НАУЧНЫЙ ЖУРНАЛ

СИСТЕМЫ СИНХРОНИЗАЦИИ, ФОРМИРОВАНИЯ И ОБРАБОТКИ СИГНАЛОВ

№3-2025 год

Учредитель:
ООО «ИД Медиа Паблишер»

Номер подписан в печать 15.05.2025 г.

СОДЕРЖАНИЕ

МОБИЛЬНЫЕ ВИРТУАЛЬНЫЕ ОПЕРАТОРЫ В СЕТЯХ 5G. МОДЕЛИ И АРХИТЕКТУРА

Гольдштейн Борис Соломонович
д.т.н., профессор
bgold@niits.ru

Елисеев Сергей Михайлович
аспирант, научно-технический центр ПРОТЕЙ
eliseev_s@protei.ru

Аннотация
В статье рассмотрены проблемы и новые задачи виртуальных операторов MVNO (Mobile Virtual Network Operator) при переходе к сетям пятого и последующих поколений (Beyond 5G) с виртуализацией сетевых функций, шарингом и слайсингом, облачными и туманными вычислениями, etc. Показаны необходимость новых подходов к перспективным MVNO для работы с PMNO (Physical Mobile Network Operators) поколений B5G, математического моделирования новых стратегий доступа к сетевым ресурсам и приоритетного обслуживания запросов, анализа вероятностно-временных характеристик системно-сетевого взаимодействия MVNO и PMNO.

Ключевые слова
Beyond 5G, виртуальные операторы мобильной связи MVNO (Mobile Virtual Network Operators), сетевые архитектуры, SLA (Service Level Agreement), показатели качества обслуживания QoS, вероятностно-временные характеристики.

Введение

В сегодняшних сетях в сетях пятого поколения используются две основные архитектуры: 5G NSA (Non-Standalone) и 5G SA (Standalone), которые различаются по степени зависимости от сетей предыдущего поколения (4G LTE) и по тем возможностям, которые они могут предложить для организации MVNO [1]. В данной статье рассматривается только 5G SA – полностью автономная архитектура, которая работает на независимом ядре сети 5G Core и обеспечивает все функции и возможности, предусмотренные в стандарте 5G.

Сдвиг парадигмы MVNO в сетях 5G SA в значительной степени обусловлен именно технологией Network Slicing, который был введен консорциумом 3GPP еще в релизе 14, а затем развит в последующих релизах 15, 16, 17. По прогнозу [5] эта новая парадигма MVNO в условиях Network Slicing является существенным изменением в мире сотовых сетей, позволяющим создавать многоуровневые сетевые структуры, схожие с современной сетью Интернет и обеспечивающие совместное использование ресурсов с логической изоляцией между несколькими MVNO. Более того, в самом ближайшем будущем представляется реальной иерархия MVNO, в результате развития которой подавляющее большинство сетей мобильной связи будут мобильными виртуальными при относительно небольшом количестве опорных физических мобильных сетей PMNO.

Но основное внимание в данной работе уделено встречному процессу, при котором один MVNO имеет возможность подключаться к нескольким PMNO. Исследование вероятностно-временных характеристик в обоих этих сценариях развития является, безусловно, актуальной задачей.

Архитектуры MVNO в сетях 5G

Традиционно, MVNO это виртуальные мобильные операторы, использующие сеть радиодоступа и, опционально, другие элементы инфраструктуры опорных классических мобильных операторов, и продающие услуги под собственным брендом.

Подходы к построению виртуальных операторов MVNO описываются функциональными моделями. Модели MVNO формируют уровни предоставляемых сервисов и сценарии взаимодействия с опорными операторами PMNO. Модели MVNO отличаются друг от друга степенью зависимости виртуального оператора от PMNO. Фактически, спектр возможностей MVNO как оператора определяется объемом сетевой инфраструктуры, которой он может управлять самостоятельно. В действующих мобильных сетях поколений 2-4G широко распространены три основные модели:

– MVNO Branded reseller – оператор, который производит продажу и маркетинг сервисов PMNO, но под собственным брендом. При этом отсутствует какое-либо управление данными сервисами.

– MVNO Light – оператор, который также предоставляет сервисы PMNO, однако есть возможность управления бизнес-приложениями, что позволяет регулировать тарифные предложения.

– MVNO Full – оператор, который обладает своим ядром мобильной сети. Либо частично, либо целиком. При данной модели MVNO самостоятельно реализует сервисы и управляет бизнес-приложениями.

В сетях пятого поколения, когда объемы их покрытия приведут к стремительному росту внедрения виртуальных операторов, данные модели будут также применимы и задействованы. Первые две из них лежат исключительно в коммерческой плоскости. Научный же интерес представляют MVNO модели Full, архитектуры сетей которых буду рассмотрены далее в рамках 5G SA.

Архитектура базовой сети 5G Core включает совокупность функциональных модулей базовой сети и сетевых интерфейсов, соединяющих эти модули [2]. Сетевые элементы 5G реализованы в виде виртуальных сетевых функций – VNF (Virtual Network Functions). Построение MVNO Full в сетях 5G возможно по трем следующим архитектурам.

Начнем рассмотрение с архитектуры MVNO 5G на базе технологии GWCN (Gateway Core Network), на рисунке 1, восходящее еще к сетям LTE и предусматривающее совместное использование несколькими операторами системы радиодоступа, модулей управления мобильностью MME, но организацию в MVNO собственных шлюзов базовой сети SGW/PGW и сервера домашней базы данных пользователей HSS [6].

