

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ**

**ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ**

**«ДОНСКОЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»**

**(ДГТУ)**

Факультет «Информатика и вычислительная техника»

Кафедра «Вычислительные системы и информационная безопасность»

|  |  |  |
| --- | --- | --- |
| И.о. Зав. кафедрой | | «ВСиИБ» |
| \_\_\_\_\_\_\_\_\_\_\_\_ | | А.Р. Газизов |
| подпись | | И.О. Фамилия |
|  | «03» февраля 2023 г. | |

**ПОЯСНИТЕЛЬНАЯ ЗАПИСКА**

Тема «КОРПОРАТИВНАЯ БЕСПРОВОДНАЯ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННАЯ СЕТЬ С ДОМЕННОЙ АУТЕНТИФИКАЦИЕЙ»

Направление подготовки 10.05.02 Информационная безопасность телекоммуникационных систем

Специализация Защита информации в системах связи и управления

Обозначение ВКР 10.05.02.770000.000 группа ВИБТ61

Обучающийся \_\_\_\_\_\_\_\_\_\_\_\_\_\_ С.А. Зубишин

(подпись, дата) И.О.Ф.

Руководитель ВКР \_\_\_\_\_\_\_\_\_\_\_\_\_\_ доц., к.т.н. В.В. Галушка

(подпись, дата) должность, И.О.Ф.

Консультанты по разделам:

Безопасность и экологичность работы \_\_\_\_\_\_\_\_\_\_\_\_\_ проф., д.т.н. В.Л. Гапонов

(подпись, дата) (должность, И.О.Ф.)

Технико-экономическое обоснование \_\_\_\_\_\_\_\_\_\_\_\_\_ ст преп. А.В. Белоусова

(подпись, дата) (должность, И.О.Ф.)

Нормоконтроль \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ ст. преп. М.А. Ганжур

(подпись, дата) (должность, И.О.Ф.)

Ростов-на-Дону

2023



МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ**

**ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ**

**«ДОНСКОЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»**

**(ДГТУ)**

Факультет «Информатика и вычислительная техника»

Кафедра «Вычислительные системы и информационная безопасность»

|  |  |  |
| --- | --- | --- |
| Зав. кафедрой | | «ВСиИБ» |
| \_\_\_\_\_\_\_\_\_\_\_\_ | | В.А. Фатхи |
| подпись | | И.О. Фамилия |
|  | «23» июня 2022 г. | |

**ЗАДАНИЕ**

на выполнение выпускной квалификационной работы

Тема «КОРПОРАТИВНАЯ БЕСПРОВОДНАЯ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННАЯ СЕТЬ С ДОМЕННОЙ АУТЕНТИФИКАЦИЕЙ»

Обучающийся Зубишин Степан Алексеевич

Обозначение ВКР 10.05.02.770000.000 группа ВИБТ61

Тема утверждена приказом по ДГТУ от «23» июня 2022 г. № 2831-ЛС-О

Срок представления ВКР к защите «\_\_» \_\_\_\_\_\_\_\_\_ 2023 г.

Исходные данные для выполнения выпускной квалификационной работы:

Методы и средства сетевой аутентификации: протоколы: TACACS, RADIUS; службы Windows Server: система доменных имён, active directory, служба политики сети.

Содержание выпускной квалификационной работы

Введение: Во введении необходимо изложить актуальность выбранной темы, обозначить объект и предмет исследования, цель и задачи выпускной квалификационной работы, теоретическую и практическую значимость работы, структуру работы.

Наименование и краткое содержание разделов:

1. Анализ технологии беспроводного доступа Wi-Fi. Развитие технологий беспроводного доступа. Основные методы передачи и модуляции сигнала. Основные стандарты 802.11. Топология беспроводных сетей. Беспроводное оборудование Wi-Fi сетей. Защита беспроводных сетей.

2. Централизованная аутентификация и авторизация. Модели разграничения доступа. Проверка подлинности в доменной сети. Протоколы аутентификации: TACACS, TACACS+, RADIUS, DIAMETR.

3. Практическая реализация централизованной аутентификации и авторизации. Общая структура телекоммуникационной сети. Настройка сервера на выполнение функций DNS, контроллера домена и управления сетевыми политиками. Настройка аутентификации и авторизации на сетевом оборудовании по протоколу RADIUS. Настройка пользовательских устройств. Оценка достижений цели.

4. Безопасность и экологичность проекта. Влияние шума на организм человека и защита от них. Расчет уровня шума на рабочем месте. Экологичность работы. Организация и обеспечение пожарной безопасности на предприятии. Выводы.

5. Экономическое обоснование. Спецификация проекта. План–график проектирования и разработки системы. Расчет затрат на разработку проекта.

Заключение: Заключение должно содержать обобщенные результаты проведенной работы в соответствии с поставленной целью и задачами, необходимо указать чем завершается работа – усовершенствованием, модернизацией, дать свои предложения.

Перечень графического и иллюстративного материалов:

1. Общая структура телекоммуникационной сети
2. Регистрация сервера сетевых политик в Active Directory
3. Настройка параметров RADIUS-сервера для точки доступа

Руководитель ВКР \_\_\_\_\_\_\_\_\_\_\_\_\_\_ доц., к.т.н. В.В. Галушка

(подпись, дата)

Задание к исполнению принял \_\_\_\_\_\_\_\_\_\_\_\_\_\_ С.А. Зубишин

**Аннотация**

Выпускная квалификационная работа посвящена изучению централизованной аутентификации, авторизации и учета в компьютерных сетях, использующих беспроводную передачу данных как основной способ взаимодействия. Исследовано развитие технологии беспроводной переда данных. Проведен сравнительный анализ методов шифрования, протоколов аутентификации и авторизации. На основе полученных данных предложен проект беспроводной корпоративной сети с доменной аутентификацией.

Объем текстового материала 89 листов (А4), количество иллюстраций 39, таблиц — 14, использованных источников — 17.

**Abstract**

Graduate qualification work is devoted to the study of centralized authentication, authorization and accounting in computer networks that use wireless data transfer as the main method of interaction. The development of wireless data transfer technology is investigated. A comparative analysis of encryption methods, authentication and authorization protocols was conducted. On the basis of the obtained data, a project of a wireless corporate network with domain authentication was proposed.

The volume of text material is 89 sheets (A4), the number of illustrations is 39, tables - 14, sources used - 17.

Содержание

[Введение 7](#_Toc125240746)

[1 Анализ технологии беспроводного доступа Wi-Fi 8](#_Toc125240747)

[1.1 Развитие технологий беспроводного доступа 8](#_Toc125240748)

[1.2 Основные методы передачи и модуляции сигнала 11](#_Toc125240749)

[1.3 Основные стандарты 802.11 13](#_Toc125240750)

[1.4 Топология беспроводных сетей 16](#_Toc125240751)

[1.5 Беспроводное оборудование Wi-Fi сетей 19](#_Toc125240752)

[1.5.1 Wi-Fi адаптеры 19](#_Toc125240753)

[1.5.2 Точки доступа Wi-Fi 20](#_Toc125240754)

[1.6 Защита беспроводных сетей Wi-Fi 21](#_Toc125240755)

[1.6.1 Протоколы беспроводной безопасности 24](#_Toc125240756)

[1.6.2 Контроль зоны покрытия беспроводного сигнала 27](#_Toc125240757)

[2 Централизованная аутентификация и авторизация 30](#_Toc125240758)

[2.1 Протокол TACACS 38](#_Toc125240759)

[2.2 Протокол TACACS+ 40](#_Toc125240760)

[2.3 Протокол RADIUS 42](#_Toc125240761)

[2.4 Протокол DIAMETER 43](#_Toc125240762)

[3 Практическая реализация 46](#_Toc125240763)

[3.1 Общая структура телекоммуникационной сети 46](#_Toc125240764)

[3.2 Настройка контроллера домена 47](#_Toc125240765)

[3.3 Настройка авторизации на сетевых устройствах через RADIUS 52](#_Toc125240766)

[3.4 Оценка достижений цели 62](#_Toc125240767)

[4 Экономическое обоснование 63](#_Toc125240768)

[4.1 Спецификация проекта 63](#_Toc125240769)

[4.2 План-график проектирования и разработки системы 64](#_Toc125240770)

[5 Безопасность и экологичность работы 73](#_Toc125240771)

[5.1 Влияние шума на организм человека 74](#_Toc125240772)

[5.2 Экологичность работы 76](#_Toc125240773)

[5.3 Организация и обеспечение пожарной безопасности на предприятии 82](#_Toc125240774)

[5.4 Вывод 85](#_Toc125240775)

[Заключение 87](#_Toc125240776)

[Перечень использованных информационных ресурсов 88](#_Toc125240777)

# **Введение**

В настоящее время во всем мире растёт потребность в беспроводном широкополосном доступе. Заметен стремительный рост количества мобильных устройств и мобильных сетей в домах, квартирах, на предприятиях, в транспорте и в городах. Кроме того, беспроводные технологии стали общепринятым стандартом, который оказывает всестороннее влияние на нашу жизнь. Подавляющее большинство школьников, студентов и работников предприятий используют портативные устройства, которыми являются смартфоны, планшеты и ноутбуки, как основные средства связи.

Беспроводные сети обеспечивают подключение пользователей там, где затруднено кабельное подключение или необходима полная мобильность. Такими местами выступают кафе, гостиницы, транспорт, учебные заведения. При этом отсутствует трудность взаимодействия с проводными сетями. В настоящее время, при проектировании любых сетей – от домашней до предприятия, необходимо учитывать беспроводные решения.

В свою очередь, чем распространение технология, тем больше злоумышленников захотят воспользоваться уязвимостями, которыми она обладает. В результате возникают угрозы нарушения конфиденциальности, целостности и доступности информации, обращающейся в сети. Для того чтобы обезопасить пользователей, пользующихся беспроводными сетями, существуют различные протоколы аутентификации. В данной выпускной квалификационной работе представлена настройка протокола RADIUS для реализации доменной аутентификации, который позволяет повысить безопасность беспроводной сети предприятия и централизованно управлять доступом к ней.

# **Анализ технологии беспроводного доступа Wi-Fi**

# **Развитие технологий беспроводного доступа**

Wi-fi – это технология беспроводной локальной сети с устройствами на основе стандартов IEEE (Институт инженеров электротехники и электроники (англ. Institute of Electrical and Electronics Engineers)) 802.11. Беспроводной протокол обмена данными был создан инженером Джоном О’Салливаном в 1991 году в лаборатории радиоастрономии CSIRO в Канберре, Австралия.

В настоящее время различают несколько типов беспроводных сетей, а именно (рисунок 1):

1. WPAN (Wireless Personal Area Network) или WPAC (Wireless Personal Area Connectivity) - беспроводная персональная сеть.
2. WLAN (Wireless Local Area Network) - беспроводная локальная сеть.
3. WMAN (Wireless Metropolitan Area Networks) - беспроводная сеть масштаба города.
4. WWAN (Wireless Wide Area Network) - беспроводная глобальная сеть.

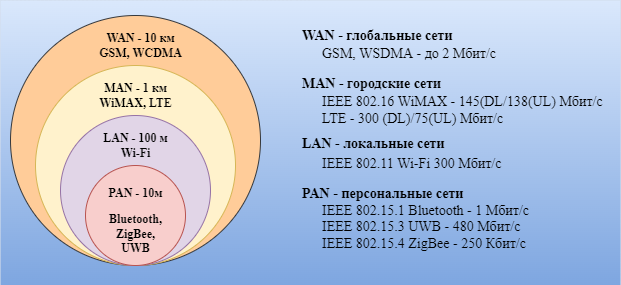


Рисунок 1 – Радиус действия беспроводных сетей.

При построении сетей WLAN и WPAN, а также систем широкополосного беспроводного доступа (WMAN или BWA - Broadband Wireless Access) применяются сходные технологии. Ключевое различие между ними - диапазон рабочих частот и характеристики радиоинтерфейса. (рисунок 2). Сети WLAN и WPAN работают в нелицензионных диапазонах частот 2,4 и 5 ГГц, т. е. при их развертывании не требуется частотного планирования и координации с другими радиосетями, работающими в том же диапазоне. Сети BWA (Broadband Wireless Access) используют как лицензионные, так и нелицензионные диапазоны (от 2 до 66 ГГц).

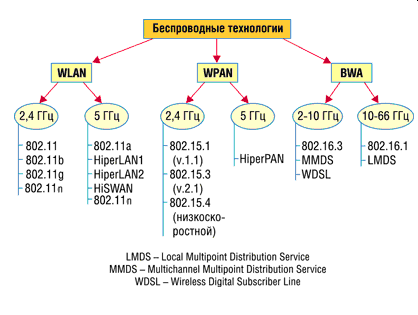


Рисунок 2 – Классификация беспроводных технологий

Персональная беспроводная сеть (WPAN) – система беспроводной передачи данных, работающая преимущественно в низкочастотном диапазоне, которая обеспечивает подключение в радиусе до нескольких десятков метров. Сеть такого типа применяется для подключения различных устройств, таких как бытовая и оргтехника, средства связи к компьютеру, или пары находящихся рядом компьютеров без использования проводного соединения. Для создания персональных беспроводных сетей используется несколько технологий, среди которых основной является Bluetooth. Она была создана компаний Ericsson в 1994 году и представляет на данном этапе развития максимальную пропускную способность в 1 Мбит/с в радиусе около 100 метров в старых версиях и до 1500 метров начиная с версии 5.0. Эта технология также известна как IEEE 802.15.1, по сравнению с другими технологиями имеет низкое энергопотребление, что делает ее особенно удобной для использования в небольших устройствах.

Беспроводная глобальная вычислительная сеть (WWAN) – разновидность беспроводных компьютерных сетей, главной особенностью которой является широкая зона охвата.

Основным отличием WWAN от локальных беспроводных сетей (WLAN) является использование технологии сотовой связи, например, GSM, UMTS, GPRS, CDMA2000, CDPD, Mobitex, LTE. Такие услуги предлагают операторы регионального, национального или даже глобального масштаба. Технологии WWAN дают пользователю возможность получать доступ к глобальной сети интернет, пользоваться электронной почтой и подключаться к виртуальным частным сетям из любой точки в пределах зоны действия оператора беспроводной связи, имея WWAN адаптер в его мобильном устройстве. Во многих устройствах присутствует уже встроенный адаптер.

Основным предназначением беспроводных локальных сетей (WLAN) является организация доступа к информационным ресурсам внутри здания с различных устройств. Из-за невысокой стоимости и простоты установки часто используется для организации общественных коммерческих точек доступа (hot spot) в людных местах. Например, в кафе, гостиницах, аэропортах, общественном транспорте, а также организация временных сетей на период проведения мероприятий (конференций, выставок).

Беспроводные локальные сети базируются на основе семейства стандартов IEEE 802.11. Эти сети также известны как Wi-Fi (Wireless Fidelity), и хотя сам термин Wi-Fi в стандартах явным образом не прописан, этот бренд получил в мире широкое распространение.

# **Основные методы передачи и модуляции сигнала**

В зависимости от стандарта беспроводной сети методы передачи и модуляции на физическом уровне меняются. Это обусловлено ограничениями каждой технологии и стремлением достичь новых результатов при использовании новейших технологий. На сегодняшний день существуют следующие методы беспроводной передачи сигнала:

* Метод прямой последовательности расширения спектра (DSSS - Direct Sequence Spread Spectrum) заключается в приведении узкополосного спектра сигнала е его широкополосному представлению, что делает возможным увеличение помехоустойчивость передаваемых данных. При использовании метода диапазон 2400 – 2483,5 МГц разделяется на четырнадцать перекрывающихся каналов или на три неперекрывающихся канала. Данные передаются по одному каналу;
* Метод псевдослучайной перестройки рабочей частоты (FHSS - Frequency-Hopping Spread Spectrum) заключающийся в частой смене несущей частоты. При использовании данного метода диапазон 2400 – 2483,5 МГц разделяется на семьдесят девять каналов шириной по 1 МГц. На основе одной из двадцати двух возможных схем, согласованных отправителем и получателем, последовательно передаются данных по разным каналам;
* Метод мультиплексирования с ортогональным частотным разделением каналов (OFDM - Orthogonal Frequency-Division Multiplexing) осуществляет параллельную передачу данных по нескольким частотам выделенного диапазона, что делает его существенно быстрее и надежнее методов DSSS и FHSS. Поддерживает работу в диапазонах, выделенных для беспроводной передачи данных, 2,4 ГГц и 5 ГГц;
* Метод двоичного пакетного сверточного кодирования (PBCC - Packet Binary Convolutional Coding) заключающийся в добавлении выбранного числа дополнительных бит каждому основному биту данных при прохождении сверточного кодера. Избыточность кода позволяет повысить устойчивость к помехам и декодировать сообщение, даже если часть его будет утеряна в процессе передачи или приема;
* Метод пространственного кодирования сигнала MIMO (Multiple Input Multiple Output) позволяет увеличить полосу пропускания канала за счёт использования нескольких передающих и принимающих антенн. Антенны разнесены настолько, чтобы минимально оказывать взаимное влияние друг на друга. В отдельно взятый момент времени передача сигнала происходит только одному клиенту.
* Метод пространственного кодирования сигнала MU-MIMO (Multi-User Multiple Input Multiple Output) является улучшенной версией MIMO и позволяет в отдельно взятый момент времени передавать сигнал нескольким клиентам, что существенно увеличивает общую пропускную способность.

