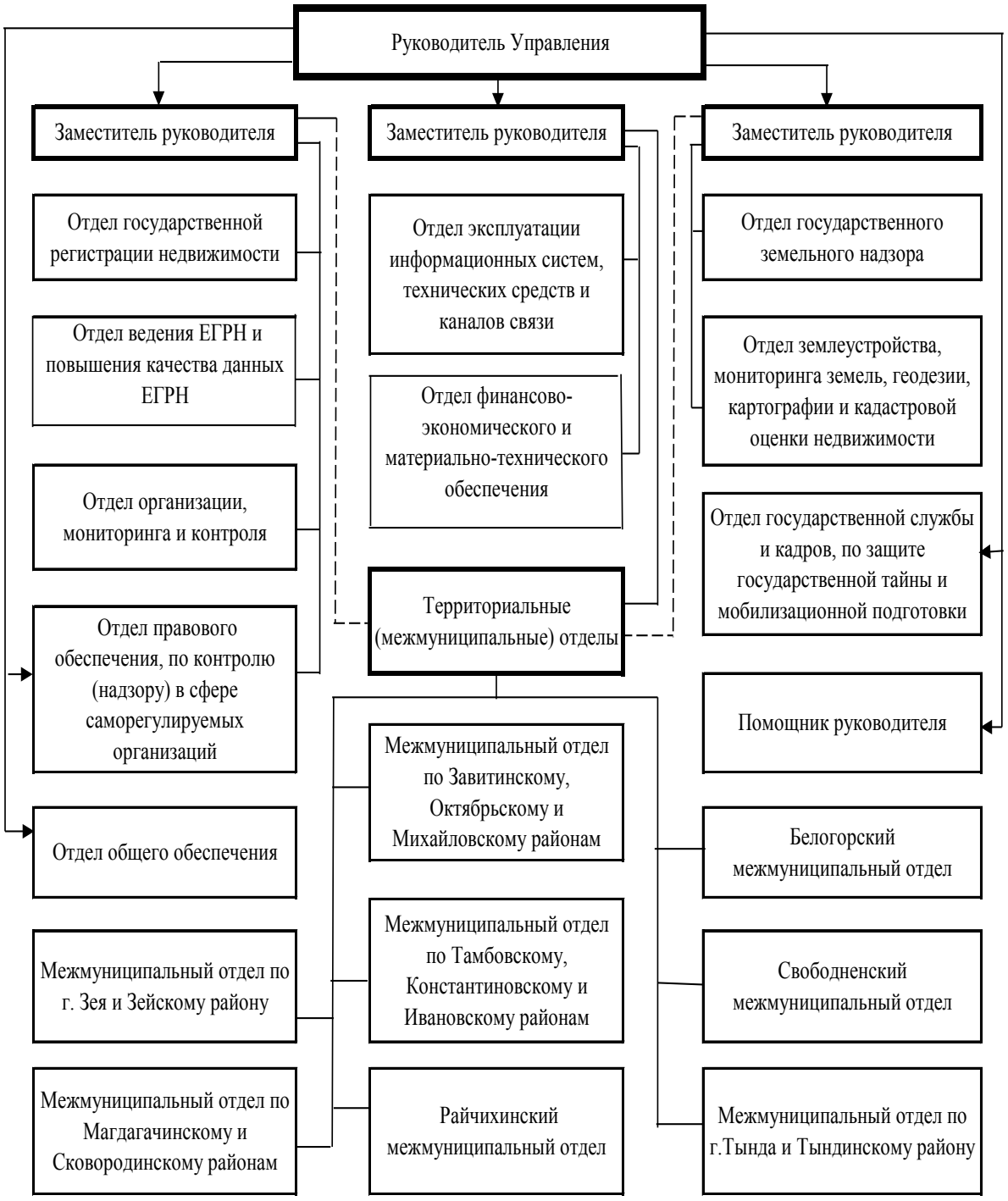


Рисунок 1 – Организационная структура «Управления Росреестра по Амурской области»

Каждый отдел предприятия возглавляется начальником, назначенным руководителем Управления. В обязанности назначенного на должность начальника отдела входит руководство деятельностью отдела на основе принципа еди-

ноначалия, обеспечение подбора, расстановки и профессиональной подготовки работников отдела, соблюдение ими служебной дисциплины, режима требуемой секретности, служебного распорядка рабочего дня. Кроме того, начальник несет персональную ответственность за выполнение всех задач и функций, возлагаемых на подконтрольный ему отдел.

На отдел ведения ЕГРН, повышения качества данных ЕГРН возлагаются задачи по организации и обеспечению, координации и контролю постоянного хранения ЕГРН; комплектованию архива управленческой документации делами постоянного и временного хранения.

Отдел организации, мониторинга и контроля осуществляет и выполняет контроль за реализацией мероприятий федеральных целевых программ и проектов Росреестра; разработку аналитических материалов по вопросам государственной регистрации прав и вопросам государственного кадастрового учета; координацию, контроль и развитие межведомственного взаимодействия; мониторинг качества предоставляемых государственных услуг по государственной регистрации и кадастровому учету; координацию формирования установленной отчетности Управления, контроль за предоставлением статистической отчетности в Росреестр [14].

Отдел правового обеспечения ответственен за правовое обеспечение деятельности Управления; осуществляет юридическую и судебную защиту прав и интересов Управления [14].

Отдел государственной регистрации недвижимости выполняет следующие задачи: проведение правовой экспертизы документов; проверка действительности поданных заявителем документов; проверка юридической силы правоустанавливающих документов; формирование разделов Единого государственного реестра прав и т.д. [14].

Финансово-экономический отдел оперативно и перспективно планирует расходы на содержание центрального аппарата Росреестра, территориальных органов и подведомственных организаций.

Отдел государственного земельного надзора реализует выполнение следующих задач: Осуществление государственного земельного надзора; участие в реализации мероприятий федеральных целевых программ, в том числе разработка технических заданий, проектов конкурсных или аукционных документаций по направлению деятельности отдела; разработка и утверждение в установленном порядке планов проверок по осуществлению государственного земельного надзора, а также контроль их реализации; участие в заключении государственных договоров, соглашений и контрактов по предмету деятельности отдела, контроль за качеством исполняемых работ.

Отдел государственной службы и кадров предназначен для выполнения следующих функций [14]:

– ведение реестра должностей государственной гражданской службы;

– формирование кадрового резерва и его эффективное использование;

– рассмотрение обращений, заявлений и жалоб физических и юридических лиц, органов государственной власти, органов местного самоуправления по вопросам, входящим в компетенцию отдела;

– координация и контроль деятельности территориальных отделов;

– оформление отпусков, командировочных удостоверений, больничных листов, пенсий за выслугу лет;

– организация и проведение конкурсов на замещение вакантных должностей федеральной государственной гражданской службы, аттестаций и др.

Отдел землеустройства и мониторинга земель, геодезии и картографии существует для организации, координации и контроля за выполнением топографо-геодезических и картографических работ; лицензирования геодезической и картографической деятельности в установленном порядке; подготовки в соответствии с законодательством Российской Федерации экспертных заключений о степени секретности геодезических и картографических материалов и данных; выявления и предотвращения незаконной геодезической и картографической деятельности; осуществления государственного геодезического надзора за

геодезической и картографической деятельностью.

Отдел эксплуатации информационных систем, технических средств и каналов связи выступал местом прохождения преддипломной практики. Поэтому его функционал следует рассмотреть более детально для составления максимально полного и подробного представления.

Отдел эксплуатации информационных систем, технических средств и каналов связи Управления Федеральной службы государственной регистрации, кадастра и картографии по Амурской области является структурным подразделением Управления Федеральной службы государственной регистрации, кадастра и картографии по Амурской области. В своей работе Отдел руководствуется Конституцией Российской Федерации, федеральными конституционными законами, федеральными законами, актами Президента Российской Федерации, Правительства Российской Федерации, актами Минэкономразвития России, Росреестра, Управления, Положением об Управлении Федеральной службы государственной регистрации, кадастра и картографии по Амурской области, утвержденным приказом Росреестра от 28.10.2009 №313, а также положением «об отделе эксплуатации информационных систем, технических средств и каналов связи Управления Федеральной службы государственной регистрации, кадастра и картографии по Амурской области».

Основными задачами отдела являются:

− обеспечение комплекса мероприятий по сопровождению государственных информационных систем Управления, их компонентов, а также информационно-коммуникационных систем, необходимых для их функционирования;

− администрирование информационных систем, а также прикладных программных средств, эксплуатируемых в Управлении, включая организацию доступа пользователей и учет информационных ресурсов Управления;

− проведение комплекса мероприятий по обеспечению информационной безопасности персональных данных, защиты конфиденциальной информации в электронном виде от несанкционированного доступа, искажения и уничтоже-

ния при ее передаче, обработке и хранении с использованием средств вычислительной Техники и криптографической защиты;

− формирование и передача информации о зарегистрированных правах организациям в порядке и сроки, предусмотренные действующим законодательством, соглашениями о порядке взаимодействия в области предоставления информации о зарегистрированных правах на объекты недвижимого имущества;

− проведение работ по повышению качества и сопоставимости данных в государственных информационных системах Управления, в рамках компетенции отдела;

− обеспечение бесперебойной работы, функционирования и модернизации компьютерной, организационной, телекоммуникационной техники, а также прикладного и системного программного обеспечения, необходимого для выполнения задач, возложенных на Управление;

− координация деятельности структурных подразделений Управления по вопросам, отнесенных в компетенцию отдела.

Отдел в соответствии с возложенными на него задачами осуществляет следующие функции [14]:

– прорабатывает единую политику развития информационных технологий в Управлении;

– участвует в выработке предложений по планированию закупок и распределению средств вычислительной и организационной техники, систем климат-контроля серверных помещений, оборудования бесперебойного электропитания, программного обеспечения, услуг аутсорсинга по направлениям информатизации в Управлении;

– обеспечивает функционирование внутриведомственного и межведомственного взаимодействия в электронном виде в рамках ответственности Управления;

– вносит руководителю Управления и заместителю руководителя Управления предложения об улучшении работы в сфере информационных технологий;

– разрабатывает проекты приказов, распоряжений в пределах компетенции Отдела;

– осуществляет разработку и развитие нормативов документов, методической базы, планов-графиков, относящихся к созданию, использованию и развитию информационных технологий, технологических процессов, а также защите информации в Управлении;

– осуществляет сбор и анализ данных об обеспечении подразделений оборудованием компьютерной и организационной техникой, необходимыми запасными частями к ним;

– взаимодействует в установленном порядке с технической поддержкой программного обеспечения и технических средств, используемых в Управлении;

– проводит внедрение новых информационных технологий, технологических процессов, а также обеспечивает их дальнейшую поддержку в рамках компетенции Отдела;

– подготавливает статистическую отчётность, установленную соответствующими приказами Федеральной службы государственной регистрации, кадастра и картографии, а также Управления, обеспечивает ее достоверность;

– проводит наполнение официального сайта (подсайта) Управления на основе заявок структурных подразделений Управления;

– разрабатывает инструкции по применению технических средств и программного обеспечения в Управлении;

– оказывает методическую и практическую помощь специалистам Управления в части компетенции отдела;

– изучает зарубежный и отечественный опыт в области информационных технологий;

– проводит предварительную экспертизу средств вычислительной техники, средств коммуникации и связи на предмет необходимости и целесообразности ремонта;

– выполняет периодические профилактические работы технических средств и программно-аппаратных комплексов, используемых в Управлении.

На примере организационной структуры предприятия видны достоинства используемой линейной структуры:

− строгое и четкое разграничение ответственности;

− относительно простой контроль подчиненных;

− простые коммуникации внутри иерархии;

− понятное определение компетенций;

− быстрые формы принятий решений.

Однако, данный тип структуры имеет и весомые недостатки:

− серьезная ответственность руководителя;

− высокие профессиональные требования к руководителю;

− авторитарная форма руководства;

− низкий уровень специализации руководителей;

− затрудненные коммуникации между исполнителями.

2 АНАЛИЗ И ХАРАКТЕРИСТИКА ПРЕДМЕТНОЙ ОБЛАСТИ

2.1 Особенности технологий беспроводного доступа

Развитие радиотехники привело к созданию беспроводного способа передачи информации, которая осуществлялась «по воздуху», без проводов. Само определение «беспроводной» (wireless) использовалось для обозначения радиосвязи как таковой в широком смысле этого слова. Однако, с течением времени определение перестало употребляться как таковое и его как эквивалент заменило слово «радио» (radio), а также «радиочастота» (radio frequency). В настоящее время и то, и другое понятия приняты синонимами в контексте описания диапазона частот 3 кГц – 300 ГГц. Впрочем, это не исключает того факта, что термин «радио» в большинстве случаев используется для описания технологий, которые давно находятся в обиходе обычных людей. Например, радиотелефония, радиовещание, радиолокация и т.д. Более новые и современные технологии, такие, как сотовая связь, абонентский доступ, доступ в интернет и т.п., характеризуют определением «беспроводной».

В основном беспроводные сети разделяют на 3 типа (рисунок 2): WWAN (Wireless Wide Area Network), WLAN (Wireless Local Area Network) и WPAN (Wireless Personal Area Network).

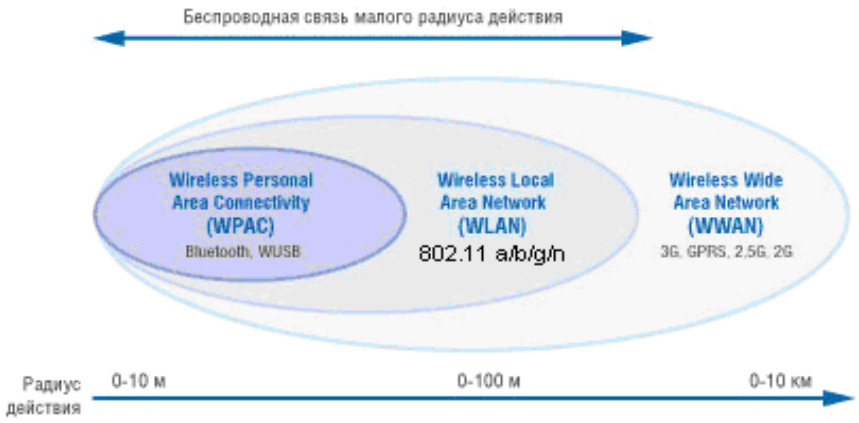


Рисунок 2 – Радиус действия персональных, локальных и глобальных беспроводных сетей

При построении некоторых беспроводных сетей могут применятся очень схожие технологии. Например, WLAN, WPAN, а также системы широкополосного беспроводного доступа BWA (Broadband Wireless Access) строятся на похожих технологиях. А разница заключена в том, что сети имеют различный диапазон рабочих частот и характеристики радиоинтерфейса (рисунок 3).

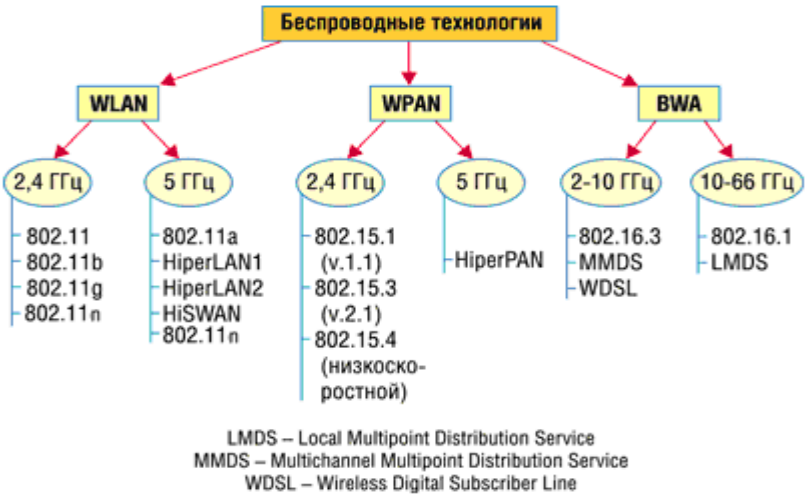


Рисунок 3 – Классификация беспроводных технологий

WLAN и WPAN поддерживают частоты от 2,4 ГГц до 5 ГГц в нелицензионных диапазонах. Они не нуждаются в частотном планировании и координации с остальными радиосетями, которые работают в том же диапазоне. В то же время сети BWA могут работать не только в нелицензионных диапазонах, но и в лицензионных, поддерживая частоты от 2 ГГц до 66 ГГц [23].

Сети WLAN – это беспроводные локальные сети, основная задача которых организация доступа к информационным ресурсам внутри одного выделенного здания. Кроме того, данные сети используются для создания общественных точек доступа (hot spots) в местах большого скопления людей. Такие точки устанавливаются чаще всего в отелях и гостиницах, кафе, аэропортах. В некоторых случаях они организуются на период проведения мероприятий, которые посещают множество людей. Такие точки могут использоваться в качестве домашнего доступа в интернет [7].

Широко известные сети, именуемые Wi-Fi (Wireless Fidelity), основаны на категории стандартов IEEE 802.11. Определение «Wi-Fi» нигде в стандартах не значится, но сам бренд Wi-Fi и его символика широко распространены и известны в мире.

2.2 История развития

В 1990 г. Комитет по стандартам IEEE 802 (Institute of Electrical and Electronic Engineers) сформировал рабочую группу по стандартам для беспроводных локальных сетей 802.11. Эта группа занялась разработкой всеобщего стандарта для радиооборудования и сетей, работающих на частоте 2.4 ГГц со скоростями 1-2 Мбит/с. Работы по созданию стандарта были завершены через семь лет, и в июне 1997 г. была ратифицирована первая спецификация 802.11 [6].

Стандарт IEEE 802.11 стал первым стандартом для продуктов WLAN от независимой международной организации. Однако к моменту выхода стандарта в свет первоначально заложенная в нем скорость передачи данных оказалась недостаточной. Это послужило причиной последующих доработок, поэтому на сегодняшний день существуют целые группы стандартов [22].

2.3 Стандарты Wi-Fi

Современные стандарты, используемые наиболее широко по всему миру, относятся к группе IEEE 802.11. Каждый из них имеет свои отличительные особенности и характеристики [7].

В таблице 1 приведены основные стандарты и их характеристики.

2.3.1 Стандарт 802.11g

Этот стандарт стал продолжателем стандарта 802.11b. Принятый уже в 2003 году он подразумевает передачу данных в аналогичном диапазоне, но при этом предлагает более высокие скорости. Несравненным достоинством является то, что стандарт 802.11g имеет обратную совместимость с 802.11b. Устройства 802.11g должны поддерживать работу с устройствами 802.11b [1].

Таблица 1 – Характеристики стандартов группы IEEE 802.11

Стандарт	802.11g	802.11a	802.11n
Частотный диапазон, ГГц	2,4-2,483	5,15-5,25	2,4 или 5,0
Метод передачи	DSSS,OFDM	DSSS,OFDM	MIMO
Скорость, Мбит/с	1-54	6-54	6-300
Совместимость	802.11 b/n	802.11 n	802.11 a/b/g
Метод модуляции	BPSK, QPSK OFDM	BPSK, QPSK OFDM	BPSK, 64-QAM
Дальность связи в помещении, м	20-50	10-20	50-100
Дальность связи вне помещения, м	250	150	500

Предельно возможная скорость в этом стандарте составляет 54 Мбит/с. Разработка стандарта 802.11g не стала однозначным решением. Две компании предложили конкурирующие технологии как альтернативу. Компания «Intersil» выдвинула для рассмотрения метод ортогонального частотного разделения OFDM, который был позаимствован из стандарта 802.11a, а метод двоичного пакетного сверточного кодирования PBCC был предложен компанией «Texas Instruments». Компромиссом в этом вопросе стало принятое решение: базовыми технологиями в стандарте применяются OFDM и CCK, использование же PBCC предусмотрено опционально.

Сверточное кодирование (Packet Binary Convolutional Coding, PBCC) в своем основании несет идею о преобразовании входящей последовательности информационных бит в сверточном кодере. Происходит оно таким образом, чтобы каждому входному биту соответствовало более одного выходного. Иными словами, сверточный кодер добавляет определенную избыточную информацию к исходной последовательности. Например, если каждому входному биту

соответствуют два выходных, то идет речь о сверточном кодировании со скоростью равной 1/2. В случае, если каждым двум входным битам соответствуют три выходных, то скорость сверточного кодирования будет составлять уже 2/3.

PBCC метод применяется по выбору в протоколе 802.11b на скоростях 5,5 Мбит/с и 11 Мбит/с. По аналогии он используется и в протоколе 802.11g для тех же скоростей. В целом из-за совместимости протоколов 802.11b и 802.11g технологии кодирования и скорости, предусмотренные 802.11b, поддерживаются так же в протоколе 802.11g. В этом плане до скорости 11 Мбит/с протоколы 802.11b и 802.11g совпадают друг с другом, за исключением того, что в протоколе 802.11g предусмотрены те скорости, которых не поддерживаются в протоколе 802.11b.

По выбору в протоколе 802.11g технология PBCC может использоваться при скоростях передачи 22 Мбит/с и 33 Мбит/с.

2.3.2 Стандарт 802.11a

Стандарт IEEE 802.11a обеспечивает передачу данных на тех же 54 Мбит/с, но в отличие от базового стандарта спецификации 802.11a предусматривают работу в новом частотном диапазоне 5ГГц. В качестве метода модуляции сигнала выбрано ортогонально частотное мультиплексирование (OFDM), обеспечивающее высокую устойчивость связи в условиях многолучевого распространения сигнала [18].