Сценарии и соглашения при взаимодействии между PMNO и MVNO при GWCN в 5G тоже аналогичны сетям LTE. Фактически, это эволюционный подход построения виртуальных операторов модели MVNO Full из LTE. Новым фактором, который вносит ограничения и который необходимо учитывать для MVNO в этом варианте архитектуры, являются сетевые сегменты (слайсы) и их совместимость между сетями MVNO и PMNO для реализации сервисов с заданными параметрами качества обслуживания. В данной архитектуре сеть радиодоступа остается закрытой для MVNO.

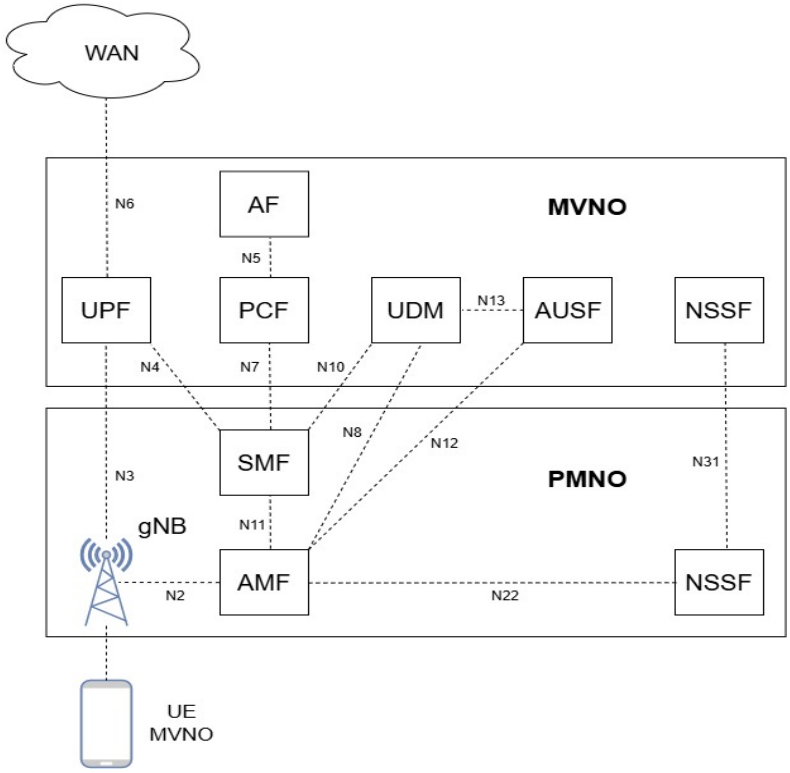


Рис. 1. Архитектура MVNO GWCN в сетях 5G

Архитектура MVNO 5G на базе технологии MOCN (Multi-Operator Core Network) определяет сценарий совместного использования только сети радиодоступа между несколькими операторами PMNO и MVNO. Опорная сеть 5G принадлежит и управляется MVNO целиком (рис. 2). Ресурсы радиодоступа распределяются между операторами на основании заключенных PMNO и MVNO соглашений SLA (Service Layer Agreement).

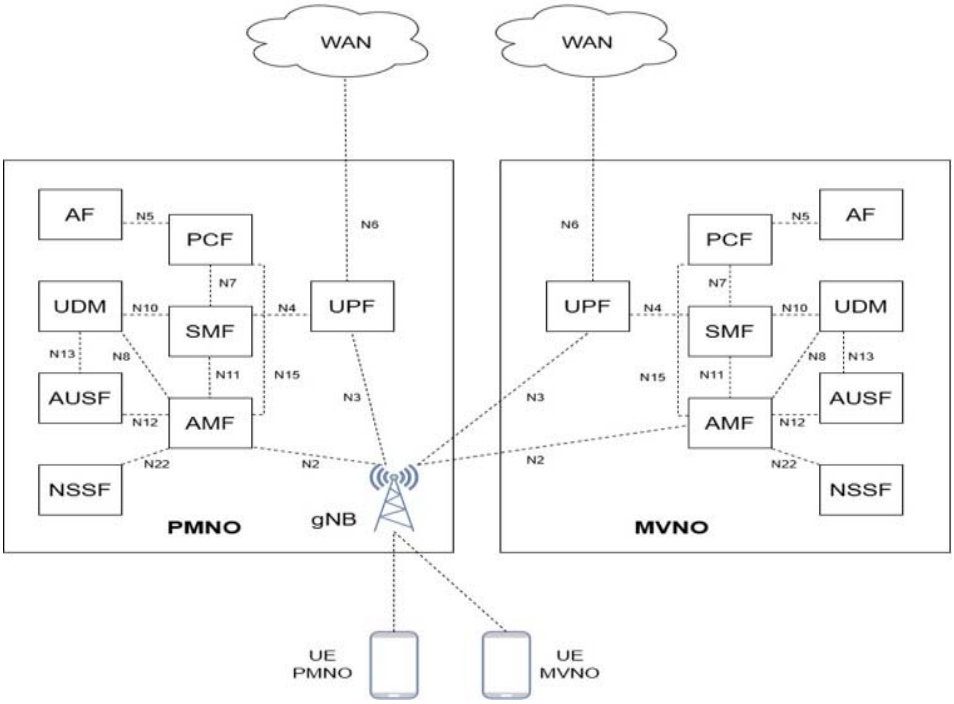


Рис. 2. Архитектура MVNO MOCN в сетях 5G

Реализация логики распределения абонентов между базовыми сетями PMNO и MVNO возлагается на базовые станции 5G (NG-RAN). Определение базовой сети (PMNO или MVNO) для абонента (SIM-карты) ведется на основании кода мобильной сети, в которой регистрируется абонент. Технология MOCN также была описана в стандартах и для сетей 4G LTE, однако широкого практического применения для построения виртуальных операторов не получила. Одна из причин – невозможность контроля и учета PMNO потоков данных виртуальных MVNO, так как трафик проходит только через базовые станции опорного оператора. Другая проблема заключается в том, что для подключения MVNO необходимо производить реконфигурацию всех базовых станций PMNO, число которых может измеряться сотнями тысяч.

