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

Факультет математики и информатики
Кафедра информационных и управляющих систем
Направление подготовки 09.03.02 – Информационные системы и технологии
Профиль: Информационные системы и технологии

ДОПУСТИТЬ К ЗАЩИТЕ
Зав. кафедрой
_____ А.В. Бушманов
«_____»_____2016 г.

БАКАЛАВРСКАЯ РАБОТА

на тему: Разработка программно-аппаратного комплекса по перехвату трафика и несанкционированному доступу в беспроводных сетях стандарта 802.11 b/g/n

Исполнитель
студент группы 255-об _____ (подпись, дата) А.С. Герасименко

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

Нормоконтроль
инженер кафедры _____ (подпись, дата) В.В.Романико

Благовещенск 2016

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

Факультет математики и информатики
Кафедра информационных и управляющих систем

УТВЕРЖДАЮ
Зав.кафедрой
_____А.В.Бушманов
«_____»_____2016 г.

З А Д А Н И Е

К бакалаврской работе студента Герасименко Александра Сергеевича.

1. Тема дипломной работы: Разработка программно-аппаратного комплекса по перехвату трафика и несанкционированному доступу в беспроводных сетях стандарта 802.11 b/g/n.

(утверждено приказом от 03.06.2016 № 1215-уч)

2. Срок сдачи студентом законченной работы 28.06.2016 г.

3. Исходные данные к дипломной работе: отчет по преддипломной практике.

4. Содержание дипломной работы: анализ предметной области; исследование программно-аппаратной инфраструктуры; разработка аппаратного обеспечения; разработка программного обеспечения.

5. Перечень материалов приложения: приложения.

6. Дата выдачи задания 09.05.2016 г.

Руководитель дипломной работы Светлана Геннадьевна Самохвалова, доцент, канд. техн. наук.

Задание принял к исполнению _____А.С. Герасименко

РЕФЕРАТ

Бакалаврская работа содержит 67 с., 39 рисунков, 1 таблицу, 22 источника.

ПРОГРАММНО-АППАРАТНЫЙ КОМПЛЕКС, ПЕРЕХВАТ ТРАФИКА, СНИФФЕР, ЛОГГЕР, РАДИОПЕРЕХВАТ, БЕСПРОВОДНЫЕ СЕТИ, СТАНДАРТ 802.11, СПЕЦИАЛЬНОЕ АППАРАТНОЕ ОБЕСПЕЧЕНИЕ

Объектом исследования данной выпускной квалификационной работы являются беспроводные сети стандарта 802.11 b/g/n. Предметом исследования является передача и перехват трафика внутри беспроводных сетей.

Цель исследования: разработать программно-аппаратный комплекс по перехвату трафика и несанкционированному доступу в беспроводных сетях стандарта 802.11 b/g/n.

Задачи исследования:

– анализ стандарта IEEE 802.11;

– исследование аппаратного и программного обеспечения;

– разработка аппаратного обеспечения;

– проектирование корпусов для аппаратных модулей;

– разработка программного обеспечения по перехвату пакетов из сети.

СОДЕРЖАНИЕ

НОРМАТИВНЫЕ ССЫЛКИ

В настоящей работе использованы ссылки на следующие стандарты:

ГОСТ 7.80-2000 Библиографическая запись. Заголовок

ГОСТ 19.004-80 ЕСПД. Термины и определения

ГОСТ 19.402-78 ЕСПД. Описание программы

ГОСТ 34.201-89 Информационная технология. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем

ГОСТ 34.601-90 Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания

ГОСТ 34.603-92 Информационная технология. Виды испытаний автоматизированных систем

ГОСТ Р 50922-96 Защита информации. Основные требования и определения

ГОСТ Р ИСО 7498-2-99 Информационная технология. Взаимосвязь открытых систем базовая эталонная модель. Часть 2. Архитектура защиты информации

ГОСТ Р ИСО/МЭК 15408-2002. Информационные технологии. Методы и средства обеспечения безопасности. Критерии безопасности информационных технологий

СТО СМК 4.2.3.05-2011 Стандарт организации. Оформление выпускных квалификационных и курсовых работ (проектов)

ОПРЕДЕЛЕНИЯ, ОБОЗНАЧЕНИЯ, СОКРАЩЕНИЯ

FTP – File Transfer Protocol;

HTTP – Hyper Text Protocol;

MS – Microsoft;

OSI – Open systems interconnection;

MAC– Medium Access Control;

TCP/IP – Transmission Control Protocol / Internet Protocol;

TFT – Thin Film Transistor;

USB – Universal Serial Bus;

UTP – Unshielded Twisted Pair;

Wi-Fi – Wireless Fidelity;

АО – аппаратное обеспечение;

БД – база данных;

ЖК – жидкокристаллический;

ИБ – информационная безопасность;

ИС – информационная система;

ИТ – информационная технология;

ЛВС – локальная вычислительная сеть;

НСД – несанкционированный доступ;

ОС – операционная система;

ПАК – программно-аппаратный комплекс;

ПК – персональный компьютер;

ПО – программное обеспечение;

РФ – Российская Федерация;

САПР – система автоматизированного проектирования;

СЗИ – средства защиты информации;

СПО – системное программное обеспечение;

ТЗ – техническое задание;

ЦП – центральный процессор.

ВВЕДЕНИЕ

В эпоху современных компьютерных технологий, когда информация повсеместно хранится, передаётся и обрабатывается в цифровом виде, остро встаёт вопрос об её защищенности. Защита информации представляет собой деятельность по предотвращению утечки защищаемой информации, а также несанкционированных и непреднамеренных воздействий на информацию. Проблема защиты информации является многоплановой, комплексной и является актуальной как в мировом или государственном масштабах, так и в масштабах фирм, организаций, учебных заведений и даже дома. Угроза преднамеренного или непреднамеренного искажения, а также несанкционированного доступа приводит к необходимости организации защиты объектов информации, каналов связи, хранилищ. Современные методы и средства построения инфокоммуникационных сетей претерпевают значительные изменения, что сказывается на качественных и количественных характеристиках любой сети.

Большинство организаций для эргономичности своей информационной системы все больше и больше отдают предпочтение беспроводным каналам связи, что, несомненно, сказывается на удобстве монтажа и дальнейшего использования сети. В любой точке города, используя включенный режим WI-FI на своем мобильном устройстве, планшете или ноутбуке можно найти точку доступа беспроводной сети, и не важно, что это будет: какой-либо кафетерий, чей-либо домашний интернет или сеть ближайшего банка, а возможно, даже и все эти сети вместе.

Главный парадокс информационных технологий можно охарактеризовать так: чем легче и удобнее работать в системе, тем она менее безопасна, а, следовательно, чем больше мы стараемся обезопасить систему, тем сложнее с ней работать. Причины перехода организаций к использованию беспроводных каналов связи – удобство, доступность и эргономичность. Из этого следует, что потенциальные угрозы безопасности могут быть направлены с учетом особен-

ностей архитектуры беспроводных сетей организации.

Объектом исследования являются беспроводные сети стандарта 802.11 b/g/n.

Предмет исследования – это отдельная проблема, отдельные стороны объекта, его характеристики и свойства, которые, не заходя за рамки исследуемого объекта, будут описаны в выпускной квалификационной работе.

Предметом исследования является передача и перехват трафика внутри беспроводных сетей.

Все, что было изложено выше, в целом определяет **цель исследования**: разработать программно-аппаратный комплекс по перехвату трафика и несанкционированному доступу в беспроводных сетях стандарта 802.11 b/g/n.

Для достижения цели в ходе работы мы должны решить следующий ряд задач:

– анализ стандарта IEEE 802.11;

– исследование аппаратного и программного обеспечения;

– разработка аппаратного обеспечения;

– проектирование корпусов для аппаратных модулей;

– разработка модуля ПО по перехвату пакетов из сети.

1 АНАЛИЗ ПРЕДМЕТНОЙ ОБЛАСТИ

1.1 Тестируемое оборудование

Объектом тестирования на предмет защищенности будут рассматриваться беспроводные инфокоммуникационные сети стандарта 802.11 b/g/n. Для проверки каналов связи на определение предмета испытанию заданным спецификациям обычно применяется термин «пентест».

Пентест нужно рассматривать как проверка (тестирование) на проникновение. Это метод оценки безопасности систем вычисления и инфокоммуникационных сетей путем организации искусственной модели атаки злоумышленника. Тестирование на проникновение под собой предполагает активный анализ системы на наличие уязвимостей или потенциальных брешей, которые в будущем смогут негативно повлиять на работу целевой системы, либо привести к полному отказу в обслуживании. Для этого применяется специализированное АО, которое нельзя найти в свободной продаже, но можно его подобрать его компоненты и собрать в одно устройство. Ситуация с СПО несколько иная, так как множество программных продуктов для некоторых этапов пентеста можно найти в свободном распространении. Результатом тестирования на проникновение является отчет, содержащий в себе все найденные уязвимости системы, а также может содержать рекомендации по их устранению. Цель испытаний на проникновение – оценить возможность проведения атаки и спрогнозировать финансово-экономические потери в результате успешного проведения атаки. Испытание на проникновение есть часть аудита безопасности.

1.2 Общие положения информационной безопасности

Информационная безопасность – это защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений, в том числе владельцам и пользователям информации и поддерживающей инфраструктуры.

Основные составляющие информационной безопасности:

Доступность – это возможность за приемлемое время получить требуемую информационную услугу.

Целостность – актуальность, непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения.

Конфиденциальность – защита от несанкционированного доступа к информации.

Для проведения пентеста системы необходимо наличие трех составляющих: тестируемая система, поддерживающая инфраструктура и потенциальный злоумышленник. Последний, в свою очередь, и представляет потенциальную *угрозу информации*. Под угрозой информации принято понимать потенциальные или реально возможные действия по отношению к информационным ресурсам, приводящие к неправомерным овладением охраняемыми сведениями.

Информационной угрозой проявляется в нарушении конфиденциальности, нарушении целостности и нарушении доступности. *Несанкционированный доступ* – это противоправное преднамеренное овладение конфиденциальной информацией лицом, не имеющим право доступа к охраняемым секретам.

1.3 Характеристика потенциальной угрозы

Так как разрабатываемый ПАК станет искусственной моделью злоумышленника, или другими словами будет представлять потенциальную угрозу для исследуемой сети, то стоит охарактеризовать модель проводимой атаки. Такая модель называется атака «посредник» или «человек посередине», которая представлена на рисунке 1.

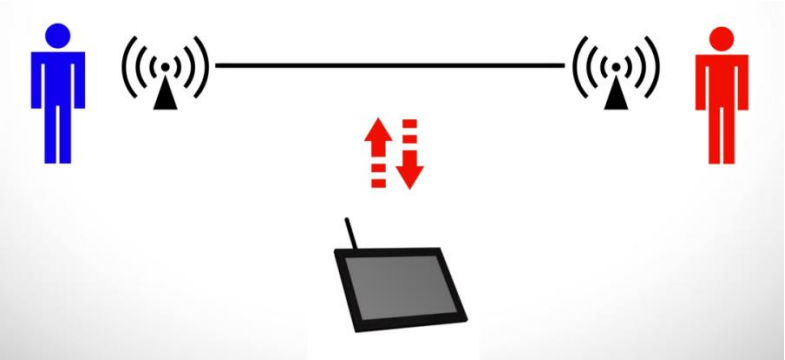

Рисунок 1 – Модель атаки «человек посередине»

На рисунке схематично изображены два абонента, два устройства поддерживающие функцию беспроводной связи, канал передачи сигнала, ПАК и его двустороннее воздействие. Когда два абонента пытаются передать какую-либо информацию друг другу с помощью технологии беспроводной связи, они используют свои устройства (смартфон, ноутбук, планшетный ПК и т.п.). Далее они определяются, кто из них на время передачи данных становится клиентом, а кто сервером. При этом организовывается между их устройствами канал связи. Так как модель атаки предполагает наличие беспроводной сети, то, следовательно, устройства передают сигналы друг другу в виде электромагнитных волн. Каждое из устройств абонентов является как передатчиком, так и приемником.

Угрозой в данной модели является ПАК, который так же является устройством, способным принимать и отправлять сигналы в виде электромагнитных волн той же частоты, что и устройства абонентов беспроводной сети. Тем самым ПАК может получать тот же трафик, который получает другой абонент, которому и предназначена отправка некоторых данных. Такие действия со стороны ПАК несомненно подвергают опасности одну из составляющих ИБ – несанкционированный доступ.

Такую же модель атаки можно использовать и при использовании сторонней точки доступа беспроводной сети, как показано на рисунке 2.

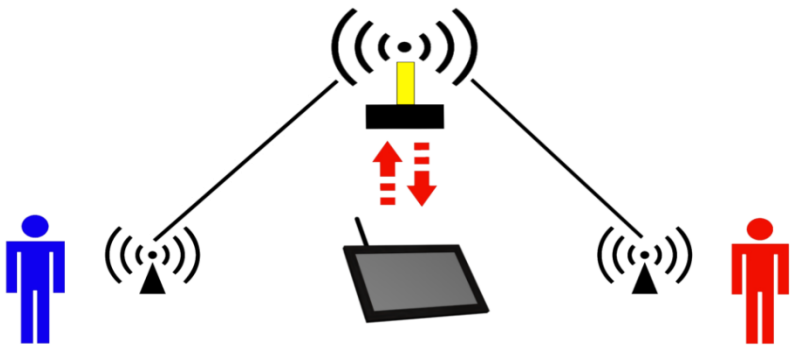

Рисунок 2 – Модель атаки «человек посередине» с использованием сторонней точки доступа беспроводной сети

В рисунке добавлена отдельное устройство беспроводной сети – точка доступа. Это устройство в основном имеет назначение сервера, но все функции приема и передачи сигнала в одном электромагнитном волновом диапазоне остаются неизменными.

В таком случае главной целью атаки ПАК будет являться точка доступа, через которую будет легче найти любого абонента, подключенного к беспроводной сети. Обычно к устройствам, работающие в режиме точки доступа относят:

– роутер;

– маршрутизатор;

– модем;

– адаптеры мобильных устройств.

Каждый из этих устройств представляет различный уровень международного стандарта сетевой модели OSI. Поэтому атака ПАК имеет больше шансов на успешное вторжение в сеть, организованную с помощью точки доступа. Но не стоит забывать, что все зависит от поддерживающей инфраструктуры.

1.4 Требования к разрабатываемому комплексу

Разрабатываемый программно-аппаратный комплекс предназначен для пентеста беспроводных сетей стандарта 802.11 b/g/n на предмет перехвата трафика и несанкционированного доступа.

ПАК должен иметь:

– независимую аппаратную платформу для мобильной работы в различных условиях;

– уникальное и в то же время понятное для оператора ПАК программное обеспечение, которое необходимо для успешного проведения пентеста сети;

– защитный корпус всей аппаратной платформы, который будет сохранять работоспособное состояние всего комплекса от внешних случайных или непредвиденных воздействий внешней среды.

Аппаратная платформа должна включать в себя:

– вычислительная платформа;

– модуль передачи данных;

– устройство распространения сигнала.

Программное обеспечение должно состоять из модулей:

– сниффер;

– дешифратор;

– логгер.

Все защитные корпуса должны быть спроектированы в САПР с учетом всех параметров аппаратного обеспечения и реализованы с помощью трехмерной печати и лазерной резки.

2 ИССЛЕДОВАНИЕ ПРОГРАММНО-АППАРАТНОЙ ИНФРАСТРУКТУРЫ

2.1 Характеристика среды передачи сигнала

Электромагнитное излучение – это электромагнитные волны, порождаемые разными объектами излучения, какими-либо заряженными частицами, молекулами, атомами, антеннами и пр. Из-за разностей длин волн можно выделить гамма-излучение, рентген-излучение, ультрафиолетовое излучение, свет улавливаемый глазом, инфракрасное излучение, электромагнитные колебания низких частот и радиоволны. В прочем, имея такие радикальные отличия, такие излучения – в целом, разные стороны единого явления.

