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 09.04.04 – Программная инженерия
Направленность (профиль) образовательной программы Управление разработкой программного обеспечения

ДОПУСТИТЬ К ЗАЩИТЕ
Зав. кафедрой
_____ А.В. Бушманов
«____» _____2021 г.

МАГИСТЕРСКАЯ ДИССЕРТАЦИЯ

на тему: Разработка программного обеспечения для тестирования беспроводной сети на основе стандарта 802.11ax

Исполнитель
студент группы 957-ом _____ (подпись, дата) М.В. Литовский

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

Руководитель научного содержания программы магистратуры
профессор, доктор техн. наук _____ (подпись, дата) И.Е. Еремин

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

Рецензент
начальник отдела информатики и выч. Техн.
ГАУЗ АО «БГКБ» _____ (подпись, дата) Д.С. Щербань

Благовещенск 2021

Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего профессионального образования
АМУРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
(ФГБОУ ВО «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: Разработка программного обеспечения для тестирования беспроводной сети на основе стандарта 802.11ax.

(утверждена приказом от 17.05.2021 №931-уч)

2. Срок сдачи студентом законченной работы: 23.06.2021 г.

3. Исходные данные к выпускной квалификационной работе: отчет по практической подготовке, нормативная документация, специальная литература.

4. Содержание выпускной квалификационной работы (перечень подлежащих разработке вопросов): аргументирование необходимости разработки, анализ области технологии Wi-Fi и ее стандартов, формирование требований к разрабатываемому продукту, выбор алгоритма реализации программмного продукта, выбор походящего инструментария и средств разработки, разработка алгоритма реализации поставленных задач, проектирование структуры программы, разработка и тестирование программы, оценка её надежности.

5. Дата выдачи задания: 25.02.2021 г.

Руководитель дипломной работы: Самохвалова С.Г, декан факультета математики и информатики, доцент, кандидат технических наук.

Задание принял к исполнению:

_____

РЕФЕРАТ

Магистерская работа содержит 104 с., 74 рисунка, 4 таблицы, 35 источников.

БЕСПРОВОДНОЙ, ИНФОРМАЦИЯ, СЕТЬ, СТАНДАРТ, WI-FI, ПРОГРАММНЫЙ ПРОДУКТ, СИГНАЛ, SSID, СКАНЕР, АНАЛИЗАТОР, МОНИТОР, МЕНЕДЖЕР, СНИФФЕР

В работе выполнен анализ области технологии Wi-Fi, ее стандартов и беспроводных сетей Wi-Fi, с целью обработки и получения информации от адаптеров беспроводной связи.

Цель магистерской диссертации: Разработка программного продукта для тестирования беспроводной сети Wi-Fi на основе стандарта 802.11ax.

Работа включает в себя:

– аргументирование необходимости разработки;

– анализ области технологии Wi-Fi и ее стандартов;

– формирование требований к разрабатываемому продукту;

– выбор алгоритма реализации программмного продукта;

– выбор походящего инструментария и средств разработки;

– разработка алгоритма реализации поставленных задач;

– проектирование структуры программы;

– разработка и тестирование программы, оценка её надежности.

Результатом магистерской работы является разработанный программный продукт, позволяющий тестировать готовую беспроводную сеть Wi-Fi. Данная программа поможет пользователям выявить проблемные участки сети, сбои устройств и подключений или проблемы, такие как узкие места трафика, ограничивающие поток данных.

СОДЕРЖАНИЕ

НОРМАТИВНЫЕ ССЫЛКИ

В настоящей магистерской диссертации использованы ссылки на настоящие стандарты 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 34.601-90. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания;

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

ГОСТ Р ИСО/МЭК 12207-2010 Информационная технология. Системная и программная инженерия. Процессы жизненного цикла программных средств;

ГОСТ 15971-90 Системы обработки информации. Термины и определения

ГОСТ 20886-85 Организация данных в системах обработки данных. Термины и определения;

ГОСТ Р 52872-2019 Интернет-ресурсы и другая информация, представленная в электронно-цифровой форме;

ГОСТ Р 57193-2016 Системная и программная инженерия. Процессы жизненного цикла систем;

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

ОПРЕДЕЛЕНИЯ, ОБОЗНАЧЕНИЯ, СОКРАЩЕНИЯ

ГГц – гигагерц;

ГОСТ - государственный общероссийский стандарт;

М – метр;

Мб – мегабайт;

Мбит/с – мегабит в секунду;

Мониторинг – режим захвата данных, который позволяет использовать Wi-Fi адаптер в режиме отслеживания;

ОС – операционная система;

ПО - программа или множество программ, используемых для управления компьютером (ISO/IEC 26514:2008);

Сниффер – программа или устройство для перехвата и анализа сетевого трафика;

СУБД – система управление базами данных;

ЭВМ – электронно-вычислительная машина;

LINQ – (Language Integrated Query) язык интегрированных запросов;

MS – Microsoft;

SQL – (Structured Query Language) структурированный язык запросов;

Wi-Fi – технология беспроводной локальной сети с устройствами на основе стандартов IEEE 802.11;

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

ВВЕДЕНИЕ

На сегодняшний день технология Wi-Fi выступает на лидирующих позициях по передаче информации по радиоканалам на рынке и распространилась практически повсеместно. Цифровую эпоху уже невозможно представить без нее.

В течении последнего десятилетия активно растет заинтересованность корпоративного сектора, так как построение сетей на основе Wi-Fi имеет ряд неоспоримых преимуществ. Проводные Ethernet сети теряют свою актуальность из-за цены и сложности обслуживания для поддержания стабильной работоспособности. Кроме того, сети Wi-Fi позволяют оптимизировать рабочий процесс и повысить производительность сотрудников, создавая удобство условий для эксплуатации. В связи с этим, все больше предприятий предпочитают переходить на сети Wi-Fi.

В независимости от своих преимуществ и недостатков, беспроводная Wi-Fi сеть остается системой, обеспечивающей обмен данными между вычислительными устройствами, в которой существует свой поток трафика, то есть вся информация, передаваемая по каналам и доступ (в случае его предоставления) к которой имеют все пользователи, подключенные к данной сети. Правильная организация беспроводной сети предполагает, что весь поток будет строго регулироваться и просматриваться в режиме реального времени на предмет наличия ошибок или обрывов в сети. Также таким образом можно выявлять подозрительную активность и анализировать загруженность трафика.

Для выполнения этих целей существуют специализированные программы-тестировщики, обычно использующиеся администраторами сетей. Поскольку большинство рабочих устройств в сети зачастую не отличается высокой вычислительной мощностью, программа должна быть легкой и не нагруженной, чтобы исключить негативное влияние на производительность рабочего устройства. Привычный функционал такой программы включает в себя определение характеристик данной сети, таких как протокол передачи,

тип подключения, ip адрес и т.д. При построении сетей такие программы находят свое применение в проверке работоспособности, помогая определять протекает ли трафик без каких-либо проблем или существуют препятствия для стабильной передачи данных.

Цель магистерской работы: Разработка программного продукта для тестирования беспроводной сети Wi-Fi на основе стандарта 802.11ax.

Выполнение работы состоит из следующих этапов:

– аргументирование необходимости разработки;

– анализ области технологии Wi-Fi и ее стандартов;

– формирование требований к разрабатываемому продукту;

– выбор алгоритма реализации программмного продукта;

– выбор походящего инструментария и средств разработки;

– разработка алгоритма реализации поставленных задач;

– проектирование структуры программы;

– разработка и тестирование программы, оценка её надежности.

Научная новизна работы состоит в разработке комплексного приложения для тестирования беспроводных сетей, отличающегося легкостью и ненагруженностью, и способного функционировать на малопроизводительных машинах.

Практическая значимость определяется возможностью программы помочь выявить неполадки внутри сети, обрывы связи и распознавать подозрительную активность.

Результатом магистерской работы является разработанный программный продукт, выполняющий тестирование параметров беспроводной сети Wi-Fi и предоставляющий пользователю необходимую информацию.

1 ТЕХНОЛОГИЯ WI-FI КАК БАЗИС ДЛЯ СОЗДАНИЯ ЛОКАЛЬНЫХ БЕСПРОВОДНЫХ СЕТЕЙ

1.1 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 1): WWAN (Wireless Wide Area Network), WLAN (Wireless Local Area Network) и WPAN (Wireless Personal Area Network).

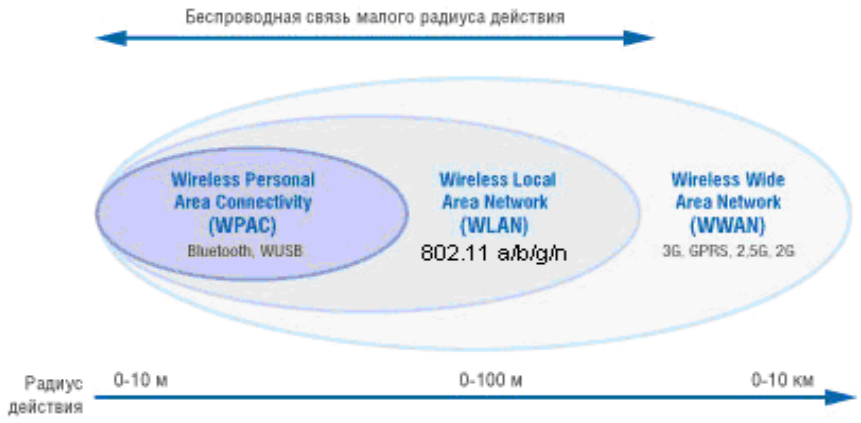

Рисунок 1 – Радиус действия персональных, локальных и глобальных беспроводных сетей

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 2).

Рисунок 2 – 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 [1].

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 [2].

Широко известные сети, именуемые Wi-Fi (Wireless Fidelity), основаны на категории стандартов IEEE 802.11. Первоначально определение «Wi-Fi» нигде в стандартах не значилось, но сам бренд Wi-Fi и его символика стали настолько широко распространены и известны в мире, что теперь наименования стандартов обрели коммерческую альтернативу.

1.2 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 [3].

В таблице 1 приведены характеристики современных стандартов группы. Предыдущие стандарты, которые внесли свое в развитие всей технологии Wi-Fi, постепенно выходят из обихода.

Таблица 1 – Характеристики стандартов группы IEEE 802.11

Стандарт	802.11n (Wi-Fi 4)	802.11ac (Wi-Fi 5)	802.11ax (Wi-Fi 6)
Год утверждения	2009	2014	2019
Рабочая частота	2.4/5 ГГц	5 ГГц	2.4/5 ГГц
Частотные каналы	20/40 МГц	20/40/80/160 МГц	20/40/80/160 МГц
Метод передачи	MIMO	MU-MIMO	MU-MIMO
Пиковая скорость, Мбит/с	600	6770	9608
Совместимость	802.11 a/b/g	802.11 b/g/n	802.11 b/g/n/ac
Максимум SU потоков	4	8	8
Максимум. MU потоков	Отсутствует	4	8
Кодирование и Метод модуляции	64-QAM OFDM	256-QAM OFDM	1024-QAM OFDM, OFDMA

1.2.1 Стандарт 802.11n

Данный стандарт был принят 11 сентября 2009 года. На момент появления 802.11n выделялся своей максимально допустимой скоростью передачи данных, которая находилась на уровне проводных стандартов и составляла примерно 600 Мбит/с. Она почти в 5 раз превышает производительность классического Wi-Fi [4].

Основными преимуществами стандарта являются [5]:

− 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 (опционально, требуется замена 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 3).

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.

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

оказывается 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);

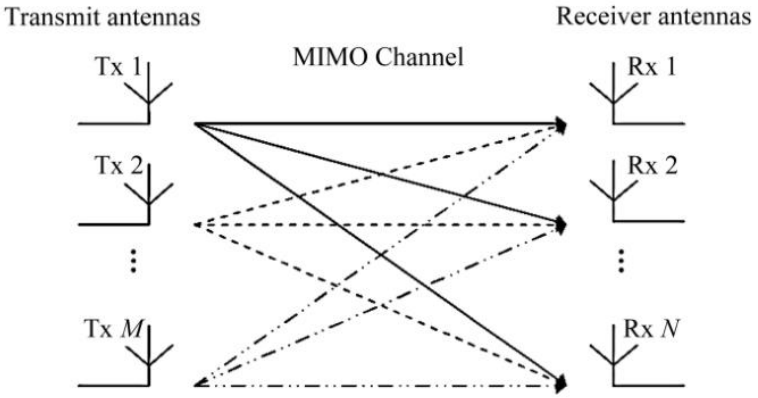

Рисунок 3 – Принцип функционирования технологии MIMO

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.

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 скорость 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 4.

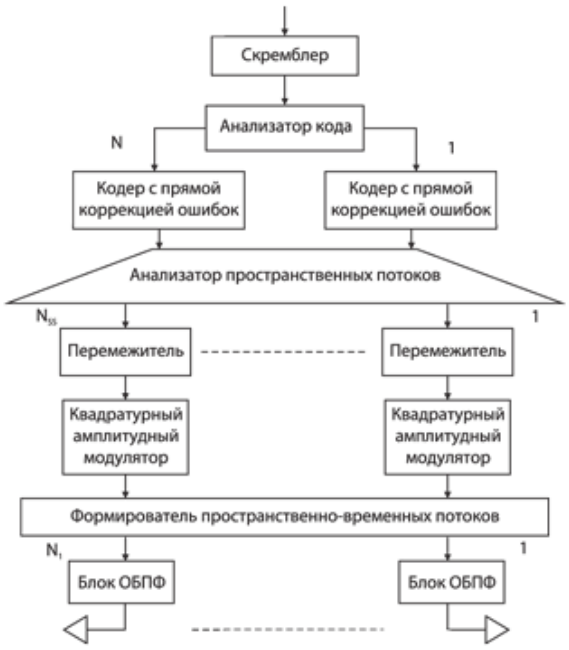

Рисунок 4 – Общая структура передатчика MIMO-OFDM

1.2.2 Стандарт 802.11ac

802.11ac, имеющий коммерческое название Wi-Fi 5, существенно отличается от своего предшественника, так как уже ориентирован на работу с несколькими устройствами в сети. Но отличия не только глобальны, но и кроются в деталях.

Был произведен переход от частоты 2.4 ГГц к 5 ГГц, по причине не только увеличенной ширины каналов связи, но и их общего большого количества. Общая зашумленность данного частотного диапазона заметно ниже, что положительно сказывается на скорости передачи по каналам связи и стабильности сигнала сети. Хоть частотный диапазон 5 ГГц и обеспечивает пониженную дальность распространения сигнала, но, в общем и целом, является более предпочтительным [6].

Частота 2.4 ГГц обладает повышенной дальностью действия сигнала, но куда более загружена и часто несет в себе помехи. Это связано с малым количеством каналов на данной частоте, их всего 14 (В РФ доступны лишь 13), непересекающихся только 3 (1, 6 и 11. Их частоты отличаются выше, чем на 20 МГц). Устройств Wi-Fi, работающих на данной частоте, уже сейчас колоссальное количество, кроме этого, данную частоту используют микроволновые печи и беспроводные телефоны, что дополнительно порождает помехи. Это неизбежно ведет к возникновению препятствий для сигнала сети.

5 ГГц хоть и предлагает пониженное расстояние распространения сигнала, имеет в своем распоряжении свыше 160-ти каналов (рисунок 5). Отсюда вытекает бесспорное преимущество данной частоты в заметном снижении загруженности и количества помех. В дополнение к этому, далеко не все устройства поддерживают данную частоту, соответственно, устройств Wi-Fi на частоте 5 ГГц суммарно меньше [7].

Усовершенствованию подверглась скорость передачи данных и теперь ее показатели доходят до 866 Мб/с по одному каналу связи. Таким образом общую пиковую скорость удалось разогнать до внушительных 6770 Мбит/с.

Достигнуть данных значений получилось за счет увеличенной до 160 МГц ширины канала связи, а также использования модуляции 256 QAM.

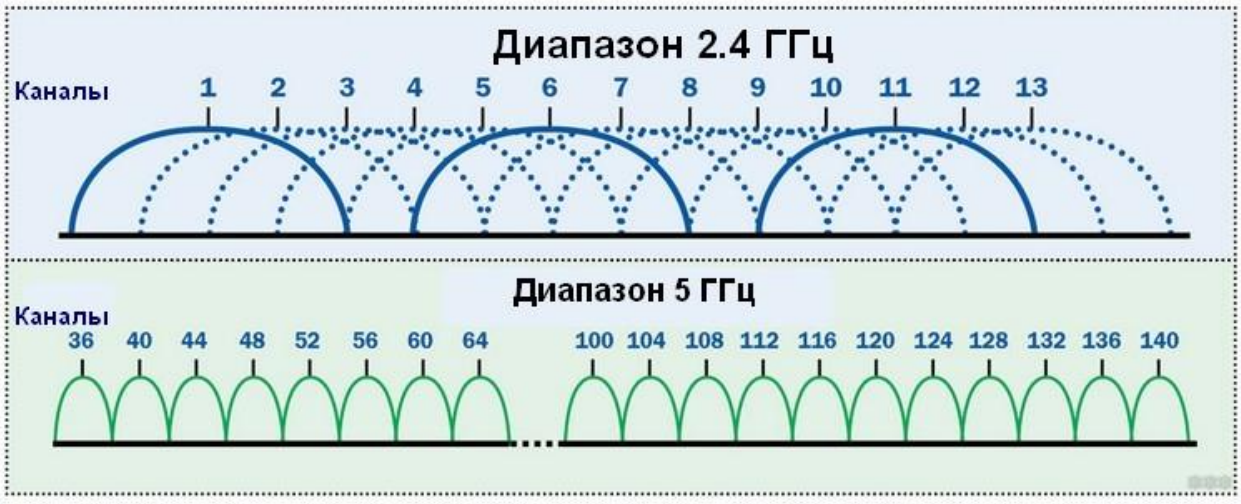

Рисунок 5 – Каналы связи 2.4 ГГц и 5 ГГц

Свое начало в 802.11ac получила технология MU-MIMO, которая дает возможность синхронно задействовать вплоть до 8 пространственных потоков данных (рисунок 6).

Рисунок 6 – Сравнение MIMO и MU-MIMO

Ранее в предшествующем стандарте 802.11n потоки загружались только для передачи данных одному клиенту, таким образом он в одиночку занимал весь канал, в то время как остальным клиентам в сети приходилось ожидать своей очереди на передачу данных. Такое использование ресурсов является крайне нерациональным. Этот серьезный минус был устранен с помощью MU-MIMO, поддерживающей OFDM мультиплексирование. Теперь происходит дробление основного канала связи на несколько более мелких OFDM

подканалов, которые используются для одновременной работы с разными клиентами в сети. Таким образом в значительной степени повышается эффективность использования сети Wi-Fi за счет исключения модели общей очереди на обслуживание [8].

1.2.3 Стандарт 802.11ax

Сегодня Wi-Fi стремительно продолжает вытеснять проводной доступ к сети и наращивать обороты. Как следствие, многократно выросло общее число устройств с поддержкой этой технологии. Беспроводные сети распространились повсеместно, располагаясь в одной области пространства. Это может стать масштабной проблемой уже в очень скором будущем, так как предшествующие стандарты группы 802.11 не были рассчитаны на такое колоссальное количество устройств и самих беспроводных сетей. Они не брали в оборот растущую межсетевую и внутрисетевую интерференцию, способную со временем практически прекратить работу беспроводных сетей, основанных на технологии Wi-Fi. Но прежде высокий уровень радиошума в частотной полосе начнет оказывать негативное влияние на работоспособность. Резкое снижение показателей пропускной способности и скорости передачи, учащенное возникновение внезапных провалов производительности, а после и вовсе временные отказы.

Начавшееся обострение данной проблемы еще в 2013 году побудило комитет стандартизации IEEE 802 создать группу для разработки к 2019 году нового стандарта, который учитывал бы ситуации с весьма плотным размещением клиентов сети и самих беспроводных сетей с целью повышения их эффективности работы. Также новый стандарт обязан был учитывать неоднородность трафика внутри современных беспроводных сетей.

Одной из ключевых особенностей 802.11ax станет использование технологии MU-MIMO при передаче не только в нисходящем канале (от точки доступа сразу нескольким устройствам-клиентам), как это было в предыдущем стандарте 802.11ac, но и в восходящем (от нескольких устройств-клиентов к точке доступа). Усовершенствованная MU-MIMO позволяет использовать до

восьми принимающих и передающих антенн. Как следствие – повышение пропускной способности в четыре раза (рисунок 7). Такой подход к методу передачи основан на отличной синхронизации клиентских устройств друг с другом, а также с точкой доступа. Создается условие для начала одновременной передачи до точки доступа без потерь сигнала, показателей скорости и качества подключения. Это предоставляет абсолютно новые возможности реализации беспроводных сетей [9].

Рисунок 7 – Сравнение Wi-Fi 5 MU-MIMO и Wi-Fi 6 MU-MIMO

MU-MIMO позволит в скором времени подключать множество устройств к сети с постоянным обменом информацией, открывая возможности для реализации Интернета вещей (IoT) [10].

Главными преимуществами 802.11ax над предшествующим стандартом являются:

− поддержание наилучшего взаимодействия точек доступа и клиентов в сети;

– обеспечение наилучшей производительности в приложениях с высокой нагрузкой на трафик (например, просмотр 4K/8K видео);

– создание полностью беспроводных рабочих офисных помещений;

– уверенная база для реализации Интернета вещей (IoT);

– улучшенное покрытие и более обширный радиус действия за счет стабильного и сильного сигнала;

– потоковая передача данных на скорости до 2,53 Гбит/с.

802.11ax открывает возможности для реализации множественного доступа с ортогональным частотным разделением (Orthogonal Frequency-Division Multiple Access, OFDMA) впервые с момента создания Wi-Fi. Обращая внимание на ожидаемый результат, технология OFDMA схожа с MU-MIMO, обе используются для организации многопользовательских передач. Разница заключена в принципе работы.

OFDMA осуществляет разделение каналов связи на блоки (ресурсные единицы), каждый из которых содержит данные и может быть передан разным клиентам одновременно (рисунок 8).

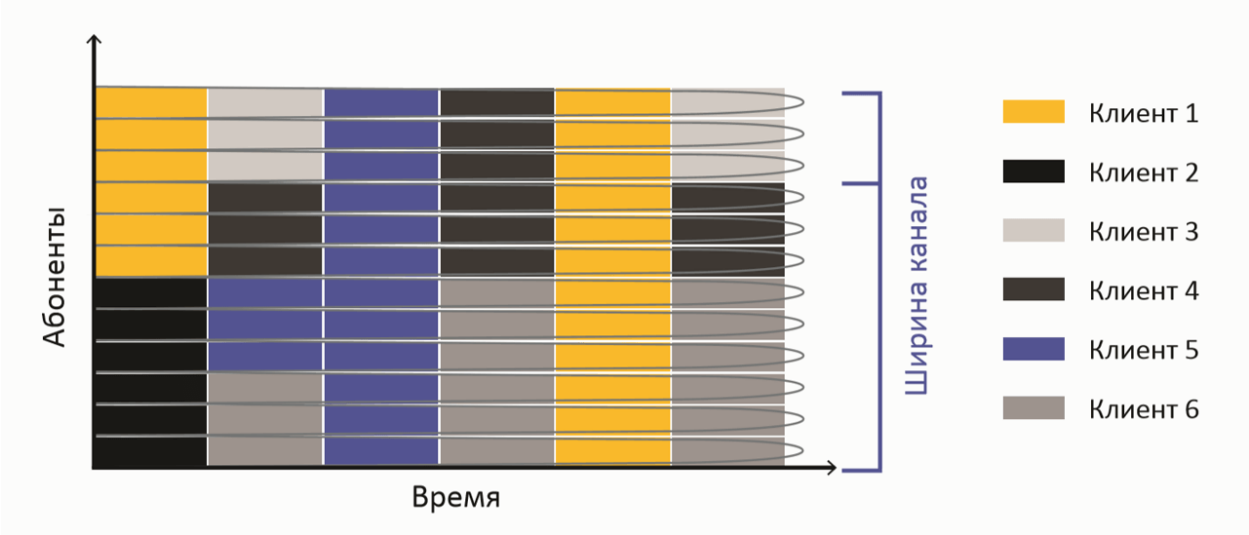

Рисунок 8 – Принцип работы технологии OFDMA

Для восходящего канала работа OFDMA имеет свои отличительные особенности, так как в таком сценарии использования происходит одновременная передача от нескольких клиентских устройств на разных группах поднесущих

(ресурсных единиц) в одном канале. Этот процесс требует координации всех клиентов в группе. Роль управляющего берет на себя точка доступа, передающая специальные триггерные кадры для указания подканала, который может использовать клиентское устройство. В случае подключения только одного клиента в сеть, точка доступа выделит канал для него целиком, но с появлением новых клиентов, пропускная способность канала будет перераспределена между всеми [11].

В дополнение, произведен переход от 256-QAM к 1024-QAM схеме модуляции. Число кодируемых бит информации в одном символе увеличилось до 10, что влечет за собой повышение скорости передачи данных и эффективность использования спектра на 25%. Модуляция столь высокого порядка, тем не менее, требует высокий уровень сигнала, а также низкое содержание шума в канале. Это обусловлено тем, что приемник принимает решение об уровне модуляции, выбирая одно из 32 состояний вдоль каждой оси, а не одно из 16 для предшествующего 256-QAM (рисунок 9).