Данные ограничения актуальны и для сетей 5G. В связи с этим, большого количества запусков MVNO на основе технологии MOCN также не прогнозируется.

Построение MVNO 5G на базе технологии Network Slicing позволяет разделить сеть 5G на несколько виртуальных сетей. Каждая виртуальная сеть может быть оптимизирована для обслуживания конкретного сервиса. Данная технология позволяет конфигурировать и многократно использовать сетевые элементы и функции в каждом сетевом сегменте (slice) для удовлетворения определенных требований.

Сеть 5G, в основе которой лежит технология Network Slicing, позволяет операторам не только выделять сегменты для реализации своих сервисов, но и предлагать их третьим сторонам. Такой подход полностью укладывается в концепцию MVNO – виртуальная сеть для виртуального оператора. Эти новые механизмы, обеспечивающие распределение ресурсов как по радиоинтерфейсу, так и по физической сети, обеспечивают возможность виртуализировать ресурсы PMNO и обеспечить высокую степень логической изоляции между MVNO, как это предусмотрено документом ассоциации GSMA [7].

Сценарий интеграции MVNO с PMNO посредством предоставления (аренды) сетевого сегмента значительно расширяет возможности виртуального оператора и выходит за рамки традиционной концепции MVNO. Впервые у MVNO появляются механизмы взаимодействия с подсистемой радиодоступа PMNO (RAN Slicing), что позволяет еще менее зависеть от опорного оператора и более гибко реализовывать сервисы с различными требованиями к параметрам качества обслуживания.

Преимуществами данного подхода также служат высокие скорости запуска MVNO и снижение порога вхождения новых виртуальных операторов на рынок, ведь теперь нет необходимости закупать дорогостоящее ПО ядра сети 5G и аппаратные ресурсы.

Открытым вопросом здесь остается проблематика, связанная с ограниченностью системы управления сетевыми сегментами в контексте предоставления индивидуальных интерфейсов третьим сторонам. Данному вопросу, а также подробному анализу такого подхода будут посвящены отдельные работы.

Анализ характеристик подключения MVNO

Наиболее значимыми параметрами подключения MVNO к PMNO являются стоимостные показатели и вероятностно-временные характеристики (ВВХ). Финансовые показатели вычисляются через стоимость C_S обслуживания абонента MVNO и соответственная оплата C_N, от оператора MVNO сети PMNO, к которой он подключен. Разумеется, $C_S > C_N$, иначе бизнес MVNO перестает быть рентабельным. С другой стороны, в выборе соотношения величин C_S и C_N иногда следует учитывать экономическую выгоду для абонента подключаться к MVNO, а не напрямую к PMNO.

Но в большинстве случаев экономия средств не является главным фактором для принятия решения относительно MVNO. Как правило, существенную роль играют некоторые дополнительные функциональные возможности, особые требования к SLA (Service Level Agreement), аспекты информационной безопасности, нумерации, администрирования и численные характеристики обслуживания. Время установления соединения $T_{connect}$ между MVNO и PMNO, которое складывается задержки сигнального обмена (signalling delays) – T_{signal}, процессов аутентификации и авторизации – T_{auth} времени выделения сетевых ресурсов – T_{alloc}

$$T_{connect} = T_{signal} + T_{auth} + T_{alloc}$$

Вероятность успешного подключения ($P_{success}$), т.е. вероятность успешного установления соединения MVNO с инфраструктурой PMNO:

$$P_{success} = 1 - P_{failure}$$

где $P_{failure}$ – вероятность отказа, которая может быть вызвана отказами оборудования, ошибками аутентификации и т.д.

Среднее время обслуживания, включая время ожидания в очереди, что для простейшей модели M/M/1 вычисляется по известной формуле:

$$M[T_{connect}] = \frac{1}{\mu - \lambda}$$

где λ – интенсивность входящих запросов подключения, а μ – интенсивность обслуживания.

Вероятность перегрузки ($P_{overload}$), когда интенсивность запросов от MVNO превышает возможность PMNO, что для простейшего случая модели Эрланга оценивается через вероятность:

$$P_{overload} = \frac{\frac{\rho^N}{N!}}{\sum_{k=0}^{N} \frac{\rho^k}{k!}}$$

где $\rho = \frac{\lambda}{\mu}$ и целый ряд других вероятностно-временных характеристик (ВВХ), для вычисления которых необходимы более сложные математические модели, в частности [3, 8, 9].

Вероятностно-временные характеристики подключения MVNO к трем PMNO

Рассмотрим ситуацию, когда MVNO имеет договоры на подключение с тремя разными операторами PMNO. Достаточно понятная ситуация при наличии в стране Большой тройки мобильных операторов PMNO (рис. 3).