В соответствии с правилами FCC частотный диапазон UNII разбит на три 100-мегагерцевых поддиапазона, различающихся ограничениями по максимальной мощности излучения. Низший диапазон (от 5,15 до 5,25 ГГц) предусматривает мощность всего 50 мВт, средний (от 5,25 до 5,35 ГГц) — 250 мВт, а верхний (от 5,725 до 5,825 ГГц) — 1 Вт. Использование трех частотных поддиапазонов с общей шириной 300 МГц делает стандарт IEEE 802.11a самым широкополосным из семейства стандартов 802.11 и позволяет разбить весь частотный диапазон на 12 каналов, каждый из которых имеет ширину 20 МГц, причем восемь из них лежат в 200-мегагерцевом диапазоне от 5,15 до 5,35 ГГц,

а остальные четыре канала — в 100-мегагерцевом диапазоне от 5,725 до 5,825 ГГц (рисунок 4). При этом четыре верхних частотных канала, предусматривающие наибольшую мощность передачи, используются преимущественно для передачи сигналов вне помещений.

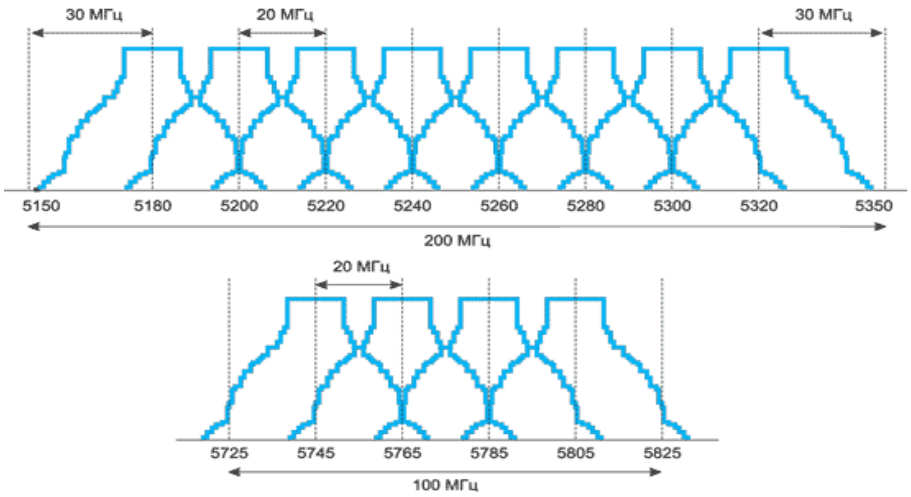


Рисунок 4 – Разделение диапазона UNII на 12 частотных поддиапазонов

Стандарт IEEE 802.11a основан на технике частотного ортогонального разделения каналов с мультиплексированием (OFDM). Для разделения каналов применяется обратное преобразование Фурье с окном в 64 частотных подканала. Поскольку ширина каждого из 12 каналов, определяемых в стандарте 802.11a, имеет значение 20 МГц, получается, что каждый ортогональный частотный подканал (поднесущая) имеет ширину 312,5 кГц. Однако из 64 ортогональных подканалов задействуется только 52, причем 48 из них применяются для передачи данных (Data Tones), а остальные — для передачи служебной информации (Pilot Tones) [17].

2.3.3 Стандарт 802.11n

Данный стандарт считается относительно новым и был принят 11 сентября 2009 года. 802.11n выделяется своей максимально допустимой скоростью передачи данных, которая находится на уровне проводных стандартов и составляет примерно 300 Мбит/с. Она почти в 5 раз превышает производительность классического Wi-Fi.

Основными преимуществами стандарта являются:

− большая скорость передачи данных;

− равномерное, устойчивое, надежное и качественное покрытие зоны действия станции, отсутствие непокрытых участков;

− совместимость с предыдущими версиями стандарта Wi-Fi.

Но наряду с этим он имеет и свои недостатки:

− большая мощность потребления;

− только два рабочих диапазона (с заменой оборудования);

− усложненная и более габаритная аппаратура.

Увеличение скорости передачи в стандарте IEEE 802.11n достигается за счет удвоения ширины канала с 20 МГц до 40 МГц, и благодаря реализации технологии MIMO.

Технология MIMO (Multiple Input Multiple Output) предполагает применение нескольких передающих и принимающих антенн. По аналогии традиционные системы, то есть системы с одной передающей и одной принимающей антенной, называются SISO (Single Input Single Output) (рисунок 5).

Стандарт IEEE 802.11n основан на технологии OFDM-MIMO. Очень многие реализованные в нем технические детали позаимствованы из стандарта 802.11a, однако в стандарте IEEE 802.11n предусматривается использование как частотного диапазона, принятого для стандарта IEEE 802.11a, так и частотного диапазона, принятого для стандартов IEEE 802.11b/g. То есть устройства, поддерживающие стандарт IEEE 802.11n, могут работать в частотном диапазоне либо 5 ГГц, либо 2,4 ГГц [16].

Передаваемая последовательность делится на параллельные потоки, из которых на приемном конце восстанавливается исходный сигнал. Здесь возникает некоторая сложность — каждая антенна принимает суперпозицию сигналов, которые необходимо отделять друг от друга. Для этого на приемном конце применяется специально разработанный алгоритм пространственного обнаружения сигнала. Этот алгоритм основан на выделении поднесущей и оказывает-

ся тем сложнее, чем больше их число. Единственным недостатком использования MIMO является сложность и громоздкость системы и, как следствие, более высокое потребление энергии. Для обеспечения совместимости MIMO-станций и традиционных станций предусмотрено три режима работы:

− Унаследованный режим (legacy mode);

− Смешанный режим (mixed mode);

− Режим зеленого поля (green field mode);

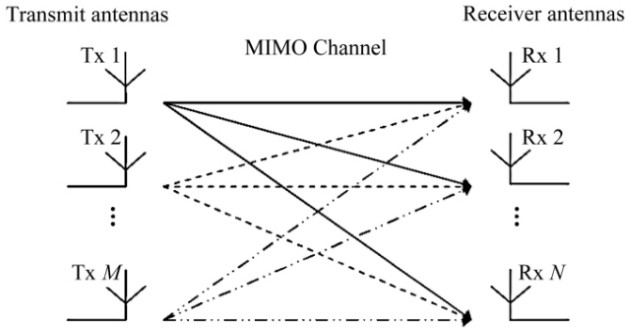


Рисунок 5 – Принцип функционирования технологии MIMO

Каждому режиму работы соответствует своя структура преамбулы — служебного поля пакета, которое указывает на начало передачи и служит для синхронизации приемника и передатчика. В преамбуле содержится информация о длине пакета и его типе, включая вид модуляции, выбранный метод кодирования, а также все параметры кодирования. Для исключения конфликтов в работе станций MIMO и обычных (с одной антенной) во время обмена между станциями MIMO пакет сопровождается особой преамбулой и заголовком. Получив такую информацию, станции, работающие в унаследованном режиме, откладывают передачу до окончания сеанса между станциями MIMO. Кроме того, структура преамбулы определяет некоторые первичные задачи приемника, такие как оценка мощности принимаемого сигнала для системы автоматической регулировки усиления, обнаружение начала пакета, смещение по времени и частоте [15].

Существует несколько режимов работы станций MIMO.

Унаследованный режим. Этот режим предусмотрен для обеспечения обмена между двумя станциями с одной антенной. Передача информации осуществляется по протоколам 802.11a. Если передатчиком является станция MIMO, а приемником — обычная станция, то в передающей системе используется только одна антенна и процесс передачи идет так же, как и в предыдущих версиях стандарта Wi-Fi. Если передача идет в обратном направлении — от обычной станции в многоантенную, то станция MIMO использует много приемных антенн, однако в этом случае скорость передачи не максимальная. Структура преамбулы в этом режиме такая же, как в версии 802.11a.

Смешанный режим. В этом режиме обмен осуществляется как между системами MIMO, так и между обычными станциями. В связи с этим системы MIMO генерируют два типа пакетов, в зависимости от типа приемника. С обычными станциями работа идет медленно, поскольку они не поддерживают работу на высоких скоростях, а между MIMO — значительно быстрее, однако скорость передачи ниже, чем в режиме зеленого поля. Преамбула в пакете от обычной станции такая же, что и в стандарте 802.11a, а в пакете MIMO она немного изменена. Если передатчиком выступает система MIMO, то каждая антенна передает не целую преамбулу, а циклически смещенную. За счет этого снижается мощность потребления станции, а канал используется более эффективно. Однако не все унаследованные станции могут работать в этом режиме. Дело в том, что если алгоритм синхронизации устройства основан на взаимной корреляции, то произойдет потеря синхронизации.

Режим зеленого поля. В этом режиме полностью используются преимущества систем MIMO. Передача возможна только между многоантенными станциями при наличии унаследованных приемников. Когда идет передача MIMO-системой, обычные станции ждут освобождения канала, чтобы избежать конфликтов. В режиме зеленого поля прием сигнала от систем, работающих по первым двум схемам, возможен, а передача им — нет. Это сделано для того, чтобы исключить из обмена одноантенные станции и тем самым повысить ско-

рость работы. Пакеты сопровождаются преамбулами, которые поддерживаются только станциями MIMO. Все эти меры позволяют максимально использовать возможности систем MIMO-OFDM. Во всех режимах работы должна быть предусмотрена защита от влияния работы соседней станции, чтобы предотвратить искажения сигналов. На физическом уровне модели OSI для этого используются специальные поля в структуре преамбулы, которые оповещают станцию о том, что идет передача и необходимо определенное время ожидания. Некоторые методы защиты принимаются и на канальном уровне.

В стандарте IEEE 802.11n допускается использование до четырех антенн у точки доступа и беспроводного адаптера. Обязательный режим подразумевает поддержку двух антенн у точки доступа и одной антенны и беспроводного адаптера. В стандарте IEEE 802.11n предусмотрены как стандартные каналы связи шириной 20 МГц, так и каналы с удвоенной шириной. Общая структурная схема передатчика изображена на рисунке 6.

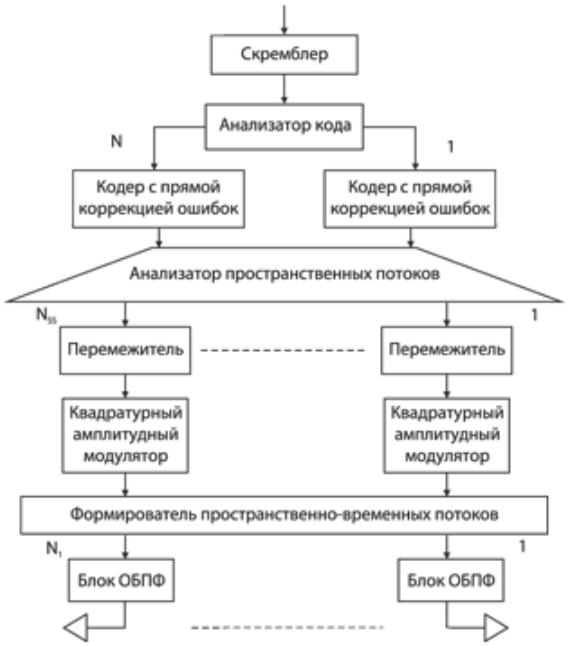


Рисунок 6 – Общая структура передатчика MIMO-OFDM

2.4 Факторы более высокой скорости передачи данных стандарта 802.11n

Стандарт 802.11n применяет три основных механизма для увеличения скорости передачи данных:

− применение нескольких приемопередатчиков и специальных алгоритмов передачи и приема радиосигнала, известный по аббревиатуре MIMO;

− увеличение полосы частот сигнала с 20 до 40 МГц;

− оптимизация протокола уровня доступа к сети.

Первый фактор. С применением MIMO появляется возможность одновременно передавать несколько потоков данных в одном и том же канале, а затем при помощи сложных алгоритмов обработки восстанавливать их на приеме. Проводя аналогию с автодорогами, можно сказать, что ранее существовал только 1 путь, соединяющий точки А и Б. Теперь таких путей несколько и общая пропускная способность системы увеличилась (рисунок 7).

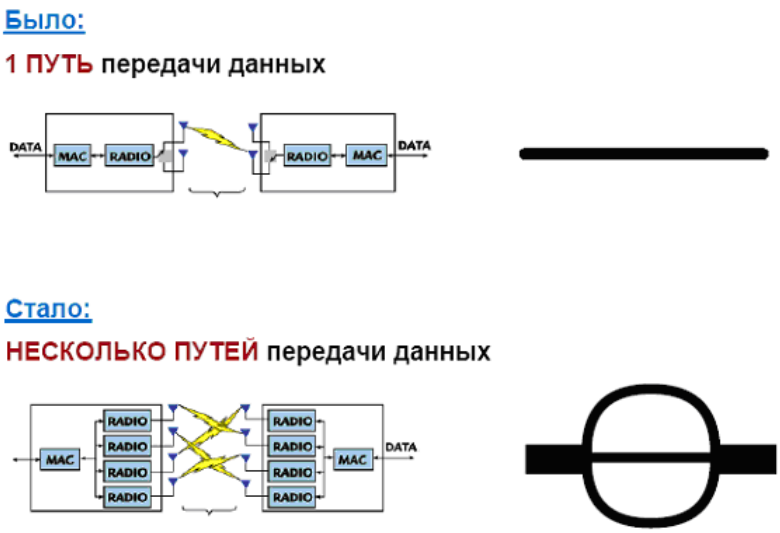


Рисунок 7 – Первый фактор увеличения скорости передачи данных

Второй фактор. Увеличение доступной ширины полосы частот. Теоретически достижимая пропускная способность канала связи напрямую зависит от ширины, занимаемой им полосы частот. В новом стандарте появилась возмож-

ность объединять соседние каналы по 20 МГц и таким образом увеличивать пропускную способность практически в 2 раза. По аналогии с автомагистралями можно считать, что вдвое увеличивается количество доступных для движения полос (рисунок 8).

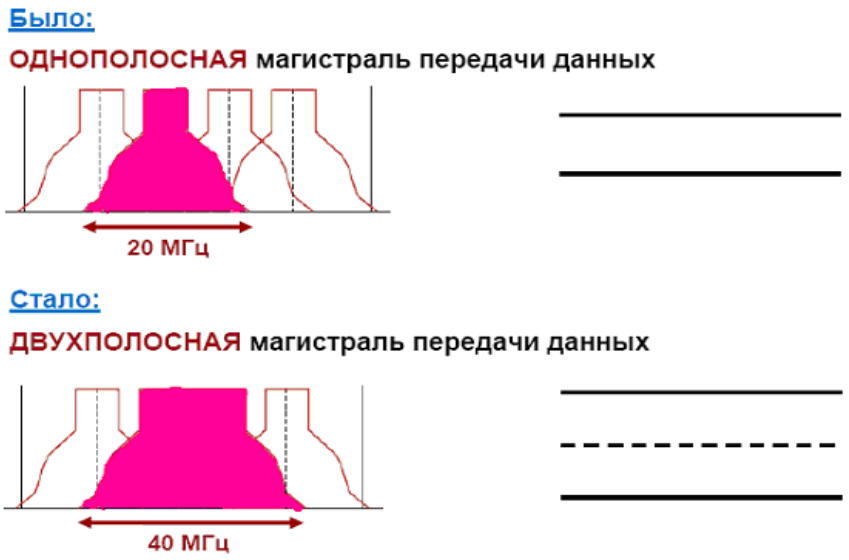


Рисунок 8 – Второй фактор увеличения скорости передачи данных

Первые два фактора относились к физическому каналу. Третий важный фактор увеличения производительности – оптимизация протокола передачи данных на уровне доступа к среде. В предыдущих версиях прием каждого переданного кадра (порции данных) должен был подтверждаться приемной стороной. В новой версии введена возможность блокового подтверждения. Приемник информации передает одно подтверждение сразу на несколько успешно принятых кадров, что уменьшает загрузку общей пропускной способности канала служебными сообщениями. Кроме того, уменьшен временной промежуток между кадрами, что также позволило повысить полезную пропускную способность. Проводя аналогии с повседневной жизнью, можно сравнить кадры с контейнерами для перевозок грузов. Новые правила 802.11 n позволили уменьшить дистанцию между контейнерами и позволили диспетчеру подтверждать не каждый груз в отдельности, а сразу партию грузов (рисунок 9).

Рисунок 9 – Третий фактор увеличения скорости передачи данных

2.5 Топологии беспроводных сетей Wi-Fi

Сети стандарта 802.11 могут строиться по любой из следующих топологий [24]:

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

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

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

− независимые базовые зоны обслуживания (IBSS).

IBSS представляет собой группу работающих в соответствии со стандартом 802.11 станций, связывающихся непосредственно одна с другой. Специальная сеть, или независимая базовая зона обслуживания (IBSS), возникает, когда отдельные устройства-клиенты формируют самоподдерживающуюся сеть без использования отдельной точки доступа (AP – Access Point). При создании таких сетей не разрабатывают какие-либо карты места их развертывания и предварительные планы, поэтому они обычно невелики и имеют ограниченную протяженность, достаточную для передачи совместно используемых данных при возникновении такой необходимости.

Поскольку в IBSS отсутствует точка доступа, распределение времени (timing) осуществляется нецентрализованно. Клиент, начинающий передачу в

IBSS, задает сигнальный (маячковый) интервал (beacon interval) для создания набора моментов времени передачи маячкового сигнала (set of target beacon transmission time, TBTT). Когда завершается TBTT, каждый клиент IBSS выполняет следующее:

– приостанавливает все несработавшие таймеры задержки (backoff timer) из предыдущего TBTT;

– определяет новую случайную задержку.

Базовые зоны обслуживания (BSS). BSS - это группа работающих по стандарту 802.11 станций, связывающихся одна с другой. Технология BSS предполагает наличие особой станции, которая называется точка доступа AP (Access Point). Точка доступа - это центральный пункт связи для всех станций BSS. Клиентские станции не связываются непосредственно одна с другой. Вместо этого они связываются с точкой доступа, а уже она направляет кадры к станции-адресату. Точка доступа может иметь порт восходящего канала (uplink port), через который BSS подключается к проводной сети (например, восходящий канал Ethernet). Поэтому BSS иногда называют инфраструктурой BSS.

Расширенные зоны обслуживания (ESS). Несколько инфраструктур BSS могут быть соединены через их интерфейсы восходящего канала. Там, где действует стандарт 802.11, интерфейс восходящего канала соединяет BBS с распределительной системой (Distribution System, DS). Несколько BBS, соединённых между собой через распределительную систему, образуют расширенную зону обслуживания (ESS). Восходящий канал к распределительной системе не обязательно должен использовать проводное соединение. На рисунке 1.12 представлен пример практического воплощения ESS. Спецификация стандарта 802.11 оставляет возможность реализации этого канала в виде беспроводного. Но чаще восходящие каналы к распределительной системе представляют собой каналы проводной технологии Ethernet.

3 РЕАЛИЗАЦИЯ ПРОЕКТА

3.1 Техническое проектирование

Управление – организация в пределах которой существует активный документооборот. Все необходимые данные и информация, участвующая в рабочем процессе, обрабатывается, анализируется и редактируется сотрудниками в соответствии с их должностными обязанностями. С целью повышения производительности работников предприятия и оптимизации рабочего процесса в Управлении, как и в любой компании, реализована локальная сеть, в которую объединены компьютеры сотрудников для быстрого обмена информацией с серверами и надежного хранения данных на них.

Рабочие станции сотрудников Управления представляют из себя стандартные компьютеры, оснащенные необходимым набором периферии и дополнительного оборудования. Они используются работниками предприятия для анализа, обработки и хранения информации, которая является ценным информационным ресурсом.

При анализе существующей проводной локальной сети предприятия было решено провести проектирование локальной беспроводной сети на основе технологии Wi-Fi. Беспроводные сети Wi-Fi обладают рядом преимуществ, которые устраняют минусы проводной локальной сети:

− легкость создания и расширения;

− мобильность;

− возможность подключения к сети другого типа;

− высокая скорость передачи данных в последних версиях протоколов.

Для организации работоспособной и достаточно быстрой беспроводной сети не потребуется много времени и усилий. А самое главное — минимум затрат. С помощью нескольких точек доступа можно объединить в единую сеть целое здание, включая все этажи. Так же это исключит неудобство в виде множества проводов.

Беспроводная сеть с легкостью позволит сотрудникам подключаться даже с мобильных устройств по типу ноутбука или планшета, работать из любой точки здания, находящейся в зоне покрытия.

При отсутствии адаптера Wi-Fi всегда можно подсоединить через кабель любой компьютер и работать так же в сети. Это очень удобно при выходе из строя сетевого оборудования компьютера, который сможет все так же использоваться для работы до устранения неполадки.

Построив сеть на современном протоколе можно нивелировать один из основных недостатков — низкую скорость передачи. В итоге возможность передавать данные с достаточно высокой скоростью будет сохранена.

Wi-Fi сеть организовывают на базе беспроводных точек доступа, к которым присоединяются клиенты и таким образом получают доступ во внутреннюю сеть. Принцип работы беспроводной точки доступа проиллюстрирован на рисунке 10.

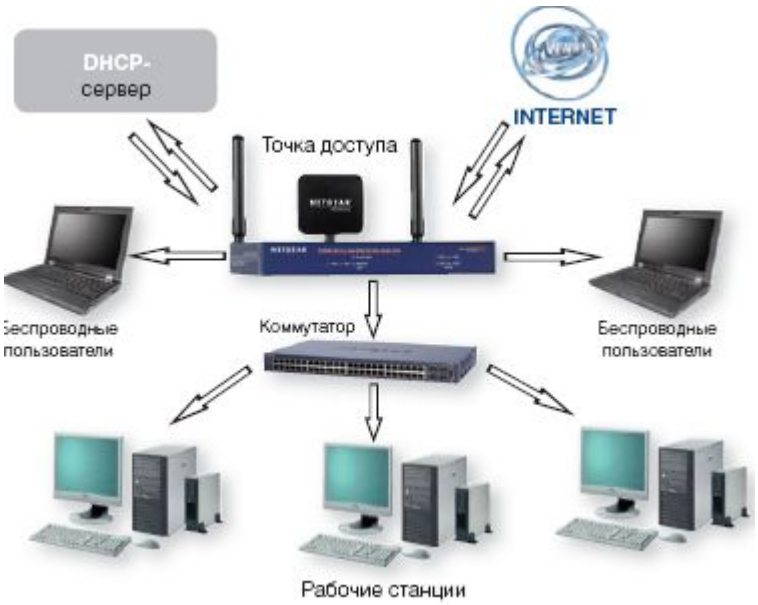


Рисунок 10 – Принцип работы точки доступа

Сперва необходимо продумать будущую локальную беспроводную сеть. Предложить несколько вариантов реализации будущей сети. Проработать каждый отдельно наиболее детально и полно. Поскольку способов реализации

может быть несколько, то необходимо выбрать наиболее подходящий для данного случая. Вариант должен быть оправдан с финансовой и технологической точки зрения, а также отвечать общим требованиям и принципам построения сети Wi-Fi на предприятии для стабильной работы. Кроме того, необходимо учитывать, что сеть строится не с нуля, так как на предприятии уже имеется локальная сеть. Все варианты реализации представлены в таблице 2.