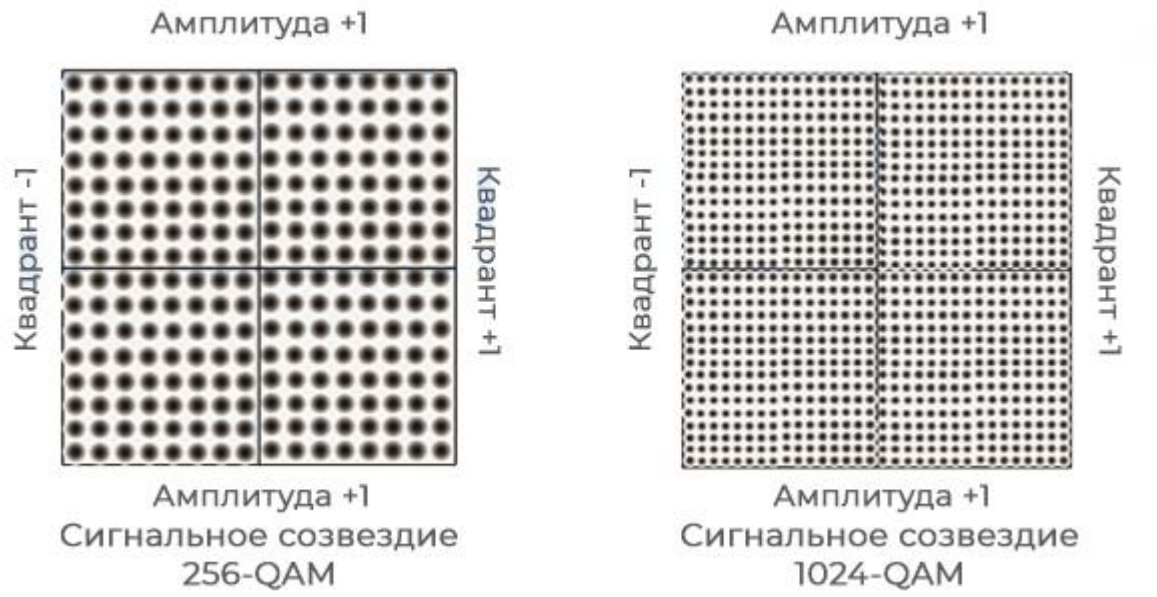

Рисунок 9 – Диаграммы сигнальных созвездий для 256- и 1024-QAM сигналов

Разработчики уделили внимание и энергоэффективности. Функция Target Wake Time (TWT) обеспечивает более эффективное планирование и

увеличение время работы устройств от аккумулятора. Она позволяет согласовать время передачи сигнала от клиентов к точке доступа и обратно. Благодаря этому сокращается время, в течение которого устройства должны быть подключены к сети, что повышает мощность передачи. Схема функционирования TWT изображена на рисунке 10.

Рисунок 10 – Иллюстрация функционирования TWT

Важным моментом остается то, что новое поколение Wi-Fi сохраняет тенденцию обратной совместимости с уже широко использующимися технологиями, принимая в оборот их возможности и повышая эффективность. Поддержка двухчастотного диапазона расширит спектр применения Wi-Fi 6 и сохранит совместимость с устройствами прошлых поколений, не исключая их возможность пользования сетями, построенных на базе нового стандарта.

Безопасность тоже подвергнута изменениям и доработке. Недавно разработанный протокол безопасности WPA3 призван сменить устаревший WPA2, запущенный в 2004 году. Основное направление изменений – устранение уязвимостей предыдущей версии протокола, в особенности, защита от атак с целью переустановки ключа (Key Reinstallation Attacks, KRACK). Такие

нововведения повышают уровень безопасности, однозначно позволяя перейти к новой версии протокола. WPA3 все так же ориентирован на два режима работы: WPA3-Personal и WPA3-Enterprise. Первый ориентирован на защиту небольших личных сетей, обычно используемых для доступа к сети Интернет. Такой режим обеспечивает 128-битное шифрование данных. Enterprise рассчитан на использование в учреждениях, где требования к безопасности и конфиденциальности информации особенно ужесточены. Для соответствия таким требованиям было введено 192-битное шифрование.

Personal режим несет в себе значительное изменение в виде интегрирования нового метода одновременной равноправной аутентификации SAE (Simultaneous Authentication of Equals), предоставляющего более дополнительную защиту от брутфорс-атак. Метод основан на идее равноправности устройств, предполагающей, что каждая сторона имеет возможность отправить запрос на соединение, после чего запускается независимая отправка информации, которая однозначно идентифицирует их. Такой механизм заменяет простой обмен сообщениями по очереди, который был реализован в методе обмена ключами PSK (Pre-Shared Key) в WPA2. SAE характеризуется и специальным вариантом установления связи, названным dragonfly handshake. В нем задействована криптография для исключения возможности угадывания ключа доступа злоумышленником. В дополнение, SAE задействует метод прямой секретности (perfect forward secrecy, PFS) с целью усиления безопасности. При каждом новом соединении устанавливается новый ключ шифрования, что усложняет процесс хакерских атак.

Новым внедренным механизмом защиты стал OWE (Opportunistic Wireless Encryption). OWE является расширением стандарта 802.11 и создан с целью обезопасить данные, передаваемые по незащищенной сети, применяя оппортунистическое шифрование. Оно не только защищает от пассивного прослушивания, но и предотвращает атаки с внедрением замаскированных пакетов данных для нарушения работы сети.

1.3 Варианты реализации локальных Wi-Fi сетей

Современные беспроводные сети можно подстроить под большое количество нужд благодаря их гибкости и вариативности. Эти наиболее ценные качества Wi-Fi сетей находят отражения в решениях, которые наилучшим образом подходят в тех или иных сферах деятельности. Каждое из них позволяет наиболее грамотно организовать беспроводную сеть, подстроить ее под определенные цели для достижения максимальной выгоды. Таким образом, Wi-Fi сеть строится с опором на множество факторов [12].

1.3.1 Решения для малого бизнеса

У данных решений имеется ряд отличительных черт, являющихся весомыми преимуществами. Прежде всего они просты в организации и их инсталляция занимает немного времени. С точки зрения затрат они экономически выгодны. Такие сети строятся для организации внутренней сети в качестве связующего звена между сотрудниками, а также доступа к сети Интернет. Используется от 3 до 6 точек доступа, по 5-9 клиентов на каждую. Необходимость в аппаратных контроллерах отпадает, т.к. настраивать и обслуживать такое небольшое количество точек доступа возможно вручную. Однако, это требует немалой квалификации IT персонала, поддерживающего стабильную работу беспроводной сети.

1.3.2 Решения для среднего бизнеса

Такие решения нередко предполагают использование программных или аппаратных контроллеров сети, по причине значительно большего количества точек доступа (10-50 штук). Настраивать и поддерживать все точки доступа по отдельности слишком затратно по времени, вследствие чего управление централизованно. IT специалист сможет оперативно и своевременно настроить нужное оборудование. Нередко такие сети комплектуются гостевой с хот-спотами, поддерживают роуминг устройств подключенных клиентов, переключая их между точками без разрыва соединений. В случае возникновения необходимости имеется возможность реализации беспроводной IP-телефонии с

выделением подсетей для данного класса оборудования. Голосовые вызовы получают наивысший приоритет над трафиком через механизмы QoS.

1.3.3 Корпоративные решения

Данный вариант решения предполагает неизбежность регулирования сети через аппаратные контроллеры высокого уровня. Общее количество точек доступа доходит до 3000, которые поддерживают беспрерывную работу до 30000 клиентских устройств. Опционально реализуется схема определения местоположения клиентов, определения источников шумов и помех, несанкционированных устройств в чети через установку точек доступа с функцией мониторинга радио эфира. Такая сеть обладает высокой устойчивостью благодаря способности к самовосстановлению: превышенный лимит шумов и помех в канале провоцирует его динамическую смену на более «чистый», а в случае выхода из строя какой-либо точки доступа ее клиенты немедленно распределяются по соседним для исключения потери связи с сетью. Отдельное внимание уделяется безопасности, которая реализована посредством RADIUS сервера с шифрованием WPA2 на базе сертификатов безопасности.

1.3.4 Решения для складских помещений и комплексов

Здесь находят свое применение точки доступа с защитой от внешних механических повреждений и физических воздействий. Важным моментом в организации такого решения является анализ места для грамотного размещения оборудования, т.к. в конструкции помещения имеется большое количество металлических частей, которые препятствуют распространению сигнала и значительно ослабляют его. Стабильная и устойчивая работа оборудования, а также бесперебойное функционирование сети в целом предполагает неукоснительное следование правилам монтажа. Чаще всего такие сети адаптированы для взаимодействия со специализированными устройствами по типу сканеров штрих-кодов, переносных терминалов и радиометок RDIF. Контроль площади обеспечивается за счет специализированных считывателей и датчиков, они объединены в целостную систему, которая представляет отдельное решение.

1.3.5 Решения для образовательных учреждений

В последнее время все чаще образовательные учреждения выражают свою заинтересованность в собственных беспроводных сетях, такой спрос не только не спадает, но и с каждым годом активно возрастает. Перенос образовательного процесса в школах и университетах в интерактивную среду с помощью беспроводного доступа открывает возможность повысить само качество обучения и, как следствие, уровень обучения. Взаимодействие студента и преподавателя значительно упрощается, т.к. не обязательно физически присутствовать в аудитории для проведения занятий, а доступ к электронным ресурсам учреждения решает вопрос с бумажными носителями информации и их ограниченным количеством. Пример организации беспроводной сети Wi-Fi в помещении учебного заведения представлен на рисунке 11.

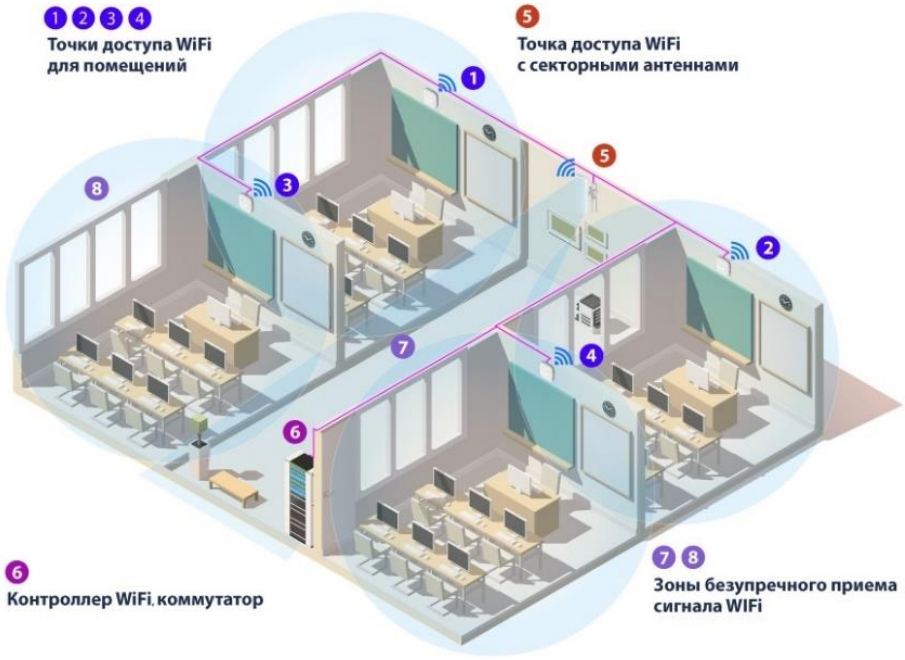

Рисунок 11 – Беспроводная сеть Wi-Fi в помещении учебного заведения

1.3.6 Объединение помещений радиомостом

Такое решение использует технологию радиомоста для связи помещений, в которых невозможно и/или экономически нецелесообразно организовать канал связи по проводным сетям. Например, если территория объекта имеет серьезные ограничения или препятствия для прокладывания кабеля под

землей, проведения воздушных линий. В иных случаях это может быть просто нерационально. Типичная ситуация – здание КПП на значительном расстоянии от основной территории и построек. Единственным вариантом является использование оборудование, спроектированное только для организации каналов точка-точка, которое не совместимо с другим Wi-Fi оборудованием. Тем не менее, это не все особенности аппаратуры. Используются точки доступа, имеющие устойчивость к агрессивным погодным условиям и защиту от перепадов температур. Их антенны имеют узкие диаграммы направленности для поддержания стабильного сигнала, а конструкция такого оборудования обычно полностью герметична. Существуют значимые ограничения, распространяющиеся на данное решение. Они обусловлены необходимостью наличия зоны прямой видимости, кроме того, область для распространения сигнала не должна содержать шумов и помех. Данная область называется зоной Френеля (рисунок 12):

Рисунок 12 – Объединение локаций радиомостом

В изображении она представлена эллипсом, на вершинах которого расположены антенны. Чаще всего антенны крепятся на мачты. С увеличением расстояния падает скорость передачи данных, в дополнение следует ожидать ослабление сигнала. Считается, что оптимальные показатели скорости и качества сигнала достигаются на расстоянии до 2 км.

1.4 Каналы связи

Для достижения наиболее значимых результатов стабильности сигнала и скорости передачи особое внимание уделяется радиочастотному диапазону и каналам связи. Современное Wi-Fi оборудование способно работать в двух частотах: 2,4 ГГц и 5 ГГц. Первая наиболее распространена в нашей стране и предлагает для использования 13 каналов. Устройства, работающие на соседних каналах, будут создавать взаимные помехи, что негативно скажется на скорости передачи и стабильности сигнала. Поэтому рекомендуется выбирать в основном независимые каналы 1, 6 и 11 (рисунок 13). В границах этих каналов отсутствуют взаимные зашумления [13].

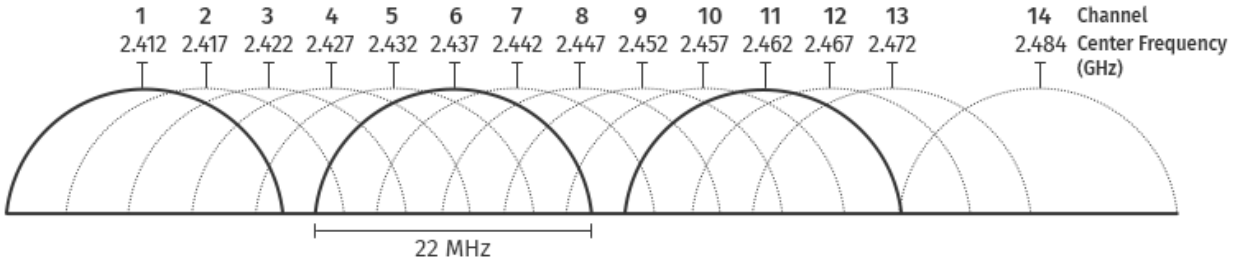

Рисунок 13 – Каналы диапазона 2.4 ГГц

Частотный диапазон 5 ГГц имеет в своем распоряжении значительно больше каналов. Из 161 независимыми являются 22, это предоставляет гораздо более обширные возможности для использования устройств без помех. В большинстве случаев частота 5 ГГц почти или абсолютна чиста. Однако, работа на данной частоте значительно снижает дальность распространения сигнала, поэтому немаловажно быть уверенным, что и оборудование, и устройства поддерживают оба частотных диапазона.

Размещать беспроводное оборудование необходимо таким образом, чтобы области покрытия соседних точек доступа перекрывались на (15-20) %. Чаще всего это гарантирует роуминг клиента в случае неисправности или сбоя работы точки. Однако следует избегать избыточного покрытия сигналов для снижения негативного влияния точек доступа друг на друга [14].

Ситуация весомо осложняется при проектировании сети в многоэтажном строении. Единственным вариантом остается учитывать возможное влияние точек доступа, размещенных на разных этажах. При проектировании имеет значение то, как распределяются точки доступа по каналам. Идеальным вариантом станет выбор разных каналов для точек доступа, размещенных на соседних этажах. На рисунке 14 изображен пример распределения каналов для двухэтажного здания.

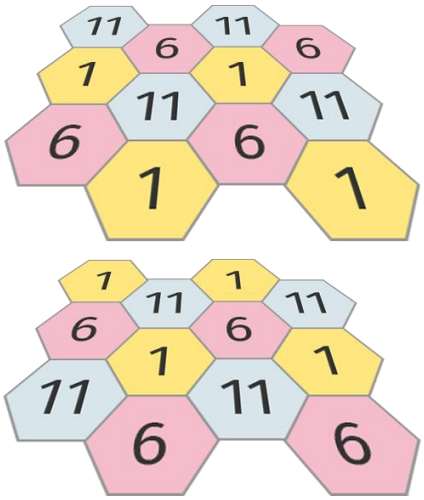

Рисунок 14 – Распределение каналов для двух этажей здания

С частотой 5 ГГц в стандарте 802.11ax все проще. Больше общее количество каналов – больше количество непересекающихся каналов. Это дает некоторую свободу выбора. Для лучшей производительности и меньшей зашумленности целесообразно по схожему принципу выставлять каналы точек доступа. Однако, Wi-Fi 6 использует механизм «раскрашивания» (рисунок 15), т.е. маркировки, пакетов в одних и тех же частотных каналах [15].

При такой схеме распределения даже расположенные рядом точки доступа на одном канале умеет различать кому какие пакеты данных принадлежат.

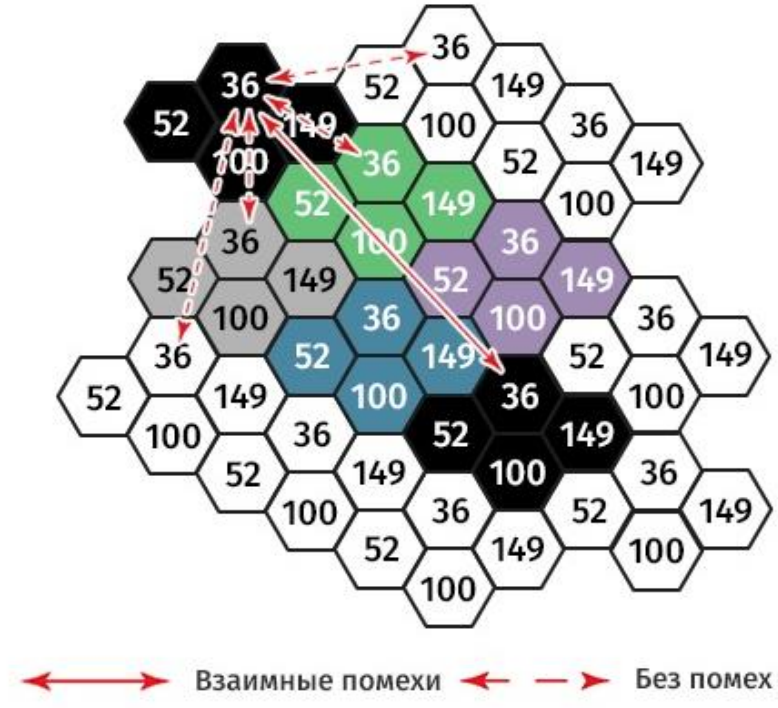

Рисунок 15 – Принцип работы механизма маркировки в Wi-Fi 6

1.5 Архитектура построения беспроводной сети

На этапе проектирования возникает вопрос, требующий детального подхода – «Количество или качество?». Иными словами, имеет смысл использовать пару мощных точек доступа или все же обойтись несколькими моделями попроще. Здесь определенно следует принять во внимание ограничения конкретного оборудования.

В спецификациях для беспроводных точек доступа может значится поддержка до 200 клиентских устройств, но на практике цифра намного скромнее. Около 20 активных беспроводных устройств. При этом, если превысить значение, то качество сигнала будет заметно ухудшаться [16]. Поэтому проектировщики прибегают к схеме установки большего количества точек доступа с сигналом меньшей мощности. Таким образом область перекрытия в процентном соотношении падает и явление радиочастотное интерференции менее выражено. Рисунок 16 отображает разницу схем построения беспроводной сети.

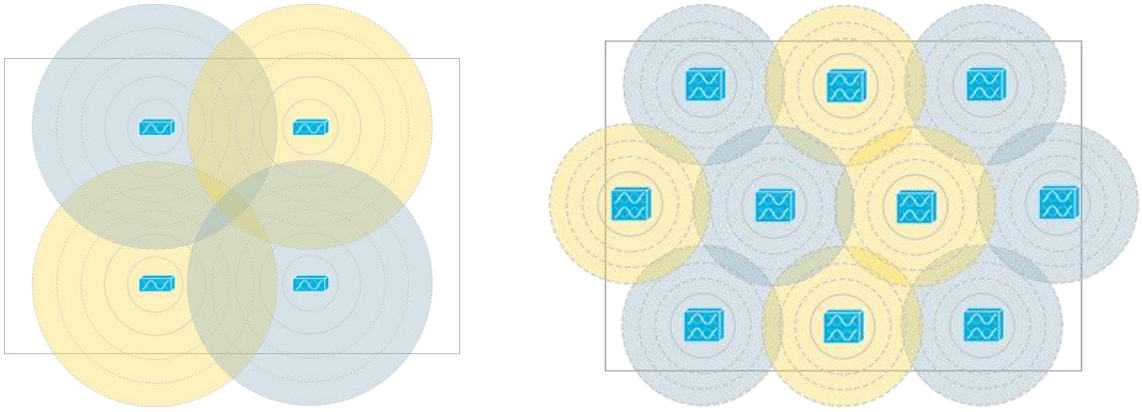

Рисунок 16 – Схемы построения беспроводной сети

Схема увеличения общего количества точек доступа хороша еще и тем, что клиент сети сможет находится ближе физически, что предоставляет возможность использования более производительной модуляции, не говоря уже об интерференции сигналов клиентов, обслуживаемых разными точками доступа, друг с другом. Еще одним плюсом выступает равномерное распределение нагрузки опорной проводной сети вкупе со снижением общего числа помех, создаваемых для соседних сетей.

Подобная модель построения сети позволяет в наилучшей степени задействовать проводную инфраструктуру и получить на практике повышения показателей скорости в условиях реального использования. Такое возможно за счет сложных модуляций, которые могут быть задействованы лишь при небольшой дистанции удаления клиента от точки доступа. Однако, в данной модели существует одна важная условность. Для управления множеством точек доступа необходим контроллер, организовывающий централизованное управление.

С точки зрения отказоустойчивости данная архитектурная модель также превалирует в сравнении с остальными. В случае выхода из строя одной точки доступа ее функции временно могут взять на себя другие, расположенные ближе всего. Таким образом работа сети не нарушается. Такое не представлялось бы возможным при покрытии определенного участка лишь одной точкой доступа.

Задействовать 5 ГГц диапазон полезно для разгрузки частоты 2.4 ГГц в которой обычно нередким явлением является зашумленность и интерференция. Но сигнал повышенной частоты сильнее подвержен поглощению разными объектами. Таким образом это вновь приводит к идее более плотной группировки точек доступа.

1.6 Качество сигнала

В корне неправильным решением будет расположить оборудование без должного плана. Точки доступа не следует располагать на объекте хаотично. Сигнал может существенно ослабляться или вовсе прерываться на определенное время из-за радиопомех. Причиной служат интерференция, работа СВЧ-печей, передача других сигналов на той же частоте и т.д. Перед установкой оборудования проводится специальная процедура радио обследования местности. Она выявляет конфликты и преграды, препятствующие качественному распространению сигнала. По результатам этой операции будет видно какие места больше подходят для расположения оборудования, а также какие каналы обеспечат лучшее качество связи [17].

Часто совершаемые ошибки также заметно ухудшают мощность сигнала. Расположение оборудования вблизи металлических конструкций тоже может стать причиной помех. Выбор более дешевого оборудования влечет за собой проблему слабого распространения сигнала из-за маломощных передающих антенн. В том числе повышается риск отказа оборудования, что неприемлемо, когда речь заходит об обширных сетях, например, для корпоративных зданий, учебных учреждений, отелей и т.д.

1.7 Оборудование

Помимо роутеров, которые создают беспроводные точки доступа и контроллера к ним потребуются приемники сигнала сети Wi-Fi для десктопных компьютеров. Они представлены в двух видах: подключаемые внешне USB-устройства и дискретные карты для установки в слот на материнской плате. Допускается использование обоих вариантов. Тем не менее устройства для подключения по USB интерфейсу в большинстве случаев предпочтительнее,

т.к. их легко заменить и переставить в другое место недалеко от настольного компьютера для лучшего сигнала приема.

Если имеется необходимость в большом количестве проводных подключений (например, аудитория с настольными компьютерами свыше 5 штук), то сетевой коммутатор станет отличным выбором. Он не только предоставляет возможность подключения большого количества клиентов, но также позволяет выполнить более удобную разводку сети. В этом случае коммутатор соединяется с роутером, а рабочие станции подключается в свою очередь к коммутатору. Такое решение может стать удобнее, чем оснащать множество рабочих компьютеров приемниками сигнала беспроводной сети.

Кроме того, коммутатор можно использовать для подключения множества точек доступа. Таким образом становится возможным построение грамотно организованной сети ячеистой структуры. Точки доступа подключается непосредственно к коммутатору, стационарные рабочие компьютеры также могут подключаться к нему. Такая схема сети предусматривает наличие контроллера точек доступа и маршрутизатора. Пример схемы сети с использованием коммутатора представлен на рисунке 17.

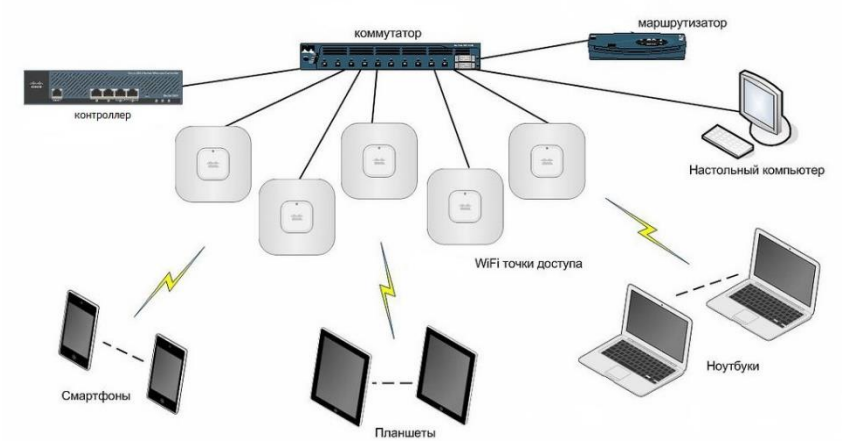

Рисунок 17 – Пример схемы беспроводной сети с использованием коммутатора

1.8 Безопасность

Вопрос безопасности беспроводной сети требует детальной проработки. Он включает в себя такие аспекты, как аутентификация пользователей (в том

числе с использованием уже реализованных систем аутентификации), авторизация в сети, защита данных при передаче по каналам связи, выявление атак и использование средств их предотвращения, обнаружение неавторизированных пользователей и их блокировка [18].

Гостевой доступ в сеть плотно соприкасается с безопасностью. Он должен быть безопасным, без угроз для гостей и предоставляться без задействования персонала. А также исключать возможность негативного влияния на работу сети и возможные угрозы для нее. Но в то же время оставаться в состоянии удовлетворить запросы клиента-гостя. Для этого необходимо определить какая область сети будет отведена для гостевого доступа и предоставить этот доступ так, чтобы не происходило снижение скорости для зарегистрированных клиентов в сети. Администрация обязана иметь возможность отследить действия гостя и контролировать его доступ.

2 ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ДЛЯ РАБОТЫ С БЕСПРОВОДНЫМИ ЛОКАЛЬНЫМИ СЕТЯМИ

Еще не так давно беспроводные локальные сети Wi-Fi, если и были реализованы, использовались с целью передачи скромного потока данных по типу почтовых сообщений, документов и различных файлов небольшого объема, служебной информации клиентских устройств в сети. Такой трафик обычно передается с низким приоритетом. Сегодня картина совершенно изменилась. Помимо вышеописанного, в настоящее время по Wi-Fi сетям в квартирах людей, в небольших компаниях и в огромных корпорациях проходит мультимедийный трафик по-настоящему колоссальных объемов в режиме реального времени. Также постоянно увеличивается общее число пользователей с мобильными устройствами, а используемые ими приложения потребляют все больше и больше трафика.

