

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И ВЫСШЕГО РЕСПУБЛИКИ КАЗАХСТАН

Некоммерческое акционерное общество «Казахский национальный исследовательский  
технический университет имени К. И. Сатпаева»

Институт Автоматики и Информационных технологий

Кафедра Электроника, телекоммуникации и космические технологии

Талгатулы Нурсултан

«Проектирование жилого комплекса Манхэттен с применением технологии IoT»

**ДИПЛОМНАЯ РАБОТА**

По образовательной программе 6В06201 Телекоммуникация

Алматы 2023

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РЕСПУБЛИКИ  
КАЗАХСТАН

Казахский национальный исследовательский технический университет  
имени К.И.Сатпаева

Институт Институт Автоматики и Информационных технологий

Кафедра, Электроника, телекоммуникации и космические технологии

**ДОПУЩЕН К ЗАЩИТЕ**

Заведующий кафедрой  
Электроники,  
телекоммуникации и космических  
технологий к.т.н., асоц. профессор  
Таштай Е.

« 02 » 06 20\_\_ г.



**ДИПЛОМНАЯ РАБОТА**

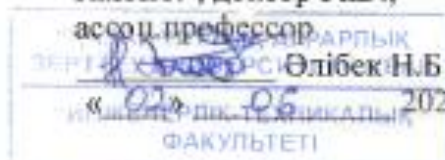
На тему: «Проектирование жилого комплекса Манхэттен с применением технологии IoT»

по специальности 6В06201 Телекоммуникация

Выполнил проект

Талгатулы Н

Рецензент  
КазНИУ, доктор PhD.,  
ассоц. профессор



« 02 » 06 2023 г.

ФАКУЛЬТЕТИ

Научный руководитель  
маг.техн. наук.,  
старший препод,

С. Маркұлы  
« 02 » 06 2023 г.

Алматы 2023

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН

Некоммерческое акционерное общество Казахский национальный исследовательский  
технический университет  
имени К.И.Сатпаева

Институт автоматики и информационных технологий

Кафедра Электроники, телекоммуникации и космические технологии



*Дипломник: Таггатулы Нурсултан*

*Тема: Проектирование жилого комплекса Манхэттен с применением технологии IoT*  
*Утверждена приказом Ректора Университета № 408-П/Ө от «23» ноября 2023 года.*

*Срок сдачи законченной работы «30» апреля 2023 г.*

*Исходные данные к дипломной работе:*

1. Методы построения и параметры функционирования технологии IoT
2. Имитационная модель сети с нормальным распределением узлов и шлюзом в ЖК Манхэттен
3. Модель IoT как системы массового обслуживания
4. Параметры модели трафика IoT образованной 100 узлами, расположенными на плоской поверхности в области, ограниченной квадратом  $200 \times 200$  м. Радиус связи узла  $R = 50$  м.
5. Программно-графическое представление сети

*Перечень вопросов* подлежащих изучить и представить в дипломной работе:

- а) Анализ возможностей построения сетей IoT на основе существующей инфраструктуры сетей мобильной связи
- б) Исследование применения IoT в ЖК Манхэттен
- в) Разработка модели и исследование вероятности связности IoT при неравномерном распределении
- д) Расчёт и моделирование IoT в программной среде OMNET++
- г) Математическая модель совместного обслуживания трафика реального времени и эластичного трафика данных в узле доступа LTE в ЖК Манхэттен

*Перечень графического материала:*

*Рекомендуемая основная литература:*

1. Ефимов М.М., Киричек Р.В.: Интернет вещей: перспективы адаптивных систем // Информационные технологии и телекоммуникации. 2020. Том 8. № 1. С. 55–66.
2. Abdellah, A.R. Machine Learning Algorithm for Delay Prediction in IoT and Tactile Internet. / Abdellah, A.R.; Mahmood, O.A.; Kirichek, R.; Paramonov, A.; Koucheryavy, A. // Future Internet 2021, Vol. 13, Issue. 12, 304, pp. 1-19.
3. 12. Abdellah, A.R. Performance Estimation in V2X Networks Using Deep Learning-Based M-Estimator Loss Functions in the Presence of Outliers. / Alshahrani, A.; Muthanna, A.; Koucheryavy, A // Symmetry 2021, Vol. 13, Issue. 11, pp. 1-18

**ГРАФИК**  
подготовки дипломной работы

Наименование разделов, перечень разрабатываемых вопросов	Сроки представления научному руководителю	Примечание
Анализ возможностей построения сетей IoT на основе существующей инфраструктуры сетей мобильной связи	1.09.2022-31.12.2022	<i>Выполнено</i>
Разработка модели и исследование вероятности связности БСС при неравномерном распределении	1.01.2023-30.01.2023	
Расчёт и моделирование IoT в программной среде OMNET++	1.02.2023-15.02.2023	
Исследование применения IoT в ЖК Манхэттен	1.02.2023-15.03.2023	
4. Написание дипломной работы	15.04.2023-30.04.2023	

**Подпись**

консультантов и нормоконтролера на законченную дипломную работу с указанием относящихся к ним разделов работы

Наименование разделов	Консультанты Ф.И.О. (уч.степень, звание)	Дата подписания	Подпись
Нормоконтролер	Магистр технических наук, ассистент Акылжан П	<i>02.06.2023 г.</i>	<i>А.А.</i>

Научный руководитель

Марксылы С

Задание принял к исполнению обучающийся  
" 22 " .. *октября* .. 2022 г.

Талгатулы Н

## АННОТАЦИЯ

В дипломной работе производится проектирование сети IoT в ЖК Манхэттен и разработка беспроводной сенсорной сети. Сеть был разработан на основе телекоммуникационной технологии “ZigBee”.

В проекте проведен обзор, анализ и классификация систем IoT. Также рассмотрены существующие системы телекоммуникации в ЖК Манхэттен и для внедрения БСС был выбран оборудования. С помощью программы OMNET++ был смоделирован БСС. Для проектирования и моделирования произведен расчет параметров потребляемой мощности, расчет шумов в тракте приема/передачи, дальность действия связи, уровень затухания и отношения сигнал-шум.

## АҢДАТПА

Дипломдық жұмыста ЖК Манхэттенге IoT желісін орналастыру және сымсыз сенсорлық желіні зерттеу жүргізіледі. Желі Zigbee телекоммуникациялық технологиясы негізінде жасалды.

Жұмыста IoT жүйелеріне шолу, талдау және жіктеу жүргізілді. Сондай-ақ, Манхэттен тұрғын үй кешені қолданыстағы телекоммуникация жүйелері қаралды және БСС енгізу үшін жабдықтар таңдалды. OMNET++ бағдарламасының көмегімен BSS модельденді. Жобалау және модельдеу үшін қуат тұтыну параметрлерін есептеу, қабылдау/беру жолындағы шуды есептеу, байланыс әрекетінің қашықтығы, өшу деңгейі және сигнал-шу қатынасы есептелді.

## ANNOTATION

In the thesis, the design of the IOT network in the Manhattan residential complex and the development of a wireless sensor network are carried out. The network was developed on the basis of the ZigBee telecommunication technology.

The project reviewed, analyzed and classified IOT systems. The existing telecommunications systems in the Manhattan residential complex were also considered, and equipment was selected for the implementation of the WSN. With the help of the OMNET++ program, the WSN was modeled. For design and simulation, the parameters of power consumption, the calculation of noise in the receive / transmit path, the communication range, the attenuation level and the signal-to-noise ratio were calculated.

## СОДЕРЖАНИЕ

Введение	7
1 Обзор и анализ технологии IoT	8
1.1 Основные понятия и архитектура Интернет-вещей (IoT)	8
1.2 Средства передачи данных Интернета вещей. Классификация технологий передачи данных в IoT	15
1.3 Технология интернета-вещей Zigbee	17
2 Методы построения и параметры функционирования технологии IoT	27
2.1 Архитектура сетей IoT/M2M	27
2.2 Платформа IMS и ее функциональные элементы	32
2.3 Особенности использования технологии NB-IoT, планы международных организаций по использованию радиочастотного спектра	37
2.4 Проектирование локальные сети Интернета вещей и M2M на базе сетей малого радиуса действия в ЖК Манхэттен	40
2.5 Выбор оборудование для проектирование IoT в ЖК Манхэттен	47
3 Расчёт и моделирование беспроводной сенсорной сети в ЖК Манхэттен	55
3.1 Программно-графическое представление сети	55
3.2 Техническое обеспечение беспроводной сенсорной сети в ЖК Манхэттен	59
3.3 Практическая реализация архитектуры беспроводной сенсорной сети	61
3.4 Расчет потребляемой мощности устройств ZigBee	62
3.5 Расчет шумов в тракте приема/передачи сети ZigBee	63
Заключение	71
Список используемой литературы	72

## ВВЕДЕНИЕ

Концепция «Интернета вещей» — одна из тех новых идей, которые способны не только коренным образом изменить облик телекоммуникационных и информационных систем, но и существенно повлиять на образ жизни людей.

Технологии беспроводного доступа с использованием устройств малого радиуса действия все шире используются в системах автоматизации управления промышленными объектами.

Каждый год количество устройств, подключенных к сети удваивается. Внедрение «Интернета вещей» — это резкое развитие экономики и повышение уровня жизни в стране с инвестиционными акциями. На сегодняшний день технология беспроводных сетей малого радиуса действия (сенсорных сетей) является единственной беспроводной технологией с длительным временем автономной работы, которую можно использовать для решения задач мониторинга и управления промышленными объектами. При организации сети связи на основе технологии ZigBee возможно создание распределенной самоорганизующейся системы сбора, обработки и передачи информации.

Развитие беспроводного стандарта передачи данных ZigBee дало возможность использовать сеть, построенную на данном протоколе беспроводной связи во многих областях автоматизации управления и мониторинга [1].

ЖК «Манхэттен» использует машинные приемники для оперативной организации связи в чрезвычайных ситуациях. При развертывании таких комплексов возможен выход в сеть по спутниковой связи. Такие комплексы имеют возможность организации телефонной связи, выхода в Интернет, организации видеоконференций.

Цель работы: Исследование технологии IoT внедрения её в ЖК Манхэттен в городе Алматы.

Задачи:

- анализ возможностей построения сетей IoT на основе существующей инфраструктуры сетей мобильной связи
- исследование применения IoT в ЖК Манхэттен
- разработка модели и исследование вероятности связности IoT при неравномерном распределении
- расчёт и моделирование IoT в программной среде OMNET++

# 1 Обзор и анализ технологии IoT

## 1.1 Основные понятия и архитектура Интернет-вещей (IoT)

В связи с бурным развитием сетей с коммутацией пакетов и, прежде всего, Интернета, в начале 2000-х мировое телекоммуникационное сообщество сначала разработало, а затем начало реализовывать новую парадигму развития связи - сети поколения NGN. Технологии СПП уже прошли эволюционный путь развития от гибких механизмов до подсистемы обнаружения каналов IMS и беспроводных сетей долгосрочного развития LTE. В то же время всегда есть сети, которые охватывают пользователей СПП, и, следовательно, большое количество абонентов в таких сетях будет ограничено охватом населения планеты Земля.

В связи с бурным развитием сетей с коммутацией пакетов и, прежде всего, Интернета, в начале 2000-х годов мировое телекоммуникационное сообщество сначала разработало, а затем приступило к внедрению новой парадигмы развития коммуникаций - сетей поколения NGN [3].

Технологии нового поколения уже полностью прошли эволюционный путь развития от коммутаторов до подсистем мультимедийной связи IMS и беспроводных сетей долго временной эволюции LTE. В связи этим всегда предполагалось, основными пользователями сетей нового поколения будут люди и, максимальное число абонентов в таких сетях всегда будет ограничено численностью населения нашей планеты.

В последнее время главное развитие получили методы радиочастотной идентификации RFID, беспроводные сенсорные сети WSN, коммуникации среднего радиуса действия NFC и межмашинные коммуникации M2M, интегрируясь с интернет, способствует обеспечить связь различных технических устройств, число которых может быть большим.

В общем смысле под Интернетом вещей понимается совокупность различных устройств, датчиков, устройств, объединенных в сеть по любым доступным каналам связи, использующих различные протоколы для взаимодействия друг с другом и единственный протокол для выхода в глобальную сеть.

В общем смысле под Интернетом вещей понимается совокупность различных приборов, датчиков, устройств, которые объединены в сеть посредством любых доступных каналов связи, использующих различные протоколы взаимодействия между собой и единственный протокол доступа к глобальной сети.

В IoT у каждой вещи есть свой уникальный идентификатор, которые совместно образуют континуум вещей, способных взаимодействовать друг с другом, создавая временные или постоянные сети. Таким образом вещи могут принимать участие в процессах своих перемещений, делиться сведениями о текущей геопозиции, а имея встроенный интеллект, могут менять свои свойства и адаптироваться к окружающей среде. Одни вещи могут обнаруживать другие, так или иначе связанные с ними вещи, и налаживать с



ними взаимодействие. IoT позволяет создавать комбинацию из интеллектуальных устройств, объединенных сетями связи, и людей. Совместно они могут создавать самые разнообразные системы, например, для работы в средах, неудобных или недоступных для человека.

Считается, что первую в мире интернет-вещь создал Джон Ромки в 1990 году, когда он подключил к сети свой тостер. Но только в 21 веке в связи с бурным развитием инфокоммуникационных технологий сформировалась концепция IoT и получила свое практическое воплощение. Процесс развития Интернета вещей проиллюстрирован технологической дорожной картой, приведенной на рисунке 1.1. Все началось с необходимости оптимизации системы логистики и управления системой снабжения предприятий [4].

Вторая волна инноваций была обусловлена необходимостью сокращения затрат в системах наблюдения, безопасности, транспорта и пр.

Третья была вызвана потребностью в геолокационных сервисах.

Четвертая волна будет обусловлена необходимостью дистанционного присутствия человека на месте совершения требующего его внимания событий, которое станет возможным благодаря миниатюрным встроенным процессорам. А следующим шагом будет возможность создания будущих сетей с ячеистой топологией, включающих в себя метки, датчики, средства измерения и управляющие устройства.



Рисунок 1.1 – Технологическая дорожная карта Интернета вещей

С развитием Интернета вещей все большее количество предметов будет подключено к глобальной сети, тем самым создавая новые возможности в сферах: безопасности, аналитики, управления. Будут открыты новые и широкие перспективы, которые будут способствовать улучшению качества жизни населения. Предполагается, что в будущем «вещи» станут активными участниками социальных и информационных процессов, где они будут

взаимодействовать между собой, обмениваясь информацией об окружающей среде, реагируя и влияя на процессы, происходящие в окружающем мире, без вмешательства человека [5].

### 1.1.1 Базовые принципы IoT

Интернет вещей основывается на трех базовых принципах. Во-первых, повсеместно распространенную коммуникационную инфраструктуру, во-вторых, глобальную идентификацию каждого объекта и, в-третьих, возможность каждого объекта отправлять и получать данные посредством персональной сети или сети Интернет, к которой он подключен.

Наиболее важными отличиями Интернета вещей от существующего интернета людей являются:

- а) фокус на вещах, а не на человеке;
- б) существенно большее количество подключенных объектов;
- в) существенно меньшие размеры объектов и невысокие скорости передачи данных;
- г) фокус на считывании информации, а не на коммуникациях;
- д) необходимость создания новой инфраструктуры и альтернативных стандартов.

Концепция сетей следующего поколения NGN предполагала возможность коммуникаций людей (непосредственно или через компьютеры) в любое время и в любой точке пространства. Концепция Интернета вещей включает еще одно направление - коммуникация любых устройств или вещей (рисунок 1.2).

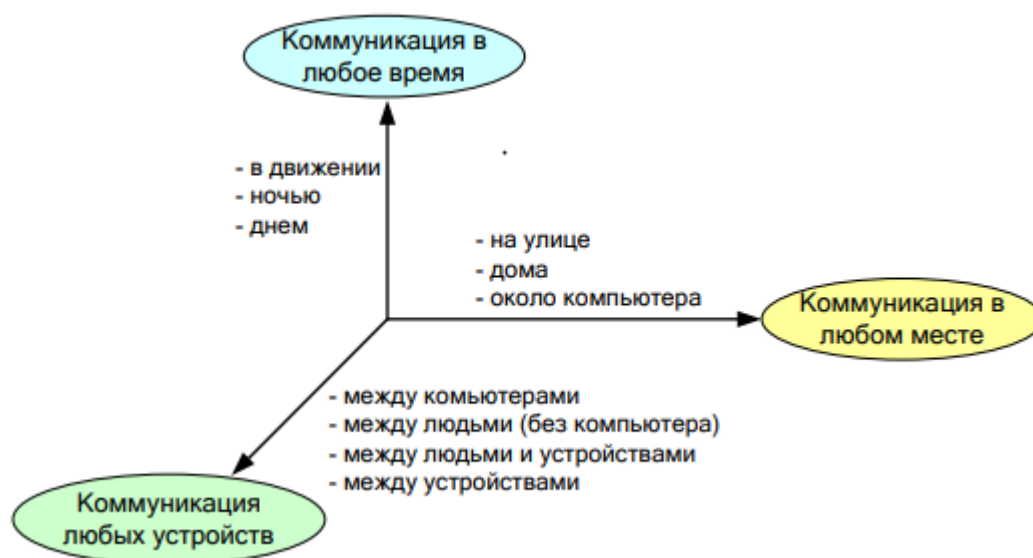


Рисунок 1.2 – Новое направление коммуникаций, реализуемое Интернетом вещей

Концепция IoT и термин для нее впервые сформулированы основателем исследовательской группы Auto-ID при Массачусетском технологическом

институте Кевином Эштоном в 1999 году на презентации для руководства компании Procter&Gamble. В презентации рассказывалось о том, как всеобъемлющее внедрение радиочастотных меток RFID сможет видоизменить систему управления логистическими цепями в корпорации.

Официальное определение Интернета вещей приведено в Рекомендации МСЭ-Т Y.2060, согласно которому IoT – глобальная инфраструктура информационного общества, обеспечивающая передовые услуги за счет организации связи между вещами (физическими или виртуальными) на основе существующих и развивающихся совместимых информационных и коммуникационных технологий [2].

Под «вещами» (things) здесь понимается физический объект (физическая вещь) или объект виртуального (информационного) мира (виртуальная вещь, например, мультимедийный контент или прикладная программа), которые могут быть идентифицированы и объединены через коммуникационные сети. Кроме понятия «вещь», МСЭ-Т также использует понятие «устройство» (device), под которым понимается часть оборудования с обязательными возможностями по коммуникации и необязательными возможностями по сенсорингу/зондированию, приведению в действие вещи, сбору, обработке и хранению данных. Отсюда следует, что МСЭ-Т в большей степени уделяет внимание аспектам коммуникаций и межсоединений, нежели приложениям IoT.

Схема отображения физических и виртуальных вещей представлена на рисунке 1.3. Из рисунка следует, что виртуальные вещи могут существовать без их физических воплощений, в то время как физическим объектам/вещам обязательно соответствует минимум один виртуальный объект. При этом ведущую роль играют именно устройства, которые могут собирать различную информацию и распространять ее по коммуникационным сетям различными способами: через шлюзы и через сеть; без шлюзов, но через сеть; напрямую между собой. Рекомендация Y.2060 описывает различное сочетание перечисленных способов соединений. Это указывает на то, что МСЭ-Т предусматривает использование для IoT множества сетевых технологий – глобальных сетей, локальных сетей, беспроводных самоорганизующихся (ad-hoc) и ячеистых (mesh) сетей. Указанные сети связи переносят данные, собранные устройствами, к соответствующим программным приложениям, а также передают команды от программных приложений к устройствам [3].

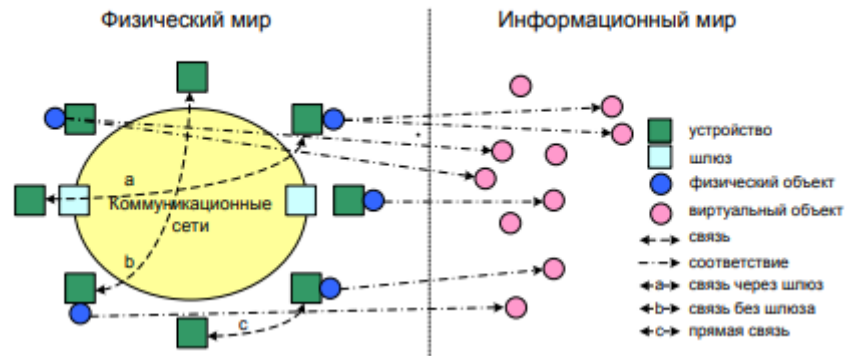


Рисунок 1.3 – Схема отображения физических и виртуальных вещей

Следует отметить, что вещи и связанные с ними устройства могут обладать полноценными управляющими процессорами для обработки данных в виде «системы-накристалле», в том числе с собственной операционной системой, блоком сенсинга/зондирования окружающей среды и блоком коммуникации.

Следует различать понятия «Интернет вещей» и «интернет-вещь». Под интернет вещью понимается любое устройство, которое: имеет доступ к сети Интернет с целью передачи или запроса каких-либо данных, имеет конкретный адрес в глобальной сети или идентификатор, по которому можно осуществить обратную связь с вещью, имеет интерфейс для взаимодействия с пользователем.

### 1.1.2 Архитектура IoT

Интернет вещей концептуально принадлежит к сетям следующего поколения, поэтому его архитектура во многом схожа с известной четырехслойной архитектурой NGN. IoT состоит из набора различных инфокоммуникационных технологий, обеспечивающих функционирование Интернета вещей, и его архитектура показывает, как эти технологии связаны друг с другом. Архитектура IoT включает четыре функциональных уровня (рисунок 1.4) описанных ниже [7].

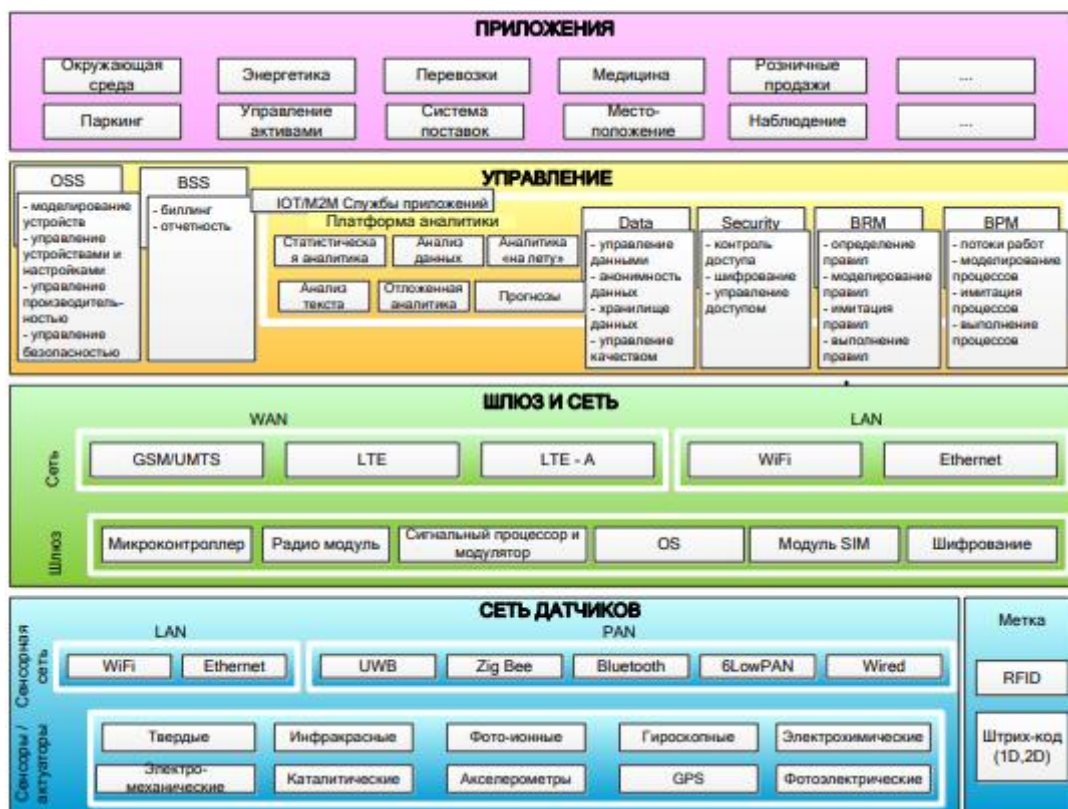


Рисунок 1.4 – Архитектура IoT

Уровень сенсоров и сенсорных сетей.