Для того чтобы повысить качество сигнала и избежать множества издержек необходимо производить его модуляцию – изменение одно или нескольких параметров высокочастотного несущего колебания по закону низкочастотного информационного сигнала. На данном этапе развития беспроводной передачи сигнала существуют следующие типы модуляции:

* Квадратурная амплитудная модуляция (QAM – Quadrature Amplitude Modulation). Используется при скорости передачи данных от 24 Мбит/с. Повышение скорости передачи заключается в изменении фазы сигнала и изменении его амплитуды. При этом применяются модуляции 16-QAM, 64-QAM, 256-QAM и 1024-QAM позволяющие кодировать различное количество бит (4, 6, 8 и 12) в одном символе при 16, 64, 256 и 1024 разных состояниях сигнала соответственно;
* Двоичная фазовая манипуляция (BPSK – Binary Phase-Shift Keying). Заключается в смещении фазы несущего колебания на одно из двух значений, нуль или π. Является простейшей формой фазовых манипуляций;
* Квадратурная фазовая манипуляция (QPSK – Quadrature Phase-Shift Keying). Использует созвездие из четырех точек, равноудаленных друг от друга и расположенных на окружности. Применяя QPSK на символ приходится два бита.

# **Основные стандарты 802.11**

В базовом (изначальном) стандарте 802.11 регламентируется работа оборудования на центральной частоте 2,4 ГГц с максимальной скоростью до 2 Мбит/с. С развитием технологии далеко ушли ограничения по максимальной скорости передачи данных, а также увеличилось количество доступных для передачи частот. В настоящее время используются преимущественно стандарты группы IEEE 802.11, перечисленные в таблице 1.

Таблица 1 – основная группа стандартов 802.11

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Показатель | Стандарт | | | | | |
| 802.11a | 802.11.b | 802.11g | 802.11n | 802.11ac | 802.11ax |
| Частотный диапазон, ГГц | 5,15-5,25 | 2,4-2,483 | 2,4-2,483 | 2,4 или 5,0 | 5,0 | 2,4 или 5,0 |
| Метод передачи | OFDM | DSSS | DSSS,  OFDM | OFDM-MIMO | MIMO, MU-MIMO | OFDMA, MU-MIMO |
| Скорость, Мбит/с | 6-54 | 1-11 | 1-54 | 6-600 | до 7 Гбит/с | до 11 Гбит/с |
| Совместимость | 802.11 n | 802.11 g/n | 802.11 b/n | 802.11 a/b/g | 802.11 a/b/g/n | 802.11a/b/g/n/ac |

Окончание таблицы 1

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Показатель | Стандарт | | | | | |
| 802.11a | 802.11b | 802.11a | 802.11n | 802.11a | 802.11ax |
| Метод модуляции | BPSK, QPSK OFDM | QPSK, DQPSK, DBPSK | BPSK, QPSK  OFDM | BPSK, 64-QAM | 256-QAM,OFDM | BPSK, QPSK, 1024-QAM, OFDMA, |
| Дальность связи в помещении, м | 0 – 20 | 20 – 100 | 20 – 50 | 50 – 100 | 50 – 100 | 100 |
| Дальность связи вне помещения, м | 100 | До 150 | До 150 | 250 | 300 | 300 |

Стандарт IEEE 802.11b был принят в 1999 году и являлся наиболее популярным благодаря ориентации на диапазон частот 2,4 ГГц. Максимальная скорость передачи данных у оборудования, работающего на базе этого стандарта, до 11 Мбит/с. Метод прямой последовательности (DSSS) был выбран для высокоскоростной передачи широкополосного канала. В этом стандарте также используется мониторинг качества канала, что позволяет автоматически изменять скорость передачи данных в зависимости от уровня сигнала и помех.

Стандарт IEEE 802.11a использует две центральные частоты в районе 5 ГГц (на территории РФ выделены частотные полосы 5,150-5,350 и 5,650-6,425 ГГц) и максимальная скорость передачи составляет до 54 Мбит/с. Является наиболее «широкополосным» из семейства 802.11. В качестве основного метода модуляции выбрано мультиплексирование с ортогональным частотным разделением сигналов (OFDM), что обеспечивает высокую устойчивость связи в условиях многолучевого распространения сигнала.

Стандарт IEEE 802.11g был одобрен в 2003 году. Является третьей модификацией стандарта для беспроводных локальных сетей и представляет собой развитие IEEE 802.11b. Он использует аналогичный частотный диапазон, но при этом скорость передачи данных возрастает до 54 Мбит/с благодаря использованию более эффективного метода модуляции сигнала – ортогонального частотного мультиплексирования, протестированного ранее при разработке стандарта 802.11a.

Стандарт IEEE 802.1n был принят в сентябре 2009 года и способен обеспечивать скорость передачи данных до 450 Мбит/с, а в идеальных условиях и 600 Мбит/с, что повышает, по сравнению с устройствами предыдущего стандарта, скорость передачи в 4-11 раз. В данном стандарте появляется важное нововведение – MIMO (много входов, много выходов). Данная технология осуществляет пространственное мультиплексирование: одновременную передачу нескольких информационных потоков по одному каналу, что увеличивает пропускную способность устройств, работающих по стандарту 802.11n.

Стандарт 802.11ac был принят в январе 2014 года. Является дальнейшим развитием технологий, введенных в стандарт 802.11n, но в отличие от него использует только диапазон частот 5 ГГц. Вследствие большего распространения устройств, работающих в диапазоне 2,4 ГГц, диапазон 5 ГГц является менее подверженным помехам, что повышает стабильность и скорость соединения. Также появляется технология многопользовательский MIMO (MU-MIMO), что также позволяет увеличить пропускную способность сети, за счет увеличения скорости передачи данных до 7 Гбит/с.

Стандарт 802.11ax утвержден в феврале 2021 года и является последней модификацией стандарта беспроводных локальных сетей на данный момент. Поддерживает работу в двух диапазонах 2.4 и 5 ГГц, но может включать дополнительные полосы частот в диапазонах от 1 до 6 ГГц. Также работает с технологиями MIMO и MU-MIMO, но превосходит предыдущие версии за счет использования многопользовательского мультиплексирования с ортогональным разделением сигнала (OFDMA). Это в свою очередь позволяет данной модификации достигать максимальной скорости передачи данных до 11 Гбит/с. Хотя увеличение скорости не является таким существенным, но главным выступает увеличение пропускной способности устройств почти в 4 раза по сравнению с 802.11ac.

# **Топология беспроводных сетей**

Сети стандарта 802.11 могу строиться по любому режиму организации беспроводных Wi-Fi сетей:

1. Независимый базовый набор услуг (Ad-Hoc или IBSS – Independent Basic Service Set).
2. Инфраструктурный базовый набор услуг (BSS - Basic Service Set).
3. Расширенная набор услуг (ESS – Extended Service Set).

Независимый базовый набор услуг (рисунок 3) представляет собой простейшую беспроводную локальную сеть, когда абонентские станции (компьютеры или ноутбуки) взаимодействуют друг с другом напрямую. Для построения такой сети необходимо чтобы каждая абонентская станция была оборудована адаптером WLAN стандарта 802.11. Данная топология в основном применяется в целях быстрого развёртывания сети и имеет большое количество изъянов, таких как ограничение дальности взаимодействия и высокая уязвимость к атакам.

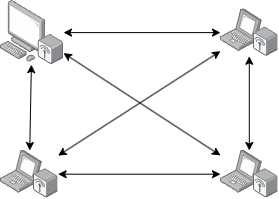


Рисунок 3 – Структура IBSS

Инфраструктурный базовый набор услуг (рисунок 4) в отличии от независимого базового набора услуг (IBSS) создается на основе точки доступа (Access Point, AP), через которую взаимодействуют сетевые узлы. Также точка доступа может выступать в роли моста для подключения беспроводных устройств к внешней проводной сети. Плюсом данной топологии выступает возможность подключения большого количества пользователей, более высокая помехоустойчивость, высокий уровень безопасности.

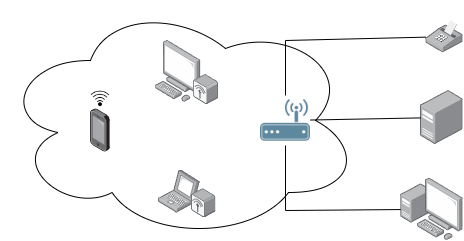


Рисунок 4 - Структура BSS

Расширенный набор услуг (рисунок 5) – это беспроводная сеть, созданная объединением нескольких точек доступа или инфраструктур BSS. Таким образом, несколько BSS, соединённых распределительной системой, образуют расширенный набор услуг (ESS). Расширенную топологию удобно применять для объединения в единую сеть нескольких пользователей или подключить несколько проводных или беспроводных сетей. Для соединения между собой точек доступа не обязательно применять проводное соединение, так как спецификация стандарта 802.11 оставляет возможность реализации этого канала в виде беспроводного.

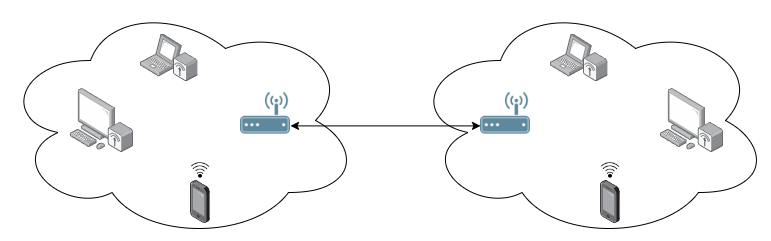


Рисунок 5 – Структура ESS

# **Беспроводное оборудование Wi-Fi сетей**

Главное преимущество беспроводных сетей – отсутствие кабелей, что позволяет предоставить подключение пользователя там, где по каким-либо причинам невозможно или затруднено подключение по обычным линейным-кабельным линиям связи. При этом беспроводные сети могут без проблем взаимодействовать с обычными проводными сетями.

# **Wi-Fi адаптеры**

Wi-Fi адаптер – это сетевое устройство, позволяющее подключить компьютер к беспроводной сети. Чаще всего в устройствах уже есть встроенный сетевой адаптер для проводного или беспроводного подключения.

Любой беспроводной адаптер должен соответствовать нескольким требованиям:

* Необходима совместимость со стандартами;
* Работа в нелицензируемом диапазоне частот 2,4 ГГц или 5ГГц;
* Поддерживать протоколы безопасности (WEP, WPA, WPA2).

По типу интерфейса все Wi-Fi адаптеры можно разделить на две группы (рисунок 6):

Адаптеры USB. В настоящее время они более распространены за счет их компактности и простоты настройки, а USB интерфейс обеспечивает функцию «горячего подключения»;

Адаптеры PCIe. Предназначены в основном для настольных компьютеров. Такие устройства подключаются непосредственно к материнской плате устройства.

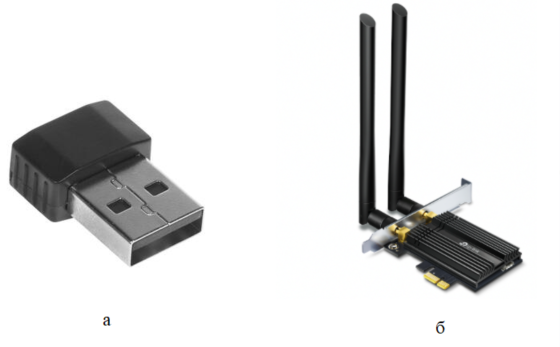


Рисунок 6 – Беспроводные адаптеры: а – адаптер USB, б – адаптер PCIe

# **Точки доступа Wi-Fi**

Точка доступа Wi-Fi (AP) - это сетевое устройство, которое обеспечивает беспроводной доступ к уже существующей сети (беспроводной или проводной) или создание новой беспроводной сети.

Все точки доступа можно разделить по способу подключения:

* Через USB порт;
* Через порт RJ45.

Точки доступа с подключением по обычной витой паре пользуются наибольшим успехом. Положительной стороной такого подключения является простота настройки и управления, а также большая скорость передачи в локальную сеть. Точки доступа могут быть внутреннего и наружного исполнения (рисунок 7). Для создания беспроводной сети внутри помещений используют внутренний вариант прибора. Он обладает меньшей стоимостью и чаще всего большим эстетическим видом. Работают такие точки доступа в пределах одной или нескольких комнат. На открытых участках местности (прямая видимость) возможна работа на расстоянии до 300 метров с использованием стандартных всенаправленных антенн. Точки доступа внешнего исполнения предназначены для создания беспроводной сети между зданиями. В зависимости от типов антенн такие устройства способны организовывать каналы связи на расстояния до 5 км.

Наибольший интерес вызывают беспроводные точки доступа, объединяющие в себе функции нескольких устройств, например, высокоскоростного беспроводного широкополосного маршрутизатора со встроенным коммутатором Fast Ethernet. Маршрутизатор позволяет быстро и легко настроить общий доступ к Интернет для проводной или беспроводной сети, или организовать совместного использование широкополосного канала связи и кабельного/DSL модема дома или в офисе.



Рисунок 7 – Исполнения точек доступа: а – внутреннее, б – внешнее

# **Защита беспроводных сетей Wi-Fi**

Беспроводные сети распространены в организациях любого масштаба. Преимущество использования Wi-Fi на малых и средних предприятиях достигается за счёт низкой цены и простоты развертывания. В крупных же организациях беспроводное соединение может использоваться как для делового общения сотрудников, так и для личных целей. Поэтому чтобы использовать все преимущества беспроводных сетей необходимо обеспечивать их защиту.

Под защитой информации понимают процесс, направленный на достижение состояния информационной безопасности. В свою очередь информационная безопасность – это состояние защищенной среды, при котором обеспечиваются ее основные аспекты, а именно:

* Конфиденциальность – состояние информации быть недоступной или закрытой для неавторизованных лиц, сущностей или процессов;
* Целостность – состояние информации, при которой ее модификация осуществляется только субъектами, имеющими на это право;
* Доступность – состояние информации, при котором субъекты, имеющие права доступа, могут реализовывать их беспрепятственно.

Нарушение какого-либо аспекта информационной безопасности происходит вследствие реализации угрозы. Угроза – это потенциальная опасность для информации или системы в случае эксплуатации недостатка системы.

Для рассматриваемых в работе систем беспроводной передачи данных перечисленные угрозы являются актуальными, хотя и имеют свою специфику. В целом, беспроводные сети считаются гораздо уязвимее, чем проводные, так как в проводных сетях данные могут быть перехвачены только в том случае, если злоумышленник получит физический доступ к среде передачи. В беспроводных сетях сигнал распространяется в эфире, поэтому любой, находящийся в зоне приема сигнала, может перехватить этот сигнал.

Обеспечить целостность и доступность информации, передаваемой по беспроводным каналам также значительно сложнее чем для проводных линий связи. Целостность означает, что данные не были изменены при выполнении какой-либо операции над ними. Однако невозможно исключить влияние помех, искажающих информацию для каналов радиосвязи. Для устранения негативных эффектов от них используются общие принципы обеспечения целостности, такие как дублирование информации или обеспечение возможности её восстановления. В системах связи дублирование выражается в посылке нескольких одинаковых сигналов подряд в расчёте на то, что, если часть из них будет искажена, остальные дойдут в правильном виде и будут интерпретированы принимающей стороной.

Для проверки целостности также используются значения, рассчитываемые как функция от основных данных, которые добавляются в конец передаваемого сообщения. Для вычисления контрольной суммы могут использоваться как криптографические, так и не криптографические функции. Наибольшей популярностью пользуется алгоритм вычисления контрольной суммы на основе циклического избыточного кода (англ. Cyclic redundancy check — CRC). Такие контрольные суммы просты в реализации и имеют хорошее соотношение количества избыточных данных к количеству обнаруживаемых ошибок. Криптографические хеш-функции также позволяют вычислять некоторые значения на основе передаваемых данных. Они, хотя и сложнее в реализации, позволяют осуществлять не только контроль целостности, но и аутентификацию отправителя.