Если же исследовать сигнал как функцию времени, то он будет, либо аналоговым, либо цифровым. Аналоговый сигнал – интенсивность во времени меняется последовательно. То есть, в сигналах нет остановок, прерываний или каких-либо разрывов. Цифровой сигнал – интенсивность, в течение временного отрезка характеризуется постоянным уровнем, а потом меняется на постоянную величину. На рисунке 3 и 4 отображены примеры цифровых и аналоговых сигналов.

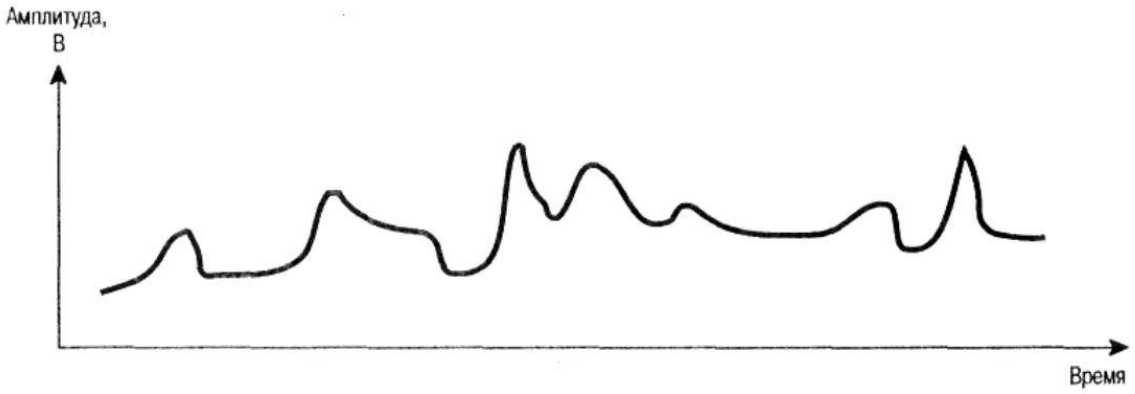

Рисунок 3 – Аналоговый сигнал

В системе связи информация передается от одной точки к другой путем передачи электрических сигналов. Аналоговый сигнал это последовательно модифицирующаяся электромагнитная волна, которая имеет свойство передаваться через различные среды, все зависит от частотных характеристик; для

примеров этих сред можно привести проводные линии (коаксиальный кабель, витая пара, оптоволокно). Также аналоговый сигнал имеет свойство распространения в атмосфере и космическом пространстве.

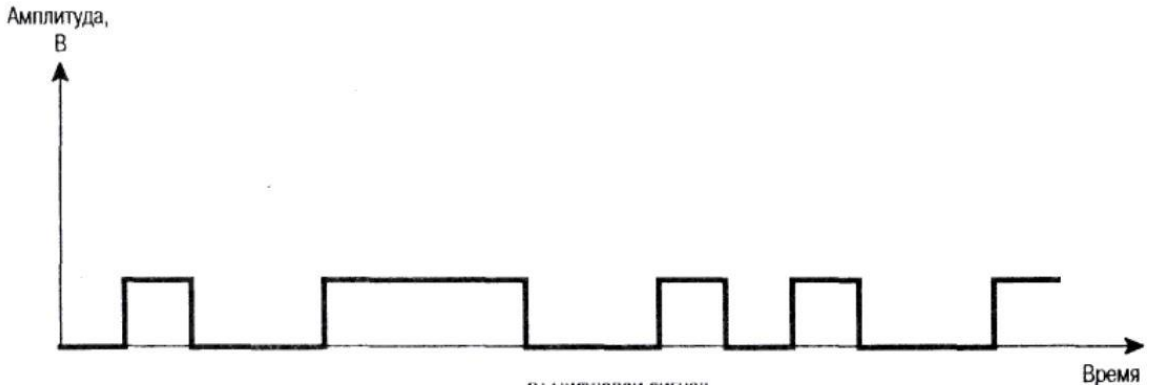

Рисунок 4 – Цифровой сигнал

Цифровой сигнал можно охарактеризовать, как некоторая последовательность импульсов напряжения, которые, также как и аналоговые сигналы, могут передаваться по проводной линии. Постоянный положительный уровень напряжения используется для представления двоичного нуля, а постоянный отрицательный уровень – для представления двоичной единицы.

В беспроводной технологии используются цифровые данные и аналоговые сигналы, так как цифровые сигналы быстрее затухают, чем аналоговые. Всегда передающиеся данные в цифровом формате можно отобразить аналоговыми сигналами, используя устройство модем (модулятор/демодулятор). В модеме происходит преобразование некоторой последовательности двоичных (двоичный нуль и двоичная единица) импульсов напряжения в сигнал аналогово формата, модулируя их с определенной частотой. Результирующий сигнал использует конкретный набор частот с серединой на определенной частоте и может передаваться во внешнюю среду. Для получения информации на конце канала связи следующий модем адаптер обратно преобразовывает, демодулирует сигнал и воссоздаёт первоначальные данные.

В ходе работы мы будем рассматривать международный стандарт IEEE (Institute of Electrical and Electronics Engineers – Институт электрики и электроники инженеров) 802.11 и его расширения, а он подразумевает распростра-

нение сигнала методом излучения радиоволн в диапазоне высоких частот от 2,402 ГГЦ до 2,482 ГГц. Как показано на рисунке 5, ширина пропускания имеет больше десяти каналов для использования передачи данных, регулируемых правительством стран или законодательством, которые используют беспроводную связь стандарта 802.11.

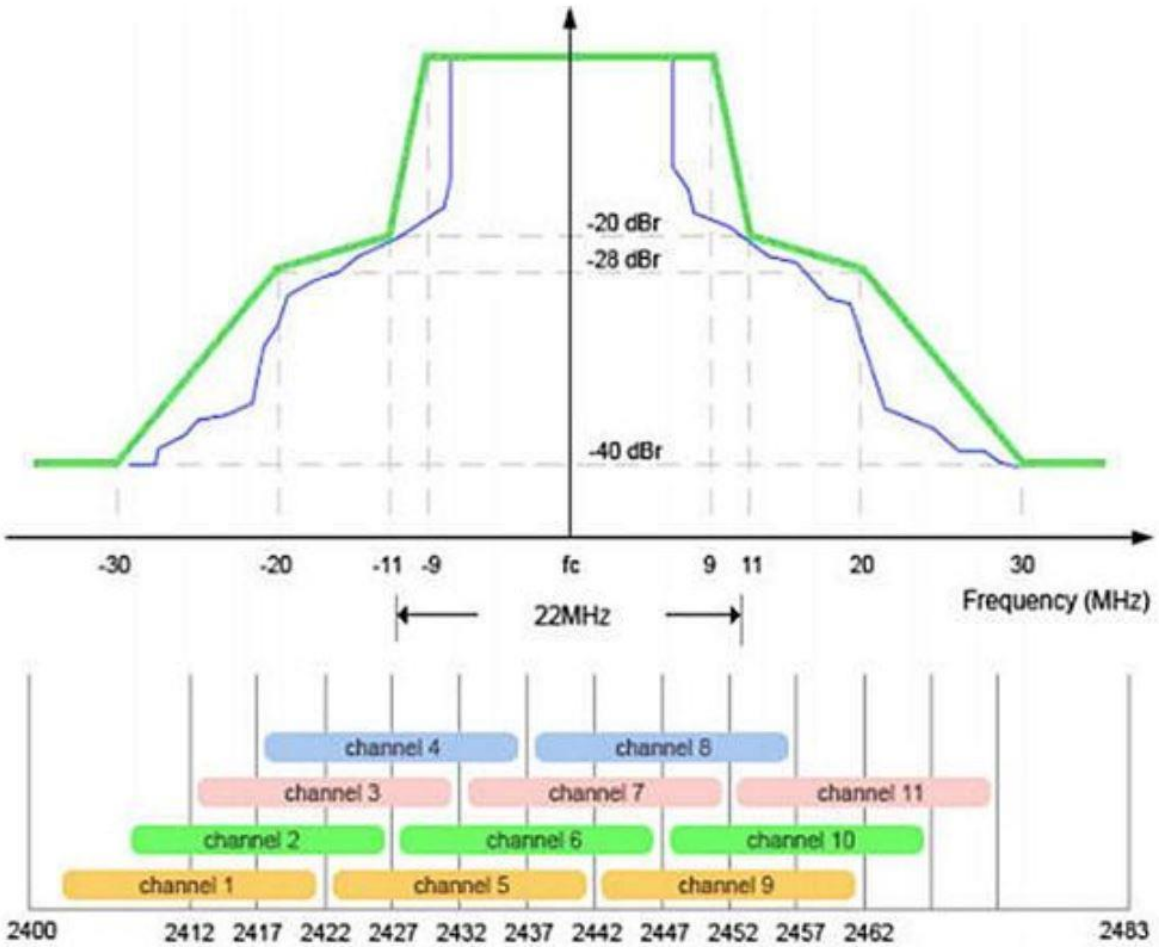

Рисунок 5 – Распределение каналов в высокочастотном диапазоне ширины пропускания

По причине, что каналы накладываются, они интерферируют между собой, и поэтому, полоса пропускания минимизируется. Для инфокоммуникационных систем с большим числом абонентов, а именно точек доступа, которые поддерживают сеть между абонентами, три точки, настроенные на 2, 6 и 10 каналы, не будут накладываться. Многоиспользуемые системы требуется настраивать так, чтобы помехи минимизировались и сводились к нулю. Как альтернатива, можно работать в спектре с большим числом каналов связи.

2.2 Стандарт IEEE 802.11

Стандарт 802.11 Wi-Fi на передачу по беспроводным каналам связи данных, скорость которых 1 и 2 Мбит/с в спектре частот 2,4 ГГц был принят в 1997 году. После принятия в 1999 году стандарта 802.11b в этом спектре передачи данных повысилась до 11 Мбит/с. 802.11a и 802.11g устанавливают предельную передачу данных на скорости 54 Мбит/с в спектре частот 5 ГГц.

Развитие стандарта 802.11 имеет большие перспективы, так как все больше и больше людей отдает ему предпочтение, например сотрудники организаций, могут оставаться в сети, выйдя за пределы своих офисов. Стандарт WiFi сейчас стал «по умолчанию» для всех моделей мобильных устройств связи. В настоящее время очень широко популярны сетевые карты для ПК, позволяющие работать со скоростями от 1 до 54 Мбит/с в обоих частотных диапазонах (2,4 и 5 ГГц) при стоимости меньшей, чем большинство людей платят за мобильный телефон. В настоящее время разрабатываются новые расширения этого стандарта, которые повысят защищенность, обеспечат поддержку стандарта на качество услуг передачи данных (QoS), улучшат управляемость и повысят скорость передачи данных до уровня, превышающего 100 Мбит/с.

Таким образом, на сегодняшний день большинство цифровых систем передачи информации, в частности, беспроводные локальные сети (WLAN – Wireless Local Area Network), строятся на основе стандартов 802.11, разрабатываемых рабочими группами IEEE. Это семейство стандартов специфицирует физический уровень (PHY - Physical level) и уровень управления доступом к среде передачи данных MAC. Рассматривая общепринятую модель OSI на рисунке 6, стандарт IEEE 802.11 b/g/n соответствует двум низшим уровням модели.

На физическом уровне определены два широкополосных радиочастотных метода передачи. Технологии широкополосного сигнала, используемые в радиочастотных методах, увеличивают надежность сигнала, пропускную способность, позволяют многим несвязанным друг с другом устройствам разде-

лять одну полосу частот с минимальными помехами друг для друга.

В свою очередь канальный уровень 802.11 состоит из двух подуровней: управления логической связью (Logical Link Control, LLC) и управления доступа к носителю (MAC).

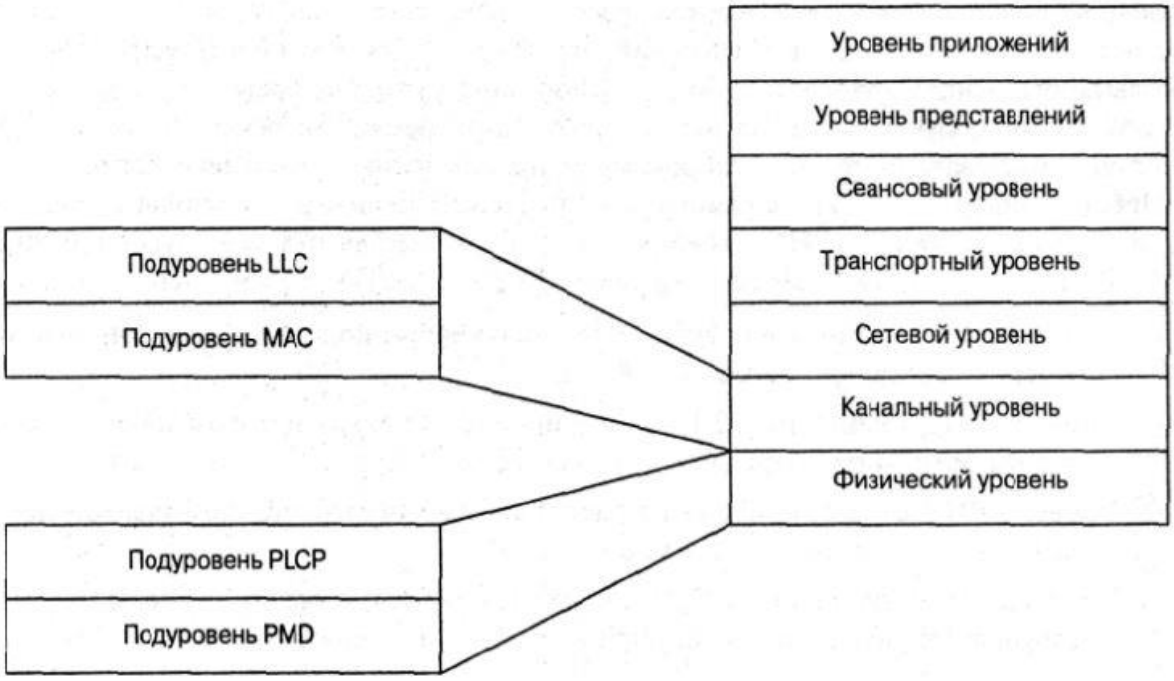

Рисунок 6 – Модель OSI для стандарта 802.11

Набор стандартов 802.11определяет целый ряд технологий реализации физического уровня, которые могут быть использованы подуровнем 802.11 MAC. К этому набору относятся:

– физический уровень стандарта 802.11 со скачкообразной перестройкой частоты (frequency hopping) в диапазоне 2,4 ГГц;

– физический уровень стандарта 802.11 с расширением спектра методом прямой последовательности (direct sequence) в диапазоне 2,4 ГГц;

– физический уровень стандарта 802.11b с расширением спектра методом прямой последовательности в диапазоне 2,4 ГГц.

– расширенный физический уровень (extended rate physical (ERP) layer) стандарта 802.11g в диапазоне 2,4 ГГц;

– физический уровень стандарта 802.11 с разделением по ортогональным частотам (orthogonal frequency division multiplexion, OFDM) в диапазоне 2,4

ГГц.

Основное назначение физических уровней стандарта 802.11 – обеспечить механизмы беспроводной передачи для подуровня MAC, а также поддерживать выполнение вторичных функций, таких как оценка состояния беспроводной среды и сообщение о нем подуровню MAC. Уровни MAC и PHY разрабатывались так, чтобы они были независимыми. Именно независимость между MAC и подуровнем PHY и позволила использовать дополнительные высокоскоростные физические уровни, описанные в стандартах 802.11b/g/n.