Таблица 2 – Варианты реализации

Критерии	№1	№2	№3
Количество пользователей	=< 10	10 <	10 <
Количество точек доступа	1 на этаж	2-3 на этаж	В соответствии с требованиями
Способ управления точками	Вручную	Централизованно (Через беспроводной контроллер)	Централизованно (Через беспроводной контроллер)
Рабочая частота	2,4 ГГц	5 ГГц	2,4 ГГц и 5 ГГц
Расположение точек доступа	Рядом с клиентским устройством	В зонах прямой видимости	В зонах прямой видимости
Режим шифрования	WEP	WPA+PSK	WPA2+PSK

Общий штат сотрудников насчитывает порядка 70 человек в расчете на то, что у каждого имеется свое рабочее место, которое необходимо включить в созданную сеть. Одной точкой доступа можно обойтись только, если речь идет об одном этаже, небольшом по площади для приемлемого покрытия и качества соединения. Здание организации имеет 4 этажа по несколько кабинетов на каждом. В связи с этим, необходимо создать сеть, которая смогла бы охватывать все здание.

Выбор используемого оборудования очень важен как часть проектирования. Беспроводные точки доступа разнятся по своим

характеристикам. Одна из таких – площадь покрытия. Любые препятствия, например, стены, значительно снижают ее. Но если точка доступа изначально имеет мощный излучатель сигнала, то даже через препятствия сигнал будет достаточно стабильным. Поэтому количество точке доступа остается неопределенной величиной до стадии непосредственного проектирования.

При немалом количестве используемых точек доступа встает вопрос об их настройке и контролировании. Одну или две точки можно настроить вручную. Но большее количество будет отнимать много времени у администратора сети. Поэтому чаще всего используются в подобных случаях беспроводные контроллеры, позволяющие централизованно осуществлять управление точками доступа [5].

Разница в частотном диапазоне также играет важную роль. Каждый диапазон имеет свои недостатки и преимущества. 5 ГГц частота имеет больше каналов связи и они «не страдают» зашумлением как большинство каналов 2,4 ГГц, так как устройств, работающих на этой частоте просто гораздо больше. 2,4 ГГц обладает большей дальностью действия, а оборудование, работающее на этой частоте ощутимо дешевле. Однако рекомендуется закупать оборудование, работающее с двухдиапазонным Wi-Fi на случай, если встанет необходимость подключить устройство, не поддерживающее один из двух диапазонов.

Правильное расположение точке доступа во многом определяет качество соединения в сети, что влияет на стабильность и скорость передачи. Размещать точки доступа лучше вдали от металлических поверхностей, в центре помещения и желательно высоко. Прямая видимость устройства с клиентских компьютеров обеспечит хороший уровень сигнала.

Защита является наиболее уязвимым местом сетей Wi-Fi. Довольно проблематично снизить риск взлома или выхода из строя компонентов сети на данный момент, это часто становится причиной отказа, для создания сети на основе технологии Wi-Fi. Однако, наиболее современный режим шифрования WPA2+PSK (AES) способен обеспечить достаточно надежную защиту [13].

Разобрав все критерии и проанализировав варианты проектирования, было решено выбрать вариант №3, т.к. он соответствует требованиям, наиболее удобен и экономен с точки зрения использования ресурсов.

Важно отметить, что далеко не все компьютеры нужно включать в общую сеть. Хоть в плане по реализации и учтен такой немаловажный аспект, как защищенность, в целях дополнительной безопасности разумно будет исключать компьютеры, на которых производится взаимодействие с персональными данными клиентов. Это положительно скажется на сохранности данных и повысит общую надежность.

Так же отдельные точки доступа можно приспособить лишь как гостевые или только для выхода в сеть интернет с любых устройств, будь то смартфон или ноутбук. В случае необходимости с помощью контроллера возможно изменить спецификацию любой точки доступа в течении некоторого времени.

3.2 Рабочее проектирование

Изначально в здании Управления была создана проводная Ethernet сеть, которая создавала множество неудобств в виде обязательной прокладки проводов к каждому рабочему месту. Кроме того, сотрудники не могли использовать мобильные устройства в рабочем процессе и были строго привязаны к своему рабочему месту. Все это стало причиной для перехода на беспроводную сеть.

Было выявлено, что существующая проводная инфраструктура подходит для развертывания Wi-Fi сети на предприятии. Поэтому было перейти непосредственно к следующему шагу – выбору используемого оборудования.

3.2.1 Точка доступа

D-Link DAP-2695**.** Данное устройство уже продолжительное время на рынке и проверено временем. Отличительной чертой этого роутера является поддержка нового стандарта 802.11ac. Устройство рассчитано на работу в двух частотных диапазонах и характеризуется суммарной пропускной способностью 1750 Мбит/с (450 Мбит/с - в полосе 2,4 ГГц, 1300 Мбит/с - в полосе 5 ГГц).

Точка доступа оснащена шестью съемными антеннами. Помимо основной роли, она может выступать в качестве системы беспроводной дистрибуции контента (WDS), совмещенной с точкой доступа, моста WDS или клиента с поддержкой WDS. Управление устройством осуществляется удаленно с помощью ПО D-Link AP Manager II или модуля SNMP-управления D-View. Используя Wireless AC1750 Simultaneous Dial-Band PoE Access Point, можно связать две сети, например, находящиеся в двух расположенных рядом зданиях. К достоинствам DAP-2695 относится поддержка технологии PoE - точку доступа можно использовать с Ethernet кабелем, который присоединяется через соответствующий порт. Общий вид оборудования представлен на рисунке 11.

Рисунок 11 – D-Link DAP-2695

В таблице 3 приведены общие наиболее значимые характеристики D-Link DAP-2695.

Таблица 3 – Общие характеристики D-Link DAP-2695

Стандарты	− IEEE 802.11a; − IEEE 802.11ac; − IEEE 802.11b; − IEEE 802.11g; − IEEE 802.11n; − IEEE 802.3ab; − IEEE 802.3af; − IEEE 802.3at; − IEEE 802.3u.
Сетевое управление	− HTTP; − Telnet; − SNMP; − MIB.
Алгоритмы	− 64/128-битное WEP-шифрование; − Управление доступом на основе MAC-адреса.
Шифрования данных	− Внутренний сервер RADIUS; − Протокол 802.1x; − Протокол HTTPS; − Протокол SSH; − WPA™-Personal; − WPA2™-Personal; − WPA™-Enterprise; − WPA2™-Enterprise.
Диапазоны частот беспроводных сетей	2,4ГГц, 5ГГц.
Модуляция	− DSSS; − OFDM.
Сертификаты	− FCC; − IC; − CE; − UL; − Wi-Fi.
Прием/Передача	− 6 Антенн x 6 dBi; − Мощность передатчика 26.5 dBM.

3.2.2 Беспроводной коммутатор

Гигабитный коммутатор D-Link DWS-3024 управления беспроводными точками доступа уровня 2+ предназначен для развертывания беспроводной сети для корпорационных офисов. Благодаря этому устройству можно создавать унифицированные масштабируемые, высокопроизводительные, безопасные и управляемые проводные/беспроводные коммутируемые локальные сети.

Располагая портами Gigabit Ethernet, поддержкой технологии Power over Ethernet и возможностью подключения резервных источников питания, коммутаторы обеспечивают предприятиям простой переход к беспроводным сетям стандарта 802.11, быстрое подключение беспроводных устройств вне зависимости от их физического расположения и централизованного управления политиками безопасности.

Гигабитный коммутатор DWS-3024 является корневым устройством, позволяющим управлять безопасностью, полосой пропускания и поддерживать функционирование всей беспроводной сети. Помимо этого, выполняя мониторинг пользователей и управляя их аутентификацией во время роуминга, коммутатор может задавать и управлять всеми параметрами беспроводных точек доступа, включая радиочастотные каналы, управление питанием, сегментацией беспроводного трафика, роумингом, балансировкой нагрузки, обнаружением несанкционированных точек доступа и параметрами безопасности. Разработанный для легкого развертывания сети, коммутатор поддерживает от 24 до 48 беспроводных точек доступа, которые могут быть подключены к его портам непосредственно или опосредованно через коммутатор локальной сети. Каждый порт коммутатора снабжен поддержкой технологии 802.3af PoE, что позволяет осуществлять подключение точек доступа, находящихся в местах, где розетки питания недоступны. Гигабитные порты являются оправданным вложением средств, с целью последующего перехода к беспроводной сети стандарта 802.11ac.

Коммутатор оборудован 24 портами 10/100/1000BASE-T и 4 комбо-портами SFP. К каждому порту 10/100/1000BASE-T можно подключить беспроводную точку доступа или проводное сетевое устройство, например, сервер, сетевое устройство хранения информации или другой коммутатор. Комбо-порты SFP обеспечивают гибкое подключение по оптике.

Общий вид оборудования представлен на рисунке 12.

Рисунок 12 – D-Link DWS-3024

В сетях малого и среднего бизнеса для управления несколькими точками доступа или для использования в смешанной проводной/беспроводной локальной сети потребуется только один коммутатор, поддерживающий управление беспроводными точками доступа. При увеличении количества точек доступа в систему централизованного управления можно объединить до 4 коммутаторов. Благодаря простоте расширения, поддержке гигабитных скоростей для подключения высокоскоростных точек доступа и маршрутизации уровня 3 для организации межсетевого роуминга, DWS-3024 обеспечивает архитектуру, которая унифицирует и упрощает сложную конфигурацию беспроводной сети, подготавливая простой переход к будущим технологиям.

Для облегчения труда персонала коммутатор обеспечивает выбор свободных или наименее используемых радиочастотных каналов для каждой беспроводной точки доступа, чтобы избежать интерференции с другими точками доступа или радиочастотными устройствами. Для каждой точки доступа коммутатор устанавливает выходную мощность передатчика, которая обеспечит устойчивый прием радиосигналов беспроводными клиентами и в то же время сведет к минимуму интерференцию с радиочастотными сигналами других устройств. При каждом добавлении новой точки доступа или удалении ее из сети коммутатор автоматически настраивает радиочастотные каналы и выходную мощность передатчика всех беспроводных точек доступа. Можно задать время или

временной интервал выполнения автоматической настройки, что позволяет минимизировать необходимость выполнения настроек вручную. В таблице 4 приведены общие характеристики D-Link DWS-3024.

Таблица 4 – Общие характеристики D-Link 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 Mbps; − 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.
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).

Коммутатор обладает двумя функциями для повышения отказоустойчивости беспроводной сети, а именно - так называемый процесс "самовосстановления" и функция балансировки нагрузки между точками доступа. Чтобы восполнить недостаточную зону покрытия в результате выхода из строя точки доступа (например, из-за сбоя питания), коммутатор автоматически увеличивает выходную мощность передатчика соседних точек доступа, чтобы увеличить их зону покрытия. Для обеспечения непрерывного подключения существующих клиентов, коммутатор выполняет балансировку нагрузки между точками доступа, когда сетевой трафик достигает определенного порогового значения. В

то же время коммутатор отклоняет подключение новых клиентов к точке доступа для того, чтобы избежать перегрузки полосы пропускания.

3.2.3 Организация сети

Созданная локальная Wi-Fi сеть соединяет четырехэтажное здание и на каждом этаже будут располагаться по два беспроводных коммутатора D-Link DWS-3024, которые в свою очередь соединены витой парой с остальными коммутаторами на этажах выше и ниже. Коммутаторы будут управлять расположенными в коридорах точками доступа D-Link DAP-2695, по 4 на этаж. Это обеспечит стабильное соединение без затухания сигнала и позволит создать обширную зону покрытия. Этот вариант реализации также обеспечит пользователям беспрерывный доступ к внутренней сети с высокой скоростью передачи данных.

RADIUS-сервер, генерирующий динамические ключи доступа для пользователей сети, будет располагаться в отдельном помещении отдела эксплуатации информационных систем, технических средств и каналов связи. Его обслуживанием и обслуживанием всей сети будут заниматься сотрудники отдела.

Для организации беспроводной сети необходимо приобрести требуемое оборудование и установить его в соответствии с приведенной схемой. Настроить беспроводные коммутаторы и точки доступа, настроить контроль трафика, а также мониторинг сети. Обеспечить защиту реализованной Wi-Fi сети с целью безопасности информации.

Пример реализации беспроводной сети одного из этажей организации представлен на рисунке 13.

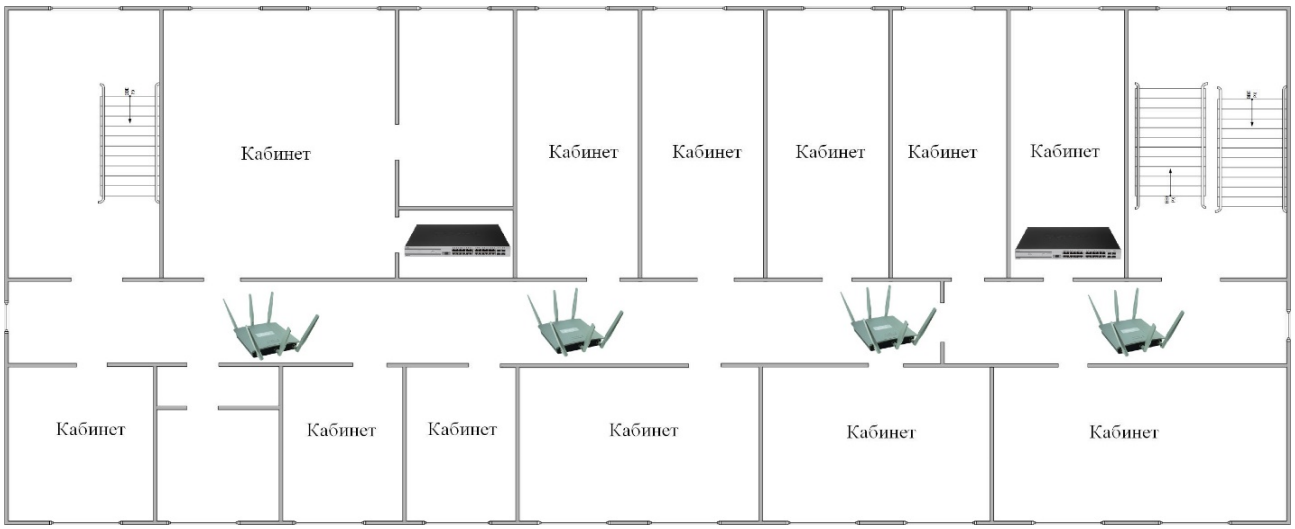


Рисунок 13 – Размещение точек доступа и коммутаторов на этаже

3.3 Разработка программного продукта

Характерной чертой для любой локальной вычислительной системы является наличие движения больших объемов информации между её узлами. Поскольку данное движение необходимо регулировать, находить наиболее узкие и загруженные места в сети, в последнее время большую роль стало играть создание прикладных программ для мониторинга и диагностики сети.

Объект разработки, являющийся программой-анализатором, нацелен прежде всего на сотрудников, которые имеют базовые знания в сфере сетевых технологий и должную квалификацию для работы с программными продуктами такого типа. Обычным пользователям будет невозможно использовать программу по прямому назначению в связи с непониманием принципа работы и назначением.

Предполагается, что разрабатываемое ПО будет развертываться на стационарных рабочих станциях и ноутбуках предприятия, которые включены в локальную Wi-Fi сеть. Был проанализирован рынок программных продуктов. Исходя из вышеизложенного, к программе предъявляются следующие требования:
− интуитивный и понятный интерфейс с поддержкой русского языка;

− невысокая требовательность к производительности системы и ее компонентам;

− информативность предоставляемых сведений для работы с ними;

− оптимизированный код;

− небольшой размер;

− совместимость с последними версиями ОС семейства Windows;

− отсутствие критических ошибок при работе;

− возможность формировать отчеты в удобном для разработчика виде;

3.3.1 Анализ теоретической части

Разработанное в проекте программное обеспечение осуществляет контроль сетевого трафика на наиболее важных узлах сети и предоставляет информацию о получении отправки и посылке пакетов сообщений между узлами сети по протоколу IP и UDP.

Поскольку сеть Wi-Fi подразумевает наличие портативных и мобильных устройств, подключающихся к ней, то определенным недостатком будет невозможность анализа с планшетов и смартфонов по причине того, что программа является ПК-совместимой. Данный недостаток частично нивелируется тем фактом, что на предприятиях сеть состоит в основном из стационарных рабочих станций, т.е. рабочих ПК. Что означает довольно низкий порог вхождения для использования программы.

Из-за использованных методов и принципов при написании кода, для запуска и работы программного продукта потребуется ОС Windows 7 x32 или новее. На более ранних версиях стабильная работа гарантироваться не может. Так как любое предприятие нуждается в самом современном ПО, то данный недостаток играет весьма незначительную роль. При выводе на рынок следующей версии ОС продукт будет обновлен до новой версии, тем самым расширяя совместимость.

Разрабатываемое ПО требует оператора – человека, компетентного и квалифицированного в определенной области, для продуктивной работы. В отсут-

ствии подготовки и должных знаний могут возникнуть трудности в обращении с продуктом.

Программа используется локально на одной рабочей станции, поэтому потребуется перенос копии для работы на другом устройстве. Эти действия не повлекут значимых неудобств в силу того, что программа имеет небольшой размер и может быть передана на другую рабочую станцию посредством общей сети.

Отличительным достоинством продукта от аналогов на рынке можно выделить «легкость» и относительную простоту в использовании. Программа не сложна в освоении и может запускаться даже на непроизводительных рабочих станциях, что позволяет ее использовать почти на любом компьютере. Кроме того, она быстро функционирует и взаимодействует с пользователем через понятный интуитивный интерфейс, что делает ее очень удобной в использовании.

Учитывая всю собранную информацию и предъявляемые требования можно сделать вывод, что разрабатываемый продукт подойдет к любой организации, использующей сеть на основе технологии Wi-Fi и будет актуален ближайшее время. Учитывая тенденции перехода все большего количества компаний на беспроводные сети, можно рассчитывать на более длительный жизненный цикл программы.

Для реализации всех сформированных требований требуется выбрать наиболее подходящий инструментарий и определить, как именно программа будет взаимодействовать с оборудованием сети и потоками данных.

Средой разработки для написания продукта была выбрана Microsoft Visual Studio 2017, так как она имеет весомые преимущества и предлагает современные средства разработки. Одна из ее редакций полностью бесплатна и может быть использована свободно. Поддержка большинства языков программирования гарантирует возможность работы программистам, специализирующимся на определенном языке. Удобный и интуитивно понятный интерфейс позволяет освоиться даже новичку, оперируя средствами разработки.

Выбор C# как языка программирования обоснован несколькими причинами:

− язык обеспечивает объектную ориентированность разрабатываемого ПО;

− C# популярен в кругах программистов и для него существует множество инструкций и руководств, что облегчает создание конечного продукта;

− наличие большого количества библиотек и шаблонов, упрощающих работу и уменьшающих затраты времени;

− язык активно развивается. Повышается быстродействие и надежность;

− интегрированная среда разработки, предоставляющая множество хороших инструментов разработки;

− строгая типизация, защищающая от критических ошибок в коде.

Основной упор сделан на функционале программы. Среда разработки Microsoft Visual Studio 2017 является крайне эффективным инструментом при работе с подобным ориентиром. Используемые библиотеки и LINQ запросы делают возможным реализацию запланированных функций программы и, что более важно, позволяют внедрять их независимо друг от друга и в произвольном порядке. Кроме того, в Visual Studio разработчики могут параллельно работать с интерфейсом будущего решения, изменяя и модернизируя его в любое время. Создаваемый интерфейс в данной среде разработки отличается интуитивностью и дружественен к конечному пользователю. А язык программирования C# отличается безопасностью, что является весомым преимуществом. Он относительно прост в освоении и позволяет разрабатывать приложение частями, создавая удобство в написании кода.

Готовое проектное решение взаимодействует с потоками трафика беспроводной сети организации. Данные в беспроводных Wi-Fi сетях проходят небольшими частями, которые принято называть пакетами. Также имеют место названия «кадры» и «блоки». Максимальная длина таких пакетов всегда строго фиксирована и не может превышать допустимое значение. Передача пакетами играет важную роль в организации движения трафика внутри сети.

Создаваемая беспроводная сеть прежде всего обязана предоставлять качественную и свободную связь всем клиентским устройствам. Одним из основных значений выступает время доступа к сети. Оно отражает определенный интервал времени до момента старта передачи. Клиент подтверждает свою готовность, после чего происходит передача информации по каналу. Не допускается, чтобы процесс занимал слишком много времени. Это может повлечь за собой снижение реальной скорости передачи данных даже при высокой скорости связи [11].

Передача информации внутри сети в основе своей является чередованием передаваемых пакетов, содержащих в себе эту информацию, которая передается от одного пользователя к другому. Программа задействует информационные потоки данных и производит сканирование с последующим анализом передаваемых пакетов. Схема действия программы представлена на рисунке 14.