Также следует учитывать, что помехи могут иметь также искусственное происхождение и создаваться злоумышленником намеренно, чтобы вызвать сбой в работе радиотехнического оборудования. Такие помехи, скорее всего, будут иметь достаточно широкий спектр, а также учитывать особенности работы оборудования, на которое они нацелены. Полностью избежать воздействия помех при передаче сигналов по радиоканалу невозможно.

Наибольшую угрозу целостности и конфиденциальности данных может нанести реализация злоумышленником атаки типа «человек посередине» (англ. Man In The Middle — MITM), которая также имеет свои особенности для беспроводных каналов передачи данных. Её техническая реализация требует внедрения злоумышленника в канал связи между устройствами, обменивающимися информацией. Однако, в условия использования радиоволн нет необходимости физически находиться между взаимодействующими устройствами. Перехват, искажение или подмена радиосигнал может быть осуществлена удалённо, при наличии достаточно мощного передатчика и чувствительного приёмника.

В целях обеспечения безопасности беспроводных сетей немаловажным процессом является аутентификация пользователя – доказательство подлинности лица, получающего доступ к элементам системы. Пользователь при подключении к сети должен предъявить доказательства, что он именно тот пользователь, идентификатор которого он вводит. Устройств, которые взаимодействуют по сети, должны предоставить друг другу доказательства своей подлинности и что ни одно из них не используется злоумышленником для ответвления или прослушивания трафика. Для этого должна быть предусмотрена процедура взаимной аутентификации устройств в протоколе взаимодействия. Взаимная аутентификация необходима для обеспечения безопасности сеанса взаимодействия между пользователем и сервером. Аутентификацию можно проводить как к отдельному пользователю, так и к целой группе пользователей.

В результате можно сделать вывод, что беспроводная связь является более уязвимой к различным атакам по сравнению с другими способами передачи данных, что приводит к повышению требований информационной безопасности для неё. Для снижения вероятности перехвата и несанкционированного доступа к информации путём прослушивания радиоэфира в беспроводных устройствах контролируется зона распространения сигнала и применяются криптографические средства защиты, включая шифрование и аутентификацию.

# **Протоколы беспроводной безопасности**

Одной из основных проблем, отсутствующей в проводных сетях, с безопасностью является общедоступность Wi-Fi сигнала. Например, чтобы подслушивать сообщения в проводной сети необходим физический доступ к такому сетевому оборудованию как коммутатор, маршрутизатор, брандмауэр, хост-компьютер или сетевая розетка. В свою очередь для подслушивания беспроводной сети достаточно приемника. Из-за данной особенности разработчики стандарта в 1997 году одобрили механизм Wired Eqiuvalent Privacy (WEP). В WEP применяется общий ключ, известные беспроводным клиентам и узлам доступа, с которыми они обмениваются информацией. Ключ можно использовать как для шифрования, так и для аутентификации в сети. Стремясь повысить безопасность беспроводных сетей, некоторые изготовители оборудования разработали расширенные алгоритмы со 128-разрадными и более длинными ключами WEP, состоящими из 104-разрядной и более длинной части пользовательского ключа, и вектора инициализации (рисунок 8).



Рисунок 8 – Шифрование данных алгоритмом WEP

Однако, увеличение длины ключа не смогло устранить проблемы алгоритма, выявленные в процессе эксплуатации, такие как слабый механизм аутентификации, раскрытие ключей шифрования методами криптоанализа и другие. На сегодняшний день данный алгоритм является надежным.

Недостатки WEP-шифрования и несовместимость с разработками различных компаний привело к тому, что ассоциация Wi-Fi Alliance приняла решение разработать единый стандарт защиты беспроводных сетей – Wi-Fi Protected Access (WPA), схема шифрования которого представлена на рисунке 9.



Рисунок 9 – Шифрования данных алгоритмом WPA

Данный стандарт превосходит WEP-шифрование за счёт добавления протокола TKIP (Temporal Key Integrity Protocol, протокол целостности временного ключи), которые использует двухуровневую систему векторов инициализации, и надежному механизму аутентификации на базе стандарта IEEE 802.11x и протокола EAP (Extensible Authentication Protocol, расширяемый протокол аутентификации). В 2004 году было принято расширения 802.11i, в котором утвердили стандарт WPA улучшив его до WPA2 для совместимости с симметричным алгоритмом блочного шифрования (AES, Advanced Encryption Standard) на смену TKIP и WEP. Плюсом WPA2 выступает обратная совместимость с WPA.

В начале 2018 года международный альянс Wi-Fi Alliance анонсировал новейший протокол беспроводной безопасности WPA3. Основными дополнениями, реализованными в этом протоколе, стали: встроенная защита от атак методом перебора паролей, индивидуальное шифрование данных для повышения конфиденциальности пользователей в открытых Wi-Fi сетях, усовершенствованный криптографический стандарт для сети Wi-Fi – «192-разрядный пакет безопасности». Так как главной уязвимостью WPA2 являлась атака с переустановкой ключей (Key Reinstallation attack - KRACK), воздействовавшая на алгоритм четырёхстороннего рукопожатия, то в WPA3 добавлена обязательная поддержка более надежного метода соединения SAE (Simultaneous Authentication of Equals), направленного на обеспечение защиты беспроводных сетей от автономных атак по словарю). В соответствии с методом SAE две и более стороны устанавливают криптографические ключи на знании пароля одной или несколькими сторонами. Результирующий сессионный ключ, полученный каждой стороной для аутентификации соединения, выбирается на основе информации из ключей, пароля и MAC-адресов сторон. Также реализован контроль целостности трафика на основе механизма защищенного управления кадрами PMF (Protected Management Frames).

# **Контроль зоны покрытия беспроводного сигнала**

Также проблема общедоступности Wi-Fi сигнала заставляет задуматься о контроле зоны распространения беспроводного сигнала в целях затруднения доступа потенциального злоумышленника, имеющего подслушивающее устройство.

В большинстве малых и средних офисах в качестве беспроводного оборудования используется одна точка доступа для всего офиса (рисунок 10). В целях доступности во всех помещениях беспроводной сети с высоким качеством сигнала увеличивается мощность передающего устройства, следствием этого значительно увеличивается зона покрытия Wi-Fi сигнала. В свою очередь это дает злоумышленнику возможность принимать сигнал с большого расстояния, оставаясь не замеченным.

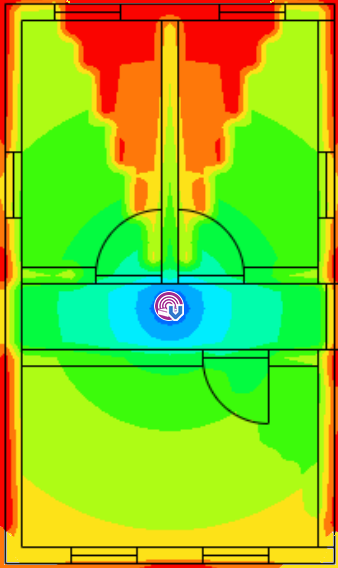


Рисунок 10 – Зона покрытия при использовании одной точки доступа

Данная проблема может быть решена использование большего числа точек доступа (рисунок 11). Это в свою очередь позволит эффективно распределить передающие устройства по площади помещения, а также даст возможность снизить уровень сигнала, не позволяя ему выходить за периметр контролируемой зоны. В данном случае, злоумышленнику потребуется приблизиться вплотную к зданию, что не останется не замеченным.

Для организации офисной Wi-Fi сети при использовании нескольких сетевых устройств целесообразно использовать технологию mesh-сети, которая позволяет не только объединить все точки доступа в единую беспроводную сеть с бесшовным роумингом между ними, но увеличить эффективность передачи данных. Также это может повысить общий уровень безопасности за счёт разбиения сети на изолированные друг от друга зоны.

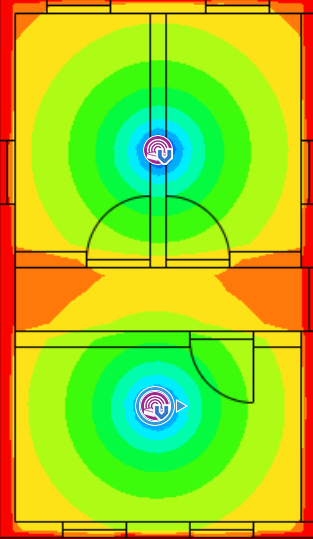


Рисунок 11 – Зона покрытия при использовании нескольких точек доступа

# **Централизованная аутентификация и авторизация**

Как было замечено раньше аутентификация – это доказательство подлинности лица, получающего доступ к элементам системы. Существуют различные методы аутентификации, различающиеся в зависимости от используемого аутентификатора, а также каким образом организован обмен данными между аутентифицируемым и аутентифицирующим элементами системы.

В теории аутентификация человека со стопроцентной надежностью является невыполнимой задачей, так как отсутствуют такие аутентификаторы, который бы с абсолютной уверенностью могли доказать аутентичность человека. Пароль можно узнать у человека методами социальной инженерии или перехватить в момент его ввода или отправки, электронный ключ – выкрасть, а большинство биометрических данных – подделать.

На деле при аутентификации ограничиваются не стопроцентным, но достаточно высоким уровнем аутентичности пользователя. Применяющиеся при этом аутентификаторы разделяют на три класса, которые также называют факторами:

* «что-то, что знаю» - включает в себя правила преобразования информации, одноразовые и многоразовые пароли;
* «что-то, что имею» - к этому классу относятся различные аппаратные аутентификаторы, которые могут быть исполнены в виде RFID, токена или ключ-карты, эти ключи имеют в своей основе защищенные электронные устройства, выполняющие функции шифрования;
* «что-то, чем являюсь» - в этот класс попадают различные биометрические показатели, использующиеся для аутентификации, такие как отпечаток пальца или рисунок радужной оболочки глаза.

В процессе аутентификации могут задействоваться несколько аутентификаторов, которые относятся к разным классам, в таком случае такая аутентификация будет называться многофакторной. Также этот термин может применятся для обозначения процесса многоступенчатой аутентификации, при которой применяются несколько аутентификаторов, относящихся к одному и тому же классу. В настоящее время двухфакторная аутентификации на основе пароля и аппаратного ключа получила наибольшее распространение.

После прохождения процесса аутентификации, пользователю предоставляются права доступ к защищаемым системой ресурсам, этот процесс называется авторизацией, а процедура приведения авторизации в действие – управление доступом. При грамотно настроенной авторизации, если пользователь попытается получить доступ к запрещенному для него ресурсу, то эта попытка должна быть отклонена механизмом контроля доступа.

Для разграничения доступа пользователей к защищаемым ресурсам принято придерживаться принципа минимальных привилегий, в соответствии с которым каждому пользователю должен быть назначен минимальный набор прав доступа, достаточный для выполнения им должностных обязанностей. Этот принцип ограничивает возможные потери, нанесенные случайными ошибками пользователей или их действиями, на которые у них нет полномочий. Для авторизации существует два различных подхода:

* Выделение особого полномочного органа, принимающего все решения о присвоении пользователю прав доступа на все защищаемые ресурсы в системе;
* Делегирование принятия решений другим пользователям или элементам системы.

Реализация этих подходов управления доступом может быть представлена различными способами, которые представляют различные методы и исполнения ограничений, тем не менее на практике эти способы можно отнести к некоторой из категорий:

* Мандатный метод управления доступом;
* Дискреционный метод управления доступом;
* Ролевой метод управления доступом.

Также система управления доступом может основываться на сочетании этих категорий.

Мандатный метод доступа реализуют схему, в которой субъекты и объекты разделяются на несколько групп, каждой из которых присваиваются метки безопасности. Для групп объектов в качестве метки безопасности выступает уровень секретности этой группы, а для групп субъектов – уровень допуска к объектам различной степени секретности. Предусматривается обязательное назначения меток безопасности всем субъектам и объектам, находящимся в системе, для того чтобы система принимала решение о допуска или запрете на их основе. Мандатный метод описывается моделью Белла-Лападулы, представленной на рисунке 12.

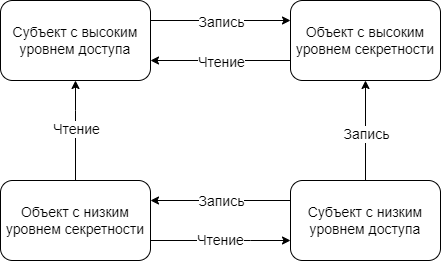


Рисунок 12 – Модель Белла-Лападулы

Мандатное разграничение доступа имеет следующие особенности, отличающие его от других:

* Проведение процесса авторизации и управления доступом выполняет центральный полномочный орган, который отвечает за безопасность. Зачастую на эту роль назначается операционной системе;
* Операционная система принимает решение о допуске или запрете к определенному объекту динамически, на основе правил, разработанных с учетом политики безопасности.

Данный метод разграничения доступа является наиболее безопасным по сравнению с остальными, так как ограничивает действия пользователей без возможности гибкой настройки прав доступа.

Дискреционный доступ является средством разграничения доступа к различным объектам системы, которое основывается на присвоении уникальных идентификаторов субъектам или группам, в которые входит этот субъект. Отличительными чертами данного метода являются:

* Права доступа задаются на основе списком контроля доступа, предоставляющие расширенные возможности настройки разрешенных операций и для каждого пользователя или группы пользователей в отношении каждого объекта системы. Пользователю, группе пользователей или объекту присваиваются уникальный идентификатор;
* Делегирование права на возможность управления доступом пользователям, которые владеют объектом. Следовательно, пользователи-владельцы могут назначать права доступа для других пользователей или групп пользователей к объектам, владельцами которых они являются, по личному усмотрению.

Следствием указанных особенностей является распределение процедуры авторизации между некоторым количеством пользователей-владельцев. В свою очередь владельцем может считаться пользователь, создавший объект, или пользователь, которого назначали на владение объектом другие пользователи с более высокими правами.

Преимуществом дискреционного разграничения доступа является высокая гибкость настройки полномочий, выраженная в возможности предоставления или ограничения доступа со стороны пользователей к своим ресурсам, а также расширенной настройкой допустимых операций.

Ролевое управление доступом базируется на назначении всем пользователям определенных «ролей», предназначенных для целей авторизации, которые могут быть выделены на основе должностных обязанностей или должности в целом. Необходимо соблюдать соответствие ролей и должностей, существующих на предприятии, для правильного разграничения доступа. Также существует возможность присвоения одной и той же роли для нескольких пользователей одновременно, так как они могут быть назначены на одну и ту же должность. Аналогично у одного пользователя может быть несколько ролей, так как он может сочетать несколько должностей.

Разрешения присваиваются не пользователям или группам пользователей, а ролям, которые в дальнейшем будут приписаны к определенному пользователю (рисунок 13). Для каждой роли необходимо определить разрешения, достаточные для выполнения пользователями их должностных обязанностей, в зависимости от назначенной роли, что способствует более четкому распределению обязанностей в организации.

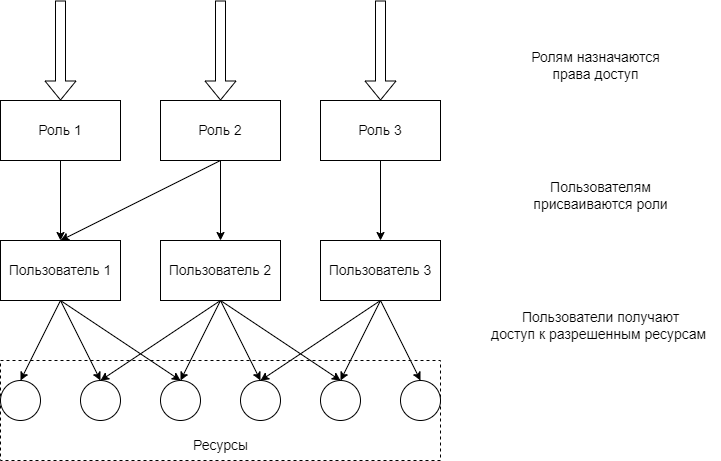


Рисунок 13 – Авторизация в ролевом разграничении доступа

Выделяют следующие особенности ролевого разграничения доступа:

* Совмещение особенностей мандатного и дискреционного методов разграничения доступа;
* Упрощенная система администрирования по сравнению с дискреционной моделью;
* Так же как мандатный метод является централизованным методом управления доступом, но обладает преимуществом гибкой настройки прав доступа;
* Не является хорошо масштабируемым. В организациях с большим количеством сотрудников поддержание большого количества ролей выступает трудоемкой и сложной работой.