Каждый из физических уровней стандарта 802.11 и имеет два подуровня:

– Physical Layer Convergence Procedure (PLCP). Процедура определения состояния физического уровня;

– Physical Medium Dependent (PMD). Подуровень физического уровня, зависящий от среды передачи.

Исходный стандарт 802.11 определяет три метода передачи на физическом уровне:

– передача в диапазоне инфракрасных волн;

– технология расширения спектра путем скачкообразной перестройки частоты (FHSS) в диапазоне 2,4 ГГц;

– технология широкополосной модуляции с расширением спектра методом прямой последовательности (DSSS) в диапазоне 2,4 ГГц.

Передача в диапазоне инфракрасных волн. Средой передачи являются инфракрасные волны диапазона 850 нм, которые генерируются либо полупроводниковым лазерным диодом, либо светодиодом (LED). Так как инфракрасные волны не проникают через стены, область покрытия LAN ограничивается зоной прямой видимости. Стандарт предусматривает три варианта распространения излучения: всенаправленную антенну, отражение от потолка и фокусное направленное излучение. В первом случае узкий луч рассеивается с помощью системы линз. Фокусное направленное излучение предназначено для организации двухточечной связи, например, между двумя зданиями.

Беспроводные локальные сети со скачкообразной перестройкой частоты (FHSS). Беспроводные локальные сети FHSS поддерживают скорости передачи 1 и 2 Мбит/с. Устройства FHSS делят предназначенную для их работы полосу частот от 2,402 до 2,482 ГГц на 79 неперекрывающихся каналов (это справедливо для Северной Америки и большей части Европы). Ширина каждого из 79 каналов составляет 1 МГц, поэтому беспроводные локальные сети FHSS используют относительно высокую скорость передачи символов, 1 МГц, и на много меньшую скорость перестройки с канала на канал. Последовательность перестройки частоты должна иметь следующие параметры: частота перескоков не менее 2,5 раз в секунду как минимум между 6-ю (6 МГц) каналами. Чтобы минимизировать число коллизий между перекрывающимися зонами покрытия, возможные последовательности перескоков должны быть разбиты на три набора последовательностей, длина которых для Северной Америки и большей части Европы составляет 26. В таблице 1 представлены схемы скачкообразной перестройки частоты, обеспечивающие минимальное перекрытие.

Таблица 1 – Результаты тестирования надёжности программного продукта

Набор	Схема скачкообразной перестройки системы
1	{0,3,6,9,12,15,18,21,24,27,30,33,36,39,42,48,51,54,57,60,63,66,69,72}
2	{1,4,7,10,13,16,19,22,25,28,31,34,37,40,43,46,49,52,55,58,61,64,67,70}
3	{2,5,8,11,14,47,20,23,26,29,32,35,38,41,44,47,50,53,56,59,62,65,68,71}

По сути, схема скачкообразной перестройки частоты обеспечивает неторопливый переход с одного возможного канала на другой таким образом, что после каждого скачка покрывается полоса частот, равная как минимум 6 МГц, благодаря чему во много сотовых сетях минимизируется возможность возник-

новения коллизий.

После того как уровень MAC пропускает MAC-фрейм, который в локальных беспроводных сетях FHSS называется также служебный элемент данных PLCCP, или PSDU (PLCP Service Data Unit), подуровень PLCP добавляет два поля в начало фрейма, чтобы сформировать таким образом фрейм PPDU (PPDU – элемент данных протокола PLCP).

На рисунке 7 представлен формат фрейма FHSS подуровня PLCP.

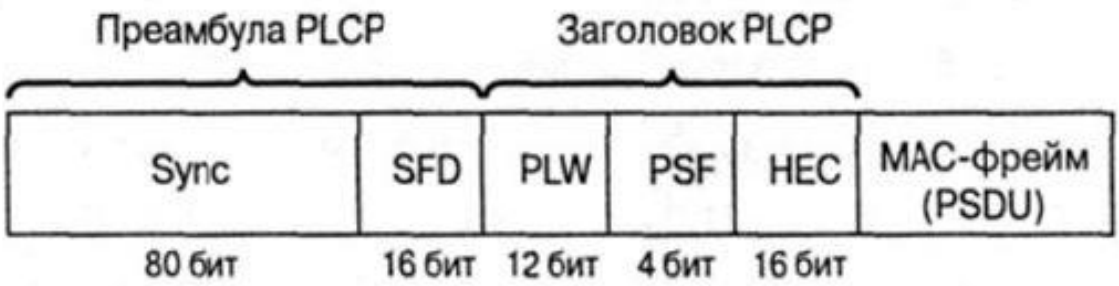

Рисунок 7 – Формат фрейма FHSS подуровня PLCP

Беспроводные локальные сети, использующие широкополосную модуляцию DSSSS с расширением спектра методом прямой последовательности. В спецификации стандарта 802.11 оговорено использование и другого физического уровня – на основе технологии широкополосной модуляции с расширением спектра методом прямой последовательности (DSSS). Как было указанно в стандарте 802.11 разработки 1997 года, технология DSSS поддерживает скорости передачи 1 и 2 Мбит/с. Аналогично подуровню PLCP, используемому в технологии FHSS, подуровень PLLCP технологии DSSS стандарта 802.11 добавляет два поля во фрейм MAC, чтобы сформировать PPDU: преамбулу PLLCP и заголовок PLCP. Формат фрейма представлен на рисунке 8.

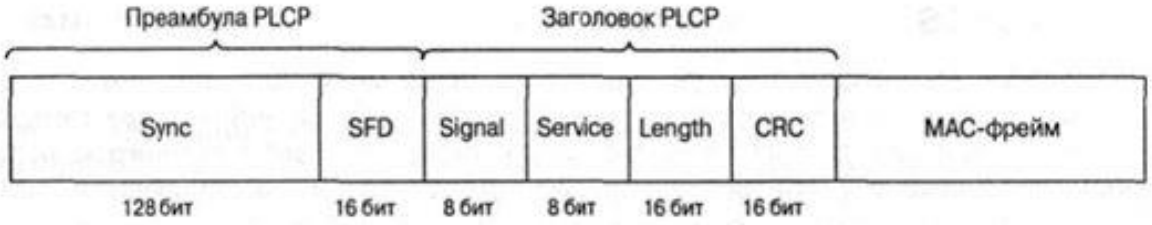

Рисунок 8 – Формат фрейма DSS подуровня PLCP

Подуровень PLCP преобразует фрейм в поток битов и передает данные на подуровень PMMD. Весь PPDU проходит через процесс скремблирования с целью рандомизации данных.

2.3 Технология шифрования

2.3.1 WEP-шифрование

WEP-шифрование (Wired Equivalent Privacy, уровень проводной связи под секретом) использующийся алгоритм RC4 (Rivest Cipher v.4, кодтровка Ривеста), представляет симметричное шифрование. Для нормального обмена пользовательскими данными ключи шифрования у абонента и точки радиодоступа должны быть идентичными.

Ядро алгоритма состоит из функции генерации ключевого потока. Эта функция генерирует последовательность битов, которая затем объединяется с открытым текстом посредством суммирования по модулю два. Дешифрация состоит из регенерации этого ключевого потока и суммирования его с шифрограммой по модулю два, восстанавливая исходный текст. Другая главная часть алгоритма − функция инициализации, которая использует ключ переменной длины для создания начального состояния генератора ключевого потока.

RC4 – фактически класс алгоритмов, определяемых размером его блока. Этот параметр n является размером слова для алгоритма. Обычно, n = 8, но в целях анализа можно уменьшить его. Однако для повышения безопасности необходимо увеличить эту величину. Внутреннее состояние RC4 состоит из массива размером 2n слов и двух счетчиков, каждый размером в одно слово. Массив известен как S-бокс, и далее будет обозначаться как S. Он всегда содержит перестановку 2n возможных значений слова. Два счетчика обозначены через i и j.

Алгоритм инициализации RC4 приведен ниже.

Этот алгоритм использует ключ, сохраненный в Key, и имеющий длину l байт. Инициализация начинается с заполнения массива S, далее этот массив перемешивается путем перестановок определяемых ключом. Так как только одно

действие выполняется над S, то должно выполняться утверждение, что S всегда содержит все значения кодового слова.

1) Начальное заполнение массива:

for i = 0 to 2n – 1

{

S[i] = i

j = 0

}

2) Скремблирование:

for i = 0 to 2n − 1

{

j = j + S[i] + Key[i mod l]

Перестановка (S[i], S[j])

}

Генератор ключевого потока RC4 переставляет значения, хранящиеся в S, и каждый раз выбирает различное значение из S в качестве результата. В одном цикле RC4 определяется одно n-битное слово K из ключевого потока, которое в последующем суммируется с исходным текстом для получения зашифрованного текста.

3) Инициализация:

i = 0

j = 0

4) Цикл генерации:

i = i + 1

j = j + S[i]

Перестановка (S[i], S[j])

Результат: K = S[S[i] + S[j]].

Особенности WEP-протокола:

− достаточно устойчив к атакам, связанным с простым перебором клю-

чей шифрования, что обеспечивается необходимой длиной ключа и частотой смены ключей и инициализирующего вектора;

− самосинхронизация для каждого сообщения. Это свойство является ключевым для протоколов уровня доступа к среде передачи, где высок уровень искажённых и потерянных пакетов;

− WEP может быть легко реализован;

− открытость;

− использование WEP-шифрования не является обязательным в сетях стандарта IEEE 802.11.

Для непрерывного шифрования потока данных используется потоковое и блочное шифрование.

При потоковом шифровании выполняется побитовое сложение по модулю 2 (функция “исключающее ИЛИ“, XOR) ключевой последовательности, генерируемой алгоритмом шифрования на основе заранее заданного ключа, и исходного сообщения. Ключевая последовательность имеет длину, соответствующую длине исходного сообщения, подлежащего шифрованию, как показано на рисунке 9.

Блочное шифрование работает с блоками заранее определенной длины, не меняющейся в процессе шифрования.

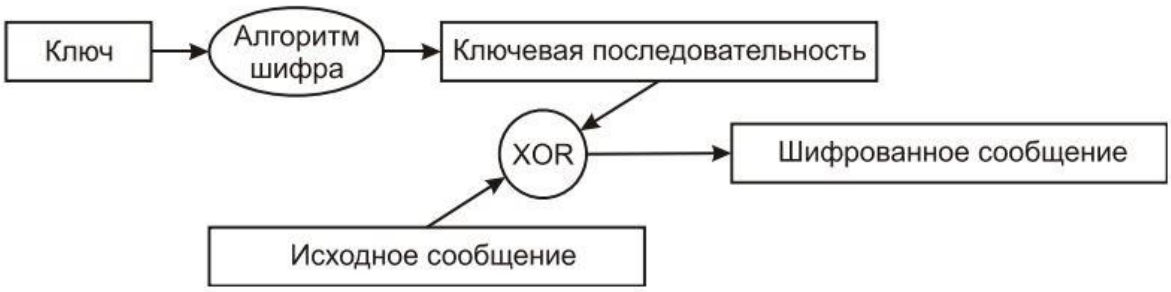

Рисунок 9 – Потоковое шифрование

Исходное сообщение фрагментируется на блоки, и функция XOR вычисляется над ключевой последовательностью и каждым блоком. Размер блока фиксирован, а последний фрагмент исходного сообщения дополняется пустыми символами до длины нормального блока, как показано на рисунке 10.

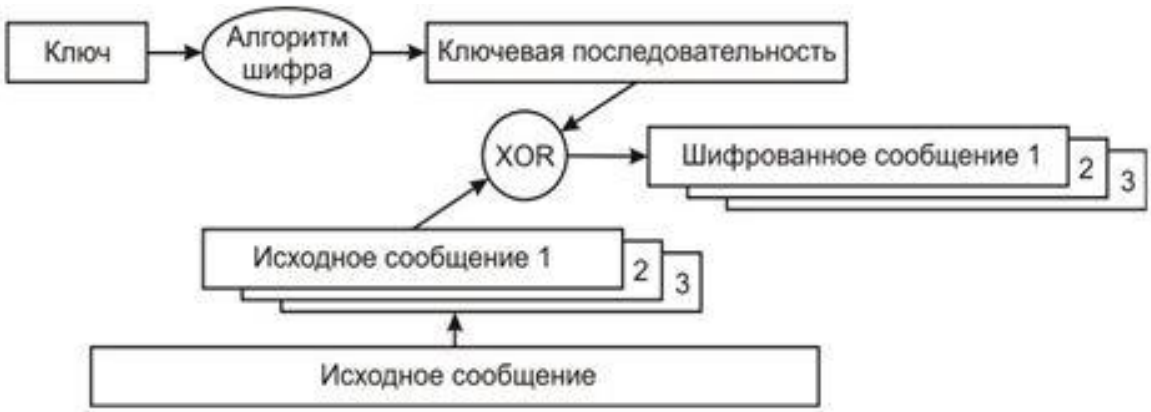

Рисунок 10 – Блочное шифрование

Потоковое шифрование и блочное шифрование используют метод электронной кодовой книги (ECB). Метод ECB характеризуется тем, что одно и то же исходное сообщение на входе всегда порождает одно и то же зашифрованное сообщение на выходе. Это представляет собой потенциальную брешь в системе безопасности, ибо сторонний наблюдатель, обнаружив повторяющиеся последовательности в зашифрованном сообщении, в состоянии сделать обоснованные предположения относительно идентичности содержания исходного сообщения.

Для устранения указанной проблемы используют:

1) векторы инициализации (Initialization Vectors, IVs);

2) обратную связь (feedback modes).

До начала процесса шифрования 40- или 104-битный секретный ключ распределяется между всеми станциями, входящими в беспроводную сеть. К секретному ключу добавляется вектор инициализации (IV).

Вектор инициализации используется для модификации ключевой последовательности. При использовании вектора инициализации ключевая последовательность генерируется алгоритмом шифрования, на вход которого подаётся секретный ключ, совмещённый с IV. При изменении вектора инициализации ключевая последовательность также меняется. На рисунке 11 исходное сообщение шифруется с использованием новой ключевой последовательности, сгенерированной алгоритмом шифрования после подачи на его вход комбинации

Рисунок 11 – Шифрование с использованием вектора инициализации

Стандарт IEEE 802.11 рекомендует использование нового значения вектора инициализации для каждого нового фрейма, передаваемого в радиоканал. Таким образом, один и тот же нешифрованный фрейм, передаваемый многократно, каждый раз будет порождать уникальный шифрованный фрейм.

Вектор инициализации имеет длину 24 бита и совмещается с 40- или 104-битовым базовым ключом шифрования WEP, таким образом, что на вход алгоритма шифрования подается 64- или 128-битовый ключ.

Вектор инициализации присутствует в нешифрованном виде в заголовке фрейма в радиоканале, с тем, чтобы принимающая сторона могла успешно декодировать этот фрейм.

Несмотря на то, что обычно говорят об использовании шифрования WEP с ключами длиной 64 или 128 битов, эффективная длина ключа составляет лишь 40 или 104 бита по причине передачи вектора инициализации в нешифрованном виде.

При настройках шифрования в оборудовании при 40-битном эффективном ключе вводятся 5 байтовых ASCII-символов (5·8=40) или 10 шестнадцатеричных чисел (10·4=40), и при 104-битном эффективном ключе вводятся 13 байтовых ASCII-символов (13·8=104) или 26 шестнадцатеричных чисел (26·4=104). Некоторое оборудование может работать со 128-битным ключом.

WEP-шифрование с обратной связью модифицируют процесс шифрования и предотвращают порождение одним и тем же исходным сообщением одного и того же шифрованного сообщения.

Обратная связь обычно используется при блочном шифровании. Наибо-

лее часто встречается тип обратной связи, известный как цепочка шифрованных блоков (CBC).