Но основании этого можно абсолютно точно сказать, что беспроводные сети Wi-Fi превращаются из некой вспомогательной структуры заднего плана в одну из самых основных и значимых. Нарушение функционала, снижение производительности и перебои связи внутри беспроводной сети могут в значительной степени повлиять на рабочий процесс целой компании, а также подвергнуть риску важную информацию, передающуюся по каналам связи в рамках беспроводной сети.

По этой причине любая реализованная беспроводная сеть Wi-Fi нуждается в тестировании и проверке, так как это поможет выявить неполадки в функционировании. Тестирование возможно проводить с помощью специализированного ПО, предназначенного для взаимодействия с сетью через адаптеры беспроводной связи. Таким образом, возможно протестировать сеть с любого клиентского устройства, оборудованного таким адаптером [19].

2.1 Алгоритм компьютеризированного решения задачи

При создании специализированного ПО, ориентированного на тестирование уже развернутой и работоспособной беспроводной сети, встает вопрос

о планируемом функционале и способе его реализации, а также алгоритме практического применения. Любая беспроводная сеть Wi-Fi базируется на проходящем в ее пределах сетевом трафике. Соответственно, в правильно и стабильно функционирующей сети этот трафик непрерывен, протекает без потерь и на максимально допустимых скоростях.

Исходя из вышеописанного, ПО должно тесно взаимодействовать с трафиком внутри сети, позволяя анализировать его на предмет потерь, обрывов и подозрительных явлений.

2.1.1 Мониторинг полосы пропускания

Мониторинг полосы пропускания является базовой операцией, задачей которой выступает предоставление информации сетевым администраторам, уполномоченным поддерживать стабильное состояние сети и обеспечивать правильное ее функционирование. Благодаря ПО для мониторинга полосы пропускания сетевые администраторы способны локализовать неполадки внутри сети, выявлять обрывы связи и распознавать подозрительную активность.

Системы мониторинга полосы пропускания помогают сетевым администраторам быстро обнаруживать сбои устройств и подключений или проблемы, такие как узкие места трафика, ограничивающие поток данных [20].

Для мониторинга полосы пропускания создается простой инструмент, который будет отображать текущую пропускную способность и другую метаинформацию о выбранном беспроводном сетевом адаптере, подключенном к компьютеру. Если подключено несколько беспроводных адаптеров, то инструмент способен обнаружить их все. Пользователь может выбрать, какой адаптер использовать для мониторинга. Кроме того, инструмент может быть модифицирован для работы с адаптерами Ethernet.

Специальный фреймворк позволяет получить доступ ко всей информации о беспроводных сетевых адаптерах через метод, используемый в коде программы. Применяя фильтрацию с помощью LINQ-запросов, информация

фильтруется, чтобы получать только информацию о беспроводных адаптерах. После этого метод взаимодействует со встроенными свойствами.

Код данного инструмента позволит рассчитать количество байтов, отправленных через беспроводной адаптер. И помимо измерения текущей скорости загрузки выбранного беспроводного адаптера открывается доступ к получению IP-адреса, связанного с беспроводным адаптером, с помощью определенного класса.

Таким образом можно реализовать небольшой инструмент, который сможет отображать параметры текущей полосы пропускания через выбранный адаптер. Данная информация полезна для подтверждения оптимальной работы сети.

2.1.2 Мониторинг сетевого трафика

Мониторинг сетевого трафика представляет собой уже куда более сложную операцию, в которую входят процесс сбора и анализа информации о сетевом трафике по которой можно судить о качественных и количественных характеристиках работоспособности сети или ее отдельных компонентов. ПО мониторинга сетевого трафика дает возможность выполнять захват пакетов данных и производить их реассемблирование для дальнейшего анализа.

Такие программы называются анализаторами сетевых пакетов или снифферами. Обычно они способны распознавать пакеты протоколов IP, TCP, UDP и DNS [21].

Для захвата пакетов используется необработанный сокет, который привязывается к IP-адресу. После установки соответствующих параметров для сокета вызывается специализированный метод. Код инструмента подразумевает, что все входящие и исходящие пакеты на конкретном беспроводном адаптере будут захвачены. Следующий параметр остается истинным, обозначая активный сокет. Затем начинается асинхронный захват всех пакетов.

Датаграмма IP инкапсулирует пакеты TCP и UDP. Она также содержит данные, отправляемые протоколами прикладного уровня, такими как DNS, HTTP, FTP, SMTP, SIP и т.д. Таким образом, пакет TCP принимается внутри

IP-датаграммы. Поэтому первое, что должно происходить – анализ IP-заголовка.

Конструктор специального класса принимает полученные байты и создает поток памяти, а затем создает двоичный считыватель для чтения данных из потока памяти байт за байтом. Данные, полученные из сети, находятся в порядке, при котором наиболее значимое значение в последовательности хранится первым, поэтому приходится исправлять порядок байтов. Это должно быть сделано для всех небайтовых элементов данных.

Заголовки TCP, UDP также анализируются идентичным образом, с той лишь разницей, что они считываются с точки, где заканчивается IP-заголовок.

2.1.3 Управление профилями точек доступа

Управление профилями точек доступа позволяет импортировать и экспортировать профили известных беспроводных точек доступа. Используя системные команды, менеджер точек доступа сохраняет из системы профиль беспроводной точки доступа, для которой пароль уже сохранен и подключение производится без его повторного ввода. Профиль сохраняется в определенной директории и может быть перенесен на другое устройство, где также с помощью менеджера происходит импорт профиля в систему. Таким образом, на новом устройстве может быть произведено подключение к беспроводной точке доступа без пароля, чей профиль был импортирован в систему.

2.1.4 Сканирование области на предмет наличия точек доступа

Сканер беспроводных точек в качестве инструмента помогает сетевым администраторам получать необходимую информацию о доступных поблизости точках доступа. Зачастую такие программы могут отображать и некоторые другие полезные данные по типу уровня сигнала, его мощность, MAC-адрес роутера, тип защиты, ее наличие или отсутствие и т.д. С помощью подобных приложений возможно посмотреть список ближайших сетей Wi-Fi и номера радиоканалов, которые они в настоящий момент используют. Из полученной информации можно будет определить менее загруженный радиоканал, радиус действия сети Wi-Fi, силу сигнала в разных местах помещения.

Посредством LINQ-запроса определяются имеющиеся активные в системе беспородные сетевые адаптеры, которые производят сканирование в радиусе своего действия. При помощи специального класса от точки доступа беспроводной адаптер получает информацию, анализируемую и преобразовываемую в привычный для пользователя вид.

Таким образом, пользователю наглядно предоставляется необходимая информация, которая может быть использована.

2.2 Обзор возможностей профильного программного обеспечения

2.2.1 Мониторинг

Программы для мониторинга способны в реальном времени отображать характеристики сетевого подключения, являясь также инструментом диагностики. Выводя полезную информацию о текущем подключении, они помогают обнаруживать отклонения показателей от штатных, что уже является сигналом о необходимости проверки и выявления причин.

В основном мониторы создаются для отслеживания скорости передачи данных, переданного объема данных и текущей операции (загрузка или выгрузка). При нагрузке на сеть неизбежно снижается скорость передачи, что сказывается на общую производительность. Монитор, используя адаптер связи, способен отобразить информацию в реальном времени, по которой администратор сети установит необходимость диагностики с целью поиска причины изменения параметров в худшую сторону.

Несмотря на относительно скромный функционал, мониторы играют важную роль в поддержании и обслуживании сетей. Они полезны как для профилактики неполадок и сбоев, так и для локализации возникающих неисправностей. Кроме того, такие программы применяются для заключения о состоянии сети на конкретно данный момент времени. Профилактическое обследование носит поверхностный характер, а единоразовое выполняется для подробного аудита состояния данной сети.

Проверять состояние сети – это общая задача мониторинга. Наибольшую эффективность мониторы проявляют в обширных и действительно

крупных сетях. Основной функцией мониторинга является отслеживание таких факторов, как:

− статус устройств. Исправно ли функционируют маршрутизаторы или же они недоступны для остальных устройств в сети? Мониторинг способен дать информацию о времени стабильного функционирования и перебоев;

− нагрузка. Wi-Fi сеть может совершать временные отказы по причине высокой нагрузки. С помощью мониторинга возможно установить моменты, когда сеть находится в стрессовых условиях;

− трафик. Мониторинг помогает получать актуальную информацию о трафике в сети, будь то объем передаваемых данных или скорость их передачи;

− уровень сигнала. Не во всех местах зоны покрытия сигнала может сохраняться стабильная качественная связь. Это явно указывает на слабый и/или затухающий сигнал от ближайшего маршрутизатора. Проверить уровень сигнала возможно с помощью мониторинга сети;

− последний доступ. Ответственный за поддержание сети администратор должен уделять внимание безопасности. В этом помогает функция многих современных устройств по отображению их последнего времени подключения к сети, т.е. время последней связи с сетью. Благодаря этому можно установить какие устройства используются чаще остальных, а какие наоборот реже, и уже на основании этой информации видоизменять сеть, подстраивая ее под необходимый режим работы.

Беспроводные Wi-Fi сети часто предполагают наличие мобильных устройств, таких как ноутбуки, которые очень популярны и пользуются огромным спросом. Например, при организации конференций или для презентаций. Поэтому им также необходимо подключение к сети. В результате мониторинг сети становится важней задачей администратора сети.

2.2.2 Анализаторы сетевого трафика или снифферы

Сниффер (от англ. «sniff» - «нюхать») – программа, способная перехватывать и анализировать данные, передаваемые по каналам связи внутри

локальной сети. Посредством этих операций может быть получена важная информация (источник передачи и назначение, протокол, контрольная сумма, длина пакета, размер заголовка, версия протокола и т.д.). Анализаторы сетевого трафика находят свое применение легальным образом в случае применения в рамках собственной сети, но также они нередко становятся инструментами злоумышленников, пытающихся перехватывать и анализировать пакеты данных чужой сети.

В руках администратора сети сниффер является отличным средством, помогающим в поддержании стабильной качественной работы сети и ее диагностике. Он работает на уровне сетевого адаптера и скрытым образом перехватывает проходящий трафик. В модели OSI снифферы расположены на канальном уровне, что означает их независимость от протоколов более высокого уровня. Сниффер игнорируют механизмы фильтрации (адреса, порты и т.д.), которые драйверы Ethernet и стек TCP/IP используют для интерпретации данных. Таким образом происходит захват всего проходящего через сетевой адаптер для просмотра и анализа. Схема работы сниффера представлена на рисунке 18.

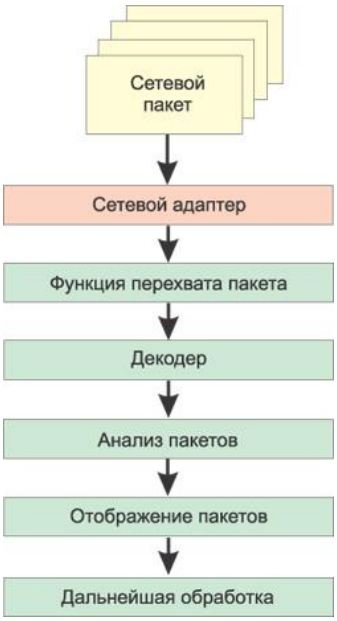

Рисунок 18 – Принцип функционирования сниффера

Для того чтобы сниффер мог перехватывать все пакеты, проходящие через сетевой адаптер, драйвер сетевого адаптера должен поддерживать режим функционирования promiscuous mode (беспорядочный режим). Именно в этом режиме работы сетевого адаптера сниффер способен перехватывать все пакеты. Данный режим работы сетевого адаптера автоматически активизируется при запуске сниффера или устанавливается вручную соответствующими настройками сниффера.

Весь перехваченный трафик передается декодеру пакетов, который идентифицирует и расщепляет пакеты по соответствующим уровням иерархии. В зависимости от возможностей конкретного сниффера представленная информация о пакетах может впоследствии дополнительно анализироваться и отфильтровываться.

Анализ проходящего трафика с помощью сниффера позволит:

− распознать вредоносный, закольцованный или паразитный трафик, который способен ощутимо загрузить каналы связи внутри сети и всю сеть целиком, а также спровоцировать сетевое оборудование на функционирование в стресс-режиме;

− обнаружить локальный разрыв связи, неисправность сети или ошибку в конфигурации агентов сети;

− перехватить несанкционированный трафик, направленный на получение конфиденциальной информации по типу паролей, логинов или другой важной информации;

− выявить вредоносное ПО;

Иными словами, анализатор сетевого трафика является довольно полезным инструментом в решении множества задач и в случае с локальными сетями представляет немалую ценность для администратора, как помощник для поддержания работоспособности сети в штатном режиме.

2.2.3 Сканеры Wi-Fi

Программы-сканеры, являющиеся, по своей сути, анализаторами, проводят сканирование области покрытия беспроводного адаптера на предмет

наличия беспроводных точек доступа Wi-Fi и выдают максимально подробную информацию о них. Кроме того, они иногда позволяют менять настройки там, где есть возможность.

У Wi-Fi сетей имеются определенные параметры, которые их характеризуют. Основные параметры, характеризующие беспроводные сети:

− стандарт. Определяет максимальную скорость передачи информации, качество сигнала точки доступа и тип используемого шифрования (802.11n, 802.11ac, 802.11ax);

− тип безопасности. Задает параметры безопасности, используемые для доступа к сети (WEP, WPA, WPA2);

− канал. Выбранный канал для передачи данных, который также определяет рабочую частоту роутера и клиентских устройств. Для каждой из рабочих частот (2,4 ГГц и 5 ГГц) существуют собственные каналы и их число разнится.

Сканер занимается сбором и анализом информации по вышеописанным показателям. Помимо этого, в рамки собираемой информации попадает имя сети (SSID), MAC-адрес роутера, а также уровень сигнала.

Сканеры подходят в качестве средств диагностики Wi-Fi сетей и определения загруженности беспроводных каналов. Они находят свое применение в замере уровня сигнала в различных помещениях у себя дома или в офисе. На основании полученной информации можно сделать выбор в пользу наиболее свободного от зашумленности и помех канала. Таким образом достигается наиболее высокая пороговая скорость и, как следствие, лучший опыт использование беспроводной сети.

2.3 Характеристика выбранного программного-технического обеспечения

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

Microsoft Visual Studio 2019 как среда разработки 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. А возможность работы с Windows-формами обеспечивает возможность создания удобных, быстродействующих и понятных интерфейсов [22].

Существующая свобода выбора языка программирования для написания программного кода позволяет рассматривать именно те варианты, проектирование на основе которых будет знакомо и понятно. Сроки выполнения строго ограничены, поэтому требуется выбрать наименее затратный по времени вариант. Программа должна работать в реальном времени, поэтому обязана 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 легче, 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, оптимизацию кода и объективную производительность в сравнении с C++. 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.

Выбор языка C# 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.

Главным приоритетом для программ выступает реализуемый функционал, поэтому на него делается особый упор. Среда разработки Microsoft Visual Studio крайне эффективный инструмент 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.

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. Кроме того, пользователь может запутаться во множестве элементов. В этом случае будет оправдано разделить модули программы на отдельные формы, которые открываются по нажатию определенных кнопок главной формы или клавиш клавиатуры, что упростит ориентацию пользователя и позволит открывать только нужные в определенный момент формы.

Ввиду своей распространенности и популярности ОС Windows 10 стала основным выбором в качестве операционной системы, под которую разрабатывается программный продукт. 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 Microsoft SQL Server, интегрированную в Microsoft 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.

Программный продукт имеет обширный функционал, базирующийся на тесной связи с беспроводной локальной сетью, на основе технологии Wi-Fi. Основной целью создаваемого продукта является сканирование и управление подключением к точкам доступа, мониторинг полосы пропускания, анализ сетевого трафика и управление профилями точек доступа через менеджер. Из этого следует, что сперва требуется определить включена ли используемая рабочая станция, на которой будет развернуто приложение, в локальную беспроводную сеть.

Для правильного взаимодействия с программой пользователь должен быть знаком с устройством беспроводной локальной сети, иметь представления о принципе ее функционирования, разбираться в терминах, используемых

программой для понимания поступающей информации, а также иметь доступ к рабочей станции. Разрабатываемая программа взаимодействует в совокупности с системными средствами ОС Windows.

Варианты реализации требований к разрабатываемому программному продукту представлены в таблице 2.

Таблица 2 – Варианты реализации требований

Критерии / № варианта	№1	№2	№3
Язык программирования	Java	C#	C++
Язык запросов	SQL	LINQ, SQL	LINQ
Количество используемых форм	1	Отдельная форма для каждого модуля	6
Операционная система	Windows 10	Windows 10	Windows 10
Подключение к сети	Да	Да	Да
Использование сетевых приложений	MS SQL Server	Не используется (интегрировано в MS Visual Studio 2019)	MS SQL Server
Разграничение доступа	Отсутствует	Системный администратор, сотрудник, гость	Системный администратор, сотрудник

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.

2.4 Проектирование программного обеспечения

2.4.1 Функциональные и нефункциональные требования

Характерной чертой для любой локальной беспроводной сети 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 проектирования, являющийся многофункциональной программой для тестирования беспроводных сетей Wi-Fi, нацелен прежде всего на сотрудников, которые имеют базовые знания в сфере сетевых технологий и должную квалификацию для работы с программными продуктами такого типа. Для обычных пользователей программа не будет представлять такой же

ценности, ввиду отсутствия у них знаний и умений использования всего функционала ПО подобного назначения.

Функциональные требования, формирующиеся для итогового программного продукта, определяют функционал, требуемый для реализации разработчиком, с целью выполнения пользователями своих задач. Они содержат положения, основываясь на которых ПО должно выполнять определенные задачи.

Прежде всего, пользователь должен иметь возможность выполнить вход с использованием своего логина и пароля для доступа к функционалу программы. Это осуществляется с целью разграничения прав доступа по ролям. При запуске программы открывается форма авторизации для ввода логина и пароля, после ввода которой должна отображаться главная форма приложения. Здесь должна выводиться информация об уровне прав авторизованного пользователя. Если роль предусматривает ограниченные права, то недоступные элементы неактивны (окрашены в красный цвет).

При нажатии на кнопку «Монитор полосы пропускания» должен происходить переход на форму с одноименным названием. Она должна содержать элемент в виде выпадающего списка с обнаруженными сетевыми адаптерами и возможностью выбора, отображать информацию по выбранному сетевому адаптеру в режиме реального времени (IP-адрес, тип операции, используемый стандарт, объем полученных данных, скорость загрузки и т.д.). Кнопка «Сохранить» должна производить запись текущих значений в БД для истории с временной меткой с целью последующего просмотра информации. Кнопка «История» отображает одноименную форму. Кнопка «Отобразить данные» выводит данные из БД в главное окно формы, а «Очистить данные» – очищает окно и записи в БД. Кнопка закрытия формы перенаправляет на главную. Кнопка «Закрыть» осуществляет переход обратно на главную форму.

После нажатия на кнопку «Анализатор трафика» открывается одноименная форма. На ней пользователь также выбирает сетевой адаптер из списка для перехвата через него сетевых пакетов данных. Кнопка «Старт» должна

начинать процесс захвата и выводить информацию о пакетах в виде раскрывающегося дерева в главном окне формы. Остановка процесса осуществляется с помощью той же кнопки, наименование которой изменяется на «Остановить». Кнопка «Очистить» очищает главное окно формы. С помощью кнопки «Сохранить» сформированное дерево с информацией должно сохраняться программой и даже после перезапуска полностью восстанавливаться через кнопку «Загрузить». Кнопка «Закрыть» закрывает форму и возвращает на главную.

Кнопка «Пользователи» выводит форму с пользовательскими данными из БД. Кнопка «Отобразить данные» должна строить таблицу с информацией по каждому существующему пользователю. Также присутствует кнопка «Закрыть». Для исключения сценария с перезапуском программы для смены пользователя должна присутствовать кнопка «Сменить пользователя», которая закроет главную форму и вновь отобразит форму регистрации. Кроме того, присутствует кнопка «Выход», завершающая работу приложения.

Предполагается, что проектируемое ПО будет развертываться на стационарных рабочих станциях и ноутбуках, которые включены в локальную Wi-Fi сеть. 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 Windows 10;

− отсутствие критических ошибок при работе;

− возможность данные в удобном для разработчика виде.

Проектируемое программное обеспечение нацелено на осуществление контроля сетевого трафика на наиболее важных узлах сети и предоставление

информации о получении, отправке и посылке пакетов данных между узлами сети по протоколу IP, TCP, UDP и DNS.

Поскольку сеть Wi-Fi подразумевает наличие портативных и мобильных устройств, подключающихся к ней, то определенным недостатком будет являться невозможность анализа с использованием планшетов и смартфонов по причине того, что программа только совместима только с ОС Windows 10. 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.

ПО проектируется для использования локально на одной рабочей станции, в связи с этим потребуется перенос копии для работы на другом рабочем устройстве. Эти действия не повлекут значимых неудобств в силу того, что программа изначально проектируется «легкой» и будет иметь небольшой размер, а также может быть передана на другую рабочую станцию посредством общей сети.

Важным моментом выступает ориентированность на непроизводительные рабочие станции. Для этого требуется учитывать, что итоговая разработка должна изначально быть спроектирована таким образом, чтобы отличаться «легкостью» и не нагружать компоненты рабочего компьютера. Таким образом, выполнение программы будет возможно даже на непроизводительных машинах.

Проектируемое ПО требует оператора – человека, компетентного и квалифицированного в определенной области, для продуктивной работы. В случае отсутствия подготовки и должных знаний могут возникнуть трудности в обращении с уже готовым продуктом.

Несмотря на этот факт, в приложении для безопасности необходимо реализовать разграничение прав доступа. В этом случае пользователям присваиваются заранее созданные роли, каждая с собственным набором прав. Стоит учитывать необходимость такого шага для предотвращения нежелательных

последствий в случае, если некомпетентный пользователь решит воспользоваться функционалом программы, который способен при неправильном использовании нанести вред системе. Для определения прав необходимо войти под своей учетной записью через ввод логина и пароля. Учетная запись администратора существует изначально и обладает полными правами, позволяя использовать весь реализованный функционал программы. Также должна присутствовать гостевая учетная запись. Гость обычно максимально ограничен в правах, имея в своем распоряжении только функционал, не предусматривающий каких-либо серьезных изменений в системе.

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.

Созданные роли должны иметь права, соответствующие предполагаемым потребностям в функционале и положениям о безопасности. Таким образом, должна присутствовать роль «Пользователь» (гостевая учетная запись), имеющая минимальный уровень прав доступа с возможностью использования сканера точек доступа, монитора беспроводной полосы пропускания и возможность сохранять данные по нажатию кнопки для истории. Роль «Сотрудник» должна иметь расширенные права, включая права предыдущего уровня. В частности, возможность не только использовать монитор беспроводной полосы пропускания с сохранением информации, но и иметь доступ в раздел истории и удалять данные истории. Кроме того, для этой роли должен предоставляться доступ к данным о пользователях (без отображения логинов и паролей пользователей) с целью получения контактов по типу номера телефона

или email, но с заблокированной функцией редактирования существующих пользователей и создания новых. Роль «Администратор» должна иметь полный набор прав, включая предыдущие уровни, а также возможность использования анализатора сетевого трафика и сохранения полученных данных, менеджера профилей точек доступа.

Интерфейс конечной программы необходимо тщательно проработать. Прежде всего, он должен создавать условия для удобного взаимодействия, таким образом обеспечивая пользователям наилучший опыт использования. Для этих целей подходит концепция интуитивно-понятного интерфейса. Существует ряд характеристик, определяющих удачный и грамотно созданный интерфейс [23]:

− общедоступность использования. Для любого пользователя не должно быть проблемой взаимодействие с программным продуктом, в ином случае он откажется от его использования. Интерфейс приложения должен быть понятен на уровне интуиции;

− минимализм. Перегруженность интерфейса оконными формами и элементами создает лишь путаницу. В конечном счете это приводит к огромным затратам по времени для пользователя просто чтобы разобраться в функционале программы. В связи с этим рекомендуется создавать элементы понятными, но с минимальной загруженностью;

− ориентированность на обычного пользователя. Интуитивного понимания интерфейса пользователем недостаточно. Стоит учитывать, что понятные самому разработчику вещи и понятия могут стать препятствием для свободного использования приложения обычным пользователем;

− «Легкость». Загруженность интерфейса формами и элементами также ведет к снижению быстродействия и, как следствие, ухудшению пользовательского опыта. Взаимодействовать с программным интерфейсом без задержек проще для любого пользователя;

− контекстное соответствие. Элементы интерфейса правильно создавать с соответствием функционалу с целью удобной и понятной работы с ними.

Несоответствие контента и элементов управления вводит пользователя в заблуждение;

− привлекательность. С точки зрения дизайна правильно подбирать такой внешний вид и цветовую схему приложения, чтобы зрительный контакт с интерфейсом не доставлял дискомфорт конечному пользователю. Элементы по габаритам следует создавать, основываясь на их функционале, а цветовую схему подбирать без ярких и высоко контрастных цветов.

Подводя итог всему вышеизложенному можно сделать вывод, что разрабатываемый продукт подойдет для любой организации, использующей сеть на основе технологии Wi-Fi и будет актуален ближайшее время, учитывая тенденции перехода все большего количества компаний на беспроводные сети.

2.4.2 Описание программных модулей

Программное обеспечение представляет собой совокупность взаимодействующих друг с другом модулей, которые составляют функционал конечного продукта. Каждый модуль предназначен для выполнения определенных процессов и должен быть тщательно проработан, протестирован и лишен ошибок в программном коде, а также в выполнении своих функций.