Самый нижний уровень архитектуры IoT состоит из «умных» (smart) объектов, интегрированных с сенсорами (датчиками). Сенсоры реализуют соединение физического и виртуального (цифрового) миров, обеспечивая сбор и обработку информации в реальном масштабе времени. Миниатюризация, приведшая к сокращению физических размеров аппаратных сенсоров, позволила интегрировать их непосредственно в объекты физического мира. Существуют различные типы сенсоров для соответствующих целей, например, для измерения температуры, давления, скорости движения, местоположения и др. Сенсоры могут иметь небольшую память, давая возможность записывать некоторое количество результатов измерений. Сенсор может измерять физические параметры контролируемого объекта/явления и преобразовать их в сигнал, который может быть принят соответствующим устройством. Сенсоры классифицируются в соответствии с их назначением, например, сенсоры окружающей среды, сенсоры для тела, сенсоры для бытовой техники, сенсоры для транспортных средств и т.д.

Большинство сенсоров требует соединения с агрегатором сенсоров (шлюзом), которые могут реализоваться быть реализованы с использованием локальной вычислительной сети (LAN, LocalAreaNetwork), таких как Ethernet и Wi-Fi или персональной сети (PAN, PersonalAreaNetwork), таких как ZigBee, Bluetooth и ультраширокополосной беспроводной связи на малых расстояниях (UWB, Ultra-WideBand). Для сенсоров, которые не требуют подключения к агрегатору, их связь с серверами/приложениями может предоставляться с

использованием глобальных беспроводных сетей WAN, таких как GSM, GPRS и LTE. Сенсоры, которые характеризуются низким энергопотреблением и низкой скоростью передачи данных, образуют широко известные беспроводные сенсорные сети (WSN, WirelessSensorNetwork). WSN набирают все большую популярность, поскольку они могут содержать гораздо больше сенсоров с поддержкой работы от батарей и охватывают большие площади [11].

2. Уровень шлюзов и сетей. Большой объем данных, создаваемых на первом уровне IoT многочисленными миниатюрными сенсорами, требует надежной и высокопроизводительной проводной или беспроводной сетевой инфраструктуры в качестве транспортной среды. Существующие сети связи, использующие различные протоколы, могут быть использованы для поддержки межмашинных коммуникаций M2M и их приложений. Для реализации широкого спектра услуг и приложений в IoT необходимо обеспечить совместную работу множества сетей различных технологий и протоколов доступа в гетерогенной конфигурации. Эти сети должны обеспечивать требуемые значения качества передачи информации, и прежде всего по задержке, пропускной способности и безопасности. Данный уровень состоит из конвергентной сетевой инфраструктуры, которая создается путем интеграции разнородных сетей в единую сетевую платформу. Конвергентный абстрактный сетевой уровень в IoT позволяет через соответствующие шлюзы нескольким пользователям использовать ресурсы в одной сети независимо и совместно без ущерба для конфиденциальности, безопасности и производительности.

3. Сервисный уровень. Сервисный уровень содержит набор информационных услуг, призванных автоматизировать технологические и бизнес операции в IoT: поддержки операционной и бизнес деятельности (OSS/BSS, OperationSupportSystem/BusinessSupportSystem), различной аналитической обработки информации (статистической, интеллектуального анализа данных и текстов, прогностическая аналитика и др.), хранения данных, обеспечения информационной безопасности, управления бизнес-правилами (BRM, BusinessRuleManagement), управления бизнес-процессами (BPM, BusinessProcessManagement) и др.

4. Уровень приложений. На четвертом уровне архитектуры IoT существуют различные типы приложений для соответствующих промышленных секторов и сфер деятельности (энергетика, транспорт, торговля, медицина, образование и др.). Приложения могут быть «вертикальными», когда они являются специфическими для конкретной отрасли промышленности, а также «горизонтальными», (например, управление автопарком, отслеживание активов и др.), которые могут использоваться в различных секторах экономики [3].

## 1.2 Средства передачи данных Интернета вещей. Классификация технологий передачи данных в IoT

Одним из главных вопросов организации Интернета вещей является реализация взаимодействия между:

- интернет-вещами,
- пользователями и интернет-вещами,
- удаленным сервером и интернет-вещами.

IoT использует большое количество вариантов сетей связи для передачи данных, начиная от сети на теле человека BAN (BodyAreaNetwork), которая работает на расстоянии в несколько десятков сантиметров, вплоть до всемирной сети интернет. Коммуникации малой дальности используют такие технологии, как RFID, NFC, Bluetooth, Wi-Fi и др.

Коммуникации большого радиуса действия реализуются на базе различных сотовых сетей (2G/3G/4G), сетей беспроводного широкополосного доступа WiMAX, сетей позиционирования GPS/ГЛОНАСС и др. По территории охвата телекоммуникационные сети, используемые в Интернете вещей, можно разделить на 4 основных типа (рисунок 1.5):

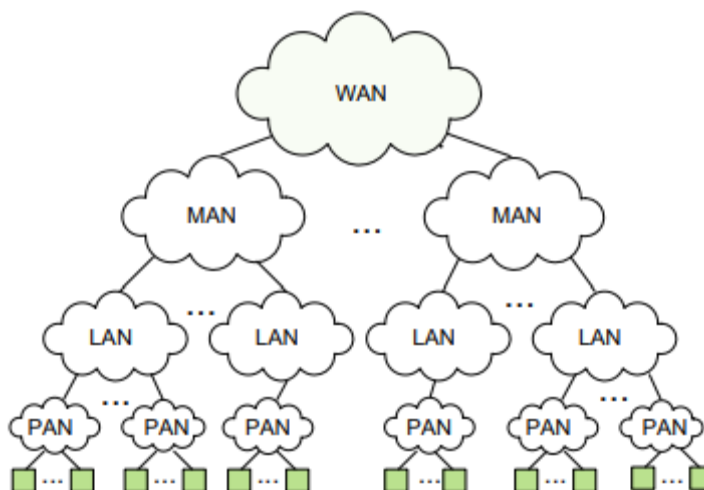


Рисунок 1.5 – Иерархия сетевых технологий, используемых в IoT

1. Персональная сеть PAN (PersonalAreaNetwork) – это сеть, построенная «вокруг» человека. Данные сети призваны объединять все персональные устройства пользователя (телефоны, смартфоны, карманные персональные компьютеры, ноутбуки, гарнитуры и др.). Применительно к IoT такая сеть строится «вокруг» устройства («вещи»).

2. Локальная сеть LAN (LocalAreaNetwork) – сеть, покрывающая обычно относительно небольшую территорию или небольшую группу зданий (дом, офис, фирму). К локальным сетям можно отнести и сеть контроллеров CAN (ControllerAreaNetwork) – промышленную сеть, ориентированную, прежде всего, на объединение в единую сеть различных исполнительных устройств и датчиков в рамках отдельного предприятия.

3. Городская сеть MAN (MetropolitanAreaNetwork) – объединяет отдельных пользователей и локальные сети в пределах города, представляет собой сеть по размерам большую, чем LAN, но меньшую, чем WAN.

4. Глобальная сеть WAN (WideAreaNetwork) – связывает пользователей и сети, рассредоточенные на расстоянии сотен и тысяч километров. Интернет вещей практически не выдвигает особых требований к технологиям LAN, MAN и WAN, кроме того они достаточно хорошо освещены в технической литературе. Поэтому в данной главе рассмотрены только стандарты и протоколы сетей малого и среднего радиуса действия, которые широко используются в IoT.

Все технологии передачи данных в Интернете вещей в зависимости от используемой среды передачи можно разделить на два больших класса: проводные и беспроводные [8].

Проводные технологии передачи данных в IoT могут использовать металлический (медный) кабель связи, электропроводку (технология PLC – PowerLineCommunication) или волоконно-оптический кабель. Однако ввиду сложностей физической реализации линий связи проводные технологии для коммуникаций интернет-вещей применяются в меньшей степени, чем беспроводные.

Беспроводные сети малого радиуса действия, используемые в IoT, можно разделить на три вида:

1. Беспроводные персональные сети WPAN (WirelessPersonalAreaNetwork). Применяются для связи различных устройств, включая компьютерную, бытовую и оргтехнику, средства связи и т.д. Физический и канальный уровни регламентируются стандартом IEEE 802.15.4. Радиус действия WPAN составляет от нескольких метров до нескольких десятков сантиметров. Такие сети используются как для объединения отдельных устройств между собой, так и для связи их с сетями более высокого уровня, например, глобальной сетью интернет. WPAN может быть развернута с использованием различных сетевых технологий, например, Bluetooth, ZigBee, 6LoWPAN и других, рассмотренных далее в данной главе.

2. Беспроводные сенсорные сети WSN (WirelessSensorNetwork). Распределенные, самоорганизующиеся сети множества датчиков (сенсоров) исполнительных устройств, объединенных между собой посредством радиоканала. Область покрытия подобных сетей может составлять от нескольких метров до нескольких километров за счёт способности ретрансляции сообщений от одного элемента к другому.

3. Малые локальные сети TAN (TinyAreaNetwork). Вычислительные сети, развертываемые в пределах небольшого офиса или отдельного жилища. Их часто называют домашними сетями, так как они объединяют компьютеры, бытовую электронику и приборы сигнализации, принадлежащие одной семье. Наиболее часто такие сети строятся на базе технологии Wi-Fi.

Для взаимодействия огромного количества разнообразных устройств в IoT требуются стандартизированные интерфейсы, форматы данных и коммуникационные протоколы. В таблице 1.1 приведен перечень некоторых



стандартов и протоколов IoT с указанием рабочей частоты, скорости передачи данных, поддержки уровней OSI (физического PHY, доступа к среде MAC, сетевого NWK, транспортного TRP), а также реализации подуровня поддержки приложений APS (ApplicationSupportSublayer), поддержки списков управления доступом ACL (AccessControlList) и 128-битного стандарта шифрования AES (AdvancedEncryptionStandart).

Таблица 1.1 – Сравнительный анализ технологии интернета вещей

Стандарт	Частота, МГц	Скорость, кбит/с	Уровни протокола						Шифрование
			PHY	MAC	NWK	TRP	APS	ACL	
IEEE 802.15.4	868/915/2400	20/40/250	+	+	-	-	-	+	+
ZigBee	2400	250	-	-	+	+	+	+	+
6LoWPAN	-	50-200	-	-	+	-	-	+	+
WirelessHART	2400	250	+	+	+	+	+	+	+
ISA100.11a	2400	250	+	+	+	+	+	+	+
Z-Wave	865/915/869	9,6/40	+	+	+	-	+	-	-
Bluetooth LE	2400	1000	+	+	+	+	+	+	+
DECT ULE	1880-1900	1000	+	+	+	-	-	+	+

### 1.3 Технология интернета вещей Zigbee

Технология Zigbee позиционировалась своими авторами для применения в системах контроля и управления, которые передают небольшие объемы данных, например, контроллеры освещенности помещения, термостаты, кондиционеры, пульта дистанционного управления, беспроводные клавиатуры и мыши для компьютера, датчики дыма и углекислого газа, устройства вызова помощи для пожилых людей и детей, устройства домашней автоматизации и т. п. В корпоративном секторе это могут быть, например, складские системы, системы автоматизации производства, различные датчики и т.п [5].

Таким образом, стандарт ZigBee ориентирован, главным образом, на использование в качестве средства связи между автономными приборами и оборудованием управления. Отсюда следуют и предъявляемые к технологии требования, которые были реализованы:

- поддержка сетей с несколькими сотнями функционирующих устройств (до 255 подключенных устройств);
- обеспечение в реальных домашних условиях среднего радиуса действия сетей порядка 30 метров;

- простота инсталляции и применения.

Для сравнения технология Wi-Fi (IEEE 802.11b) поддерживает 50 устройств без потери производительности сети, WirelessUSB и Bluetooth (основные конкуренты Zigbee) — по семь элементов в каждой пикосети.

С другой стороны, дальность действия в домашних условиях для Wi-Fi составляет 100 метров, а для WirelessUSB и Bluetooth — до 10 метров. Таким образом, потребительская ниша новой технологии очевидна — частичная конкуренция с упомянутыми технологиями и полная замена проводных и радиопроводных систем аналогичного назначения (LonWorks, HomePNA и др.) [9].

### 1.3.1 Архитектура стандарта Zigbee

Для того чтобы понять, что же представляет собой ZigBee, как такая беспроводная сеть функционирует, как «дышит», что на самом деле передается по воздуху помимо данных, как организуется доступ устройств к сети и прочие тонкости, нам как раз и поможет IEEE 802.15.4.

Архитектура LR-WPAN сети, в общем, стандартна и очень схожа с классическими компьютерными сетями. LR-WPAN состоит из набора «кирпичиков», слоев или уровней, соединенных между собой логическими связями. Каждый слой отвечает за выполнение набора каких-то конкретных функций, а также предоставляет сервисы для вышестоящих уровней. Структура слоев IEEE 802.15.4 соответствует стандартной общепринятой модели OSI (OpenSystemsInterconnection). Основным используемым методом доступа к физической среде, предлагаемым стандартом, является случайный доступ с контролем несущей и предотвращением конфликтов — CSMA-CA (CarrierSenseMultipleAccesswithCollisionAvoidance). Здесь также реализованы и такие дополнительные функции, как детектирование энергии (ED — Energydetection) и индикатор качества соединения (LQI — Linkqualityindication). Для передачи могут использоваться 16 каналов в диапазоне 2450 МГц, 10 каналов в диапазоне 915 МГц и 1 канал на частоте 868 МГц.

Одной из отличительных особенностей сети IEEE 802.15.4 является поддержка так называемой «суперфреймовой» структуры. Формат суперфрейма определяется координатором сети. Напомним, координатор — это главное сетевое устройство, которое управляет передачей всех потоков данных. Суперфрейм начинается с передачи специального фрейма — «сетевого маркера» (NetworkBeacon), который посылает сам координатор. «Маркер» предназначен, в первую очередь, для синхронизации и управления работой всех активных в сети устройств. После отправки «маркера» координатор самоотстраняется от управления сетью, предоставляя устройствам самостоятельно «разбираться», кто главнее. Для этого в суперфрейме предназначен специальный отрезок времени — период конкурентного доступа устройств к радиоканалу (ContentionAccessPeriod), который разбит на фиксированные временные участки — так называемые

временные слоты (timeslots). В то же время для приложений, критичных к скорости и темпу передачи данных, после участка конкурентного доступа могут идти дополнительные временные слоты (ContentionFreePeriod), в течение которых они гарантированно смогут отправить или получить срочную информацию [9].

Традиционно разработчики стандартов технологий беспроводной связи особое внимание уделяют двум-трем нижним уровням семиуровневой модели открытых систем ISO. На рисунке 1.6 показана архитектура стандарта, где (снизу, вверх) показаны физические уровни (PHY) диапазонов 868 МГц (Европа) и 915 МГц (США), а также физический уровень общего диапазона 2,4 ГГц. Над ними расположен транспортный уровень, определяющий разделение радиосигналов при их доступе к устройству сети.

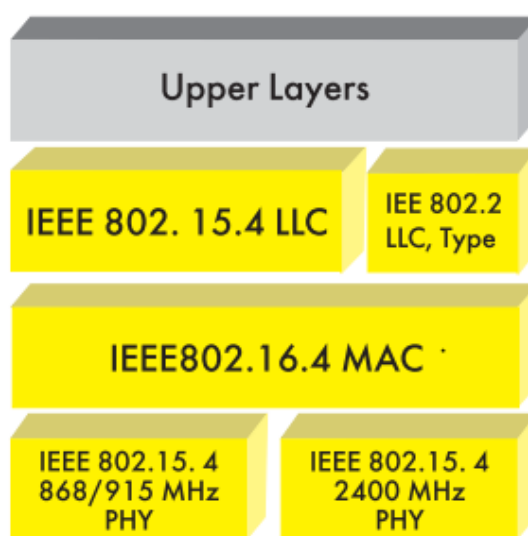


Рисунок 1.6 – Архитектура стандарта

Распределение «зон ответственности» разработчиков и потребителей технологии выглядит следующим образом (рисунок 1.7). Нижние уровни определяются стандартом IEEE, средняя часть находится целиком в ведении ZigBeeAlliance (рисунок 1.7), однако пользуется технологией пользователь (customer), который диктует потребительские свойства эксплуатируемых устройств. Доступ к среде передачи в данной технологии типа CSMA-CA — (CarrierSenseMultipleAccesswithCollisionAvoidance) — множественный доступ с прослушиванием несущей и избеганием коллизий. Данный вид доступа является традиционным для стандартов RadioEthernet[7].

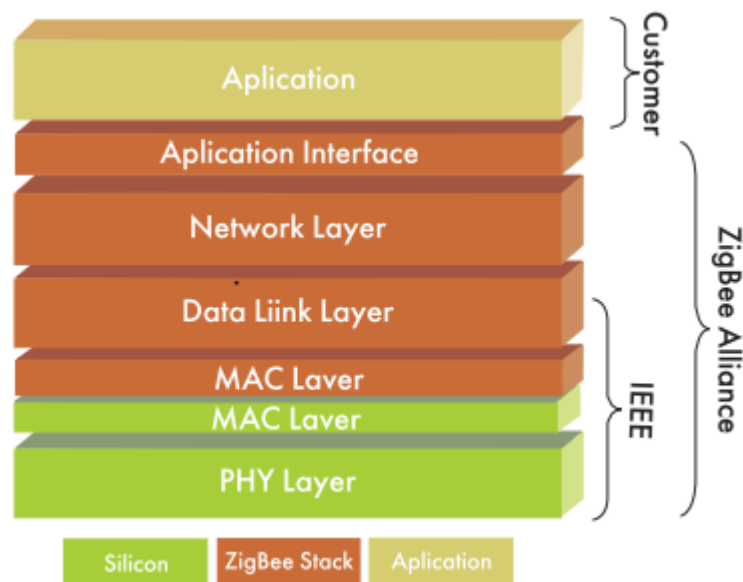


Рисунок 1.7 – Распределение слоев семиуровневой модели

Структура пакета данных показана на рисунке 1.8. Технические параметры технологии (особенно скорость передачи данных) отличаются для различных диапазонов частот.

1. В диапазоне 2,4 ГГц (универсальном в мире):
  - информационная скорость передачи 250 кбит/с;
  - техническая скорость передачи 62,5 кбод при кодировании 4 бит/символ;
2. В диапазоне 868 МГц (Европа) или 915 МГц (США):
  - информационная скорость передачи 20 кбит/с;
  - техническая скорость передачи 20 кбод при кодировании 1 бит/символ.

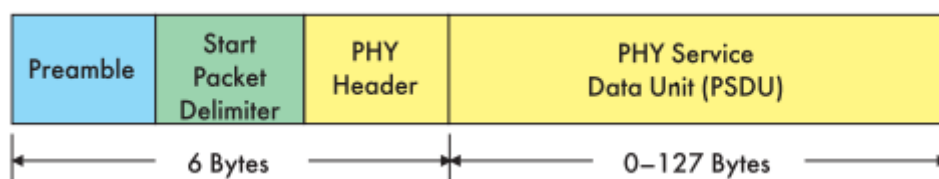


Рисунок 1.8 – Структура пакета данных

Поля пакета (слева направо): преамбула (32 бита) используется для синхронизации пакета, маркер пакета (8 битов) определяет один из трех применяемых типов пакетов, заголовок (8 битов) определяет длину поля данных, PSDU — поле данных от 0 до 127 байтов.

Встречаются данные о достижении скорости передачи данных 40 кбит/с в данном диапазоне. Для всех вариантов вид модуляции несущего колебания одинаков — относительная фазовая манипуляция; для передачи используются нелицензируемые диапазоны частот [3].

Обзор разрешенных для передачи в сети команд (в количестве девяти) позволит составить представление как о возможностях самой сети ZigBee, так и о функционирующих в ней устройствах. Итак, перечислим их: • «Associationrequest» — запрос на присоединение к существующей сети. Данный запрос устройство посылает координатору, когда хочет подключиться к сети. В запрос включается информация о характеристиках устройства — способно ли оно выполнять функции координатора сети, тип устройства (полнофункциональное устройство или устройство с ограниченными возможностями), способ питания (от обычной сети или иной), отключает ли устройство радиоприем, когда находится в «спящем» режиме, поддерживается ли криптозащита, 16- или 64-разрядный адрес хочет иметь устройство. Запрос на подсоединение могут посылать только те устройства, которые к данной сети еще не подключались [2].

- «Associationresponse» — ответ координатора сети устройству, запросившему присоединение к сети. При этом координатор может: подключить это устройство к сети с присвоением адреса, сообщить, что свободных мест нет, или отказать в доступе без объяснения причин.

- «Disassociationnotification» — команда отключения от сети. Может посылаться координатором, при этом он сообщает адрес устройства, которое из сети исключается. Команда также может посылаться и любым устройством в сети, при этом оно сообщает координатору свой адрес.

- «Datarequest» — команда, которую посылает устройство при запросе данных от координатора.

- «PAN ID conflictnotification» — команда, которую посылает устройство координатору сети, когда оно обнаруживает конфликт идентификаторов сети.

- «Orphannotification» — команда, которую посылает включенное в сеть устройство при потере синхронизации с координатором.

- «Beaconrequest» — команда, которую посылает устройство для выявления в пределах дальности своей работы всех координаторов сетей.

- «Coordinatorrealignment» — команда ресинхронизации сети, которую посылает координатор либо в ответ на команду потери синхронизации (Orphannotification), либо если какие-то атрибуты сети претерпели изменения. В первом случае команда отправляется конкретному устройству, испытывающему проблемы с синхронизацией, во втором случае отправляется широковещательная команда всем доступным устройствам. —

- «GTS request» — команда, которая предназначена для управления гарантированными временными слотами, предоставляемыми некоторым устройствам для передачи данных в пределах маркерного фрейма. GTS request позволяет устройствам как запрашивать выделение таких слотов, так и освобождать уже выделенные. Гарантированные слоты предоставляются только устройствам с короткими адресами, в запросе указывается число требуемых или высвобождаемых слотов времени, направление передачи данных (только прием или только передача относительно запрашивающего устройства) и 1 разряд — собственно просьба (выделить или освободить указанные временные слоты).

При рассмотрении действующих в сети ZigBee команд обращает на себя внимание следующий факт. Устройства с ограниченными возможностями могут не поддерживать подавляющее большинство из них. Причем, что характерно, в спецификации про эти команды говорится по-разному. Некоторые являются «необязательными», другие могут присутствовать «опционально». В чем конкретно разница между этими двумя случаями — непонятно, скорее всего, это одно и то же.

Надежность. Вернемся к возможностям IEEE 802.15.4. Как вы помните, одной из заявленных характеристик беспроводных сетей, строящихся на базе этого стандарта, является высокая надежность передачи данных. Какие механизмы применяются для этого на уровнях PHY и MAC, нам и предстоит сейчас разобраться.