В основе использования цепочки шифрованных блоков лежит идея вычисления двоичной функции XOR между блоком исходного сообщения и предшествовавшим ему блоком шифрованного сообщением.

Поскольку самый первый блок не имеет предшественника, для модификации ключевой последовательности используют вектор инициализации.

Работа цепочки шифрованных блоков представлена на рисунке 12.

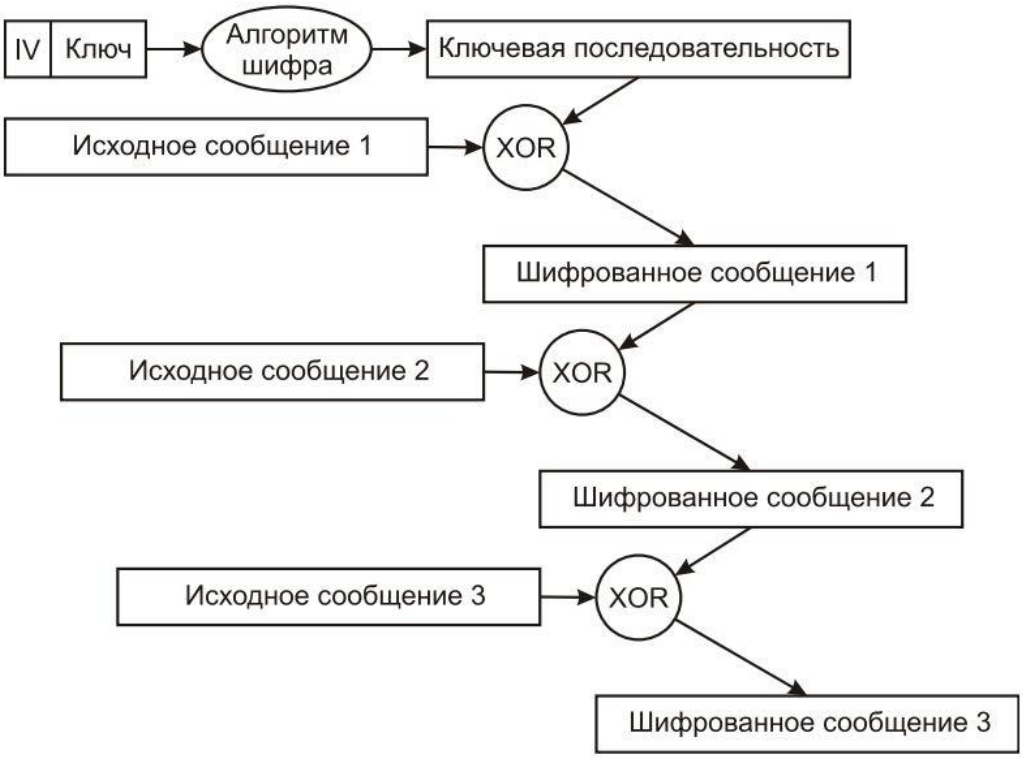

Рисунок 12 – Шифрование с обратной связью

2.3.2 Аутентификация стандарта 802.11

Стандарт IEEE 802.11 с традиционной безопасностью (Tradition Security Network, TSN) предусматривает два механизма аутентификации беспроводных абонентов: *открытую аутентификацию* (Open Authentication) и *аутентификацию с общим ключом* (Shared Key Authentication). В аутентификации в беспроводных сетях также широко используются два других механизма выходящих за рамки стандарта 802.11, а именно назначение *идентификатора беспроводной локальной сети* (Service Set Identifier, SSID) и *аутентификация абонента по*

его MAC-адресу.

Идентификатор беспроводной локальной сети (SSID) представляет собой атрибут беспроводной сети, позволяющий логически отличать сети друг от друга. В общем случае, абонент беспроводной сети должен задать у себя соответствующий SSID для того, чтобы получить доступ к требуемой беспроводной локальной сети. SSID ни в коей мере не обеспечивает конфиденциальность данных, равно как и не аутентифицирует абонента по отношению к точке радиодоступа беспроводной локальной сети. Существуют точки доступа позволяющие разделить абонентов подключаемых к точке на несколько сегментов, это достигается тем, что точка доступа может иметь не один, а несколько SSID.

Аутентификация в стандарте IEEE 802.11 ориентирована на аутентификацию абонентского устройства радиодоступа, а не конкретного абонента как пользователя сетевых ресурсов. На рисунке 13 процесс аутентификации абонента беспроводной локальной сети IEEE 802.11 состоит из следующих этапов:

1) абонент посылает фрейм Probe Request во все радиоканалы;

2) каждая точка радиодоступа, в зоне радиовидимости которой находится абонент, посылает в ответ фрейм Probe Response;

3) абонент выбирает предпочтительную для него точку радиодоступа и посылает в обслуживаемый ею радиоканал запрос на аутентификацию (Authentication Request);

4) точка радиодоступа посылает в свое подтверждение аутентификации (Authentication Reply);

5) в случае успешной аутентификации абонент посылает точке радиодоступа фрейм ассоциации (Association Request);

6) точка радиодоступа посылает в ответ фрейм подтверждения ассоциации (Association Response);

7) абонент может теперь осуществлять обмен пользовательским трафиком с точкой радиодоступа и проводной сетью.

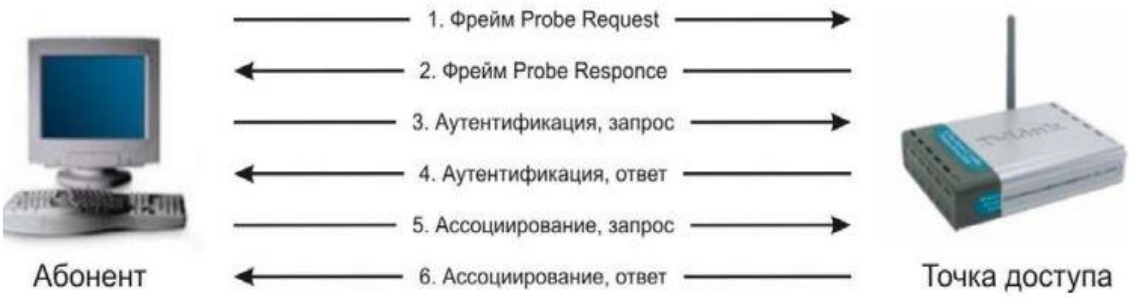

Рисунок 13 – Аутентификация по стандарту 802.11

При активизации, беспроводный абонент начинает поиск точек радиодоступа в своей зоне радиовидимости с помощью управляющих фреймов Probe Request. Фреймы Probe Request посылаются в каждый из радиоканалов, поддерживаемых абонентским радиоинтерфейсом, в попытке найти все точки радиодоступа с требуемыми клиенту идентификатором SSID и поддерживаемыми скоростями радиообмена. Каждая точка радиодоступа из находящихся в зоне радиовидимости абонента и удовлетворяющая запрашиваемым во фрейме Probe Request параметрам отвечает фреймом Probe Response, содержащем синхронизирующую информацию и данные о текущей загрузке точки радиодоступа. Абонент определяет, с какой точкой радиодоступа он будет работать, путем сопоставления поддерживаемых ими скоростей радиообмена и загрузки. После того, как предпочтительная точка радиодоступа определена, абонент переходит в фазу аутентификации.

Открытая аутентификация, по сути, не является алгоритмом аутентификации в привычном понимании. Точка радиодоступа удовлетворит любой запрос открытой аутентификации. На первый взгляд, использование этого алгоритма может показаться бессмысленным, однако следует учитывать, что разработанные в 1997 году методы аутентификации IEEE 802.11 ориентированы на быстрое логическое подключение к беспроводной локальной сети. Вдобавок к этому, многие IEEE 802.11-совместимые устройства представляют собой портативные блоки сбора информации (сканеры штрих-кодов и т. п.), не имеющие достаточной процессорной мощности, требующейся для реализации сложных

алгоритмов аутентификации.

В процессе открытой аутентификации происходит обмен сообщениями двух типов:

– запрос аутентификации (Authentication Request);

– подтверждение аутентификации (Authentication Response).

Таким образом, при открытой аутентификации возможен доступ любого абонента к беспроводной локальной сети. Если в беспроводной сети не используется шифрование, то любой абонент, знающий идентификатор SSID точки радиодоступа, получит доступ к сети. При использовании точками радиодоступа шифрования WEP сами ключи шифрования становятся средством контроля доступа. Если абонент не располагает корректным WEP-ключом, то даже в случае успешной аутентификации он не сможет ни передавать данные через точку радиодоступа, ни расшифровывать данные, переданные точкой радиодоступа.

Аутентификация с общим ключом является вторым методом аутентификации стандарта IEEE 802.11. Аутентификация с общим ключом требует настройки у абонента статического ключа шифрования WEP. Процесс аутентификации разбит на следующие этапы:

1) абонент посылает точке радиодоступа запрос аутентификации, указывая при этом необходимость использования режима аутентификации с общим ключом;

2) точка радиодоступа посылает подтверждение аутентификации, содержащее Challenge Text;

3) абонент шифрует Challenge Text своим статическим WEP-ключом, и посылает точке радиодоступа запрос аутентификации;

4) если точка радиодоступа в состоянии успешно расшифровать запрос аутентификации и содержащийся в нем Challenge Text, она посылает абоненту подтверждение аутентификации, таким образом предоставляя доступ к сети.

Аутентификация абонента по его MAC-адресу не предусмотрена стандартом IEEE 802.11, однако поддерживается многими производителями обору-

дования для беспроводных сетей, в том числе D-Link. При аутентификации по MAC-адресу происходит сравнение MAC-адреса абонента либо с хранящимся локально списком разрешенных адресов легитимных абонентов, либо с помощью внешнего сервера аутентификации. Аутентификация по MAC-адресу используется в дополнение к открытой аутентификации и аутентификации с общим ключом стандарта IEEE 802.11 для уменьшения вероятности доступа посторонних абонентов.

2.3.3 WPA-шифрование

До мая 2001 г. стандартизация средств информационной безопасности для беспроводных сетей 802.11 относилась к ведению рабочей группы IEEE 802.11e, но затем эта проблематика была выделена в самостоятельное подразделение. Разработанный стандарт 802.11i призван расширить возможности протокола 802.11, предусмотрев средства шифрования передаваемых данных, а также централизованной аутентификации пользователей и рабочих станций.

Основные производители Wi-Fi-оборудования в лице организации WECA (Wireless Ethernet Compatibility Alliance), иначе именуемой Wi-Fi Alliance, устав ждать ратификации стандарта IEEE 802.11i, совместно с IEEE в ноябре 2002 г. анонсировали спецификацию Wi-Fi Protected Access (WPA), соответствие которой обеспечивает совместимость оборудования различных производителей.

Новый стандарт безопасности WPA обеспечивает уровень безопасности куда больший, чем может предложить WEP. Он перебрасывает мостик между стандартами WEP и 802.11i и имеет то преимущество, что микропрограммное обеспечение более старого оборудования может быть заменено без внесения аппаратных изменений.

IEEE предложила временный протокол целостности ключа (Temporal Key Integrity Protocol, TKIP).

Основные усовершенствования, внесенные протоколом TKIP:

– пофреймовое изменение ключей шифрования. WEP – ключ быстро изменяется, и для каждого фрейма он другой;

− контроль целостности сообщения. Обеспечивается эффективный контроль целостности фреймов данных с целью предотвращения проведения тайных манипуляций с фреймами и воспроизведения фреймов;

− усовершенствованный механизм управления ключами.

Атаки, применяемые в WEP, использующие уязвимость слабых IV (Initialization Vectors), таких, которые применяются в приложении AirSnort, основаны на накоплении нескольких фреймов данных, содержащих информацию, зашифрованную с использованием слабых IV. Простейшим способом сдерживания таких атак является изменение WEP-ключа, используемого при обмене фреймами между клиентом и точкой доступа, до того как атакующий успеет накопить фреймы в количестве, достаточном для вывода битов ключа.

IEEE адаптировала схему, известную как пофреймовое изменение ключа (per-frame keying). Основной принцип, на котором основано пофреймовое изменение ключа, состоит в том, что IV, MAC-адрес передатчика и WEP-ключ обрабатываются вместе с помощью двухступенчатой функции перемешивания. Результат применения этой функции соответствует стандартному 104-разрядному WEP-ключу и 24-разрядному IV.

IEEE предложила также увеличить 24-разрядный вектор инициализации до 48-разрядного IV.

На рисунке 14 представлен образец 48-разрядного IV и показано, как этот IV разбивается на части для использования при пофреймовом изменении ключа.

Рисунок 14 – Разбиение 48-и разрядного вектора инициализации

Процесс пофреймового изменения ключа представлен на рисунке 15, где отображены следующие этапы:

1) базовый WEP-ключ перемешивается со старшими 32 разрядами 48-разрядного IV и MAC-адресом передатчика. Результат этого действия называется ключ 1-й фазы. Этот процесс позволяет занести ключ 1-й фазы в кэш и также напрямую поместить в ключ;

2) ключ 1-й фазы снова перемешивается с IV и MAC-адресом передатчика для выработки значения пофреймового ключа;

3) вектор инициализации (IV), используемый для передачи фрейма, имеет размер только 16 бит (16-разрядные числа могут принимать значения 0-65 535). Оставшиеся 8 бит (в стандартном 24-битовом IV) представляют фиксированное значение, используемое как заполнитель;

4) пофреймовый ключ используется для WEP-шифрования фрейма данных;

5) когда 16-битовое пространство IV оказывается исчерпанным, ключ 1-й фазы отбрасывается и 32 старших разряда увеличиваются на 1;

6) значение пофреймового ключа вычисляется заново, как на этапе 2.

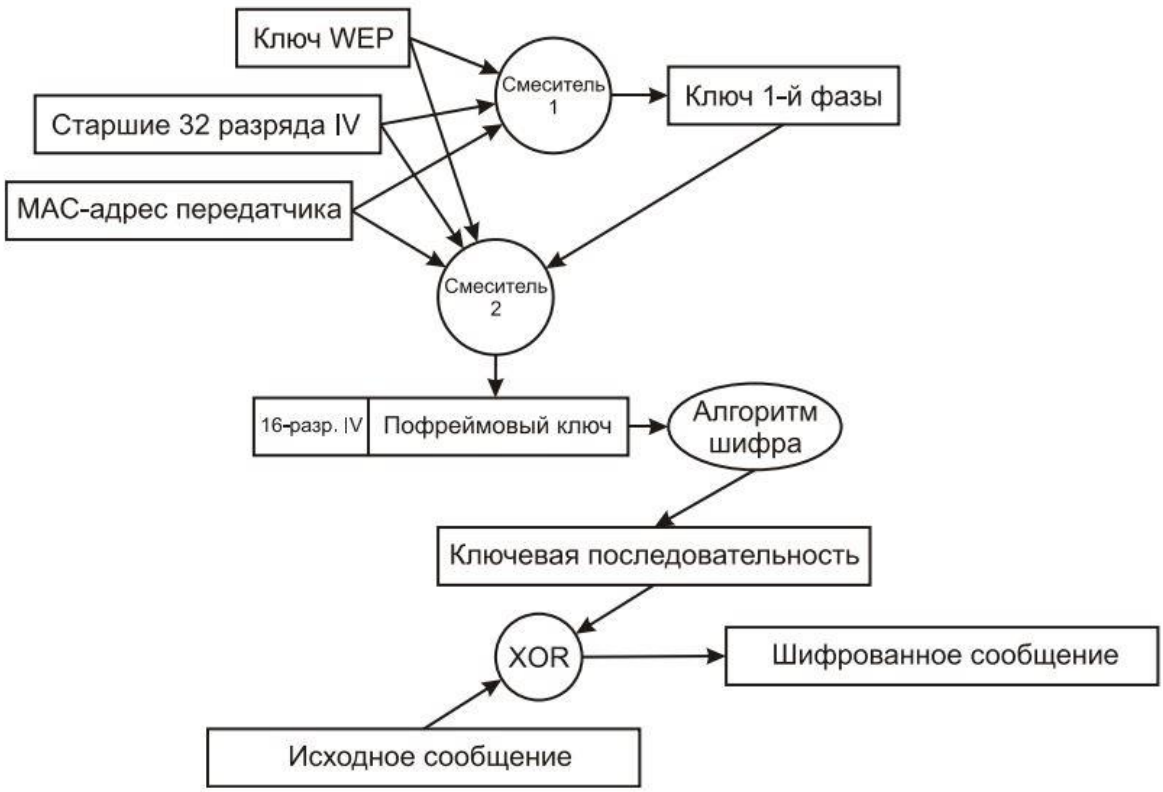

Рисунок 15 – Процесс создания шифрованного сообщения в WPA

Процесс пофреймового изменения ключа можно разбить на следующие этапы.