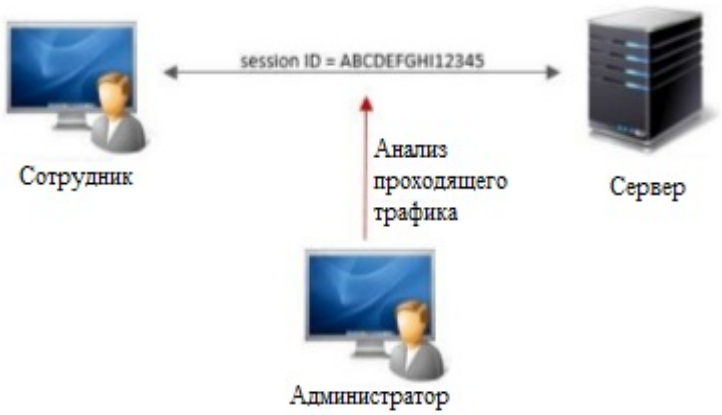


Рисунок 14 – Схема действия программы

Каждый тип пакетов строго определяется используемым стандартом передачи информации. Этот стандарт также задает параметры в виде размера, строение и другие дополнительные особенности. Характеристики пакета опираются и на особенности аппаратного обеспечения беспроводной сети, ее топологию и тип информационной среды. Строго говоря, все определяет используемый протокол передачи данных.

Структура пакета обычно определяется общими принципами построения

пакетов. Данные принципы берут во внимание особенности передачи информации в рассматриваемых типах сетей. Общепринято, что пакет имеет несколько основных полей вне зависимости от типа [2]. На рисунке 15 отображено строение пакета.

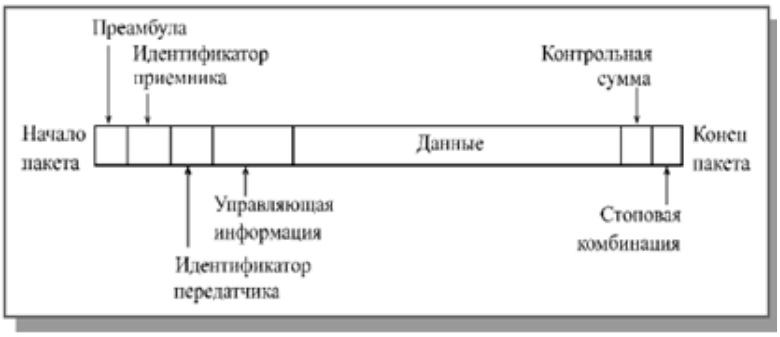


Рисунок 15 – Основные поля пакета

− преамбула, начальная комбинация битов, которая производит первичную настройку сетевого оборудования, подготавливая его к приему и обработке пакета. Тем не менее, преамбула не обязательна и может просто отсутствовать в пакете. В некоторых случаях она прописывается одним единственным стартовым битом информации;

− идентификатор приемника несет в себе сетевой адрес приемника. Это уникальная комбинация цифр (номер), присваиваемая всем принимающим абонентам внутри данной сети, отдельная для каждого. Приемник анализирует комбинацию цифр и на основе произведенного анализа определяет кому адресован передаваемый пакет;

− идентификатор передатчика отражает сетевой адрес абонента, передающего пакеты данных. Так же, как и с приемником, он представляет собой уникальный номер, присваиваемый всем передающим абонентам внутри данной сети, отдельный для каждого. Эта комбинация цифр позволяет принимающей стороне распознать откуда передан пакет. Особенно важно данное поле в случае попеременной передачи приемником множества пакетов от разных передатчиков;

− управляющая или служебная информация, содержит в себе характеристики

пакета. К какому типу он принадлежит, его размер в битах, формат и т.д.;

− поле данных содержит в себе конкретно ту основную информацию, которую передают пакетами. Ее требуется доставить другому абоненту сети. Длина поля данных непостоянна, но именно она определяет основную длину всего пакета. Данное поле может отсутствовать. В таком случае пакет называется управляющим, в отличие от информационного, содержащего поле с информацией. Управляющие пакеты начинают и завершают сеансы связи, являясь сетевыми командами. Также служат для запросов и подтверждений передачи;

− контрольная сумма является некой числовой комбинацией, которая создается передатчиком с учетом правил формирования. Она содержит информацию о всем пакете, но в сжатом виде. Принимающая сторона производит повторные операции расчета контрольной суммы и затем сравнивает ее с контрольной суммой отправленного пакета. При выявлении различий приемник отправляет запрос на повторную передачу;

− стоповая комбинация информирует оборудование принимающей стороны о конце пакета. Производит остановку режима приема у принимающего абонента. Поле может не присутствовать в пакете в случае использования самосинхронизирующегося кода. Он имеет возможность автоматически определять момент окончания передачи.

Данные поля передаются в пакете вместе с основной информацией и позволяет идентифицировать пакет.

3.3.2 Проектирование программного продукта

Реализация сформированных требований может быть произведена по нескольким вариантам, поэтому одной из главных задач данного этапа является выбор наиболее подходящего из предложенных. Первым шагом важно определить структуру программы. Затем предложить варианты реализации требований к продукту, а после проанализировать каждый и сделать выбор в пользу лучшего.

Существующая свобода выбора языка программирования для написания программного кода позволяет рассматривать именно те варианты, проектирование на основе которых будет знакомо и понятно разработчику. Сроки выполнения строго ограничены, поэтому требуется выбрать не только наиболее близкий разработчику вариант, но и наименее затратный по времени. Программа должна работать в реальном времени, поэтому должна присутствовать быстрая обработка входящих данных и вывод необходимой информации пользователю. Требования к программному интерфейсу автоматически сужают круг выбора языков, так как необходима поддержка работы с windows-формами. Подходящими языками выступают C++, Java и C#. Достоинства языка Java отлично проявляются при программировании под мобильные платформы, но, поскольку, программный продукт ориентирован на десктопные компьютеры и ноутбуки, работающие под управлением ОС Windows, то надобность в кроссплатформенности отпадает. Стоит обратить внимание на оставшиеся варианты – C++ и C#, так как в других аспектах они предпочтительнее. C# позволяет стартовать разработку быстрее, что выливается в более быстрое создание рабочего прототипа решения за счет использования шаблонов и готовых конструкторов. Оба языка обладают кроссплатформенностью, но, как отмечалось раннее, данный фактор не учитывается. C# предлагает простоту разработки, красоту кода и объективную производительность в сравнении с C++ [21]. Большое количество библиотек .net идет в базе, а вместе с ними множество свободно доступных библиотек, которые необходимы для первостепенных задач разработки под Windows. Кроме того, он предлагает более удобный отладчик, что упрощает процесс разработчика.

Программа должна использовать запросы для получения важных данных о типе соединения, протокола, операции. Выбор языка запросов упирается в компактность и оптимизацию кода. По этой причине лучшим вариантом будет LINQ.

При разработке интерфейса программы стоит вопрос о более подходящей реализации. Создавать одну форму для вывода необходимой информации нецелесообразно. Окно программы будет громоздким и слишком большим, закрывая рабочую часть экрана пользователя. Целесообразно разделить модули программы на отдельные формы, которые открываются по нажатию определенной кнопки главной формы, что упростит ориентацию пользователя и позволит открывать только нужные формы.

В ввиду своей распространенности и популярности программа разрабатывается под операционные системы семейства Windows.

Программа работает локально, используя собственную базу данных для записи, и требует подключения к локальной сети для анализа потока данных.

Разработка базы данных ведется с помощью СУБД Visual Studio. В связи с этим, устанавливать дополнительные приложения СУБД не требуется, как и не требуется подключение сторонней базы данных. Это существенно экономит время и сокращает трудовые затраты.

Выбор ограничений доступа на запуск исполняемого файла программы очень важен для обеспечения безопасности информации. Поскольку данные о передаваемых пакетах в большинстве случаев представляют конфиденциальную информацию, то следует ограничить допуск обычных сотрудников к использованию программного продукта. Это позволит снизить риск хищения и/или разглашения информации, непредназначенной для распространения вне территории предприятия. Права на использование программы и информации, получаемой с ее помощью, только доверенному лицу – системному администратору.

Разобрав все критерии и проанализировав варианты проектирования, было решено выбрать вариант №2, т.к. он соответствует требованиям, наиболее удобен и экономен с точки зрения использования ресурсов.

Основной целью создаваемого продукта является мониторинг полосы пропускания и анализ сетевого трафика. Из этого следует, что сперва требуется

определить включена ли используемая рабочая станция в общую локальную беспроводную сеть.

Для правильного взаимодействия с программой пользователь должен быть знаком с устройством сети предприятия, иметь представления о принципе ее функционирования, разбираться в понятиях программы для понимания поступающей информации и иметь доступ к рабочим станциям организации. Разрабатываемая программа может взаимодействовать в совокупности с системными средствами ОС Windows для повышения производительности работы сотрудника, отвечающего за поддержание сети предприятия.

Варианты реализации требований к разрабатываемому программному продукту представлены в таблице 5.

Критерии	№1	№2	№3
Язык программирования	Java	C#	C++
Язык запросов	SQL	LINQ, SQL	LINQ
Количество используемых форм	1	Отдельная форма для каждого модуля	3
Операционная система	Windows 7 x32 и новее	Windows 7 x32 и новее	Windows 7 x32 и новее
Подключение к сети	Да	Да	Да
Использование сетевых приложений	SQL Server	Не используется	SQL Server
Разграничение доступа	Отсутствует	Системный администратор, сотрудник, гость	Только системный администратор

Таблица 5 – Варианты реализации требований

Вывод данных и взаимодействие с программой происходят в нескольких формах, которые включают в себя следующие компоненты:

− подмодуль разграничения прав на основе типа учетной записи для входа;

− подмодуль хранения списка пользователей и их данных, включая данные учетной записи (логин и пароль);

− подмодуль, определяющий активные адаптеры рабочей станции для соединения с сетью предприятия;

− подмодуль для анализа полосы пропуска для выбранного адаптера связи с выводом информации (стандарт, скорость загрузки в реальном времени, операция ip-адрес, количество полученных байт, период времени доступности);

− подмодуль сбора данных из монитора полосы пропуска и занесения данных в хранилище;

− подмодуль для захвата передаваемых пакетов и просмотра подробной информации о них с формированием отчета.

Работник, специализирующийся на поддержании работоспособности сети, будет назначен оператором программы для взаимодействия с ней и выводимыми ею данными. Поскольку это требует квалифицированного специалиста, то программа предназначается для системного администратора, который запускает программу на рабочих станциях для выявления разрывов и ошибок сети, подозрительного трафика и анализа проходящих данных.

Суммируя и подводя итог всего вышеизложенного контекстную модель программы возможно представить с помощью диаграммы IDEF0 (рисунок 16).

Рисунок 16 – Контекстная модель программы

Входными данными являются логин и пароль, информация о выбранном адаптере беспроводной сети, через который будут приниматься пакеты и на основании чего происходит формирование данных на выходе. Так же входными данными является выбор передаваемого пакета, характеристики которого можно просмотреть.

Управляющая информация это данные об адаптере (информация о нем в системе), данные о пользователях и LINQ запросы, позволяющие осуществлять мониторинг полосы пропускания. Механизмы, осуществляющие операции – системный администратор (оператор программы), программное обеспечение (позволяет сверять подлинность данных, выводимых программой), средства ОС (с их помощью осуществляется доступ к необходимым данным об адаптере и передаваемой информации). Выходной информацией являются данные о пакетах в виде отчета.

Проведя декомпозицию диаграммы IDEF0, получим декомпозированную диаграмму в соответствии с имеющимися подмодулями программы.

Несмотря на этот факт, в программе реализовано разграничение прав для трех типов учетных записей: Administrator (системный администратор организации), Employee (сторонний сотрудник компании), Guest (гость). Для определения прав необходимо войти под своей учетной записью через ввод логина и пароля. Учетная запись администратора обладает полными правами и позволяет использовать весь реализованный функционал программы. Права сотрудника и гостя ограничены. Сотрудник не может просмотреть данный пользователей в базе данных, использовать анализатор трафика и сохранять данные о пакетах для отчета. Гость максимально ограничен в правах и поэтому сверх указанного ранее лишен права просматривать историю и выполнять операцию ее удаления, оставляя за собой права лишь на использование монитора полосы пропуска.

Функциональная декомпозиция программы представлена на рисунке 17.

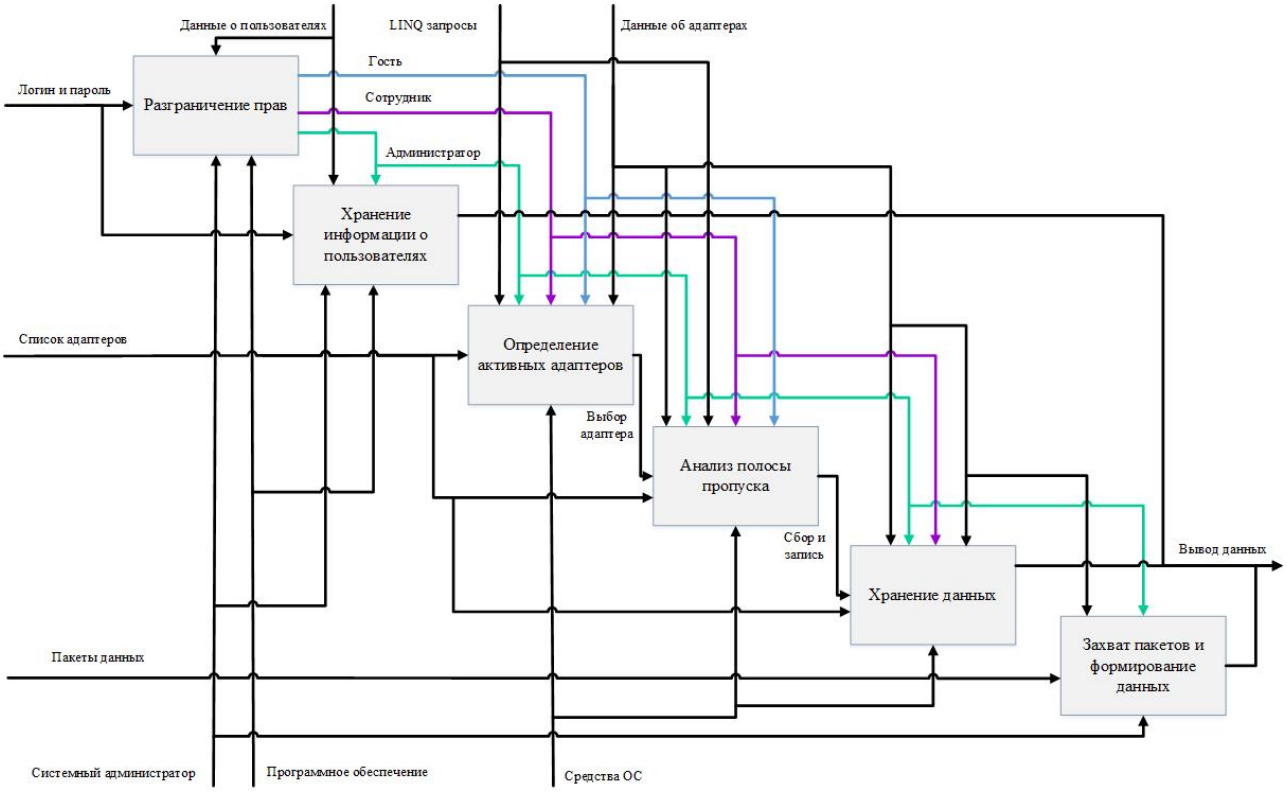


Рисунок 17 – Функциональная декомпозиция программы

Схему разграничения прав можно представить в виде UML-диаграммы сценария выполнения, на которой изображены роли пользователей программы и их возможности. (рисунок 18).

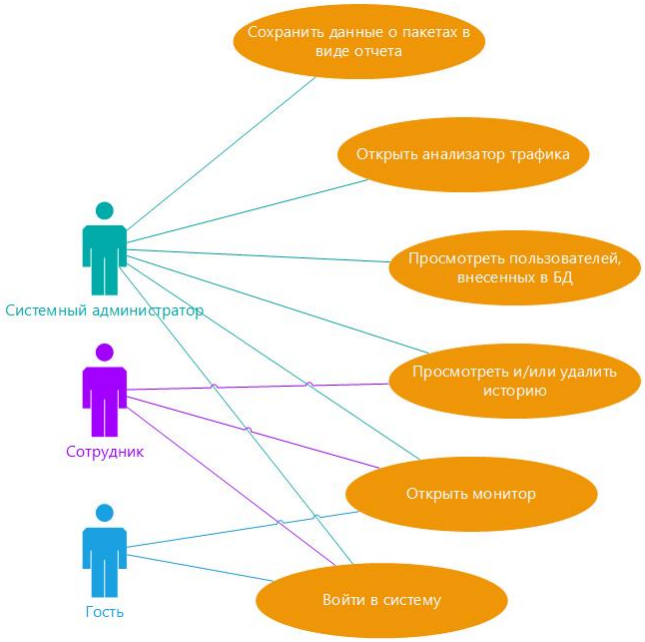


Рисунок 18 – UML-диаграмма сценария выполнения

В процессе разработки программа менялась, совершенствовалась и дополнялась. Финальный этап разработки включает работу над интерфейсом приложения. При проектировании интерфейса сначала обращают внимание на расположение управляющих элементов, затем переходят к дизайну. Прототип интерфейса программы во многом схож с финальной версией, но имеет множество различий в количестве элементов, дизайне и расположении функциональных компонентов. На рисунке 19 представлен прототип пользовательского интерфейса программы.

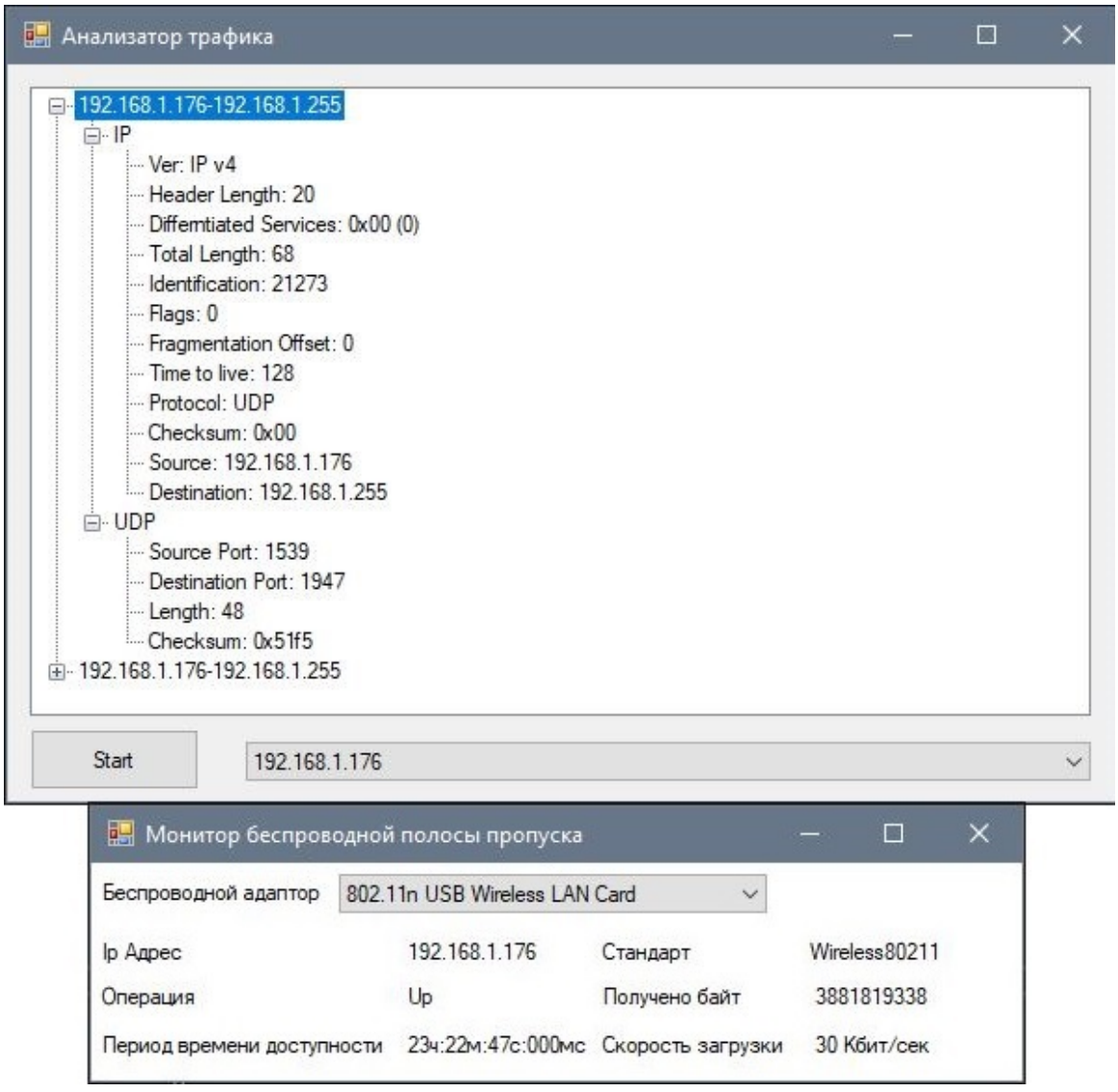


Рисунок 19 – Прототип пользовательского интерфейса

3.3.3 Разработка программного продукта

Программа работает с таблицами (сущностями), которые созданы с целью сбора, хранения и изменения данных:

− *сущность* «login» хранит данные о пользователях, имеющих учетные записи для входа в программу. Здесь сохраняются логин и пароль для входа, роль (тип учетной записи), имя и номер телефона для связи с определенным сотрудником в экстренных ситуациях (таблица 6).