В данной LR-WPAN применяются различные механизмы для обеспечения надежности и достоверности передаваемой информации. Эти методы включают в себя использование механизма передачи CSMA-CA, фреймы подтверждения получения и верификации данных. Рассмотрим их подробнее.

В IEEE 802.15.4 используется два типа доступа к каналам передачи, зависящие от конфигурации сети. В сетях, где «маркерные» фреймы не используются (Nonbeacon-enabled networks) и доступ к каналу происходит случайным образом, задействуется механизм, называемый «unslotted CSMA-CA channel access mechanism». Каждый раз, когда устройству требуется передать фрейм данных или MAC команду, оно должно сначала выждать некоторый промежуток времени (его длительность выбирается случайным образом). Если канал после этого окажется свободным, устройство передает свои данные. Если же канал оказывается занятым после этой произвольной задержки, устройству следует подождать еще один случайный отрезок времени и потом опять попытаться получить доступ к каналу [4].

В сетях с «маркерными» фреймами используется механизм с фиксированными временными слотами ожидания передачи «slotted CSMA-CA», идущими сразу после «маркерного» фрейма. Каждый раз, когда устройство захочет передать данные в период конкурентного доступа к каналу, оно должно сначала определить границу ближайшего слота ожидания и отсчитать от него случайное число подобных слотов. Если канал окажется занят после этой паузы, устройству предстоит подождать следующее случайное число фиксированных временных слотов, перед тем как попытаться получить доступ к каналу снова. Если канал свободен, устройство может начать передачу сразу с границы ближайшего слота ожидания.

Энергопотребление. Как неоднократно говорилось выше, одним из главных достоинств стандарта ZigBee является ориентация на малое энергопотребление беспроводных устройств. Не зря ведь в анонсах и рекламных проспектах одним из первых оговаривается именно этот немаловажный параметр. На деле, как обычно, все оказывается немного сложнее. Дело в том, что в основе ZigBee — стандарте IEEE 802.15.4 — о низком потреблении говорится совсем немного. Здесь, например,

оговаривается следующий момент: данный стандарт разработан, в принципе, с возможностями применения в условиях ограниченного питания. Однако физическое применение стандарта требует дополнительных изысканий в этом направлении, а это уже выходит за рамки IEEE 802.15.4. При всем этом разработчики дают общие указания о том, как уменьшить энергопотребление устройств, которым это действительно необходимо. В аппаратуре подобного типа, использующей в качестве элементов питания батареи или аккумуляторы, предлагается в обязательном порядке применение циклического режима работы. Большую часть времени такие устройства должны проводить в «спящем» режиме. Причем им следует периодически включать радиотракт и прослушивать эфир на случай готовящихся для передачи сообщений. Этот простой и в то же время гибкий механизм, прежде всего, позволит разработчикам программных приложений на высоком уровне соблюдать баланс между экономией электроэнергии и задержкой в передаче сообщений [6].

Безопасность. Еще одним наиважнейшим параметром, характеризующим любую сеть, а тем более беспроводную, является безопасность передаваемых данных и защита их от несанкционированного доступа. В привычных для нас локальных проводных сетях эта проблема на аппаратном уровне обычно не решается, безопасность передаваемых данных обеспечивается сервисами и службами более высокого программного уровня.

Точно так же могли поступить и создатели IEEE 802.15.4, однако они все же ввели в стандарт некоторый набор базовых функций, обеспечивающих начальный уровень безопасности на MAC-уровне. Базисными сервисами в этом направлении стали: поддержка списков контроля доступа ACL (accesscontrollist) и криптографическое шифрование передаваемых данных.

Способность выполнять простейшие действия по обеспечению безопасности не является обязательной, однако разработчики настоятельно рекомендуют использовать эти функции постоянно и во всех устройствах.

### 1.3.2 Структуры сетей Zigbee

В соответствии с технологией Zigbee сети беспроводной передачи включают в свой состав устройства двух классов — полнофункциональные (Fullfunctiondevice — FFD) и устройства с ограниченной функциональностью (Reducedfunctiondevice — RFD).

Устройства первого типа обеспечивают расширенные возможности по построению топологии сети, могут выполнять роль координатора работы сети (главной станции радиосети) и могут обмениваться сообщениями с любой другой станцией сети. Устройства второго типа могут работать только в сети звездообразной формы, не могут выполнять функции координации работы сети обмена данными и имеют упрощенную конструкцию. Последнее свойство — изначально заложенное в идеологию технологии неравенство возможностей устройств при их работе в единой сети — как раз и позволяет обеспечить их чрезвычайно низкое энергопотребление.

Если для устройств Bluetooth с точки зрения энергопотребления характерен подход, аналогичный сотовой телефонии — периодическая подзарядка батарей, то здесь ориентация осуществлена в направлении длительного использования источников однократного применения (пальчиковых элементов) для многочисленных абонентских устройств и домашней электросети — для координатора [7].

Также существенно отличаются для данных технологий и временные параметры алгоритмов работы сетей: для Bluetooth время выхода устройства из «спящего» режима составляет около трех секунд, а для Zigbee — 15 мс; время доступа подчиненного устройства к среде передачи — 15 мс и 2 мс соответственно; даже длительность «прописывания» нового элемента в сети существенно различна — более 3 с для Bluetooth и менее 30 мс для Zigbee. Одним из главных достоинств технологии является обещаемое сверх длительное использование автономных источников питания, предполагается, что двух-трех пальчиковых элементов хватит для функционирования автономного устройства в течение нескольких месяцев. Фактически эти данные подчеркивают то, что сравниваемые технологии рассчитаны на применение в различных сферах приложений, а значит, они попросту несравнимы.

На рисунке 1.9 показана структура сети типа «звезда». Задачи главной станции сети:

- передает сетевые маркеры;
- объединяет абонентские устройства в единую сеть;
- управляет абонентскими устройствами;
- хранит информацию о состоянии сети;
- организует передачу данных между тяготеющими элементами сети;
- получает питание от электросети;
- постоянно находится в режиме приема.

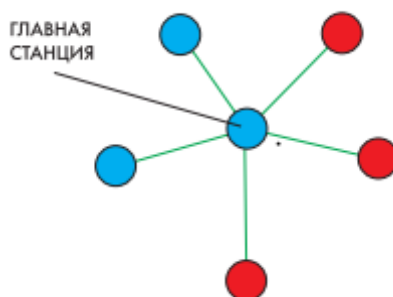


Рисунок 1.9 – Структура сети типа «звезда»

В центре находится станция первого типа, выполняющая функции главной станции сети. Она связана со станциями обоего типа, являющимися подчиненными.

В свою очередь, подчиненная станция сети:



- принимает и передает данные в соответствии с выполняемым приложением;
- определяет, имеются ли данные, которые необходимо передать;
- запрашивает, в случае необходимости, необходимые данные от координатора сети;
- обычно обеспечивается электропитанием от автономной батареи;
- может находиться в спящем режиме длительное время.

Станции первого типа могут также создавать однородные структуры вида, показанного на рисунке 1.10 [7].

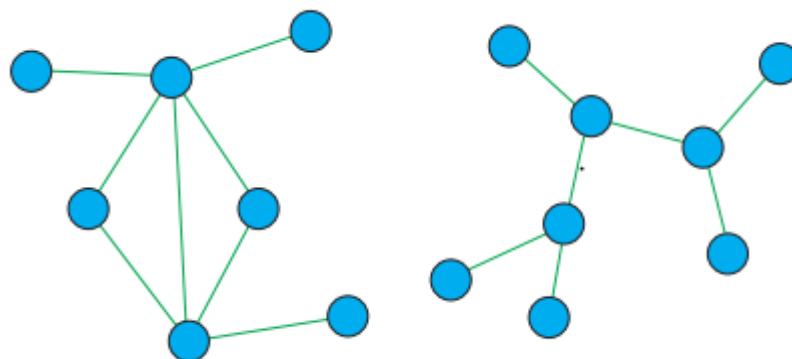


Рисунок 1.10 – Структуры сетей однородного типа

Наконец, подобно Bluetooth, технология позволяет строить структуры смешанного типа (рисунок 1.11).

В зависимости от вида структуры сети меняется и адресация ее элементов. Применяются следующие способы адресации: сеть + идентификатор устройства (звездообразная структура), идентификаторы источника/получателя сообщений (однородная структура), дерево кластеров источников/получателей сообщений + идентификатор устройства (структуры смешанного типа). Алгоритмы процесса передачи данных оптимизированы под вид входящего трафика, который может иметь следующие временные параметры:

- данные, передаваемые через определенные промежутки времени в различных направлениях (датчики, сенсоры, телеметрия);
- данные, передаваемые через случайные интервалы времени в различных направлениях (управление освещением, оконными шторами);
- случайная длительная прерывистая передача данных в одном направлении (работа мыши или клавиатуры ПК).

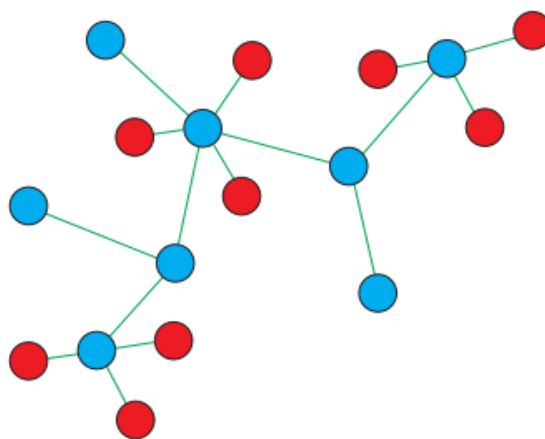


Рисунок 1.11 – Структуры смешанного типа

Протокол ZigBee определяет характер работы сетей датчиков. Устройства образуют иерархическую сеть, которая может содержать координатор, маршрутизаторы и конечные устройства. Корнем сети является координатор ZigBee. Маршруты могут учитывать иерархию, возможна также оптимизация информационных потоков. Координатор ZigBee определяет сеть и устанавливает для нее оптимальные параметры. Маршрутизаторы ZigBee включаются в сеть либо через координатора ZigBee, либо через другие, уже входящие в сеть маршрутизаторы. Конечные устройства могут соединяться с любым маршрутизатором ZigBee или координатором ZigBee. По умолчанию трафик сообщений распространяется по ветвям иерархии. Если маршрутизаторы имеют соответствующие возможности, они могут определять оптимизированные маршруты к определенной точке и хранить их для последующего использования в таблицах маршрутизации [8].

Для разработчиков приложений ZigBee существует программное обеспечение Z-Stack. Данное ПО обеспечивает уровни стека протоколов от транспортного до уровня приложений, то есть дает возможность конфигурировать работу беспроводной системы и отдельных ее компонентов через профили устройств. Пакет Z-Stack позволяет организовывать сети с различными топологиями (“точка-точка”, “звезда”, “кластерное дерево”, “многочейковая сеть”). Также данный пакет гарантирует совместимость с другими сертифицированными ZigBee-устройствами и обеспечивает поддержку и обновление для приобретенного ПО. В пакете Z-Stack содержится полный набор документации (руководства пользователя, инструкция по разработке и т.д.).

## 2 Методы построения и параметры функционирования технологии IoT

### 2.1 Архитектура сетей IoT/M2M

Для оказания и управления услугами M2M могут использоваться как специализированные сети M2M, создаваемые сервис-провайдерами услуг M2M, так и уже имеющаяся у операторов инфраструктура сетей LTE. Современные мобильные сети создавались и предназначены для решения задачи обеспечения мобильности и оказания речевых услуг, передачи SMS, MMS, мультимедийных сообщений на интерфейсе «человек – человек» (human-to-human (H2H)) или «сервер-человек» (загрузка данных приложений /передача потокового аудио/видео). Поэтому технологии и архитектура сетей мобильной беспроводной связи, построенные на принципах H2H, не являются оптимальными по отношению к услугам M2M, что является стимулом для работ по созданию новой инфраструктуры сетей связи, ориентированных на услуги M2M и соответствующих приложений. Сети M2M определяются как сети, объединяющие оконечные устройства, работающие без участия или с ограниченным участием человека, или с ограниченным вмешательством человека как конечного пользователя [3-4]. Нужно отметить, что человек, как конечный пользователь, является не типичным инициатором входа в сеть M2M, и только случайно или разово потребителем результатов работы сетей M2M. Главной особенностью и отличием сетей M2M от мобильных сетей связи является низкий уровень трафика оконечных устройств и необходимость объединения в сети огромного количества оконечных устройств на порядок превышающих число абонентов мобильных сетей в единые сети. Архитектура сетей M2M. Основные элементы архитектуры сетей M2M разделены на три домена: домен устройств M2M (домен капиллярной сети); сетевой домен (ядро базовой сети M2M) и домен приложений [5]. Кроме указанных доменов, в состав сети M2M включаются соответствующая сеть доступа и транспортная сеть, которые строятся на основе сетей 3GPP NGN сетей. Устройства M2M: позволяют быстро применить и воспользоваться услугами M2M и функциями доменной сети. Устройство M2M может быть соединено с сетью доступа либо напрямую, либо через локальную сеть M2M и шлюз M2M. Локальные сети M2M предоставляет соединение между устройствами M2M и шлюзами M2M. Примеры: PAN-технологии такие, как IEEE 802.15, SRD, UWB, Zigbee, Bluetooth или локальные сети такие, как PLC, M-BUS, Wireless M-BUS. Шлюзы M2M: представляют собой оборудование, обеспечивающее устройствам M2M гарантированное межсетевое взаимодействие и подключение к сети и прикладным доменам. Шлюз M2M может использоваться для различных приложений устройств M2M. Функционально шлюз M2M может быть объединен в одном модуле с устройством или группой M2M Сети доступа: представляет собой сети, позволяющие домену устройств M2M обеспечивать соединение с ядром сети M2M (базовой сетью). Функциональные возможности сетей доступа M2M базируются на

возможностях существующих сетей доступа (xDSL, HFC, PLC, VSAT, GERAN, UTRAN, LTE, W-LAN и WiMAX) и позволяют обеспечивать расширение как перечня услуг, так и их возможностей. Транспортная сеть: представляет собой сеть, позволяющую обеспечивать транспортировку данных между сетевым доменом и доменом приложений. Функциональные возможности транспортных сетей в сетях M2M базируются на возможностях существующих транспортных сетей и так же, как и сети доступа позволяют обеспечивать расширение как перечня услуг M2M, так и их возможностей. Базовая сеть M2M (Ядро сети): состоит из базовой сети и ее сервисных функциональных характеристик. Базовая сеть M2M: предоставляет функциональные возможности IP соединения элементов сети M2M, сервисные и сетевые функции управления, межсетевое взаимодействие, роуминг и обеспечение безопасности. Функциональные возможности базовой сети M2M основываются на соответствующих функциональных возможностях существующих базовых сетей 3GPP CN (например, GPRS, EPC, ETSI TISPAN CN) [6]. Сервисные функциональные модули M2M: реализуются базовой сетью M2M и предоставляют возможность выполнения функций, которые могут объединять различные приложения. Они взаимодействуют на основе открытых интерфейсов сети M2M. В дополнение к собственным функциональным возможностям сеть M2M позволяет использовать функциональные возможности базовых сетей 3GPP и TISPAN. Модули обеспечивают также возможности упрощения и оптимизации используемых приложений и услуг M2M. Основные функциональные возможности базовой сети M2M (Service Capability), реализуемые соответствующими функциональными модулями сети M2M, включают: – управление возможностями приложений - Application Enablement (xAE); – обеспечение общих взаимосвязей в сети - Generic Communication (xGC); – обеспечение достижимости устройств/шлюзов, адресации и хранение данных - Reachability, Addressing and Repository (xRAR); – выбор взаимосвязей - Communication Selection (xCS); – удаленное управление устройствами - Remote Entity Management (xREM); – обеспечение безопасности - SECURITY (xSEC); – сохранение истории и данных - History and Data Retention (xHDR); – управление обработкой запросов - Transaction Management (xTM); – управление компенсацией - Compensation Broker (xCB); – экспозиция базовой сети операторам связи - Telco Operator Exposure (xTOE); – доверительное сетевое взаимодействие Interworking Proxy (xIP). Основные сетевые интерфейсы сетей M2M. Основные сетевые интерфейсы сетей M2M стандартизованы и приведены в TS 102 921[6]. При их разработке учитывались три основных аспекта, которые определялись для точек сопряжения элементов сети M2M, чтобы обеспечить эквивалентность и полноту стандартизации интерфейсов, а именно:

- терминологическое определение протокола/прикладного интерфейса (API); - определение ресурсов и суб-ресурсов сети M2M; - взаимодействие используемых протоколов, в том числе определение ключевых базовых протоколов. Основные функции базовой сети M2M построенной на платформе

IMS включают [7-8]: регистрацию, аутентификацию, авторизацию, хранение базы данных абонентов сети, управление сессиями, управление политиками сети, процедуру трансляции сетевых адресов NAT и др. Учитывая особенности базовой сети M2M, не охватываемые платформой IMS в полном объеме, некоторые сервисные функциональные характеристики базовой сети M2M (например, функции безопасности NSEC и обеспечение достижимости сетевых элементов NRAR) могут быть дополнены к функциям IMS в целях обеспечения управления сетью M2M. В соответствии с принципами построения функциональной архитектуры сетей M2M интерфейсы должны удовлетворять следующим требованиям: - быть применимыми широкому спектру сетевых технологий и не ограничивать их применимость при использовании в других сетях (например, использованием других протоколов); - быть инвариантными ко всем областям применения сетей M2M, быть независимыми от приложений M2M и используемых сетей доступа. Интерфейсы сети M2M mla, dla, mld: обеспечивают на основе принципа открытых интерфейсов взаимодействие между доменом приложений и базовой сетью M2M, между прикладным и функциональным уровнем домена устройств M2M, между устройствами M2M и шлюзом M2M соответственно. Типовые интерфейсы с привязкой к точкам сопряжения элементов сети M2M показаны на рисунке 2.1 [7].



Рисунок 2.1 – Интерфейсы сети M2M и точки сопряжения

Интерфейс mla сети M2M обеспечивает взаимодействие приложения M2M с функциональными модулями базовой сети M2M или домена приложений.

Интерфейс dla сети M2M обеспечивает взаимодействие приложения M2M, активированного в M2M устройстве, иметь доступ к функциональным модулям этого M2M устройства или M2M шлюза, а также взаимодействие

приложения M2M, активированного в M2M шлюзе с приложением M2M устройства, иметь доступ к функциональным модулям этого M2M шлюза.

Интерфейс mld сети M2M обеспечивает взаимодействие M2M устройства или M2M шлюза с модулями основных функций M2M в сети и доменом приложений. Интерфейс mld использует функции присоединения базовой сети в качестве своего базового уровня

Интерфейсы взаимодействия базовой сети M2M при использовании платформы IMS. Подсистема мультимедийных услуг IMS обладает всеми функциональными возможностями базовой сети (Core Network), позволяющими реализовывать сервисные функциональные х объеме, некоторые сервисные функциональные характеристики базовой сети M2M (например: функции безопасности NSEC и обеспечения достижимости сетевых элементов NRAR) могут быть дополнены к функциям IMS в целях обеспечения управления сетью M2M [9].

Взаимодействие основных функциональных модулей базовой сети M2M, платформы IMS, интерфейсов сети M2M (mla,mld) и внутренних интерфейсов (ISC,Gm) базовой сети M2M, а также устройств M2M/M2M шлюзов соответствующего сервис-провайдера услуг M2M показано на рисунке 2.2.

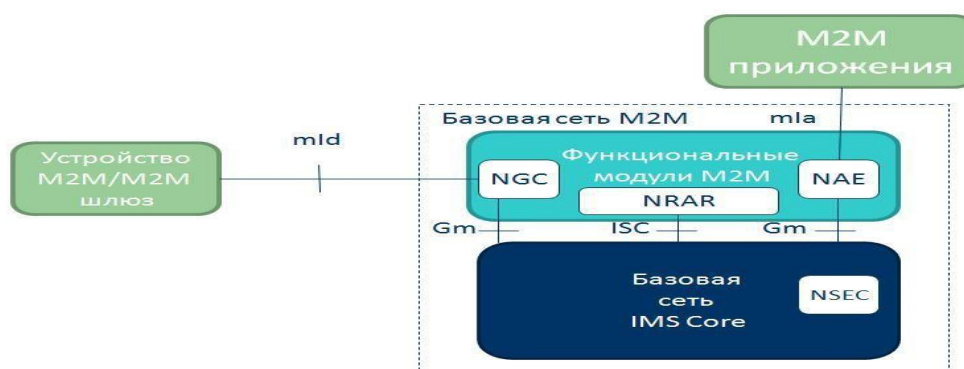


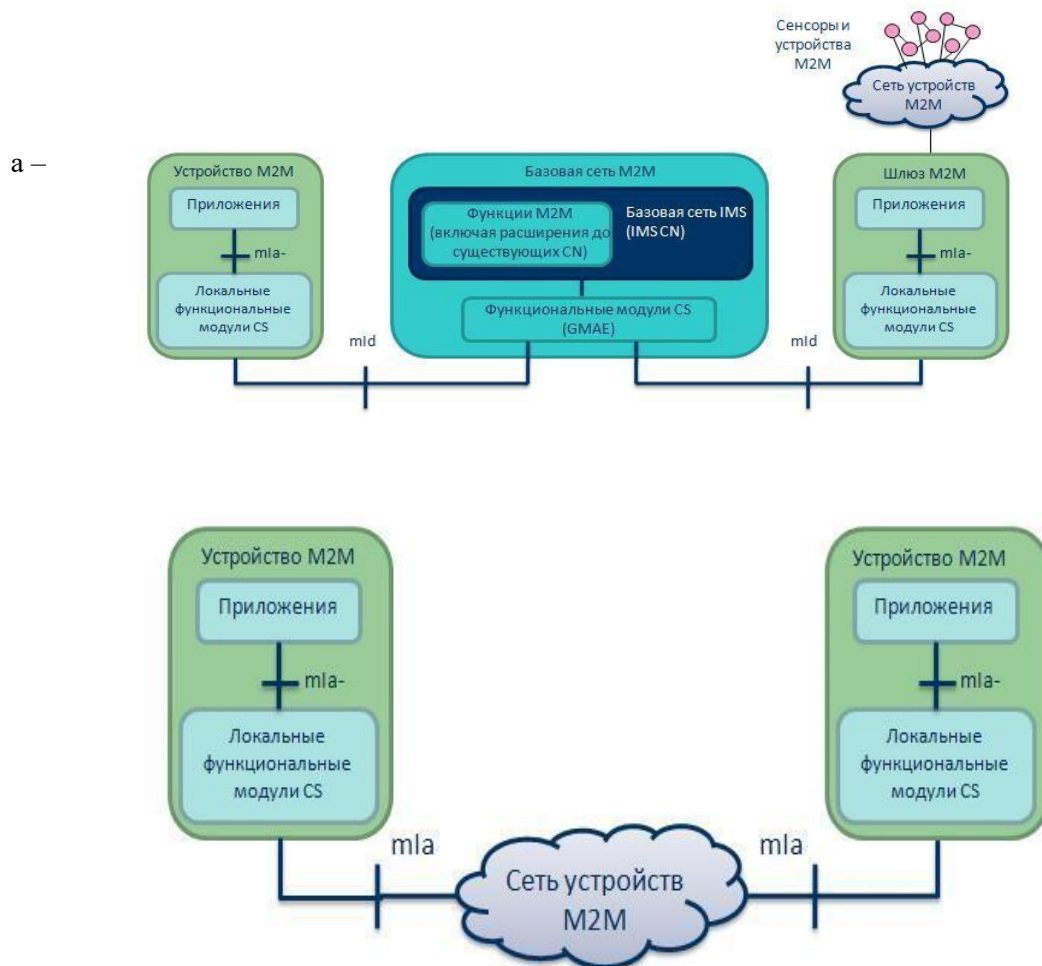
Рисунок 2.2 - Взаимодействие основных функциональных модулей базовой сети M2M

Интерфейс ISC базовой сети M2M обеспечивает обмен данными и присоединение сервера приложений, и доступ к услугам M2M, а также доступ информации и использование функциональных возможностей базовой сети IMS Core.