Устройство инициализирует IV, присваивая ему значение 0. В двоичном представлении это будет значение из 32-х нулей.

Первые 32 разряда IV (в рассматриваемом случае – первые 32 нуля) перемешиваются с WEP-ключом (например, имеющим 128-разрядное значение) и MAC-адресом передатчика (имеющим 48-разрядное значение) для получения значения ключа 1-й фазы (80-разрядное значение).

Ключ 1-й фазы вновь перемешивается с первыми (старшими) 32 разрядами IV и MAC-адресом передатчика, чтобы получить 128-разрядный пофреймовый ключ, первые 16 разрядов которого представляют собой значение IV (16 нулей).

Вектор инициализации пофреймового ключа увеличивается на 1. После того как пофреймовые возможности IV будут исчерпаны, IV 1-й фазы (32 бита) увеличивается на 1 (он теперь будет состоять из 31 нуля и одной единицы) и т.д.

Этот алгоритм усиливает WEP до такой степени, что почти все известные сейчас возможности атак устраняются без замены существующего оборудования. Следует отметить, что этот алгоритм (и TKIP в целом) разработан с целью убрать бреши в системе аутентификации WEP и стандарта 802.11. Он жертвует слабыми алгоритмами, вместо того чтобы заменять оборудование.

2.3.4 WPA2-шифрование

В июне 2004 г. IEEE ратифицировал стандарт обеспечения безопасности в беспроводных локальных сетях − 802.11i.

Созданный с учетом слабых мест WEP, он представляет собой очень надежную систему безопасности, и обратно совместим с большинством существующего Wi-Fi-оборудования. WPA – практическое решение, обеспечивающее более чем адекватную безопасность для беспроводных сетей.

Однако WPA, в конце концов, компромиссное решение. Оно все еще ос

новано на алгоритме шифрования RC4 и протоколе TKIP. Хотя и малая, но все же имеется вероятность открытия каких-либо слабых мест.

Абсолютно новая система безопасности, целиком лишенная брешей WEP, представляет собой лучшее долгосрочное и к тому же расширяемое решение для безопасности беспроводных сетей. С этой целью комитет по стандартам принял решение разработать систему безопасности с нуля. Это новый стандарт 802.11i, также известный как WPA2 и выпущенный тем же Wi-Fi Alliance.

Стандарт 802.11i использует концепцию повышенной безопасности (Robust Security Network, RSN), предусматривающую, что беспроводные устройства должны обеспечивать дополнительные возможности. Это потребует изменений в аппаратной части и программном обеспечении, т.е. сеть, полностью соответствующая RSN, станет несовместимой с существующим оборудованием WEP. В переходный период будет поддерживаться как оборудование RSN, так и WEP (на самом деле WPA/TKIP было решением, направленным на сохранение инвестиций в оборудование), но в дальнейшем устройства WEP будут отмирать.

802.11i приложим к различным сетевым реализациям и может задействовать TKIP, но по умолчанию RSN использует AES (Advanced Encryption Standard) и CCMP (Counter Mode CBC MAC Protocol) и, таким образом, является более мощным расширяемым решением.

RSN определяет иерархию ключей с ограниченным сроком действия, сходную с TKIP. В AES/CCMP, чтобы вместить все ключи, требуется 512 бит – меньше, чем в TKIP. В обоих случаях мастер-ключи используются не прямо, а для вывода других ключей. К счастью, администратор должен обеспечить единственный мастер-ключ. Сообщения составляются из 128-битного блока данных, зашифрованного секретным ключом такой же длины (128 бит). Хотя процесс шифрования сложен, администратор опять-таки не должен вникать в нюансы вычислений. Конечным результатом является шифр, который гораздо сложнее, чем даже WPA.

WPA2 – это наиболее устойчивое, расширяемое и безопасное решение, предназначенное в первую очередь для больших предприятий, где управление ключами и администрирование были первой проблемой.

Производительность канала связи, как свидетельствуют результаты тестирования оборудования различных производителей, падает на 5-20% при включении как WEP, так и WPA. Однако испытания того оборудования, в котором включено шифрование AES вместо TKIP, не показали сколько-нибудь заметного падения скорости. Это позволяет надеяться, что WPA2-совместимое оборудование предоставит нам долгожданный надежно защищенный канал без потерь в производительности. WPA2, так же как и WPA, может работать в двух режимах: Enterprise (корпоративный) и Pre-Shared Key (персональный).

2.4 Аппаратное обеспечение

2.4.1 Модуль вычисления

В качестве модуля вычисления должна быть высокопроизводительная вычислительная платформа, имеющая на борту характерный минимум для выполнения задач ПО. Основные составляющие вычислительной платформы отражены в следующем списке:

1) процессор – устройство, выполняющее арифметические и логические операции, и управляющее другими устройствами компьютера. В его состав входят: арифметико-логическое устройство, устройство управления, регистры;

2) оперативное запоминающее устройство – устройство хранения данных и команд для дальнейшей их передачи процессору на обработку;

3) постоянное запоминающее устройство − энергонезависимая память, используемая только для чтения, на которой хранится информация;

4) интерфейсы передачи данных – устройства, соединяющие внешние и внутренние части ПАК и обеспечивающие их взаимодействие;

5) блок питания − источник электрического тока для питания устройств вычислительной платформы.

2.4.2 Модуль передачи данных

Под модулем передачи данных будем понимать WiFi адаптер. Его будем использовать для реализации функции беспроводной сети в разработке ПАК. Он позволяет комплексу принимать и передавать сигнал как от беспроводной сети так и к ней. Сейчас существует два типа адаптеров: первые способны только принимать сигнал, вторые могут работать в режиме приема и в режиме передачи сигнала. Адаптеры, в которые встроена функция SoftAP, позволяют создать на своем компьютере точку доступа WiFi.

При выборе адаптера следует учитывать фактор расположенности относительно модуля вычисления, а именно, как будет подключаться адаптер, напрямую к плате или же через интерфейсы передачи данных. Следовательно, WiFi адаптеры бывают; внутренние и внешние, примеры изображены на рисунках 16 и 17.

Рисунок 16 – Внутренний WiFi адаптер

Рисунок 17 – Внешний WiFi адаптер

2.4.3 Устройство распространения сигнала

К устройствам распространения сигнала относят антенны и антенные комплексы, которые предназначены для излучения или приёма радиоволн.

Антенны в зависимости от назначения подразделяются на приёмные, передающие и приёмопередающие. Антенна в режиме передачи преобразует энергию поступающего от радиопередатчика электромагнитного колебания в распространяющуюся в пространстве электромагнитную волну. Антенна в режиме приёма преобразует энергию падающей электромагнитной волны в электромагнитное колебание, поступающее в радиоприёмник. Таким образом, антенна является преобразователем подводимого к ней по фидеру электромагнитного колебания (переменного электрического тока, канализированной в волноводе электромагнитной волны) в электромагнитное излучение и наоборот.

Для нашей работы будет интересна такая характеристика, как направленность. В зависимости от направленности, антенны можно разделить на две категории:

1) всенаправленные – излучающие по всем направлениям (360 градусов) одинаково;

2) однонаправленные – максимум излучения в определенном направлении.

На рисунке 18 всенаправленная антенна излучает во всех направлениях приблизительно с одинаковой мощностью. Так как такая антенна не имеет выделенного направления передачи, усиление у нее довольно низкое. Такие антенны обычно используются, когда некоторое количество передатчиков находятся на небольших расстояниях от приемника. При увеличении направленности увеличивается и усиление.

Рисунок 19 показывает, как усиление растет с уменьшением ширины пучка, то есть с усилением направленности антенны.

Направленность антенны показывает ее возможность фокусировать энергию в определенном направлении при передаче или сфокусироваться на опре-

деленном направлении при приёме.

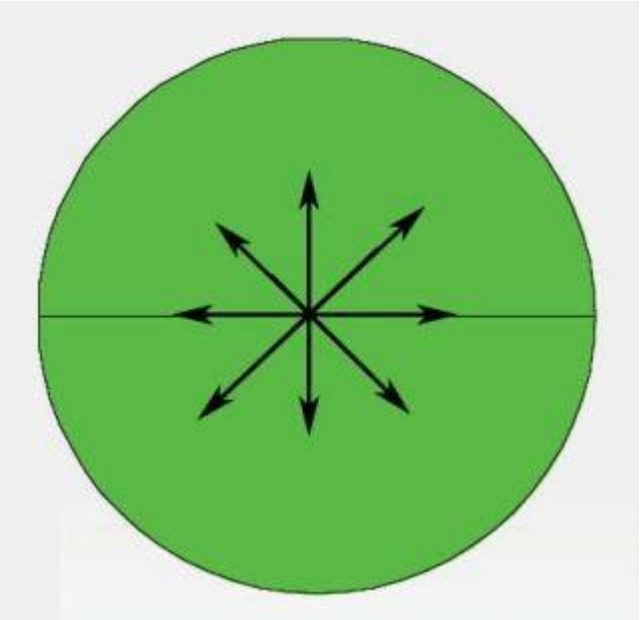

Рисунок 18 – Спектр всенаправленной антенны

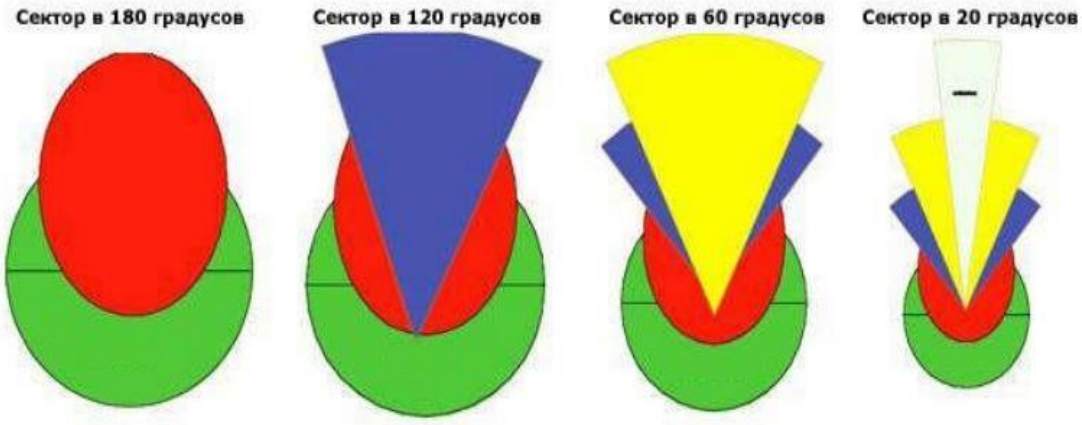

Рисунок 19 – Спектр направленной антенны

Если беспроводная связь устанавливается между двумя неподвижными устройствами, можно использовать направленность антенны для концентрации излучаемой энергии в определенном направлении. В подвижных системах невозможно предсказать местоположение устройств, поэтому оптимальным вариантом в этом случае будет антенна, одинаково излучающая по всем направлениям.

Усиление – это безразмерная характеристика, в отличие, например, от мощности, измеряемой в Ваттах, или сопротивления (в Омах). Усиление зада-

ется относительно стандартной антенны. Два основных типа «стандартных» антенн – это изотропная антенна и резонансная полуволновая дипольная антенна. Мы остановимся на изотропной антенне.

Изотропная антенна излучает одинаково по всем направлениям. Реальных изотропных антенн, конечно, не существует, но они создают простую характеристику, с которой удобно сравнивать реальные антенны. Любая реальная антенна в некоторых направлениях излучает сильнее. Так как антенны – пассивные элементы, полная излучаемая ими мощность равна мощности изотропной антенны, подключенной к той же системе. Дополнительная энергия, рассеиваемая в некоторых направлениях, появляется за счет того, что в остальных направлениях рассеивается энергия, меньшая изотропного аналога.

Усиление антенны в заданном направлении – это энергия, рассеянная ей в этом направлении, отнесенная к энергии изотропной антенны в том же направлении при ее подключении к источнику аналогичной выходной мощности. Как правило, нас будет интересовать максимальное усиление, то есть усиление в направлении, в котором антенна рассевает наибольшее количество энергии. Усиление, например, антенны в 3 дБ в сравнении с изотропной антенной, будет записываться как 3 дБi

Диаграмма направленности описывает относительную мощность рассеивания в различных направлениях от антенны на одном и том же расстоянии от нее. Диаграмма направленности излучения также описывает и диаграмму направленности приема, тем самым она описывает и приемные свойства антенны. Диаграмма направленности трехмерна, но обычно измеряются двумерные диаграммы направленности, т. е. срезы трехмерной диаграммы в горизонтальной или вертикальной плоскостях. Эти диаграммы представляются как в прямоугольных, так и в полярных координатах. Рисунок 20 показывает диаграмму направленности антенны усилением 18 дБi, обычно устанавливаемую в системах, где необходимо среднее усиление. Несмотря на то, что представленная информация довольно подробна, существуют и лучшие представления характе-

ра излучения антенны в различных направлениях.

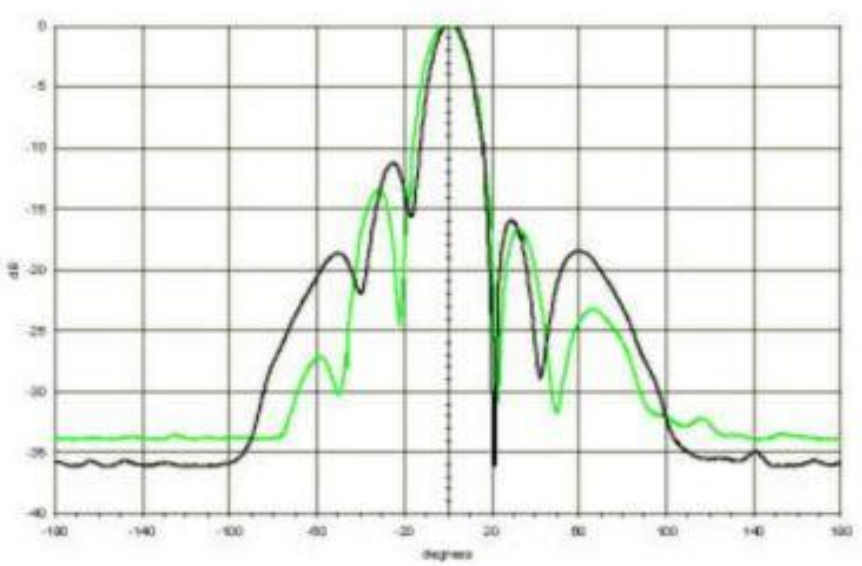

Рисунок 20 – Диаграмма направленности

Наиболее универсальна полярная система координат. В полярных координатах точки расположены в зависимости от угла, а удаленность их от центра показывает интенсивность, излучаемую в данном направлении. Рисунок 21 представляет собой линейную диаграмму направленности антенны с усилением 16 дБi и углом рассеяния в 27 градусов, сама антенна представлена на рисунке рядом. Полярные системы координат можно разделить на два класса: линейные и логарифмические. В линейной координатной системе концентрические окружности отстоят друг от друга на равные расстояния.