Спроектированное приложение будет включать в себя следующие модули (рисунок 19):

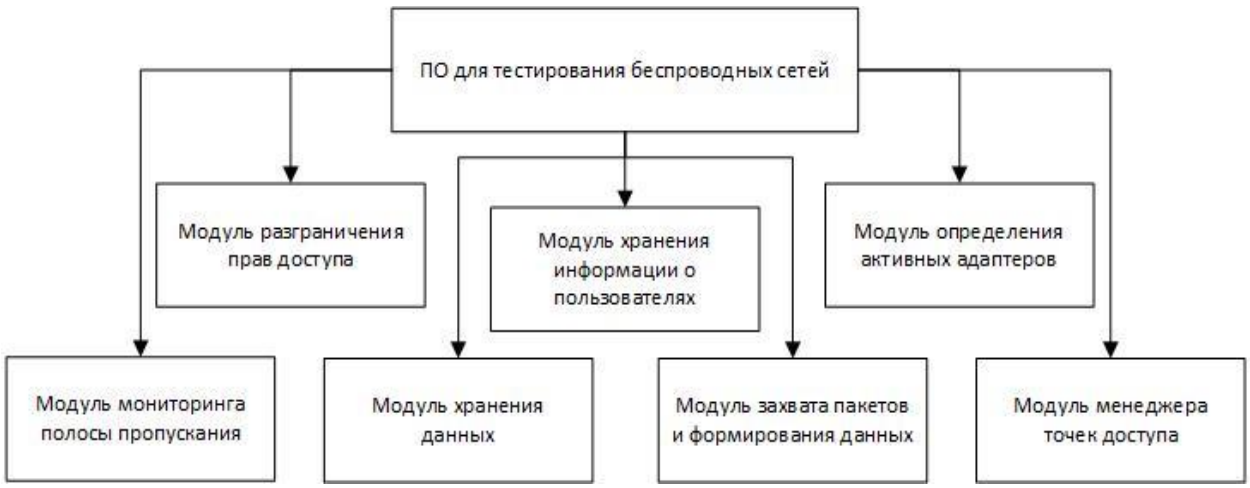

Рисунок 19 – Модули программного продукта

− модуль разграничения прав доступа. Производит анализ данных пользователей, занесенных в БД, определяя по специальному полю «role» роль, выбранную администратором при создании пользователя («Пользователь», «Сотрудник» или «Администратор»). В коде осуществляется проверка и, на основании записи в поле «role», модуль выдает права учетной записи, ограничивая функционал или предоставляя полный доступ в случае с администратором. Осуществляет авторизацию пользователей. Входными данными являются логин и пароль, а выходными – присвоенная роль и права доступа;

− модуль хранения информации о пользователях. Осуществляет сохранение данных пользователей в БД, включая логины и пароли, присвоенную роль, а также дополнительную информацию в виде контактных данных. Запись данных реализуется через SQL запросы в коде. Входными данными являются роль пользователя из модуля разграничения прав, логин и пароль, дополнительные данные, а выходными – сформированная таблица в БД;

− модуль определения активных адаптеров. Определяет установленные в системе сетевые адаптеры для соединения с беспроводной сетью и формирует из них список. Для получения сетевых адаптеров, используемых в системе, используются LINQ запросы в коде. Формируется список из созданного массива. Входными данными является информация об определенных системой адаптерах, а выходными – список активных адаптеров;

− модуль мониторинга полосы пропускания. Анализирует полосу пропускания для выбранного сетевого адаптера и предоставляет вывод информации в реальном времени (IP-адрес, скорость передачи данных, используемый стандарт связи и т.д.). С помощью библиотек .NET получает доступ к сетевому адаптеру через определенный метод, а LINQ позволяет отбирать только адаптеры беспроводной сети для отображения. Входными данными является сформированный модулем определения активных адаптеров список беспроводных адаптеров, а выходными – информация, получаемая от адаптера в реальном времени;

− модуль хранения данных. Служит связующим звеном между программой и БД. Предназначен для сбора и сохранения информации из монитора полосы пропускания в БД. Запись данных реализуется через SQL запросы в коде. Входными данными является информация, полученная модулем анализа полосы пропускания, а выходными – сформированная таблица в БД;

− модуль захвата пакетов и формирования данных. Производит захват пакетов и формирует информацию в удобном для пользователя виде. С помощью специального метода в коде происходит привязка к ip адресу и происходит перехват пакетов с последующим построением дерева для отображения. Входными данными являются список адаптеров из модуля определения активных адаптеров, а выходными – выводимые данные в виде дерева;

− модуль менеджера профилей точек доступа. Осуществляет возможность управления профилями точек доступа, к которым ранее производилось подключение, в формате xml. Используя обращение к системной утилите Netsh, программа позволяет манипулировать профилями точек доступа. В число действий входит экспорт профилей по выбору или сразу всех имеющихся, импорт сохраненных профилей для внедрения в систему с целью подключения к точке доступа без ввода пароля, удаление сохраненных профилей. Входными данными являются информация о точке доступа из профиля в системе, а выходными – профили точек доступа в формате xml.

Взаимодействие пользователя с модулем менеджера профилей точек доступа можно представить в виде UML-диаграммы последовательности (рисунок 20).

Блок «Поиск точек доступа» сперва получает от модуля авторизации права текущего пользователя и на их основании разрешает или запрещает доступ к управлению подключением и менеджеру точки доступа. Используя блок, пользователь получает выводящийся в виде таблицы список активных точек доступа и, если уровень прав это подразумевает, то подключается к выбранной точке доступа. Также в любой момент он может отключиться от нее. Для точки доступа появляется возможность использовать менеджер, в котором

пользователь может получить информацию о выбранной точке. В дополнение, пользователь имеет возможность выполнить импорт/экспорт профиля точки доступа.

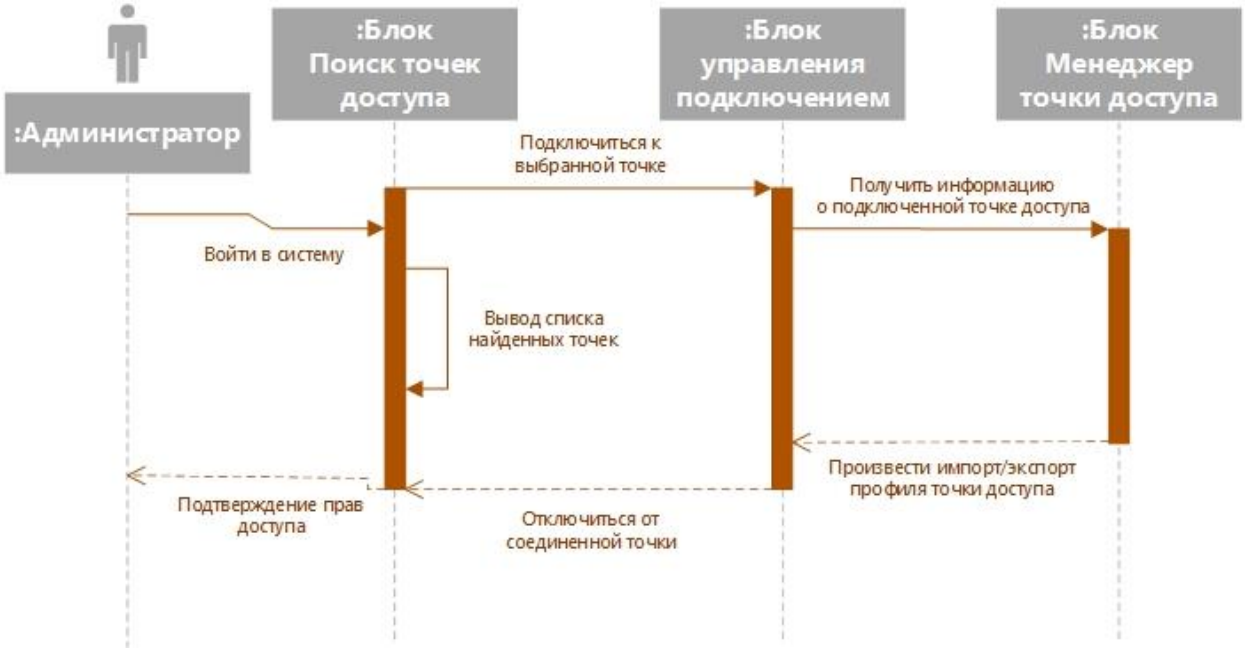

Рисунок 20 – Диаграмма последовательности

С помощью UML-диаграммы состояний можно отразить как объект (точка доступа) переходит из одного состояния в другое в процессе использования программного продукта пользователем (рисунок 21).

Точка доступа выступает как объект. Сперва происходит обнаружение точки доступа, основная информация выводится для пользователя в таблицу по колонкам. При достаточном уровне прав пользователь имеет возможность управлять подключением к выбранной точке доступа или отключением от нее. Если подключение не произведено, точка доступа находится в общем списке обнаруженных, ожидая дальнейших действий пользователя. В этом состоянии перехода в другое состояние не происходит до вмешательства пользователя. При подключении открывается доступ к менеджеру точки доступа, в котором можно произвести экспорт профиля подключенной точки доступа или импорт имеющегося профиля. При экспорте локально создается файл со служебной информацией, который можно использовать в дальнейшем. Импорт профиля означает, что вся информация с параметрами точки доступа будет перенесена

на данное устройство, что позволит подключиться к ней сразу без ввода пароля и настройки. Таким образом, точка доступа проходит несколько состояний на протяжении сеанса использования программы.

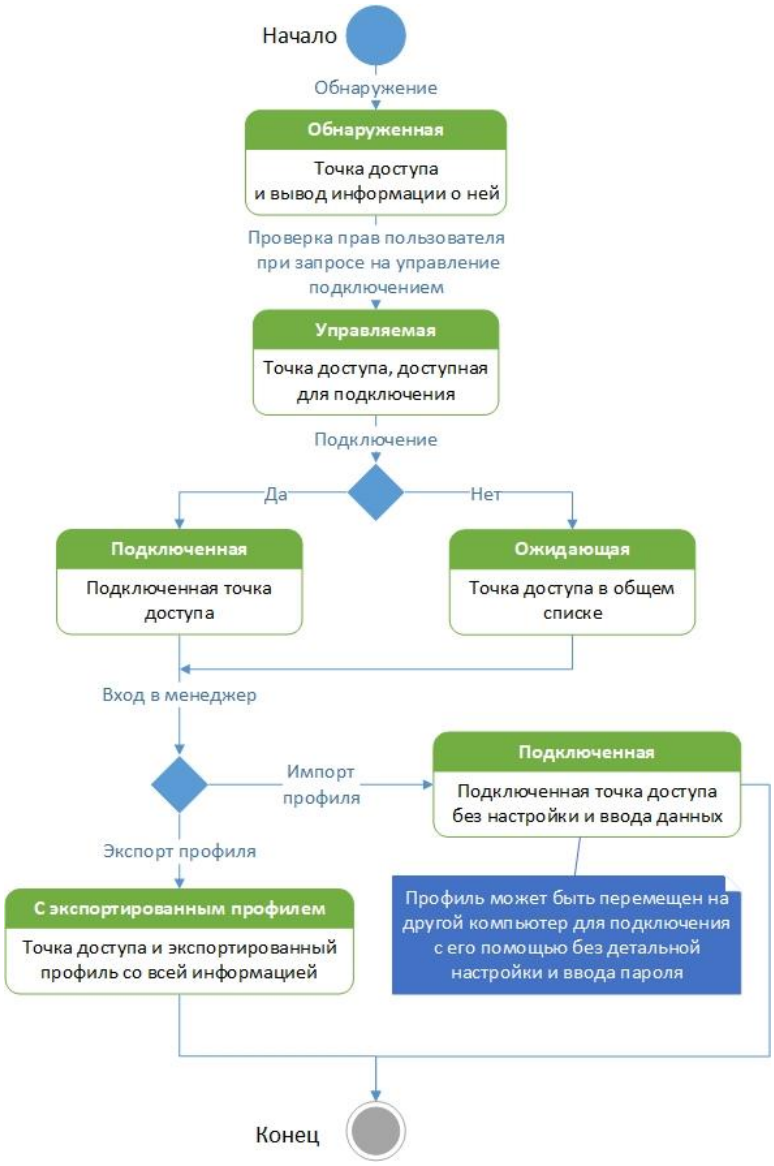

Рисунок 21 – Диаграмма состояний

UML-диаграмма активностей отражает динамические аспекты поведения системы. На ней наглядно отражается, как поток управления переходит от одной деятельности к другой (рисунок 22).

Пока происходит построение списка активных обнаруженных точек проверяется уровень доступа пользователя, запрещая ему или позволяя использовать элементы управления подключением, а также менеджер точки

доступа. Формируется таблица с информацией по точкам доступа, в это же время пользователь уже может подключиться к выбранной точке доступа.

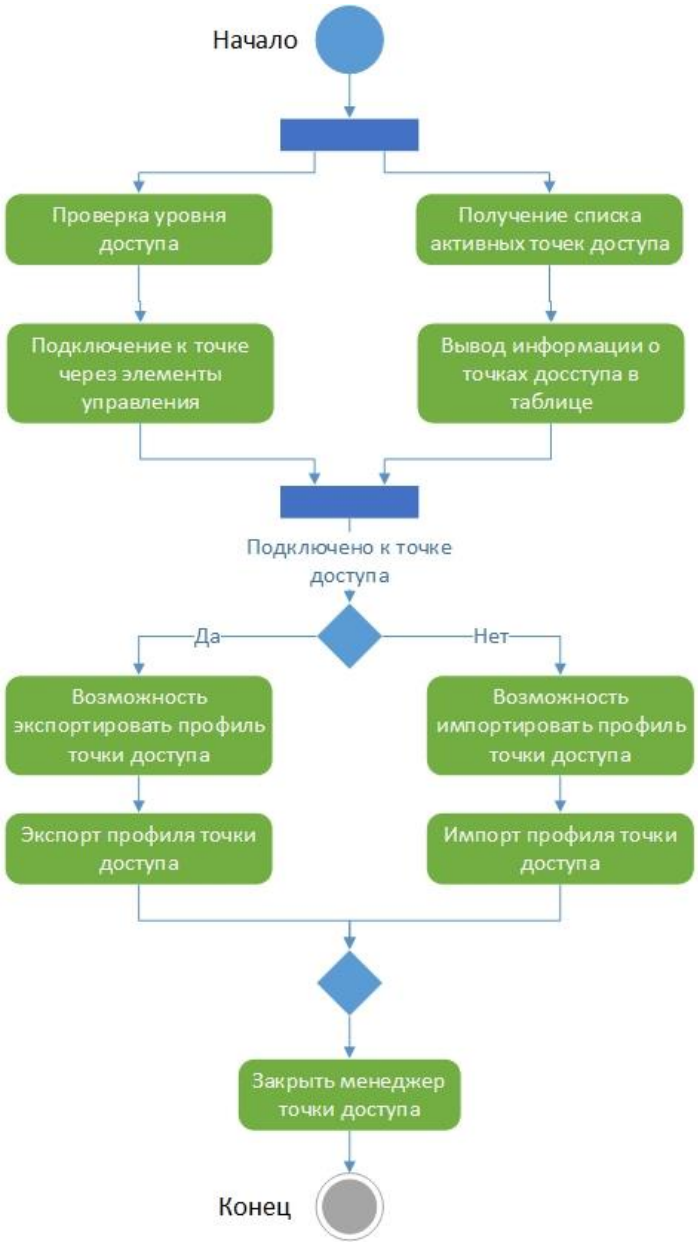

Рисунок 22 – Диаграмма деятельности

Таким образом, эти действия выполняются параллельно. Далее следует проверка, произведено ли подключение к какой-либо точке доступа. В случае подключения у пользователя имеется возможность экспортировать профиль точки доступа, с которой соединен компьютер. Иначе пользователь может использовать раннее полученный профиль точки доступа и подключиться к ней

с его помощью, если она находится в зоне покрытия сигнала адаптера беспроводной сети. После этого менеджер точки доступа закрывается.

UML-диаграмма классов применяеется при проектировании и описании существующих и используемых систем, таким образом, она служит отличным вспомогательным инструментом (рисунок 23).

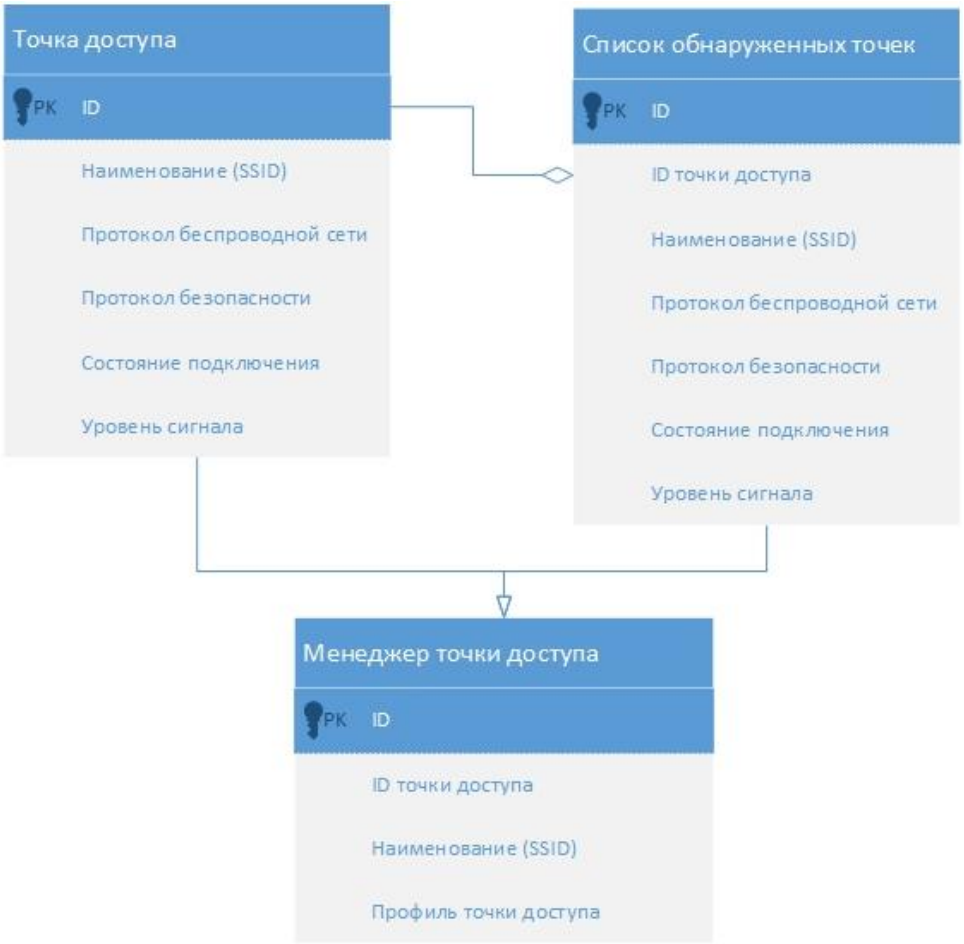

Рисунок 23 – Диаграмма классов

Сущность «Точка доступа» содержит в себе атрибуты, отражающие ее параметры: ID по номеру обнаружения, Наименование точки доступа (SSID), Протокол беспроводной сети, Протокол безопасности, Состояние подключения. Уровень сигнала (в %). На основании объектов этой сущности строится список из обнаруженных точек доступа. Сущность «Список обнаруженных точек доступа» соединена связью «агрегация» с сущностью «Точка доступа», т.к. список состоит из обнаруженных точек доступа. В сущность передаются все атрибуты точки доступа, в том числе и ключевой атрибут «ID», который

записывается в новую сущность как «ID точки доступа». Все атрибуты передаются по причине вывода информации в таблице для пользователя. Сущность «Менеджер точки доступа» соединен с двумя предыдущими сущностями связью «наследование», она использует атрибут «ID точки доступа», «Наименование (SSIS)» и «Профиль точки доступа».

UML-диаграмма компонентов отражает разбиение модуля на структурные компоненты и связи (зависимости) между ними. В качестве физических компонентов могут выступать файлы, библиотеки, модули, исполняемые файлы, пакеты и т. п. (рисунок 24).

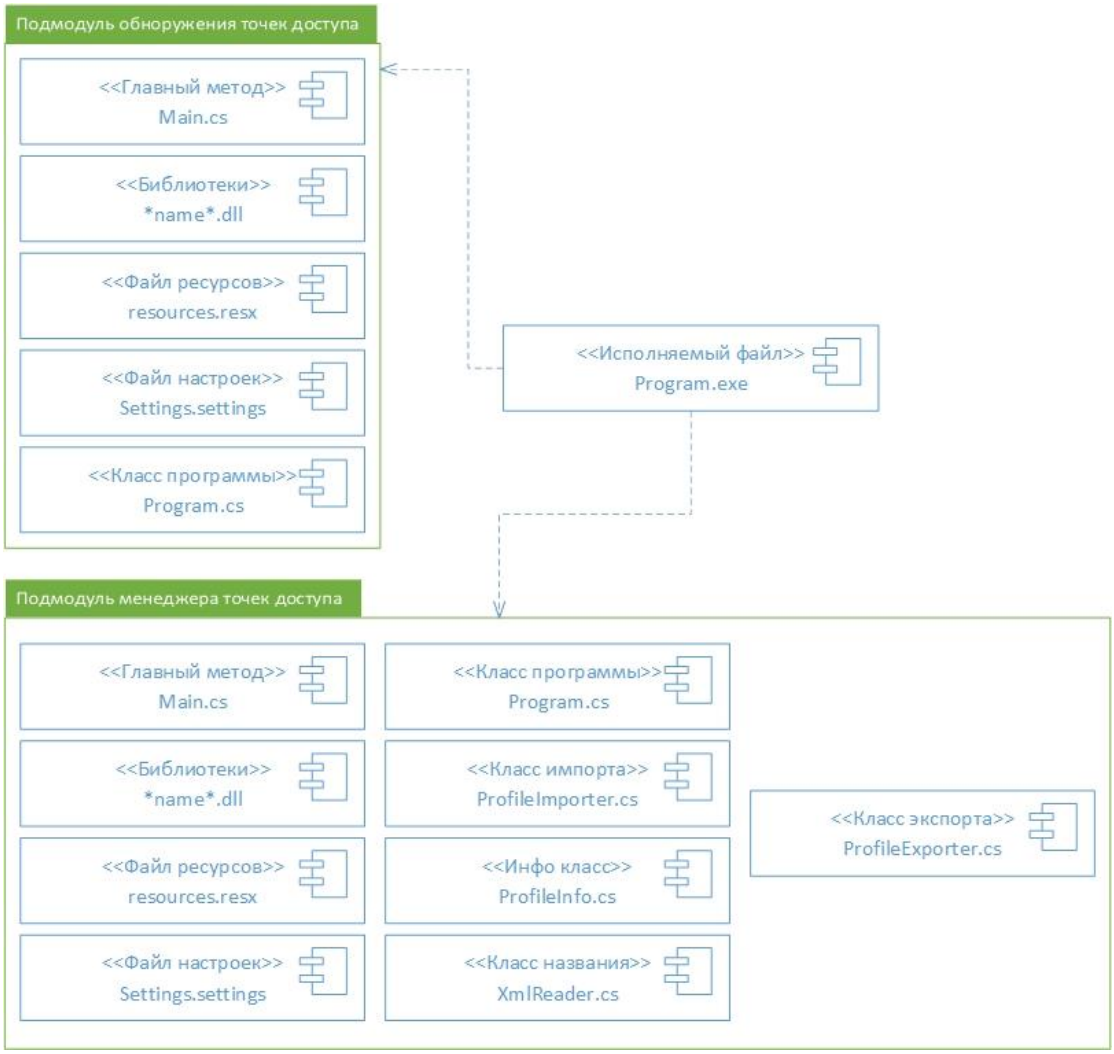

Рисунок 24 – Диаграмма компонентов

Подмодуль обнаружения точек доступа включает в себя компоненты:

– главный метод Main.cs. Главный метод программы, ее входная точка, является частью класса Program;

– библиотеки dll. Динамические библиотеки, многократно используемые приложением. Функции библиотеки могут использоваться процессами;

– файл ресурсов resources.resx. Ресурсы, такие как строки, изображения или данные объектов, можно включать в файлы ресурсов, чтобы сделать их легко доступными для приложения;

– файл настроек Settings.settings. Сохраняет настройки на диске. Осуществляет запись параметров на диск при выходе из программы и последующее их чтение при повторном запуске программы;

– класс программы Program.cs. Главная входная точка программы.

Подмодуль менеджера точек доступа также содержит вышеперечисленные компоненты, но вместе с тем использует дополнительные классы для осуществления функционала: ProfileImporter.cs и ProfileExporter.cs содержат функционал для импорта и экспорта профиля точки доступа соответственно, ProfileInfo.cs используется для получения информации о доступных профилях, XmlReader.cs возвращает наименование профиля в xml-файл конфигурации.

Компоненты подмодулей связываются через зависимости с помощью исполняемого exe-файла Program.exe.

Суммируя и подводя итог всего вышеизложенного контекстную модель программы возможно представить с помощью диаграммы IDEF0 (рисунок 25).

Рисунок 25 – Контекстная модель программы

Схему разграничения прав можно представить в виде UML-диаграммы прецедентов, на которой изображены роли пользователей программы и их возможности (рисунок 26).

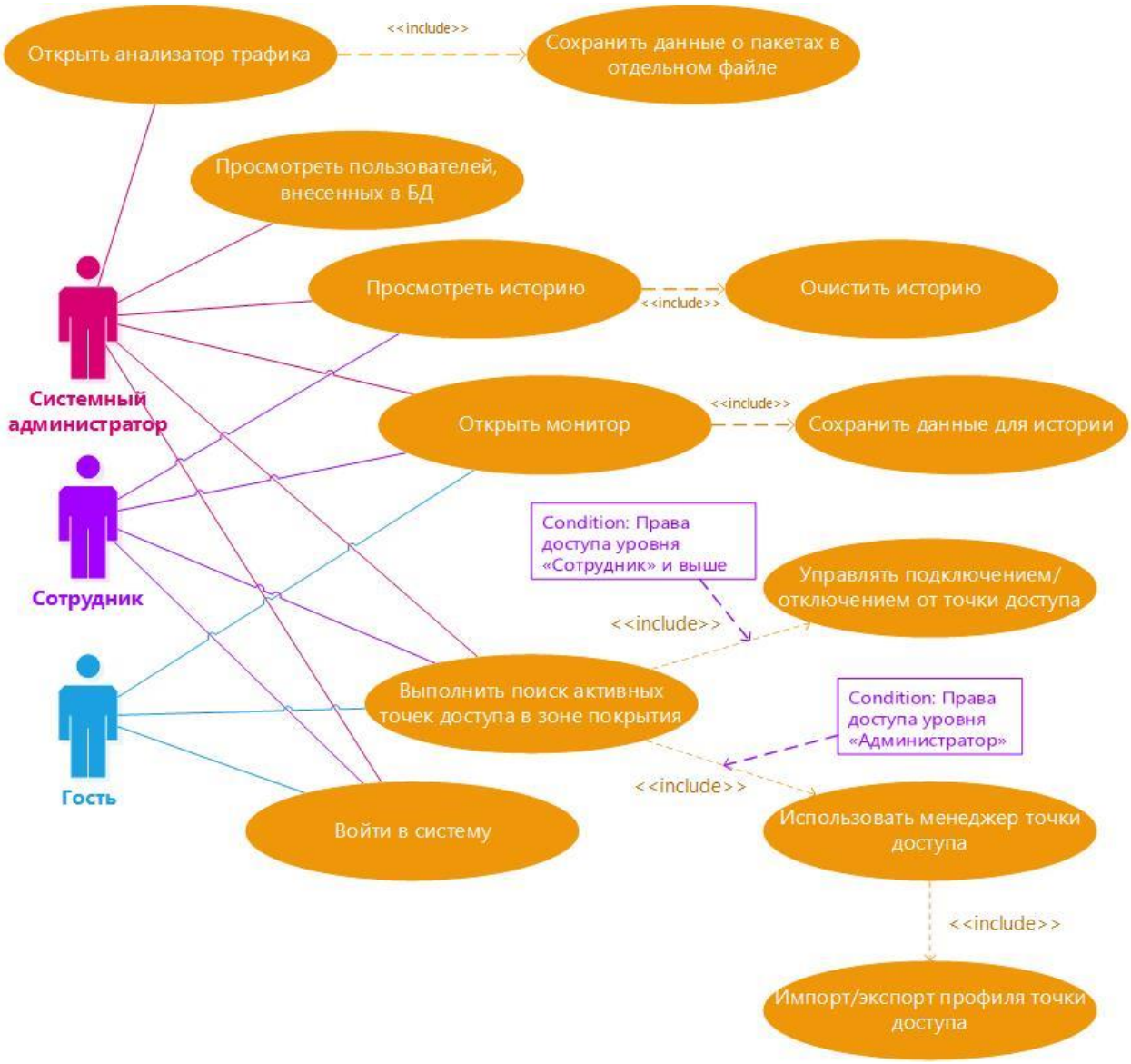

Рисунок 26 – Диаграмма прецедентов

С системой могут взаимодействовать три действующих лица, которые разграничены по правам доступа к функционалу системы – Системный администратор, Сотрудник и Гость.