Таблица 6 – Спецификация атрибутов сущности «login»

Название атрибута	Описание атрибута	Тип данных	Диапазон значений	Пример атрибута
username	Ключевой атрибут, однозначно определяющий пользователя	Текстовый	50 символов	User1
password	Пароль пользователя	Текстовый	50 символов	Pass1
role	Роль (тип учетной записи пользователя)	Текстовый	50 символов	Administrator
name	ФИО пользователя	Текстовый	50 символов	Romanov P.A.
Phone number	Номер телефона пользователя	Числовой	>= 0	555666

− *сущность* «monitor» хранит данные, которые пользователи сохраняют в хранилище из монитора полосы пропуска. В этой таблице содержатся наименование адаптера, ip-адрес, период времени доступности, стандарт, количество полученных байт, дата и время (таблица 7).

Название атрибута	Описание атрибута	Тип данных	Диапазон значений	Пример атрибута
Дата и время	Ключевой атрибут, однозначно определяющий строку истории	Дата Время	Присваивается значением	04.07.2019 13:26
Ip-адрес	Уникальный сетевой адрес узла	Текстовый	50 символов	169.254.18.235
Период времени доступности	Период времени, в течение которого адрес может оставаться доступным	Текстовый	50 символов	06h:28m:15s
Стандарт	Стандарт связи для коммуникации	Текстовый	50 символов	Wireless80211
Получено байт	Количество полученных байт	Числовой	>= 0	752886603

Таблица 7 – Спецификация атрибутов сущности «monitor»

Используемые таблицы данных выступают в качестве хранилища данных. Связи между сущностями отсутствуют, таблицы могут изменяться независимо друг от друга. В качестве первичного ключа выбраны поля, которые не повторяются являются уникальными. В таблице «login» первичный ключ заносится вручную системным администратором, а дата и время таблицы «monitor» могут быть одинаковыми в таблице, но в программе идет учет не только на секунды, но и на миллисекунды, что делает поле даты и времени для каждой записи уникальным.

При запуске программы пользователя встречает форма входа, в которую нужно ввести данные учетной записи (логин и пароль) для авторизации с правами, соответствующими учетной записи. Для этого в обработчик кнопки встроен SQL запрос:

```
SqlDataAdapter sda = new SqlDataAdapter("select role from login where username = '" + text-
Box1.Text + "' and password = '" + textBox2.Text + "'", conn);
            DataTable dt = new DataTable();
                  sda.Fill(dt);
```

По нажатию кнопки «Пользователи» главной формы открывается форма «Пользователи». На ней расположена кнопка «Отобразить данные», используемая для вывода таблицы «login» в элемент dataGridView1. Данная операция реализуется тоже с помощью SQL запроса:

```
SqlDataAdapter sda = new SqlDataAdapter("select * from login", conn);
            SqlCommandBuilder cb = new SqlCommandBuilder(sda);

            DataSet ds = new DataSet();
                  sda.Fill(ds, "login");
```

При открытии формы «Монитор беспроводной полосы пропуска» автоматически выполняется LINQ запрос для определения беспроводных адаптеров в сети и формирование списка для элемента cmbAdaptors, который является ComboBox`ом:

```
IEnumerable<NetworkInterface> nics = NetworkInter-
face.GetAllNetworkInterfaces().Where(network => network.OperationalStatus == Operational-
Status.Up
                  && (network.NetworkInterfaceType == NetworkInterfaceType.Ethernet || net-
work.NetworkInterfaceType == NetworkInterfaceType.Wireless80211));
```

Данные сущности «monitor» вносятся не вручную, для этих целей используются SQL запросы. Нажимая кнопку «Сохранить» на форме «Монитор беспроводной полосы пропуска» происходит захват данных в соответствии с запросом в коде:

```
string sqlFormattedDate = myDateTime.ToString("yyyy-MM-dd HH:mm:ss.fff");
            SqlDataAdapter sda1 = new SqlDataAdapter (" insert into monitor (Адаптер,[ip-
адрес],[Период времени доступности],Стандарт,[Получено байт],[Дата и время]) " +
                  "VALUES ('" + cmbAdptors.Text + "' , '" + lblIP.Text + "' , '" + lblVal-
lifetime.Text + "' , '" + lblType.Text + "' , '" + lblReceived.Text + "', '" + myDateTime +
"') ", CON);
```

Данные из элементов label берутся в виде текста и вносятся в соответствующие колонки таблицы «monitor».

Главная форма содержит кнопку «История». Нажав ее, пользователь попадет на форму «История», содержащую активную кнопку «Отобразить данные». Данная кнопка отображает данные таблицы «monitor» через использование SQL запроса в элемент HistoryTable:

```
SqlDataAdapter sda1 = new SqlDataAdapter("select * from monitor", conn);
            SqlCommandBuilder cb1 = new SqlCommandBuilder(sda1);

            DataSet ds1 = new DataSet();
            sda1.Fill(ds1, "monitor");

           HistoryTable.DataSource = ds1.Tables[0];
```

А кнопка «Очистить данные базы» позволяет безвозвратно стереть уже занесенные раннее данные в таблицу, сразу обновляя элемент HistoryTable на форме:

```
SqlCommand cmd = new SqlCommand("DELETE FROM monitor;", conn);
            SqlDataAdapter MyDA = new SqlDataAdapter();
            BindingSource bSource = new BindingSource();
            DataTable monitor = new DataTable();
            bSource.DataSource = monitor;
            MyDA.SelectCommand = cmd;
            MyDA.Fill(monitor);
                  HistoryTable.DataSource = bSource;
```

3.3.4 Руководство пользователя

Программа начинает свою работу сразу после запуска исполняемого exe файла «FORMI.exe». Открывается форма авторизации, на которой необходимо ввести данные пользователя, внесенного в БД, для входа (логин и пароль) на основную форму. Форма входа представлена на рисунке 20.

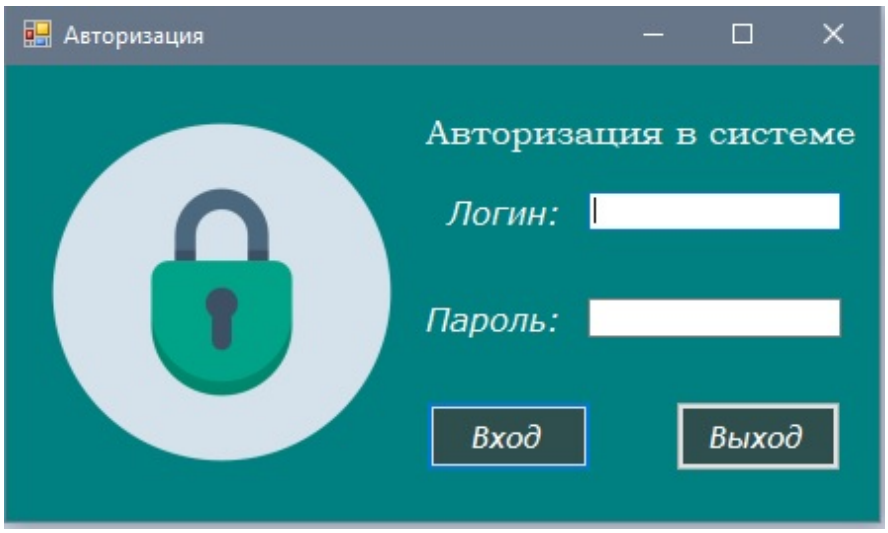


Рисунок 20 – Форма входа

Введя данные учетной записи, пользователь попадает на главную форму программы. В левом нижнем углу отображается тип учетной записи (Administrator, Employee, Guest) в зависимости от которого меняется доступ к функционалу программы. Ниже расположена кнопка «Сменить пользователя», позволяющая вернуться на предыдущую форму и ввести другие данные в случае беспрерывной работы программы с двумя сотрудниками, имеющими различные типы учетных записей. Главная форма изображена на рисунке 21.

Кнопка «Выход» завершает работу и закрывает окно программы. Остальные кнопки вызывают соответствующие формы.

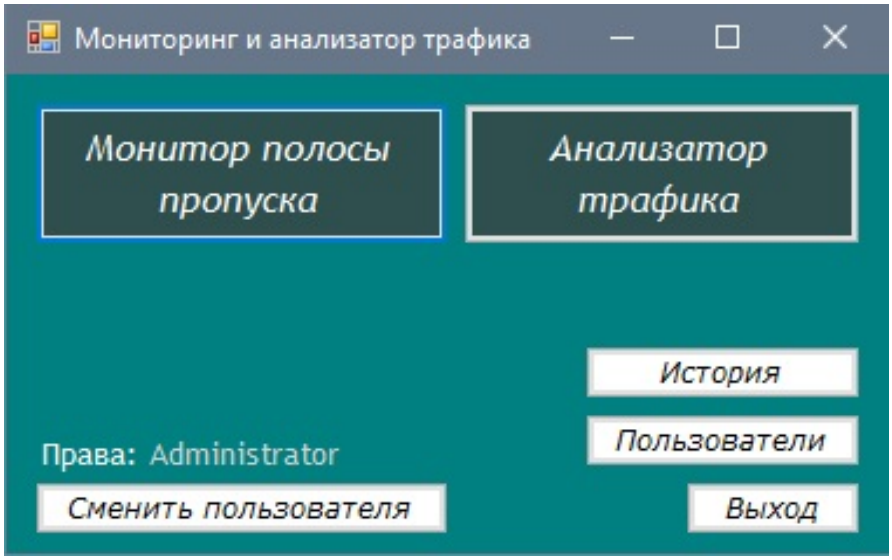


Рисунок 21 – Главная форма

По нажатию кнопки «Монитор полосы пропуска» выполняется переход на одноименную форму. Здесь пользователю предлагается выбрать беспроводной адаптер из списка для отображения данных. Кнопка «Сохранить» заносит текущие данные в БД и информирует об успешном выполнении операции. Кнопка «Закрыть» закрывает форму и завершает работу монитора. Форма «Монитор беспроводной полосы пропуска» изображена на рисунке 22.

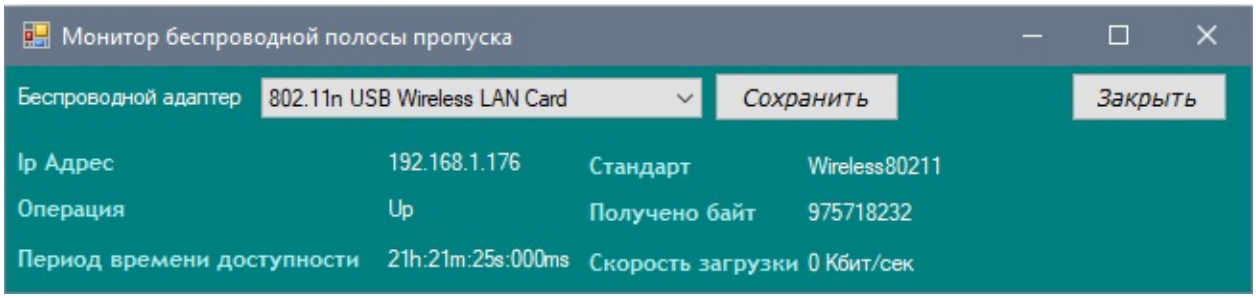


Рисунок 22 – Форма монитора беспроводной полосы пропуска

Нажатие кнопки «Анализатор трафика» перенаправляет на соответствующую форму. Важно отметить, что ввиду разграничения прав данная кнопка будет доступна только в том случае, если учетная запись имеет тип Administrator (рисунок 23).

Нажатие кнопки «Стоп» процесс останавливается. «Сохранить» позволяет создать текстовый файл в директории программы, называющийся «Отчет.txt». В него заносятся все данные из дерева на момент нажатия. Поле очищается. Файл отчета нечитаем средствами ОС и возможность его просмотра предоставляется только по нажатию кнопки «Загрузить». По нажатию этой кнопки дерево сначала очищается, а после заполняется данными из текстового файла. При повторном сохранении файл перезапишется с новыми данными. Кнопка «Очистить» просто очищает поле дерева для заполнения новыми данными. «Закрыть» закрывает текущую форму.

Кнопка «История» на главной форме осуществляет переход на одноименную форму программы. Здесь расположены три кнопки. «Отобразить данные» выводит данные из БД в поле DataGridView. По нажатию кнопки «Очи-

стить данные базы» происходит удаление записей таблицы из БД и автоматическое обновление DataGridView на форме. «Закрыть» закрывает текущую форму. Форма «История» изображена на рисунке 24.

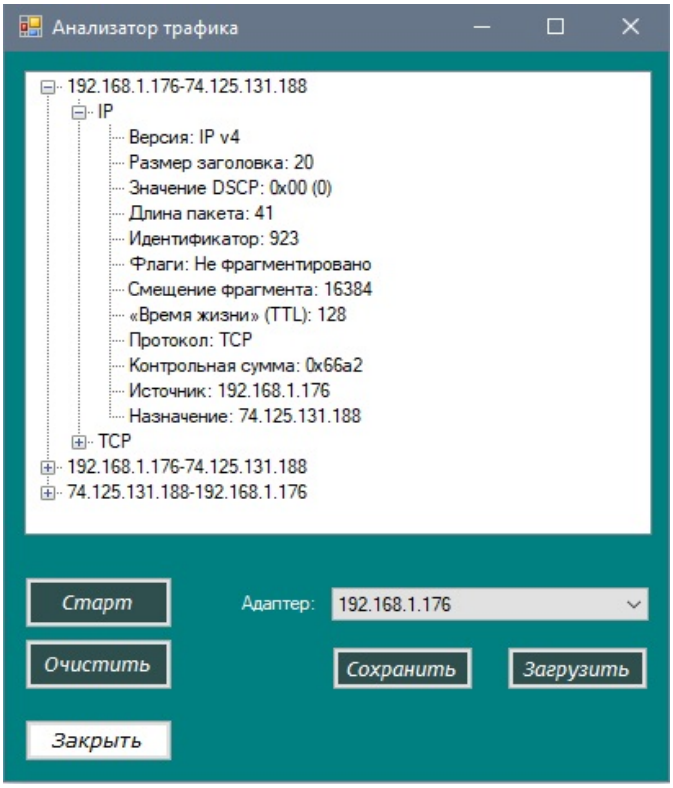


Рисунок 23 – Форма «Анализатор трафика» с захваченными пакетами

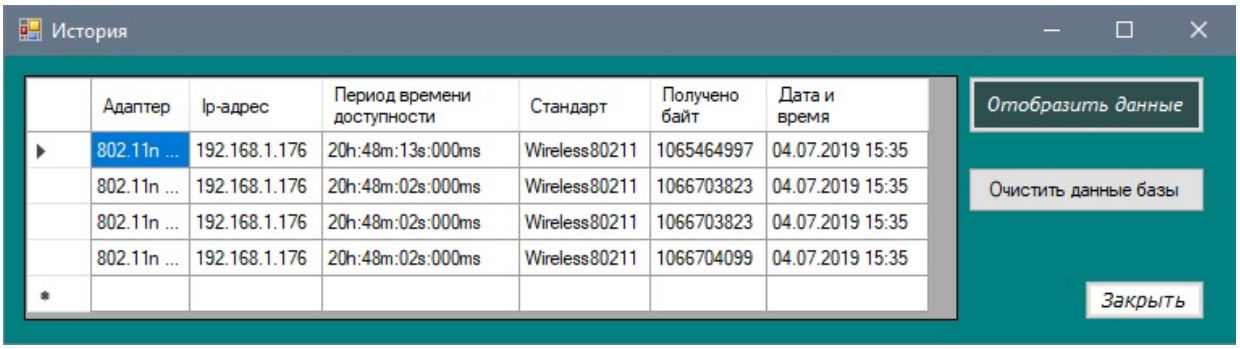
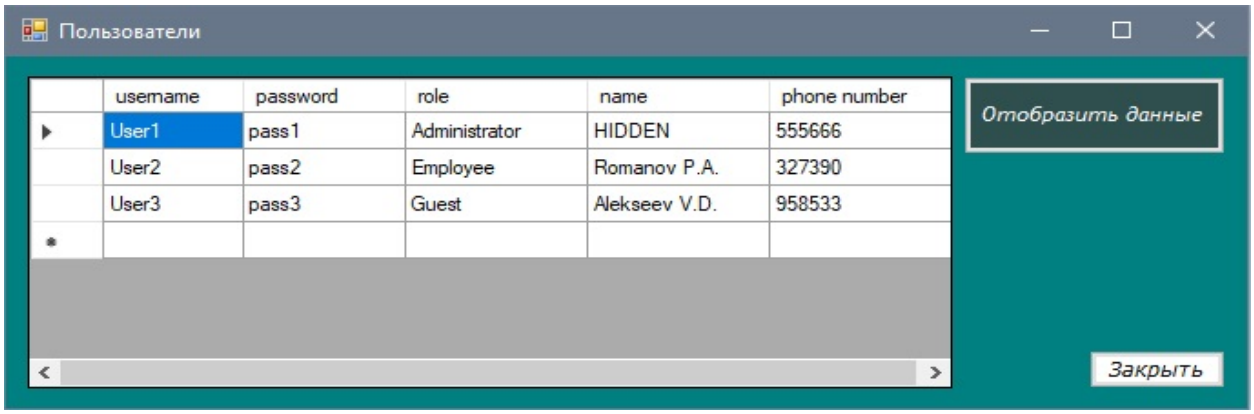


Рисунок 24 – Форма истории с выведенными данными из хранилища

Нажатие кнопки «Пользователи» главной формы позволяет открыть соответствующую форму. На ней расположены две кнопки. «Отобразить данные»



выводит таблицу в поле элемента DataGridView. Кнопка «Закрыть» закрывает текущее окно программы (рисунок 25).

Рисунок 25 – Форма «Пользователи» с выведенными данными из хранилища

3.3.5 Тестирование и оценка качества программного продукта

По окончанию написания программного продукта значимым этапом является его тестирование. Оно проводится с целью оценки реализованного функционала и других характеристик.

Тестирование функций предполагает проверку возможностей программы в течении тестовой сессии. Основное внимание уделяется соответствию требованиям, предъявленным к продукту.

Интерфейс программы спроектирован таким образом, чтоб он был простым, интуитивным, но в то же время функциональным. Программа не перегружена формами и их элементами, назначение которых понятно любому пользователю, запустившему программу.

Программа нетребовательна к производительности, поэтому может полноценно функционировать даже на слабых компьютерах.

Данные, предоставляемые программой информативны и полны, что позволяет работать с ними и обрабатывать их.

Размер готовой программы составляет 1,23 мб. Это вполне удовлетворяет требованию малого размера программы (рисунок 26).

Рисунок 26 – Размер программы

Код программы максимально оптимизирован для высокой скорости работы и экономии места.

Программа протестирована на ОС Windows 7 x32 и более поздних версиях. Весь функционал сохранен, критических ошибок не обнаружено.

В программе реализовано создание отчета в виде текстового файла, который можно прочитать только лишь в самой программе, что снизит риск прочтения информации в случае ее похищения.

Из вышесказанного следует, что все требования были выполнены в готовом продукте и заказчик может приступать к использованию программы.

Для удобства и информативности в программе реализована обработка исключительных ситуаций. При вводе неверного логина и/или пароля, несовпадающих с занесенными в БД программа выдаст ошибку (рисунок 27).

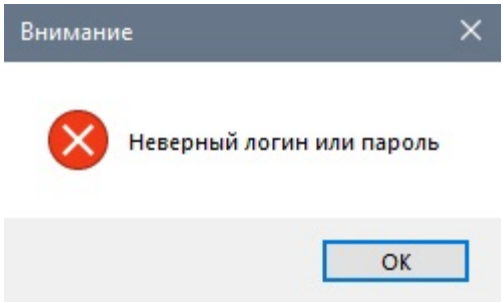


Рисунок 27 – Ошибка ввода логина и/или пароля

При нажатии кнопки «Старт» с невыбранным адаптером на форме «Анализатор трафика» программа выдаст окно с ошибкой (рисунок 28).

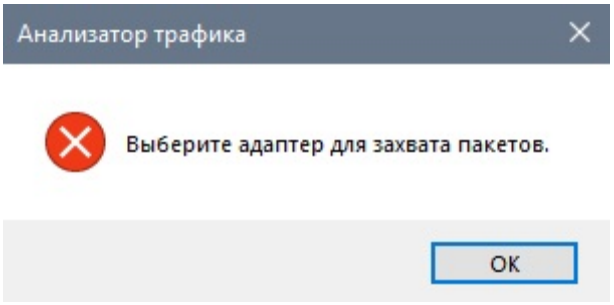


Рисунок 28 – Ошибка при отсутствии выбранного адаптера

Если программа запущена не от имени администратора, то при попытке захвата пакетов появится окно, оповещающее об ошибке доступа (рисунок 29).

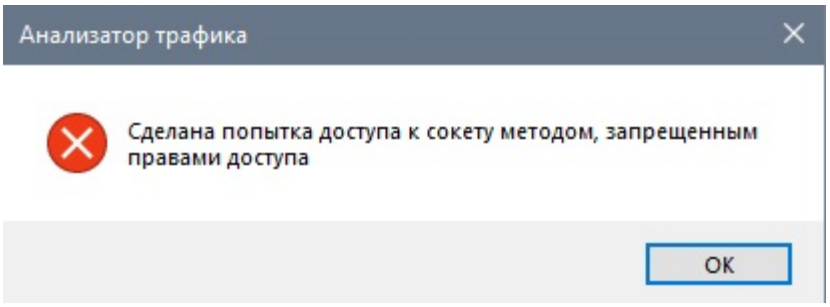


Рисунок 29 – Ошибка доступа при входе не от имени администратора

При сохранении данных на форме «Монитор беспроводной полосы пропуска» программа информирует об успешном завершении операции и выводит окно с сообщением (рисунок 30).

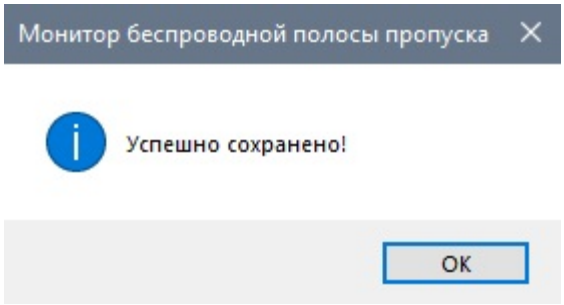


Рисунок 30 – Сообщение об успешном сохранении

Формы программы можно открывать неограниченное количество раз, что может привести к снижению производительности на слабых рабочих станциях. Поэтому рекомендуется открывать не более трех экземпляров каждой формы. На тестовом компьютере стрессовое тестирование не вызвало ошибок или сбоев. Весь функционал сохранен.