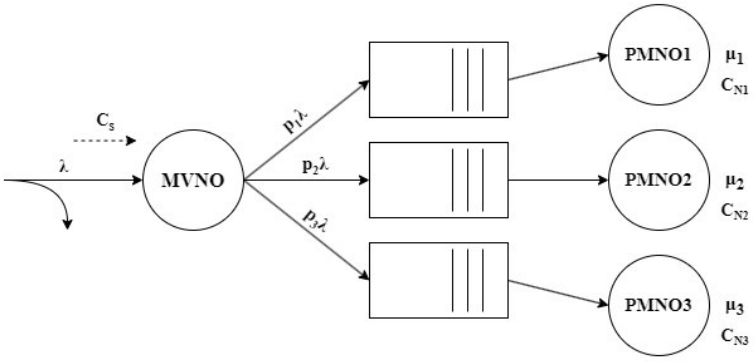


Рис. 3. ВВХ подключения MVNO к трем PMNO

Продолжаем считать поток пуассоновским с интенсивностью λ, который распределяется в три потока таким образом, что пуассоновский поток со средней скоростью поступления $\lambda_1 = p_1\lambda$ направляется в PMNO 1, пуассоновский поток со средней скоростью поступления $\lambda_2 = p_2\lambda$ направляется в PMNO 2, а пуассоновский поток со средней скоростью поступления $\lambda_3 = p_3\lambda$ направляется в PMNO 3.

Во всех трех PMNO поддерживается стационарное состояние с $\lambda_i < \mu_i$, т.е. для каждого потока от MVNO к PMNO должно быть $p_i\lambda < \mu_i$, для i = 1, 2, 3.

Вероятности p_i - коэффициенты распределения трафика MVNO между PMNO:

$$p_1 + p_2 + p_3 = 1.$$

Соответственно среднее время пребывания (ожидания и обслуживания) вычисляется по следующей формуле:

$$M[T_{connect}] = \frac{p_1}{p_1\lambda - \mu_1} + \frac{p_2}{p_2\lambda - \mu_2} + \frac{1 - p_1 - p_2}{(1 - p_1 - p_2)\lambda - \mu_3}$$

Таким образом, оператор MVNO получая текущие значения μ_1, μ_2 и μ_3 от каждого PMNO может пересчитывать вероятности p_1, p_2, p_3, чтобы при обязательном соблюдении ограничения $p_i\lambda < \mu_i$ минимизировать время $M[T_{connect}]$ или максимизировать экономический эффект $C_S - C_N$.

Назначая и переназначая значения p_1, p_2, p_3 в реальном времени оператор MVNO может перераспределять трафик между тремя PMNO и тем самым оптимизировать свой бизнес.

Заключение

Можно с уверенностью сказать, что сети пятого поколения мобильной связи открывают следующий этап развития виртуальных операторов MVNO. Фундаментальные технологии, заложенные в 5G, в частности виртуализация сетевых функций и Network Slicing, привнесли принципиально новые механизмы и подходы к организации, построению и управлению MVNO. При этом опыт, накопленный виртуальными операторами в сетях 2-4G, будет также актуален на первых этапах внедрения MVNO в 5G [10, 11].

В данной работе представлены основные модели и архитектуры построения MVNO в сетях 5G SA, обсуждены некоторые аспекты проблематики функционирования MVNO в сетях поколений 5G и B5G и сделан весьма оптимистический прогноз относительно дальнейших перспектив MVNO, постепенного преобразования мобильных операторов в направлении виртуализации их деятельности, развития целой иерархии сетей MVNO.

Основное внимание уделено вероятностно-временным характеристикам подключения MVNO и функционированию MVNO в среде мульти-MNO. Рассмотрен частный случай, когда число PMNO равно трем. Предложен инструмент для оптимизации перераспределения трафика с целью повышения эффективности функционирования MVNO в мобильных сетях связи.

Литература

1. *Кучерявый А., Гольдштейн Б.* Сети пост-NGN. СПб.: БХВ-Петербург, 2013.

2. *Тихвинский В., Девяткин Е., Белявский В.* По пути от 5G к 5G Advanced: релизы 17 и 18 // Первая миля, выпуск 6, 2021.

3. *Yarkina N., Gaidamaka Y., Correia L., Samouylov K.* An Analytical Model for 5G Network Resource Sharing with Flexible SLA-Oriented Slice Isolation. Mathematics 2020, 8, 1177; doi:10.3390/math8071177

4. *Гольдштейн Б.С.* Инфокоммуникационные сети и системы. СПб.: БХВ-Петербург, 2024

5. *Молчанов Д.А., Бегишев В.О., Самуйлов К.Е., Кучерявый Е.А.* Сети 5G/6G: архитектура, технологии, методы анализа и расчета: монография. М.: РУДН, 2022. 516 с.

6. *Зайчик Е.* Совместное использование сетевой инфраструктуры операторами связи // Первая миля, выпуск 7, 2019.

7. GSMA NG.116 «Generic Network Slice Template», Version 9.0, 2023.

8. *Abdelhamied A. Ateya, Ahmed A. Abd El-Latif, Ammar Muthanna, Artem Volkov, Andrey Koucheryavy*. Enabling Metaverse and Telepresence Services in 6G Networks // River Publishers Series in Communications and Networking, 2025.

9. *Елисеев С., Гринева А*. Подходы к виртуализации сетей мобильных операторов связи поколения 4/5G // Сборник научных статей АПИНО, 2021. С. 426-442.

10. *Вэнь Тонг, Пейин Чжу*. Сети 6G. Путь от 5G к 6G глазами разработчиков. От подключенных людей и вещей к подключенному интеллекту / пер. с англ. М.: ДМК Пресс, 2022.

11. *Darshan A. Ravi, Vijay K. Shah, Chengzhang Li, Tom Hou, Jeffrey H. Reed.* RAN Slicing in Multi-MVNO Evironment under Dynamic Channel Conditions arXiv:2104.04900v1 [eess.SP] 11 Apr 2022.