В связи с тем, что в любой организации задумываются о том, как будет проходить аутентификация пользователя в корпоративной сети, как разграничить полномочия пользователей и вести учет используемых сетевых ресурсов, следует продумывать как будут проходить все эти процессы ещё на стадии планирования.

Первым шагом в решении перечисленных проблем является организация вместо корпоративной сети, функционирующей на основе рабочих групп, доменной сети, которая позволит управлять доступом сотрудников к ресурсам сети, предоставит централизованное управление учетными записями пользователей и за счет гибкости настройки систем аутентификации значительно повысят безопасность информационной инфраструктуры организации.

Домен является основной единицей администрирования сетевой инфраструктуры предприятия, в которую входят все сетевые объекты, например, компьютеры, принтеры, пользователи, общие ресурсы. В настоящий момент, подавляющее большинство доменных сетей организованы на базе службы каталогов Active Directory для операционных систем семейства Windows Server, которая представляет собой распределённую базу данных, содержащую все объекты домена. Для хранения базы данных используются выделенные серверы, называемые контроллерами домена.

Организация, которая переходит с использования рабочих групп на доменную сеть, получает следующий преимущества:

* Единую точку аутентификации. Учётные записи пользователей хранятся в базе данных контроллера домена и все устройства обращаются к ней за авторизацией, в отличие от рабочей группы, в которой необходимо вручную добавлять на каждый компьютер в сети список пользователей, которым необходим сетевой доступ;
* Единую точку управления политиками. При использовании Active Directory, пользователей распределяют по подразделениям, к которым применяются единые групповые политики. Политики предоставляют возможность использовать единые параметры для подразделений и пользователей. В рабочей группе все компьютеры в сети равноправны и отсутствует возможность управления другими компьютерами, что делает невозможным использование единых параметров на всех устройствах в сети;
* Повышенный уровень информационной безопасности. Это преимущество достигается за счёт использования единой защищенной базы данных учётных записей, хранящейся на защищенном от внешнего доступа контроллере домена. Также преимуществом является использования более продвинутого и защищенного протокола аутентификации.

Проверка подлинности в доменной сети происходит с помощью служб аутентификации SAM (диспетчер учётных записей безопасности (от англ. Security Account Manager)), в старых версиях операционных систем, и Active Directory в современных. При вводе логина и пароля пользователя механизм системы преобразует эту информацию и с помощью протоколов аутентификации, использующимися для транспортировки, передает запрос контроллеру домена для последующей обработки. В настоящее время основными протоколами являются следующие:

* LAN Manager. Генерирует хеш паролей, который в дальнейшем используется для процесса аутентификации. Считается ненадежным за счёт ограничения длины пароля в четырнадцать символов и простого алгоритма хеширования, который позволяет преобразовать хеша обратно в текст;
* NTLM (NT LAN Manager). При появлении нового поколения операционных систем компания Microsoft спроектировала новый протокол, устраняющий недостатки предыдущего. Он способен содержать пароль до 128 символов и использует более надежный алгоритм преобразования в хеш, а также расширенный список доступных символов для пароля;
* NTLMv2 (NTLM версии 2). Улучшенная версия NTLM, использующая более защищенный алгоритм хеширования HMAC-MD5, а также присваивающая последовательности запрос-ответ метки времени, чтобы избежать атак с предварительно записанными учетными данными легитимных пользователей для последующего использования;
* Kerberos. Выбираемый по умолчанию протокол доменной аутентификации. Является самым безопасным из перечисленных протоколов за счёт взаимной аутентификации между клиентом и сервером, шифрованием всех сеансов связи, добавления метки времени последовательности запрос-ответ.

После успешной проверки данных службой аутентификации система собирает данные о членстве пользователя в группах. Зачастую пользователь является членом нескольких групп. Система проверяет локальные и глобальные группы на контроллере домена и присваивает учетной записи маркер доступа. При обращении к ресурсам система предоставляет доступ на основании полученного от отправителя запроса маркера доступа и списка контроля доступа, заданного на ресурсе.

Для централизованной аутентификации и авторизации, а также учёта используемых ресурсов при подключении к беспроводной точке доступа, VPN-серверам или коммутаторам и маршрутизаторам с проверкой подлинности требуется использование протоколов аутентификации отличных от принятых по умолчанию на контроллере домена. К наиболее распространенным протоколам централизованного контроля доступа относятся протоколы TACACS (англ. Terminal Access Controller Access Control System) и RADIUS (англ. Remote Authentication in Dial-In User Service), а также их усовершенствованные версии TACACS+ и DIAMETER. Для использования данных протоколов возможно использовать как контроллер домена, так и отдельный сервер, называемый серверов доступа.

# **Протокол TACACS**

Сеансовый протокол TACACS изначально использовался на серверах доступа ARPNET (компьютерная сеть, созданная Агентством Министерства обороны США и являвшаяся прототипом сети интернет).

Протокол стандартизирует схему взаимодействия серверов доступа с сервером TACACS на основе определения возможных типов запросов, соединений и ответов. Сервер получает строго определенный запрос от клиента и должен ответить на него соответствующим сообщением. Также определяются несколько типов соединений на основе последовательности пар запросов и ответов.

Заданы три типа соединений:

* AUTH – выполняется только аутентификация;
* LOGIN – выполняется аутентификация и фиксируется логическое соединение с пользователем;
* SLIP – выполняется аутентификация, фиксируется логическое соединение и подтверждается IP-адрес.

При помощи соединения типа AUTH серверы доступа перенаправляют серверу TACACS запросы на логическое подключение пользователей ко всей сети. При этом сервер доступа посылает всего одно сообщение – пакет AUTH, ответом на который является сообщение REPLY. Пакет AUTH имеет формат (username, password, line, style), в котором:

* username – имя пользователя;
* password – пароль пользователя;
* line – номер порта, по которому установилось соединение;
* style – способ аутентификации.

Сервер TACACS проверяет данные и отправляет ответ в виде пакета REPLY, где указывает успешно или неуспешно прошла аутентификация. Явным минусом протокола является передача пароля между сервером доступа и сервером TACACS в открытом виде.

В свою очередь тип соединения LOGIN перенаправляет запросы на логическое подключение к отдельным устройствам в сети. Запрос LOGIN имеет следующий вид (username, password, line), где значения полей идентичны запросу AUTH. Ответ всегда имеет вид (result1, result2, result3), в котором все поля – это целые числа, конкретные значение которых в протоколе не уточняются. Они могут быть интерпретированы в соответствии с соглашением, между конкретным типом сервера доступа и сервером TACACS. Например, на серверах доступа Cisco поле result3 понимается как номер списка прав доступа, который необходимо применить к запрашивающему подключение пользователю.

Соединение типа SLIP применятся, когда назначена дополнительная проверка IP-адреса пользователя. Запрос формируется только после установления соединения типа LOGIN. Данное соединение имеет запросы двух форм. Для начала соединения используется SLIPON (username, password, line, SLIPaddress), где к уже известным полям добавляется SLIPaddress, в которое указывается IP-адреса пользователя, запросившего соединение, ответы сервера на этот запрос аналогичны ответам в соединение LOGIN (result1, result2, result3). Для окончания соединения применятся запрос SLIPOFF (username, password, line, reason), где в поле reason указывается причина по которой удаленное подключение разрывается.

# **Протокол TACACS+**

Недостаток протокола, связанные с передачей пароля в открытом виде, был устранен компанией Cisco в новой версии протокола, которая получила название «TACACS+». В данной версии пароль для передачи по сети шифруется с помощью алгоритма MD5.

TACACS+ основан на стандартах TCP и является простым протоколом управления доступом, функционирует по технологии клиент-сервер.

В процессе аутентификации, протокол использует три типа пакетов: START (начало), CONTINUE (продолжение) и REPLY (ответ). Данный процесс можно описать следующим образом (рисунок 14):

* сервер доступа посылает пакет START серверу TACACS+ для начала процесса аутентификации;
* в ответ получает пакет GETUSER, содержащий запрос имени пользователя;
* сервер доступа запрашивает у клиента имя пользователя и отправляет его серверу TACACS+ вложенным в пакет CONTINUE;
* в ответ приходит пакет GETPASS, включающий запрос пароля;
* аналогично с именем пользователя сервер запрашивает пароль и отправляет введенные данные серверу защиты в пакете CONTINUE;
* сервер защиты проверяет данные полученные данные и высылает в ответ пакет PASS (успех) или FAIL (неудача), который указывает на результат аутентификации.

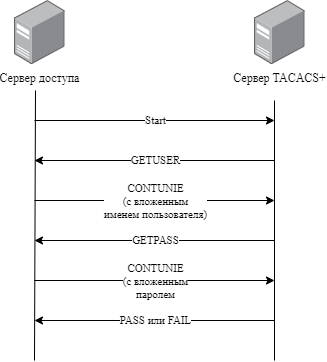


Рисунок 14 – Процесс аутентификации через сервер TACACS+

Процесс авторизации с помощью протокола TACACS+ происходит при помощи двух типов пакетов: REQUEST (запрос) и RESPONSE (ответ). Процесс контролируется посредством обмена парами «атрибут/значение» между сервером доступа и сервером TACACS+, которые содержат фиксированный набор полей, идентифицирующих процесс или пользователя и переменный набор аргументов, которые описывают сервисы и параметры, необходимые для авторизации.

Процесс аудита TACACS+ во многом схож с процессом авторизации, в нем используются такие же типы пакетов. Во время аудита создаются информационные записи о пользовательской активности в различных сервисах.

# **Протокол RADIUS**

В 1997 Карлом Ригни, работающим на тот момент в компании Livingston Enterprises, был разработан протокол RADIUS (англ. Remote Authentication in Dial-In User Service), который передает сведения между центральной платформой и оборудованием для реализации централизованной аутентификации, авторизации и сбора сведений об использованных ресурсах.

В настоящее время протокол используется для получения доступа виртуальным частным сетям, точкам беспроводного доступа, коммутаторам, DSL и другим типам сетевого доступа. Открытость, простота внедрения и постоянное усовершенствование сыграли важную роль в становлении RADIUS’а одним из основных стандартов для удаленной и централизованной аутентификации.

Принцип работы протокола можно описать следующим образом (рисунок 15): пользователь отправляет запрос на сервер доступа для подключения к определенному сетевому ресурсу, используя сертификат доступа. Данный сертификат пересылается на сервер доступа и далее отправляется на RADIUS-сервер (Access-Request). Запрос включает в себя сертификаты доступа, предоставленные в виде имени пользователя и пароля или сертификата безопасности. Также запрос может включать в себя дополнительные параметры проверки, такие как номер телефона, сетевой адрес устройства пользователя, информацию о физическом адресе.

Далее, при помощи выбранной в процессе настройки схемы аутентификации (PAP, CHAP, EAP, MD5), RADIUS-сервер проверяет эту информацию на корректность.

После проверки серверу доступа поступает один из трех возможных ответов:

* Access-Reject указывает на неверный пользовательский запрос;
* Access-Challenge, который запрашивает дополнительную информацию от пользователя, например, пин-код, второй пароль и т.п.;
* Access-Accept указывает, что пользователю разрешен доступ. Далее происходит проверка авторизации на использование запрошенных ресурсов.

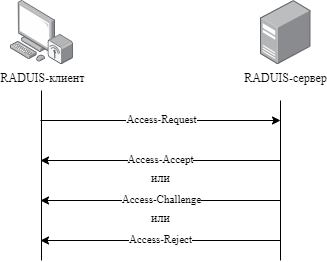


Рисунок 15 – Процесс аутентификации через RADUIS-сервер

# **Протокол DIAMETER**

Существует также улучшенная версия протокола RADIUS, называемая DIAMETR. Он значительно расширяет возможности предыдущей версии и устраняет проблемы с надежностью, масштабируемостью, безопасностью и гибкостью.

Как и RADIUS, DIAMETER используется для аутентификации, авторизации и учета, но использует протоколы гарантированной доставки сообщений TCP и SCTP вместо UDP, передавая этим протоколам обнаружение проблем связи и их обработку.

Протокол имеет одноранговую архитектуру, в которой каждый сетевой узел может выступать в роли клиента либо сервера, в зависимости от инфраструктуры сети. В связи с этим «DIAMETER-узел» применяется для обозначения «DIAMETER-клиент», «DIAMETER-сервер» или «DIAMETER-агент».

В протоколе явно определен узел, выступающий в роли агента. Он выступает в качестве промежуточного узла между клиентом и серверов и выполняет функции управления трафиком. Определяется четыре типа агентов:

* Relay Agent (агент-ретранслятор). Применяется для перенаправления сообщения определенному адресату в зависимости от информации, которая содержится в сообщении. Этот агент может агрегировать запросы от различных областей (регионов) в определенную область. Никак не модифицирует поля в сообщении;
* Proxy Agent (прокси-агент). Аналогично агенту-ретранслятору используется для перенаправления сообщений, но также может изменять содержимое сообщения, что расширяет его возможности. Например, можно предоставлять дополнительные службы, применять правила для определенных типов сообщений или выполнять административные задачи для областей;
* Redirect Agent (агент перенаправления). Выступает в качества централизованной точки контроля маршрутов других DIAMETER-узлов. Получая сообщение, он проверяет свою таблицу маршрутизации и указывает ее в ответном сообщении. Это снижает нагрузку на другие узлы, так как им нет необходимости хранить таблицу маршрутизации локально;
* Translation Agent (агент преобразования). Используется для преобразования сообщения из одного вида протокола доступа в другой, в случае их несовместимости. Например, выполнить преобразование между двумя разными версиями DIAMETER или осуществить преобразование из RADIUS в DIAMETER и обратно.

Сообщения в протоколе используются для передачи управляющей команды или оповещений сторонни DIAMETER-узлам. Для различных целей протокол имеет разные типы сообщений, определяющиеся их кодом команды. Реальные данные передаются в формате пар атрибут/значение (AVP). Набор общих атрибутов предопределен. Плюсом выступает возможность личного написания таких атрибутов с соответствием с форматом, определенным в протоколе. Указанные AVP передают информацию о маршрутизации, безопасности и возможностях между двумя DIAMETER-узлами.

Установление сессии по протоколу можно свести к следующему (рисунок 16): клиент отправляет сообщение к серверу доступа, которое содержит запрос аутентификации и уникальный идентификатор сессии, через агента, в зависимости от типа, агент выполняет заложенные в него действия и направляет запрос серверу доступа. Ответный AVP от сервера клиенту также направляется через агента.

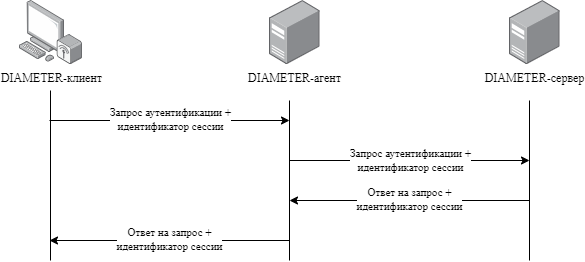


Рисунок 16 – Процесс установления DIAMETER сессии

# **Практическая реализация**

# **Общая структура телекоммуникационной сети**

Общая структура телекоммуникационной сети, описывающая основные элементы, представлена на рисунке 17.

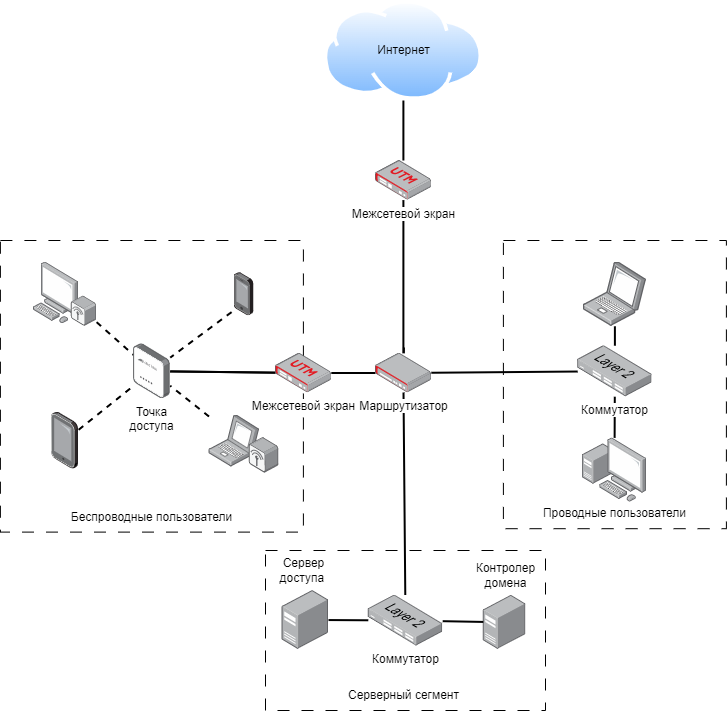


Рисунок 17 – Общая структура телекоммуникационной сети

В корпоративной сети можно выделить несколько сегментов:

* Беспроводные пользователи. В данный сегмент входят корпоративные или личные беспроводные устройства, такие как ноутбук, планшет, телефон, периферийные устройства, подключаемыми через точку доступа установленную в помещении организации;
* Проводные пользователи. В сегменте располагаются устройства, подключаемые по проводным линиям связи. Примером таких устройств могут быть компьютеры, ноутбуки, а также периферийные устройства;
* Серверные сегмент. Данный сегмент выделен под серверы, необходимые для эффективного и защищенного функционирования сети, такие как контролер домена и сервер доступа (могут быть установлены на одном сервере).