Поиск активных точек доступа – базовый функционал разрабатываемого модуля. После входа в систему каждое из действующих лиц имеет доступ на поиск активных точек доступа. Через модуль осуществляется управление подключением к найденным активным точкам доступа, что недоступно Гостю с

целью безопасности работы системы. По тем же соображениям менеджер точки доступа и анализатор трафика, с помощью которого производится импорт и экспорт профиля точки доступа, неактивен для всех, кроме Системного администратора.

Таким образом, дополнительный функционал включается в модуль поиска активных точек доступа, что позволяет более детально проработать сценарии использования.

2.4.3 Прототип пользовательского интерфейса

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 рисунках 27 и 28 представлен прототип пользовательского интерфейса программы.

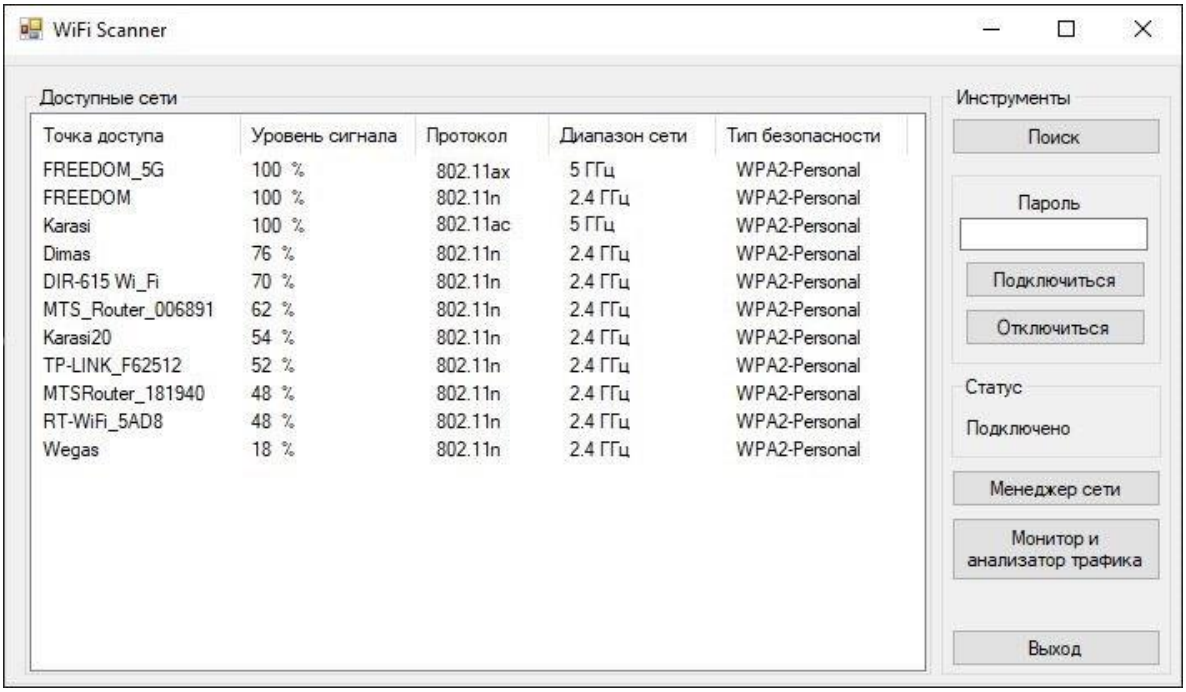

Рисунок 27 – Прототип главной формы

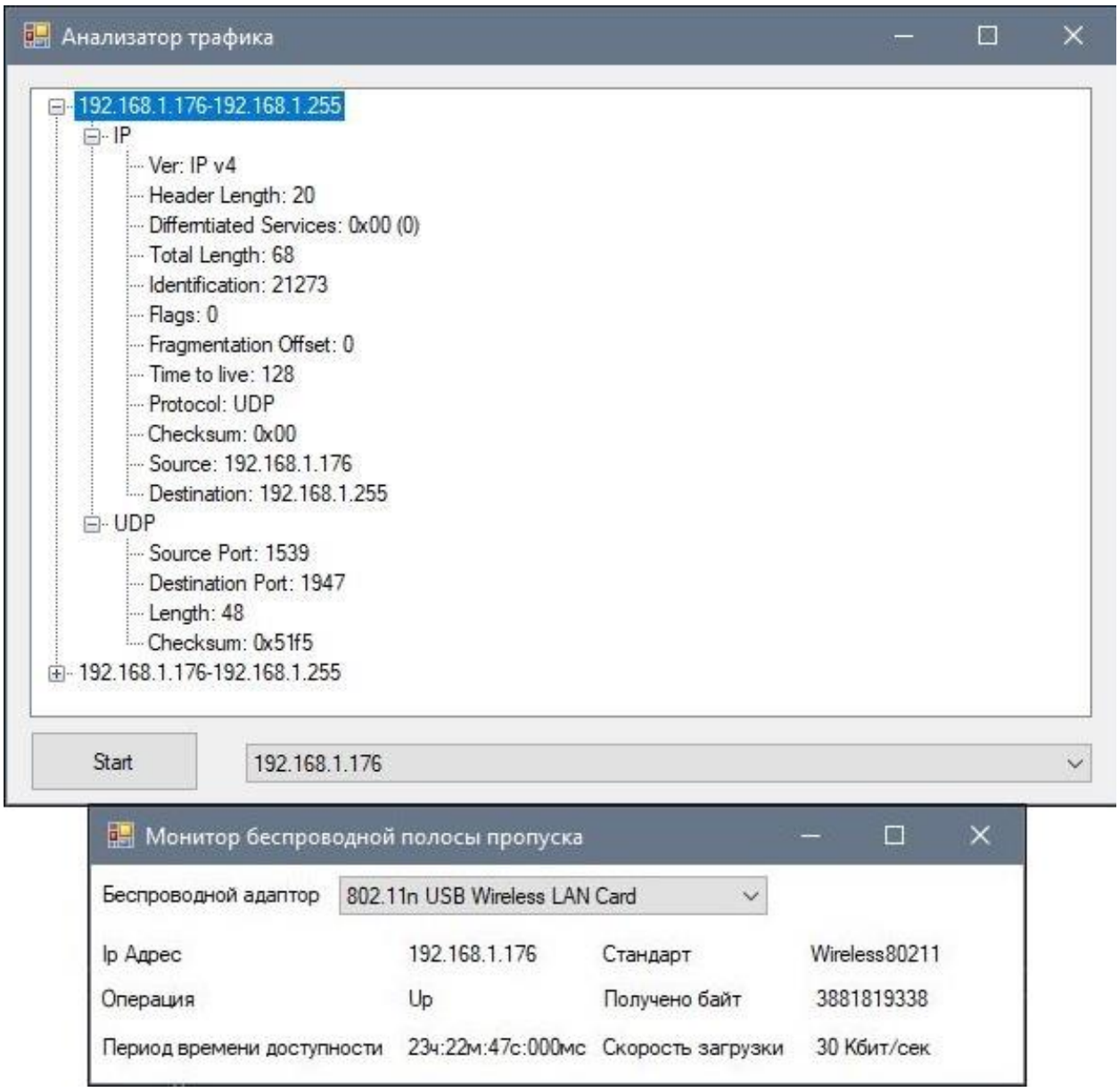

Рисунок 28 – Прототип формы монитора и анализатора трафика

2.4.4 Обоснование выбора модели жизненного цикла

Жизненный цикл ИС можно представить как ряд событий, происходящих в процессе создания и использования программного продукта.

Модель жизненного цикла отражает различные состояния, начиная с момента возникновения необходимости в данной программе и заканчивая моментом ее полного выхода из употребления.

В настоящее время известны и используются три модели жизненного цикла, каждая из которых обладает своими особенностями (рисунок 29).

Рисунок 29 – Модели жизненного цикла

Поэтапная модель с промежуточным контролем – модель, аналогичная каскадной, но отличающаяся от нее наличием промежуточных точек контроля. Она является более гибкой, так как предполагает возможность возвращения к предыдущим этапам для внесения определенных изменений. Это увеличивает время разработки при каждом возврате назад и внесении изменений, однако существенно снижаются риски получения некачественного продукта на выходе и растет надежность системы в целом. Однако, слишком часто встречаются ситуации, когда программный продукт прекращает свое существование еще на стадии проекта, причиной чему становится низкий уровень технологий анализа и проектирования систем, так как методы управления проектами внедрения часто не соответствуют сложности самих проектов.

Для нивелирования рисков, связанных с вышеописанной проблемой, была предложена спиральная (итерационная) модель, позволяющая на протяжении цикла создания системы сформировать несколько прототипов, проверяемых на соответствие требованиям заказчика и рынка. Несколько раундов доработок интерфейса, функциональности и других элементов системы позволяют создать продукт и протестировать его работоспособность, а также снизить риск получения несоответствующего ожиданиям продукта. При необходимости, возможно начать работу с первыми релизами, в дальнейшем внося новые изменения (однако сроки для различных версий могут составлять от

нескольких недель до целых месяцев или даже лет). В то же время возрастает степень неопределенности для команды подрядчиков, разрабатывающих/внедряющих программный продукт, и в целом планирование ограничений проекта по времени, содержанию и стоимости затрудняется.

Рассмотренные достоинства и недостатки представленных моделей жизненного цикла позволяют подобрать наиболее подходящий вариант. На основании учитываемых сроков и характера разработки в рамках выпускной квалификационной работы можно сделать вывод, что каскадная модель является наиболее приемлемым вариантом. Сроки разработки строго ограничены, а описанные жесткие требования к программному продукту накладывают дополнительные ограничения.

3 РАЗРАБОТКА ПРОГРАММНОГО ПРОДУКТА

3.1 Реализация программного продукта

Программа начинает свою работу сразу после запуска исполняемого exe файла «WiFi.exe». Открывается форма авторизации, на которой необходимо ввести данные пользователя (логин и пароль), внесенного в БД, для доступа к основной форме. Форма входа представлена на рисунке 30.

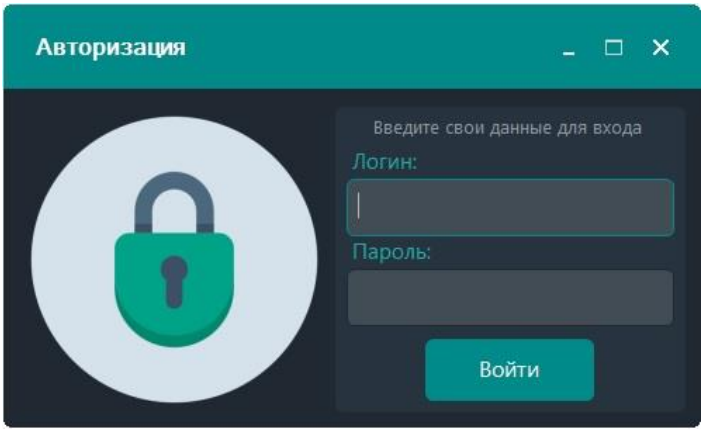

Рисунок 30 – Форма входа

Введя данные учетной записи, пользователь попадает на главную форму программы (рисунок 31).

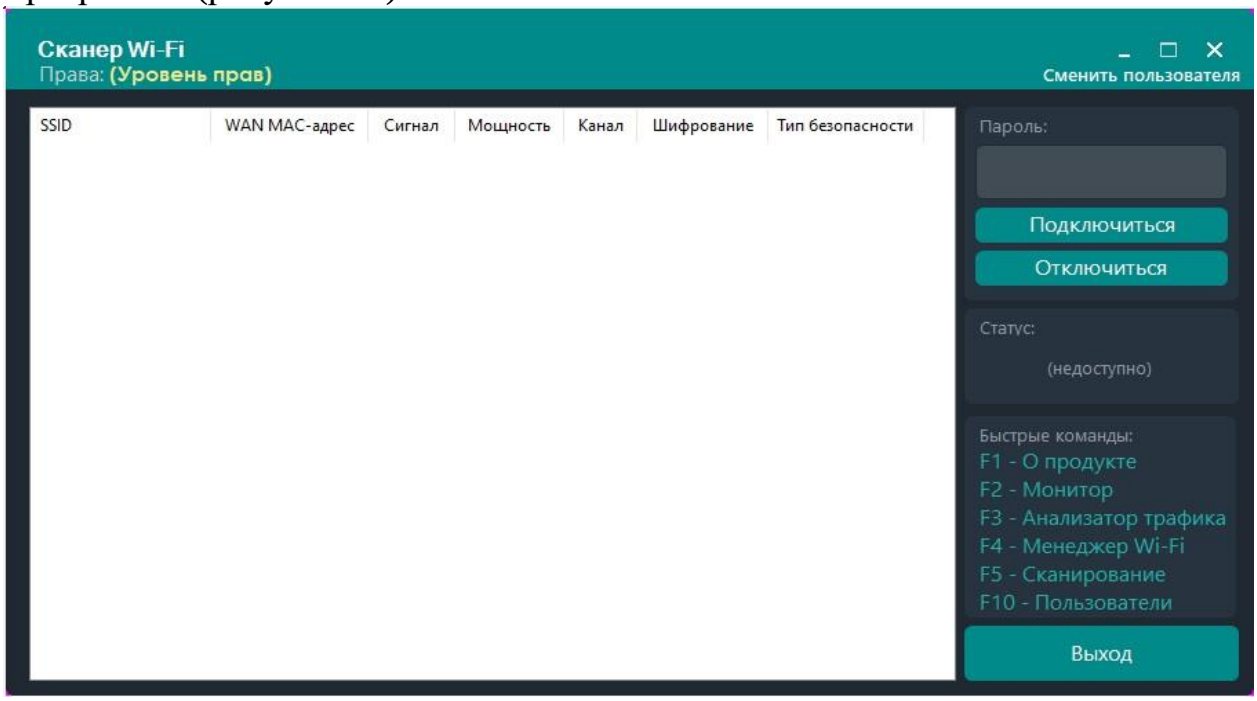

Рисунок 31 – Главная форма

Форма содержит в себе таблицу, в которой выводятся обнаруженные с помощью беспроводного адаптера точки доступа Wi-Fi. Каждая точка доступа имеет свойства, сведенные в таблицу для удобства восприятия информации: наименование точки доступа (SSID), MAC-адрес точки доступа (WAN MAC-адрес), уровень сигнала в процентах (Сигнал), мощность сигнала в децибел милливатт (мощность), используемый канал точкой доступа (Канал), тип шифрования подключения точки доступа (Шифрование), тип безопасности подключения точки доступа (Тип безопасности). Блоки справа предназначены для управления подключения к точке доступа, информирования пользователя о статусе подключения (надпись статуса изменяется в режиме реального времени на основании информации из системы о подключении) и быстрых командах, которые можно использовать для отображения других функциональных форм. В правом нижнем углу находится кнопка выхода из программы, которая прекращает работу приложения. Под заголовком формы расположена надпись, отображающая уровень прав, в зависимости от профиля, используемого для работы с программой. В правом верхнем углу отображается ссылка смены пользователя, нажав на которую произойдет переход обратно к форме входа. Нажатие клавиши F1 вызовет форму «О продукте» (рисунок 32).

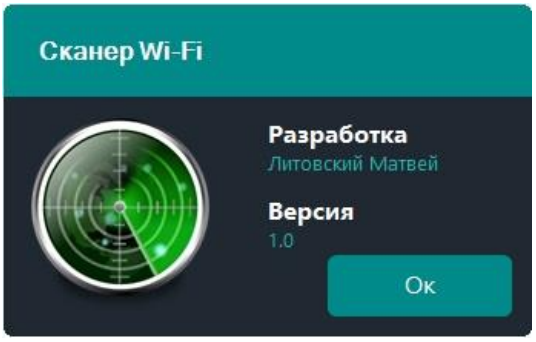

Рисунок 32 – Форма «О продукте»

Клавиша F2 открывает форму «Монитор полосы пропускания». 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. Кнопка история производит переход к форме «История». Форма «Монитор беспроводной полосы пропуска» изображена на рисунке 33.

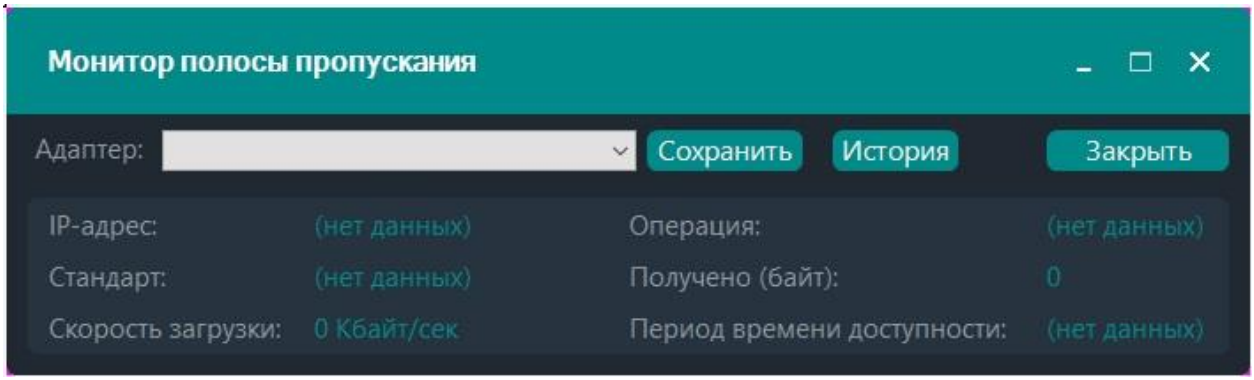

Рисунок 33 – Форма монитора беспроводной полосы пропускания

Кнопка «История» на данной форме осуществляет переход на одноименную форму программы. Здесь расположены три кнопки. «Отобразить данные» выводит данные из БД в поле DataGridView. По нажатию кнопки «Удалить данные из базы» происходит удаление записей таблицы из БД и автоматическое обновление DataGridView на форме. Кнопка «Очистить таблицу» убирает из элемента DataGridView все записи. Форма «История» изображена на рисунке 34.

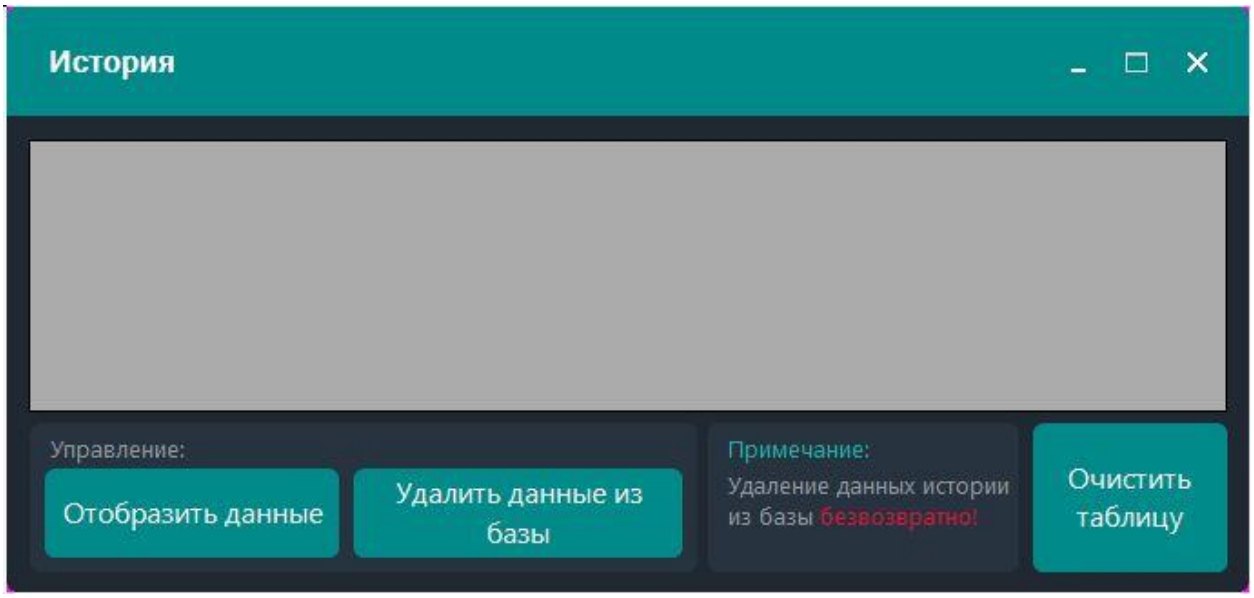

Рисунок 34 – Форма истории с выведенными данными из хранилища

Нажатие кнопки F3 главной формы перенаправляет на соответствующую форму. Важно отметить, что ввиду разграничения прав данная кнопка будет доступна только в том случае, если учетная запись имеет уровень прав Administrator (рисунок 35).

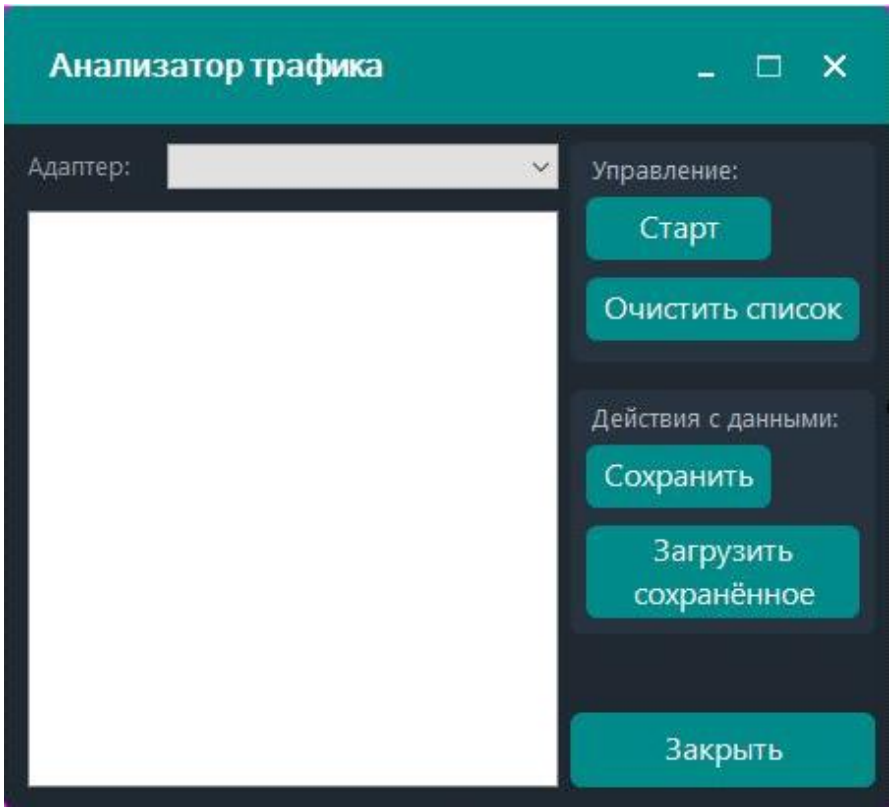

Рисунок 35 – Форма «Анализатор трафика»

Для начала захвата пакетов пользователю предлагается выбрать адаптер в виде IP-адреса из выпадающего списка. После нажатия кнопки «Старт» начнется процесс захвата пакетов с выводом раскрывающегося многоуровневого дерева. Нажатие кнопки «Стоп» завершает процесс. «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 сохранённое». По нажатию этой кнопки дерево сначала очищается, а после заполняется данными из текстового файла. При повторном сохранении файл перезапишется с

новыми данными. Кнопка «Очистить список» очищает поле для последующего заполнения новыми данными. «Закрыть» закрывает текущую форму.

Для перехода к менеджеру сети Wi-Fi используется клавиша F4. Открывается форма «менеджер беспроводных сетей», представленная на рисунке 36.

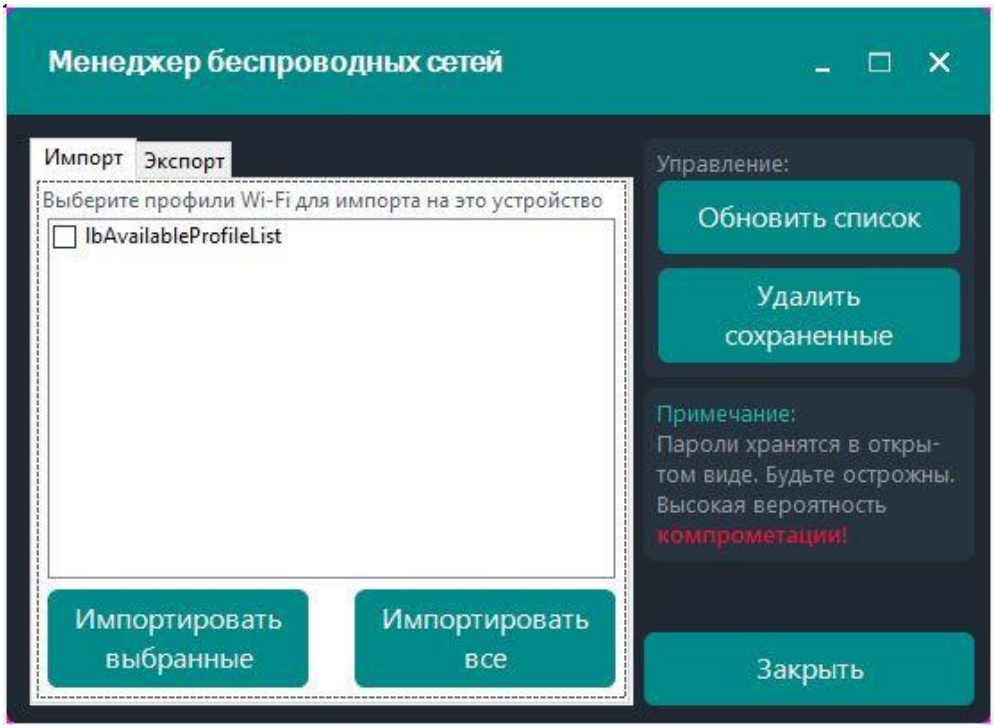

Рисунок 36 – Форма менеджера беспроводных сетей

Кнопка «Обновить список» служит для обновления списка с профилями, «Удалить сохраненные» – для удаления сохраненных конфигураций (профилей сетей), а «Закрыть» – для закрытия формы.