Программа отвечает заявленному качеству и работает стабильно. Конечные пользователи программы могут использовать ее в рабочем процессе.

3.5 Расчет общей стоимости проекта

Чтобы провести данный расчет относительно спроектированной сети нужно принять во внимание стоимость всего оборудования, которое было закуплено и стоимость монтажных работ.

Данный расчет будет примерным и нужен для ответа на вопрос, насколько созданная Wi-Fi сеть оказалась затратной с финансовой точки зрения.

Здание имеет 4 этажа с примерно одинаковой планировкой. Исходя из схем по реализации беспроводной сети, можно сказать, что в качестве оборудования будут закуплены 8 гигабитных коммутаторов D-Link DWS-3024 (по 2 на этаж) и 16 роутеров D-Link DAP-2695 (по 4 на этаж), работающих в режиме точки доступа.

Качественное сетевое оборудование требует немалых затрат на покупку, поэтому нужно заранее рассчитать стоимость оборудования, которое нужно закупить. На один этаж выделяются по 2 коммутатора и 4 роутера. Просуммировав стоимость этих единиц оборудования найдем общую стоимость оборудования на один этаж:

$$(17764{,}00 \times 4) + (94346{,}00 \times 2) = 259748{,}00 \text{ (тыс. руб.)}$$

В общую сеть всего нужно включить четыре этажа, что можно рассчитать путем умножения:

$$259748{,}00 \times 4 = 1038992{,}00 \text{ (тыс. руб.)}$$

За основу были взяты средние цены торгового сервиса «Яндекс.Маркет» по региону г. Благовещенска за май 2019 года [25].

Общая затраченная сумма на оборудование известна. Теперь можно так же рассчитать затраты на монтажные работы для установки необходимого оборудования. По данным сайта компании «Электрон» монтаж Wi-Fi оборудования рассчитывается на одну единицу оборудования с учетом высоты помещения. Поскольку было решено, что точки доступа будут расположены в коридорах этажей, то речь идет об установке на высоте свыше 2 метров (400 руб.). Также необходимо провести проектирование кабельной разводки для каждого из коммутаторов, что числится отдельной платной услугой (500 руб.) [12].

Для наглядности сведем все затраты в единую таблицу (таблица 8).

Таблица 8 – Общие финансовые затраты

Наименование	Количество, шт.	Цена за ед., руб.	Сумма, руб.
Роутер D-Link DAP-2695	16	17 764	284 224
Беспроводной коммутатор D-Link DWS-3024	8	94 346	754 768
Монтаж точек доступа в помещении выше 2 м	16	400	6 400
Проектирование кабельной проводки	8	500	4 000
ИТОГО:			1 049 392

Учитывая стоимость работ в данных условиях, получаем цену для одного этажа:

$$(400{,}00 \times 4) + (500{,}00 \times 2) = 2600{,}00 \text{ (тыс. руб.)}$$

И также для всех этажей:

$$2600{,}00 \times 4 = 10400{,}00 \text{ (тыс. руб.)}$$

Для соединения оборудования витой парой были использованы уже имеющиеся кабели, поэтому дополнительных затрат это не повлекло.

Важно учитывать, что каждое беспроводное устройство потребляет электроэнергию, что в конечном счете будет увеличивать расходы. Однако, с точки зрения практичности, удобства и преимуществ беспроводная сеть оправдывает выбор.

4 ЭКСПЕРИМЕНТАЛЬНЫЕ ИССЛЕДОВАНИЯ

Данные исследования направлены на получение дополнительных сведений о реализованной Wi-Fi сети, которые помогут определить дальность сигнала и определить зону покрытия, используя специальные формулы для расчета, и могут быть произведены после внедрения новых технологий.

4.1 Зона покрытия Wi-Fi сети

Изготовитель Wi-Fi оборудования, обычно указывает зону покрытия, в пределах которой гарантируется надежная и устойчивая работа его товара. К примеру, имеющаяся мощность передатчика 16 – 18 dBm обеспечит зону устойчивой работы 200 м. Учитывая эти параметры и принимая во внимание, что мощность сигнала падает пропорционально квадрату расстояния, можно рассчитать необходимую дополнительную мощность сигнала для передачи на любое расстояние:

$$\Delta P=20(Log10L - 2,3), \quad (1)$$

где ΔP – дополнительная мощность [dBm] необходимая системе;

L – расстояние [м].

Дополнительная мощность достигается путем установки антенн, маркировка которых указывается в dBi (коэффициент усиления по отношению к изотропной антенне). Его необходимо перевести в dBd (коэффициент усиления по отношению к дипольной антенне):

$$dBd = dBi - 2,2, \quad (2)$$

Использование антенн означает, что на коэффициент усиления системы будут влиять:

− потери в фидерах;

− коэффициент усиления антенны передатчика;

− коэффициент усиления антенны приемника.

Потери в фидерах (кабельных сборках) рассчитываются по следующим характеристикам:

– потери в пиктейлах - 2 dBm/m;

– потери в кабеле RJ-8U - 0,3 dBm/m;

– потери в конекторах - 1-2 dBm/m.

Предметы, расположенные в зоне действия сигнала Wi-Fi влияют на радиус сигнала и его мощность. Такие предметы в некоторых случаях полностью способны поглощать сигнал. В других ситуациях они отражают микроволны, препятствуя распространению сигнала.

4.2 Расчет зоны действия сигнала

Дальность действия радиосигнала высчитывается по формуле расчета дальности, которая вытекает из инженерной формулы расчета потерь в свободном пространстве:

$$FSL = 33+20\ (1gF+1gD), \quad (3)$$

где FSL (Free Space Loss) - потери в свободном пространстве (дБ);

F – частота канала связи (МГц);

D – расстояние между двумя точками (км).

FSL определяется суммарным усилением системы. Оно рассчитывается следующим образом:

$$\text{УдБ} - P_t, \text{дБмВт} + G_t, \text{дБи} + G_T, \text{дБи} - P_{min}, \text{дБмВт} - L_t, \text{дБ} - L_T, \text{дБ}, \quad (4)$$

где $P_t, \text{дБмВт}$ – мощность передатчика;

$G_t, \text{дБи}$ – коэффициент усиления передающей антенны;

$G_T, \text{дБи}$ – коэффициент усиления приемной антенны;

P_{min}, дБмВт – чувствительность приемника на данной скорости;

L_t, дБ – потери сигнала в коаксиальном кабеле и разъемах передающего тракта;

L_r, дБ – потери сигнала в коаксиальном кабеле и разъемах приемного тракта.

Каждая скорость характеризуется своей чувствительностью приемника. Чувствительность отражает минимальный уровень входящего сигнала, который способно принять устройство. Невысокие скорости отличаются наибольшей чувствительностью. Например, скорость 1-2 Мегабита имеет чувствительность от минус 90 дБмВт до минус 94 дБмВт. По мере возрастания скорости чувствительность снижается. Для самых высоких скоростей чувствительность может составлять всего лишь минус 60 дБмВт. Чувствительность определяется со знаком минус.

В таблице 9 приведены значения чувствительности для некоторых скоростей.

Таблица 9 – Чувствительность приемника при разных скоростях

Скорость	Чувствительность
54 Мбит/с	Минус 66 дБмВт
48 Мбит/с	Минус 71 дБмВт
36 Мбит/с	Минус 76 дБмВт
24 Мбит/с	Минус 80 дБмВт
18 Мбит/с	Минус 83 дБмВт
12 Мбит/с	Минус 85 дБмВт
9 Мбит/с	Минус 86 дБмВт
6 Мбит/с	Минус 87 дБмВт

Разные модели разных марок могут иметь отличающиеся значения максимальной чувствительности. Она также может варьироваться для каждой отдельной модели в небольших пределах. В зависимости от дальности меняется скорость. FSL вычисляется по формуле:

$$\mathrm{FSN} = Y_{\text{дБ}} - \mathrm{SOM}, \quad (5)$$

где SOM (System Operating Margin) – запас в энергетике радиосвязи (дБ). Этот коэффициент учитывает факторы, негативно отражающиеся на дальность связи. Это температурный дрейф приемника и выходной мощности передатчика, природные условия и явления (снег, дождь, туман), нарушение связи между приемником и антенной.

Считается, что коэффициент SOM берется равным 10 дБ. ПО причине того, что 10-децибельный запас по усилению достаточен для инженерного расчета. Каждый радиоканал имеет отдельную рабочую частоту. Не все приемники могут поддерживать 14 каналов связи и некоторые их них ограничены. Однако все современные адаптеры способны обнаружить все 14, а значит, работают на всех частотах.

Центральная частота канала F берется из таблицы 10.

Таблица 10 – Центральная частота каналов

Канал	Центральная частота
1	2412
2	2417
3	2422
4	2427
5	2432
6	2437
7	2442
8	2447
9	2452
10	2457
11	2462
12	2467
13	2472
14	2484

В итоге получаем формулу для расчета дальности связи:

$$D = 10\left(\frac{FSL}{20} - \frac{33}{20} - \lg F\right) \quad (6)$$

5 ЗАЩИТА БЕСПРОВОДНЫХ WI-FI СЕТЕЙ

Технология Wi-Fi на сегодняшний день распространена настолько широко, что в каждом жилом доме можно обнаружить несколько десятков точек доступа с помощью смартфона, ноутбука или любого другого мобильного устройства, оснащенного адаптером беспроводной связи Wi-Fi. Но большинство людей не придают защите своей сети должного внимания. Часто такое халатное отношение приводит к несанкционированному доступу, зачастую даже без ведома владельца.

Но если попытку проникновения и сам факт несанкционированного доступа к домашней сети можно относительно просто вычислить и устранить уязвимость сменой пароля на более сложный, то с корпоративными сетями все значительно сложнее. Обычно злоумышленники, заинтересованные в хищении конфиденциальной информации предприятий, обладают такими методами несанкционированного проникновения в сеть, которые многократно превосходят таковые при взломе системы безопасности домашней сети.

В связи с этим, в наше время методы и концепции защиты Wi-Fi сетей безостановочно прогрессируют и развиваются, чтобы обеспечить максимальную защиту и предотвратить хищение важной информации.

5.1 Развитие технологий безопасности

Созданная группа стандартов беспроводной связи IEEE 802.11 начала обретать известность и популярность в конце XX – начале XXI века из-за своего удобства применения и единого набора протоколов беспроводной связи. Это повлекло активное развитие технологии через многочисленные тестирования, сертификацию и поддержку стандартов Wi-Fi. Со временем модернизировались не только скорость передачи данных, радиус действия и частотные диапазоны, но и механизмы защиты беспроводных сетей. В противном случае, если бы компании-разработчики не уделили должного внимания безопасности и надеж-

ности, то перспективы технологии могли бы оказаться весьма неопределенными.

Базовый и самый первый стандарт 802.11 имел в наличии довольно простой механизм защиты от несанкционированного доступа к сети, который был назван WEP (Wired Equivalent Privacy). Если перевести расширенное название, то станет ясно, что данный механизм защиты существовал лишь для того, чтобы не оставлять беспроводную сеть полностью уязвимой, так как предполагал примерно такой же уровень защиты, как и в проводных сетях Ethernet, где данный передаются по каналам связи в открытом виде, ни о каком шифровании речи не идет. Но все же для доступа к ним необходимо было преодолеть защиту с помощью определенных манипуляций с техникой и протоколами.

Уязвимости такой системы безопасности не заставили долго ждать первых способов взлома, и защита WEP была преодолена в рамках исследования группой людей из университетов и индустрии уже в 2001 году. Эксперты в области криптографии отметили, что секретный криптоключ возможно восстановить в сети всего лишь за пару часов, используя при этом средний на тот момент по производительности ноутбук. Впоследствии методики взлома совершенствовались и разрабатывались новые виды. Тогда уже было возможно удачно совершить взлом примерно за одну минуту, а в публичной демонстрации на конференции по безопасности в 2007 году этот процесс занял лишь 3 секунды.

Все это дало понять, что WEP был способен защитить лишь от случайного проникновения в сеть, в то время как злоумышленники с серьезными намерениями хищения данных или проникновению в сеть буквально в пару щелчков мыши преодолевали эту легкую преграду. WEP стал непригоден и нужно было срочно разрабатывать новые средства защиты беспроводных сетей.

Организацией IEEE была создана рабочая группа, чьей задачей было разработать замену WEP, которую можно было бы использовать для более серьезной защиты сетей. Но при этом стояла задача сохранить совместимость с уже

имеющимся на рынке оборудованием. Итогом стала новая система защиты TKIP, конструкция которой позволяла обеспечить совместимость с уже эксплуатирующимся оборудованием посредством обновления прошивок и драйверов. Это было приоритетной задачей и уже в начале 2003 года TKIP был интегрирован в новый стандарт защиты, названный WPA.

Однако, было разработано и второе решение, которое стало заделкой на будущее. WPA2 – более надежное решение, которое ориентировалось на будущие версии Wi-Fi и совместимое оборудование. В данный стандарт была внедрена криптосистема, базирующая на алгоритме AES. AES оснащал длинным и сложным для расшифровки ключом, а также имел особый режим работы CCMP, позволивший защитить целостность передаваемых данных. С помощью данного алгоритма производится шифрование потоковых данных в виде пакетов, способствуя при этом сохранению их целостности, таким образом предотвращая появление поддельных пакетов данных в канале. Принцип работы алгоритма AES представлен на рисунке 31.

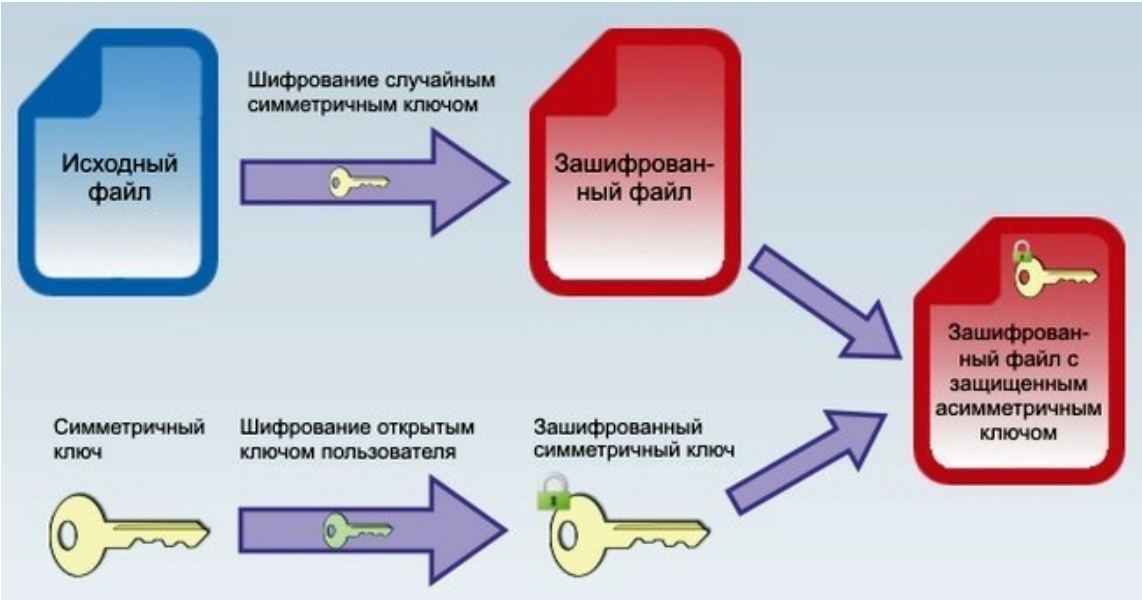


Рисунок 31 – Принцип работы AES шифрования данных

WPA2 был выпущен вместе с окончанием разработки нового алгоритма шифрования и в отличие от WPA, поддерживающего лишь TKIP, мог использовать и TKIP, и AES. Вместе с тем, почти все имеющие устройства Wi-Fi на тот

момент были модифицирована для совместимости с AES. Позже, в 2006 году, Wi-Fi Alliance принял стандарт защиты WPA2 обязательным для всего оборудования, прошедшего сертификацию.

5.2 Уязвимости WPA

Все попытки создать более безопасный стандарт безопасности Wi-Fi сетей привели к тому, что на данный момент WPA2 является приоритетным выбором при создании беспроводных сетей. Однако, в наше время все еще применяется и WPA. Но даже эти стандарты не могут обеспечить стопроцентную защищенность данных и имеют общие уязвимости, которые и используют взломщики в своих целях.

Сам стандарт WPA был создан с учетом сервера 802.1X и работы с ним. Сервер проверяет подлинность через распределение уникальных ключей для каждого пользователя, который находится в сети. Но у него имеется и другой режим работы. PSK (Pre-Shared Key) не столь безопасен как вариант работы с сервером, но предлагает свои удобства. Изначально он создавался для созданных в домашних условиях сетей, а вскоре стал использоваться и в сетях некрупных организаций, в которых все пользователи проходят процесс аутентификации с помощью единого пароля.

PSK предполагает шифрование 256-битным ключом пакетов данных в сетевом трафике каждым подключенным к сети устройством. Данный ключ может представлять собой уникальную последовательность 64 шестнадцатеричных цифр или, на усмотрение пользователя, парольную фразу, введенную «клавиатурными» символами кода ASCII, длина которой будет в пределах от 8 до 63. При использовании кода ASCII 256 бит ключа высчитываются из введенной парольной фразы путем использования криптографической функции PBKDF2. Она присоединяет к паролю SSID (идентификатор сети) и проводит 4096 битовых «замесов» при использовании хеш-преобразования.

Но даже с такими особенностями режим PSK остается крайне уязвимым и подобрать пароль возможно путем перебора или так называемым брут форсом.

При этом взломщиком используются словари, при помощи которых программа подбирает пароль для доступа к сети. В случае со слабым паролем процесс происходит довольно быстро, но с длинными фразами, состоящими из множества разных символов, это время увеличивается в десятки раз. Ни для кого не секрет, что фиксированный пароль сам по себе является уязвимостью. При его использовании следует обратиться к основам компьютерной безопасности, где рекомендуется выбирать менее предсказуемые и простые парольные фразы, разбавлять их символами верхнего и нижнего регистров, задействовать цифры и специальные символы для усложнения и повышения надежности. Обычно в условиях PSK пользователи используют случайную последовательность различных символов длинной от 13 знаков.

Вторая значимая и более опасная уязвимость стандарта WPA заключается в обратной совместимости с предыдущим поколением беспроводных устройств. Разработчики по неосторожности оставили в WPA врожденную лазейку через алгоритм TKIP, который совместим с адаптерами, поддерживающими легко взламываемый механизм защиты WEP. Данная дыра в защите может быть использована злоумышленниками для проведения серьезных атак. Заключается она в контрольных суммах, используемых для обеспечения целостности пакетов, передаваемых в пределах беспроводной сети.

Контрольные суммы функционируют по собственному механизму: подлежащая к передаче последовательность битов видоизменяется через некоторое преобразование по окончанию которого для проверки получают короткий результат, помещая его сразу после готовой к передаче последовательности. При помощи таких манипуляций становится возможным выявление ошибочных битов или пробелов в структурах пакетов данных.

Беспроводная передача данных характеризуется высокой вероятностью потерь битов или их искажения, контрольные суммы же позволяют выявлять данные ошибки и обеспечивают общую целостность данных. При совпадении

контрольных сумм и различиях в содержимом передаваемых пакетов можно говорить о факте подделки пакета.

С помощью специального метода «Chop-chop» пакеты данных дешифруются и модифицируются перестановкой байтов с конца пакета в самое начало. Данные действия проводятся без особых трудностей, так как сама контрольная сумма не шифруется. После все модифицированные пакеты отправляются точке доступа, которая отсеивает экземпляры с несовпадающей контрольной суммой. Эта операция много кратно повторяется и за 256 попыток стопроцентно подбирается один байт, после чего «Chop-chop» начинает подбирать следующий байт.

Данная уязвимость позволила многократно транслировать поддельные пакеты данных, следствием чего появились несколько новых типов атак на Wi-Fi сети. В частности, создание хаоса в работе сети, принудительно сопоставляя выбранный IP-адрес с другими Wi-Fi-адаптерами. А также стало возможным обманывать межсетевые экраны, которые умели блокировать исключительно входящие соединения.

Конечно, подделка пакетов и последующее их внедрение в сеть нельзя охарактеризовать взломом стандарта WPA. Все же информация, защищаемая с помощью этой технологии, остается в относительной безопасности, так как ключ не вскрывается и прочесть зашифрованные им данные не выйдет. Тем не менее, считать WPA надежным средством защиты уже нельзя.

WPA2 лишен таких слабостей, поэтому сегодня он является основным средством защиты Wi-Fi сетей. Он не лишен уязвимостей, но выступает наиболее надежным стандартом защиты на данный момент. В связи с этим, большинство отдают предпочтение этому методу.

5.3 Стандарт защиты WPA2

WPA2 можно считать глубоко модернизированным и улучшенным механизмом защиты WEP, который был присущ базовому стандарту 802.11. Благодаря более надежному методу шифрования, основанному на мощном алгоритме

AES, и современным протоколам, используемым в WPA2, его можно назвать хорошим средством защиты Wi-Fi сетей.

WPA2 способен функционировать в двух режимах аутентификации: персональном (WPA2-Personal) и корпоративном (WPA2-Enterprise). Вся разница заключена в ключе шифрования.

Как ранее упоминалось, использование PSK, то есть статического ключа, приводит к резкому снижению надежности и защищенности Wi-Fi сети. Он может быть скомпрометирован, что вероятно повлечет за собой нежелательный доступ посторонних лиц. Поэтому в подобной ситуации он подлежит как можно более быстрой смене. Именно такой вариант используется в персональном режиме. Для домашних сетей это не настолько критично и если использовать сложный для подбора пароль, то шанс взлома резко сокращается [20].