# **Настройка контроллера домена**

Настройка выполняется с использованием виртуальных машин на базе Windows Server 2012 R2 и Windows 10, а также физическое оборудование, такое как ноутбук на базе Windows 10 и маршрутизатор Mikrotik «RB951Ui-2HnD».

Первым шагом в настройке сервера является присвоение ему статического IP-адреса (рисунок 18), а также смена имени сервера на «srv-domain-ctrl».

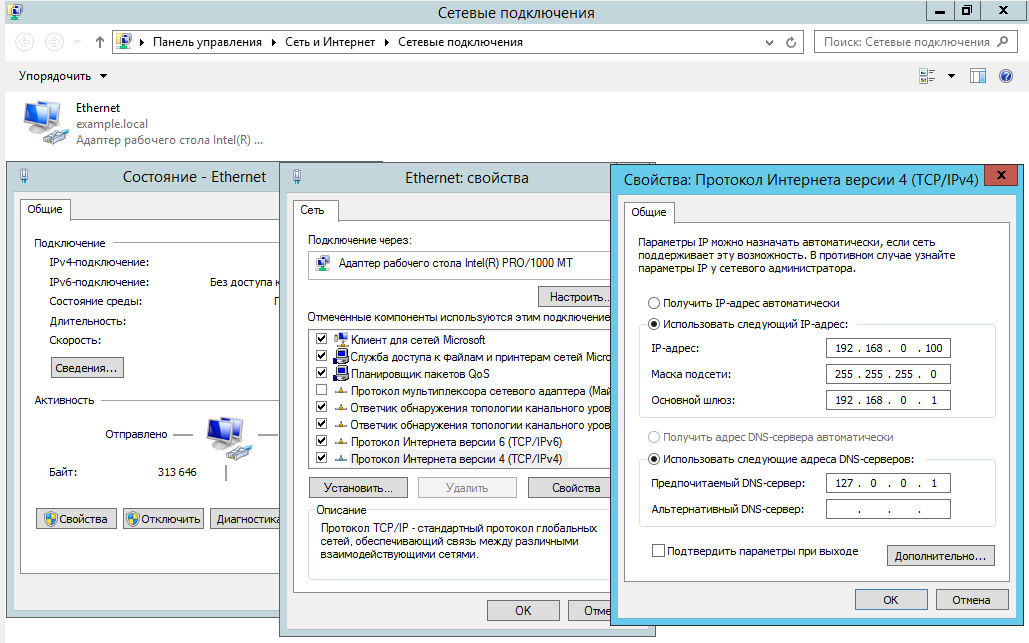


Рисунок 18 – Задание статического IP-адреса серверу

Далее нужно установить на сервер с помощью мастера добавления ролей и компонентов роль «DNS-сервер». Эта роль нужна для поддержки доменных служб, таких как Netlogon, при предоставлении устройствам в сети возможности находить контроллеры домена.

При помощи диспетчера DNS необходимо создать зону прямого просмотра, которая указывает, что создаваемый DNS-сервер будет полномочным для DNS-имен локальных ресурсов, но все остальные запросы пересылает поставщику услуг Интернета. Назовем ее по имени будущего домена «example.local».

Аналогично добавлению роли «DNS-сервер», нужно добавить роль «Доменные службы Active Directory». После добавления роли необходимо запустить мастер установки доменных служб, чтобы назначить сервер полнофункциональным контроллером домена. Для этого нужно перейти в меню «Выполнить» сочетанием клавиш Win+R и ввести там команду dcpromo.exe, либо перейти в мастер установки через графический интерфейс утилиты «Диспетчер серверов».

В открывшемся меню управления, необходимо создать новый домен в новом лесу (рисунок 19).

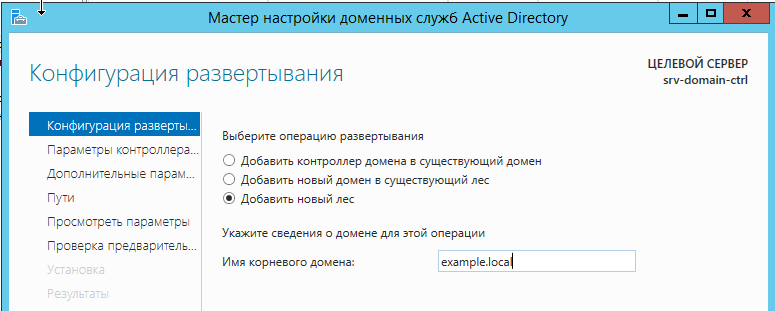


Рисунок 19 – Создание нового леса и домена

После перезагрузки, при помощи имени домена, указанного перед именем пользователя через обратный слеш (\), можно убедится, что вход осуществляется от имени доменного администратора, а не локального.

Завершив настройки Active Directory, необходимо разрешить службе DNS принимать обновление сопоставлений доменного имени и IP-адреса при подключении новых устройств к домену. Для этого нужно открыть диспетчер сервера, развернуть в дереве конфигурации следующие узлы: «Роли» → «DNS-сервер» → «DNS» → «srv-domain-ctrl» → «Зоны прямого просмотра», нажать правой кнопкой мыши на «example.local» и выбрать «Свойства». В появившемся окне нужно нажать кнопку «Изменить…» напротив надписи «Тип: Основной» и в следующем окне необходимо установить галочку «Хранить зону в Active Directory» (рисунок 20).

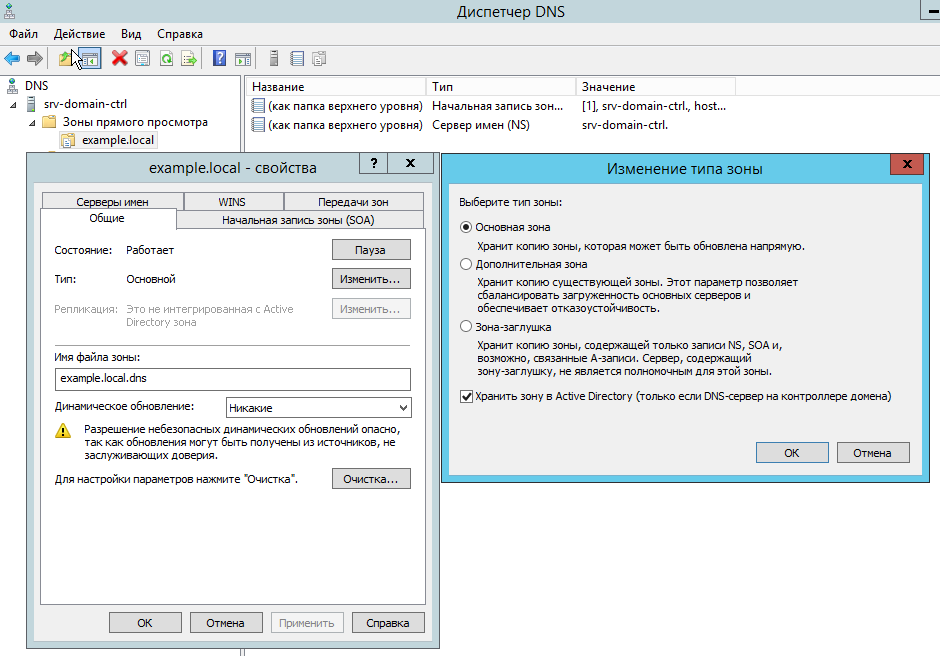


Рисунок 20 – Интеграция доменной зоны с Active Directory

Далее необходимо переходим во вкладку «Серверы имен», выбрать нужный сервер и нажать кнопку «изменить». К имени сервера необходимо дописать имя домена «example.local» и нажать кнопку «Разрешить в адрес».

На этом базовая настройка контролера домена закончена и можно переходить к настройке виртуальной машины пользователя.

Зададим статический IP-адрес виртуальной машине пользователя по аналогии с тем как это делалось в Windows Server. Параметры сетевого подключения укажем следующие: IP-адрес – 192.168.0.101, маска подсети – 255.255.255.0 и предпочитаемый DNS-сервер – 192.168.0.100. Далее проверим наличие связи с виртуальной машиной с Windows Server командой «ping».

После того как связь проверена перейдем к подключению виртуальной машины пользователя к домену.

Перейдем в меню настройки системы и выберем пункт меню «Дополнительные параметры системы». В появившемся окне нужно нажать кнопку «изменить» и ввести имя компьютера «pc-example», после этого укажем, что компьютер является членом домена «example.local» (рисунок 21).

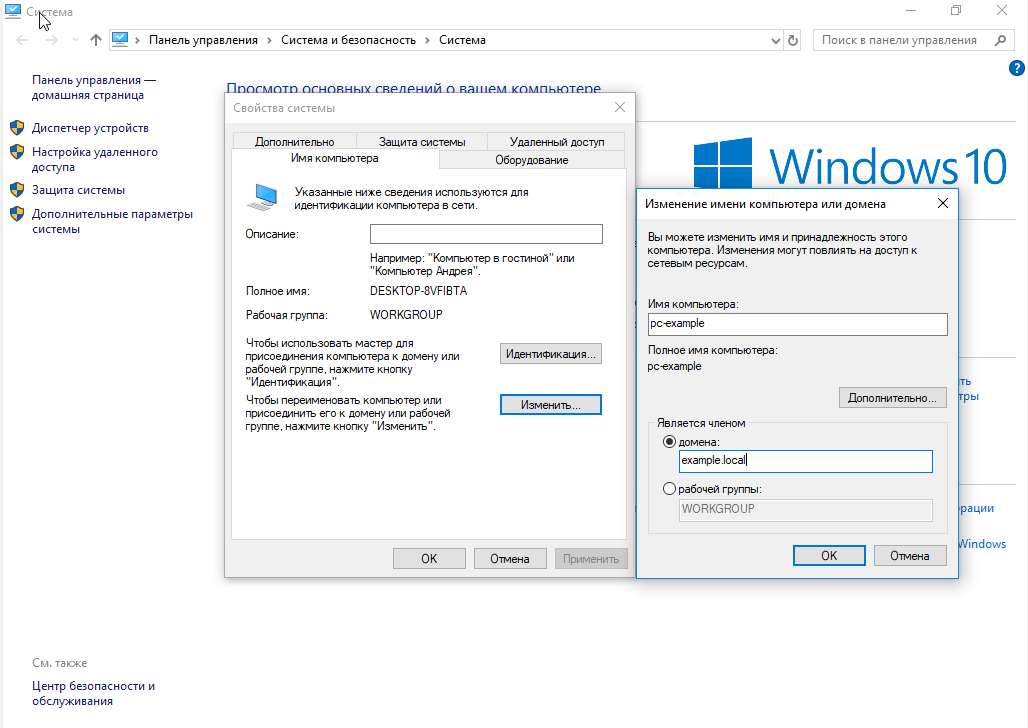


Рисунок 21 – Подключение виртуальной машины пользователя к домену

После ввода логина и пароля администратора домена, система оповестит о наличии ошибок или выведет сообщение об успешном подключении к домену.

Проверить наличие компьютера в домене можно как локально на самом компьютере, наведя мышку на иконку подключения, так и с Windows Server. Для проверки необходимо перейти в меню «Active Directory – пользователи и компьютеры» и выбрать в домене «example.com» директорию «Computers», в которой должна находится подключенная виртуальная машина пользователя (рисунок 22).

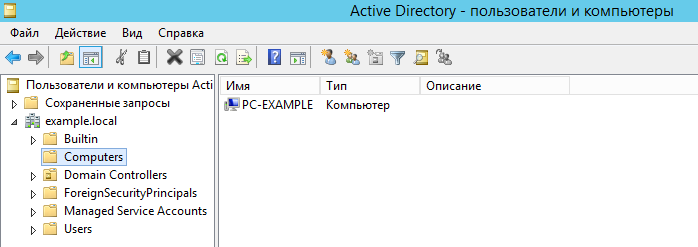


Рисунок 22 – Проверка наличия виртуальной машины пользователя в домене

# **Настройка авторизации на сетевых устройствах через RADIUS**

Для начала необходимо настроить сервер централизованной аутентификации, авторизации и сбора событий, для этого будем использовать сервер – контроллер домена.

Первым шагом является запуск мастера добавления ролей и компонентов и установить «Службы политик сети и доступа» со всеми ее компонентами, по аналогии с добавлением ролей «DNS-сервер» и «Active Directory контроллер домена», что даст возможность установить RADIUS-сервер для контроля подключений.

На этапе выбора служб роли достаточно выбрать «сервер политики сети», так как необходимые протокол RADIUS уже включен в состав выбираемой роли (рисунок 23).

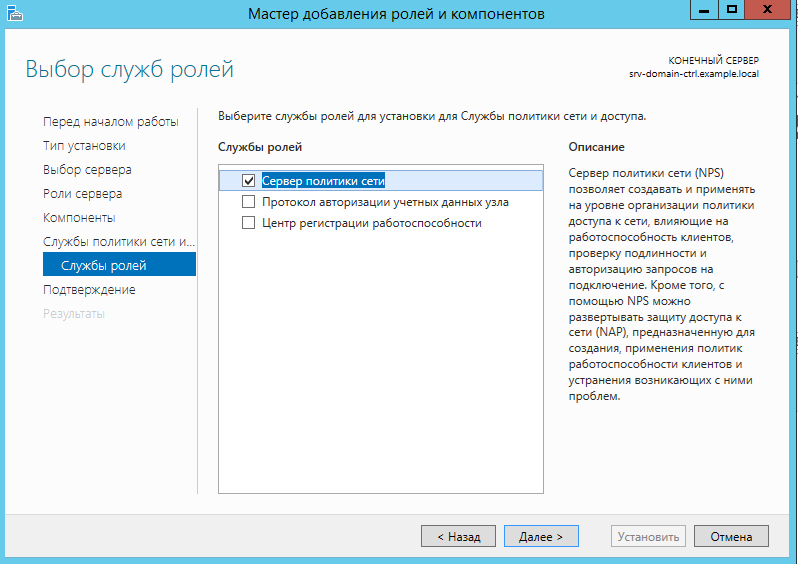


Рисунок 23 – Добавление роли «Сервер политики сети»

Для использования всего функционала сервера политик сети необходимо зарегистрировать его в домене Active Directory. Для этого нужно перейти в настройки сервера сетевых политик и нажать правой кнопкой мыши по «NPS (локально)» и выбрать пункт «Зарегистрировать сервер в Active Directory» (рисунок 24).

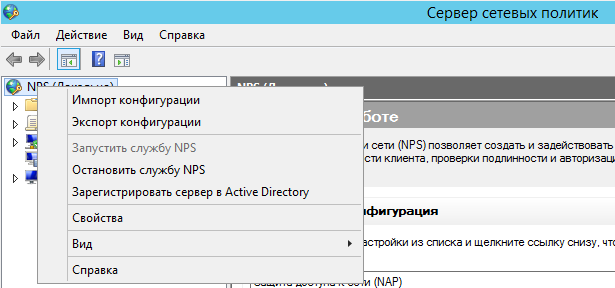


Рисунок 24 – Регистрация NPS-сервера в Active Directory

После этого нужно выдать разрешение серверу на чтение свойств учетных записей пользователей, относящихся к параметрам удаленного доступа. Сервер при этом будет добавлен во встроенную группу «Серверы RAS и IAS» (рисунок 25).

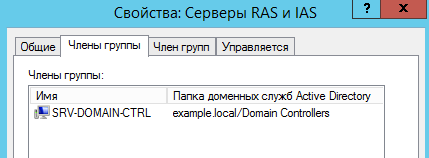


Рисунок 25 – Члены группы «Серверы RAS и IAS»

Далее нужно создать группу безопасности «mikrotik-example-group» в домене Active Directory (рисунок 26), в которую необходимо добавить пользователя «admin-mikrotik», которому в дальнейшем рприсвоить полномочия для аутентификации на сетевых устройствах.