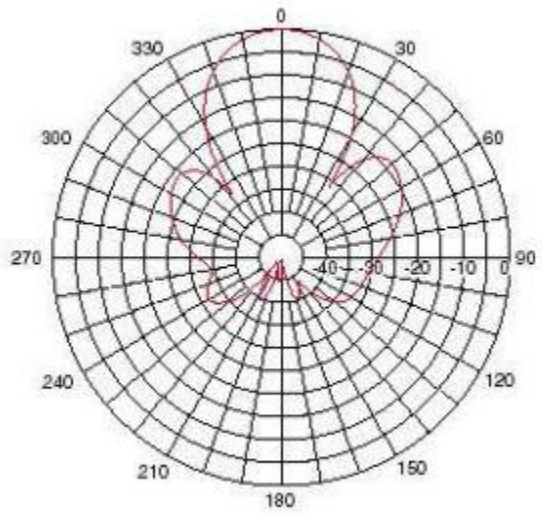

Рисунок 21 – Диаграмма направленности в полярных координатах

Такая система может быть использована для создания линейного чертежа мощности сигнала. Для простоты сравнения, равноотстоящие концентрические окружности можно заменить соответствующим образом помещенными окружностями уровня усиления в дБ с нулем на внешнем круге. В таком графике более мелкие лепестки станут еще меньше. Это представление данных позволяет получить диаграммы, на которых у антенны очень высокая направленность и небольшие побочные лепестки. В логарифмической полярной системе координат концентрические окружности распределены по логарифму напряжения сигнала. Для логарифмической постоянной могут быть использованы любые числа, но выбор повлияет на внешний вид диаграмм. Как правило, нулевой уровень находится на внешнем крае диаграммы.

Разница между точками 0 дБ и -3 дБ больше, чем между -20 дБ и -23 дБ, а разница между -20 дБ и -23 дБ соответственно больше, чем между -50 дБ и -53 дБ. Получается, что расстояние между изолиниями соответствует относительной производительности антенны.

Ни одна антенна не способна излучать всю энергию в одном направлении. Некоторая часть неизбежно излучается в другие стороны. Эти пики называются боковыми лепестками и обычно указываются в дБ относительно основного.

Нулевой зоной в диаграмме направленности называется зона минимального рассеивания энергии. У нулевой зоны, как правило, гораздо более узкий угол направленности, чем у основного пучка. Поэтому нуль полезен в некоторых случаях, например для подавления интерферирующих сигналов в заданном направлении.

2.5 Программное обеспечение

2.5.1 Сниффер

Сниффер (от английского sniffer – нюхач) это программа, которая устанавливается под сетевую интерфейсную карту, иначе называемую Ethernet карта. Как известно информация по сети передается пакетами - от одной машины к

удаленной. Сниффер, установленный на промежуточной машине, через который будут проходить пакеты – способен захватывать их, пока они еще не достигли цели. У разных снифферов процесс захвата информации реализован по разному.

Стандартный пакет переходит из машины через сеть. Каждая машина должна игнорировать пакет если он не предназначен для ее IP адреса. Тем не менее, машина со сниффером принебригает этим правила и принимает любой пакет, который через нее проходит. Сниффер также известен как сетевой анализатор. Нет реального различия между сетевым анализатором и сниффером, но компании по безопасности и Федеральное правительство предпочитают второе название поскольку оно звучит более официальным.

Для злоумышленника, сниффер отличный инструмент для наблюдения за посылаемой информацией, и это считается пассивным типом атаки. *Пассивная атака* - эта та атака, которой непосредственно не вторгаются в чужую сеть или компьютер. С другой стороны, активная атака непосредственно связывается с дистанционной машиной. Дистанционные переполнения буфера хоста, сетевые наводнения попадают под категорию активной атаки. Пассивная атака сниффера не может быть обнаружена. Следы его деятельности нигде не отражаются. При этом атака сниффера также серьезна, как и любая активная атака.

Наиболее популярный тип снифферов использует кратковременный забор информации и работает в небольших сетях. Причина этого кроется в том, что невозможно поставить сниффер, который бы постоянно отслеживал пакеты и при этом не сильно использовал мощность центрального процессора. Чрезмерная загрузка центрального процессора и файловой системы являются единственным путем обнаружения снифферов. Эти снифферы осуществляют быстрый и кратковременный забор информации, чтобы утилиты безопасности не смогли обнаружить их.

Следующий тип снифферов, работает на больших протоколах передачи данных, соответственно, потребление ресурсов в центральном процессоре зна-

чительно больше. В больших сетях, такие снифферы могут сгенерировать вплоть до десяти мегабайтных протоколов в день, если в сниффере установлена регистрация всего диалогового движения. Если стоит и обработка почты то объемы могут расти быстрее.

Следующий тип снифферов записывает только первые X байтов пакета, чтобы захватить имя/пароль. Другой метод заключается в захвате целого сеанса, и отключения ключа. Более модернизированные типы снифферов поддерживают оба метода.

2.5.2 Дешифратор

Дешифратор – это комбинационное устройство, предназначенное для преобразования параллельного двоичного кода в унитарный, т.е. позиционный код. Обычно, указанный в схеме номер вывода дешифратора соответствует десятичному эквиваленту двоичного кода, подаваемого на вход дешифратора в качестве входных переменных, вернее сказать, что при подаче на вход устройства параллельного двоичного кода на выходе дешифратора появится сигнал на том выходе, номер которого соответствует десятичному эквиваленту двоичного кода. Отсюда следует то, что в любой момент времени выходной сигнал будет иметь место только на одном выходе дешифратора.

В зависимости от типа дешифратора, этот сигнал может иметь как уровень логической единицы (при этом на всех остальных выходах уровень логического 0), так и уровень логического 0 (при этом на всех остальных выходах уровень логической 1). В дешифраторах каждой выходной функции соответствует только один минтерм, а количество функций определяется количеством разрядов двоичного числа. Если дешифратор реализует все минтермы входных переменных, то он называется полным дешифратором.

Существует несколько разновидностей дешифраторов:

– прямоугольные;

– матричные;

– пирамидальные.

Матричные являются типовыми, наиболее простыми разновидностями дешифраторов, на их основе строятся различные более сложные схемы.

В прямоугольных реализуется ступенчатая дешифрация. Входной сигнал условно разбивается на группы, каждая из которых обрабатывается отдельными матричными дешифраторами. На последующих ступенях дешифрации (второй, третьей и т.п.) формируется произведение полученных сигналов.

Главным преимуществом пирамидальных дешифраторов считается простота наращивания числа входов, а недостатком – аппаратная неизбыточность.

2.5.3 Логгер

Логгер – программа сбора информации в унифицированном стандарте для предоставления сводки о работе системы.

Естественной потребностью системного администратора или специалиста по безопасности является некий анализ того, что происходит как на конкретном компьютере конкретного пользователя, так и в сети. Технически задача выполнима, ибо разработчики множества приложений, которыми мы пользуемся, заложили в свои продукты функцию логгирования информации.

Для того чтобы грамотно добывать полезную информацию из логов, иногда достаточно текстового редактора, но часто встречаются ситуации, когда лог и просмотреть довольно сложно, и трактовать правильно тяжело. В этом случае полезно знать о некоторых особенностях структуры различных лог-файлов и об информации, которая в них встречается.

Типы логов:

1) логгирование в текстовый файл. Способ, при котором отдельное событие представляет собой отдельную строку. Используется очень часто. Способ хорош как с точки зрения реализации – довольно легко наладить такое логгирование в коде большинства языков программирования, – так и со стороны использования – читать такой лог можно любым текстовым редактором.

2) лог-файлы, в которых отдельное событие представляет собой не одну строку, а несколько. С некоторым допущением к этому же типу относятся логи,

которые пишутся в формате XML. Такой лог гораздо более сложен для анализа, потому что каждое событие может представлять собой набор более мелких записей. Для чтения таких логов чаще всего используется специально ПО, так как лог, в котором каждое событие растянуто на несколько строк, а еще и сами события зависят друг от друга, довольно тяжело интерпретировать.

3) Бинарный лог представляет собой самый нечитаемый тип логов. Для того чтобы с ними работать, нужна специальная программа, с помощью которой бинарный лог и анализируется. Обычно бинарный лог – это последовательно сбрасываемые в файл структуры, которые разделяются символом-разделителем. Обрабатывать такой лог очень тяжело, впрочем, довольно часто в технической информации, которую предоставляет производитель, есть описание структуры такого лога.

2.6 Обзор комплексов для перехвата трафика

1) RS1000 – многофункциональный перехватчик трафика различных радиочастотных диапазонов:

– GSM 890-960 МГц;

– 3G/UMTS2100, 1920-1980 МГц, 2110-2170 МГц;

– 3G/UMTS900, 880-915 МГц, 925-960 МГц;

– 4G/LTE2500, 2300-2700 МГц;

– 4G/LTE800, 791-862 МГц;

– сети WiFi 2,4 ГГц;

– сети WiFi 5 ГГц

На рисунке 22 показан развернутый комплекс RS1000

2) ПАК информационно-технического воздействия в системах беспроводной радиосвязи стандарта 802.11 на рисунке 23.

Главное преимущество ПАК по сравнению с предыдущим это мобильность и целенаправленность. ПАК направлен на перехват трафика в беспроводных сетях только стандарта 802.11.

Рисунок 22 – Передвижной комплекс по перехвату трафика в беспроводных сетях RS1000

Рисунок 23 – ПАК беспроводных сетей стандарта 802.11

3 РАЗРАБОТКА АППАРАТНОГО ОБЕСПЕЧЕНИЯ

3.1 Выбор вычислительной платформы.

Главными приоритетами для программно-аппаратного комплекса стоят:

– мобильность;

– модульность;

– относительно высокая производительность.

При этих приоритетах выбор пал на три микрокомпьютера.

Последняя модель итальянского производителя электротехники – Arduino Uno Rev3 на рисунке 24. Она выполнена на базе процессора ATmega328p с тактовой частотой 16 МГц, обладает памятью 32 кБ и имеет 20 контролируемых контактов ввода и вывода для взаимодействия с внешним миром.

Рисунок 24 – Arduino Uno Rev3

Arduino – это открытая платформа, которая позволяет собирать всевозможные электронные устройства. Arduino будет интересен креативщикам, дизайнерам, программистам и всем пытливым умам, желающим собрать собственный гэджет. Устройства могут работать как автономно, так и в связке с компьютером.

Платформа состоит из аппаратной и программной частей; обе чрезвычайно гибки и просты в использовании. Для программирования используется

упрощённая версия C++, известная так же как Wiring. Разработку можно вести как с использованием бесплатной среды Arduino IDE, так и с помощью произвольного C/C++ инструментария. Поддерживаются операционные системы Windows, MacOS X и Linux.

Arduino Uno может питаться как от USB подключения, так и от внешнего источника: батарейки или обычной электрической сети. Источник определяется автоматически. Платформа может работать при наличии напряжения от 6 до 20 В. Однако при напряжении менее 7 В работа может быть неустойчивой, а напряжение более 12 В может привести к перегреву и повреждению. Поэтому рекомендуемый диапазон: 7−12 В.

Платформа оснащена 32 кБ flash-памяти, 2 кБ из которых отведено под так называемый загрузчик. Он позволяет прошивать Arduino с обычного компьютера через USB. Эта память постоянна и не предназначена для изменения по ходу работы устройства. Её предназначение − хранение программы и сопутствующих статичных ресурсов.

Также имеется 2 кБ SRAM-памяти, которые используются для хранения временных данных вроде переменных программы. По сути, это оперативная память платформы.

На платформе расположены 14 контактов (pins), которые могут быть использованы для цифрового ввода и вывода. Какую роль исполняет каждый контакт, зависит от вашей программы. Все они работают с напряжением 5 В, и рассчитаны на ток до 40 мА. Также каждый контакт имеет встроенный, но отключённый по умолчанию резистор на 20 - 50 кОм. Ещё имеется 1 кБ ROM-памяти для долговременного хранения данных. По своему назначению это аналог жёсткого диска для Arduino. Размер платы составляет 6,9 × 5,3 см.

Гнёзда для внешнего питания и USB выступают на пару миллиметров за обозначенные границы. На плате предусмотрены места для крепления на шурупы или винты. Расстояние между контактами составляет 0,1″ (2,54 мм), но в случае 7-го и 8-го контакта − расстояние: 0,16″.

Рисунок 25, на нем представлена еще одна вычислительная платформа Arduino Due. 32-битный ARM-процессор AT91SAM3X8E от Atmel. Он обладает тактовой частотой 84 МГц, а его 32-битная архитектура позволяет выполнять большинство операций на целыми числами в 4 байта за один такт.

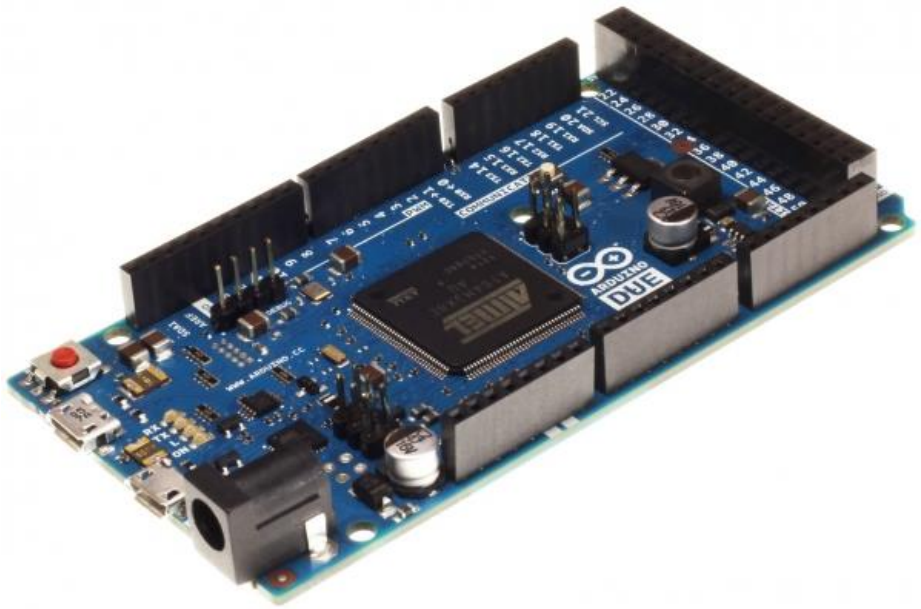

Рисунок 25 – Arduino Due

На борту SAM3X – 2 блока по 256 Кб флеш-памяти для хранения программы. Загрузчик (bootloader) располагается в отдельной памяти только для чтения и прошит на заводе Atmel. Оперативная SRAM-память поделена на 2 банка: 64 и 32 Кб.

Любая память доступна для последовательной адресации из программы. Содержимое флеш-памяти может быть очищено зажатием на несколько секунд кнопки Erase на плате.

Arduino Due позволяет взаимодействовать с компьютером, другими Arduino, микроконтроллерами и различными устройствами вроде телефонов, планшетов, фотоаппаратов. Для этого плата предоставляет три аппаратных последовательных порта (UART/USART), две шины TWI/I²C, интерфейс SPI и USB-порт.

Один USB-порт используется для прошивки Arduino Due. Он подключён к чипу ATmega16U2 на плате, который является мостом между USB и аппарат-

ным портом SAM3X, используемым для программирования процессора и связи с компьютером.

Второй USB-порт может использоваться для связи с другими устройствами как в режиме slave (эмуляция мыши, клавиатуры), так и в режиме host (приём данных с фотоаппаратов, управление мышью, клавиатурой, телефоном).