Корпоративные сети требуют более серьезного подхода к защите информации. Для них используются динамические ключи шифрования. Такие ключи являются уникальными для каждого пользователя, работающего на данный момент времени. Для удобства они способны обновляться в ходе рабочего процесса, при этом не провоцируя разрыв соединения. Но если постоянно создаются новые ключи, то должно быть и оборудование, генерирующее их. Таким компонентом в сети выступает сервер авторизации, и чаще всего это RADIUS-сервер.

Основой корпоративного режима служит стандарт 802.1X. Он поддерживает аутентификацию пользователей и машин, базирующуюся на контроле портов. Данный способ подходит для проводных коммутаторов и беспроводных точек доступа. Главными компонентами аутентификации 802.1X выступают сервер аутентификации, непосредственно аутентификатор и клиентский «запросчик», отсылающий запрос на сервер. «Запросчиком» можно назвать любое устройство, которое производит запрос к выбранной сети.

Сравнительные параметры безопасности стандартов приведены в таблице 11.

Корпоративный метод требует дополнительного рассмотрения в рамках проекта. В данном режиме аутентификации используется в дополнение целый набор разных протоколов. Со стороны клиентского устройства размещается специальный компонент, включенный в ПО, соискатель (supplicant), который часто является частью ОС, пытается авторизоваться через аутентификатор и взаимодействует с AAA сервером. На рисунке 32 отражена работа унифицированной радиосети. Она создана с использованием контроллера и легковесных точек доступа. Посредником между сервером и клиентским устройством может стать и сама точка доступа. В таком случае клиентский соискатель передает сформированные данные в протокол 802.1X, а уже попадая на контроллер они преобразуются в RADIUS-пакеты.

Таблица 11 – Параметры безопасности стандартов

Свойство	Статический WEP	Динамический WEP	WPA	WPA 2 (Enterprise)
Идентификация	Пользователь, компьютер, карта WLAN	Пользователь, компьютер	Пользователь, компьютер	Пользователь, компьютер
Авторизация	Общий ключ	EAP	EAP или общий ключ	EAP или общий ключ
Целостность	32-bit ICV	32-bit ICV	64-bit MIC	CRT/CBC-MAC Part of AES
Шифрование	Статический ключ	Сессионный ключ	Попакетный ключ через TKIP	CCMP (AES)
Распределение ключей	Однократное, вручную	PMK	Производное от PMK	Производное от PMK
Вектор инициализации	Текст, 24 бита	Текст, 24 бита	Расширенный вектор, 65 бит	48-бит номер пакета (PN)
Алгоритм	RC4	RC4	RC4	AES
Длина ключа, бит	64/128	64/128	128	До 256
Инфраструктура	Нет	Radius	Radius	Radius

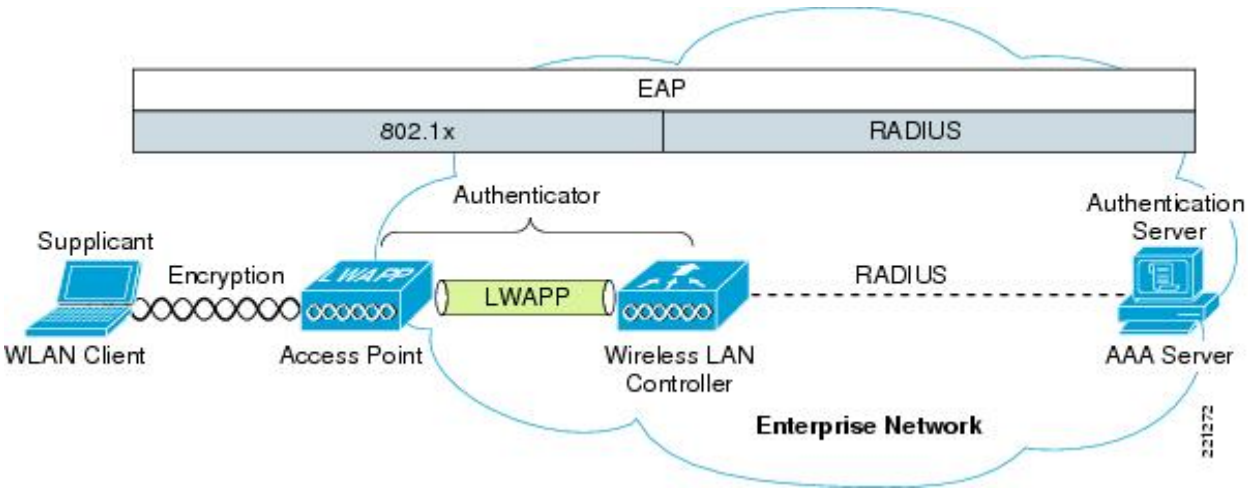


Рисунок 32 – Схема действия унифицированной радиосети

Использование фреймворка аутентификации EAP означает, что сразу после успешного подтверждения подлинности клиентского устройства точкой доступа (взаимодействуя с имеющимся контроллером), она посылает запрос на подтверждение прав доступа клиента RADIUS-серверу (рисунок 33).

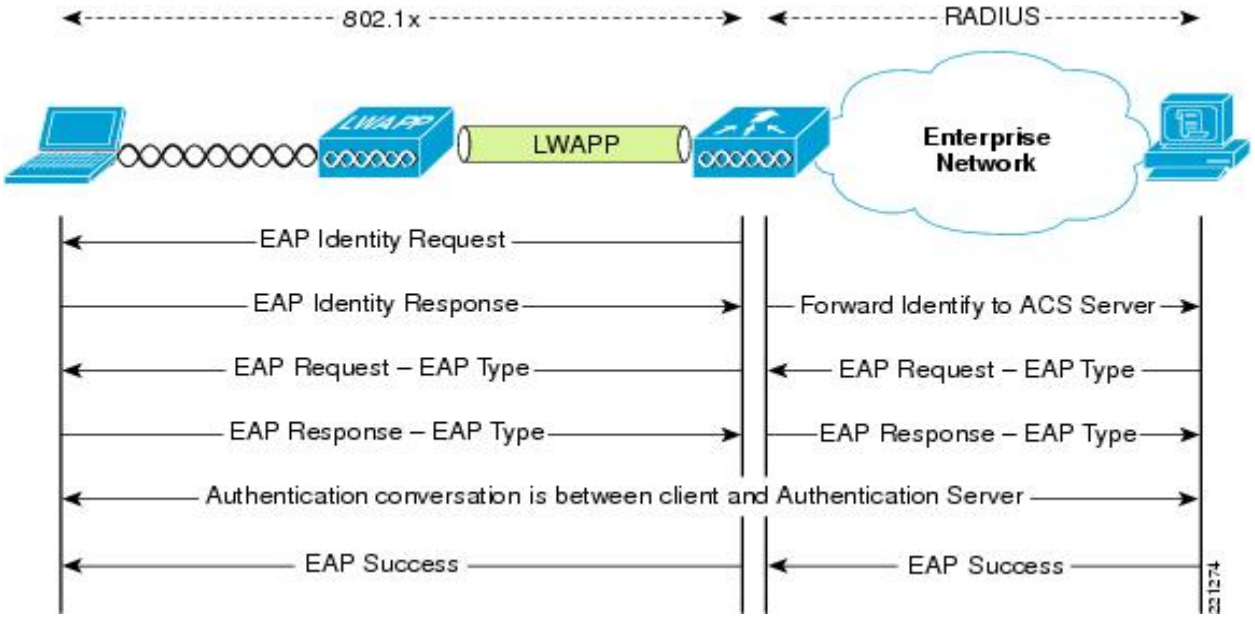


Рисунок 33 – Принцип работы EAP

Работа корпоративного режима WPA2-Enterprise подразумевает наличие RADIUS-сервера в беспроводной сети.

На данный момент наиболее подходящими для создания такого сервера являются несколько продуктов:

− Microsoft Network Policy Server (NPS) — настраивается через MMC и бесплатен. Требует купленной ОС Windows;

− Cisco Secure Access Control Server (ACS) 4.2, 5.3 — настраивается через веб-интерфейс, обладает мощным функционалом, позволяет создавать распределенные и отказоустойчивые системы. Лицензия стоит больших денег;

− FreeRADIUS — настраивается текстовыми файлами конфигурации, не удобен в плане управления и мониторинга. Бесплатен.

Контроллер при таком варианте является наблюдателем, который внимательно следит за передачей информации, ожидает успешной авторизации клиентского устройства или отказа в доступе. В первом случае RADIUS-сервер имеет возможность передать точке доступа дополнительные параметры. Например, QoS профиль, какой IP-адрес присвоить абоненту, в какой VLAN его разместить и т.д. После успешной операции обмена между точкой доступа и клиентом RADIUS-сервер позволяет им сгенерировать ключи шифрования и произвести обмен этими ключами, которые будут уникальными и действительными лишь для данной сессии (рисунок 34).

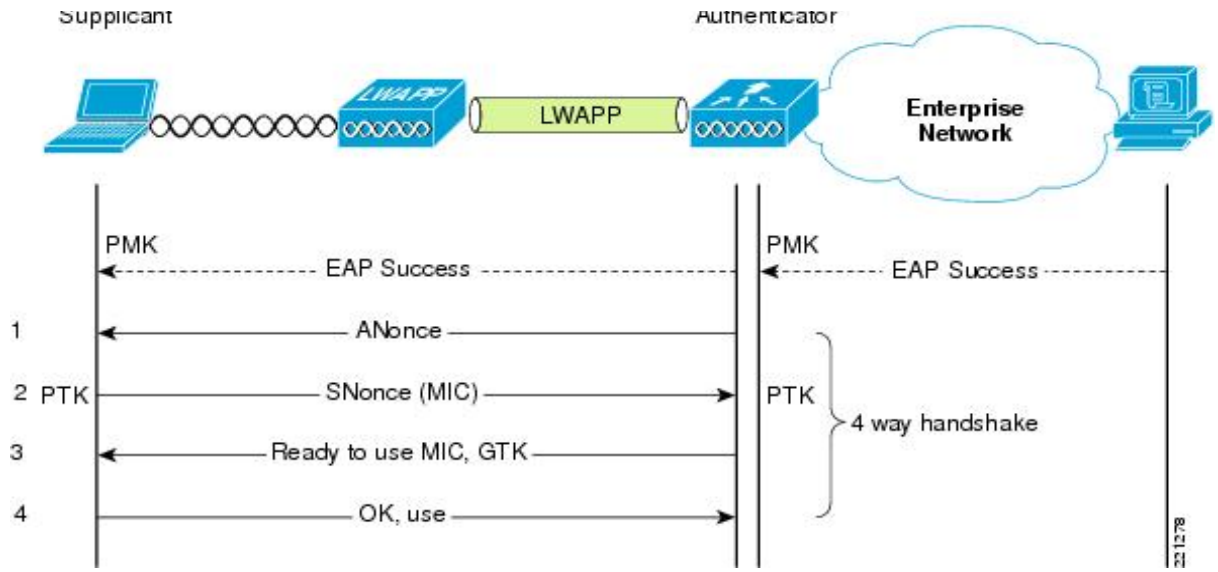


Рисунок 34 – Процесс обмена клиента с точкой доступа

Грамотно проектируя корпоративную сеть с использованием механизма защиты WPA2-Enterprise можно быть уверенным в безопасности конфиденциальных данных, доступных в пределах данной сети. Кроме того, злоумышленники не смогут беспрепятственно получить доступ в сеть даже при использовании современных средств взлома, что делает такую сеть почти неуязвимой для всех известных типов атак. Однако всегда присутствует человеческий фактор и защитить информацию от всех видов угроз разглашения, хищения, изменения или удаления просто невозможно. Но с точки зрения технического и программного обеспечения беспроводную корпоративную Wi-Fi сеть можно защитить очень хорошо.

6 БЕЗОПАСНОСТЬ И ЭКОЛОГИЧНОСТЬ

Безопасность предприятия и рабочих мест в целом это неотъемлемая часть любого технологического процесса. Сотрудники организации должны быть уверены, что в течении продолжительного времени нахождения на своем месте и на территории предприятия их здоровью и жизни ничего не вредит и не угрожает.

В связи с этим, в любой компании должен иметься свод документов, которые утверждают общий порядок и выполнение указанных правил и норм безопасности. Каждому сотруднику доводятся до сведения все имеющиеся правила и рекомендации, являющиеся обязательными к исполнению. В противном случае общая безопасность на территории и рабочих местах не может быть гарантирована.

Основная цель проекта – создание беспроводной локальной сети на основе технологии Wi-Fi для здания организации Управление Федеральной службы государственной регистрации, кадастра и картографии по Амурской области.

Из числа сотрудников отдела эксплуатации информационных систем, технических средств и каналов связи один работник назначается главным техническим специалистом беспроводной сети.

6.1 Безопасность

Работа персонала связана с компьютерами и техникой, что определяет наличие вредного воздействия на здоровье сотрудников, которое определяется по ряду факторов. В связи с эти снижается производительность труда.

Этими факторами являются:

− напряжение;

− недостаточная освещенность;

− отклонение от параметров микроклимата.

Ссылаясь на ГОСТ 12.1.005-88 ССБТ «Общие санитарно-гигиенические требования к воздуху рабочей зоны», можно сказать, что работа персонала в

помещении относится к работе легкой тяжести (1а), в связи с дистанционным управлением необходимого оборудования через компьютер.

Помещения с ЭВМ должны иметь определенные климатические условия на каждый период года.

Для холодного периода года:

- оптимальные температурные границы (22-24) С˚. Допустимые 18-26 С˚;
- относительная влажность воздуха (40-60) %, допустимая – до 75%;
- движение воздуха 0,1 м/с.

Для теплого периода года:

- оптимальные температурные границы (23-25) С˚. Допустимые 20-30 С˚;
- относительная влажность воздуха (40-60) %, допустимая – до 75%;
- движение воздуха в допустимых границах (0,1 – 0,2) м/с.

Помещение отдела эксплуатации информационных систем, технических средств и каналов связи представляет из себя кабинет, разделенный на две части. Одна отведена под рабочие места сотрудников отдела, вторая – под серверную, в которой расположены сервера.

Рабочее место сотрудника отдела состоит из нескольких компонентов:

- стол;
- эргономичный стул;
- рабочий компьютер и необходимая периферия;
- требуемая для работы оргтехника.

План рассматриваемого помещения отдела эксплуатации информационных систем, технических средств и каналов связи изображен на рисунке 35.

Помещение ориентировано на четырех сотрудников, у каждого из которых имеется свое персональное рабочее место.

Рисунок 35 – План рабочего помещения

Рабочие места организованы таким образом, что два стола сдвинуты вместе около окон, размещаясь почти вплотную в северной части кабинета. Оставшиеся два располагаются в южной и юго-восточной части соответственно. В соответствии с пунктом 9.1 СанПиН 2.2.2/2.4.1340-03 «Гигиенические требования к персональным электронно-вычислительным машинам и организации работы» (с изменениями на 21 июня 2016 года), можно отметить нарушение требований к организации рабочих мест пользователей, так как расстояние между столами с рабочими видеомониторами должно составлять не менее 2 м, а расстояние между боковыми поверхностями видеомониторов – не менее 1,2 м. Рабочие места нужно расположить в соответствии с требованиями постановления для предотвращения неблагоприятного влияния на здоровье сотрудников [2].

Для достижения этой цели рекомендуется сократить количество рабочих мест в кабинете до 3, убрав одно из расположенных в северной части помещения возле окон.

Рекомендованное размещение рабочих мест представлено на рисунке 36.

Рисунок 36 – Рекомендованное размещение рабочих мест

Рабочие сервера изолированы от основной части помещения стеной и вынесены в отдельную часть с организованным воздухообменом, так как рабочие места с ПЭВМ в помещениях с источниками вредных производственных факторов должны размещаться в изолированных кабинах с организованным воздухообменом.

Экраны видеомониторов находятся на расстоянии от 520 до 650 мм от глаз пользователя, что в общем удовлетворяет требованиям постановления,

так как экран видеомонитора должен находиться от глаз пользователя на расстоянии (600-700) мм, но не ближе 500 мм с учетом размеров алфавитно-цифровых знаков и символов.

Рабочий стол пользователя позволяет оптимально размещать используемое оборудование на рабочей поверхности. Конструкция столов устойчива и надежна, а коэффициент отражения поверхности находится в допустимых значениях.

Конструкция рабочего стула (кресла) обеспечивает поддержание рациональной рабочей позы при работе на ПЭВМ, позволяет изменять позу с целью снижения статического напряжения мышц шейно-плечевой области и спины для предупреждения развития утомления у сотрудника. Рабочие стулья (кресла) подъемно-поворотные, регулируются по высоте и углам наклона сиденья и спинки. Поверхность сиденья, спинки и других элементов стула (кресла) полумягкая, с нескользящим, слабо электризующимся и воздухопроницаемым покрытием, обеспечивающим легкую очистку от загрязнений. В соответствии с пунктом 9.6 постановления рекомендуется заменить стулья (кресла) на модели с функцией регулировки расстояния спинки от переднего края сидения для большего удобства пользователя.

Клавиатура находится поверхности стола на допустимом расстоянии от края, обращенного к пользователю.

В помещении используется общая система равномерного освещения осветительными приборами, которая освещает рабочие места в пределах допустимых норм. Рабочие столы следует размещать таким образом, чтобы видеодисплейные терминалы были ориентированы боковой стороной к световым проемам, чтобы естественный свет падал преимущественно слева. Поэтому рекомендуется изменить расположение некоторых столов, относительно источников естественного света.

При выполнении основных или вспомогательных работ с использованием ПЭВМ уровни шума на рабочих местах не превышают предельно допусти-

мых значений, установленных для данных видов работ в соответствии с действующими санитарно-эпидемиологическими нормативами. Шумящее оборудование в виде серверов, уровни шума которых превышают нормативные, размещаются вне основной части помещения за стеной, отделяемой дверью, проем которой обит специальной резиной, поглощающей излишний шум.

ПЭВМ сотрудников соответствуют требованиям настоящих санитарных правил и полностью безопасны для рабочих манипуляций с ними.

Таким образом, организация рабочих мест пользователей нуждается в корректировке по некоторым пунктам постановления для минимизации вредоносного влияния на здоровье.

При работе за ПЭВМ рекомендуется выполнять физические упражнения, снимающие нервное напряжение и расслабляющие тело:

− медленно опустить подбородок на грудь и оставаться в таком положении 5 с. Проделать 5-10 раз;

− откинуться на спинку кресла, положить руки на бедра, закрыть глаза, расслабиться и провести в такой позе 10-15 с.;

− выпрямить спину, тело расслабить, закрыть глаза. Медленно наклонять голову вперед, назад, вправо, влево;

− сидя прямо с опущенными руками, резко напрячь мышцы всего тела. Затем быстро полностью расслабиться, опустить голову, закрыть глаза. Провести в такой позе 10-15 с. Проделать упражнение 2-4 раза;

− сесть удобно, слегка расставив ноги. Руки положить на середину живота. Закрыть глаза и глубоко вздохнуть через нос. Задержать дыхание (насколько возможно). Медленно выдохнуть через рот (полностью). Проделать упражнение 4 раза (если не возникнет головокружение).

При организации и проверке локальной вычислительной сети на основе технологии Wi-Fi пользователи будут использовать разработанное в ходе создания проекта приложение для выявления возможных ошибок, обрывов связей или шумов, заглушающих сигнал. При создании интерфейса windows приложе-

ния следует обращать внимание на использованные элементы интерфейса, выбранную цветовую схему и задействованные шрифты. Общий вид приложения должен не напрягать глаза пользователей, работающих с ним, так как это может повлечь быстрое утомление и снижение остроты зрения. В интерфейсе должны отсутствовать чересчур яркие или темные элементы, а шрифт необходимо сделать легко читаемым и приемлемого размера. Так же помимо вышеизложенного, рекомендуется располагать элементы приложения таким образом, чтоб они рационально использовали место окна и были удобны для ориентации конечного пользователя в интерфейсе [3].

Главная форма разработанного программного продукта представлена на рисунке 37.

Как видно из рисунка, главным (доминантным) цветом выбран мятно-изумрудный, более темный, на котором хорошо видны более светлые элементы интерфейса. Кроме того, такая цветовая гамма успокаивающе воздействует на глаза и не так сильно нагружает их. Функциональные кнопки главной формы выполнены в темно-оливковом цвете с белой окантовкой для выделения на темном фоне. Так же использован белый шрифт Trebuchet MS, 12pt. Дополнительные кнопки выполнены белым цветом с черным текстом шрифтом Verdana, 9pt.

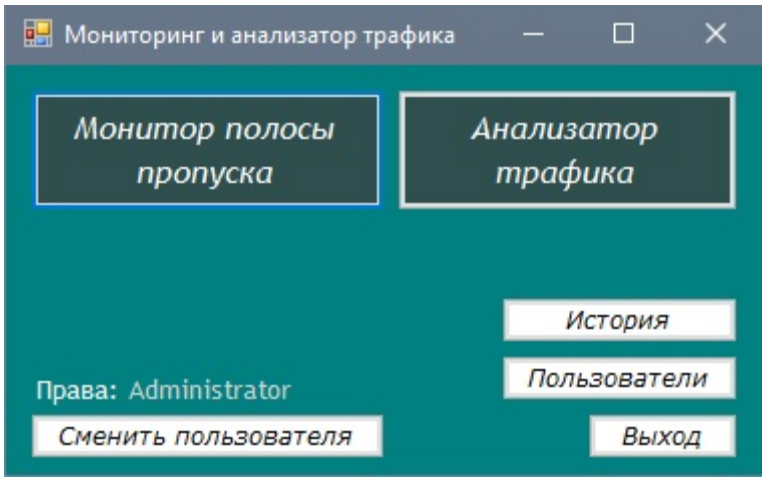


Рисунок 37 – Главная форма

Формы имеют небольшой размер и не занимают много пространства рабочего стола. Все элементы расположены с рациональным использованием свободного места, сгруппированы по принципам приоритетности использования, чтобы наиболее важные и часто используемые элементы находились на виду и выделялись цветом в сравнении с другими менее приоритетными.