Интерфейс Gm сети M2M, выполняющий аутентификацию и авторизацию различных приложений M2M-устройств, а также сетевых приложений, используется для реализации ряда функций базовой сети M2M (SC). Он также связан с базовой сетью IMS через ISC интерфейс в целях обмена информацией с приложениями M2M-устройств через модуль NGC. Обмен информацией базовой сети M2M SC с сетевыми приложениями осуществляется через модуль NAE [8].

Варианты взаимодействия устройств M2M подразумевают их взаимодействие как с использованием базовой сети M2M и шлюзов M2M, так их взаимодействие без ее использования и показаны на рисунках 2.3а и 2.3б.

В первом случае абонентское устройство сети M2M представляет собой также точку взаимодействия интерфейса m1d домена M2M устройств, соединяющего M2M устройство/M2M шлюз и базовую сеть M2M.



взаимодействие M2M-устройств через сеть;

б – прямое взаимодействие M2M-устройств.

Рисунок 2.3 – Варианты взаимодействия устройств M2M

Во втором случае абонентское устройство сети M2M представляет собой также точку взаимодействия интерфейса m1a домена M2M устройств между приложениями и функциональными модулями, поддерживающими основные функции сети M2M на местном уровне. Интерфейс m1a в этом случае также используется для взаимодействия с локальной сетью устройств M2M [5].

## 2.2 Платформа IMS и ее функциональные элементы

Подсистема IMS (IP Multimedia Subsystem) — базовая подсистема услуг IP-мультимедиа сети LTE, осуществляющая управление и синхронизацию при передаче пакетов данных (речи, видео, аудио, текстовых сообщений) пользователя, а также резервирование сетевых ресурсов, маршрутизацию IP-пакетов в режиме реального времени, поддержку интерфейса с серверами приложений, системами управления и биллинга оператора [2, 9-14]. В соответствии с этим назначением IMS выполняет следующие функции:

- маршрутизацию сигнализации и адресацию пакетов данных согласно SIP-протоколу между абонентским терминалом UE и сервером приложения, между абонентским терминалом UE и сервером присутствия (Present) подсистемы IMS;
- аутентификацию и авторизацию абонентов подсистемы IMS;
- управление качеством услуг QoS;
- сжатие (компрессию) SIP-сообщений для оптимизации трафика сигнализации;
- поддержку режима регистрации и сеансов обмена данными SIP протокола;
- подготовку отчетов для системы тарификации.

Подсистема IMS предназначена, прежде всего, для оказания пользователям сети LTE услуг телефонии (voice), услуг обмена короткими (SMS), мультимедийными (MMS) и мгновенными (IM) сообщениями, обеспечивает взаимодействие сети LTE с другими сетями: сетями подвижной радиотелефонной связи (PLMN), сетями фиксированной телефонной связи (PSTN), сетями передачи данных (PDN), сетями VoIP. Для обеспечения непрерывности голосовых услуг с помощью подсистемы IMS реализуется технология SRVCC [6].

В состав базовой подсистемы IMS входят следующие основные функциональные элементы:

- AS (Application Server) — сервер приложений (например, SIP Application Server, OSA Application Server или CAMEL IM-SSF), содержащий логику обработки сигнализации и обеспечивающий предоставление услуг конечным пользователям;
- HSS (Home Subscriber Server) — домашний сервер базы данных пользователей, представляющий собой совокупность HLR/AuC и содержащий базу данных профилей абонентов, доступную для узлов AS, MME, S-CSCF, I-CSCF, пульта управления COPM (PIU COPM);
- SLF (Subscription Locator Function) — сервер определения базы данных HSS, хранящей профиль пользователя; сервер SLF предоставляет информацию S-CSCF, I-CSCF об адресе обслуживающего HSS и используется, когда в подсистеме IMS реализовано несколько HSS;



- LRF (Location Retrieval Function) — сервер определения местоположения абонентов на основе данных регулярного обновления местоположения мобильными терминалами ( updated location information);
- P-CSCF (Proxy Call Session Control Function) — прокси-сервер, являющийся первым сетевым элементом подсистемы IMS, с которым устанавливает контакт абонентский терминал UE;
- S-CSCF (Serving Call Session Control Function) — центральный обслуживающий сервер подсистемы IMS, обеспечивающий аутентификацию авторизацию пользователей, управление сессиями и статусами присутствия пользователей;
- I-CSCF (Interrogating Call Session Control Function) — опрашивающий сервер, являющийся граничным элементом подсистемы IMS, с которым устанавливает контакт внешняя подсистема IMS.
- E-CSCF (Emergency Call Session Control Function) — сервер подсистемы IMS, обеспечивающий предоставление услуг конечному пользователю по вызову экстренных оперативных служб 112 (911);
- EATF (Emergency Access Transfer Function) — сервер подсистемы IMS, обеспечивающий непрерывность услуг конечному пользователю по вызову экстренных оперативных служб;
- ATCF (Access Transfer Control Function) — контроллер, обеспечивающий реализацию функциональности SRVCC;
- MGCF (Media Gateway Control Function) — контроллер медиашлюза IMS-MGW, обеспечивающий управление ресурсами медиашлюза по протоколу H.248/MEGACO;
- IMS-MGW (Media Gateway Function) — медиашлюз, обеспечивающий передачу голосового трафика (User Plane) по протоколу реального времени RTP, транскодирование голосового сигнала (смена голосового кодека);
- BGCF (Breakout Gateway Control Function) — контроллер, обеспечивающий выбор сети PLMN (CS Domain), PSTN и маршрута передачи сообщений сигнализации SIP от S-CSCF в сеть регистрации вызываемого абонента;
- SGW (Signalling Gateway Function) — шлюз сигнализации, являющийся пограничной точкой обмена сообщениями сигнализации между подсистемой IMS и сетями PLMN, PSTN; шлюз сигнализации SGW реализует функции контроля безопасности и преобразование сообщений SIGTRAN SCTP/IP в сообщения SS7 MTP и обратно;
- MRB (Media Resource Broker) – сервер управления ресурсами мультимедиа MRF (MRFC, MRFP), обеспечивающий идентификацию приложений и выделение для них требуемых ресурсов мультимедиа в соответствии с настраиваемыми правилами, критериями QoS и SLA;

- MRFP (Multimedia Resource Function Processor) — процессор ресурсов мультимедиа, обеспечивающий предоставление (воспроизведение) аудио и видео контента пользователю;
- MRFC (Multimedia Resource Function Controller) — контроллер, обеспечивающий управление процессором ресурсов мультимедиа MRFP в соответствии с командами от серверов AS и S-CSCF, генерацию записей CDR;
- IBCF (Interconnection Border Control Function) — пограничный контроллер сигнализации, обеспечивающий обмен сигнализацией SIP/SDP между подсистемой IMS и внешними сетями VoIP, управление ресурсами транзитного медиашлюза TrGW;
- TrGW (Transition Gateway) — транзитный шлюз, обеспечивающий передачу мультимедиа трафика (Media Plane) по протоколу реального времени RTP, транскодирование мультимедиа трафика. Функциональные модули базовой сети M2M на основе платформы IMS [10].

Подсистема мультимедийных услуг IMS Core обладает всеми функциональными возможностями базовой сети M2M, позволяющими реализовывать сервисные функциональные характеристики сети M2M при взаимодействии с приложениями M2M устройств и базовыми сетевыми приложениями сети доступа.

Основные функции базовой сети M2M, построенной на платформе IMS, включают регистрацию, аутентификацию, авторизацию, хранение базы данных абонентов сети, управление сессиями, управление политиками сети, процедуру трансляции сетевых адресов NAT и др. Учитывая особенности базовой сети M2M, не охватываемые платформой IMS в полном объеме, некоторые сервисные функциональные характеристики базовой сети M2M (например: функции безопасности NSEC и обеспечения достижимости сетевых элементов NRAR) могут быть дополнены к функциям IMS в целях обеспечения управления сетью M2M.

Сервисные функциональные характеристики базовой сети M2M реализуются в виде соответствующих функциональных модулей, которые определены стандартом ETSI на функциональную архитектуру сети M2M. Наиболее важными функциональными модулями, обеспечивающими возможности управления сетью M2M, и реализация которых требуется в базовой сети M2M на платформе IMS, являются модули NAE, NGC, NRAR и NSEC.

Модуль NAE (Network Application Enablement) обеспечивает взаимодействие приложений M2M на уровне сетевого домена и домена приложений M2M, а также:

- открывает доступ приложений M2M к функциональным модулям базовой сети M2M Core по интерфейсу m1a;
- обеспечивает скрытность топологии функциональных модулей SC и адресов NAE, выдавая только необходимую для работы приложений M2M;
- обеспечивает регистрацию приложений M2M в соответствующих функциональных модулях SC;

- обеспечивает аутентификацию и авторизацию приложений M2M через модуль безопасности, а также проверяет наличие соглашения у провайдера приложений M2M и его уровень взаимодействия с функциональными модулями SC;
- проверяет через интерфейс m1a возможности применения функциональных модулей SC и выдает отчет об ошибке при невозможности маршрутизации к другим функциональным модулям.

В дополнение к своим главным функциям модуль NAE обеспечивает межсетевое взаимодействие базовой сети IMS core через интерфейс Gm для авторизации и аутентификации только сетевых приложений. Кроме того, использование интерфейса Gm предполагается для поддержки файловой системы FFS [3].

Модуль NGC (Network Generic Communication) обеспечивает установление транспортных сессий и их последовательное прекращение в случае отсутствия подтверждения установленных ключей безопасности. Установление ключей безопасности осуществляется модулем безопасности NSEC и используется для формирования ключей конкретной сессии. Типовая сессия на уровне приложений между M2M устройством/M2M шлюзом и модулем NGC базируется на протоколе HTTP. В некоторых случаях сессия с данными о безопасности (secure data session) может базироваться на протоколе TLS-PSK.

Кроме того, модуль NGC:

- обеспечивает шифрование/интегральную защиту данных для устройств M2M и M2M шлюзов;
- устанавливает туннели безопасности сессий от M2M шлюзов и M2M устройств, если приложение требует установления туннеля безопасности (например, туннель между домовым шлюзом домовладения – абонента сети и одним из функциональных модулей базовой сети M2M);
- предоставляет средства для транспортировки сообщений между следующими элементами сети M2M: устройствами M2M, шлюзами M2M, функциональными модулями базовой сети M2M, приложениями M2M входящими в сетевой домен и домен приложений;
- идентифицирует всех адресатов, передающих сообщения модулю NGC на основе использования индивидуальных уникальных идентификаторов.

Модуль NRAR (Network Reachability, Addressing and Repository) обеспечивает:

установление соответствия между именами M2M устройства или M2M шлюза, или группы M2M устройств/M2M Gateways и установление сетевых адресов маршрутизации устройств M2M или M2M шлюзов (например, в случае использования сети GPRS каждое устройство M2M или M2M шлюз может иметь два адреса: IP адрес и MSISDN);

- установление статуса достижимости для присоединения устройств M2M или M2M шлюзов;

- получение запросов от других функциональных модулей и уведомление о доступности устройства M2M или получении устройством M2M нового адреса как следствие его мобильности, изменение совокупности приложений для устройств M2M согласно регистрируемой информации;
- получение другими модулями базовой сети M2M адресных материалов и статусов достижимости для присоединения устройств M2M или M2M шлюзов;
- создание групп M2M, стирание и составление списков устройств M2M и M2M шлюзов, входящих в соответствующие группы.

Модуль NSEC (Network Security) – обеспечивает безопасность сети M2M на уровне сетевого домена и домена приложений и выполняет:

- регистрацию устройств M2M на уровне сервисов через аутентификацию ключей об обслуживании на основе соглашений;
- управление обменом ключами обслуживания между устройствами M2M/M2M шлюзами и модулем NSEC;
- аутентификацию приложений до предоставления ими услуг;
- взаимодействие M2M сервера аутентификации (MAS) для получения данных об аутентификации, необходимых для выполнения аутентификации устройств M2M или M2M шлюзов и управления ключами обслуживания.

Варианты взаимодействия устройств M2M подразумевают их взаимодействие как с использованием базовой сети M2M и шлюзов M2M, так их взаимодействие без ее использования [4].

Адресация и идентификация устройств M2M при оказании услуг с использованием платформы IMS.

Каждая услуга M2M идентифицируется в базовой сети M2M [6], построенной на основе платформы IMS, при помощи идентификатора IMS услуг (ICSI). Приложения M2M домена приложений и приложения абонентских устройств M2M идентифицируются на основе идентификаторов IM приложений (IARI).

Для опознавания и регистрации аутентификации) и сохраняемую в подсистеме IMS Core базовой сети (например, для использования при процедуре регистрации устройства M2M). Также идентификатор IMPU используется базовой сетью M2M SC для запросов при присоединении и взаимодействии с устройством M2M.

Базовая сеть M2M SC использует подсистему IMS для регистрации сетевых приложений. Для этих целей базовая сеть M2M SC поддерживает взаимосвязи между модулями приложений M2M (используя их для приложений M2M), при этом каждому присваиваются свой идентификатор IMPU для идентификации и идентификатор IARI соответственно.

## 2.3 Особенности использования технологии NB-IoT, планы международных организаций по использованию радиочастотного спектра

Существующие сценарии использования (бизнес-кейсы) предназначены традиционно для двух сегментов применения технологии NB-IoT. Это, прежде всего, промышленный сегмент и потребительский сегмент рынка IoT/M2M, который может быть разделен еще на четыре [19-20]: бытовых домашних IoT-устройств (IoT Appliance); персональных устройств IoT (IoT Personal); решений IoT для общественных (публичных) нужд (IoT Public); промышленных решений IoT (IoT Industry).

Наиболее востребованными для применения технологии NB-IoT будут следующие бизнес-сегменты: электронное здоровье/E-Health; розничная торговля; безопасность и охрана; автомобили и логистические перевозки; энергетика и ЖКХ; промышленное производство; умный город; умный дом и другие.

Исходя из технических характеристик, покрытие для абонентских устройств NB-IoT будет иметь бюджет радиолинии, равный 164 дБ по сравнению с бюджетом для радиолинии GPRS, который составляет 144 дБ (TR 45.820), и с бюджетом для радиолинии LTE, составляющим 142.7 дБ (TR 36.888). Таким образом, технология NB-IoT будет иметь улучшенное покрытие (бюджет радиолинии на 20 дБ превышает, аналогичный бюджет для сотовых сетей стандартов GPRS и LTE).

Помимо улучшенного покрытия, базовая станция LTE для абонентских устройств NB-IoT будет иметь значительно большую ёмкость за счёт низких скоростей передачи у данных устройств. По расчётам компаний Neul и Huawei, а также партнёрского проекта 3GPP [6] одна макробазовая станция LTE с радиусом действия 1 км может обслуживать более 50 тысяч абонентских устройств NB-IoT. Ёмкости такой базовой станции будет достаточно для обслуживания потребителей в плотных городских условиях, когда на один квадратный километр приходится около 1500 домохозяйств, в каждом из которых будет 40 IoT-устройств. Однако следует отметить, что под таким большим числом обслуживаемых абонентских устройств понимаются не одновременно обслуживаемые устройства, а количество обслуживаемых абонентских устройств базовой станцией за один час в одном канале 180 кГц, при условии, что каждое устройство передаёт 100 байт информации. Зависимость количества обслуживаемых абонентских устройств в соте от радиуса соты, для различных уровней дополнительных потерь проникновения в здания, представлена на рисунке 7.7. При этом, даже при условии высоких потерь проникновения в здания, до 40 дБ, одна базовая станция LTE с радиусом действия 1 км может обслуживать до 45 тыс. абонентских устройств IoT в час [2].

Другим важным преимуществом абонентских устройств NB-IoT, по сравнению с обычными мобильными устройствами GSM/UMTS/LTE, будет значительно более длительный срок автономной работы. По данным 3GPP,

срок автономной работы абонентских устройств NB-IoT от аккумуляторной батареи ёмкостью 2500 мАч в идеальных теоретических условиях будет достигать 36 лет. Данный показатель рассчитан при условии, что абонентское устройство NB-IoT будет выходить на связь один раз в сутки для передачи не более 50 байт данных, а ослабление сигнала между антенной базовой станции и антенной IoT-устройства не превышает 144 дБ. При более частой передаче данных устройством NB-IoT до 200 байт каждые два часа и при более сильном ослаблении сигнала в радиоканале до 164 дБ срок автономной работы абонентских устройств NB-IoT составит менее 2 лет. В среднем модули NB-IoT смогут работать автономно от одной аккумуляторной батареи около 10 лет.

Следует отметить, что в данных расчётах не учитывается эффект саморазряда аккумуляторных батарей, который может существенно снизить время автономной работы IoT-устройства. Стоимость батарей с низким коэффициентом саморазряда может во много раз превышать стоимость самого IoT-устройства.

Учитывая требования к технологии NB-IoT по улучшенной (расширенной) зоне покрытия, развертывание сетей с технологией NB-IoT в полосах частот 700, 800 и 900 МГц будет являться основной стратегией использования спектра для IoT/M2M-приложений, поскольку эти диапазоны уже имеют достаточно развитую регуляторную базу использования спектра на международном, региональных и национальных уровнях управления спектром.

Вторым фактором, ускоряющим внедрение технологии NB-IoT в этих диапазонах, будет наличие лицензий (разрешений) на использование спектра операторов сетей доступа IoT/M2M. Для мобильных операторов, работающих в диапазонах GSM-900 или LTE-800/700, необходимы относительно небольшие вложения, чтобы быстро развернуть оборудование на основе технологии NB-IoT.

Диапазоны частот, специфицированные 3GPP для сетей LTE в полосе 694-790 МГц, входят в число диапазонов, определенных в Рекомендациях МСЭ-Р М.1036-4 для развития сетей мобильного беспроводного доступа 4G. Гармонизированное распределение частотных каналов в полосе 694-790 МГц для парного использования полос частот (FDD 2x30 МГц) и дополнительное непарное использование полос частот 738-758 МГц до четырех блоков по 5 МГц для режима поддержки дополнительных каналов вниз (SDL) в сетях LTE определено Решением ЕСС/DEC/(15)01[9].

Комитетом ЕСС СЕРТ подготовлен отчет ЕСС 242 «Изучение совместимости и совместного использования для узкополосных M2M-приложений в диапазоне 733-736/788-791 МГц», который содержит анализ совместного использования сетей радиодоступа «машина - машина» (M2M) в диапазоне 733-736 / 788-791 МГц и других радиослужб в соседних полосах. В целях удовлетворения национальных потребностей в спектре в отчете предложены альтернативные варианты совместного использования спектра репортажными станциями PMSE (Programme Making and Special

Events), станциями служб спасения PPDR (Public Protection and Disaster Relief) и сетями доступа M2M, а также сетями LTE (диапазоны B28 и B20) в полосе частот 700 МГц.

Кроме того, в отчете ЕСС 242 были сделаны следующие выводы по использованию спектра:

Особенности использования полосы «цифрового дивиденда» 790-862 МГц и частотного плана определены Решением ЕСС/DEC/(09)03 от 30 октября 2009г., которые включают:

- инверсный режим FDD (обратное использование полосы передачи и приема) для снижения влияния абонентских терминалов (АТ) на РЭС цифрового ТВ;

- требования разделения режимов FDD и TDD и использования разных частотных планов;

- необходимость определения размера частотных блоков для LTE;

- необходимость определения шага сетки частот в Плане (1 МГц или

2

МГц);

- введение защитной полосы FDD (между дуплексными полосами) – более 10 МГц (лучше 12 МГц);

- использование дополнительной фильтрации для развязки каналов DLUL (устранение перетекания мощности из-за близости дуплексных полос).

В соответствии с этим Решением ЕСС, гармонизированным европейским распределением каналов является использование двух полос 2x30 МГц с дуплексным разносом 11 МГц, основанном на использовании частотных блоков (каналов) шириной 5 МГц. Европейский подход к использованию полосы частот 790...862 МГц, как и поход МСЭ-Р, основан на парном использовании полос частот на основе частотного дуплекса FDD и реверсном принципе использования дуплексных полос, а также наличии защитного интервала шириной в 1 МГц (790-791 МГц).

Полоса частот, используемая LTE в линии вниз для режима FDD, находится ниже полосы линии вверх и начинается с частоты 791 МГц, а полоса FDD линии вверх соответственно 832 МГц.

Комитет по электронным коммуникациям (ЕСС) СЕРТ открыл в 2016 году в рабочей группе РТ1 новый исследовательский вопрос «M2M через мобильные сети», в рамках которого должно быть рассмотрено использование 9 -ти частотных диапазонов, специфицированных 3GPP для использования в сетях LTE в интересах NB-IoT и M2M: 700 МГц, 800 МГц, 900 МГц, 1800 МГц, 2100 МГц, 2300 МГц, 2600 МГц, 3400-3600 МГц и 3600-3800 МГц [10], что может существенно расширить области применения технологии NB-IoT.

Таким образом, появление на рынке сетей LTE Advanced с технологией узкополосной передачей данных для Интернета вещей (NB-IoT) существенно повысит конкуренцию на рынке беспроводных технологий Интернета вещей по отношению набирающим популярность UNB, LoRa, LPWAN и другим технологиям, использующим нелицензируемые полосы частот.

Технология NB-IoT будет обладать рядом преимуществ по скорости, массовости производства и, как следствие, дешевизне. Возможность использовать для NB-IoT уже освоенные лицензируемые диапазоны частот для операторов мобильных сетей 4G, а также уже развернутое сетевое оборудование приведет к интенсивному развитию сектора IoT в структуре бизнеса мобильных операторов. Для внедрения технологии NB-IoT на казахстанском рынке в ближайшее время потребуются внесение изменений в нормативно-правовую базу использования радиочастотного спектра, так и правил применения нового оборудования на сетях связи общего пользования

#### **2.4 Проектирование локальные сети Интернета вещей и M2M на базе сетей малого радиуса действия в ЖК Манхэттен**

Сетевой базой для реализации концепции Интернета вещей являются самоорганизующиеся сети, обеспечивающие автоматический выбор топологии сети, автоматическое подключение новых устройств к сети, автоматический выбор маршрутов передачи пакетов данных в сети без участия человека. Наиболее широкое распространение среди таких сетей получили беспроводные персональные сети WPAN (Wireless Personal Area Networks) или беспроводные сенсорные сети.

Беспроводная персональная вычислительная сеть представляет локальную сеть с малым радиусом действия, обычно не превышающим 10-20 м. Характерной особенностью сетей WPAN является их невысокое энергопотребление. Поэтому использование в радиоустройствах автономных источников электропитания позволяет отнести эти сети к мобильным средствам связи с ограниченным радиусом действия. Сети WPAN используются в основном внутри помещений для связи различных бытовых и промышленных устройств, включая компьютерную и оргтехнику, системы «умный дом» и «умный офис», в связи с этим в нашей работе мы проектируем IoT в ЖК Манхэттен.

Для организации беспроводных персональных сетей WPAN Институтом инженеров электротехники и электроники IEEE разработано семейство стандартов IEEE 802.15, которые описывают два нижних уровня протоколов модели взаимодействия открытых систем (Open System Interconnection, OSI): физический (Physical Layer, PHY) и уровень доступа к среде передачи (Medium Access Control, MAC).