ТЕХНОЛОГИИ ОПТИМИЗАЦИИ СЕТЕВОГО ТРАФИКА

Гадасин Денис Вадимович
МТУСИ, доцент кафедры СИТиС, к.т.н., Москва, Россия
dengadiplom@mail.ru

Кобелькова Александра Дмитриевна
МТУСИ, Москва, Россия
kad08.02@mail.ru

Родина Алина Андреевна
МТУСИ, Москва, Россия
alina_rodina2004@mail.ru

Сурова Мария Андреевна
МТУСИ, Москва, Россия
surrovamma@mail.ru

Аннотация
В современном мире функционирование онлайн-сервисов невозможно представить без анализа сетевого трафика и его оптимизации. С ростом числа пользователей и объемов передаваемых данных анализ трафика становится крайне важным для поддержания стабильности, масштабируемости и надежности сетевых решений. В статье рассматриваются методы и технологии анализа трафика с использованием сетевого оборудования, особое внимание уделено оптимизации трафика с помощью современных подходов, включая балансировку нагрузки, сети доставки контента (CDN) и протоколы маршрутизации BGP и OSPF. Практическая часть статьи демонстрирует влияние настройки данных протоколов на пропускную способность сети, что подтверждает их эффективность в реальных условиях.

Ключевые слова
Трафик, оптимизация трафика, способы оптимизации сетевого трафика, сетевые протоколы, управление трафиком, протокол BGP, протокол OSPF.

Введение

В соответствии с определением под сетевым трафиком понимается объем данных, передаваемых между двумя оконечными точками посредством сетевых устройств за определенный период времени. Трафик включает в себя все виды информации, такие как текстовые сообщения, мультимедийные файлы, запросы к веб-сайтам и другие данные, которые перемещаются между узлами сети в битах за единицу времени. Суммарный трафик для произвольного узла возможно поделить на входящий и исходящий. Под входящим трафиком понимается поток данных, который поступает получателю из внешней сети, а исходящий – поток данных, поступающий во внешнюю сеть от данного получателя, что подробно рассмотрено в работах [1-2].

В условиях постоянно растущего объема данных и увеличения числа пользователей, эффективная обработка трафика становится крайне важным фактором для поддержания высокого уровня производительности, надежности и удобства использования сервисов. Для достижения этих целей организация обработки трафика должна быть более гибкой и иметь возможность подстраиваться под изменяющиеся условия. Оптимизация является одним из способов управления трафиком в целях эффективного и результативного использования доступной пропускной способности [3-5].

Обработка трафика сетевым оборудованием представляет собой сложный процесс, который включает в себя множество взаимосвязанных компонентов и механизмов, необходимых для обеспечения стабильной и безопасной работы онлайн-сервисов и представляет собой процесс, который начинается с приема запросов к серверу. В том случае если клиенту необходимо отправить электронное письмо, то почтовому сервера, к файловому серверу, если клиент запрашивает доступ к конкретному файлу, веб-серверу если клиентом был отправлен запрос на загрузку веб-страницы. Подобные методы обработки были рассмотрены в работе [6].

Процесс обработки трафика

Основная нагрузка в процессе управления трафиком ложится на сетевое оборудование, к которому относятся маршрутизаторы, коммутаторы, межсетевые экраны и прокси-серверы. Наиболее эффективное использование сетевых ресурсов и достижение максимальной надежности передачи данных достигается по-

средством пакетной передачи данных. Для чего, на передающем узле формируется пакет данных, который помимо самой информации включает в себя адрес устройства-получателя, IP-адрес сервера, и адрес устройства-отправителя – IP-адрес клиента. IP-адреса необходимы для маршрутизации пакета через сеть и обеспечения доставки данных в нужное целевое устройство. При прохождении пакета данных передается через сеть, он обрабатывается на транзитных узлах так же посредством сетевого оборудования.

Алгоритм обработки трафика возможно рассмотреть на примере пользовательского запроса на загрузку веб-страницы. На первом этапе происходит обработка пакетов данных маршрутизаторами и состоит в анализе IP-адресов назначения пакета, и определении наиболее подходящего пути для его передачи. Определение пути передачи происходит на основе таблиц маршрутизации, содержащих данные о структуре сети и доступных маршрутах, что позволяет маршрутизатору выбрать наиболее подходящий путь для передачи данных. Способы реализации этой технологии были рассмотрены в работах [7-8].

На следующем этапе пакет данных поступает на коммутаторы, которые отвечают за передачу данных между устройствами в локальной сети. Коммутаторы производят анализ MAC-адресов устройств и обеспечивают получение пакетов устройствами, являющимися конечными пунктами назначения, что является необходимым условием для минимизации нагрузки на сеть и увеличения скорости передачи данных. В том случае, если пакет данных необходимо передать за пределы локальной сети, то он снова попадает на маршрутизатор, который направляет его в соответствующую сеть исходя из таблицы маршрутизации.

В качестве устройства, которое принимает участие в обработке трафика задействуются межсетевые экраны. Основное назначение межсетевых экранов – анализ пакетов на предмет соответствия правилам безопасности, фильтрация трафика и блокировка потенциально опасных запросов, например запрос, содержащий в себе атаку типа «отказ в обслуживании» или попытка несанкционированного доступа к передаваемым данным [9]. Таким образом при передаче трафика осуществляется обеспечение защиты сети от угроз и поддержание высокого уровня безопасности.

В качестве дополнительного этапа обработки трафика возможно применить прокси-серверы, выступающие в роли посредника между клиентом и сервером и осуществляющие кэширование данных, что значительно ускоряет доступ к часто запрашиваемым ресурсам, так как это устраняет необходимость в повторной их загрузке. Помимо этого, прокси-сервер фильтрует трафик и блокирует нежелательный контент, что является особенно важным для корпоративных сетей, где необходимо обеспечить контроль доступа сотрудников к определенным ресурсам.