Raspberry Pi 2 Model B – сочетание всех приоритетов, которым придерживаемся в разработке ПАК. На рисунке 26 представлена плата.

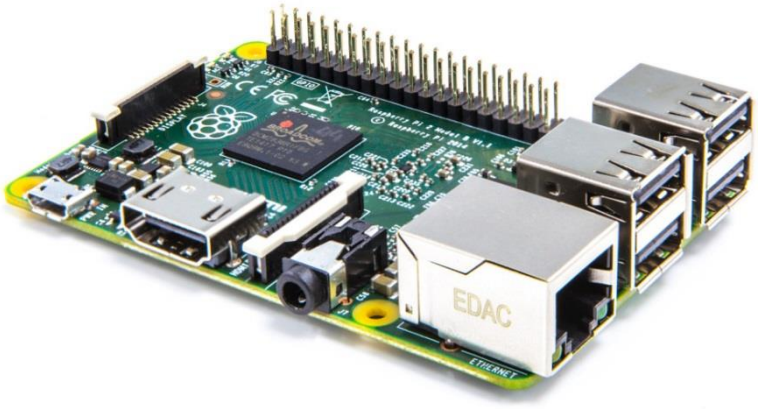

Рисунок 26 - Raspberry Pi 2 Model B

Компьютер выполнен на базе SoC (System on Chip) Broadcom BCM2836. Четырёхядерный процессор построен на архитектуре ARM Cortex-A7 и наделён тактовой частотой 900 МГц на ядро.

Графическое ускорение компьютера аппаратно поддерживает OpenGL ES 2.0, OpenVG, MPEG-2, VC-1, кодирование и воспроизведение 1080p30 H.264/MPEG-4. Выдаваемое разрешение можно варьировать от 640×350 (EGA) до 1920×1200 (WUXGA).

На композитном выходе можно генерировать сигналы 576i или 480i в формате PAL или NTSC.

Raspberry Pi 2 Model B наделили 1 ГБ оперативной памяти. Эта память делится с графической подсистемой.

Raspberry Pi 2 Model B может быть запитана через microUSB-кабель или через пины питания. Номинальное напряжение питания − 5 В. Компьютер по-

требляет до 800 мА без внешних устройств.

Размер платы: 85×54 мм. USB-порты, Ethernet-гнездо, HDMI, аудио-гнездо выступают за обозначенные рамки на несколько миллиметров.

Аппаратный выключатель питания на плате отсутствует. Для включения компьютера достаточно просто подсоединить кабель питания. Для выключения используйте штатную функцию операционной системы.

Вместо традиционного для обычных компьютера жёсткого диска, Raspberry Pi использует microSD флеш-карту. Она должна быть предварительно подготовлена, на неё следует установить операционную систему на выбор.

Подводя итог по вычислительной платформе, было решено в качестве вычислительной платформы поставить Raspberry Pi 2 Model B, так как именно она больше всего подходит выдвинутым приоритетам.

3.2 Модуль беспроводной связи

Ранее в работе мы анализировали адаптеры WiFi, которые будут работать в частотных диапазонах стандарта 802.11 от 2,402 ГГц до 2,852. В первой версии ПАК будет использован внутренний WiFi адаптер ESP8266MOD, что представлен на рисунке 27.

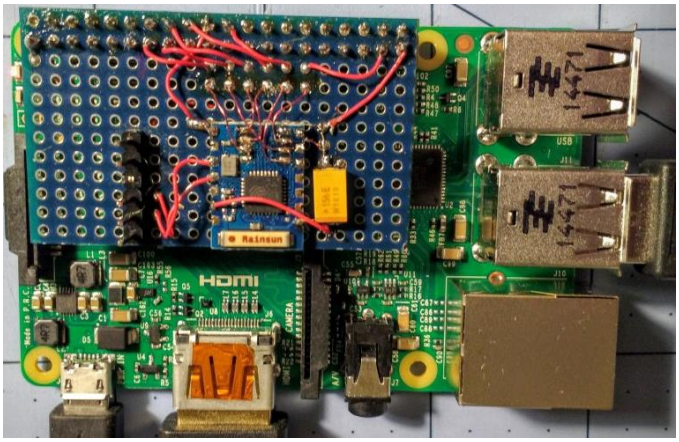

Рисунок 27 – Установленный внутренний WiFi адаптер ESP8266MOD

В последующих версиях ПАК было принято решение использовать внешний WiFi адаптер на рисунках 28, у которого будет возможность подключить внешнее устройство распространения сигнала.

Рисунок 28 – Внешний WiFi модуль

3.3 Устройство распространения сигнала

Так как у нас выбран внешний WiFi адаптер, для него была подобрана всенаправленная антенна, представленная на рисунке 29.

Для следующей версии программно-аппаратного комплекса стоит идея реализации направленной антенны, которая поможет улавливать и передавать сигнал на большие расстояния относительно всенаправленной.

Рисунок 29 – Всенаправленная антенна

3.4 Проектирование и разработка внешних корпусов

Для создания внешних защитных корпусов было принято использовать систему автоматизированного проектирования (САПР) «SolidWorks». SolidWorks – это программный комплекс САПР для автоматизации работ промышленного предприятия на этапах конструкторской и технологической подготовки производства. Обеспечивает разработку изделий любой степени сложности и назначения. Работает в среде Microsoft Windows.

3.4.1 Корпус вычислительной платформы

Для начала были взяты размеры с Raspberry Pi, сделаны снимки всех проекций. Была спроектирована вся плата, которая представлена на рисунке 30.

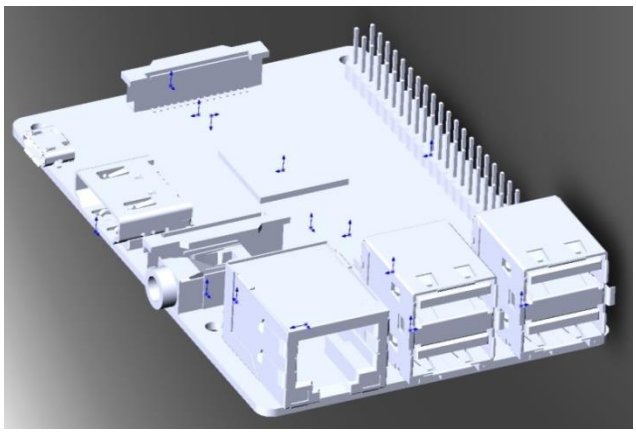

Рисунок 30 – Трехмерная модель вычислительной платформы

Для трехмерной модели был спроектирован и смоделирован защитный корпус, который представлен на рисунке 31. Крепления корпуса было задумано автономным без применения каких-либо болтов для крепления частей. Всего 6 частей, все они скреплены между собой внешними замками, т.е. при проектировании было решено сделать отверстия в четырех планках по периметру, а нижняя и верхняя планки имели выступы, которые плотно входят в отверстия.

Тем самым корпус стал более мобильным и крепким, что также является в приоритете разрабатываемого ПАК. Все детали были нарезаны с помощью лазерной резки.

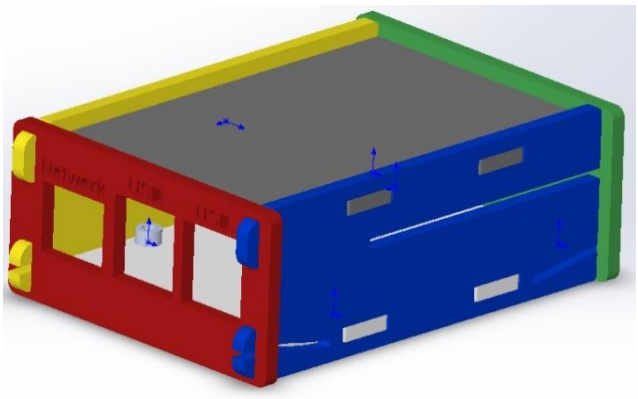

Рисунок 31 – Защитный кейс вычислительной платформы

3.4.2 Корпус устройства распространения сигнала

Так же, для начала были взяты размеры с WiFi адаптера, и сделаны снимки всех проекций. Было спроектировано все устройство, которое представлено на рисунке 32.

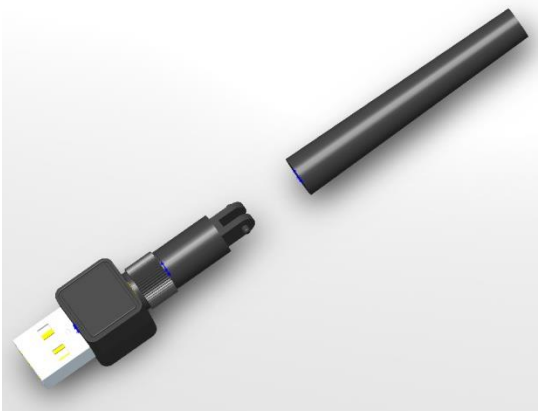

Рисунок 32 – Трехмерная модель WiFi адаптера и антенны

3.5 Архитектура комплекса

Под архитектурой программно-аппаратного комплекса будем понимать совокупность всех внешних и внутренних модулей и периферийного оборудования, а именно, все компоненты аппаратного обеспечения и их взаимодействие между собой.

На рисунке 33 представлена наглядная схема модулей и периферийного оборудования программно-аппаратного комплекса и их взаимодействия между собой.

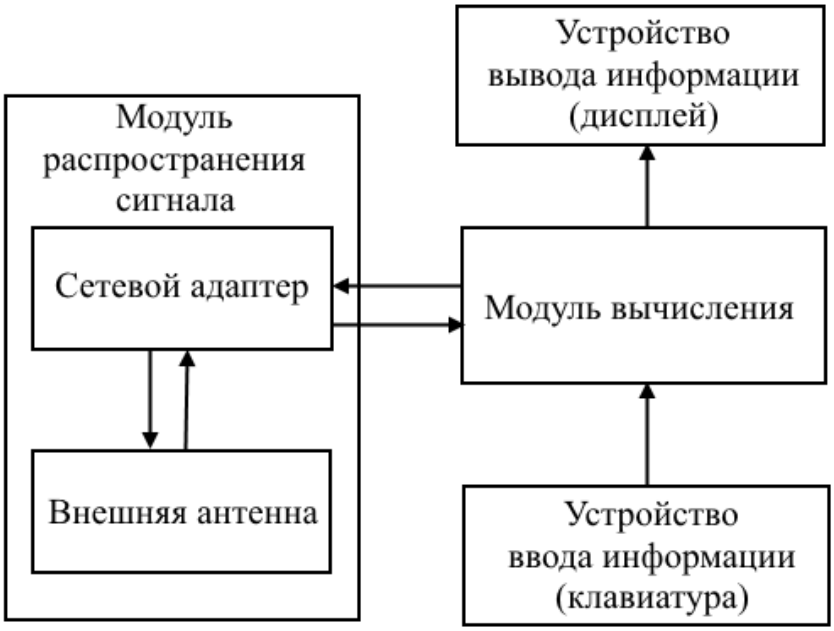

Рисунок 33 – Архитектура программно-аппаратного комплекса

Как видно из схемы, ПАК состоит из двух модулей связанных между собой: модуль вычисления и модуль распространения сигнала. Последний, в свою очередь, имеет под собой аппаратную основу из двух устройств – это сетевой адаптер и внешняя антенна. Сетевой адаптер выполняет функцию модулятора при исходящем трафике и демодулятора – при входящем. Антенна же отвечает за прием и передачу аналогово сигнала в окружающую среду.

К модулю вычисления подключено отдельное периферийное оборудование, такое как устройство ввода информации (клавиатура) и устройство вывода информации (дисплей). Дисплей имеет под собой основу преобразования графической информации через видеокарту, которая подключена напрямую к вычислительной платформе.

4 РАЗРАБОТКА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

4.1 Общие сведения

Наименование программы: Программный пакет для программно-аппаратного комплекса «Призрак».

Программное обеспечение разрабатывается под операционную систему BackTrack 5, Kali 2.0 базирующиеся на ядре Linux. Язык программирования C++. Для реализации мастера отчета применяется Microsoft Visual Studio.

Модульность ПО обеспечивается тремя параметрами:

– открытость кода ядра ОС;

– свободно распространяемая лицензия внутренних утилит;

– компилируемость нескольких кодов.

Ядро Linux – это центральная часть большой и сложной операционной системы. При этом, несмотря на колоссальные размеры, оно имеет четкую структурную организацию в виде подсистем и уровней.

Одна из целей архитектурного анализа может состоять в том, чтобы лучше понять исходный код системы. В ядре Linux реализован целый ряд важных архитектурных элементов. И на самом общем, и на более детальных уровнях ядро можно подразделить на множество различных подсистем. С другой стороны, Linux можно рассматривать как монолитное целое, поскольку все базовые сервисы собраны в ядре системы. Такой подход отличается от архитектуры с микроядром, когда ядро предоставляет только самые общие сервисы, такие как обмен информацией, ввод/вывод, управление памятью и процессами, а более конкретные сервисы реализуются в модулях, подключаемых к уровню микроядра.

Другой важный ресурс, которым управляет ядро – это память. Для повышения эффективности, учитывая механизм работы аппаратных средств с виртуальной памятью, память организуется в виде страниц (в большинстве архитектур размером 4 КБ). В Linux имеются средства для управления имеющейся па-

мятью, а также аппаратными механизмами для установления соответствия между физической и виртуальной памятью.

В условиях наличия большого числа пользователей памяти возможны ситуации, когда вся имеющаяся память будет исчерпана. В связи с этим страницы можно удалять из памяти и переносить на диск. Этот процесс обмена страниц между оперативной памятью и жестким диском называется подкачкой.

На рисунке 34 представлена функциональная модель комплекса, которая отображает все входящие потоки данных, нормативные документы, алгоритмы и поддерживающую инфраструктуру.

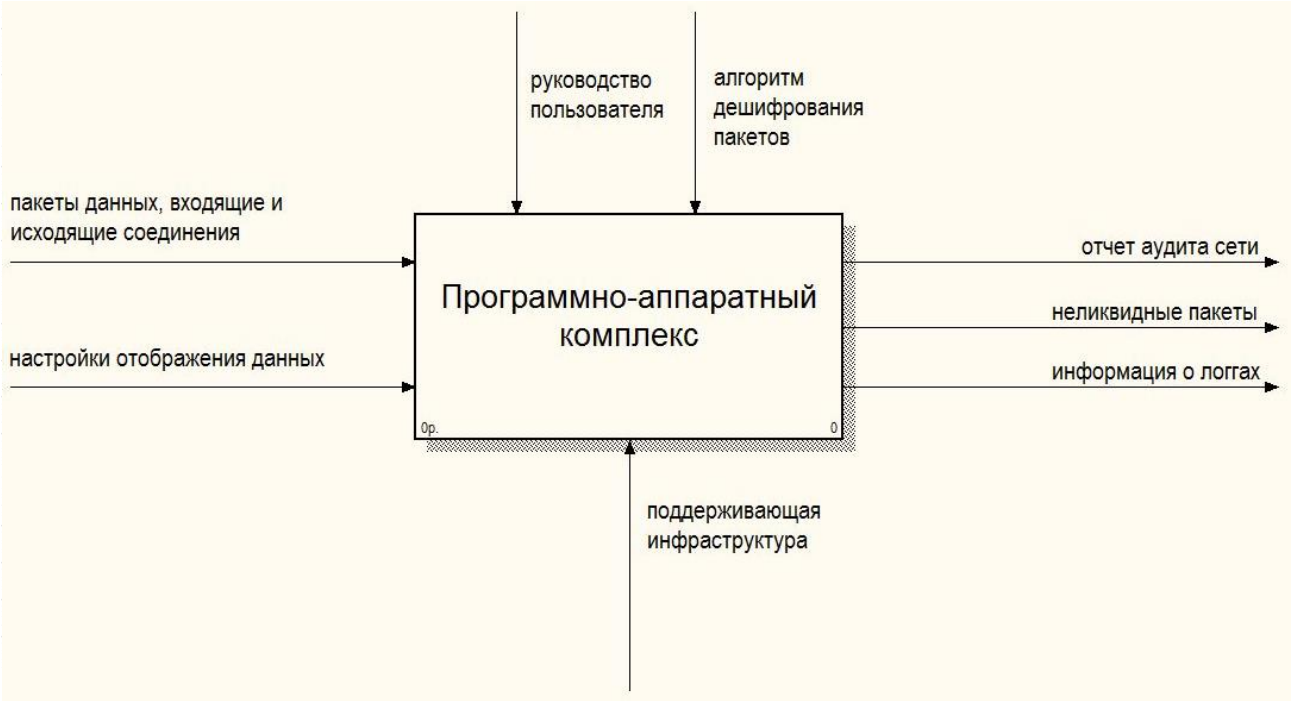

Рисунок 34 – Функциональная модель комплекса

На рисунке мы можем увидеть, что результатом работы программно-аппаратного комплекса является отчет аудита сети, информация о логгах и неликвидные пакеты, которые формируются средствами программного пакета.