Одним из первых стандартов беспроводных персональных сетей, стал стандарт IEEE 802.15.1, в основе которого лежала технология Bluetooth. Сети стандарта IEEE 802.15.1 (Bluetooth) используются для обмена информацией между такими устройствами, как персональные компьютеры, мобильные устройства, принтеры, цифровые фотоаппараты и беспроводные наушники.

Однако для некоторых устройств, работающих в сетях WPAN, оказалось недостаточно скоростей, обеспечиваемых технологией Bluetooth, возникла потребность в разработке стандарта, позволяющего создавать беспроводной



канал передачи данных с пропускной способностью в десятки сотни мегабит в секунду. Такие стандарты образовали семейство стандартов IEEE 802.15.3, на базе которых строятся сверхширокополосные сети UWB (Ultra-Wide Band). Данные сети отлично подходят для передачи больших объемов информации (голоса, данных, видео) с высокой скоростью.

Для устройств, которые не нуждаются в высоких скоростях передачи информации, однако, требуют длительных сроков автономной работы от аккумуляторной батареи и низкой стоимости таких, как разнообразные датчики, системы сбора информации и управления, разработан стандарт IEEE 802.15.4 низкоскоростных сетей WPAN.

В основе технологии Bluetooth лежит объединение устройств в пикосети, которые представляют собой беспроводные сети передачи данных, состоящие из небольшого количества устройств, находящихся друг от друга на небольших расстояниях, как правило, не превышающих 10 м.

Элементарная пикосеть – это два взаимодействующих устройства с модулями Bluetooth, одно из которых называется главный (master), а другое ведомый (slave). Причем, главное устройство выполняет инициацию и поддержку функционирования соединения. Максимальное количество соединений для одного главного устройства равно семи, а суммарная скорость передачи данных не превышает максимальной скорости для данной версии технологии. Функции главного и ведомого жестко не фиксируются за устройствами и в зависимости от загрузки могут меняться. Устройство в разных соединениях может выполнять разные роли, а также может быть ведомым для разных главных.

Технология Bluetooth использует частотный диапазон 2,4...2,4835 ГГц, свободный от лицензирования. В радиотракте Bluetooth применяется метод расширения спектра со скачкообразной перестройкой частоты (Frequency Hopping Spread Spectrum, FHSS), который обеспечивает устойчивость системы связи к широкополосным помехам. Согласно алгоритму, FHSS несущая частота сигнала Bluetooth скачкообразно меняется 1600 раз в секунду, при этом выделяется 79 рабочих каналов шириной 1 МГц. Последовательность переключения между частотами для каждого соединения является псевдослучайной, и она известна только передатчику и приемнику, которые каждые 625 мкс (один временной слот) синхронно перестраиваются с одной несущей частоты на другую. Таким образом, если рядом работают несколько пар «приемник-передатчик», то они не мешают друг другу. Этот алгоритм является также составной частью системы защиты конфиденциальности передаваемой информации: переход происходит по псевдослучайному алгоритму и определяется отдельно для каждого соединения.

В технологии Bluetooth предусмотрено временное разделение дуплексных каналов (Time Division Duplex, TDD). Главное устройство передает пакеты данных в нечетные временные интервалы, а ведомое устройство – в четные временные интервалы. Пакеты в зависимости от длины могут занимать до пяти временных интервалов, при этом частота канала не меняется до окончания передачи пакета.

Технология Bluetooth поддерживает асинхронный канал для передачи данных и до трех синхронных каналов для передачи голоса, также поддерживается одновременная асинхронная передача данных и синхронная передача голоса. Скорость передачи голосовых данных в синхронном канале равна 64 кбит/с в каждом направлении.

При передаче цифровых данных и аудиосигнала используются различные схемы кодирования, так как цифровые данные при потере пакета информации могут быть переданы повторно, аудиосигнал, как правило, повторно не передается.

Модули с поддержкой первых версий спецификаций Bluetooth 1.0 (1998 г.) и 1.0 B (1999 г.), выпускаемые различными производителями, имели плохую совместимость друг с другом. В этих версиях спецификаций была обязательной передача адреса устройства (Bluetooth device address, BD\_ADDR) на этапе установления связи, что делало невозможной реализацию анонимности соединения устройств на протокольном уровне, и было основным недостатком данной спецификации. Максимальная скорость передачи данных через соединение Bluetooth составляла 721 кбит/с.

В спецификации Bluetooth 1.1, которая вышла в 2002 г., было исправлено множество ошибок, найденных в версиях 1.0 и 1.0 B; была добавлена поддержка нешифрованных каналов и индикация уровня мощности принимаемого сигнала (Received Signal Strength Indication, RSSI).

В версии Bluetooth 1.2, вышедшей в 2003 г., была добавлена технология адаптивной перестройки рабочей частоты AFH (Adaptive Frequency Hopping) для борьбы с электромагнитной интерференцией, возникающей при совместном использовании сетей Bluetooth и беспроводных локальных сетей, таких, как Wi-Fi, работающих в том же частотном диапазоне. В данной версии Bluetooth была добавлена технология расширенного синхронного канала, ориентированного на соединение eSCO (Extended Synchronous Connection Oriented), которая улучшила качество передачи голоса путём повторения повреждённых пакетов. Для подключения модулей Bluetooth к внешним устройствам была добавлена поддержка трёхпроводного интерфейса UART (Universal Asynchronous Receiver-Transmitter).

Версия 2.0 спецификации Bluetooth появилась в ноябре 2004 г. Она имеет обратную совместимость с предыдущими версиями 1.x. Основным нововведением стала поддержка более высокой скорости передачи данных (до 2100 кбит/с в асимметричном режиме и 1430 кбит/с в симметричном). Максимальный размер сети был увеличен с 8 до 256 устройств, также был добавлен механизм контроля качества услуги (Quality of Service, QoS), который обеспечивает взаимодействие устройств с минимальными задержками [6].

В августе 2008 г. была выпущена версия Bluetooth 2.1. В эту версию добавлена технология энергосбережения (Sniff Subrating), которая позволяет в пять раз снизить потребление энергии и тем самым увеличить время автономной работы устройства Bluetooth. В Bluetooth 2.1 повышен уровень

защиты данных и упрощена процедура распознавания и соединения устройств Bluetooth.

В 2009 г. выпущена версия Bluetooth 3.0, поддерживающая скорость передачи данных до 24 Мбит/с, которая достигается благодаря применению двух радиомодулей: обычного модуля Bluetooth, обеспечивающего скорость передачи данных 2,1 Мбит/с, и дополнительного модуля, работающего по протоколу 802.11 и обеспечивающего скорость передачи данных до 24 Мбит/с. Выбор модуля для передачи данных зависит от размера передаваемого файла. Небольшие файлы передаются по медленному каналу,

В июне 2010 г. выпущена версия Bluetooth 4.0. Основной задачей новой спецификации было устранение высокого энергопотребления в версии Bluetooth 3.0. Спецификация Bluetooth 4.0 включает в себя протоколы классической низкоскоростной технологии Bluetooth, основанной на спецификациях предыдущих версий Bluetooth, протоколы высокоскоростной технологии Bluetooth, основанной на технологии Wi-Fi, и протоколы технологии Bluetooth с низким энергопотреблением. Низкое энергопотребление достигается благодаря использованию специального алгоритма работы, согласно которому передатчик включается только на время отправки данных. Таким образом, обеспечивается возможность работы устройства Bluetooth в течение нескольких лет от одной батарейки типа CR2032. Модули Bluetooth 4.0 могут эффективно использоваться как в миниатюрных электронных датчиках и сенсорах, так и в различных смартфонах и ПК.

### 2.3.1 Использование сетей радиосвязи для создания сетевой доступа M2M. Стандарты IEEE 802.15.3. и IEEE 802.15.4., ZigBee, Z-wave, LORA

Стандарт IEEE 802.15.3 описывает беспроводную сеть, в которой несколько независимых устройств могут непосредственно взаимодействовать друг с другом. Размеры такой сети, как правило, не превышают 10 м. Основные требования к ней – высокая скорость передачи данных, простая инфраструктура, лёгкость установления соединения и подключения к сети, средства защиты данных и предоставление для определённых типов трафика гарантированного качества обслуживания. Для работы таких персональных сетей выделен частотный диапазон 2400...2483,5 МГц. Стандарт предусматривает пять допустимых скоростей передачи данных. Скорость 22 Мбит/с является базовой, её обязаны поддерживать все устройства стандарта IEEE 802.15.3.

Стандартом IEEE 802.15.3 предусмотрено два частотных плана: 1) режим высокой плотности абонентских устройств, в котором используется четыре частотных канала, 2) режим совместимости с сетью стандарта IEEE 802.11b, в котором используется три частотных канала, чьи центральные частоты совпадают с частотами стандарта IEEE 802.11b. Общее количество частотных каналов с учетом двух частотных планов равно пяти, полоса пропускания каждого канала равна 15 МГц.

В 2009 г. вышла новая версия стандарта высокоскоростных беспроводных персональных сетей IEEE 802.15.3с, использующих миллиметровые радиоволны в диапазоне 57...66 ГГц [10]. Отличительной особенностью данного диапазона частот является сильное затухание радиоволн в атмосферных газах и гидрометеорах, по этой причине его можно использовать только для связи на небольших расстояниях, обычно до 10 м. Основным достоинством диапазона является сверх широкая доступная полоса частот. Малая длина волны существенно снижает габариты антенных систем и, как следствие, самих приемо-передающих устройств. Также использование данного частотного диапазона позволяет устранить проблему интерференции между различными источниками сигнала из-за сильного ослабления и решить проблему повторного использования частот. Именно поэтому во многих странах данный диапазон является безлицензионным. В Казахстане, диапазон частот 58,25...63,25 ГГц выделен для радиоэлектронных средств фиксированной службы.

Стандарт IEEE 802.15.3с обеспечивает скорость передачи данных до 5 Гбит/с. В стандарт добавлена возможность работы в режиме формирования диаграммы направленности (Beamforming) передатчика. На MAC-уровне появилась опция агрегации различных входящих данных в единые пакеты для повышения эффективности системы связи.

На физическом уровне описано три режима работы:

- режим передачи на одной несущей (Single Carrier, SC), оптимизированный для минимизации энергопотребления и сложности систем;
- режим высокоскоростного интерфейса (High-Speed Interface, HSI), предназначенного для двунаправленной связи с минимальными задержками;
- режим аудио/видео (Audio/Video, AV) для трансляции потоков несжатых данных видео и аудио высокого разрешения.

Другим конкурирующим стандартом высокоскоростных беспроводных персональных сетей является стандарт WHDI (Wireless Home Digital Interface - беспроводной домашний цифровой интерфейс). Стандарт был разработан израильской компанией Amimon и продвигается на рынке консорциумом WHDI, в который входят такие производители бытовой электроники, как Hitachi, LG Electronics, Motorola, Samsung, Sharp и Sony.

Сети WHDI работают в нелицензируемом диапазоне частот 5,1...5,9 ГГц, передача сигнала осуществляется в канале шириной 40 МГц. Пропускная способность 3 Гбит/с в сетях стандарта WHDI обеспечивает беспроводную передачу несжатого видеосигнала высокого разрешения и звука.

Маломощные, низкоскоростные беспроводные персональные сети введены стандартом IEEE 802.15.4. Этот стандарт, утвержденный в 2003 г., ориентирован на создание маломощных беспроводных сетей с максимальной дальностью действия от 10 до 100 м. Стандарт определяет следующие скорости передачи данных: 250, 100, 40 и 20 кбит/с - и позволяет работать в трех возможных нелицензируемых радиочастотных диапазонах:

- 868,0...868,6 МГц используется в Европе;
- 902...928 МГц; используется в Северной Америке;

- 2400...2483,5 МГц; используется во всем мире, включая Казахстан. В стандарте IEEE 802.15.4 выделяется два вида узлов беспроводной сети:

- устройства с ограниченными функциями RFD (Reduced-Function Device), осуществляющие сбор информации в некоторой окрестности точки своего размещения;

- полнофункциональные устройства FFD (Full-Function Device), выполняющие как ретрансляцию пакетов данных, так и сбор информации.

Сети стандарта IEEE 802.15.4 могут быть построены как по одноранговой (равноправной) структуре, так и по топологии «звезда». В каждой сети должно быть, по меньшей мере, одно полнофункциональное устройство для работы в качестве координатора. Стандарт IEEE 802.15.4 является основой для более высокоуровневых протоколов (ZigBee, 6LoWPAN, DigiMesh и др).

Технология ZigBee. В 2004 г. на основе стандарта IEEE 802.15 Альянс ZigBee разработал спецификацию протоколов сетевого и прикладного уровня ZigBee. Альянс ZigBee объединяет более 180 фирм, работающих совместно над продвижением стандартов, стека протоколов и прикладных профилей для потребительского и промышленного сектора экономики. Прикладные профили ориентированы, в частности, на автоматизацию зданий, промышленный мониторинг, вентиляцию и кондиционирование, работу с датчиками. Спецификация ZigBee описывает построение сети, вопросы безопасности, прикладное программное обеспечение.

Устройства сети ZigBee благодаря встроенному программному обеспечению обладают способностью при включении питания сами находить друг друга и формировать сеть, а в случае выхода из строя какого-либо из узлов могут устанавливать новые маршруты для передачи сообщений [4].

Сеть ZigBee включает три типа логических устройств: координатор ZigBee, маршрутизатор ZigBee и оконечное устройство ZigBee. В функции координатора ZigBee входит сканирование частотных каналов для нахождения свободного канала и создания сети, формирование идентификатора сети (PAN ID), подключение новых сетевых устройств (маршрутизаторов и оконечных узлов), маршрутизация и буферизация данных для спящих оконечных узлов. В одной сети ZigBee должен присутствовать только один координатор. В функции маршрутизатора ZigBee входит ретрансляция пакетов, маршрутизация и буферизация данных для спящих оконечных узлов. Оконечные узлы ZigBee выполняют только прикладные действия (сбор информации и управление удаленным объектом) и не осуществляют ретрансляцию данных.

Протоколы ZigBee могут быть использованы как для реализации простых соединений «точка-точка» и «звезда», так и для образования сложных сетей с топологиями «дерево» и «ячеистая сеть»

Дальность уверенной передачи радиосигнала узлов ZigBee сети зависит от многих параметров (в первую очередь – от чувствительности приемника и мощности передатчика), но в среднем расстояние между узлами сети Zigbee

на открытом пространстве составляет сотни, а в помещении – десятки метров

Все устройства, работающие в сети ZigBee любой топологии, снабжаются уникальными 16- или 64-битными адресами, которые могут использоваться для прямых коммуникаций в пределах персональной сети (Personal Area Networks, PAN). Назначение устройствам уникальных адресов осуществляет единый координатор сети при её организации.

Технология ZigBee позволяет в рамках одной сети решать множество различных прикладных задач, не связанных друг с другом. Для возможности разделения пакетов данных по различным приложениям, для которых они предназначены, используются 8-битные идентификаторы приложений Endpoint ID.

– Для обеспечения полной совместимости устройств разных производителей и их взаимодействия в едином распределённом приложении, в технологии ZigBee применяется понятие профилей, которые различаются в пакетах данных с помощью 16-битного идентификатора. Профиль описывает ряд технических параметров, соглашений о структурах данных и форматах сообщений, которых жестко должны придерживаться изготовители, чтобы их изделия были совместимы по этому профилю. Текущий список профилей приложений, опубликованных альянсом ZigBee, включает: домашнюю автоматизацию, автоматизацию коммерческих зданий, розничную торговлю, «умные» энергосети, телекоммуникационные услуги, здравоохранение, дистанционное управление, устройства ввода информации, устройства управления освещением.

*Технология Z-Wave* использует нелицензируемые частоты ниже 1 ГГц, различающиеся в зависимости от региона. В США используется частота 908,42 МГц, в Европе — 868,42 МГц, в России для технологии Z-Wave в соответствии с решением ГКРЧ № 08-24-01-001 от 28.04.2008 выделен частотный диапазон 868,7...869,2 МГц.

Скорость передачи данных в сети Z-wave зависит от используемого оборудования и может достигать 100 кбит/с. Технология предназначена для передачи управляющих команд с малыми задержками

(например, включить/выключить прибор или изменить яркость освещения). Для потоковой передачи данных технология Z-Wave не подходит. Предельная дальность связи между двумя напрямую взаимодействующими устройствами Z-Wave составляет от 10 до 30 м (в зависимости от окружающей обстановки) [6].

Технология Z-Wave имеет функцию подтверждения доставки пакета - если команда не достигла получателя, то устройство выполняет повторную отправку.

*Сеть Z-Wave* использует ячеистую топологию, каждое устройство в сети Z-Wave является как приемником, так и передатчиком. Благодаря этому увеличивается надежность сети - при выходе из строя одного устройства сигнал пойдёт через соседнее, а зона покрытия расширяется простым добавлением новых устройств, которые могут работать в качестве

ретрансляторов сигнала, передавая сигнал по цепочке. В сети Z-Wave не нужны дополнительные повторители и усилители сигнала, достаточно, чтобы любое устройство сети Z-Wave находилось в радиусе действия соседнего устройства.

Сеть Z-Wave состоит из узлов двух различных типов:

- управляющие узлы (контроллеры), которые осуществляют маршрутизацию в сети и обеспечивают взаимодействие с другими сетями;
- исполнительные узлы, которые могут посылать, принимать и исполнять команды, но не имеют функции маршрутизации; в то же время исполнительные узлы могут работать в сети Z-Wave как ретрансляторы сигнала.

Оба типа узлов могут быть использованы в различных устройствах. Максимальное количество узлов сети, определяемое технологией Z-Wave, составляет 232 узла. Управляющие и исполнительные узлы, в зависимости от назначения и применения, бывают разных видов. Для идентификации устройств в сети, а также различения сетей Z-Wave существуют идентификаторы Network ID (называемый также Home ID) и Node ID.

## **2.5 Выбор оборудование для проектирования IoT в ЖК Манхэттен**

Система BreezeMAX™, новейшая разработка компании Alvarion поддерживающая передовую платформу WiMAX. Используя современную OFDM технологию и адаптивную модуляцию (до 64QAM) система работает в условиях близких к отсутствию прямой видимости (NLOS). Высокая спектральная эффективность системы BreezeMAX™ позволяет операторам начать строить сети WiMAX уже сегодня. Работая в диапазоне частот 3.5 ГГц, BreezeMAX™ выполняет требования пользователей иметь следующее поколение рентабельной BWA системы с платформой, обеспечивающей выполнение стандартов WiMAX: IEEE 802.16 и HiperMAN. Мы в своей работе для проектирование IoT в ЖК Манхэттен, выбрали системы BreezeMAX™.

Особенности системы BreezeMAX (рисунок 2.4):

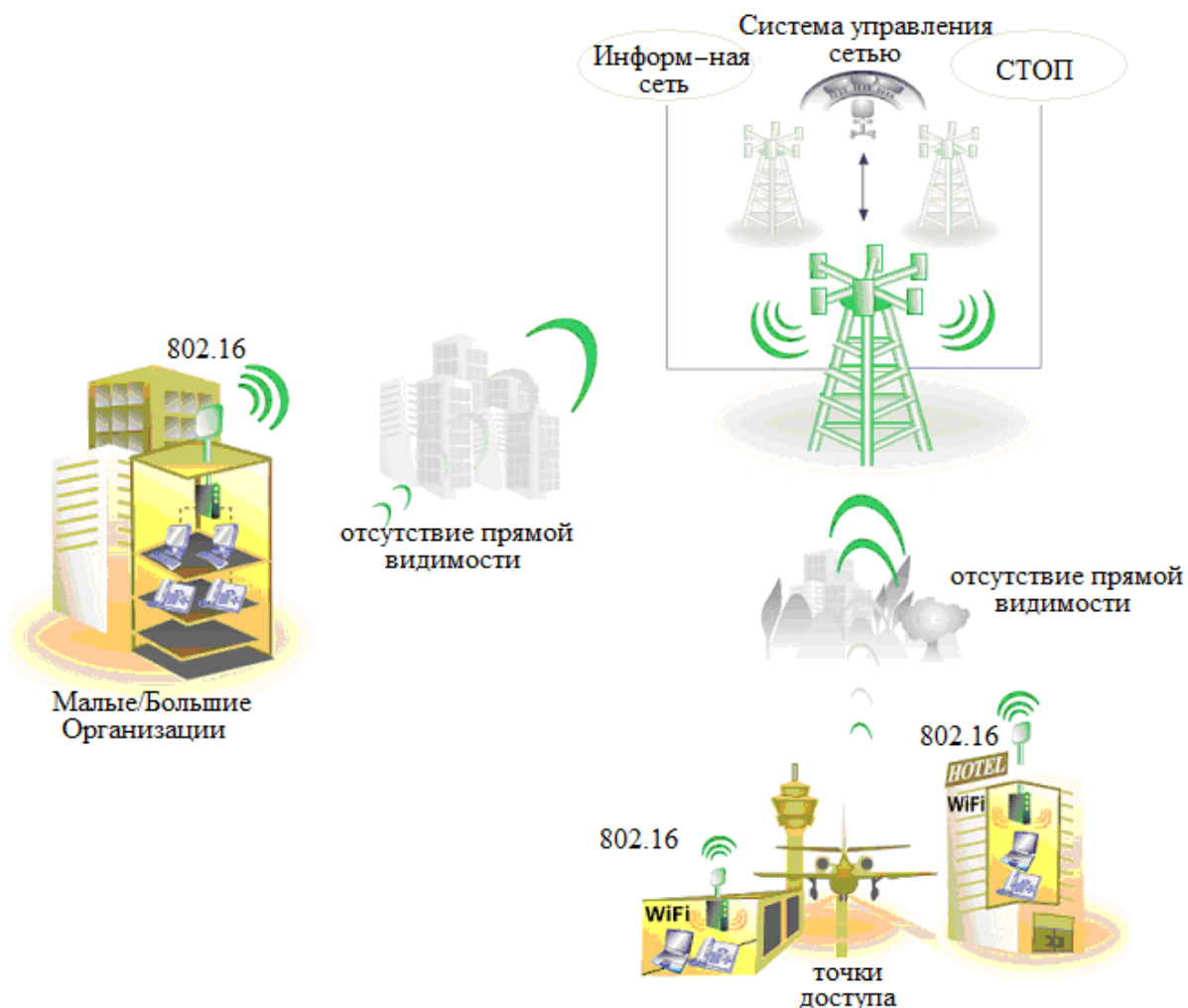


Рисунок 2.4 – Широкополосный беспроводный доступ IoT

- предназначена для различных рынков - подходит для обслуживания пользователей в жилом секторе, бизнес пользователей, MDU/MTU, горячих точек, Backhauls и организации беспроводных приложений домашних сетей;
- низкая себестоимость - поддерживая простую инсталляцию и «оплату по мере роста»;
- система операторского класса - высокая производительность и доступность, избыточность компонентов, гибкая система управления сетью);
- масштабируемая конфигурация оборудования Базовой станции - Базовая станция на основе шасси (High density) наиболее подходит для крупномасштабных развертываний в городских и пригородных областях. Миниатюрная Базовая станция является идеальным и рентабельным решением для сельской местности и регионов с низкой плотность населения;
- высокая производительность и пропускная способность - полнодуплексные и многоканальные функциональные возможности базовой станции позволяют одиночной базовой станции поддерживать очень большое число абонентов;



- NLOS охват - OFDM модуляция позволяет увеличить производительность в условиях близким к отсутствию прямой видимости;

- система управления AlvariSTAR - NMS платформа операторского класса, которая поддерживает полные функциональные возможности 2.3

### Основные принципы и особенности оборудования BreezeMAX

Система BreezeMAX™, новейшая разработка компании Alvarion поддерживающая передовую платформу WiMAX. Используя современную OFDM технологию и адаптивную модуляцию (до 64QAM) система работает в условиях близких к отсутствию прямой видимости (NLOS). Высокая спектральная эффективность системы BreezeMAX™ позволяет операторам начать строить сети WiMAX уже сегодня. Работая в диапазоне частот 3.5 ГГц, BreezeMAX™ выполняет требования пользователей иметь следующее поколение рентабельной BWA системы с платформой, обеспечивающей выполнение стандартов WiMAX: IEEE 802.16 и HiperMAN (рисунок 2.3).