На завершающем этапе обработки трафика происходит обработка запроса веб-сервером или приложением. Сервер формирует ответ, который в дальнейшем отправляется обратно пользователю. Ответ проходит через те же этапы обработки, что и запрос, и в итоге достигает устройства пользователя. Схема обработки трафика представлена на рисунке 1.

В условиях сложных и динамически изменяющихся сетевых топологий одной из ключевых задач при передаче данных является эффективная маршрутизация, что подробно рассмотрено в работах [10-11].

Проблема выбора маршрута передачи данных возникает из-за постоянных изменений в структуре сети, например, в случае добавления или удаления узлов или изменениях пропускной способности каналов связи. Неправильная маршрутизация может привести к увеличению времени передачи данных, перегрузке отдельных каналов связи и снижению общей производительности сети. Для решения этих задач используются протоколы маршрутизации, такие как OSPF (Open Shortest Path First) и BGP (Border Gateway Protocol), которые позволяют адаптироваться к изменениям в сети и выбирать эффективные пути передачи данных.

OSPF является внутренним протоколом маршрутизации, который используется в локальных сетях (LAN) для определения оптимальных путей на основе алгоритма кратчайшего пути (Shortest Path First). OSPF работает по принципу обмена информацией между маршрутизаторами о состоянии сети, что позволяет быстро адаптироваться к изменениям в топологии. Основные преимущества OSPF включают автоматическое обновление таблицы маршрутизации при изменении топологии сети, что минимизирует время восстановления после сбоев, а также поддержку зон обслуживания и уменьшает объем данных, необходимых для обработки маршрутизатором.

BGP представляет собой протокол внешней маршрутизации, который используется для обмена информацией между автономными системами (AS) в глобальной сети. BGP позволяет выбирать маршруты между различными сетями, учитывая различные факторы, например, политику маршрутизации и надежность путей. Основные преимущества BGP включают возможность настройки сложные правила для выбора маршрутов, что особенно важно для крупных сетей с множеством путей, поддержку мультипротокольной маршрутизации, которая позволяет работать с различными типами адресов, включая IPv4 и IPv6, а также устойчивость к сбоям, так как BGP автоматически обнаруживает сбои в сети и перенаправляет трафик по альтернативным маршрутам (см. рис. 1).

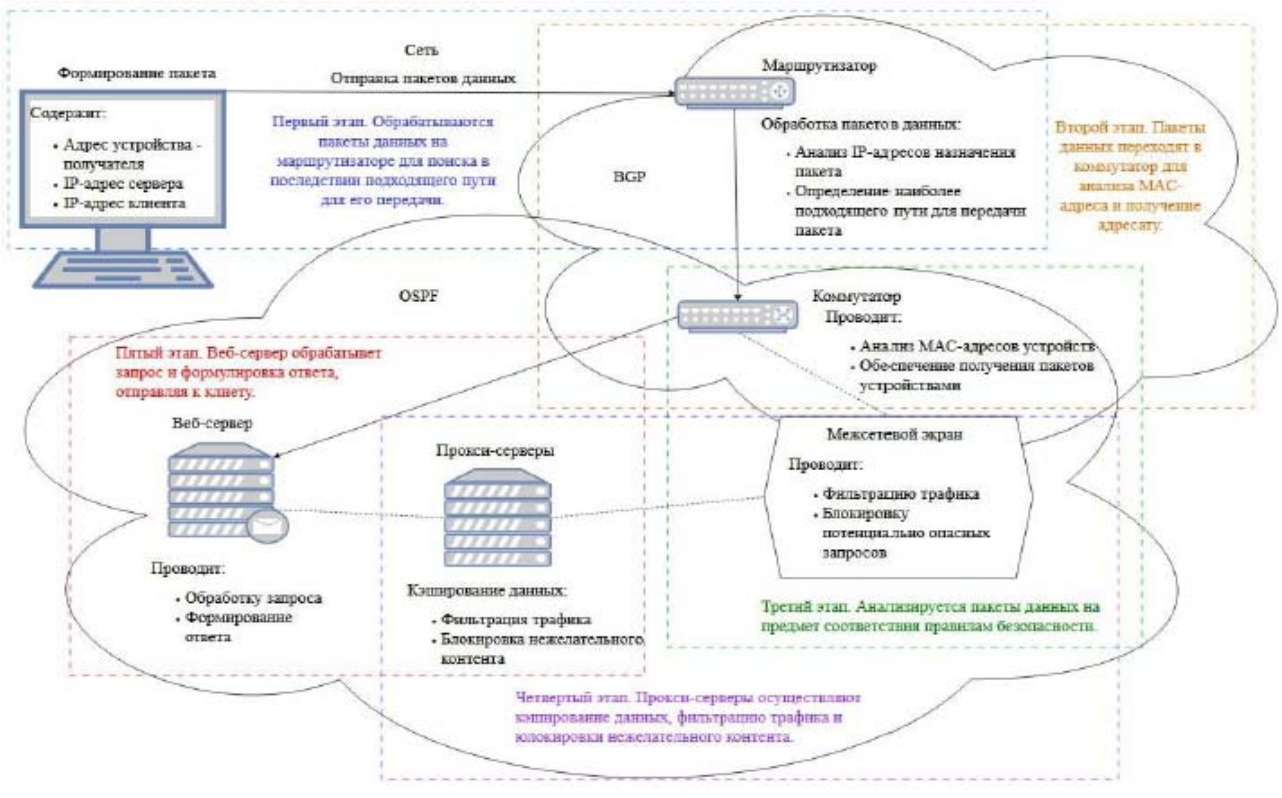


Рис. 1. Схема обработки трафика

Эффективность протоколов BGP и OSPF

Для того, чтобы практически исследовать использование протоколов динамической маршрутизации OSPF и BGP и доказать, что эти протоколы позволяют существенно повысить пропускную способность сети, снизить нагрузку на сервер и улучшить общую производительность системы в условиях динамически изменяющихся сетевых топологий, с использованием оборудования кафедры СИТиС МТУСИ и инструментов приложения «Cisco Packet Tracer» был проведен эксперимент, в рамках которого были смоделированы условия работы сети без применения оптимизирующих протоколов, а затем проведено тестирование после их настройки. Для реализации были использованы материалы работ [12-14].