4.2 Описание модулей

Далее, рассматривая декомпозицию функциональной модели комплекса на рисунке 35, можно подробнее увидеть программные модули и их работу. Рассматривая работу модулей, можно проанализировать, как поступает входя-

щая информация, как и в виде чего она поступает к последующим модулям для обработки.

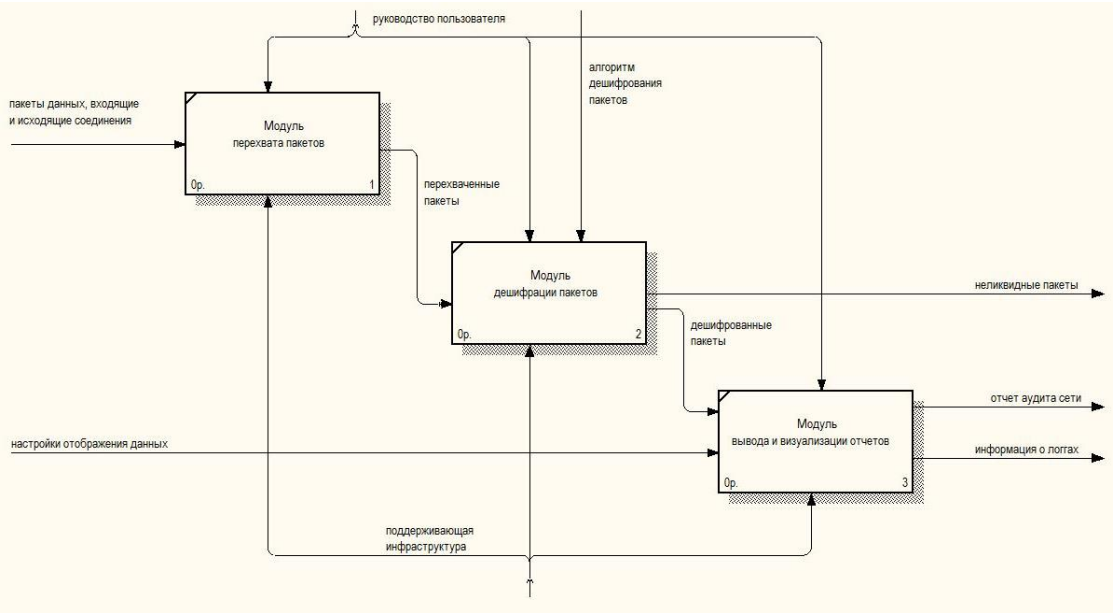

Рисунок 35 – Декомпозиция функциональной модели комплекса

Как видно из рисунка функциональная модель состоит из трех модулей:

– модуль перехвата пакетов;

– модуль дешифрации пакетов;

– модуль вывода и визуализации отчетов.

Первый модуль имеет функцию перехвата пакетов из сети. При инициализации аудита, активируется функция перехвата пакетов и создает входящее соединение, при котором все пакеты из целевой сети передаются через модуль распространения сигнала на оперативно запоминающее устройство аппаратного обеспечения, которое в дальнейшем обрабатывает все полученные пакеты. На рисунке 36 представлена работа модуля перехвата пакетов.

Далее все перехваченные пакеты идут на модуль дешифрации. В нем пакеты представляются в виде символьной последовательности, используя кодировку Unicode. Далее выбирается один из алгоритмов дешифрования пакета («прямоугольный», «треугольный», «пирамидальный» и т.д.). Дешифрованные пакеты представляются в кодировке UTF-8. Все неликвидные файлы, т.е. непрошедшие дешифрацию, сохраняются в постоянное запоминающее устрой-

ство аппаратного обеспечения в виде отдельных файлов.

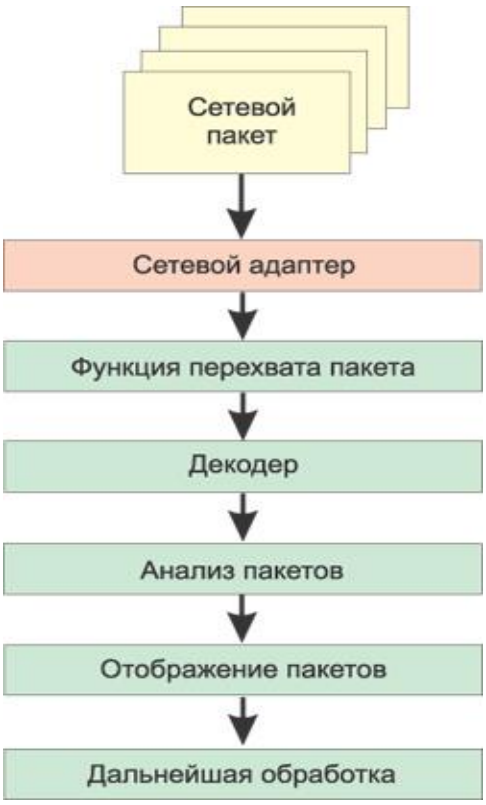

Рисунок 36 – Схема работы модуля перехвата пакетов

После дешифрации, пакеты передаются в последний модуль программно-аппаратного комплекса, где происходит нахождение ключевых записей на предмет соответствия с целями аудита, например, pin-код атакуемой сети, списки mac-адресации, соединения точки доступа и абонентов.

Далее, составляется отчет-рекомендация по проведенному аудиту сети, который включает в себя следующие положения:

– время аудита;

– точка доступа;

– ssid атакуемой сети;

– количество подключенных абонентов;

– количество перехваченных пакетов;

– количество дешифрованных пакетов;

– количество уязвимостей;

– рекомендации.

4.3 Интерфейс программы

Вызов программы производится из терминала командой:

root@kali:~# sniff –a start

После вызова открывается окно программы, которое представлено на рисунке 37.

Рисунок 37 – Окно программы

В окне программы отображается начальная информация, которая была собрана стандартными сетевыми и операционными службами, а именно Название программы, автор, использование сокетов, хост машины, ip-адрес и режим перехвата.

Далее предлагается использовать консольный режим отображения работы программы. На рисунке 38 отображены условные обозначения принимаемых пакетов и расшифровка содержимого этих пакетов.

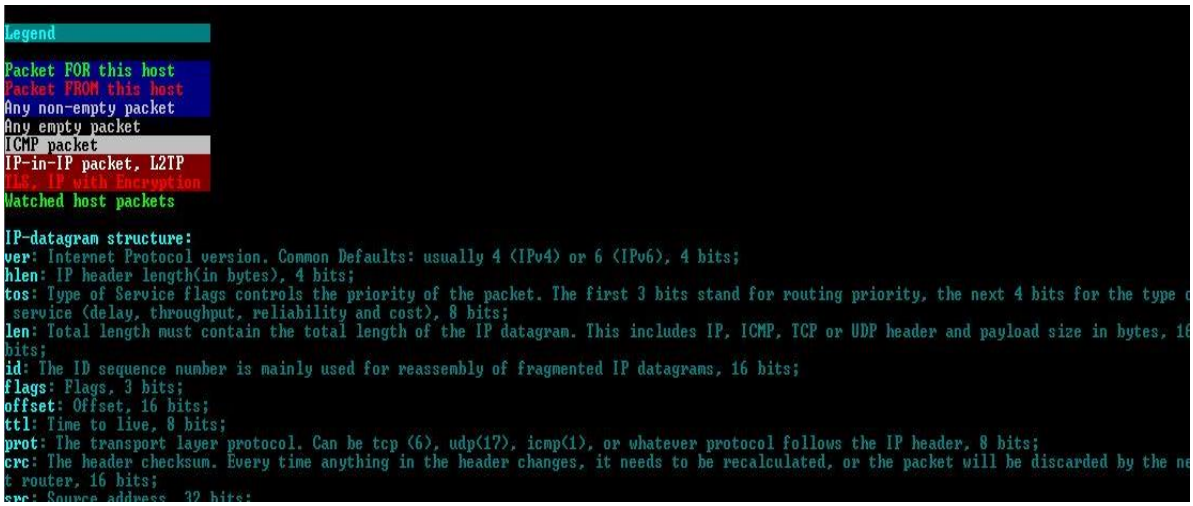

Рисунок 38 – Описание визуализации пакетов

Как показано на рисунке 39, после ознакомления с условными обозначениями начинается перехват пакетов из сети.

Рисунок 39 – Перехват пакетов сети

Вся сессия соединения, то есть перехват всех пакетов записывается в лог-файл, который в дальнейшем послужит основой для рекомендации.

Остановка программы вызывается нажатием клавиши «пробел».

ЗАКЛЮЧЕНИЕ

В ходе выполнения бакалаврской работы с помощью аппаратного и программного обеспечения был разработан программно-аппаратный комплекс по перехвату трафика и несанкционированному доступу в беспроводной сети стандарта 802.11 b/g/n.

ПАК имеет несколько модификаций, что позволяет ему найти применение в различных направлениях пентеста.

Цель была достигнута за счет выполнения задач, а именно:

1) был проведен глубокий анализ аппаратного и программного обеспечения;

2) рассмотрены аналоговые комплексы по перехвату трафика в сети и выявлены преимущества;

3) исследован международный стандарт 802.11 по беспроводным сетям;

4) были подобраны все модули для реализации аппаратной части комплекса;

5) спроектированы и разработаны защитные корпуса ПАК;

6) разработан модуль программного обеспечения по перехвату пакетов в беспроводной сети.

Исходя из выше перечисленного, можно считать, что все задачи данной бакалаврской работы были полностью реализованы и цель исследования была достигнута.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1 Аклаков, С.В. BPwin и ERwin. CASE-средства разработки информационных систем / С.В. Аклаков. – М.: Диалог-МИФИ, 2000. – 15 с.

2 Волифер, В.Г. Основы сетей передачи данных / В.Г. Волифер, Н.А. Олифер. – СПб: Питер, 2009. – 663 с.

3 Волевой, Ю.А. Сети. Выбор, установка, использование и администрирование / Ю.А. Волевой, С.В. Омелянский. – К.: Юниор, 2007. – 544 с.

4 Голифер, В.Г. Компьютерные сети. Принципы, технологии, протоколы / В.Г. Голифер, Н.А. Голифер. – СПб: Питер, 2009. – 598с.

5 Золотов, С.Ю. Проектирование информационных систем [Электронный ресурс]: учебное пособие/ С.Ю. Золотов. − Электрон. текстовые данные. − Томск: Томский государственный университет систем управления и радиоэлектроники, Эль Контент, 2013. − 88 с.

6 Казанский, А.А. Объектно-ориентированное программирование на языке Microsoft Visual C# в среде разработки Microsoft Visual Studio 2008 и .NET Framework. 4.3 [Электронный ресурс]: учебное пособие и практикум/ А.А. Казанский − Электрон. текстовые данные. − М.: Московский государственный строительный университет, ЭБС АСВ, 2011. − 180 с.

7 Кивран, В.К. Программирование в среде Visual C++ 6 [Электронный ресурс]: учебное пособие/ В.К. Кивран. − Электрон. текстовые данные. − Самара: Самарский государственный архитектурно-строительный университет, ЭБС АСВ, 2014. − 118 с.

8 Култыгин, О.П. Администрирование баз данных. СУБД MS SQL Server [Электронный ресурс]: учебное пособие/ О.П. Култыгин. − Электрон. текстовые данные. − М.: Московский финансово-промышленный университет «Синергия», 2012. − 232 с.

9 Лягинова, О.Ю. Разработка схем и диаграмм в Microsoft Visio 2010 [Электронный ресурс]/ О.Ю. Лягинова. − Электрон. текстовые данные. − М.: Интернет-Университет Информационных Технологий (ИНТУИТ),

2016. − 127 с.

10 Медведкова, И.Е. Базы данных [Электронный ресурс]: учебное пособие / И.Е. Медведкова, Ю.В. Бугаев, С.В. Чикунов. − Электрон. текстовые данные. − Воронеж: Воронежский государственный университет инженерных технологий, 2014. − 105 с.

11 Меркулова, А.Ш. Формирование баз данных [Электронный ресурс]: учебно-методический комплекс для студентов очной и заочной форм обучения по направлению 071900 «Библиотечно-информационная деятельность», профиль подготовки «Информационно-аналитическая деятельность» / А.Ш. Меркулова. − Электрон. текстовые данные. − Кемерово: Кемеровский государственный университет культуры и искусств, 2013. − 104 с.

12 Молдованова, О.В. Информационные системы и базы данных [Электронный ресурс]: учебное пособие/ О.В. Молдованова. − Электрон. текстовые данные. − Новосибирск: Сибирский государственный университет телекоммуникаций и информатики, 2014. − 178 с.

13 Новиков, Ю.В. Основы локальных сетей [Электронный ресурс]/ Ю.В. Новиков, С.В. Кондратенко. − Электрон. текстовые данные. − М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. − 405 с.

14 Пакулин, В.Н. 1С. Бухгалтерия 8.1 [Электронный ресурс]/ В.Н. Пакулин. − Электрон. текстовые данные. − М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. − 67 с.

15 Самуйлов, С.В. Базы данных [Электронный ресурс]: учебно-метод. пособие для выполнения лабораторной и контрольной работы/ С.В. Самуйлов. – Электрон. текстовые данные. − Саратов: Вузовское образование, 2016. − 50 с.

16 Терещенко, П.В. Интерфейсы информационных систем [Электрон-ный ресурс]: учебное пособие/ П.В. Терещенко, В.А. Астапчук. − Электрон. текстовые данные. − Новосибирск: Новосибирский государ-

ственный технический университет, 2012. − 67 с.

17 Швецов, В.И. Базы данных [Электронный ресурс]/ В.И. Швецов. − Электрон. текстовые данные. − М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. − 218 с.

18 Шрочкин, В.И. Информационная безопасность: учебник для студентов вузов / В.И. Шрочкин. – Москва: Трикста: Акад. проект, 2008. – 542 с.

20 Щавличева, Е.Н. Введение в информационные системы управления предприятием [Электронный ресурс]: учебное пособие/ Е.Н. Щавличева, В.А. Дикарев. − Электрон. текстовые данные.− М.: Московский городской педагогический университет, 2013.− 84 с.

21 Ющенко, В.К. Архитектура высокопроизводительных вычислительных систем [Электронный ресурс]: учебное пособие/ В.К. Ющенко. − Электрон. текстовые данные.− Новосибирск: Новосибирский государственный технический университет, 2013.− 40 с.

22 Янюк, В.Г. Алгоритмы и структуры данных [Электронный ресурс]: лабораторный практикум. Учебное пособие/ В.Г. Янюк, Ю.Д. Рязанов. − Электрон. текстовые данные.− Белгород: Белгородский государственный технологический университет им. В.Г. Шухова, ЭБС АСВ, 2013.− 204 с.