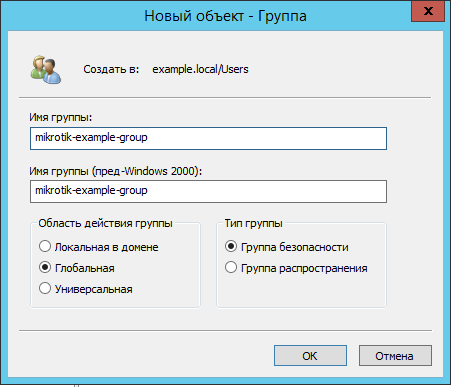


Рисунок 26 – Создание группы безопасности Active Directory

Далее следует переходить к добавлению клиента RADIUS. Для этого в дереве консоли сервера сетевых политик нужно развернуть раздел «RADIUS-клиенты и серверы» и в элементе «RADIUS-клиенты» выбрать пункт «новый документ» (рисунок 27).

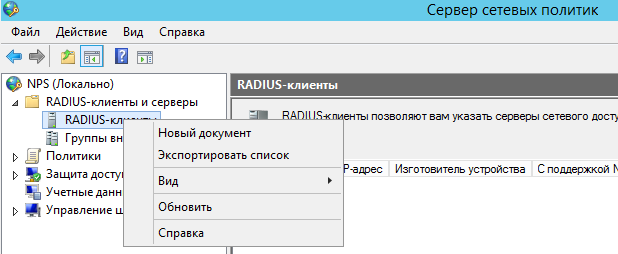


Рисунок 27 – Добавление RADIUS-клиента

В появившемся окне, во вкладке «Параметры» необходимо включить RADIUS-клиента, заполнить поля «Понятное имя» и «Адрес», а также придумать пароль и вписать его в поля «Общий секрет» и «Подтверждение общего секрета» (рисунок 28).

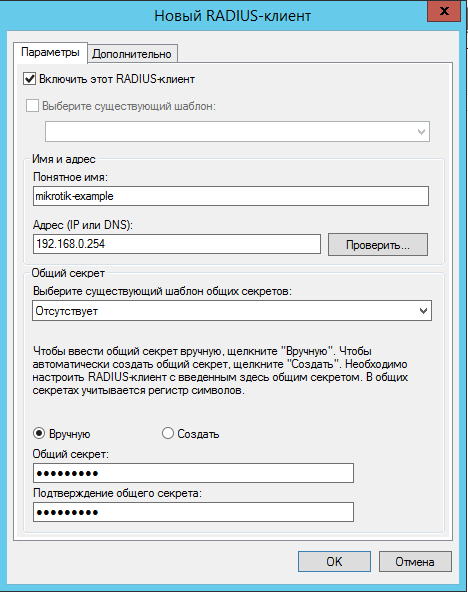


Рисунок 28 – Создание нового RADIUS-клиента

Далее необходимо связать RADIUS-клиента и доменную группу пользователей, создав политику на RADIUS-сервере. Для этого нужно открыть ветку «Политики» и создать новый документ в сетевых политиках.

После указания имени необходимо задать условия для подключения. Следует выбрать условие, что пользователь должен являться членом доменной группы «mikrotik-example-group».

В методах проверки подлинности следует указать шифрованную проверку подлинности второй версии (MS-CHAP-v2).

Обязательно для оборудования Mikrotik нужно во вкладке «Параметры» настроить атрибуты RADIUS, зависящие от поставщика (рисунок 29) и указать следующие настройки:

* Поставщик – Пользовательский;
* Атрибут – Vendor-Specific.

Настройки в следующем меню:

* Код поставщика – 14988;
* Указать что атрибут спецификации RADIUS RFC соответствует атрибутам поставщика.

В настройках атрибута:

* Назначенный поставщиком номер атрибута – 3;
* Формат атрибута – строковый;
* Значение атрибута – full.

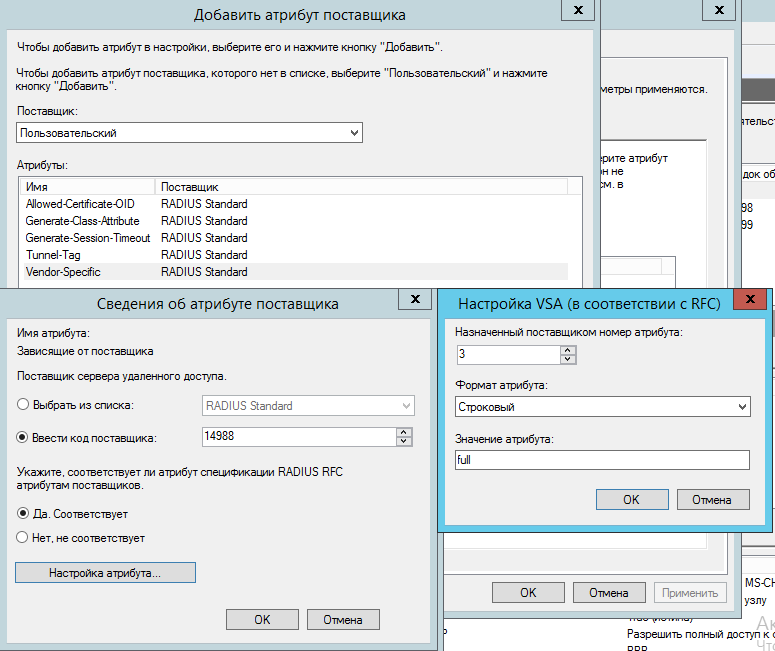


Рисунок 29 – Настройка атрибутов RADIUS-клиента

Дальнейшие пункты настройки политики необходимы для тонкой настройки, которые в рамках данной выпускной квалификационной работы не рассматриваются, поэтому их можно пропустить.

На последнем экране необходимо убедиться в правильности всех созданных настроек политики. После проверки подтвердить создание политики, нажав кнопку «Готово».

Перейдем к настройке маршрутизатора, выполняющего функции точки доступ «Mikrotik».

Первым шагом нужно задать беспроводному интерфейсу ip-адрес 192.168.0.254 и проверить связь с сервером доступа командой ping.

Далее все настройки удобнее производить через графический интерфейс для настройки маршрутизаторов Mikrotik – WinBox.

Необходимо задать, что авторизация будет проходить через протокол RADIUS (рисунок 30).

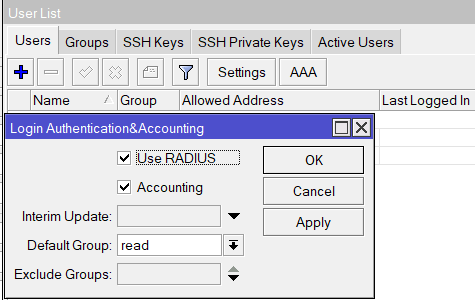


Рисунок 30 – Настройка авторизации по протоколу RADIUS

После этого выполнить настройки пересылки запросов на сервер доступа. Для этого в меню настроек RADIUS-сервера требуется задать настройки, как представлено на рисунке 31.

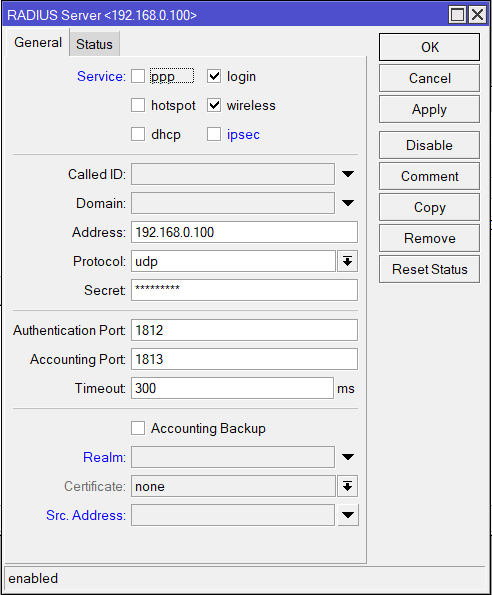


Рисунок 31 – Настройка параметров RADIUS-сервера для точки доступа

На этом настройка Mikrotik закончена. Попробуем подключиться к устройству по учетной записи, созданной на контроллере домена Active Directory, через ssh-клиент «Putty» (рисунок 32).

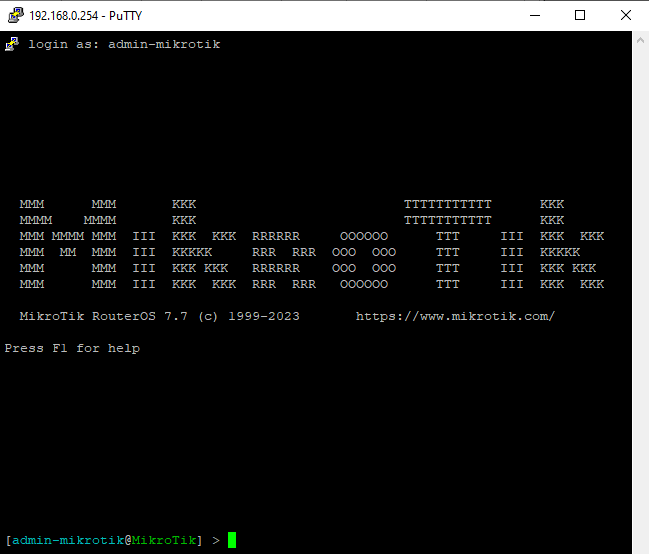


Рисунок 32 – Успешная авторизация на устройстве

Подключение по доменной учетной записи прошло успешно. Убиться в подключении через протокол аутентификации RADIUS возможно проверив список пользователей в графическом интерфейсе (рисунок 33).

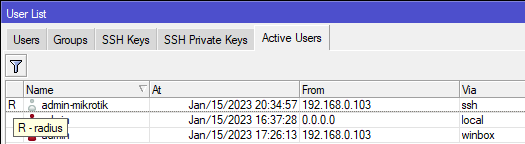


Рисунок 33 – Успешное подключение в графическом интерфейсе

Так как для подключения к домену через беспроводную сеть требуется наличие подключения перед аутентификацией, то необходимо выполнить такие настройки, выбрав в параметрах безопасности подключения пункт «Подключаться автоматически, если сеть в радиусе действия» (рисунок 34).

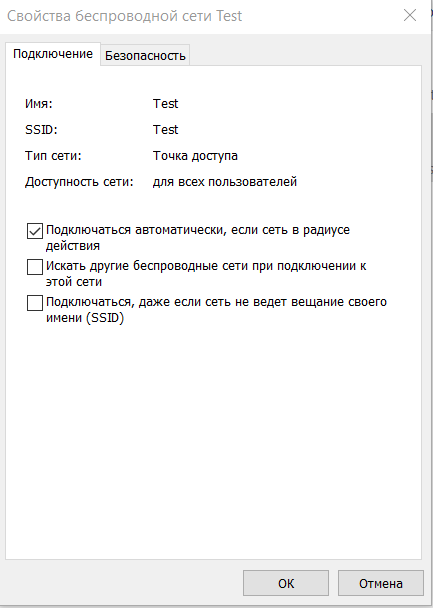


Рисунок 34 – Настройка автоматического подключения к точке доступа

Далее необходимо создать профиль подключения к домену через кнопку «Идентификация…», которая представлена ранее на рисунке 21, так как через беспроводную сеть возникают многие программные сложности с установкой и настройкой доменного профиля на устройстве. Далее необходимо выбрать пункт «Моя организация использует сеть с доменами», в следующем окне указать имя пользователя в домене, его пароль и сам домен, к которому требуется подключиться. Далее следует указать имя компьютера в домене и начать процесс подключения ноутбука к домену, через беспроводную сеть.

В следующем меню требуется ввести параметры подключения к домену ещё раз (рисунок 35) и далее выбрать требуемый уровень полномочий, соответствующий полномочиям на контроллере домена Active Directory. В случае несоответствия аутентификация будет отклонена сервером. После выполненных действий следует перезагрузить устройство.

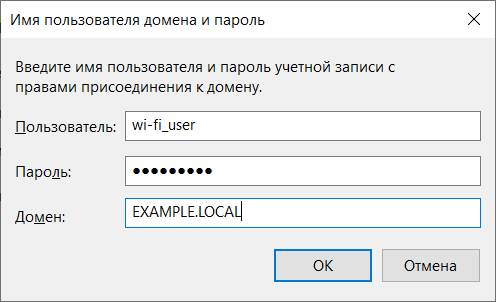


Рисунок 35 – Ввод учетных данных для подключения к домену

После перезагрузки устройство будет использовать доменную сеть организации, это можно проверить, перейдя в список подключенных компьютеров в меню «Active Directory – пользователи и компьютеры» и выбрать в домене «example.com» директорию «Computers» (рисунок 36).

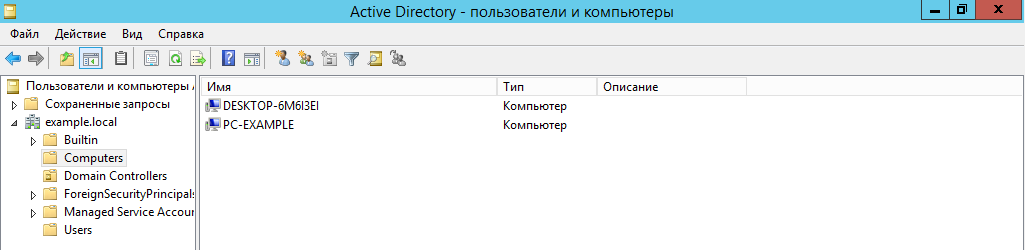


Рисунок 36 – Проверка наличия беспроводного устройства в домене

# **Оценка достижений цели**

Выполненные настройки позволяют централизованно управлять аутентификацией, разрешениями на подключение и вести сбор и учёт использования сетевых ресурсов на персональных компьютерах, подключенных по проводному соединению, на сетевом оборудовании, такому как маршрутизатор, коммутатор или точка доступа, а также на беспроводных устройствах, поддерживающих доменную аутентификацию.

# **Экономическое обоснование**

С целью повышения безопасности передачи данных по беспроводным каналам связи была реализована система централизованной аутентификации в домене Active Directory. Для подсчёта экономических показателей разработанной системы был составлен план-график разработки и внедрения системы, определены затраты на её разработку и внедрение, включая затраты на оплату труда, материалы, затраты на использование машинного времени, общехозяйственные затраты.

# **Спецификация проекта**

Спецификация проекта входит в состав проектной документации и является конструкторским документом, который включает информацию о материалах, изделиях и оборудовании. Эта информация необходима для определения общей потребности комплектации материальными ресурсами объекта строительства. Спецификация предназначена для:

— определения полного перечня требуемых материалов, изделий, оборудования с их подробным описанием;

— подсчета количества материальных ресурсов.

На основе данных единой ведомости можно определить потребность в материалах, рассчитать стоимость и грамотно составить график их приобретения для обеспечения непрерывности процессов разработки системы.

Спецификация разработанной системы оценки защищённости беспроводных устройств представлена в таблице 2.

Таблица 2 — Спецификация системы

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Материалы | Единица измерения | Требуемое количество | Цена за единицу руб. | Сумма, руб. |
| Ноутбук HUAWEI BOHK-WAX9X | шт. | 1 | 51 999 | 51 999 |
| Ноутбук HIPER TeachBook HLP-04R/i5 | шт. | 1 | 55 463 | 55 463 |
| Маршрутизатор Mikrotik RB951Ui-2HnD | Шт | 1 | 11 700 | 11 700 |
| Итого |  | | | 119 162 |

# **План-график проектирования и разработки системы**

Выбор комплекса работ по разработке проекта производится в соответствии со стандартом «ГОСТ Р ИСО/МЭК 12207-99 Информационная технология. Процессы жизненного цикла программных средств», устанавливающим стадии разработки программных продуктов, приведен в таблице 3.