Для тестирования технологии была создана модель сети, для построения которой были использованы устройство клиента (PC-PT PC0), сетевые коммутаторы (2050T-24 Switch0 и 2950T-24 Switch1), маршрутизаторы (1841 Router2 и 1841 Router3) и устройство сервера (Server-PT Server0) (рис. 2).

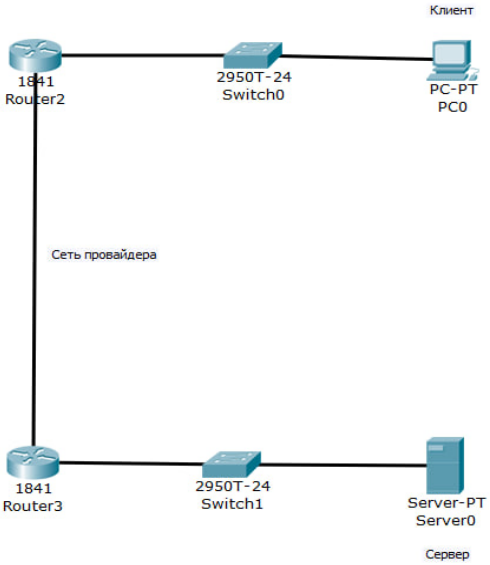


Рис. 2. Схема сети

Для демонстрации пропускной способности и уровня загруженности сервера была развернута виртуальная машина в среде VMware. В качестве гостевой операционной системы использовался Ubuntu Server 20.04 LTS, а в качестве гипервизора – VMware Workstation Pro 16.

Виртуальная машина была настроена с использованием двух виртуальных процессоров, оперативной памяти объемом 4 ГБ и жесткого диска емкостью 40 ГБ типа SCSI. Для обеспечения сетевого взаимодействия был задействован сетевой адаптер с режимом NAT. В качестве операционной системы на виртуальной машине была установлена 64-битная версия Linux – Ubuntu Server 20.04 LTS.

Изначально виртуальная машина была запущена без внедрения протоколов динамической маршрутизации OSPF и BGP, что позволило зафиксировать базовые показатели пропускной способности и уровня загруженности сервера. Затем были настроены и активированы указанные протоколы, после чего проведены повторные измерения для оценки их влияния на производительность системы. Сравнение полученных данных до и после внедрения протоколов позволило проанализировать их эффективность в контексте оптимизации пропускной способности и снижения нагрузки на сервер.

Анализ данных проводился при помощи утилиты iperf3, которая предназначена для измерения пропускной способности сетевого соединения. Установить Iperf3 на обеих машинах можно через пакетный менеджер, например, apt для Ubuntu или brew для macOS.

Iperf3 представляет собой инструмент, функционирующий по клиент-серверной модели, который генерирует TCP- и UDP-трафик для оценки пропускной способности сети. С его помощью можно точно определить максимальную пропускную способность между сервером и клиентом, а также провести нагрузочное тестирование сетевого канала, что позволяет выявить его производительность и устойчивость к высоким нагрузкам.

Для демонстрации процесса на одной из машин необходимо активировать Iperf3 в режиме сервера, что выполняется при помощи команды: iperf3 -s -p 2323. Данная команда инициирует прослушивание входящих соединений на указанном порту (2323), что позволяет серверу ожидать подключения клиентов для проведения измерений пропускной способности сети (рис. 3).

```
root@bst2201:/home/bst2201# iperf3 -s -p 2323
-----------------------------------------------------------
Server listening on 2323 (test #1)
-----------------------------------------------------------
Accepted connection from ::1, port 45630
[  5] local ::1 port 2323 connected to ::1 port 45636
[ ID] Interval           Transfer     Bitrate
[  5]   0.00-1.00   sec  0.00 Bytes  0.00 bits/sec
[  5]   1.00-2.00   sec  0.00 Bytes  0.00 bits/sec
[  5]   2.00-3.00   sec  0.00 Bytes  0.00 bits/sec
[  5]   3.00-4.00   sec  0.00 Bytes  0.00 bits/sec
[  5]   4.00-5.00   sec  0.00 Bytes  0.00 bits/sec
[  5]   5.00-6.00   sec  0.00 Bytes  0.00 bits/sec
[  5]   6.00-7.00   sec  0.00 Bytes  0.00 bits/sec
```

Рис. 3. Активация режима сервера

На другой машине Iperf3 запускается в режиме клиента с указанием IP-адреса сервера с помощью команды: iperf3 -c <IP-адрес-сервера>. В операционных системах Linux поддерживаются два режима работы – клиент и сервер, которые могут быть активированы на разных вкладках терминала. Этот процесс осуществляет тестирование пропускной способности сети, в ходе которого клиент начинает передачу данных на сервер для измерения скорости и оценки производительности сетевого соединения.

В процессе настройки теста определяются ключевые параметры, такие как длительность тестирования, задаваемая через флаг -t <seconds>, размер пакета, указываемый с помощью флага -l <length>, тип используемого протокола (TCP или UDP), где UDP активируется флагом -u, а также количество потоков, регулируемое параметром -P <number>. Пример команды с использованием утилиты Iperf3 может выглядеть следующим образом: iperf3 -c <IP-адрес-сервера> -t 10 -P 4, где задается тест длительностью 10 секунд с использованием 4 потоков.