Основные WiMAX архитектура - IEEE 802.16 и ETSI HiperMAN. Предназначена для различных рынков - подходит для обслуживания пользователей в жилом секторе, бизнес пользователей, MDU/MTU, горячих точек, Backhuls и организации беспроводных приложений домашних сетей.

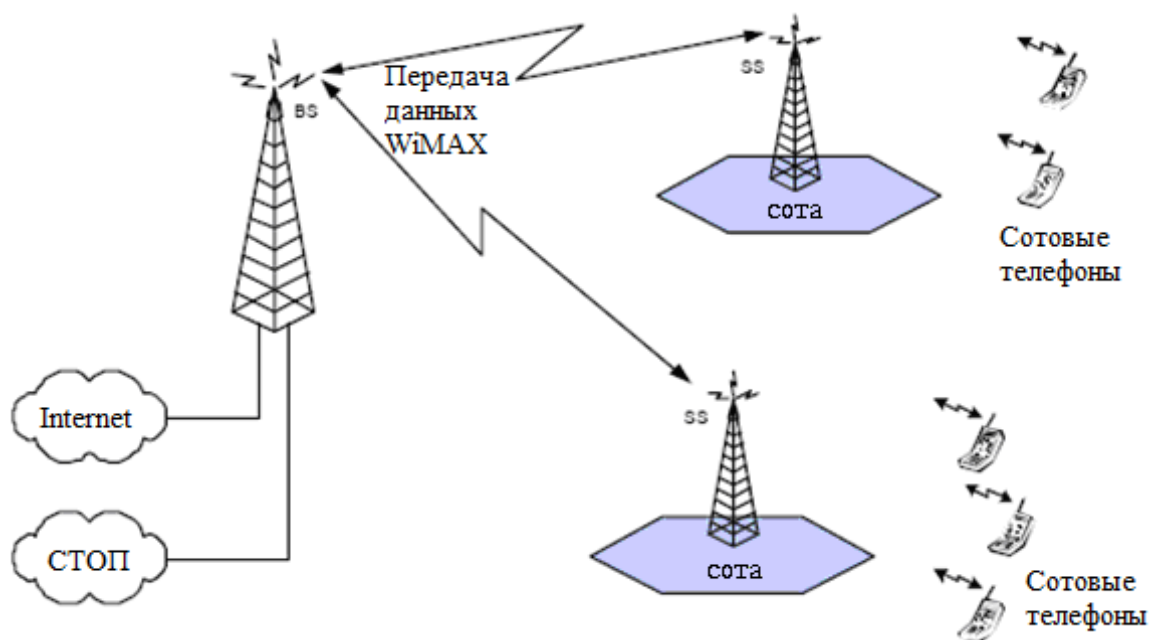


Рисунок 2.5 – Организация IoT в ЖК Манхэттен

Низкая себестоимость, поддерживает простую инсталляцию и «оплату по мере роста». Система операторского класса, высокая производительность и доступность, избыточность компонентов, гибкая система управления сетью

Масштабируемая конфигурация оборудования базовой станции - Базовая станция на основе шасси (High density) наиболее подходит для крупномасштабных развертываний в городских и пригородных областях.

Миниатюрная Базовая станция является идеальным и рентабельным решением для сельской местности и регионов с низкой плотностью населения

Высокая производительность и пропускная способность - Полнодуплексные и многоканальные функциональные возможности базовой станции позволяют одиночной базовой станции поддерживать очень большое число абонентов.

NLOS охват - OFDM модуляция позволяет увеличить производительность в условиях близким к отсутствию прямой видимости

Технология адаптивной модуляции. Система управления AlvariSTAR - NMS платформа операторского класса, которая поддерживает полные функциональные возможности FCAPS

Оборудование базовой станции BreezeMAX доступно в двух основных конфигурациях: Базовая станция High Density для развертываний крупного масштаба в городах и пригородных зонах и миниатюрная базовая станция для сельских районов и областей с низкой плотностью населения

Таблица 2.1 Компоненты базовой станции

Тип продукта	Имя продукта	Описание продукта
Для крупно-масштабных развертываний (город, пригород)	BMAX-BST-SH	BreezeMAX 3500 base station shelf
	BMAX-BST-NPU	BreezeMAX 3500 base station network processor unit
	BMAX-BST-AU-IDU-2CH	BreezeMAX 3500 base station access unit interface module
	BMAX-BST-PSU	BreezeMAX 3500 base station power supply unit
	BMAX-BST-PIU	BreezeMAX 3500 base station power interface unit
Миниатюрная (для сельских местностей)	BMAX-MBST-IDU-2CH-AC	BreezeMAX 3500 micro base station indoor unit, AC power
	BMAX-MBST-IDU-2CH-DC	BreezeMAX 3500 micro base station indoor unit, DC power

Платформа BreezeMAX предлагает несколько типов эффективного по стоимости оборудования конечного пользователя, чтобы обеспечивать операторов гибкостью в обслуживании разнообразных пользователей в жилом и бизнес секторах (таблица 2.2).

Таблица 2.2 Компоненты абонентской станции

Продукта	Имя продукта	Описание продукта
CPE Indoor (внутренние)	BMAX-CPE-IDU-1D	BreezeMAX 3500 broadband data CPE indoor module with one 10/100 BaseT
	BMAX-CPE-IDU-VG-1D1V	BreezeMAX 3500 broadband voice gateway CPE indoor module with one 10/100 BaseT data port + one RJ11
	BMAX-CPE-IDU-VG-4D2V	BreezeMAX 3500 broadband voice gateway CPE indoor module with four 10/100 BaseT data ports + two RJ11
	BMAX-CPE-IDU-NG-4D1WLAN	BreezeMAX 3500 networking gateway CPE indoor module with four 10/100 BaseT data ports + one 802.11b/g
CPE Outdoor (наружные)	BMAX-CPE-ODU-AV-3.5	BreezeMAX 3500 subscriber outdoor radio unit with integrated vertical antenna, frequency band 3.5a+b
	BMAX-CPE-ODU-AH-3.5	BreezeMAX 3500 subscriber outdoor radio unit with integrated horizontal antenna, frequency band 3.5a+b
	BMAX-CPE-ODU-E-3.5	BreezeMAX 3500 subscriber outdoor radio unit with connector for external antenna,

### 2.5.1 Базовая станция BreezeMAX

Система BreezeMAX, новейшая разработка компании Alvarion поддерживающая передовую платформу WiMAX. На рисунке 2.4 показана типовая схема WiMAX.

Используя современную OFDM технологию и адаптивную модуляцию (до 64QAM) система работает в условиях близких к отсутствию прямой видимости.

Работая в диапазоне частот 3.5 ГГц, BreezeMAX™ выполняет требования пользователей иметь следующее поколение рентабельной BWA системы с платформой, обеспечивающей выполнение стандартов WiMAX: IEEE 802.16 и HiperMAN.

Применены секторные антенны. Количество секторов может меняться. Интерфейс Ethernet 10/100 Base TX на каждом внутреннем модуле.

С платформой BreezeMAX™ предлагаются несколько вариантов оборудования конечного пользователя, которые позволяют операторам эффективно обслуживать разнообразных пользователей в деловых и жилых секторах [6].

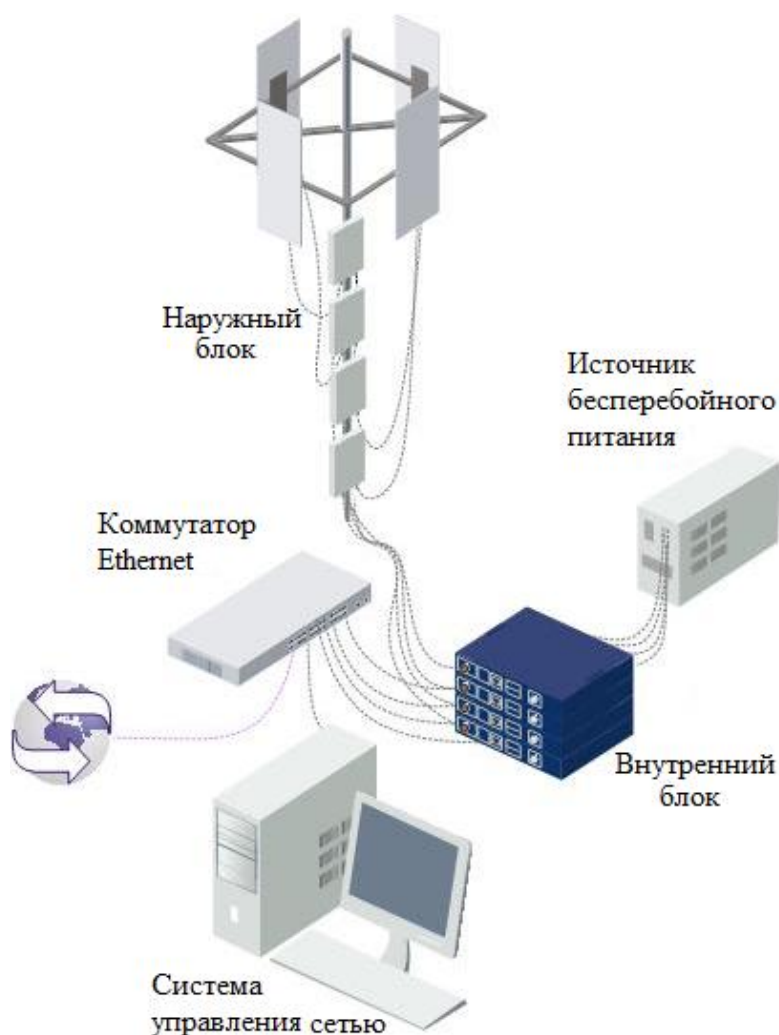


Рисунок 2.6 – Схема базовой станции WiMAX

Абонентское оборудование BreezeMAX™ основано на разработке с высокой степенью интеграции, которая обеспечивает высокую надежность и служит эффективной платформой для большого числа сервисов (рисунок 2.5).

Система BreezeMAX™ обеспечивает своих абонентов высокоскоростным доступом, со скоростью передачи данных до 12,7 Мбит/с по 3.5 МГц каналам.

Абонентское оборудование BreezeMAX™ поддерживают следующие основные приложения:

Широкополосные данные плюс голос, организация домашних сетей и транспортные соединения для горячих точек.

Абонентское оборудование BreezeMAX™ состоит из внутреннего и наружного модулей [8].

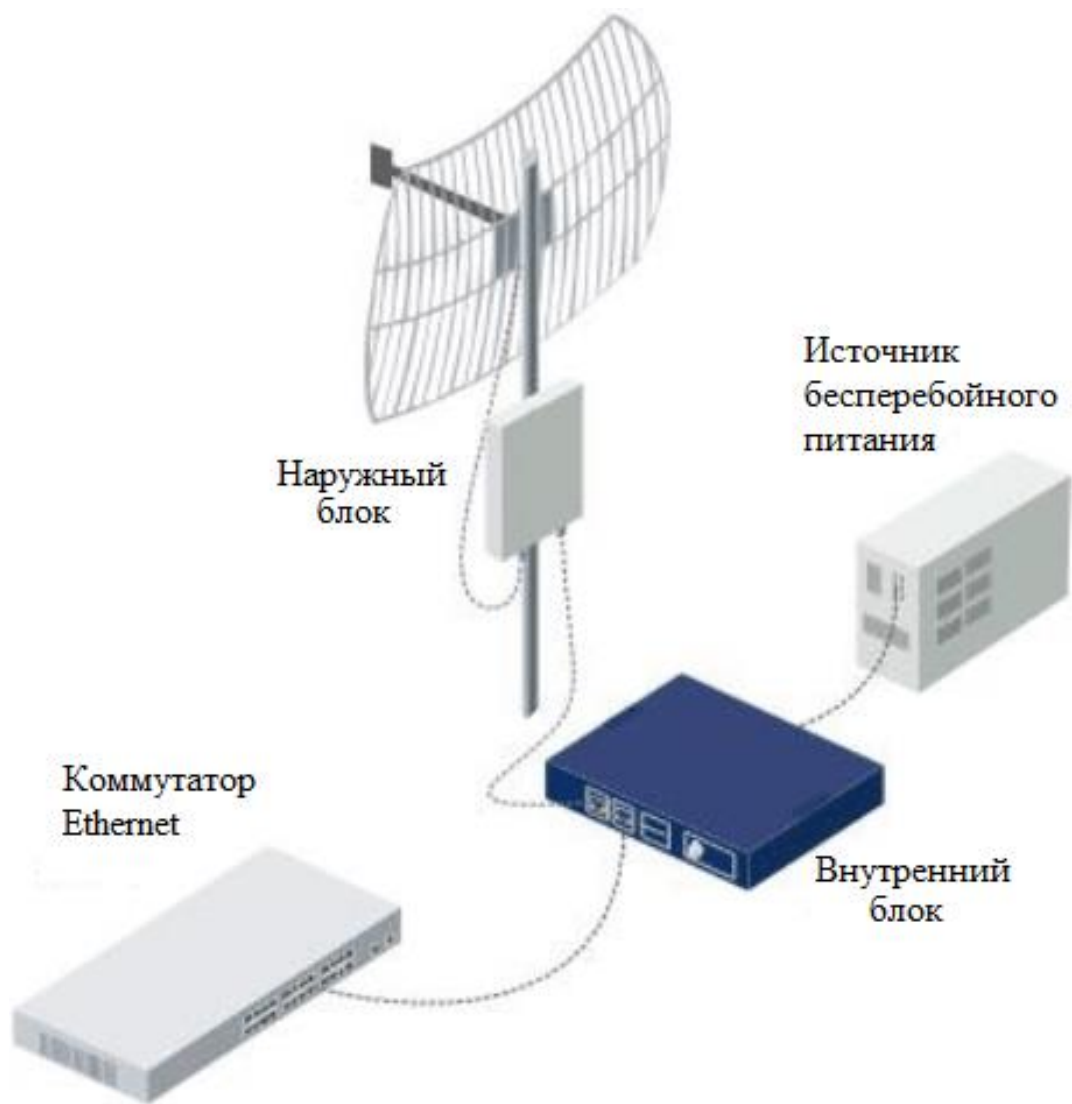


Рисунок 2.7 – Типовая схема абонентской станции WiMAX

Наружный модуль содержит все активные компоненты и плоскую интегрированную антенну с высоким усилением. Внутренний модуль соединяется с наружным через Ethernet кабель 5 категории. Через этот кабель передаются Ethernet данные, сигналы контроля состояния, управления и сброса от внутреннего модуля, а также питание (54В постоянного тока) к наружного модуля.

### 2.5.2 Разработка модели и исследование вероятности связности БСС при неравномерном распределении

Как было отмечено выше, во многих практических задачах распределение узлов сети отличается от пуассоновского поля (рис. 2.8).

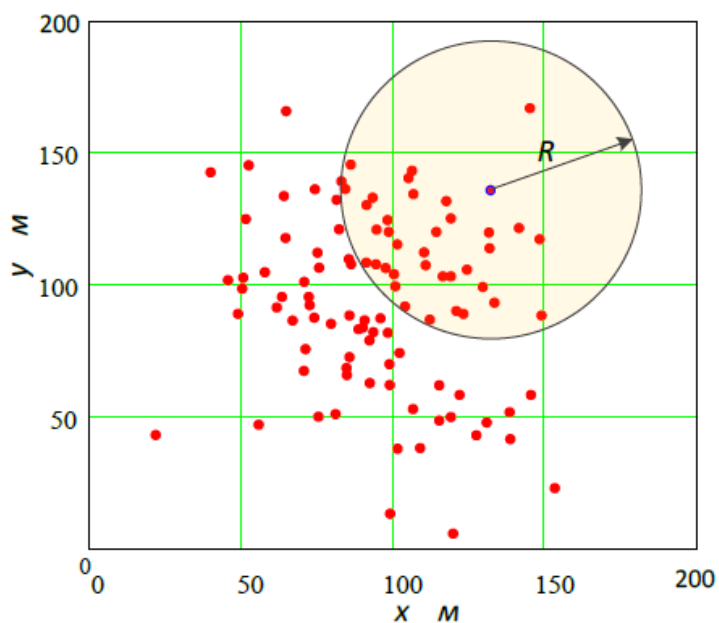


Рисунок 2.8 – Графическое представление аналитической модели БСС (гауссово поле)

В общем случае, оно может быть унимодальным или мультимодальным с областями высокой и малой плотности узлов. Для исследования свойств поля отличного от пуассоновского, рассмотрим сеть, образованную узлами, размещенными в области обслуживания по нормальному закону, т. е. образующими гауссово поле точек на плоскости. Данная модель, в общем случае, может быть использована при неравномерном распределении узлов сети в рассматриваемой зоне обслуживания.

Полагаем, что плотность узлов в каждой точке поверхности является случайной величиной и задается случайными, независимыми координатами  $x$  и  $y$ . Тогда, функция плотности вероятности будет определяться совместной функцией распределения случайных  $x$  и  $y$  [6].

## 3 Расчёт и моделирование беспроводной сенсорной сети в ЖК Манхэттен

### 3.1 Программно-графическое представление сети

В графическом редакторе OMNET++ беспроводная сенсорная сеть Castalia представлена следующим образом (в Приложении А приведен код, описывающий БСС):

- SN - имя сети (используется для моделирования);
- wireless Channel - модуль беспроводного канала;
- node[numNodes] - модуль элементов сети;
- physical Process [num Physical Processes] – модуль физических процессов.

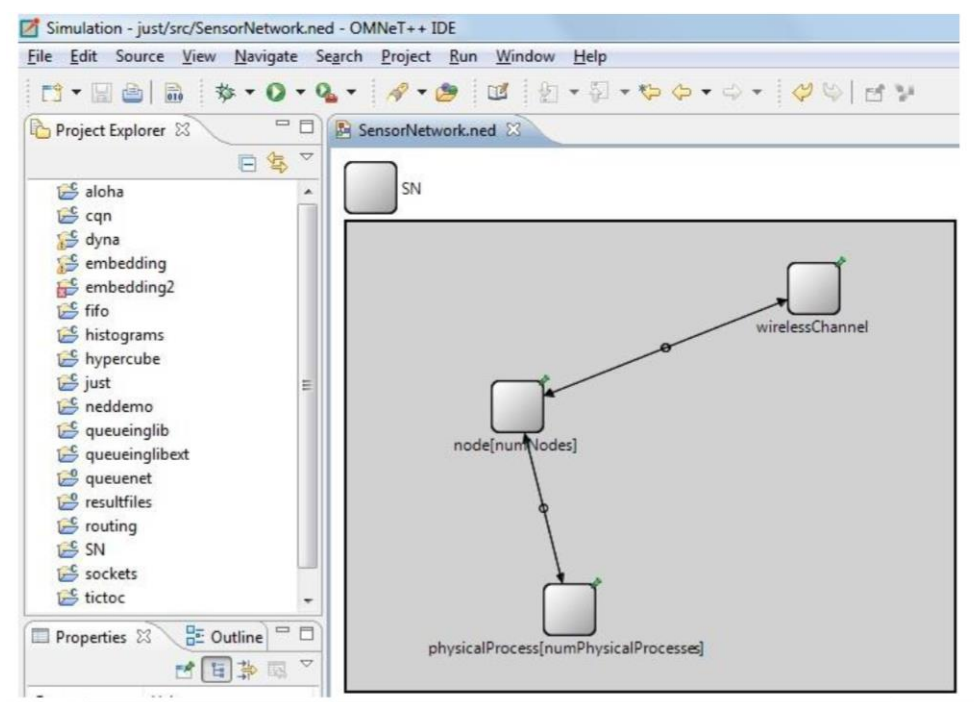


Рисунок 3.1 – Структура БСС

Node - это элемент который описывает каждую рабочую станцию и его параметры настраиваются numNodes, он определяет число станций в данной сети.

Модули из которых состоит станция (в Приложении А приведен код, описывающий модуль Node):

- Node - имя сети (используется для моделирования);
- Communication - модуль связи;
- Sensor Manager - модуль, описывающий количество датчиков;
- Resource Manager - модуль потребляемых ресурсов;
- Application - модуль приложений;
- Mobility Manager - модуль мобильности узлов.

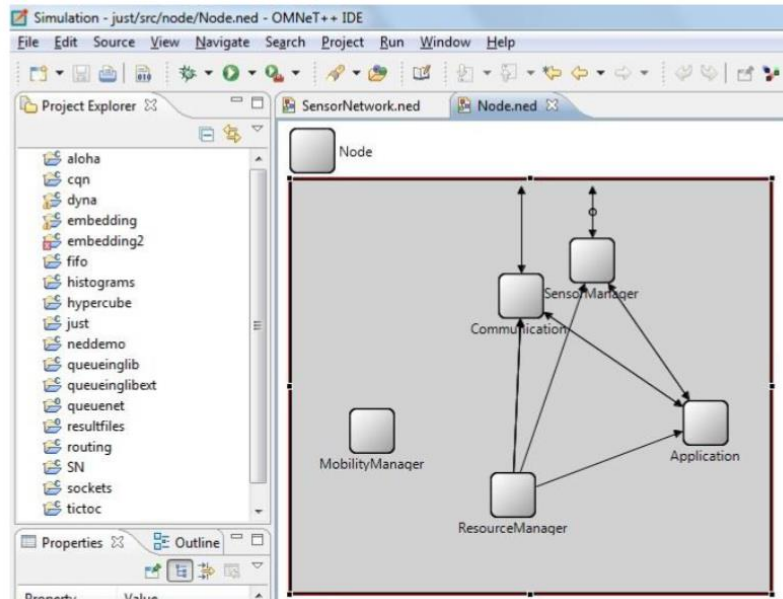


Рисунок 3.2 – Модуль Node

Структура модуля связи (в Приложении А приведен код, описывающий модуль Communication Module):

- Radio - модуль радиоканала;
- MAC - модуль физического уровня;
- Routing - модуль маршрутизации.

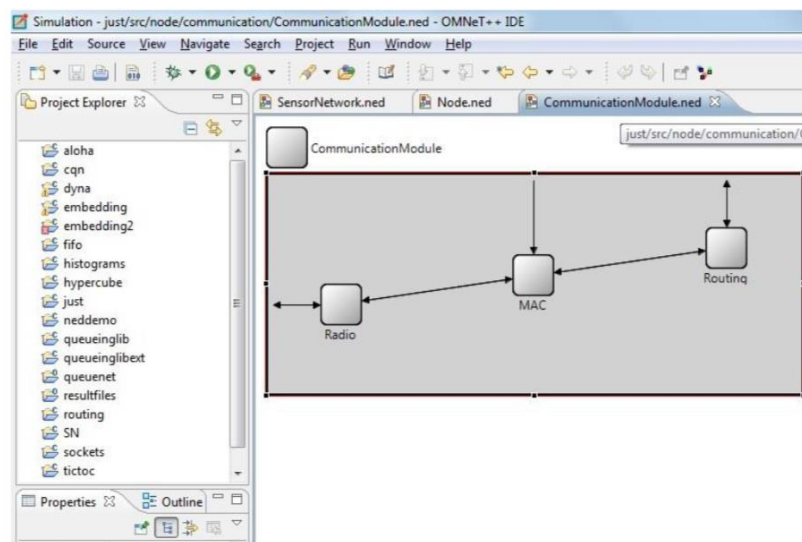


Рисунок 3.3 – Модуль CommunicationModule

Ошибки и не правильная симуляция сети может возникнуть из за изменения или удаления, какого либо элемента, все элементы сети важны[8].