Таблица 3 — Комплекс работ по разработке системы анализа радиоэфира

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Содержание работ | Исполнители | Длитель-ность в календар-ных днях | | Загрузка | | |
| в днях | в % | |
| 1 Разработка технического задания | | | | | | |
| 1.1 Исследование и обоснование разработки | | | | | | |
| 1.1.1 Постановка задачи | Руководитель | 3 | | 3 | 100 | |
| Программист | 3 | 100 | |
| 1.1.2 Сбор исходных данных | Руководитель | 5 | | 2 | 40 | |
| Программист | 5 | 100 | |
| 1.2 Поиск аналогов и прототипов | | | | | | |
| 1.2.1 Анализ существующих методов | Руководитель | 8 | | 8 | 100 | |
| Программист | 8 | 100 | |
| Продолжение таблицы 3 | | | | | | |
| 1.2.2 Обоснование необходимости разработки и внедрения | Руководитель | 4 | | 4 | 100 | |
| Программист | 0 | 0 | |
| 1.3 Анализ требований | | | | | | |
| 1.3.1 Определение и анализ требований к разрабатываемой системе | Руководитель | | 5 | 2 | | 50 |
| Программист | | 5 | | 100 |
| 1.3.2 Определение структуры входных и выходных данных | Руководитель | | 5 | 2 | | 40 |
| Программист | | 5 | | 100 |
| 1.3.3 Согласование и утверждение технического задания | Руководитель | | 3 | 3 | | 100 |
| Программист | | 3 | | 100 |
| Итого по этапу 1 | Руководитель | | 33 | 24 | | 73 |
| Программист | | 29 | | 88 |
| 2 Проектирование | | | | | | |
| 2.1 Проектирование архитектуры системы | Руководитель | | 18 | 14 | | 78 |
| Программист | | 4 | | 22 |
| 2.2 Выбор аппаратных средств цифровой радиосвязи | Руководитель | | 12 | 7 | | 58 |
| Программист | | 12 | | 100 |
| 2.3 Сборка макета системы на основе аппаратных модулей для тестирования и отладки | Руководитель | | 12 | 2 | | 17 |
| Программист | | 12 | | 100 |
| Итого по этапу 2 | Руководитель | | 42 | 23 | | 55 |
| Программист | | 28 | | 67 |
| 3 Разработка и тестирование модулей системы | | | | | | |
| 3.1 Разработка программных модулей системы | Руководитель | | 20 | 10 | | 50 |
| Программист | | 20 | | 100 |
| 3.2 Тестирование программной части | Руководитель | | 7 | 0 | | 0 |
| Программист | | 7 | | 100 |
| 3.3 Сборка и испытание системы | Руководитель | | 12 | 4 | | 30 |
| Программист | | 12 | | 100 |
| 3.4 Анализ результатов экспериментов, формулирование выводов | Руководитель | | 7 | 3 | | 36 |
| Программист | | 7 | | 100 |
| Итого по этапу 3 | Руководитель | | 46 | 17 | | 37 |
| Программист | | 46 | | 100 |

Окончание таблицы 3

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 4 Оформление рабочей документации | | | | |
| 4.1 Проведение расчетов показателей безопасности жизнедеятельности | Руководитель | 3 | 0 | 0 |
| Программист | 3 | 100 |
| 4.2 Проведение экономических расчетов | Руководитель | 7 | 0 | 0 |
| Программист | 7 | 100 |
| 4.3 Оформление пояснительной записки | Руководитель | 31 | 0 | 0 |
| Программист | 31 | 100 |
| Итого по 4 этапу | Руководитель | 41 | 0 | 0 |
| Программист | 41 | 100 |
| Итого по проекту | Руководитель | 162 | 64 | 40 |
| Программист | 148 | 90 |

На основании вышеописанных таблиц был составлен план-график (таблица 4) по проектированию и реализации корпоративной беспроводной информационно-телекоммуникационной сети с доменной аутентификацией, показывающий последовательность и взаимосвязь выполнения комплекса работ.

Таблица 4 — Календарный график выполнения работ

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Содержание работ | Исполнители | Длитель-ность в днях | График работ | |
| начало 1 сентября | окончание 31 января |
| Постановка задачи | Руководитель | 3 | 1 авг | 3 авг |
| Программист | 3 | 1 авг | 3 авг |
| Сбор исходных данных | Руководитель | 2 | 4 авг | 5 авг |
| Программист | 5 | 4 авг | 8 авг |
| Анализ существующих методов | Руководитель | 8 | 9 авг | 15 авг |
| Программист | 8 | 9 авг | 15 авг |
| Обоснование необходимости разработки и внедрения | Руководитель | 4 | 16 авг | 19 авг |
| Программист | 0 | 16 авг | 16 авг |
| Определение и анализ требований к системе | Руководитель | 2 | 20 авг | 21 авг |
| Программист | 5 | 20 авг | 24 авг |
| Определение структуры входных и выходных данных | Руководитель | 2 | 24 авг | 26 авг |
| Программист | 5 | 24 авг | 29 авг |

Окончание таблицы 4

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Согласование и утверждение технического задания | Руководитель | 3 | 30 авг | 1 сен |
| Программист | 3 | 30 авг | 1 сен |
| Проектирование архитектуры системы | Руководитель | 14 | 2 сен | 15 сен |
| Программист | 4 | 16 сен | 19 сен |
| Выбор аппаратных средств цифровой радиосвязи | Руководитель | 7 | 20 сен | 26 сен |
| Программист | 12 | 20 сен | 1 окт |
| Сборка макета системы на основе аппаратных модулей для тестирования и отладки | Руководитель | 2 | 2 окт | 3 окт |
| Программист | 12 | 2 окт | 13 окт |
| Разработка программных модулей системы | Руководитель | 10 | 14 окт | 23 окт |
| Программист | 20 | 14 окт | 2 ноя |
| Тестирование программной части | Руководитель | 0 | 3 ноя | 3 ноя |
| Программист | 7 | 3 ноя | 9 ноя |
| Сборка и испытание системы | Руководитель | 4 | 10 ноя | 13 ноя |
| Программист | 12 | 10 ноя | 21 ноя |
| Анализ результатов экспериментов, формулирование выводов | Руководитель | 3 | 22 ноя | 24 ноя |
| Программист | 7 | 22 ноя | 28 ноя |
| Проведение расчетов показателей безопасности жизнедеятельности | Руководитель | 0 | 29 ноя | 29 ноя |
| Программист | 3 | 29 ноя | 1 дек |
| Проведение экономических расчетов | Руководитель | 0 | 2 дек | 2 дек |
| Программист | 7 | 2 ноя | 8 дек |
| Оформление пояснительной записки | Руководитель | 0 | 9 дек | 9 дек |
| Программист | 31 | 9 дек | 10 янв |

На основе данных, приведённых в таблице 4 сформирован график этапов работ, представленный на рисунке 37.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **янв** | **10** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **декабрь** | **31** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **20** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **10** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **ноябрь** | **31** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | Рисунок 37 — План-график разработки проекта |
| **20** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **10** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **октябрь** | **30** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **20** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **10** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **сентябрь** | **31** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **20** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **10** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **август** | **30** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **20** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **10** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **Содержание работы** | | Постановка задачи | Сбор исходных данных | Анализ существующих методов | Обоснование необходимости разработки и внедрения | Определение и анализ требований к разрабатываемой системе | Определение структуры входных и выходных данных | Согласование и утверждение технического задания | Проектирование архитектуры системы | Выбор аппаратных средств цифровой радиосвязи | Сборка макета системы на основе аппаратных модулей для тестирования и отладки | Разработка программных модулей системы | Тестирование программной части | Сборка и испытание системы | Анализ результатов экспериментов, формулирование выводов | Проведение расчетов показателей безопасности жизнедеятельности | Проведение экономических расчетов | Оформление пояснительной записки |

* 1. **Расчет затрат на разработку проекта**

Предпроизводственные затраты представляют собой единовременные расходы на разработку обеспечивающих или функциональных систем и элементов на всех этапах проектирования, а также затраты на обработку материалов исследования, разработку технического задания, проверки. Сюда включаются затраты на разработку алгоритмов и программ, разработку технического и рабочего проекта системы и её опытной проверки.

Основная заработная плата разработчиков определяется по формуле:

,

где *O* — должностной оклад, руб;

— число рабочих дней в году;

— затраты времени на разработку, рабочие дни.

Число рабочих дней на разработку определяется по формуле:

,

где — календарные дни;

— коэффициент перевода календарных дней в рабочие;

Данный коэффициент равен отношению рабочих дней в году к общему числу календарных дней.

Согласно данным из таблицы 3, рассчитаем трудозатраты руководителя:

Рассчитаем трудозатраты программиста:

.

В компании оклад руководителя равен 120 000 руб., а оклад программиста 75 000 руб.

Рассчитаем заработную плату программиста и руководителя по формуле:

Отсюда следует, что основная заработная плата на разработку:

Рассчитаем дополнительную зарплату:

где — коэффициент начисления на дополнительную зарплату.

Премия рассчитывается согласно следующей формуле:

где — коэффициент начисления на премию.

Рассчитаем начисления на единый страховой сбор:

Ввиду того, что проектируемая система должна быть разработана и отлажена с помощью компьютеров, к суммарным затратам на разработку добавляются затраты на их использование.

Доля амортизационных отчислений на компьютерное оборудование, приходящаяся на разработку проекта, определяется по формуле:

где — балансовая стоимость компьютерного оборудования;

— продолжительность использования компьютера программистом, час;

— срок службы компьютерного оборудования. = 6 лет;

число одновременно выполняемых проектов (*z* = 1…3).

 — действительный годовой фонд времени компьютерного оборудования;

Действительный годовой фонд компьютерного оборудования рассчитывается по формуле:

где — номинальный фонд времени работы компьютерного оборудования;

— коэффициент потерь времени; *y* = 3 – 5 %.

Рассчитаем амортизационные отчисления для компьютерного оборудования:

Используемое при конструкторской подготовке системы анализа радиоэфира относится к нематериальным активам предприятия. Амортизационные отчисления на программное обеспечение, приходящиеся на конструкторскую подготовку производства, определяются по формуле:

Где — балансовая стоимость программного обеспечения, руб.;

— срок службы программного обеспечения (при отсутствии фактических данных применяется равным 10 годам).

Рассчитаем затраты электроэнергии, необходимые на проектирование и разработку системы.

где — установленная мощность компьютера, кВт;

— коэффициент загрузки установленной мощности.

— цена электроэнергии, руб/кВт.

Итого затраты на энергию будут следующими:

руб.

Итого затраты на машинное время:

Общехозяйственные расходы:

В таблице 5 представлены затраты на разработку и материалы в соответствии со спецификацией, приведённой в п. 5.1.

Таблица 5 — Затраты на разработку

|  |  |
| --- | --- |
| Статьи затрат | Затраты |
| Основная заработная плата | 737 489,88 |
| Дополнительная зарплата | 110 623,48 |
| Премия | 294 995,95 |
| Отчисления на социальные нужды | 342 932,79 |
| Затраты на материалы | 119 162,00 |
| Затраты на машинное время | 24 224,48 |
| Общехозяйственные расходы | 147 497,98 |
| ИТОГО | 1 776 926,56 |

В результате проведенных расчетов определено, что себестоимость разработки составляет 1 776 926,56 руб. С учетом нормативной рентабельности *R* = 15% планируемая прибыль *П* составит:

*П* = *С* · *R* = 1 776 926,56 · 15% = 266 538,98 руб.

A цена продукта составит:

*Ц* = *С* + *П* = 1 776 926,56 + 266 538,98 = 2 043 465,54 руб.

Цена продукта с учётом НДС составит:

*ЦНДС* = 1,2·*Ц* = 1,2 · 2 043 465,54 = 2 452 158,65 руб.

Потенциальными покупателями разработанной системы являются компании, занимающиеся внедрением и поддержкой систем безопасности, государственные органы и отделы информационной безопасности организаций, в которых требуется повышенный уровень безопасности.

# **Безопасность и экологичность работы**

Наука, изучающая опасности, способы защиты от опасностей и ликвидации последствий их воздействия, называется безопасность жизнедеятельности (далее БЖД). Опасностями называются явления, процессы, предметы способные угрожать жизни и здоровью человека, реализующиеся в виде потоков, вещества, энергии и информации. БЖД изучает действующие в техносфере естественные, техногенные и антропогенные опасности, чтобы выработать наиболее эффективные средства и способы защиты от их воздействия. Обеспечению безопасности труда человека и его трудовой деятельности в целом уделяется особо внимание. Основной целью БЖД является разработка способов защиты здоровья и жизни человека и его имущества в техносфере, защита его от воздействия опасностей техногенного, естественного и антропогенного (искусственного) происхождения и создание комфортных условий жизнедеятельности.

Охрана труда – это деятельность, направленная на принятие комплекса мер по сохранению жизни и здоровья человека в процессе его трудовой деятельности, включающая в себя правовые следующие мероприятия:

* Правовые – создание организационно-правовых норм безопасности и охраны труда, формирование законодательных и нормативно-правовых актов по обеспечению их соблюдения, составление правил эксплуатации производственного оборудования;
* Санитарно-гигиенические и лечебно-профилактические – направленны на обеспечение благоприятных условий труда и предотвращение профессиональных заболеваний путем обеспечения чистоты и порядка на рабочих местах, снижением уровня воздействия вредных и опасных производственных факторов, а также проведением регулярных и внеочередных медицинских осмотров персонала;

Организационно-технические – заключаются в использовании оборудования, соответствующего установленным стандартам, обеспечение работников актуальными инструкциями по технике безопасности, обеспечение достаточной освещенности, вентиляции и оптимального температурного режима на рабочих местах, а также соблюдение работниками техники безопасности труда и правил эксплуатации оборудования для снижения риска получения травм на рабочем месте.

# **Влияние шума на организм человека**

Неблагоприятным фактором производственной среды является высокий уровень производственного шума, создаваемый различным офисным оборудованием, таким как принтер или сканер, оборудованием для кондиционирования воздуха в помещении, кулерами персональных компьютеров.

Производственный шум снижает работоспособность, производительность труда, увеличивает вероятность неврозов и нервных заболеваний, вызывает мигрень, сильнее истощает организм человека и заметно снижает внимание и сосредоточенность на работе и т.д. Подобные нарушения в работе организма человека могут стать причиной негативных изменений в эмоциональном состоянии человека, вызывая стресс и депрессию. Фактором, вызывающим ошибки и затрудняющим работу, является шум с частотой более 500 Гц. Громкий шум снижает способность человека правильно оценивать расстояние и время, распознавать цвета, нарушает восприятие зрительной информации. Также уменьшается производительность труда на 5-12%. Согласно ГОСТ 12.1.003-2014 МЕЖГОСУДАРСТВЕННЫЙ СТАНДАРТ. Система стандартов безопасности труда. ШУМ. Общие требования безопасности длительное воздействие интенсивного шума (80-90 дБ) на слух человека снижают производительность труда на 30-60% и может приводить к частичной или полной потере слуха.

В таблице 6 указаны предельные уровни звука в зависимости от напряженности труда и категории его тяжести, которые по стандартам допустимы и безопасны в отношении сохранения здоровья на рабочих местах.

Уровень шума у разработчиков новых программ не должен превышать 40 дБ, а в помещениях, в которых операторы обрабатывают данные на персональных компьютерах, не более 65 дБ.

Таблица 6 – Предельные уровни звука на рабочих местах

В децибелах

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Категория  напряженности труда | Категория тяжести труда | | | |
| Легкая | Средняя | Тяжелая | Очень тяжелая |
| Мало напряженный | 80 | 80 | 75 | 75 |
| Умеренно напряженный | 70 | 70 | 65 | 65 |
| Напряженный | 60 | 60 | - | - |
| Очень напряженный | 40 | 40 | - | - |

Заключение о необходимость снижения уровня шума принимается на основе показателей, полученных при замере на рабочих местах операторов.

При нескольких одновременно работающих некогерентных источников уровень шума возможно вычислить на основании принципа энергетического суммирования излучений отдельных источников:



где *L*i — уровень звукового давления *i*-го источника шума;

*n* — количество источников шума.

Полученные в результате расчёта данные сравниваются с допустимым значением уровня шума для данного рабочего места. Если данные превышают допустимое значение уровня шума, то необходимо предпринять специальные меры по снижению шума. К таким мерам можно отнести: применение звукопоглощающих конструкций (звукопоглощающие облицовки, кулисы, штучные поглотители), использование акустических экранов (отгородок), рациональная организация рабочего места оператора.

Уровни звукового давления источников шума, действующих на оператора на его рабочем месте представлены в таблице 7.

Таблица 7 — Уровни звукового давления различных источников

|  |  |
| --- | --- |
| Источник шума | Уровень шума, дБ |
| Жесткий диск | 42 |
| Кулер | 43 |
| Монитор | 15 |
| Клавиатура | 13 |
| Принтер | 41 |
| Сканер | 44 |

Обычно рабочее место оператора оснащено следующим оборудованием: жесткий диск в системном блоке, кулеры систем охлаждения ПК, монитор, клавиатура, принтер и сканер.

Подставив значения уровня звукового давления для каждого вида оборудования в формулу, получим:

дБ.

Значение, полученное в результате вычислений, не превышает допустимый уровень шума для рабочего места оператора, который установлен в размере 65дБ. При учёте малой вероятности одновременного использования такого офисного оборудования как принтер и сканер, полученное значение будет еще меньше.