Другие формы приложения выполнены в такой же цветовой схеме и по схожим принципам построения интерфейса, что позволяет отметить общую удачную эргономику разработанного приложения. Пользователям будет удобно работать с данным приложением, используя его в рабочем процессе.

6.2 Экологичность

Все устройства и техника, используемые на предприятии, учитываются при с помощью присвоенных инвентарных номеров, которые заносятся в базы данных организации и числятся в них как рабочие до момента списания. Списание производится по трем причинам:

- физический износ;
- моральный износ;
- неустранимая поломка или порча.

Компьютерная техника отличается тем, что чаще всего она морально изнашивается и устаревает. Технологии активно развиваются и продвигаются вперед, что неостановимо влечет необходимость заменять все еще исправную и рабочую технику на предприятии для выполнения новых задач. В связи с этим для компьютерной техники и оргтехники законодательством установлены сравнительно короткие сроки полезного действия для расчета амортизации — от 3 до 5 лет.

На предприятии техника может работать дольше 5 лет, находясь в рабочем состоянии и выполняя возложенные на нее задачи. По этой причине, обновление устройств может происходить реже. В связи с этим рекомендуется снизить срок рабочей техники до установленных 5 лет и по прошествии данно-

го времени заменять устаревшие образцы на более новые модели. Это повысить производительность рабочего процесса, а также снизит риск опасных поломок техники, так как большинство устройств могут быть пожароопасны при неправильной эксплуатации.

Для списания компьютерной техники и оргтехники на предприятии создается комиссия из сотрудников учреждения, которые обладают соответствующей квалификацией. Члены данной комиссии составляют акт, где подробно описывается причина, препятствующая последующему использованию данной единицы оборудования. Решение комиссии должно быть законным, поэтому к нему прилагаются документы, такие как приказ о создании комиссии, копии инвентарных карточек, копии актов о поломке и т.д.

После утверждения акта производится демонтаж списываемой техники, для извлечения компонентов, в которых содержатся драгметаллы. После такие детали отправляются на аффинажное предприятие, где из них извлекут золото и серебро. Оставшиеся части списанного оборудования доставляются на завод, который специализируется на утилизации опасных отходов предприятий.

Проведя все этапы, можно приступать к составлению акта на основании которого техника снимается с учета. К данному акту прилагаются документы, подтверждающие, что драгметаллы извлечены из оборудования, а оставшийся мусор утилизирован в соответствии с установленным порядком.

В управлении списание производится при помощи специальной фирмы, специализирующейся на утилизации офисного оборудования, что тоже допустимо. В данном случае процесс списания производится быстрее и менее трудоемкой для сотрудников предприятия.

Кроме компьютерной техники и оргтехники отдельного внимания требуют осветительные приборы. На предприятии используются люминесцентные лампы для освещения рабочих помещений. Пары ртути, которые содержатся в таких осветительных приборах, относятся к первому классу опасности (чрезвы-

чайно опасные вещества). В связи с этим, такие лампы должны утилизироваться в специальном порядке [19].

Вышедшие из строя люминесцентные лампы немедленно удаляются из осветительного прибора и упаковываются в отдельную картонную коробку. При отсутствии таких упаковок, каждая лампа надежно заворачивается в плотную бумагу или в картон, для предотвращения механических повреждений.

В соответствии с пунктами 2.4 и 2.5 постановления Правительства РФ от 3 сентября 2010 г. N 681 «Об утверждении Правил обращения с отходами производства и потребления в части осветительных устройств, электрических ламп, ненадлежащие сбор, накопление, использование, обезвреживание, транспортирование и размещение которых может повлечь причинение вреда жизни, здоровью граждан, вреда животным, растениям и окружающей среде», накопление отработанных ртутьсодержащих производится в отдельном помещении, в изоляции от других отходов [10].

Для утилизации и изъятия накопленных отходов привлекается специализированная организация, с которой составляется договор о предоставлении экологических услуг по изъятию отходов. В нем указывается:

− наименование отходов, которые подлежат изъятию;

− класс опасности отходов;

− количество;

− агрегатное состояние отходов;

− местонахождение отходов, наличие тары и ее характеристики;

− периодичность очистки временного места размещения отходов;

− условия и порядок загрузки и транспортировки.

Факт сдачи вышедших из строя ламп оформляется актом приемки-передачи, который подписывают обе стороны (предприятие и организация, принимающая отходы).

6.3 Чрезвычайные ситуации

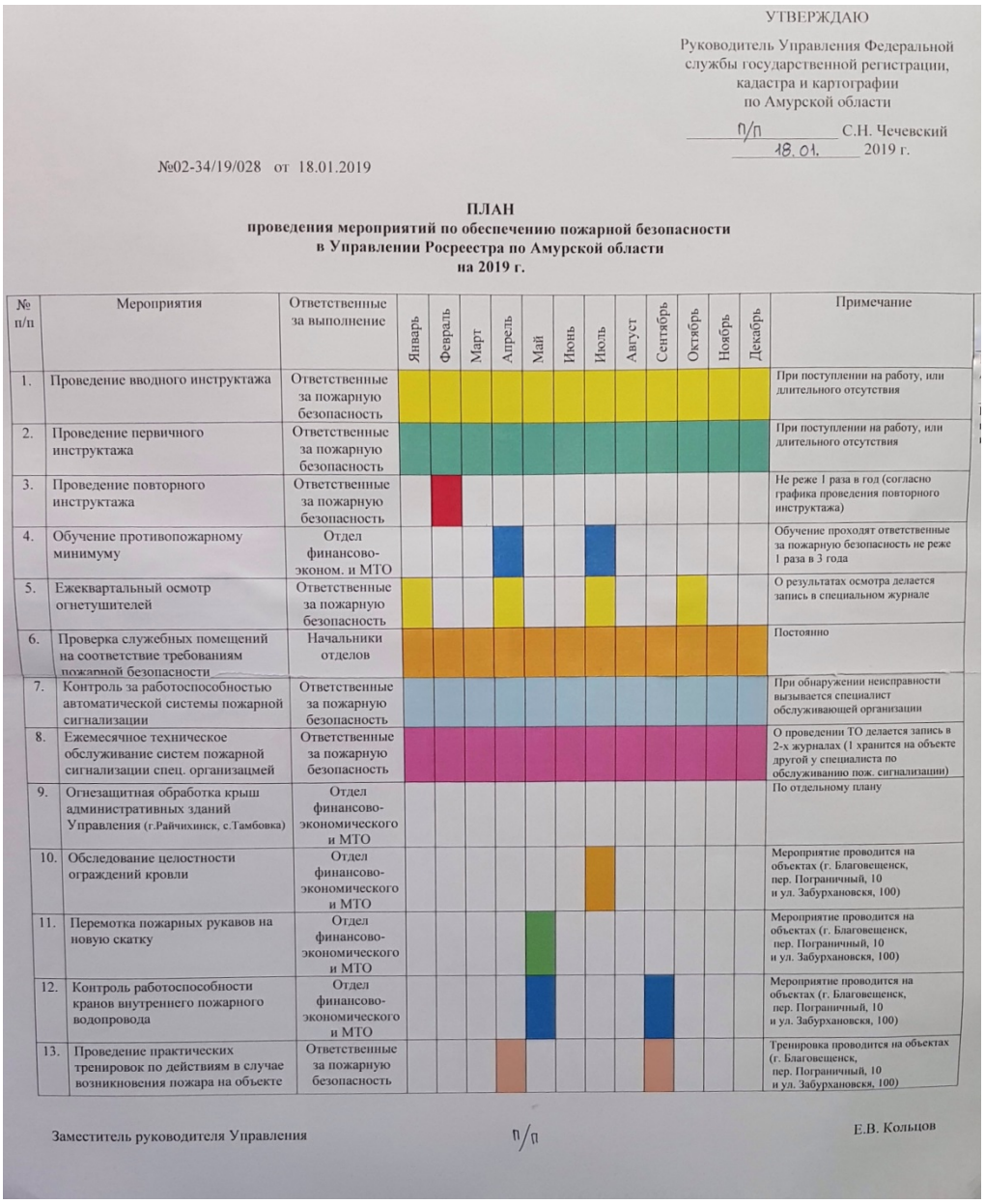
Поскольку основная техника предприятия — компьютеры с периферией и оргтехника, то наиболее вероятной чрезвычайной ситуацией является пожар. Большее количество оборудования, используемого в Управлении, является пожароопасным при неправильной эксплуатации. В связи с этим каждый сотрудник обязан соблюдать правила противопожарного режима, изложенные в Постановлении Правительства РФ от 25.04.2012 N 390 «О противопожарном режиме» [8].

На каждом объекте предприятия обязан находиться ответственный за противопожарную безопасность и пожарную сигнализацию. Для назначения ответственного лица руководитель предприятия издает приказ, которым утверждает сотрудника на данную должность. Ответственный составляет план проведения мероприятий по обеспечению пожарной безопасности в Управлении, согласно которому каждый пункт должен строго выполняться в назначенное время и фиксироваться. План проведения мероприятий представлен на рисунке 38.

Для всех сотрудников без исключений проводятся инструктажи не менее 1 раза в год, проведение которых фиксируется в журнале с обязательными подписями каждого прошедшего инструктаж. План мероприятий составляется каждый год.

В организации в соответствии с требованиями имеются порошковые огнетушители для ликвидации очагов возгорания. В серверных могут использоваться углекислотные, которые не оставляют следов. Огнетушители располагаются в строго назначенных местах и проверяются раз в квартал. В организации имеются паспорта на огнетушители. На каждый огнетушитель отводится отдельная страница в специальном журнале, где фиксируются результаты проверки с указанием даты, состоянием огнетушителя, подписью ответственного лица. Огнетушители проверяются на давление, наличие пломбы, отсутствие

механических повреждений и т.д. Срок эксплуатации каждого огнетушителя 10 лет.



УТВЕРЖДАЮ

Руководитель Управления Федеральной службы государственной регистрации, кадастра и картографии по Амурской области

п/п С.Н. Чечевский

18.01. 2019 г.

№02-34/19/028 от 18.01.2019

ПЛАН
проведения мероприятий по обеспечению пожарной безопасности в Управлении Росреестра по Амурской области на 2019 г.

№ п/п	Мероприятия	Ответственные за выполнение	Январь	Февраль	Март	Апрель	Май	Июнь	Июль	Август	Сентябрь	Октябрь	Ноябрь	Декабрь	Примечание
1.	Проведение вводного инструктажа	Ответственные за пожарную безопасность													При поступлении на работу, или длительного отсутствия
2.	Проведение первичного инструктажа	Ответственные за пожарную безопасность													При поступлении на работу, или длительного отсутствия
3.	Проведение повторного инструктажа	Ответственные за пожарную безопасность													Не реже 1 раза в год (согласно графика проведения повторного инструктажа)
4.	Обучение противопожарному минимуму	Отдел финансово-эконом. и МТО													Обучение проходят ответственные за пожарную безопасность не реже 1 раза в 3 года
5.	Ежеквартальный осмотр огнетушителей	Ответственные за пожарную безопасность													О результатах осмотра делается запись в специальном журнале
6.	Проверка служебных помещений на соответствие требованиям пожарной безопасности	Начальники отделов													Постоянно
7.	Контроль за работоспособностью автоматической системы пожарной сигнализации	Ответственные за пожарную безопасность													При обнаружении неисправности вызывается специалист обслуживающей организации
8.	Ежемесячное техническое обслуживание систем пожарной сигнализации спец. организацией	Ответственные за пожарную безопасность													О проведении ТО делается запись в 2-х журналах (1 хранится на объекте другой у специалиста по обслуживанию пож. сигнализации)
9.	Огнезащитная обработка крыш административных зданий Управления (г.Райчихинск, с.Тамбовка)	Отдел финансово-экономического и МТО													По отдельному плану
10.	Обследование целостности ограждений кровли	Отдел финансово-экономического и МТО													Мероприятие проводится на объектах (г. Благовещенск, пер. Пограничный, 10 и ул. Забурхановская, 100)
11.	Перемотка пожарных рукавов на новую скатку	Отдел финансово-экономического и МТО													Мероприятие проводится на объектах (г. Благовещенск, пер. Пограничный, 10 и ул. Забурхановская, 100)
12.	Контроль работоспособности кранов внутреннего пожарного водопровода	Отдел финансово-экономического и МТО													Мероприятие проводится на объектах (г. Благовещенск, пер. Пограничный, 10 и ул. Забурхановская, 100)
13.	Проведение практических тренировок по действиям в случае возникновения пожара на объекте	Ответственные за пожарную безопасность													Тренировка проводится на объектах (г. Благовещенск, пер. Пограничный, 10 и ул. Забурхановская, 100)

Заместитель руководителя Управления п/п Е.В. Кольцов

Рисунок 38 – План проведения мероприятий по обеспечению пожарной безопасности в Управлении

Кроме огнетушителей в коридорах установлены пожарные краны, которые так же используются для ликвидации пожара на территории. Отдельно для пожарных кранов назначается ответственный человек, который следит за их состоянием. Каждый пожарный кран проверяется 2 раза в год. Производится

осмотр в присутствии лиц от специальной организации, которые подтверждают исправность пожарного крана. Рукава раз в год перематываются во избежание разрыва на сгибах льняных нитей лицами этой же организации. На каждую процедуру строго составляется отдельный акт.

В зависимости от общего количества персонала проводится инструктаж действий при пожаре (> 25 человек). 2 раза в год отрабатывается учебная эвакуация из здания, которая тоже фиксируется в журнале. Для эвакуации существует специальная инструкция, которой должен следовать каждый сотрудник при пожаре:

− в случае возникновения и обнаружения признаков пожара необходимо оповестить пожарную охрану, передать информацию;

− оповестить людей, нажав кнопку пожарной сигнализации, если не сработал датчик;

− если пожар малых размеров, то принять меры по тушению. В противном случае по схемам эвакуации покинуть здание;

− встретив сотрудника наряда по ликвидации пожара, сообщить ему место очага и информацию о том, все ли были эвакуированы.

На объектах в коридорах должны быть информационные знаки, план эвакуации и схема эвакуации, по которой нужно двигаться при возникновении пожара, если здание большое по площади. Инструкция на каждом объекте разная, но они похожи в силу однотипности зданий. План эвакуации 3-го этажа административного здания проиллюстрирован на рисунке 39.

На территории предприятия в помещениях установлены датчики пожарной сигнализации. В кабинетах с подвесным потолком дополнительные датчики устанавливаются за потолок. Сигнализация проверяется раз в квартал с составлением специального акта. Для этого заключается договор с обслуживающей компанией.

Рисунок 39 – План эвакуации

Сотрудники, отвечающие за пожарную безопасность должны иметь лицензию. Лицензия получается по окончанию обучения и действует 3 года, после чего необходимо проходить курс переобучения.

Все деревянные конструкции на крыше здания предприятия обрабатываются специальным огнезащитным раствором раз в 5 лет.

Таким образом были изучены безопасность рабочих мест на предприятии, проанализирована система противопожарной безопасности и обор технических отходов. Кроме того, из-за некоторых несоответствий были вынесены рекомендации.

ЗАКЛЮЧЕНИЕ

В качестве объекта исследования для бакалаврской работы было выбрано предприятие «Управление Росреестра по Амурской области», которое является территориальным органом федерального органа исполнительной власти, реализующим на территории Амурской области полномочия Росреестра.

Цель выпускной квалификационной работы – проектирование беспроводной сети на основе технологии Wi-Fi для внедрения в процесс деятельности организации современных технологий связи.

Для реализации поставленной цели в рамках выполнения бакалаврской работы были решены следующие задачи.

Произведен анализ предметной области рассмотрены функции, выполняемые отделами, в частности отдела эксплуатации информационных систем, технических средств и каналов связи. Для анализа функций организации составлены диаграммы в нотации DFD и IDEF0. Составлен проект по организации Wi-Fi сети в здании организации на основе нескольких вариантов, дано обоснование реализации проекта.

В рамках проекта разработано программное приложение для мониторинга полосы пропуска и анализа сетевого трафика. Выполнен анализ методов защиты информации в пределах Wi-Fi сетей с обоснованием выбора. Проанализированы безопасность и экологичность предприятия с вынесением необходимых рекомендаций, а также рассмотрен противопожарный режим организации.

Цель и задачи выпускной квалификационной работы, сформулированные на начальном этапе полностью выполнены. Разработанная программа проходит тестирование в Управлении Росреестра.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 Ватаманюк, А. И. Беспроводная сеть своими руками : моногр. / А. И. Ватаманюк. – СПб. : Питер, 2006. – 193 с.

2 Гигиенические требования к персональным электронно-вычислительным машинам и организации работы [Электронный ресурс]: постановление Главного государственного санитарного врача от 13 июня 2003 года. N 118. с изм. и доп. Доступ из справ.-правовой системы «Кодекс».

3 ГОСТ Р ИСО 14915-1-2016. Эргономика мультимедийных пользовательских интерфейсов. Часть 1. Принципы проектирования и структура. – М. : Стандартиформ, 2016. с изм. и доп. – 14 с.

4 Кабушкин, Н.И Основы менеджмента. / Н.И Кабушкин. – 11-е изд., испр. – М.: Новое знание, 2009. — 336 с.

5 Лиэри, Джонатан. Основы построения беспроводных локальных сетей стандарта 802.11 : моногр. : пер. с англ. / Д. Лиэри, П. Рошан – М. : Вильямс, 2004. – 302 с.

6 Маккалоу, Джек. Секреты беспроводных технологий : моногр. : пер. с англ. / Д. Маккалоу. – М. : НТ-Пресс, 2005. – 408 с.

7 Мауфер, Томас. WLAN: практическое руководство для администраторов и профессиональных пользователей : моногр. : пер. с англ. / Т. Мауфер. – М. : КУДИЦ-Образ, 2005. – 368 с.

8 О противопожарном режиме [Электронный ресурс]: постановление Правительства РФ от 25 апреля 2012 года. N 390. с изм. и доп. Доступ из справ.-правовой системы «Кодекс».

9 Об утверждении Положения об Административно-хозяйственном управлении [Электронный ресурс]: Приказ судебного департамента при верховном суде РФ от 14 июня 2007 года. N 74. с изм. и доп. Доступ из справ. - правовой системы «Кодекс».

10 Об утверждении Правил обращения с отходами производства и

потребления в части осветительных устройств, электрических ламп, ненадлежащие сбор, накопление, использование, обезвреживание, транспортирование и размещение которых может повлечь причинение вреда жизни, здоровью граждан, вреда животным, растениям и окружающей среде [Электронный ресурс]: постановление Правительства РФ от 3 сентября 2010 года. N 681. с изм. и доп. Доступ из справ.-правовой системы «Кодекс».

11 Олифер, В. Г. Компьютерные сети. Принципы, технологии, протоколы : моногр. / В. Г. Олифер, Н. А. Олифер – 5-е изд., перераб. и доп. – СПб : Питер, 2019. – 992 с.

12 ООО «Электрон39» [Электронный ресурс]. Калининград : 2013. URL:http://www.electron39.ru/service/wifi (дата обращения: 25.05.2019).

13 Распаев, Ю. А. Сети и системы радиодоступа / Ю. А. Распаев, В. А. Григорьев, О. И. Лагутенко. – М. : Эко-Трендз, 2005. – 384 с.

14 Росреестр [Электронный ресурс]. URL: https://rosreestr.ru/site/about/struct/territorialnye-organy/upravlenie-rosreestra-po-amurskoy-oblasti/ (дата обращения: 24.05.2019).

15 Слюсар, В. И. Системы MIMO: принципы построения и обработка сигналов / В. И. Слюсар // ЭЛЕКТРОНИКА: НАУКА, ТЕХНОЛОГИЯ, БИЗНЕС. – 2005. – № 8. – С. 52-58.

16 Столлингс, Вильям Беспроводные линии связи и сети : моногр. : пер. с англ. / В. Столлингс. – М. : Вильямс, 2003. – 640 с.

17 Таненбаум Эндрю. Компьютерные сети : моногр. : пер. с англ. / Э. Таненбаум, Д. Уэзеролл – 5-е изд., перераб. и доп. – СПб. : Питер, 2010. – 960 с.

18 Технология современных беспроводных сетей Wi-Fi. Учебное пособие : моногр. / Е. В. Смирнова [и др.] ; под ред. А. В. Пролетарского. – М. : МГТУ им. Н. Э. Баумана, 2017. – 448 с.

19 Федеральный закон от 24 июня 1998 г. № 89-ФЗ (в ред. ФЗ от 30.12.2018 № 309-ФЗ) «Об отходах производства и потребления» // Собр. законодательства Российской Федерации. – 1998. № 26. ст. 3009.

20 Хабр. Ру [Электронный ресурс] : офиц. сайт. 26.05.2006. URL:https://habr.com/ru/post/150179/ (дата обращения: 27.05.2019).

21 Шарп, Д. Microsoft Visual C#. Подробное руководство/Д. Шарп. – 8-е изд. – СПб.: Питер, 2017. – 848 с.

22 Шахнович, И. В. Современные технологии беспроводной связи : моногр. / И. В. Шахнович. – М. : Техносфера, 2006. – 288 с.

23 Щербак, Н. Переход к цифровому телевизионному вещанию / Н. Щербак // ЭЛЕКТРОНИКА: НАУКА, ТЕХНОЛОГИЯ, БИЗНЕС. – 2002. – № 1. – С. 14-16.

24 Щербо, В. К. Стандарты вычислительных сетей : моногр. / В. К. Щербо. – М. : КУДИЦ-Образ, 2000. – 272 с.

25 Яндекс.Маркет. Ру [Электронный ресурс] : офиц. сайт. 30.11.2000. URL:https://market.yandex.ru/ (дата обращения: 24.05.2019).