В графическом режиме топология сети будет выглядеть следующим образом:



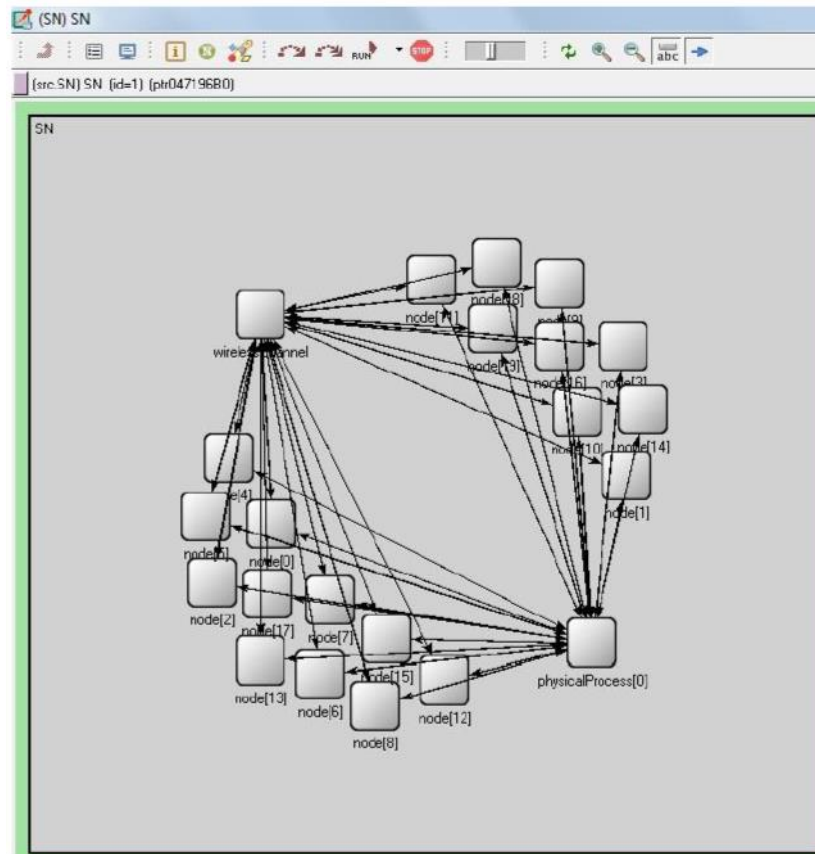


Рисунок 3.4 - Топология сети

Для просмотра собранной статистики запускаем скрипт Castalia Results (статистика отразится в файле gen.txt):

Castalia Results -igen.txt

Таблица 3.1- Статистика сети

Module	Output	Dimensions
Communication.MAC	Fraction of time with out PAN connection	19x1(3)
	Number of bea consreceived	19x1
	Number of bea consent	1x1
Communication.Radio	RX pktbreakdown	20x1(5)
	Txedpkts	20x1
ResourceManager	Consumed Energy	20x1
wirelessChannel	Fade depthdistribution	1x1(14)

Смоделировав сеть, перейдем к рассмотрению энергопотребления каждой из станций. Для просмотра статистики вводим в терминале следующую команду:

Castalia Results -igen.txt -senergy -n

Таблица 3.2 - Энергопотребление в час. Resource Manager:Consumed Energy

node=0	32,756	node=10	24,632
node=1	24,991	node=11	24,632
node=2	24,565	node=12	24,631
node=3	26,5	node=13	24,632
node=4	24,589	node=14	24,632
node=5	25,772	node=15	24,631
node=6	24,632	node=16	24,632
node=7	24,632	node=17	24,632
node=8	24,632	node=18	24,631
node=9	24,631	node=19	24,632

Для удобства представим полученные данные графически:

Castalia Results -i gen.txt -s energy -n | CastaliaPlot -o energy.jpg -s histogram

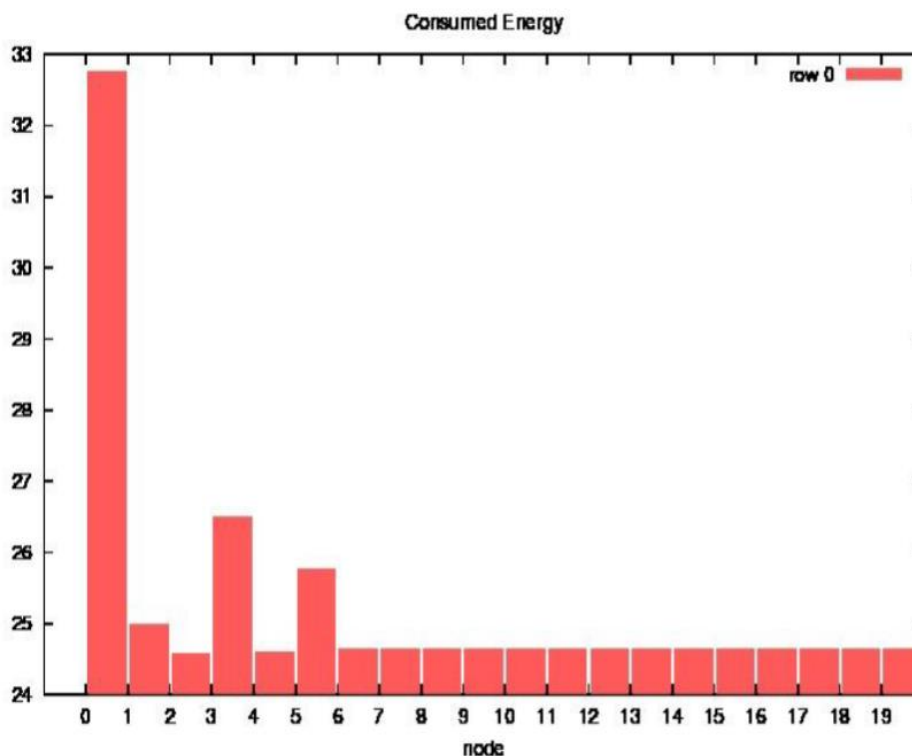


Рисунок 3.5 – Энергопотребление

Рассчитаем максимальное время работы каждого устройства.

Одна батарейка АА имеет емкость 2122 мАч. Следовательно, максимальное время работы (в часах), при использовании двух батареек АА, каждой станции составляет:

Таблица 3.3: Максимальное время работы

node=0	130	node=10	172
node=1	170	node=11	172
node=2	173	node=12	172
node=3	160	node=13	172
node=4	173	node=14	172
node=5	165	node=15	172
node=6	172	node=16	172
node=7	172	node=17	172
node=8	172	node=18	172
node=9	172	node=19	172

В Приложении В указана структура работы системы.

### 3.2 Техническое обеспечение беспроводной сенсорной сети в ЖК Манхэттен

Комплекс Манхэттен состоит из шести ярко-оранжевых 18, 19 и 20-этажных жилых домов с голубыми пирамидальными крышами. В каждом доме по одному подъезду. Комплекс имеет витражное остекление и стильный декор фасадов.

Жилой комплекс «29-й квартал» от застройщика Global Building Contract расположен на улице Брусиловского, 163, в районе улиц Шакарима — Прокофьева — Кулымбетова, в Алмалинском районе Алматы.

В дипломной работе, для передачи информации по беспроводному каналу были выбраны ZigBee модули JN5139-Z01-M02 компании Jennic у которых имеются настраиваемые усилители мощности.

Используемые модули компании Jennic для построения беспроводной сенсорной сети JN513x являются семейством недорогих, мало потребляющих беспроводных микроконтроллеров работающих по стандартам 802.15.4 и ZigBee. Благодаря данным модулям нет необходимости в дорогостоящей и продолжительной разработке дизайна платы и проведении набора тестов. В модулях реализовано взаимодействие с беспроводным микроконтроллером Jennic. JN5139, что позволяет получить комплексное высокопроизводительное решение. Существует 5 вариантов исполнения аппаратной части модулей: aJN5139-xxx-M00 имеет встроенную антенну, JN5139-xxx-M01/M03 – антенный коннектор, а JN5139-xxx-M02/M04 – усилитель мощности и МШУ для обеспечения большой дальностисвязи. В каждой из вариантов может быть запрограммирован сетевой протокол ZeeBee (JN5139-xxx-Z01/Myy).[8]

Особенности модулей для обеспечения большой дальности связи:

- диапазон 2.4 ГГц;
- аппаратный обработчик MAC – протоколов;
- дальность связи до 4 км;

- чувствительность приемника -100 дБм;
- выходная мощность передатчика +19 дБм;
- габариты модуля 18x41 мм;
- промышленный температурный диапазон от -20 до +70С.

Модули устанавливаются на сенсорной плате маршрутизатора DR1048 с интегрированными датчиками температуры, влажности, освещенности, имеющие выходы UART0 и UART1 для соединений с ЭВМ через кабель TTL-232R-3V3 (рисунок 3.6) [8]

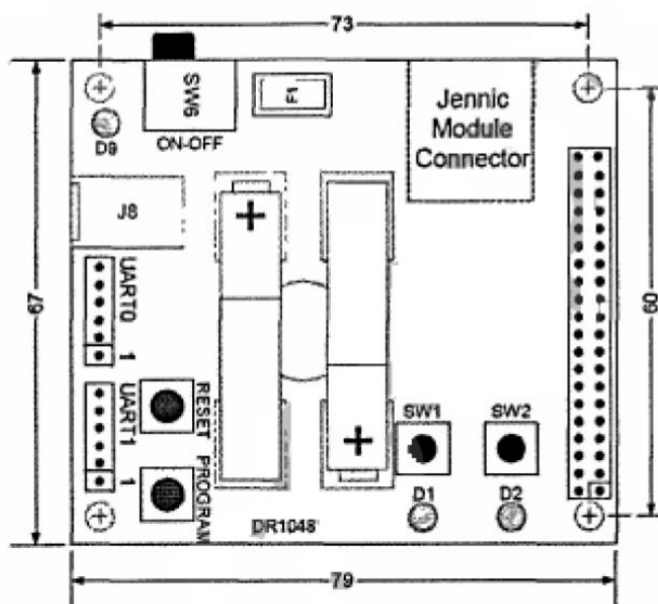


Рисунок 3.6 – Сенсорная плата DR1048

Отладочный комплект JN5139.

IEEE802.15.4/Jen Net Evaluation Kit предоставляет полную среду для быстрой разработки беспроводных приложений подключения на основе JN5139 беспроводного микроконтроллера. Включены все аппаратные и программные средства, необходимые для разработки продукта, с пятью узлами сети, набор разработчика программного обеспечения, программы для тестирования и примеры. Библиотеки предусмотренные IEEE802.15.4 и слоем Jen Net сетей, поддерживают топологии звезда, дерево линейную до 1000 узлов и обеспечивают само восстановление функциональных возможностей сети для надежной связи.[8]

Набор содержит одну плату контроллера, выступающего в роли координатора сети, и четыре маршрутизируемых сенсорных платы. Каждая плата содержит чип JN5139, выполненный в компактном референсном модуле.[8].

### 3.3 Практическая реализация архитектуры беспроводной сенсорной сети

Для внедрения беспроводной сенсорной сети был выбран крыша дома. Предназначенный для доступа к сети, то есть с помощью КШМ данные от БСС будут отправляться в центр управления. В состав КШМ входит оборудования спутниковой связи SE2Pro, самоноводящиеся антенна. То есть от БСС к центру управления данные будут отправляться через спутниковую связь, так как самая оперативная организация связи в сложных условиях боя. Задержка канала 600-800мс, скорость канала 4Мбит/с напередачу 8Мбит/с наприем.

SE2Pro имеет 4 порта Ethernet для доступа к сети. Два из которых используется для передачи данных, два для телефонии. Далее один порт передачи данных от SE2Pro используется для организации ВКС выделяется отдельная несущая для ВКС, например, 1Мбит/с на передачу 1Мбит/с. Второй порт для передачи данных подключается к Microtik-у который имеет 8 портов. Для доступа к сети интернет и для организации передачи данных выделяется отдельный порт от Microtik-а и отдельный Vlan. Для беспроводной сенсорной сети также выделится отдельный порт и Vlan. Скорость для БСС 512кбит/с прием/передача. Координатор сети будет установлен в КШМ и подключен к Microtik-у. Далее все данные поступают в кординатор от радиомодулей и выходят в сеть. Радиомодули подключаются потопологии Mesh. Топология Mesh позволяет передавать данные на большие расстояния путём разбиения длинного маршрута на серию коротких переходов между узлами. Особенность этой топологии гибкость и адаптивность. Так как при выходе из строя одного радиомодуля система будет перестроен под текущую ситуации и продолжать работу (Рисунок 3.7).

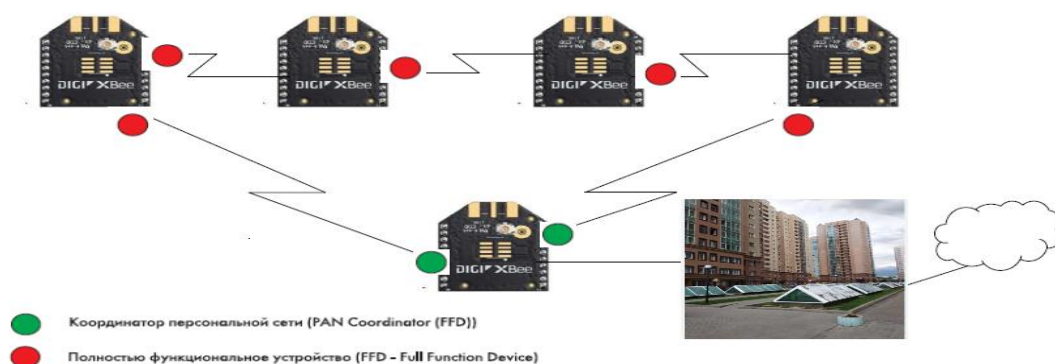


Рисунок 3.7 Структурная схема БСС для ЖК Манхэттен

### 3.4 Расчет потребляемой мощности устройств ZigBee

Потребляемая мощность при передаче данных непосредственно связана с размером пакета данных. Ток потребления при передаче для JN5139-Z01-M02 указан производителем и составляет 26,9 мА. Значение потребляемой мощности при использовании 3 В батареи, во время передачи будет составлять

$$P = UI$$

(3.1)

$$P = 26,9 \cdot 10^{-3} \cdot 3 = 80,7 \text{ мВт.}$$

Ток потребления во время приема данных для JN5139-Z01-M02 указан производителем и составляет 26,7 мА. Значение потребляемой мощности при использовании 3 В батареи, во время приема в соответствии с формулой (4.1), будет составлять

$$P = 26,7 \cdot 10^{-3} \cdot 3 = 80,1 \text{ мВт}$$

Ток потребления устройств ZigBee во время режима "сна" составляет 0,5 мкА, при использовании 3 В батареи потребляемая мощность во время режима "сна" будет иметь значение

$$P = 0,5 \cdot 10^{-6} \cdot 3 = 1,5 \text{ мкВт}$$

Антенна используемая в JN5139-Z01-M02 четверть волновая с коэффициентом усиления 2,2 дБ. Найдем усиление антенны во время передачи и приема сигнала в натуральных числах из формулы

$$G = 10^{\frac{G_{дд}}{10}} \quad (3.2)$$

$$G = 10^{\frac{2,2}{10}} = 1,667.$$

Чувствительность приемника определяется как минимальный входной сигнал который может успешно декодирован. JN5139-Z01-M02 имеет чувствительность приемника -95 дБм. Для нахождения значения в ваттах, используем формулу

$$P_r = \frac{10^{\frac{P_{дБм}}{10}}}{1000} \quad (3.3)$$

$$P_r = \frac{10^{\frac{-95}{10}}}{1000} = 3,1623 \cdot 10^{-13} \text{ Вт.}$$

### 3.5 Расчет шумов в тракте приема/передачи сети ZigBee

Для любой передачи данных справедливо утверждение, что полученный сигнал состоит из переданного сигнала, модифицированного различными искажениями, которые вносятся самой системой передачи, а также из дополнительных нежелательных сигналов, взаимодействующих с исходной волной в течение ее распространения от точки передачи к точке приема. Эти нежелательные сигналы принято называть шумом. Шум является основным фактором, ограничивающим производительность систем связи.

Верхний предел производительности систем связи определяет тепловой шум. Который распределен по всему спектру частот, и оказывает влияние на устройства передачи и приема, а также на среду передачи электромагнитных сигналов.

Спектральная плотность теплового шума не зависит от частоты, поэтому в широком диапазоне частот может рассматриваться как белый шум. Тепловой шум не зависит от частоты, поэтому плотность мощности шумов на ширину канала составляет

$$N = kTB[\text{Вт}] \quad (3.4)$$

где  $k = 1,3803 \cdot 10^{-23}$  Дж/К постоянная Больцмана;

T - абсолютная температура в Кельвинах;

B - ширина канала связи, Гц.

Запишем формулу нахождения плотности мощности шумов используя децибел-ватты

$$N = 10 \lg k + 10 \lg T + 10 \lg B. [\text{дБВт}] \quad (3.5)$$

Ширина канала Zigbee составляет 5 МГц, находим значение плотности мощности шумов, для стандартного канала связи Zigbee со стандартными условиями по температуре 298К, а также в условиях пониженной и повышенной температуры

$$N = 10 \lg(1,38 \cdot 10^{-23}) + 10 \lg 298 + 10 \lg 5 \cdot 10^6 = -136,3 [\text{дБВт}]$$

$$N = 10 \lg(1,38 \cdot 10^{-23}) + 10 \lg 323 + 10 \lg 5 \cdot 10^6 = -136 [\text{дБВт}]$$

$$N = 10 \lg(1,38 \cdot 10^{-23}) + 10 \lg 223 + 10 \lg 5 \cdot 10^6 = -138 [\text{дБВт}]$$

Необходимо упомянуть о возможности возникновения импульсных помех, возникновение этих помех является случайным процессом.

### 3.5.1 Модель "Затенения"

Модель свободного пространства и двухлучевая модель наиболее подходят для описания уровня сигнала и распространения для коротких линий связи. Но на больших расстояниях, передаваемый сигнал может быть подвержен различным эффектам, таким как замирание и многолучевое распространение, которые две первые модели не принимают во внимание, поэтому в этом случае целесообразнее использовать модель "Затенения" [1].

В данной модели учитывается фактор окружающей среды при передаче данных. Расположения в зонах затрудненной видимости, наличие большого количества препятствий создают проблему многолучевого распространения радиосигнала.

При описании канала связи системы ZigBee внутри помещения, в зоне затрудненной видимости необходимо учитывать два аспекта присущих распространению радиосигнала:

- а) размеры зоны покрытия сети ZigBee гораздо меньше, чем в условиях распространения на открытой местности;
- б) условия распространения радиоволн в данной зоне более многообразны.

Распространение радиоволн внутри помещения в основном определяется следующими параметрами:

- планировкой здания;
- строительными материалами;
- типом здания.

Уровень сигнала будет зависеть от расположения антенн, от того закрыты или открыты двери в комнатах. Внутри помещения часто очень много перегородок и стен, различных предметов, все это существенно влияет на возможности распространения радиосигнала.

Стены и перегородки внутри зданий часто разделяют на два типа:

- а) "жесткие" стены, которые являются частью конструкции здания;
- б) "мягкие" стены – перегородки, которые могут перемещаться.

Модель "Затенения" состоит из двух частей, первая часть модели называется моделью потерь в тракте передачи и предсказывает среднее значение принимаемой мощности относительно мощности на эталонном расстоянии.

$$\left[ \frac{P_r(d)}{P_r(d_0)} \right]_{\text{дБ}} = -10\beta * \log \left( \frac{d}{d_0} \right) \quad (3.6)$$

где  $\beta$  - постоянная потеря в тракте, и определена экспериментально.

Значение постоянной потерь  $\beta$  зависит от внешней среды, для зон с затрудненной видимостью имеет максимальное значение и выбирается в пределах от 4 до 6. Наименьшее значение равно 2 постоянная потеря  $\beta$  имеет для зоны свободной от препятствий (таблица 3.4)



Таблица 3.4 – Значения постоянной потерь  $\beta$

Внешняя среда		$\beta$ (постоянная потерь)
Открытая местность	Свободное от препятствий	2
	Застроенная городская	2,7-5
Закрытое помещение	Прямой видимости	1,6-1,8
	Затрудненный	4-6

Рассчитаем значение принимаемой мощности в закрытом помещении с затрудненной передачей, при котором значение постоянной  $\beta$  составляет от 4 до 6.

Для оценки качества тракта передачи при расположении датчиков ZigBee в зависимости от местоположения оборудования на электрической подстанции рассчитаем значения отношения принимаемой мощности к мощности на эталонном расстоянии при различных расстояниях для зон с затрудненной и прямой видимости. Полученные значения приведены в таблице 3.5.

Передача данных в зоне прямой и затрудненной видимости возможно при использовании ZigBee сетей в зданиях КРЭУ, ОПУ где возможно получения данных на центральный координатор. Рассчитанные значения приведены в таблице 3.5.

По рассчитанным значениям отношения принимаемой мощности к мощности на эталонном расстоянии был построен график зависимости данного показателя от расстояния (рисунок 3.7)

Как видно из графика на рисунке 3.8 отношение принимаемой мощности к мощности на эталонном расстоянии для зоны затрудненной видимости имеет большее значение, чем для зоны прямой видимости. Для зоны затрудненной видимости это значение при расстоянии 40 м составило -90 дБм, при этом для зоны прямой видимости это значение составило -30 дБм.

Таблица 3.5 – Результаты расчета

Расстояние между передатчиком и приемником сети ZigBee, d(м)	Значение $\left[ \frac{P_r(d)}{P_r(d_0)} \right]_{дБ}$ дБ (закрытое помещение с затрудненной передачей)	Значение дБ $\left[ \frac{P_r(d)}{P_r(d_0)} \right]_{дБ}$ дБ (закрытое помещение с зоной прямой видимости)
5	-41,94	-13,98
10	-60	-20

Продолжение таблицы 3.5

15	-70,57	-23,52
20	-78,06	-26,02
25	-83,88	-27,96
30	-88,63	-29,54
35	-92,64	-30,88
40	-96	-32,04
45	-99	-33,98

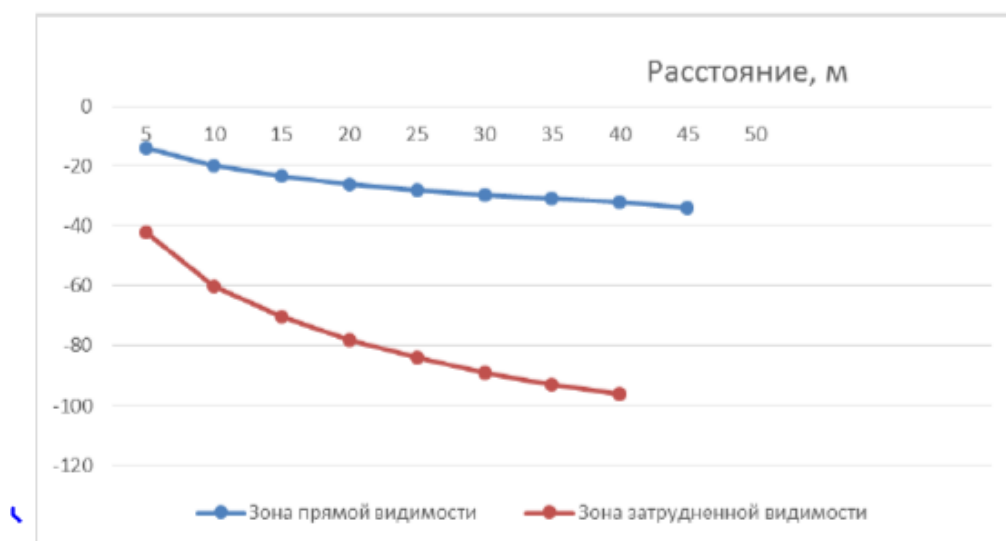


Рисунок 3.8 – Отношение принимаемой мощности к мощности на эталонном расстоянии

### 3.5.2 Определение уровня затухания и отношения сигнал-шум при передаче данных в системе ZigBee

Уровень затухания при распространение радиосигнала от передатчика к приемнику зависит от частоты на которой ведется передача, от расстояния между модулями, а также от значения нулевой гауссовой переменной [18].