# **Экологичность работы**

Предельно допустимые уровни воздействия на человека электромагнитных излучений устанавливаются санитарными правилами и нормами СанПиН 1.2.3685-21 «Гигиенические нормативы и требования к обеспечению безопасности и (или) безвредности для человека факторов среды обитания» в диапазоне частот 30 кГц – 300 ГГЦ (таблица 8).

Магнитная составляющая по своей величине не имеет существенного значения при работе теле, радио и иных передающих станций, в следствии чего интенсивность электромагнитного излучения оценивается исключительно по величине напряженности электрического поля (Е, в/м).

Таблица 8 – Предельно допустимые уровни электромагнитного излучения

|  |  |
| --- | --- |
| Частота, МГц | Предельно допустимый уровень, в/м |
| 30-60 | 5 |
| 60-120 | 4 |
| 120-240 | 3 |
| 240-300 | 2,5 |

При одновременном облучении от нескольких источников, для которых установлены разные ПДУ, должно соблюдаться следующее условие:

где *Еi* — напряженность электрического поля, создаваемого *i*-источником,

ПДУ*i* — предельно-допустимый уровень для *i*-источника, в/м.

Для защиты населения от электромагнитных излучений мощных передающих станций (свыше 100 кВт) КВ диапазона, они должны размещаться за пределами населенных мест, вдали от жилой застройки.

Вокруг передающих станций создают санитарно-защитные зоны, размеры которых должны обеспечивать предельно-допустимый уровень электромагнитных излучений в населенных местах (таблица 9).

Таблица 9 — Размеры санитарных зон

|  |  |
| --- | --- |
| Суммарная мощность передатчика,  кВт | Размеры санитарной зоны, м |
| до 10 | в пределах технической территории |
| 10-75 | 200-300 |
| 75-160 | 400-500 |
| более 160 | 500-1000 |

Санитарная зона разделяется на зону строгого режима (50-100 м) и зону ограниченного пользования в зависимости от мощности передатчика. В зоне строгого режима допускается пребывание только работников передающей станции, и ограниченное время. В зоне ограниченного пользования можно располагать объекты, в которых граждане могли бы находиться менее 8 час (гаражи, хозяйственно-бытовые помещения и др.)

Определим напряженности электрического поля на разном расстоянии от передающей антенны (рисунок 38).

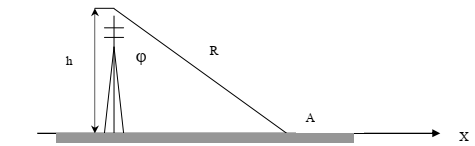


Рисунок 38 — Напряжённость электрического поля на расстоянии от антенны

Электрическая напряженность электромагнитного излучения в расчетной точке А определяется по формуле:

где *Р* — мощность источника, Вт,

φ — коэффициент направленности антенны, рад.

где *R* — расстояние от антенны до расчетной точки, м,

*h* — высота антенны, м,

*x* — расстояние от основания антенны до расчетной точки, м.

Электрическая напряженность электромагнитного излучения в жилом помещении определяется по формуле:

*Еж* = *k* · *Е*

где *k* — ослабление электромагнитного излучения стенами здания.

*k* = 1 — для кирпичных стен;

*k* = 0,2 — для панельных стен.

Исходные данные для расчётов приведены в таблице 10.

Таблица 10 — Исходные данные для расчётов

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| *h*, м | 1 канал | | 2 канал | | 3 канал | |
| *f*1 | *P*1 | *f*2 | *P*2 | *f*3 | *P*3 |
| 280 | 33 | 1300 | 63 | 3300 | 123 | 6300 |

Где *h* — высота антенны;

*fi* — частота, МГц;

*рi* — мощность передатчика, Вт.

Определим ПДУ для каждого канала по таблице 8 и занесем в таблицу 11.

Определим электрическую напряженность в расчетных точках и результаты расчета сведем в таблицу 11 и рисунок 39.

Для *x* = 50 м:

Таблица 11 — Мощности электромагнитного излучения на разном расстоянии от передающей станции

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| *x* | arctg(*x*/*h*) | *E*1 | *E*2 | *E*3 | *α* |
| 0 | 0 | 0 | 0 | 0 | 0 |
| 50 | 0,18 | 0,29 | 0,47 | 0,64 | 0,06 |
| 100 | 0,34 | 0,39 | 0,62 | 0,86 | 0,11 |
| 150 | 0,49 | 0,44 | 0,69 | 0,96 | 0,14 |
| 200 | 0,62 | 0,45 | 0,72 | 1,00 | 0,15 |
| 250 | 0,73 | 0,45 | 0,72 | 0,99 | 0,15 |
| 300 | 0,82 | 0,44 | 0,69 | 0,96 | 0,14 |
| ПДУ | – | 5 | 4 | 3 | 1 |

Суммарная мощность передатчиков: 1300 + 3300 + 6300 = 10900 Вт = 12 кВт. Отсюда по таблице 9 определяем размер санитарной зоны — 200 м.

Рисунок 39 – Мощность электромагнитного излучения на разном расстоянии от передающей станции

Находим по таблице 11 величину *Е* для *x* = 200 м и рассчитываем напряженность электрического поля в кирпичном и панельном домах.

Таблица 12 — Напряженность электрического поля в кирпичном и панельном зданиях

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | *E*1 | *E*2 | *E*3 | *α* |
| *x* = 200 | 0,45 | 0,72 | 1,00 | 0,15 |
| Кирпичный  дом | 0,45 | 0,72 | 1,00 | 0,15 |
| Панельный  дом | 0,09 | 0,144 | 0,2 | 0,006 |
| ПДУ | 5 | 4 | 3 | 1 |

На границе санитарной зоны ЭМИ в кирпичных и панельных зданиях не превышает допустимые значения.

# **Организация и обеспечение пожарной безопасности на предприятии**

Системы пожарной защиты и предотвращения пожара обеспечивают пожарную безопасность в соответствии с техническим регламентом о требованиях пожарной безопасности: федер. закон: [принят Гос. Думой Федер. собрания РФ 22 июля 2008 г. №123-ФЗ] и о противопожарном режиме [утв. и введен в действие постановления Правительства Российской Федерации от 25.04.2012 г. №390 с изм. на 30.12.2017 г.] – Введ. 2012–05–02; НПБ 105–03. Определение категорий помещений, зданий и наружных установок по взрывопожарной и пожарной опасности. Введ. 2003-08-01. Во всех рабочих помещениях обязательно наличие плана эвакуации людей при пожаре, который регламентирует действия работников в случае возникновения очага возгорания и указывающий места расположения пожарной техники.

Пожар в служебном помещении представляет особую опасность для здоровья и жизни работников, а также сопряжен с большими материальными потерями. Возникновению пожара способствует взаимодействие горючих веществ, окисления и источников зажигания. В рассматриваемом служебном помещении присутствуют все три основные фактора, в результате взаимодействия которых может начаться пожар.

Анализ показал, что горючими компонентами в рабочем помещении являются строительные материалы, предназначенные для эстетической и акустической отделки помещения, а также деревянные полы, двери, перегородки, изоляция кабелей и др.

Противопожарная защита – это комплекс организационно-технических мероприятий, различных планировочных решений и технических средств, направленных на обеспечение безопасности здоровья и жизни человека и предотвращение пожара, ограничение его распространения, а также способствующих для успешного тушения пожара.

Возгорание горючих материалов могут вызвать следующие источники: электронных схемы, устройства электропитания, кондиционирования воздуха, приборы, использующиеся во время технического обслуживания и другие устройства, в которых в результате нарушения функционирования могут образоваться перегретые элементы, электрические искры и дуги, вызывающие возгорание горючих материалов.

В современном электронном оборудовании высокая плотность размещения элементов электронных схем, таких как соединительные провода и кабели. Прохождение электрического тока через них неизбежно сопровождается выделением значительного количества теплоты, при длительном и чрезмерном воздействии которого возможно оплавление изоляции. Чтобы отвести избыточную теплоту применяют системы охлаждения и вентиляции воздуха, которые в свою очередь, при постоянной работе, представляют дополнительную пожарную опасность.

На начальных стадиях возгорания для тушения применяют огнетушители, при оперативном использовании которых можно избежать распространения огня. В настоящее время распространены углекислотные огнетушители, положительной чертой которых является эффективность в тушении пожара, минимальный ущерб для электронного оборудования, особые диэлектрические свойства углекислого газа, что дает возможность использовать такой тип огнетушителей даже при условии невозможности отключения электроустановки.

Рассмотрим аналитический прогноз горения зданий.

Расчет протяженности зон теплового воздействия *R*, м, при горении зданий и промышленных объектов производится по формуле:

где *q*соб –– плотность потока собственного излучения пламени пожара, кВт/м2, (таблица 13);

*q*кр –– критическая плотность потока излучения пламени пожара, падающего на облучаемую поверхность и приводящую к тем или иным последствиям, кВт/м2 (таблица 14);

*R*\* –– приведенный размер очага горения, м, равный:

–– для горящих зданий,

(1,75…2,0)·––для штабеля пиленого леса,

0,8·*D*рез –– для горения нефтепродуктов в резервуаре;

*l*, *h* –– длина и высота объекта горения, м;

*D*рез –– диаметр резервуара, м.

Таблица 13 — Теплотехнические характеристики материалов и веществ

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Плотность потока пламени пожара, *qсоб*, кВт/м2 | | | | | | |
| Ацетон | Бензол | Бензин | Керосин | Мазут | Нефть | Древесина |
| 1200 | 2500 | 1780 —1220 | 1520 | 1300 | 874 | 260 |

Задавая ту или иную степень поражения человека, сооружения и т.п., по формуле определяют искомое расстояние от очага пожара. Определим расстояние от очага пожара, возникшего в здании цеха до границы зоны появления ожогов II степени и возгорания горючих материалов.

Таблица 14 — Критические значения плотностей потока, падающего излучения

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Критические значения плотностей потока, *q*кр, кВт/м2 | | | | |
| Безопасное нахождение человека | возгорание древесины через 10 минут | возгорание древесины через 5 минут | возгорание ЛВЖ через 3 минуты | возгорание ГЖ через 3 минуты |
| 1,5 | 14,0 | 17,5 | 35,0 | 41,0 |

Рассчитаем протяженность зоны теплового воздействия *R*, м безопасного нахождения людей при горении деревянного здания и резервуара с керосином.

В случае возгорания в деревянном здании высотой 12 м и длиной 60 м, граница зоны возгорания древесины через 3 минут будет равняться:

м.

Определим расстояние от очага пожара, возникшего в резервуаре с нефтью диаметром 20 м до границы зоны возгорания горючей жидкости через 3 минуты:

м.

Рекомендовано установить в анализируемое помещение оборудование для стационарного автоматического пожаротушения. Целесообразно использование оборудования, основной принцип действия которого основан на быстром заполнении помещения газовым веществом, способствующим тушению пожара, путем сжижения содержащегося в воздухе кислорода.

Пожарная безопасность обеспечивается системой предотвращения пожара и системой пожарной защиты. В рабочих помещения размещены «Планы эвакуации людей при пожаре», регламентирующие действия работников при возникновении очага возгорания и указывающие места расположения пожарной техники.

В местах, соответствующих стандартам, размещены ручные огнетушители (углекислотные ОУ-8 в количестве четырех штук).

Средствами обнаружения и оповещения о пожаре являются автоматические датчики-сигнализаторы о пожаре типа ДТП, реагирующие на повышение температуры. В качестве средства оповещения сотрудников о пожаре выступает речевой оповещатель на основе громкоговорителей, подключенных к усилителям низкой частоты, которые соединены с цифровым запоминающим устройством.

# **Вывод**

В отделе информационных технологий обеспечивается и соблюдается необходимый микроклимат, допустимый уровень шума, рабочие места приведены к удобному и правильному с точки зрения эргономики виду в соответствии с принятыми нормами.

Для работников отдела, во время выполнения их должностных обязанностей, важнейшим фактором, который влияет на их работоспособность, является достаточное освещение рабочего места. Достаточный уровень освещения достигается за счёт грамотного выбора и расположения осветительных приборов.

В итоге условия труда сотрудников отдела информационных технологий соответствуют установленным нормам, работники обеспечены комфортом и благоприятными условиями труда.

**Заключение**

В результате выполнения выпускной квалификационной работы проведён сравнительный анализ существующих стандартов беспроводной связи, а также методов шифрования, протоколов аутентификации и авторизации. На основе полученных данных был предложен проект беспроводной сети с доменной аутентификацией, имеющий высокий уровень информационной безопасности, благодаря использованию современных протоколов аутентификации, авторизации и учета событий. Использование рассмотренных средств предоставляет широкие возможности по управлению сетевым доступом, для различных потребностей организаций.

Разработанная сеть может представлять интерес для специалистов в области сетевой безопасности и системных администраторов, работающих в организация по установке, настройке и сопровождению систем информационной безопасности. Представленные методы аутентификации и авторизации, а также способы настройки windows serves, в частности настройки сервера сетевых политик, могут применяться на серверах различного назначения.

**Перечень использованных информационных ресурсов**

1. Олифер В., Олифер Н. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов/ В. Олифер, Н. Олифер. - СПб.: Питер, 2020. - 1008 c.
2. Пятибратов А.П. Вычислительные системы, сети и телекоммуникации / А.П. Пятибратов, Л.П. Гудыно, А.А. Кириченко. — М.: КНОРУС, 2013. — 284 с.
3. Холмогоров В. Компьютерная сеть своими руками. Самоучитель / В. Холмогоров. — СПб.: Питер, 2004. — 171 с.
4. IEEE 802.11. Р.А. Бельфер [Электронный ресурс] // Национальная библиотека им. Н.Э. Баумана – URL: https://ru.bmstu.wiki/IEEE\_802.11 (дата обращения 07.10.2022).
5. Беспроводные сети: классификация, организация, принцип работы [Электронный ресурс] // Проект Posetke. – URL: https://posetke.ru/wifi/besprovodnie-seti-klassifikaciya-princip-raboti.html (дата обращения 09.10.2022).
6. Особенности защиты беспроводных и проводных сетей / Хабр – Habr [Электронный ресурс] // Проект Habr – URL: https://habr.com/ru/company/zyxel/blog/516508/ (дата обращения 13.10. 2022).
7. Протокол контроля доступа TACACS. Финсет К. [Электронный ресурс] // Проект RFC Editor. – URL: https://www.rfc-editor.org/rfc/rfc1492 (дата обращения 01.11.2022).
8. Протокол контроля доступа TACACS+. Грант Л. [Электронный ресурс] // Проект RFC Editor. – URL: https://www.rfc-editor.org/rfc/rfc8907 (дата обращения 03.11.2022).
9. Удаленная аутентификация в службе пользователей с телефонным подключением. Ригни К. [Электронный ресурс] // Проект RFC Editor. – URL: https://www.rfc-editor.org/rfc/rfc2865 (дата обращения 05.11.2022).
10. Базовый протокол DIAMETR. Аррко Дж. [Электронный ресурс] // Проект RFC Editor. – URL: https://www.rfc-editor.org/rfc/rfc6733 (дата обращения 09.11.2022).
11. Документация по сетевому взаимодействию. [Электронный ресурс] // Майкрософт – Microsoft. – URL: https://learn.microsoft.com/ru-ru/windows-server/networking/ (дата обращения 15.11.2022).
12. Руководство пользователя микротик: Беспроводной интерфейс. [Электронный ресурс] // Микротик – Mikrotik. – URL: https://help.mikrotik.com/docs/display/ROS/Wireless+Interface (дата обращения 25.11.2022).
13. Федеральный закон от 22.07.2008 № 123-ФЗ «Технический регламент о требованиях пожарной безопасности».
14. СанПиН 1.2.3685-21 «Гигиенические нормативы и требования к обеспечению безопасности и (или) безвредности для человека факторов среды обитания».
15. ГОСТ 12.1.003-2014 МЕЖГОСУДАРСТВЕННЫЙ СТАНДАРТ.
16. Трудовой кодекс Российской Федерации от 30.12.2001 № 197-ФЗ (ред. от 19.12.2022) [Электронный ресурс]: справочная правовая система КонсультантПлюс. URL: https://www.consultant.ru/document/cons\_doc\_LAW\_346-83/ (дата обращения: 24.12.2022).
17. Налоговый кодекс Российской Федерации (НК РФ) от 31 июля 1998 года № 146-ФЗ [Электронный ресурс]: справочная правовая система КонсультантПлюс. URL: https://www.consultant.ru/document/cons\_doc\_LAW\_196-71/ (дата обращения: 24.12.2022).