Вкладки «Импорт» и «Экспорт» переключают окна формы, которые используются для импорта и экспорта соответственно. Окно импорта остается пустым пока не имеется ни одной сохраненной конфигурации сети. На окне экспорта появляются беспроводные сети, к которым ранее выполнялось подключение.

Для экспорта можно выбрать одну или несколько позиций и нажать «Экспортировать выбранные», после чего произойдет сохранение профилей в

папку. Либо использовать кнопку «Экспортировать все» для экспорта всех позиций разом.

Экспортированные профили отображаются на вкладке «Импорт», доступные для импорта на другом устройстве при перенесении профиля в папку хранения профилей.

Импорт происходит по схожему алгоритму. Выбираются профили для импорта, либо нажимается кнопка «Импортировать все» для мгновенного импорта имеющихся профилей. Таким образом к точкам доступа с импортированными профилями можно подключаться без ввода пароля.

Нажатие клавиши F10 на главной форме откроет форму «Пользователи». Здесь расположены две кнопки. «Отобразить данные» выводит таблицу в поле элемента DataGridView. Кнопка «Очистить таблицу» убирает из элемента DataGridView все записи (рисунок 37).

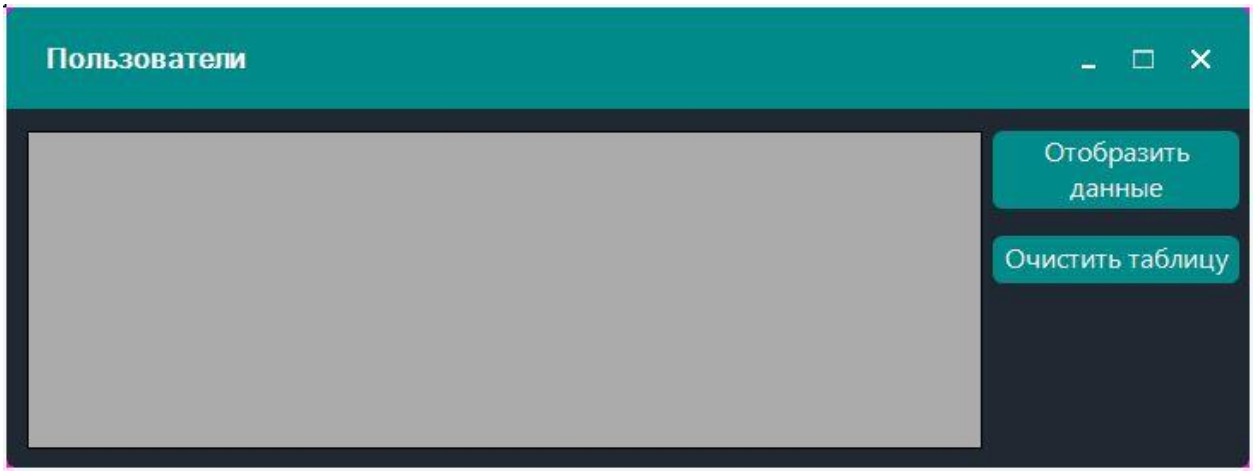

Рисунок 37 – Форма «Пользователи»

Клавиша F5 на главной форме выполняет повторное сканирование и обновление списка точек доступа.

3.2 Взаимодействие с базой данных

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 3).

Таблица 3 – 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» содержит данные, которые пользователи сохраняют в хранилище из монитора полосы пропускания. В этой таблице содержатся наименование адаптера, IP-адрес, период времени доступности, стандарт, количество полученных байт, дата и время (таблица 4).

Таблица 4 – Спецификация атрибутов сущности «monitor»

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

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 (рисунок 38).

```
SqlDataAdapter sda = new SqlDataAdapter("select role from login where username = '" +
TextBoxLogin.MonoFlatTB.Text + "' and password = '" + TextBoxPassword.MonoFlatTB.Text +
"'", conn);
            DataTable dt = new DataTable();
                   sda.Fill(dt);
```

Рисунок 38 – Код, осуществляющий авторизацию

По нажатию кнопки «Пользователи» главной формы открывается форма «Пользователи». На ней расположена кнопка «Отобразить данные», используемая для вывода таблицы «login» в элемент dataGridView. Данная операция реализуется также с помощью SQL запроса (рисунок 39).

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

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

Рисунок 39 – Код для вывода таблицы с данными пользователей

При открытии формы «Монитор беспроводной полосы пропускания» автоматически выполняется LINQ запрос для определения беспроводных адаптеров в системе и формирование списка для элемента comboBoxAdaptors, который является ComboBox`ом (рисунок 40).

Данные сущности «monitor» вносятся не вручную, для этих целей используются SQL запросы. Нажимая кнопку «Сохранить» на форме «Монитор беспроводной полосы пропускания» происходит захват данных в соответствии с запросом в коде (рисунок 41).

```
IEnumerable<NetworkInterface> nics =
NetworkInterface.GetAllNetworkInterfaces().Where(network => network.OperationalStatus ==
OperationalStatus.Up
            && (network.NetworkInterfaceType == NetworkInterfaceType.Ethernet ||
network.NetworkInterfaceType == NetworkInterfaceType.Wireless80211));

            comboBoxAdaptors.DisplayMember = "Description";
            comboBoxAdaptors.ValueMember = "Id";
            foreach (NetworkInterface item in nics)
            {
                comboBoxAdaptors.Items.Add(item);
            }
            if (comboBoxAdaptors.Items.Count > 0)
                        comboBoxAdaptors.SelectedIndex = 0;
```

Рисунок 40 – Код для определения беспроводных адаптеров в системе

```
SqlConnection conn = new SqlConnection(@"Data
Source=(LocalDB)\MSSQLLocalDB;AttachDbFilename=" + Application.StartupPath +
@"\testlogin.mdf;Integrated Security=True;Connect Timeout=30");
            conn.Open();

            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];
```

Рисунок 41 – Код для сохранения данных в БД

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

Форма «Монитор беспроводной полосы пропускания» 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 (рисунок 42).

```
CON.Open();
            DateTime myDateTime = DateTime.Now;
            string sqlFormattedDate = myDateTime.ToString("yyyy-MM-dd HH:mm:ss");
            SqlDataAdapter sda1 = new SqlDataAdapter(" insert into monitor (Адаптер,[ip-
адрес],[Период времени доступности],Стандарт,[Получено байт],[Дата и время]) " +
            "VALUES ('" + comboBoxAdaptors.Text + "' , '" + LinkLabelIP.Text + "' , '" +
LinkLabelValidLifetime.Text + "' , '" + LinkLabelStandart.Text + "' , '" +
LinkLabelRecieved.Text + "', '" + sqlFormattedDate + "') ", CON);
            sda1.SelectCommand.ExecuteNonQuery();
                  CON.Close();
```