Найдем значение затухания по формуле

$$\bar{P}_L(d_0) = 20 \log_{10}(f_{MHz}) + 10\beta \log(d) - 28 + N(0, \sigma_{ch}^2), \quad (3.7)$$

где  $f_{MHz}$  - частота модуля равная – 2400 МГц;  
расстояние между модулями внутри помещения допустимо 50 м.

Берем значение нулевой гауссовой переменной  $N(0, \sigma_{ch}^2)$  равным 1 (завод, зона затрудненной видимости),  $\beta = 2$ , тогда затухание на эталонном расстоянии будет найдено из следующего выражения

$$\overline{P}_L(d_0) = 20 \log_{10}(2405) + 10 * 2 \log(1) - 28 + 1 = 40(\text{дБ})$$

Найдем значение логарифмически-нормального распределения потерь в тракте с учетом ослаблений за счет препятствий по формуле

$$P_L(d) = \overline{P}_L(d_0) + 10\beta \log\left(\frac{d}{d_0}\right) + N(0, \sigma_{ch}^2), \quad (3.8)$$

где  $\overline{P}_L(d_0)$  – затухание на эталонном расстоянии (дБ);

$d$  – расстояние между передатчиком и приемником (м);

$d_0$  – эталонное расстояние (м);

$\beta$  – показатель степени потерь в тракте (среднее значение для помещений берется равным 6, для зоны затрудненной видимости);

$N(0, \sigma_{ch}^2)$  –случайная гауссова переменная (дБ).

Данный расчет дает приближенное значение потерь в тракте, так как не учитываются особенности пути распространения радиосигнала, а также тип материала из которого выполнены препятствия, а также размеры. Поэтому при передачи данных необходимо учитывать многолучевое распространение.

Из расчета по определению затухания в тракте передачи с учетом ослабления за счет препятствий видно, что сигнал при распространение в зоне затрудненной видимости испытывает многочисленное отражение и поглощение, в следствие этого уже при расстоянии 30 метров затухание сигнала достигает значения 70 дБ (таблица 3.6).

Таблица 3.6 – Затухание в тракте передачи.

Расстояние между передающим и приемным устройством, м	Затухание в тракте с учетом ослаблений за счет препятствий, дБ
5	55
10	61
15	64,52
20	67
25	68,96
30	70,54
35	71,88
40	73,04
45	74,06

Из графика на рисунке 3.9 видно, что значение затухания в тракте передачи с учетом ослабления за счет препятствий, достигает значения 75 дБ при расстоянии 45 метров. Уровень принимаемой мощности при использовании

системы передачи данных ZigBee на электрической подстанции в зонах затрудненной видимости, может иметь низкое значение даже при расстояниях 10-15 метров.

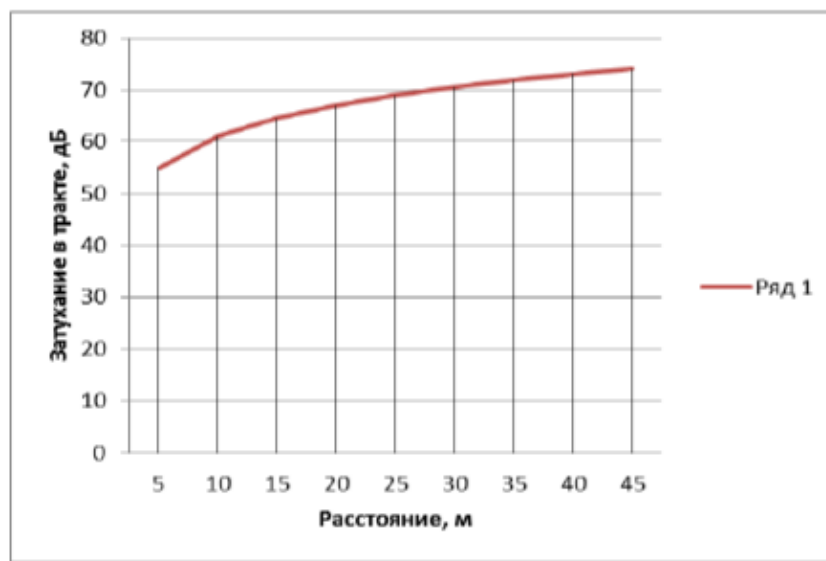


Рисунок 3.9 – Затухание в тракте с учетом ослаблений за счет препятствий

Найдем значения отношения сигнал-шум (ОСШ) на входе приемника последующей формуле.

$$\gamma(d) = N(\bar{P}_t, \sigma_t^2) - P_L(d) - N(\bar{P}_n, \sigma_n^2), \text{ дБ}$$

где  $\bar{P}_t$  - средняя (номинальная) выходная мощность передатчика (дБм);

$\sigma_t^2$  - дисперсия выходной мощности;

$\bar{P}_n$  - средний (номинальный) уровень шумов приемника (дБм);

$\sigma_n^2$  - дисперсия уровня шумов.

В таблице 3.7 приведены значения полученные при расчете отношения сигнал-шум на входе приемника при разных расстояниях между модулями.

На рисунке 3.10 показан график зависимости отношения сигнал-шум от расстояния. Как видно из графика отношение сигнал-шум с увеличением расстояния резко уменьшается и при 45 метров составляет около 22 дБ, что соответствует низкому уровню качества связи.

Таблица 3.7 – Значение ОСШ на входе приемника

Расстояние между передающим и приемным устройством, м	Отношение сигнал-шум (ОСШ) на входе приемника, дБ.
5	41,5
10	35,5
15	31,98
20	29,5
25	27,54
30	25,96
35	24,62
40	23,46
45	22,5

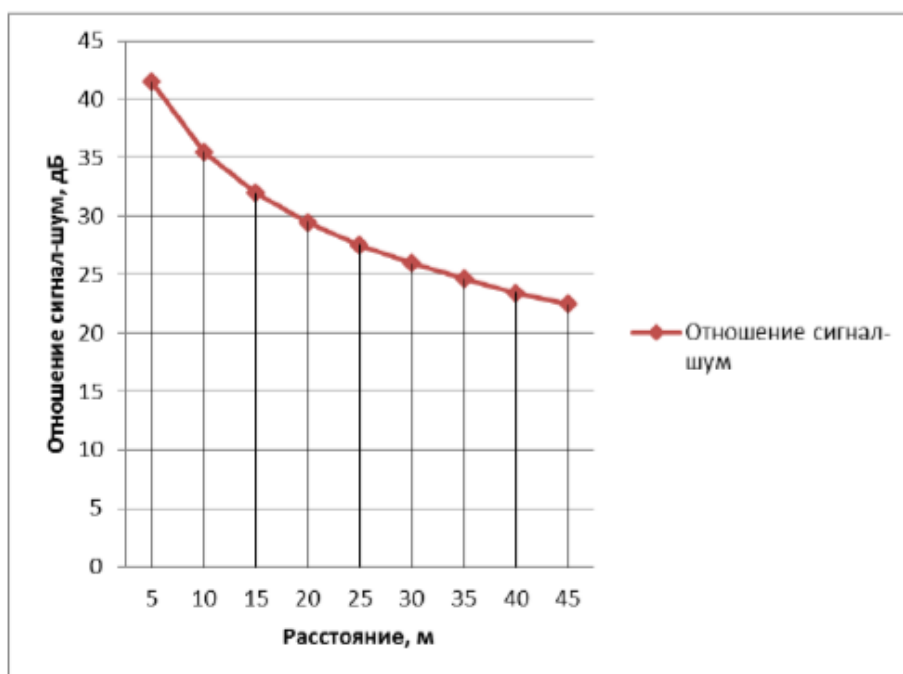


Рисунок 3.10 – Зависимость отношения сигнал-шум от расстояния

В третьей главе смоделирована беспроводная сенсорная сеть ZigBee в ЖК Манхэттен графическом редакторе OMNET++, вывели статистику энергопотребления каждой из станций. В качестве радио модуля ZigBee был выбран JN5139-Z01-M02 компании Jennic, в качестве координатора сети был выбран JN5139. Рассмотрели основные технические характеристики и особенности. Также с помощью программы Visio спроектировали архитектуру беспроводной сенсорной сети для IoT. Топология сети Mesh. Особенность топологии mesh в том что радиомодули могут работать между собой без координатора есть без центрального шлюза, это дает возможность гибкости сети и адаптивность в реальном бою. Если один из радиомодулей выключит сеть будет дальше функционировать обновляя таблицу маршрутизации.

В расчетной части были рассчитаны потребляемая мощность радиомодуля (в режиме приема и передачи и во время сна), рассчитали шумы при распространении сигнала для нахождения отношения сигнал-шум, который показывает реальный уровень сигнала при определенном расстоянии. Для расчета дальности связи был выбран модель "Затенения", который принимает во внимание различные эффекты, такие как замирание и многолучевое распространение и т.д.

## ЗАКЛЮЧЕНИЕ

В работе рассмотрена возможность передачи данных от различных датчиков используемых в ЖК Манхэттен с базовой станции системы мониторинга за параметрами с помощью беспроводной сети ZigBee.

Для практической реализации были выбраны радиомодули, координатор сети, точка доступа к сети, смоделировали БСС для ZigBee, построили схему подключения радиомодулей.

В расчетной части были рассчитаны потребляемая мощность радиомодуля (в режиме приема и передачи и во время сна), рассчитали шумы при распространении сигнала для нахождения отношения сигнал-шум, который показывает реальный уровень сигнала при определенном расстоянии. Для расчета дальности связи был выбран модель "Затенения", который принимает во внимание различные эффекты, такие как замирание и многолучевое распространение и т.д.

Внедрения технологии IoT дает большое преимущество в сборе информации. Это сеть взаимосвязанных сущностей или «вещей» в военной сфере, которые постоянно общаются друг с другом, чтобы координировать, учиться и взаимодействовать с физической средой, чтобы выполнять широкий спектр действий более эффективным и осозанным образом.

## СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Ефимов М.М., Киричек Р.В.: Интернет вещей: перспективы адаптивных систем // Информационные технологии и телекоммуникации. 2020. Том 8. № 1. С. 55–66.
2. Abdellah, A.R. Machine Learning Algorithm for Delay Prediction in IoT and Tactile Internet. / Abdellah, A.R.; Mahmood, O.A.; Kirichek, R.; Paramonov, A.; Koucheryavy, A. // Future Internet 2021, Vol. 13, Issue. 12, 304, pp. 1-19.
3. 12. Abdellah, A.R. Performance Estimation in V2X Networks Using Deep Learning-Based M-Estimator Loss Functions in the Presence of Outliers. / Alshahrani, A.; Muthanna, A.; Koucheryavy, A // Symmetry 2021, Vol. 13, Issue. 11, pp. 1-18
4. Stepanov S.N. The Analysis of Resource Sharing for Heterogenous Traffic Streams over 3GPP LTE with NB-IoT Functionality / S.N. Stepanov, M.S. Stepanov, U. Andrabi, J. Ndayikunda. // Distributed Computer and Communication Networks. DCCN 2020. Lecture Notes in Computer Science. — 2020. — Vol 12563. — P. 422-435.
5. TinyOS, <http://www.tinyos.net>
6. Сури, Ниранджан; Тортонези, Мауро; Михаэлис, Джеймс; Будулас, Питер; Бенинкаса, Джакомо; Рассел, Стивен; Стефанелли, Чезаре; Винклер, Роберт (2016). «Анализ применимости Интернета вещей к среде поля боя». 2016 Международная конференция по военным коммуникациям и информационным системам (ICMCIS)
7. Удзикевич, Ян; Фуртак, Януш; Зелински, Збигнев (2015). «Отказоустойчивые методы Интернета военных вещей». 2015 IEEE второй Всемирный форум по Интернету вещей (WF-IoT).
8. Концепция организации беспроводных сенсорных сетей и их применение. Молодежный научно - технический журнал вестник. Издатель ФГБОУ ВПО «МГТУ им. Н.Э. Баумана». Эл. № ФС77-51038
9. УДК 004.051 Анализ энергоциклов узлов беспроводных сенсорных сетей. А.Н. Зеленин Кандидат технических наук, профессор. В.А. Власова Аспирантка E-mail: zлата\_ne@bk.ru Кафедра «Сети связи» Харьковский национальный университет радиоэлектроники пр. Ленина, 14, г. Харьков, 61166
10. Meier A., NoSE: Efficient Maintenance and Initialization of Wireless Sensor Networks [Электронный ресурс] / A. Meier, M. Woehrle, M. Weise, J. Beutel, L. Thiele // Electronics Laboratory. – 2009. Режим доступа: <ftp://ife.ee.ethz.ch/pub/people/andream/papers/MWWBT2009.pdf>.
11. Курпатов Р.О., Исследование и разработка энергоэффективного метода локализации элементов беспроводных сенсорных сетей [Текст] / Р.О. Курпатов // Атореф. диссертации на соиск. ученой степени к.т.н. – М. – 2011. – 23 с



12. Иваненко В.А., Анализ протоколов передачи данных от узлов в беспроводных сенсорных сетях [Текст]/ В.А. Иваненко // Восточно-Европейский журнал передовых технологий. – 2011. – 2/10 (50). – С. 9-12.
13. Баскаков С., Оценка энергопотребления беспроводных узлов в сетях MeshLogic [Текст]/ С. Баскаков // Беспроводные технологии. – 2010. – №1. – С. 28-31.
14. Олифер В.Г., Компьютерные сети. Принципы, технологии протоколы: Учебник для ВУЗов [Текст]/ В.Г. Олифер, Н.А. Олифер.– 3-е изд. – СПб.: Питер. – 2006. – 958 с.: ил.
15. Финогеев А. Г., Дильман В. Б., Маслов В. А., Финогеев А. А. Оперативный дистанционный мониторинг в системе городского теплоснабжения на основе беспроводных сенсорных сетей. 2010 г.
16. Д. Чен, К. Яо, Р. Е. Хадсон. Ресурсы позиционирования – 2002.
17. К. Чинтапулади, Р. Говиндан. Обнаружение в сенсорных сетях – 2003.
18. К. Чинтапулади, Р. Говиндан, Д. Сухтаме. Позиционирование с использованием ранжирования и группировки – 2004.

## РЕЦЕНЗИЯ

на дипломную работу

Талғатулы Н

6В06201 Телекоммуникация

**Тема: «Проектирование жилого комплекса Манхэттен с применением технологии IoT»**

В дипломной работе производится проектирование сети IoT в ЖК Манхэттен и разработка беспроводной сенсорной сети. Сеть был разработана на основе телекоммуникационной технологии "ZigBee".

В проекте проведен обзор, анализ и классификация систем IoT. Также рассмотрены существующие системы телекоммуникации в ЖК Манхэттен и для внедрения БСС был выбран оборудования. С помощью программы OMNET++ был смоделирован БСС. Для проектирования и моделирования произведен расчет параметров потребляемой мощности, расчет шумов в тракте приема/передачи, дальность действия связи, уровень затухания и отношения сигнал-шум.

В расчетной части были рассчитаны потребляемая мощность радиомодуля (в режиме приема и передачи и во время сна), рассчитали шумы при распространении сигнала для нахождения отношения сигнал-шум, который показывает реальный уровень сигнала при определенном расстоянии.

Внедрения технологии IoT дает большое преимущество в сборе информации. Это сеть взаимосвязанных сущностей или «вещей» в военной сфере, которые постоянно общаются друг с другом, чтобы координировать, учиться и взаимодействовать с физической средой, чтобы выполнять широкий спектр действий более эффективным и осознанным образом.

Общие требования к составлению, изложению, оформлению и содержанию текстовых и графических материалов работы выполнены в соответствии с ГОСТ

Дипломная работа выполнена на оценку 90/A+ /«отлично», а дипломант, Талғатулы Н достоин степени бакалавра специальности 6В06201 Телекоммуникация.

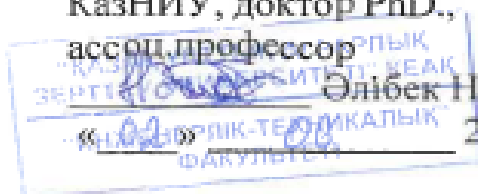
Рецензент

КазНИУ, доктор PhD.,

ассоц. профессор

Элібек Н.Б

2023 г.



## ОТЗЫВ

на дипломную работу

Талгатулы Нурсултан

ОП 6В06201 Телекоммуникация

**Тема: «Проектирование жилого комплекса Манхэттен с применением технологии IoT»**

В дипломной работе производится проектирование сети IoT в ЖК Манхэттен и разработка беспроводной сенсорной сети. Сеть была разработана на основе телекоммуникационной технологии "ZigBee".

Структура дипломной работы включает в себя: введение, три основных раздела, заключение, список использованной литературы.

В первом разделе проведен обзор, анализ и классификация систем IOT. Также рассмотрены существующие системы телекоммуникации в ЖК Манхэттен и для внедрения БСС был выбран оборудования.

Во втором разделе для практической реализации были выбраны радиомодули, координатор сети, точка доступа к сети, смоделировали БСС для ZigBee, построили схему подключения радиомодулей

В третьем разделе с помощью программы OMNET++ был смоделирован БСС. Для проектирования и моделирования произведен расчет параметров потребляемой мощности, расчет шумов в тракте приема/передачи, дальность действия связи, уровень затухания и отношения сигнал-шум.

Внедрения технологии IoT в ЖК Манхэттен дает большое преимущество в сборе информации. Это сеть взаимосвязанных сущностей или «вещей» в любой сфере, которые постоянно общаются друг с другом, чтобы координировать, учиться и взаимодействовать с физической средой, чтобы выполнять широкий спектр действий более эффективным и осознанным образом.

В заключении даны основные выводы по проделанной работе. Общие требования к составлению, изложению, оформлению и содержанию текстовых и графических материалов работы выполнены в соответствии с ГОСТ

Дипломная работа выполнена на оценку 85/В+/*«хорошо»*, а дипломант, Талгатулы Нурсултан достоин степени бакалавра ОП 6В06201 Телекоммуникация.

Отзыв руководителя  
м.т.н., старший преподаватель  
кафедры ЭТнКТ,

Маркесулы С

« 19 » 10 2023 г

## Протокол

### о проверке на наличие неавторизованных заимствований (плагиата)

Автор: Талгатулы Нурсултан

Соавтор (если имеется):

Тип работы: Дипломная работа

Название работы: Проектирование жилого комплекса Манхэттен с применением технологии IoT

Научный руководитель: Сунгат Маркесұлы

Коэффициент Подобия 1: 11.1

Коэффициент Подобия 2: 4.9

Микропробелы: 0

Знаки из других алфавитов: 0

Интервалы: 0

Белые Знаки: 0

После проверки Отчета Подобия было сделано следующее заключение:

Заимствования, выявленные в работе, является законным и не является плагиатом. Уровень подобия не превышает допустимого предела. Таким образом работа независима и принимается.

Заимствование не является плагиатом, но превышено пороговое значение уровня подобия. Таким образом работа возвращается на доработку.

Выявлены заимствования и плагиат или преднамеренные текстовые искажения (манипуляции), как предполагаемые попытки укрытия плагиата, которые делают работу противоречащей требованиям приложения 5 приказа 595 МОН РК, закону об авторских и смежных правах РК, а также кодексу этики и процедурам. Таким образом работа не принимается.

Обоснование:

2023-06-02

*Дата*

*Заведующий кафедрой*



**Университеттің жүйе администраторы мен Академиялық мәселелер департаменті  
директорының ұқсастық есебіне талдау хаттамасы**

Жүйе администраторы мен Академиялық мәселелер департаментінің директоры көрсетілген еңбекке қатысты дайындалған Плагиаттың алдын алу және анықтау жүйесінің толық ұқсастық есебімен танысқанын мәлімдейді:

**Автор: Талғатулы Нурсултан**

**Тақырыбы: Проектирование жилого комплекса Манхэттен с применением технологии IoT**

**Жетекшісі: Сұңғат Марксұлы**

**1-ұқсастық коэффициенті (30): 11.1**

**2-ұқсастық коэффициенті (5): 4.9**

**Дәйексөз (35): 1.3**

**Әріптерді ауыстыру: 0**

**Аралықтар: 0**

**Шағын кеңістіктер: 0**

**Ақ белгілер: 0**

**Ұқсастық есебін талдай отырып, Жүйе администраторы мен Академиялық мәселелер департаментінің директоры келесі шешімдерді мәлімдейді :**

Ғылыми еңбекте табылған ұқсастықтар плагиат болып есептелмейді. Осыған байланысты жұмыс өз бетінше жазылған болып санала отырып, қорғауға жіберіледі.

Осы жұмыстағы ұқсастықтар плагиат болып есептелмейді, бірақ олардың шамадан тыс көптігі еңбектің құндылығына және автордың ғылыми жұмысты өзі жазғанына қатысты күмән тудырады. Осыған байланысты ұқсастықтарды шектеу мақсатында жұмыс қайта өңдеуге жіберілсін.

Еңбекте анықталған ұқсастықтар жосықсыз және плагиаттың белгілері болып саналады немесе мәтіндері қасақана бұрмаланып плагиат белгілері жасырылған. Осыған байланысты жұмыс қорғауға жіберілмейді.

**Негіздеме:**

**2023-06-02**

*Күні*

*Кафедра меңгерушісі*



## Протокол

### о проверке на наличие неавторизованных заимствований (плагиата)

Автор: Талгатулы Нурсултан

Соавтор (если имеется):

Тип работы: Дипломная работа

Название работы: Проектирование жилого комплекса Манхэттен с применением технологии IoT

Научный руководитель: Сүңғат Марқсұлы

Коэффициент Подобия 1: 11.1

Коэффициент Подобия 2: 4.9

Микропробелы: 0

Знаки из других алфавитов: 0

Интервалы: 0

Белые Знаки: 0

После проверки Отчета Подобия было сделано следующее заключение:

- Заимствования, выявленные в работе, является законным и не является плагиатом. Уровень подобия не превышает допустимого предела. Таким образом работа независима и принимается.
- Заимствование не является плагиатом, но превышено пороговое значение уровня подобия. Таким образом работа возвращается на доработку.
- Выявлены заимствования и плагиат или преднамеренные текстовые искажения (манипуляции), как предполагаемые попытки укрытия плагиата, которые делают работу противоречащей требованиям приложения 5 приказа 595 МОН РК, закону об авторских и смежных правах РК, а также кодексу этики и процедурам. Таким образом работа не принимается.
- Обоснование:

2023-06-02

*Дата*

Сүңғат Марқсұлы

  
*проверяющий эксперт*