Рисунок 42 – Код для вывода таблицы истории

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;
```

Рисунок 43 – Код для очистки таблицы истории

3.3 Результаты фактического тестирования 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 имеющихся понятно любому пользователю, запустившему программу.

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

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

Размер готовой программы составляет 19,2 Мб. Это вполне удовлетворяет требованию малого размера программы (рисунок 44).

Размер:	19,2 МБ (20 188 796 байт)
На диске:	19,4 МБ (20 344 832 байт)

Рисунок 44 – Размер программы

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

Программа протестирована на ОС Windows 10. Весь функционал сохранен, критических ошибок не обнаружено.

Из вышесказанного следует, что все требования были выполнены в готовом продукте и программа готова к использованию в рабочих целях.

3.3.1 Тестирование главной формы

С открытием главной формы в автоматическом режиме производится сканирование с помощью адаптера беспроводной сети. Собранная информация анализируется и обрабатывается программой. На основании обработки строится список из обнаруженных точек доступа с выводом параметров в столбцах. Точки доступа в списке отсортированы по уровню сигнала. Это визуализировано иконками разного цвета. Нажатие F5 выполняет повторное сканирование с очисткой таблицы и повторное ее наполнение (рисунок 45).

Статус «Подключено» сообщает об активном подключении к точке доступа. Нажатие кнопки «Отключиться» производит разрыв соединения и изменение статуса на «Не подключено» (рисунок 46).

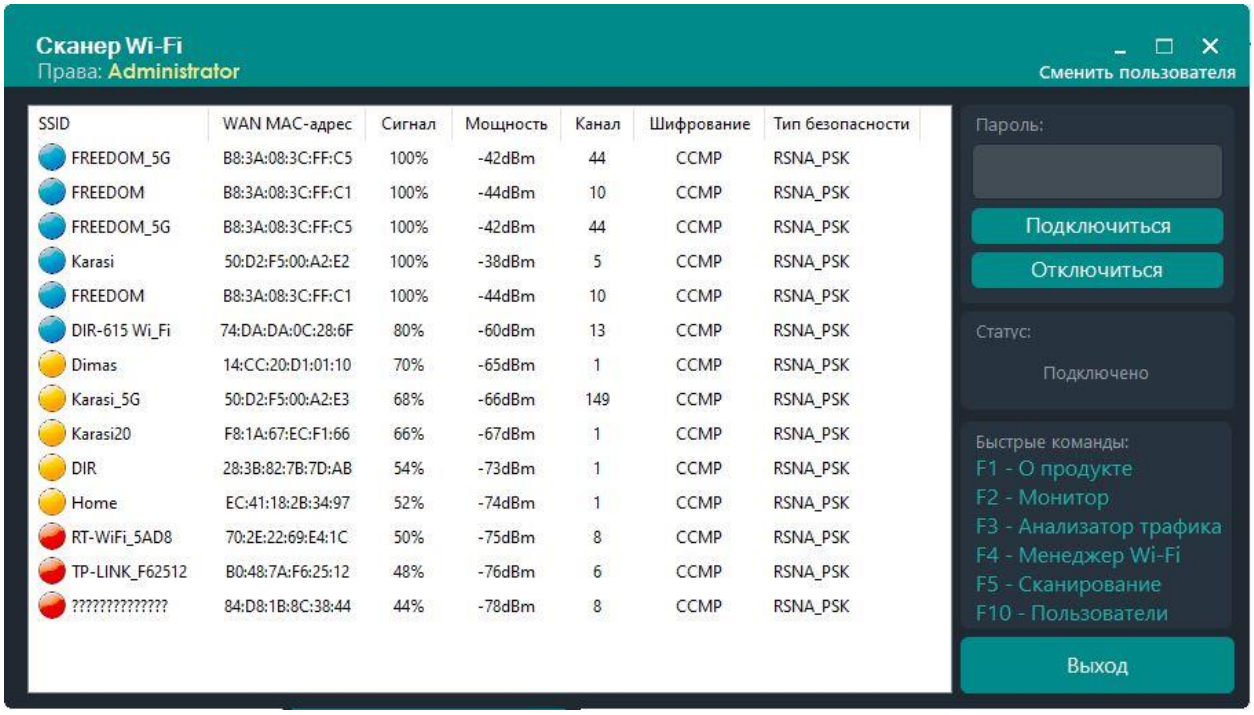

Рисунок 45 – Обнаруженные точки доступа

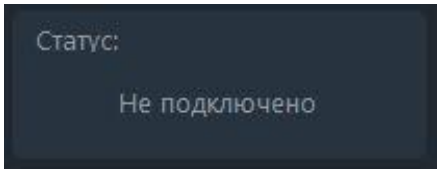

Рисунок 46 – изменение статуса

После выбора точки доступа из списка и ввода пароля нужно нажать кнопку «Подключиться» для подключения к выбранной точке доступа. При этом статус окрашивается в светло-зеленый цвет и меняется на «Подключено», кнопка «Подключиться» блокируется (рисунок 47).

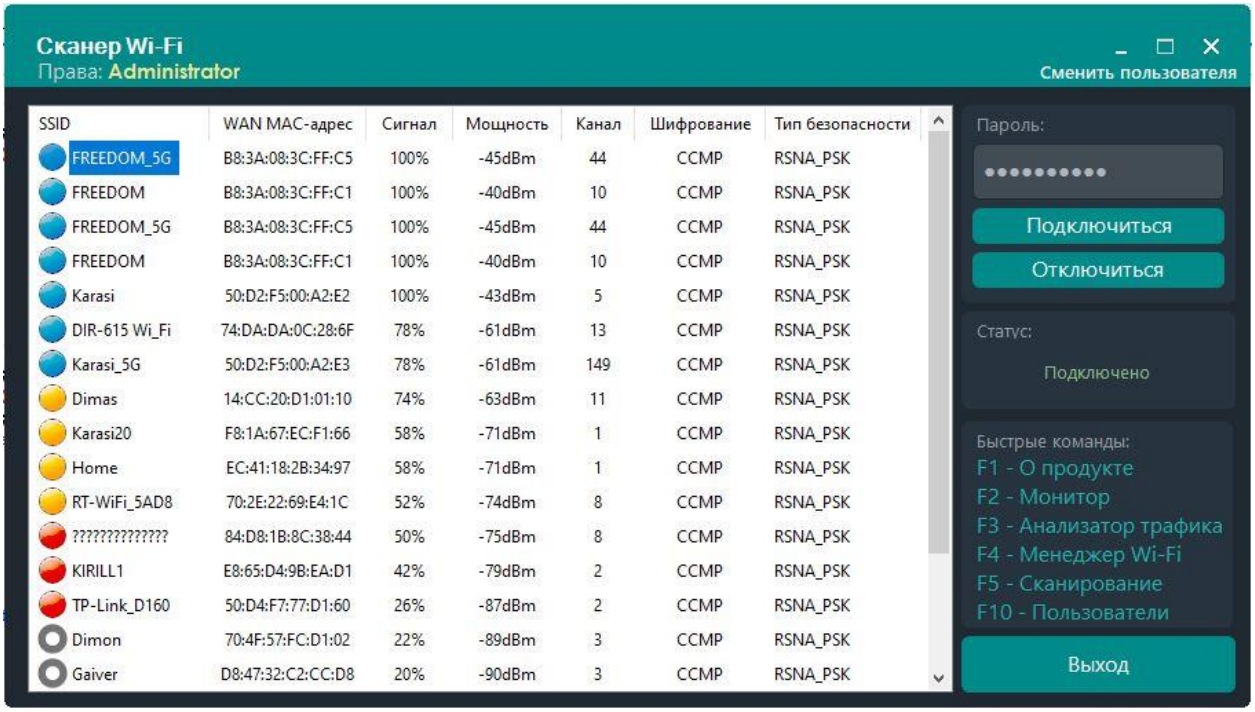

Рисунок 47 – Подключение к точке доступа

При попытке подключения с неверно введенным паролем программа оповестит о сбое, изменив статус на «Сбой подключения!», давая понять пользователю, что подключение не удалось и нужно попробовать снова (рисунок 48).

Главная форма реагирует на нажатие специальных клавиш клавиатуры, что отражено в текстовом блоке в правом нижнем углу формы для информирования пользователя. Клавиша F1 откроет форму «О продукте» (рисунок 49).

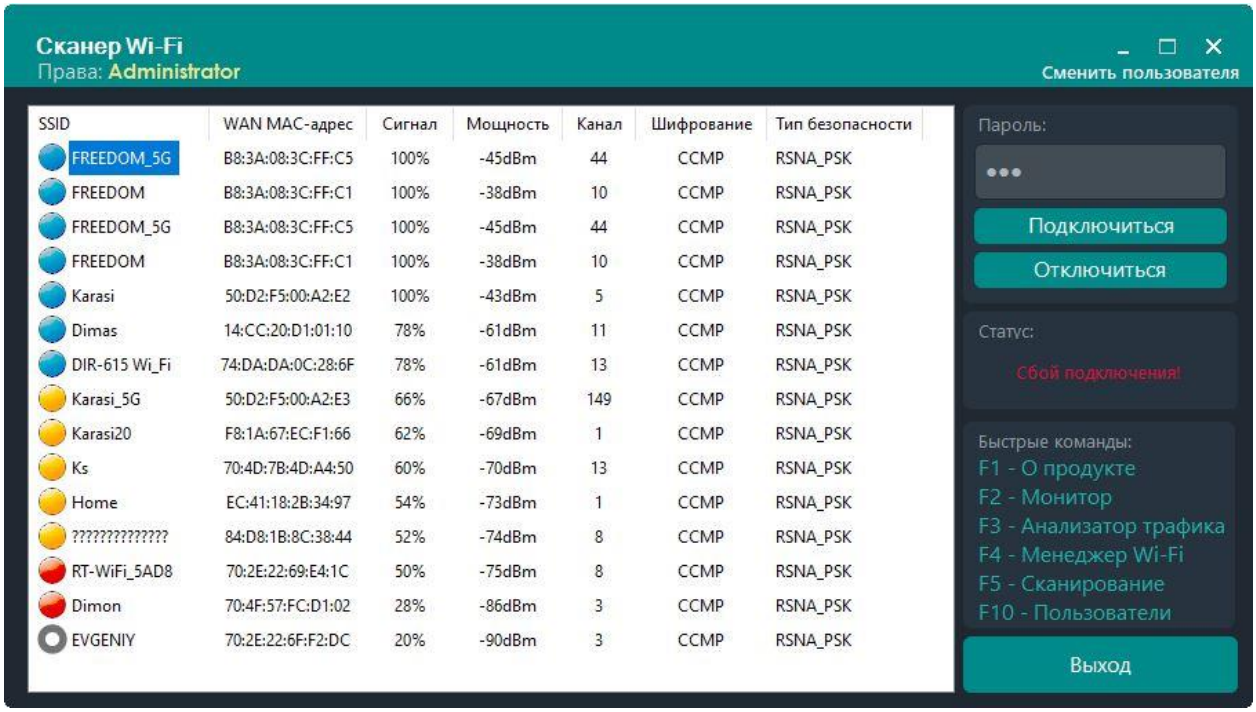

Рисунок 48 – Сбой подключения

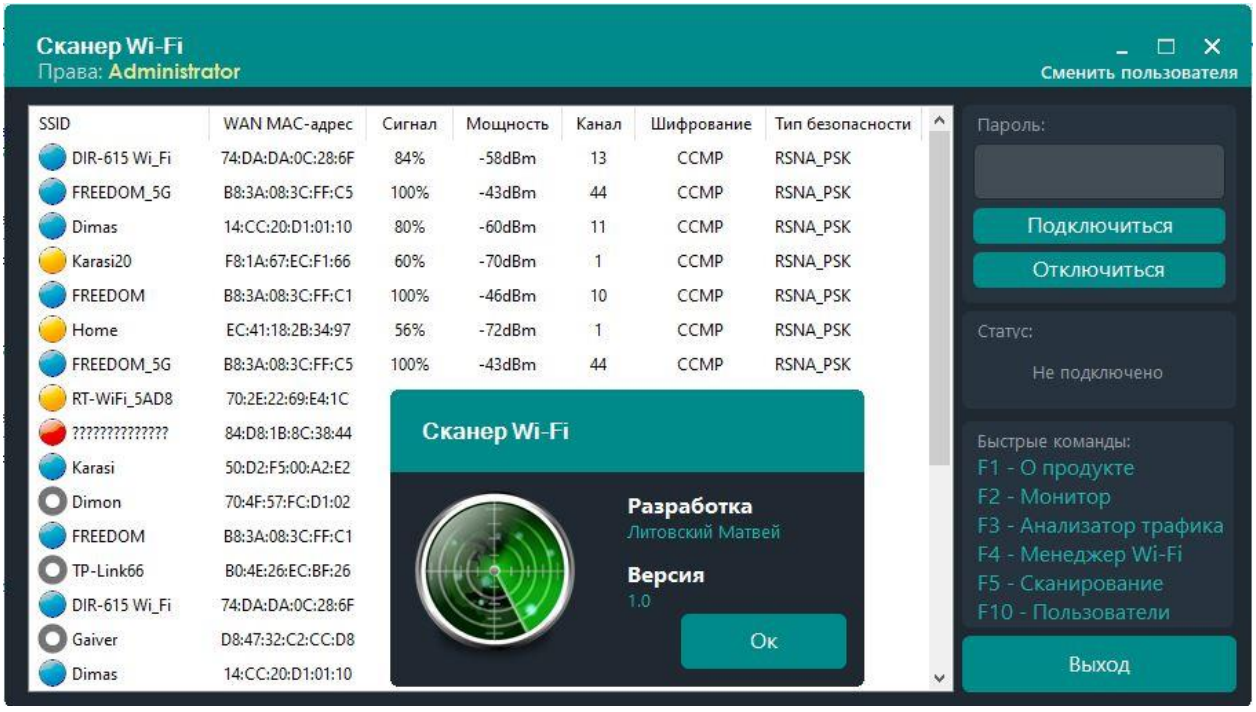

Рисунок 49 – Открытая форма «О продукте»

В зависимости от уровня прав пользователя интерфейс программы меняется, блокируя некоторый функционал. Надпись «Права» отобразит

текущий уровень прав для наглядности. Таким образом, пользователи будут понимать какие действия им доступны, а какие – нет (рисунок 50 и 51).

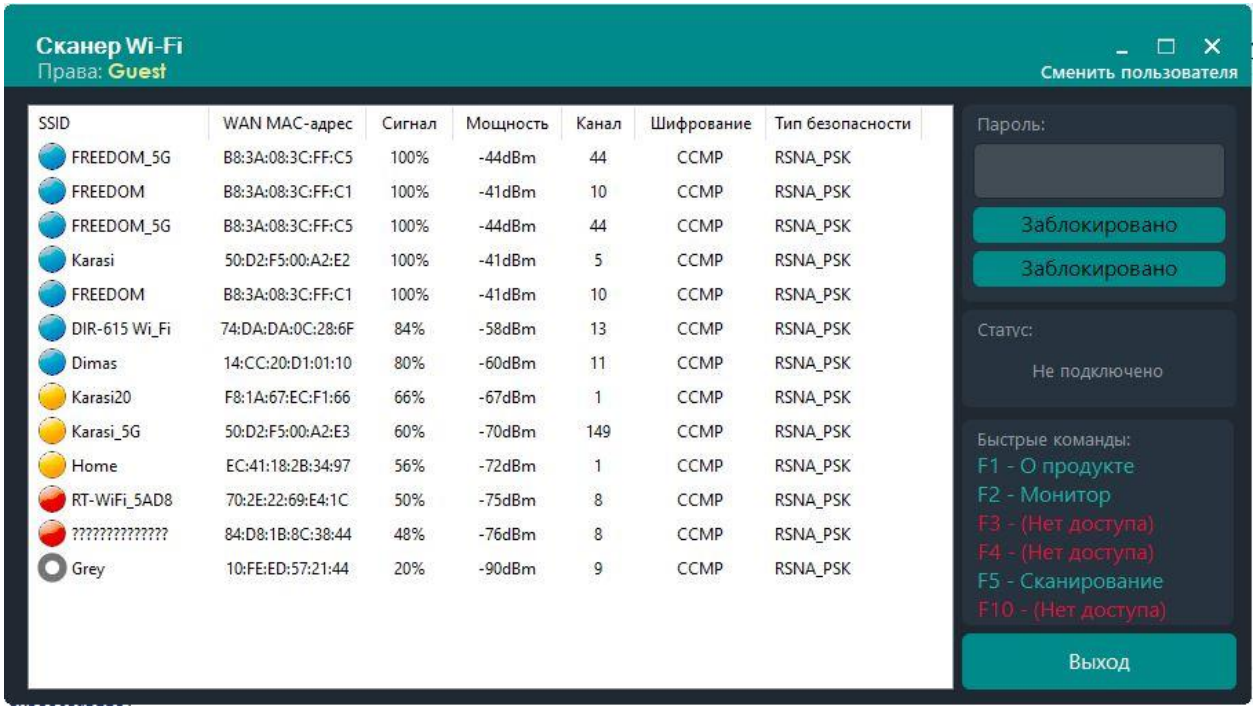

Рисунок 50 – Интерфейс с правами уровня «Сотрудник»

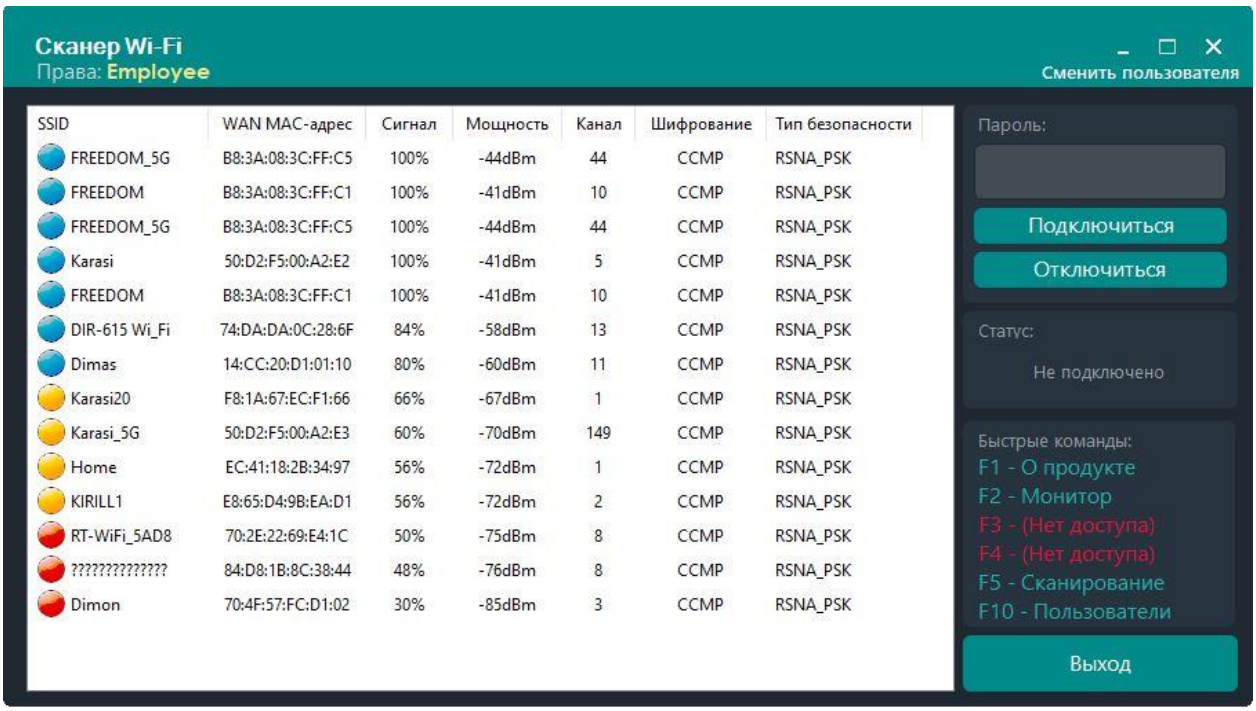

Рисунок 51 – Интерфейс с правами уровня «Гость»

Главная форма самая функциональная. Ее тестированию уделено больше всего времени, так как здесь выше шанс получить сбой или непредвиденное завершение работы программы. По результатам тестовой сессии ошибок выявлено не было.

3.3.2 Тестирование формы «Монитор полосы пропускания»

Форма содержит элемент ComboBox, в который заносятся обнаруженные адаптеры беспроводной сети Wi-Fi. Формируется выпадающий список. При выборе адаптера параметры динамически изменяются. Таким образом, можно определять параметры по выбранному беспроводному адаптеру (рисунок 52).

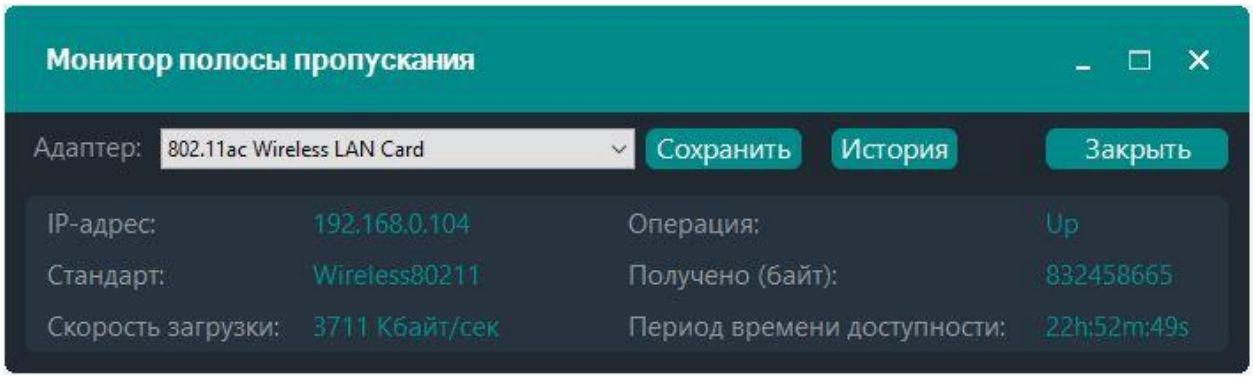

Рисунок 52 – Выбранный адаптер и параметры

Кнопкой «Сохранить» сохраняются данные по выбранному параметру и заносятся в таблицу базы данных. После перехода по нажатию кнопки «История» открывается одноименная форма. Кнопка отображения данных выстраивает таблицу со столбцами, названиями которых служат отображаемые параметры на форме монитора (рисунок 53).

Очищение таблицы происходит при нажатии кнопки «Очистить таблицу» (рисунок 54). Кнопка «Удалить данные из базы» полностью очищает данные таблицы в базе данных, стирая их безвозвратно. В этом случае, при попытке вывести данные повторно, таблица на форме останется пустой, так как не существует данных для вывода.

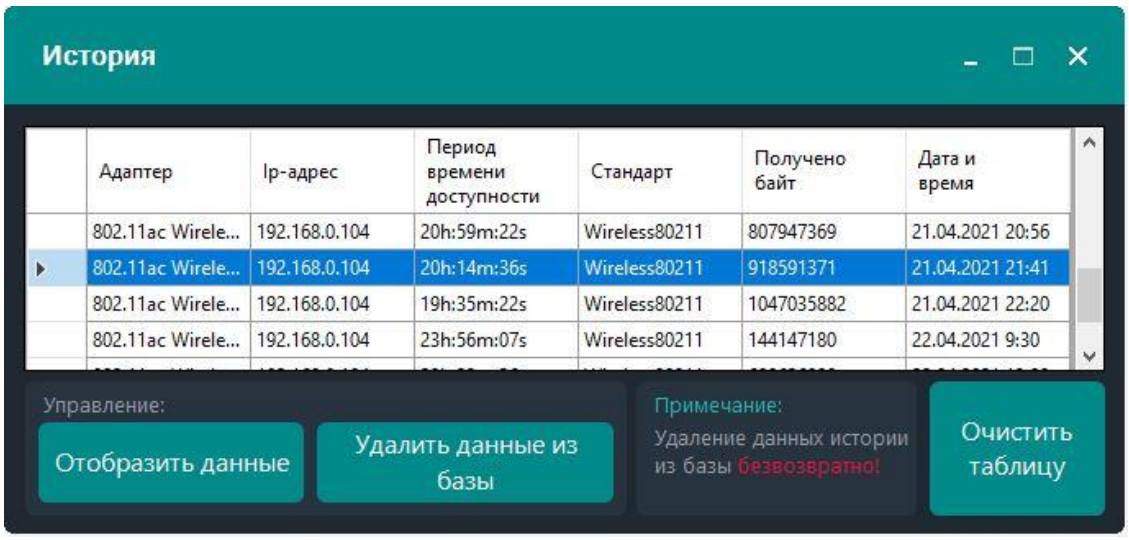

Рисунок 53 – Форма истории с выведенными данными из хранилища

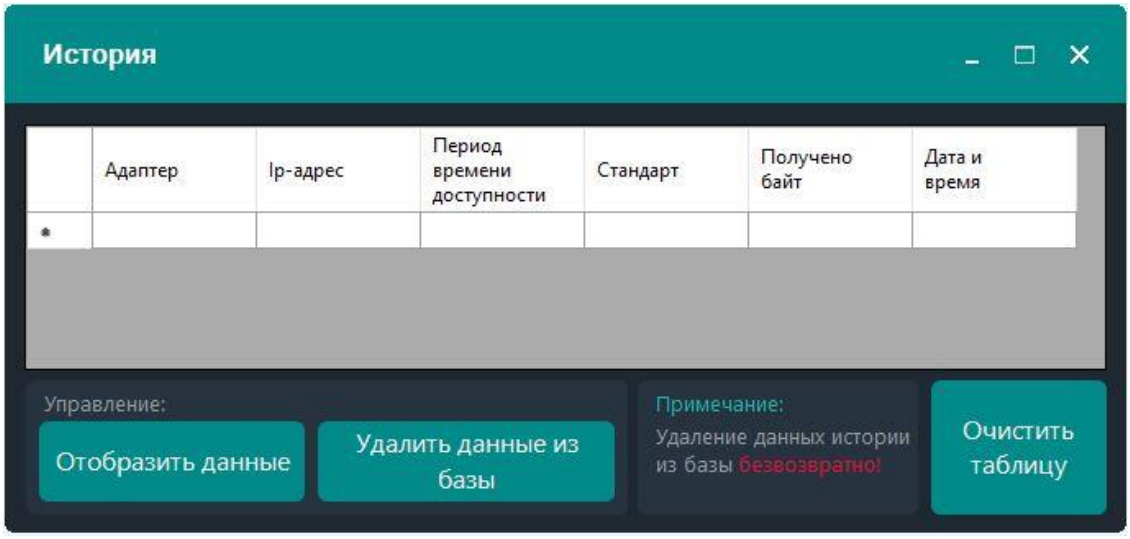

Рисунок 54 – Форма истории с очищенной таблицей

3.3.3 Тестирование формы «Анализатор трафика»

Форма «Анализатор трафика» производит захват пакетов данных и формирует список-дерево для вывода на элемент формы. Так информация предоставляется пользователю в наглядном виде (рисунок 55).

Важно отметить, что программа используемый метод доступа к сокету, захватывающему пакеты, который запрещен правами доступа на уровне системы. Для функционала анализатора необходимо запускать исполняемый файл программы от имени администратора.

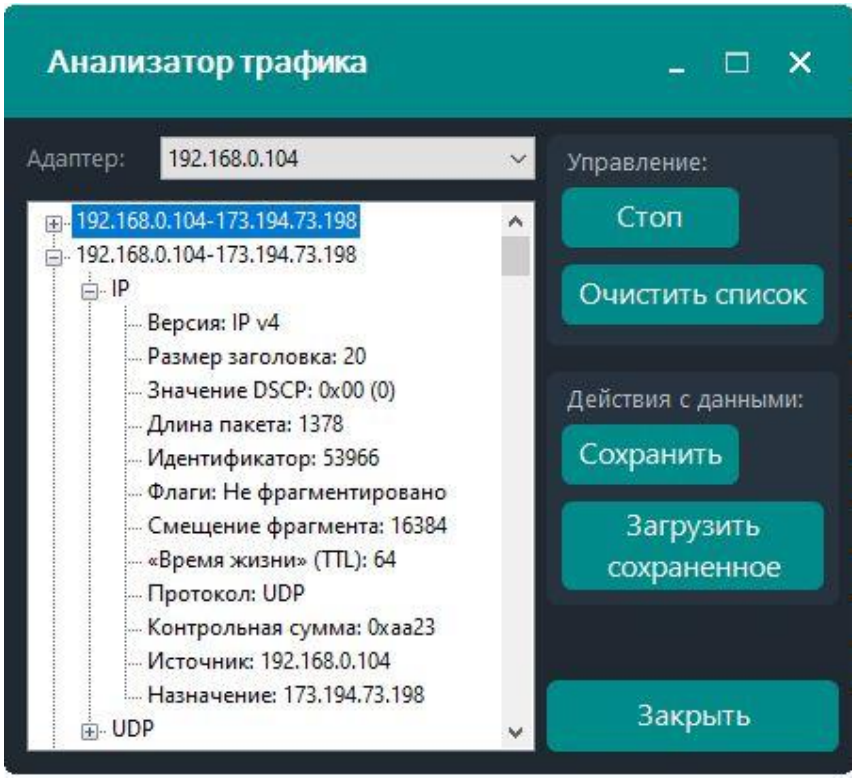

Рисунок 55 – Анализатор трафика с построенным списком-деревом

3.3.4 Тестирование формы «Менеджер беспроводных сетей»

При запуске формы менеджера на вкладке «Импорт» отсутствуют профили для импортирования на данное устройство (рисунок 56).

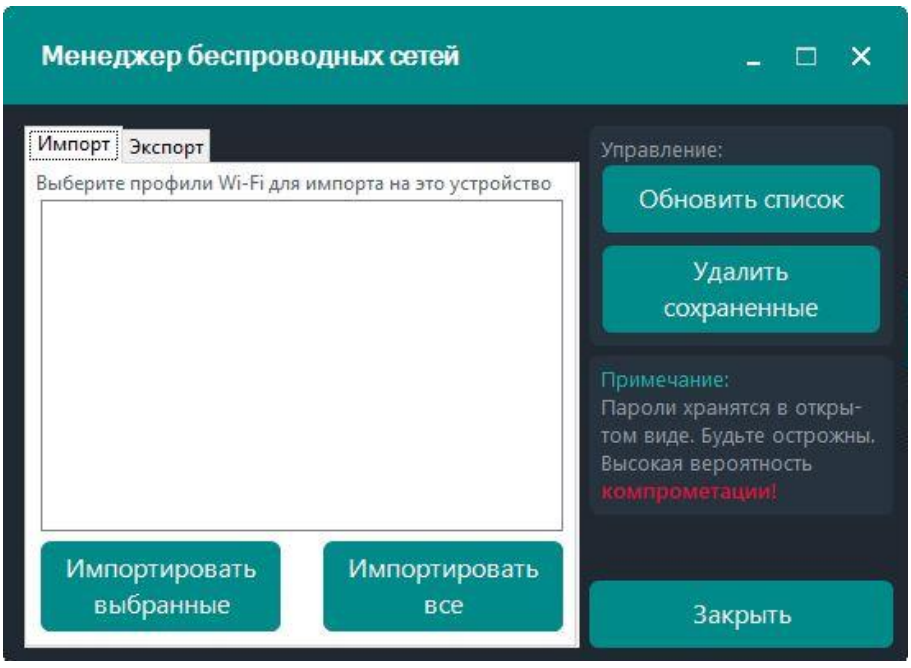

Рисунок 56 – Форма менеджера без профилей для импорта

Нажатие на вкладку «Экспорт» перемещает пользователя на другую часть элемента, где отображаются два профиля тестовых точек доступа, к которым производилось подключение стандартными средствами ОС Windows 10 с вводом пароля (рисунок 57).

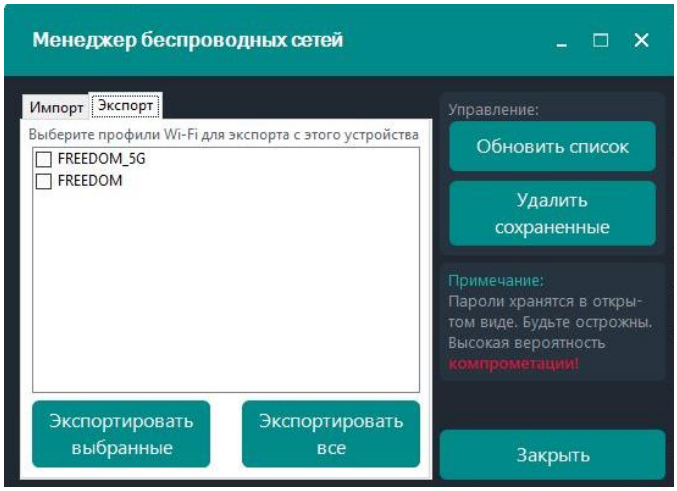

Рисунок 57 – Форма менеджера с профилями тестовых точек доступа для экспорта

3.3.5 Обработка исключительных ситуаций

Для удобства и информативности в программе реализована обработка исключительных ситуаций. При вводе на форме авторизации неверного логина и/или пароля, несовпадающих с занесенными в БД, программа выдаст ошибку (рисунок 58).

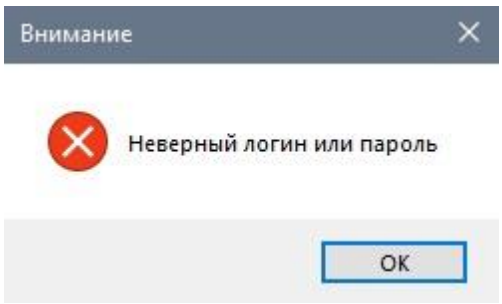

Рисунок 58 – Ошибка ввода логина и/или пароля

Попытка нажатия кнопки «Подключиться» на главной форме без выбранной точки доступа и/или введенного пароля приведет к выводу сообщения об ошибке (рисунок 59).

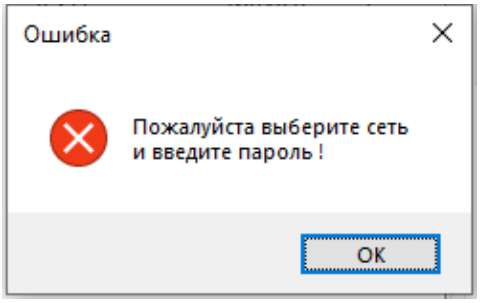

Рисунок 59 – Ошибка при подключении к точке доступа

При нажатии кнопки «Старт» с невыбранным адаптером на форме «Анализатор трафика» программа выдаст окно с ошибкой (рисунок 60).

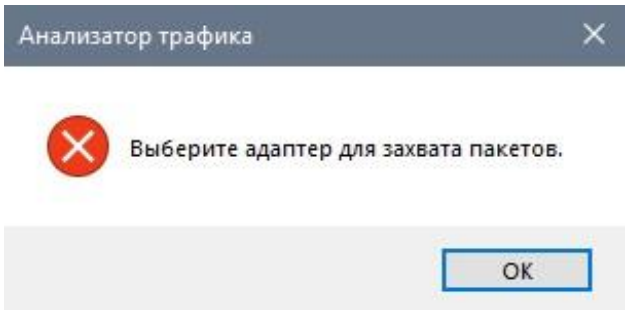

Рисунок 60 – Ошибка при отсутствии выбранного адаптера

Если программа запущена не от имени администратора, то при попытке захвата пакетов появится окно, оповещающее об ошибке доступа (рисунок 61).

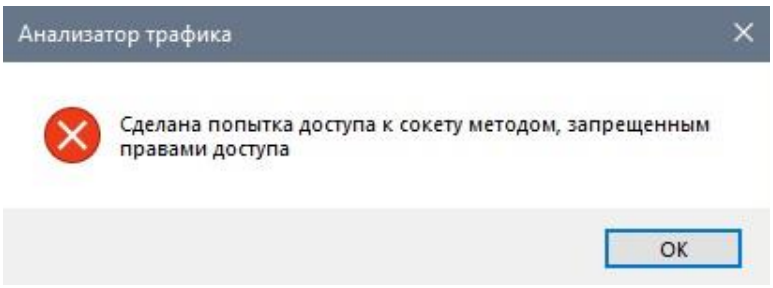

Рисунок 61 – Ошибка доступа при входе не от имени администратора

При сохранении данных на форме «Монитор беспроводной полосы пропуска» программа информирует об успешном завершении операции и выводит окно с сообщением (рисунок 62).

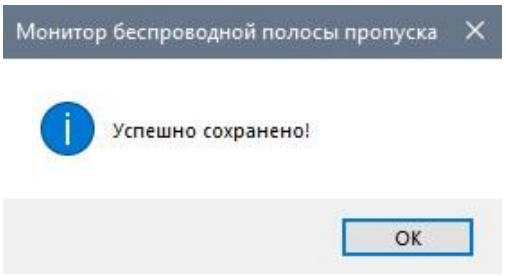

Рисунок 62 – Сообщение об успешном сохранении

Ограничения на количество одновременно активных форм не предусмотрено/ Формы программы можно открывать неограниченное количество раз, что может привести к снижению производительности на слабых рабочих станциях. Поэтому рекомендуется открывать не более двух экземпляров каждой формы.

3.4 Анализ достоверности и практической значимости результатов

Анализ достоверности является немаловажным этапом разработки программного продукта и проводится с целью выявления неточностей функционирования реализованного приложения. По результатам тестирования программа может функционировать без сбоев и критических ошибок, однако выдаваемые результаты могут быть ошибочны. Такие ситуации недопустимы. С целью их предотвращения проводят многократное тестирование отдельных функций программы на предмет наличия неточностей в реализованном функционале.

3.4.1 Результат выполнения кода главной формы

Главная форма представляет собой наиболее информативную часть разработанного продукта. На ней расположен элемент, в котором формируется список обнаруженных точках доступа, а также составляется таблица с занесением в нее данных каждой точки доступа (рисунок 63). Объем получаемых данных довольно обширен и следует удостовериться в их соответствии реальным данным, хранящимся в системе.

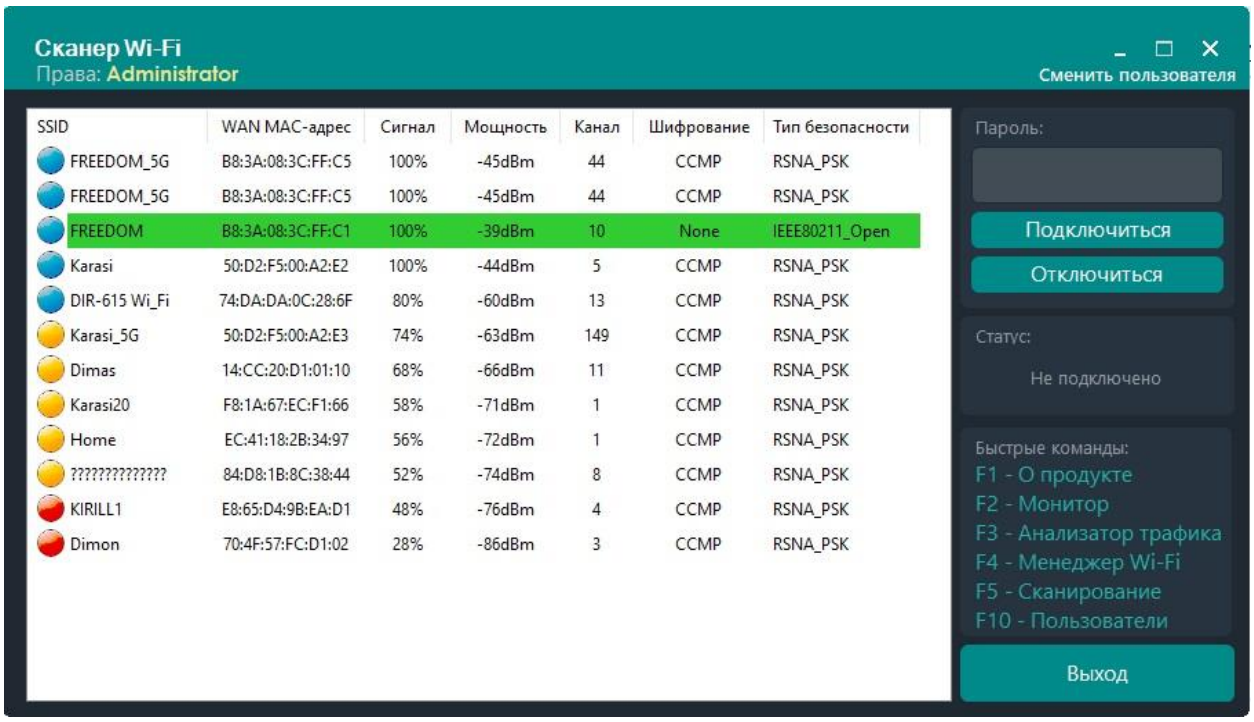

Рисунок 63 – Главная форма со списком обнаруженных точек и их дополнительными данными

Сравнивая полученную из приложения информацию с информацией из ОС (рисунок 64), можно сделать вывод, что приложение правильно обнаруживает точки доступа, так как присутствуют точки с одинаковыми наименованиями (SSID), а также их уровень сигнала примерно одинаков, что можно увидеть на примере точки доступа «Home», которой соответствует желтая иконка в программе, обозначающая средний уровень сигнала. Подтверждение этого можно увидеть в списке ОС, где иконка этой же точки доступа имеет неполные деления уровня сигнала. Тип безопасности в таблице программы указывает, что точки доступа защищены паролем и используют протокол WPA 2 – PSK (RSNA_PSK). Тестовая точка доступа «FREEDOM» была специально переведена в режим отключенного механизма безопасности. Она подсвечивается зеленым и ее тип безопасности отображается как «IEEE80211_Open», что эквивалентно указанию отключенного механизма безопасности у точки доступа (иконка замка не появляется в списке ОС).

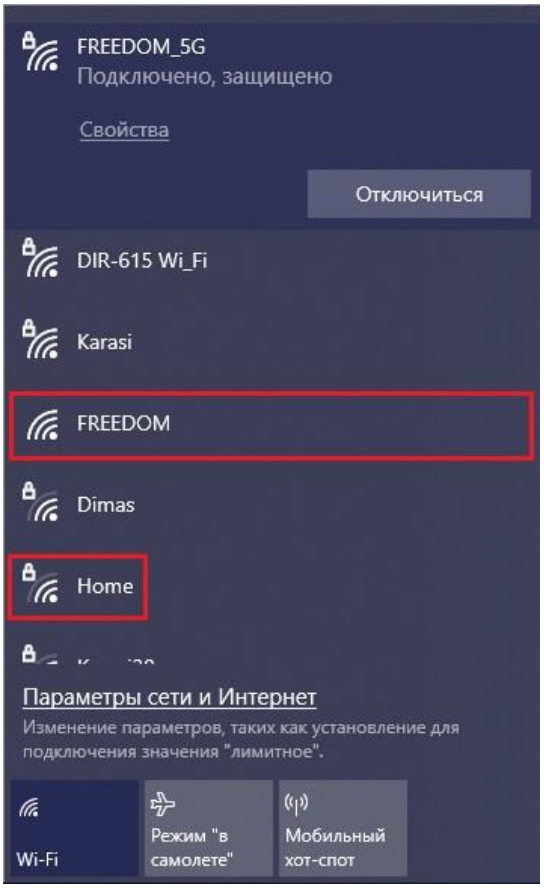

Рисунок 64 – Список обнаруженных точек доступа в ОС Windows 10

Стоит обратить внимание на параметр «WAN MAC-адрес». Это уникальный адрес, который присваивается точке доступа на основании MAC-адреса роутера. Адрес роутера можно увидеть в ПО роутера (рисунок 65).

Рисунок 65 – Информация из ПО роутера

При сравнении адресов можно заметить, что они схожи вплоть до последней цифры. Точка доступа «FREEDOM_5G» имеет цифру 5, в то время

как «FREEDOM» – цифру 1. Эта разница обусловлена тем, что обе тестовые точки принадлежат одному и тому же роутеру, но работают в разных частотных диапазонах (5 ГГц и 2,4 ГГц соответственно). Каждую точку нужно идентифицировать. С этой целью их адреса отличаются последней цифрой.

Кроме того, можно проверить информацию об используемом канале точкой доступа. По данным программы это 44 канал для «FREEDOM_5G» и 10 канал для «FREEDOM». Из данных ОС можно сделать вывод о достоверности этой информации (рисунок 66).

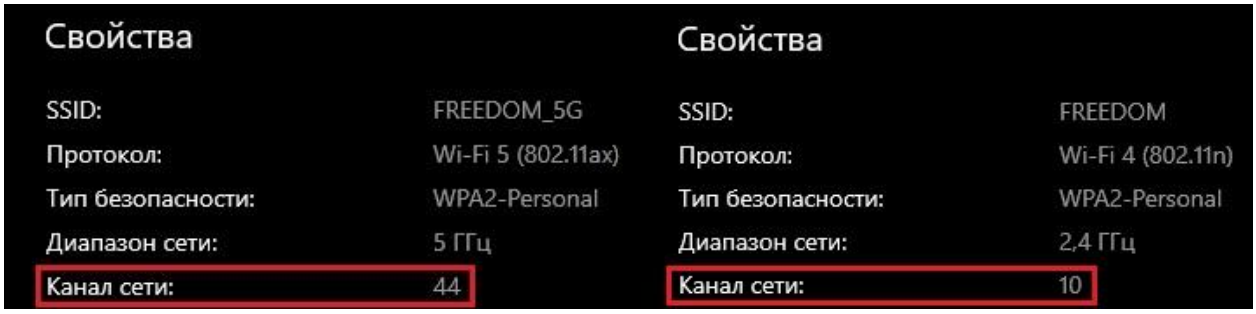

Рисунок 66 – Свойства тестовых точек доступа

3.4.2 Результат выполнения кода формы «Монитор полосы пропускания»

Монитор через LINQ-запрос определяет беспроводные адаптеры в системе и при обращении к выбранному из списка адаптеру получает необходимые данные, которые выводятся на форму (рисунок 67).

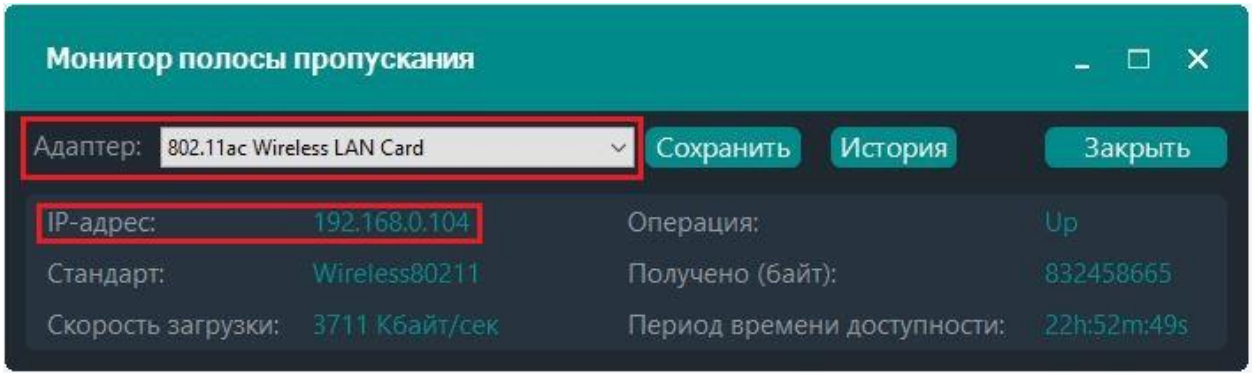

Рисунок 67 – Монитор с выбранным адаптером и выводом параметров

Полученные данные также можно проверить. В частности, определение адаптера и используемый IP-адрес. С помощью средств ОС их также можно просмотреть в «Параметры сети и интернет» - «Wi-FI» - «Свойства оборудования» (рисунок 68).

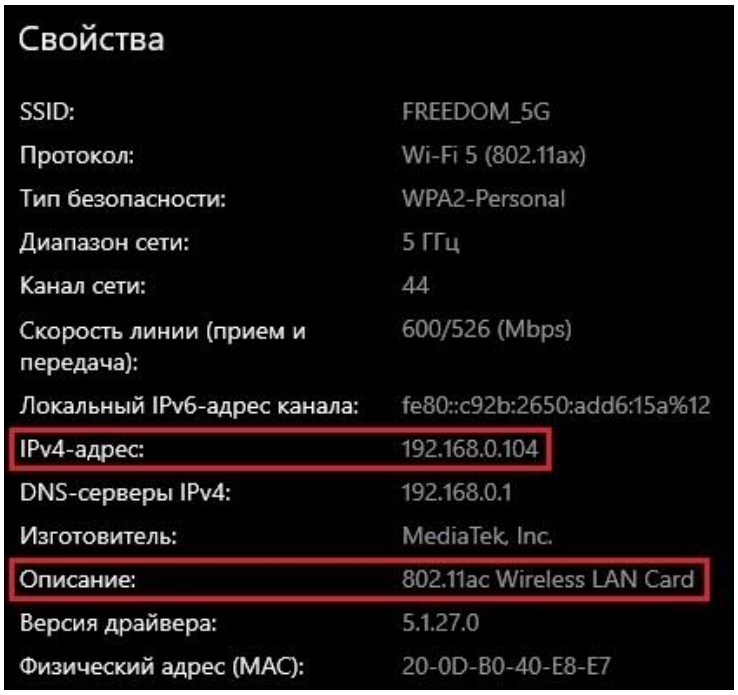

Рисунок 68 – IP-адрес и беспроводной адаптер в средствах просмотра Windows 10

3.4.3 Результат выполнения кода формы «Анализатор трафика»

Анализатор трафика после нажатия кнопки «Старт» открывает сокет, захватывающий пакеты, происходит его привязка к выбранному адаптеру по IP-адресу, который передается в выпадающий список и становится доступен для выбора пользователю. На основе информации о захваченных пакетах происходит построение списка-дерева, куда сводятся их данные (рисунок 69).

IP-адрес источника указан как «192.168.0.104», что соответствует тестовому беспроводному адаптеру. Верхняя строка «192.168.0.104 – 87.240.137.158» означает откуда и куда направляются пакеты данных. Данную информацию возможно проверить с помощью специальных сервисов. Тестовая сессия производилась с помощью сайта социальной сети «ВКонтакте»,

захват пакетов производился при посещении данного сайта. В этом случае неизбежно происходит обмен пакетами данных.

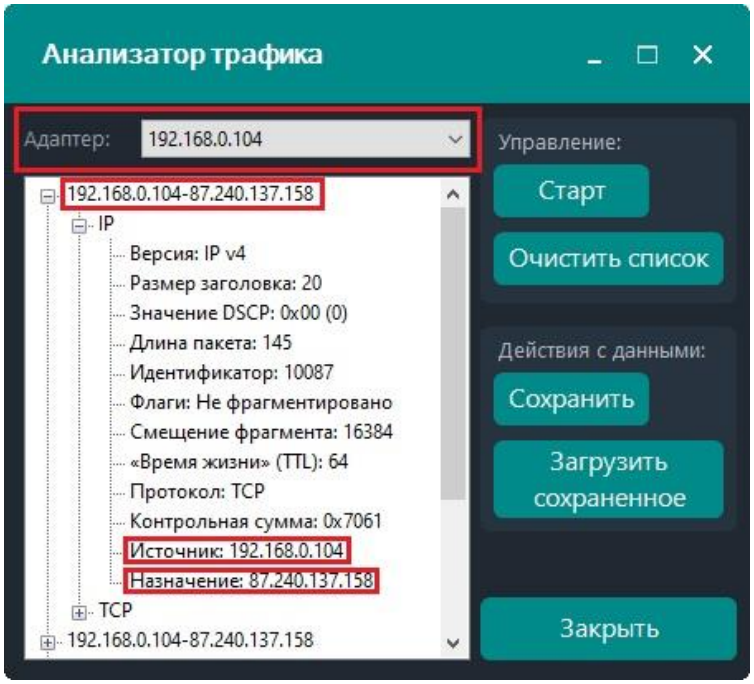

Рисунок 69 – Анализатор трафика с выбранным адаптером и захваченными пакетами

С помощью специального сервиса проверки IP-адреса можно увидеть, что адрес «87.240.137.158» действительно принадлежит «ВКонтакте» (рисунок 70). Кроме того, отображенный IP-адрес попадает в диапазон, а доменное имя «vk.com» соответствует сайту социальной сети «ВКонтакте».

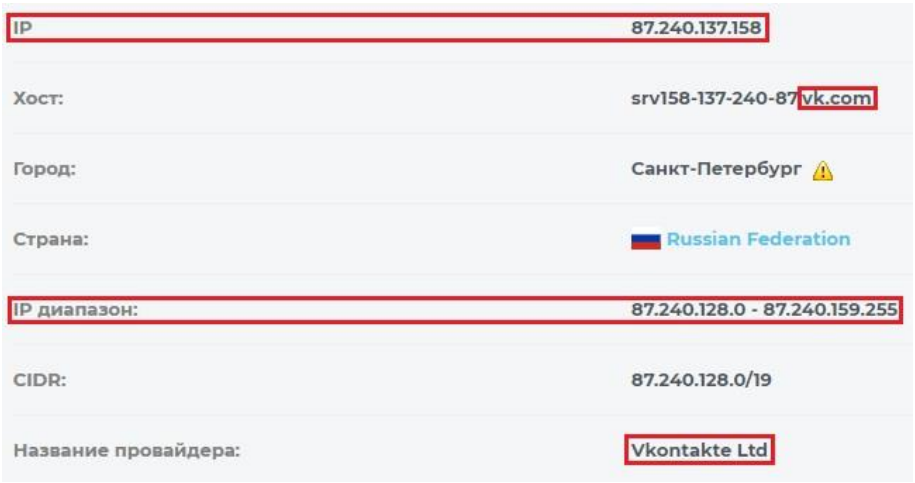

Рисунок 70 – Информация об IP-адресе «87.240.137.158»

Нажатие кнопки «Сохранить» приводит к сохранению текущей информации из окна формы в виде текстового файла в директории программы под названием «Данные_анализатор.txt» (рисунок 71). Данные из этого файла можно загрузить в форму программы с помощью кнопки «Загрузить сохраненное». Повторное сохранение информации перезаписывает файл, поэтому рекомендуется сохранять файл в отдельном месте, если необходимо в будущем использовать информацию из него. Текстовый файл не представляется возможным прочитать с помощью стандартных средств ОС Windows.

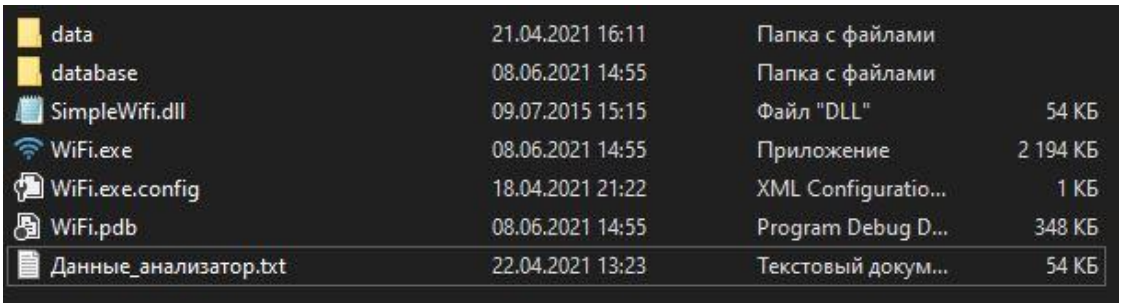

Рисунок 71 – Данные анализатора в виде текстового файла в директории программы

3.4.4 Результат выполнения кода формы «Менеджер беспроводных сетей»

Менеджер беспроводных сетей отображает на вкладке «Экспорт» профили точек доступа, к которым ранее производилось подключение с вводом пароля. Эта информация берется из ОС. Наглядно она представлена в «Параметры сети и интернет» - «Wi-FI» - «Управление известными сетями» (рисунок 72). Здесь отображаются точки, которые уже известны системе. Информация об их пароле при подключении сохраняется в системе, однако, свойствами ОС просмотреть эту информацию довольно непросто. Такая реализация направлена на повышение безопасности, так как пароль защищенной точки доступа мог быть легко скомпрометирован, что недопустимо, когда речь идет о каких-то корпоративных сетях с оборотом конфиденциальной информации внутри беспроводной сети Wi-Fi.

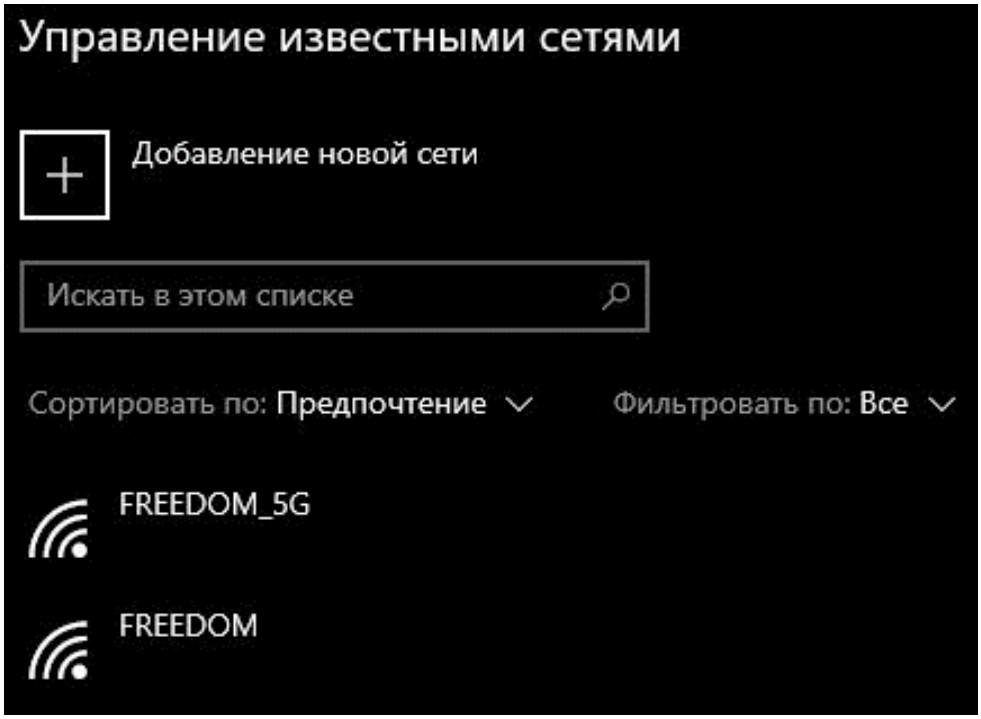

Рисунок 72 – Известные точки в системе

На вкладке «Экспорт» менеджера беспроводных сетей также представлены две позиции с профилями известных тестовых точек доступа (рисунок 73).

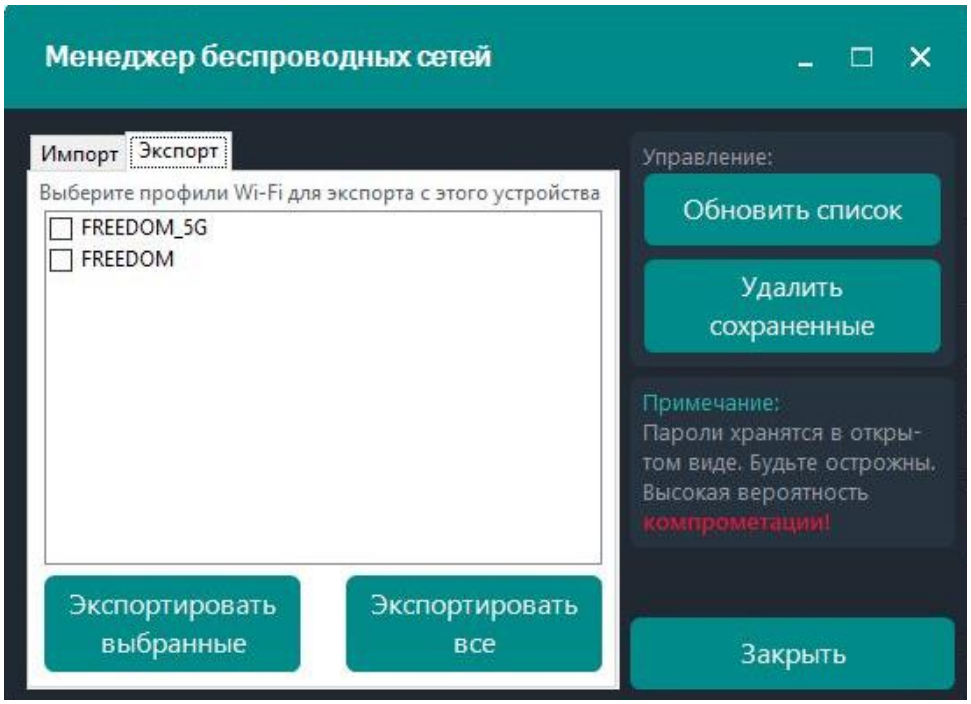

Рисунок 73 – Профили известных точек доступа в менеджере

Нажатие кнопки «Экспортировать все» приводит к сохранению профилей всех точек доступа из списка в директорию программы в виде xml-файлов, которые возможно просмотреть и увидеть всю информацию, включая пароль в открытом виде (рисунок 74).

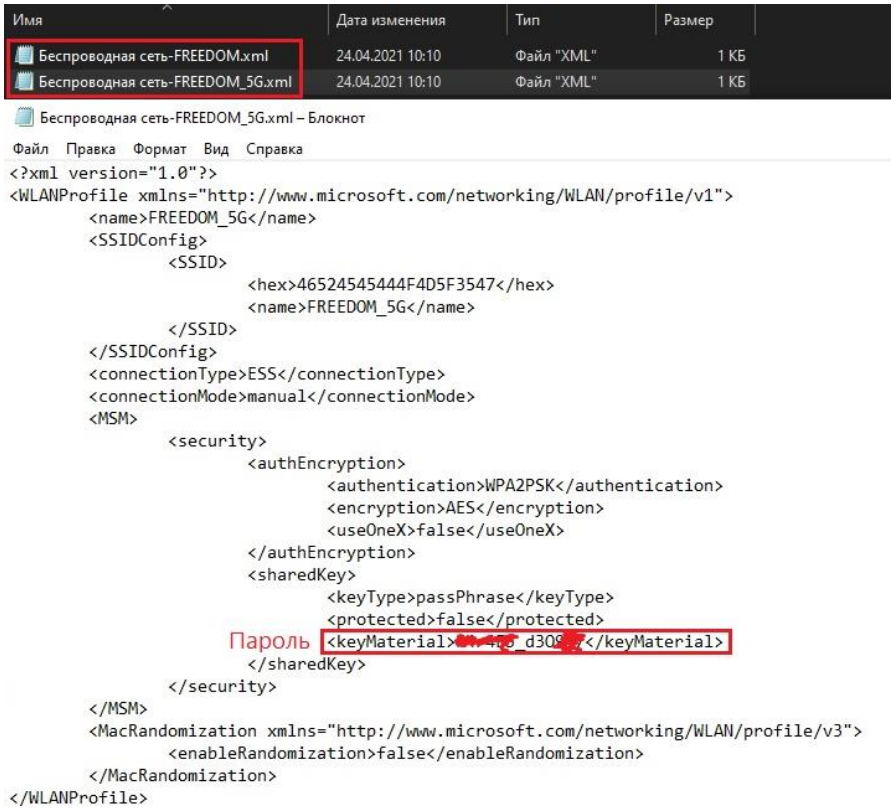

Рисунок 74 – Профили точек доступа в проводнике Windows 10

Хранение пароля в открытом виде необходимо для импорта профиля в систему на другом устройстве. В связи с этим, рекомендуется удалять xml-файлы профилей после их использования для снижения вероятности компрометации.

Кнопка «Удалить сохраненные» удаляет данные профили из директории программы. Также эти профили можно скопировать на другое устройство и с помощью программы импортировать в систему, чтобы подключиться к выбранной точке доступа без ввода пароля.

3.4.5 Практическая значимость результатов

Исходя из вышеизложенного, можно сделать вывод о положительном результате разработки программного обеспечения. Тестирование и анализ

достоверности результатов показали, что разработку возможно применять для решения практических задач и использовать по прямому назначению, а также для достижения целей, на которые была ориентирована разработка.

Разработанная программа может использоваться для любых беспроводных Wi-Fi сетей, поэтому она подходит и для обширных корпоративных сетей, и для небольших домашних локальных беспроводных сетей.

ЗАКЛЮЧЕНИЕ

Анализ предметной области показал, что к построению Wi-Fi сетей необходимо подходить с использованием знаний об особенностях используемого стандарта. Каждый стандарт беспроводной связи имеет свои особенности, которые отражаются на принципах построения беспроводных сетей.

Говоря о новом стандарте 802.11ax (Wi-Fi 6), важно учитывать то, на каких частотах функционирует оборудование, как и с помощью каких технологий происходит связь оборудования и устройств в рамках одной беспроводной сети, а также какого типа сети необходима для конкретного помещения или здания.

В ходе выполнения практической части работы была достигнута поставленная цель по проектированию легкой, не нагруженной программы, способной обнаруживать активные точки доступа Wi-Fi, сканировать поток данных в заданной сети с выявлением ее характеристик используемой точки доступа, таких как протокол передачи, скорость передачи, тип подключения, IP-адрес и т.д., а также анализировать пакеты передаваемых данных.

Была изучена предметная область и проведен ее анализ, рассмотрены существующие модели жизненного цикла и сделан выбор в пользу каскадной модели, подробно составлены функциональные и нефункциональные требования к программному продукту, произведен выбор и обоснование средств реализации, детально описаны модули системы, а также описан процесс проектирования с характерными особенностями. Был детально изучен процесс проектирования и написания кода.

Изучение большого объема теоретического материала позволило грамотно спроектировать задуманный функционал программы и выбрать концепцию для создания интерфейса итогового продукта. В качестве визуализации процессов были использованы скриншоты для подкрепления теоретического материала и демонстрации функционирования готового программного продукта.

Разработанное программное обеспечение позволит протестировать созданную беспроводную сеть, локализовать ошибки внутри сети, обнаружить перебои связи и подозрительный трафик внутри беспроводной сети.

Готовый программный продукт направлен на регистрацию для получения свидетельства «О государственной регистрации программы для ЭВМ».

БИБЛИОГРАФИЧЕСКИЕ ССЫЛКИ

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

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

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

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

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

6 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.

7 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.

8 Там же, С. 67.

9 Литовский М. В., Самохвалова С. Г. Wi-Fi 6 как основа для построения беспроводных сетей нового поколения // Modern scientific researches. 2020. № 12-01 (2020). С. 29-34.

10 Там же, С. 32.

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 Колисниченко, Д. Н. Беспроводная сеть дома и в офисе : моногр. / Д. Н. Колисниченко. – М. : БХВ-Петербург, 2015. – 997 с.

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

14 Колисниченко, Д. Н. Беспроводная сеть дома и в офисе : моногр. / Д. Н. Колисниченко. – М. : БХВ-Петербург, 2015. – 997 с.

15 Там же, С. 443.

16 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.

17 Росс, Джон. Wi-Fi. Беспроводная сеть : моногр. : пер. с англ. / Д. Росс. – М. : НТ-Пресс, 2007. – 320 с.

18 Лагунов, А. Ю. Проблемы безопасности в беспроводных сетях стандарта IEEE 802.11 / А.Ю. Лагунов, А.В. Орлов // SWorld. – 2015. – № 38. – С. 41-46.

19 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.

20 Современные сетевые технологии. Учебное пособие : моногр. / П. Н. Башлы. – М. : Горячая линия – Телеком, 2006. – 334 с.

21 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.

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

23 Там же, С. 337.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1 Беспроводные сети передачи данных. Учебное пособие : моногр. / В. И. Шубин. – М. : Вузовская книга, 2013. – 104 с.

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

3 Гейер, Джим. Беспроводные сети. Первый шаг : моногр. : пер. с англ. / Дж. Гейер. – М. : Вильямс, 2005. – 187 с.

4 Гейер, Джим. Беспроводные сети. Установка и устранение неполадок за 5 минут : моногр. : пер. с англ. / Дж. Гейер, Э. Гейер, Дж.Р. Кинг– М. : НТ Пресс, 2015. – 176 с.

5 Голубицкая, Е.А. Экономика связи : моногр. / Е. А. Голубицкая, Г. М. Жигуляская. – М. : Радио и связь, 1999. – 488 с.

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

7 Колисниченко, Д. Н. Беспроводная сеть дома и в офисе : моногр. / Д. Н. Колисниченко. – М. : БХВ-Петербург, 2015. – 997 с.

8 Кузнецов, М.А. Современные технологии и стандарты подвижной связи : моногр. / М. А. Кузнецов, А. Е. Рыжков. – СПб. : Линк, 2006. – 480 с.

9 Лагунов, А. Ю. Проблемы безопасности в беспроводных сетях стандарта IEEE 802.11 / А.Ю. Лагунов, А.В. Орлов // SWorld. – 2015. – № 38. – С. 41-46.

10 Литовский М. В., Самохвалова С. Г. Проектирование Wi-Fi сети // Наука и инновации – современные концепции: сборник научных статей по итогам работы Международного научного форума / Коллектив авторов. Москва, 2019. Т. 1. С. 108-112.

11 Литовский М. В., Самохвалова С. Г. Wi-Fi 6 как основа для построения беспроводных сетей нового поколения // Modern scientific researches. 2020. № 12-01 (2020). С. 29-34.

12 Литовский М. В., Самохвалова С. Г. Wi-Fi 6 – Новое поколение технологии беспроводной передачи данных // Молодёжь XXI века: шаг в будущее: Материалы XXI региональной научно-практической конференции / Министерство образования и науки амурской области [и др.]. Благовещенск, 2020. Т. 4. С. 118-119.

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

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

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

16 Мерит, Максим. Безопасность беспроводных сетей : моногр. : пер. с англ. / М. Мерит – М. : Компания АйТи, ДМК Пресс, 2004. – 288 с.

17 Молодежь XXI века: шаг в будущее: матер. XXI регион. науч.- практ. конф. (Благовещенск, 20 мая 2020 г.). В 4 т. – Благовещенск: Изд-во Дальневост. гос. аграр. ун-та, 2020. –Т. 4: Сельскохозяйственные науки. Физико-математические науки. Химические науки. Информационные технологии. Технические науки. – 235 с.

18 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.

19 Олифер, В. Г. Базовые технологии локальных сетей : моногр. / В. Г. Олифер, Н. А. Олифер – СПб : Питер, 1999. – 387 с.

20 Пахомов, С. Ю. Анатомия беспроводных сетей / С.Ю. Пахомов // Компьютер-Пресс. – 2002. – № 7. – С. 167-175.

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

22 Росс, Джон. Wi-Fi. Беспроводная сеть : моногр. : пер. с англ. / Д. Росс. – М. : НТ-Пресс, 2007. – 320 с.

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

24 Современные сетевые технологии. Учебное пособие : моногр. / П. Н. Башлы. – М. : Горячая линия – Телеком, 2006. – 334 с.

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

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

27 Технология разработки программного обеспечения [Электронный ресурс] : учеб. – метод. пособие / АмГУ, ФМиИ ; сост. Т. А. Галаган. – Благовещенск : Изд-во Амур. гос. ун-та, 2015. – 49 с. Режим доступа: http://irbis.amursu.ru/DigitalLibrary/AmurSU_Edition/6799.pdf – 26.11.2020.

28 Технология разработки программного обеспечения [Электронный ресурс] : сб. учеб.-метод. материалов для направления подготовки 09.04.04 "Программная инженерия" / АмГУ, ФМиИ ; сост. Т. А. Галаган. - Благовещенск : Изд-во Амур. гос. ун-та, 2017. - 51 с. Режим доступа: http://irbis.amursu.ru/DigitalLibrary/AmurSU_Edition/10382.pdf – 08.02.2021.

29 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.

30 Хабрейкен, Джо. Домашние беспроводные сети : моногр. : пер. с англ. / Д. Хабрейкен. – М. : НТ-Пресс, 2014. – 400 с.

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

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

33 Широкополосные беспроводные сеети передачи информации :

моногр. / В. М. Вишневский [и др.]. – М. : Эко-Трендз, 2005. – 592 с.

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

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