По завершении тестирования Iperf3 формирует отчет, содержащий ключевые метрики, такие как пропускная способность, выраженная в Mbps или Gbps, общее время выполнения теста, объем переданных данных, а также статистику, включающую потери пакетов и показатели задержек.

Клиент осуществляет передачу данных на сервер в течение заданного временного интервала. В процессе передачи Iperf3 фиксирует объем переданных данных и время, затраченное на их отправку.

Сервер, в свою очередь, отображает информацию о передаче данных с указанием временных интервалов. В представленном примере реализации, в силу специфики тестового запуска, за все секунды выполнения теста не было передано ни одного байта данных, что привело к нулевому значению битрейта – показателя, характеризующего скорость передачи данных.

На клиенте, подключенном к серверу для измерения пропускной способности сети, была запущена утилита Iperf3, были получены данные о передаче информации за каждый интервал, равный одной секунде. В первом интервале, соответствующем промежутку от 0.00 до 1.00 секунды, объем переданных данных составил 622 МБ, что эквивалентно скорости передачи примерно 637008 КБ/с.

За все проверяемые интервалы передача была стабильной с незначительными колебаниями как в объеме переданных данных, так и в скорости передачи (рис. 4).

```
Connecting to host localhost, port 5201
[  5] local ::1 port 58150 connected to ::1 port 5201
[ ID] Interval           Transfer     Bitrate         Retr  Cwnd
[  5]   0.00-1.00   sec   622 MBytes  637008 KBytes/sec    0   1.19 MBytes
[  5]   1.00-2.00   sec   662 MBytes  677444 KBytes/sec    0   1.19 MBytes
[  5]   2.00-3.00   sec   645 MBytes  660447 KBytes/sec    0   1.19 MBytes
[  5]   3.00-4.00   sec   654 MBytes  669368 KBytes/sec    0   1.19 MBytes
[  5]   4.00-5.00   sec   623 MBytes  637488 KBytes/sec    0   1.19 MBytes
[  5]   5.00-6.00   sec   621 MBytes  636140 KBytes/sec    0   1.19 MBytes
[  5]   6.00-7.00   sec   598 MBytes  612358 KBytes/sec    0   1.19 MBytes
[  5]   7.00-8.00   sec   645 MBytes  660680 KBytes/sec    0   1.19 MBytes
[  5]   8.00-9.00   sec   644 MBytes  659287 KBytes/sec    0   1.19 MBytes
[  5]   9.00-10.00  sec   569 MBytes  582930 KBytes/sec    0   1.19 MBytes
[  5]  10.00-11.00  sec   606 MBytes  621311 KBytes/sec    0   1.25 MBytes
[  5]  11.00-12.00  sec   578 MBytes  592162 KBytes/sec    0   1.25 MBytes
[  5]  12.00-13.00  sec   609 MBytes  623238 KBytes/sec    0   1.31 MBytes
[  5]  13.00-14.00  sec   618 MBytes  632398 KBytes/sec    0   1.31 MBytes
[  5]  14.00-15.00  sec   567 MBytes  580445 KBytes/sec    0   1.31 MBytes
[  5]  15.00-16.00  sec   636 MBytes  651053 KBytes/sec    0   1.37 MBytes
[  5]  16.00-17.00  sec   554 MBytes  566785 KBytes/sec    0   1.37 MBytes
[  5]  17.00-18.00  sec   564 MBytes  577115 KBytes/sec    0   1.37 MBytes
^C[  5]  18.00-18.93  sec   562 MBytes  620422 KBytes/sec    0   1.37 MBytes
- - - - - - - - - - - - - - - - - - - - - - - - -
[ ID] Interval           Transfer     Bitrate         Retr
[  5]   0.00-18.93  sec  11.3 GBytes  626238 KBytes/sec    0             sender
[  5]   0.00-18.93  sec  0.00 Bytes  0.00 KBytes/sec                  receiver
iperf3: interrupt - the client has terminated
```

Рис. 4. Проверка без дополнительных протоколов

Настройка протокола BGP (Border Gateway Protocol) на маршрутизаторе Cisco начинается с активации BGP и указания номера автономной системы (AS), к которой принадлежит маршрутизатор. Это выполняется с помощью команды router bgp 65001, где 65001 — номер автономной системы. Для проверки состояния BGP-сессий и маршрутов используется команда: show ip bgp summary. Далее указываются IP-адреса соседних маршрутизаторов и их номера AS с помощью команды neighbor 192.168.1.1 remote-as 65002, где 192.168.1.1 – IP-адрес соседа, а 65002 – номер его автономной системы. Для анонсирования сетей через BGP применяется команда network 10.0.0.0 mask 255.255.255.0, которая объявляет сеть 10.0.0.0 с маской 255.255.255.0. Состояние BGP-сессий и маршрутов проверяется с использованием команды show ip bgp summary.

BGP использует протокол TCP для установления соединений между соседними маршрутизаторами и обмена маршрутной информацией. Каждый маршрут в BGP имеет собственный набор атрибутов, определяющих его приоритет и оптимальность. BGP использует алгоритм выбора маршрута, основанный на анализе множества атрибутов, что позволяет определить оптимальный путь для передачи данных. Протокол периодически обновляет маршрутную информацию, обеспечивая актуальное отражение изменений в топологии сети.

Настройка OSPF на маршрутизаторе Cisco выполняется в несколько этапов [15-17]. Активация OSPF осуществляется после перехода в режим конфигурации с использованием команды configure terminal, после чего включается OSPF и назначается идентификатор процесса командой router ospf 1. Устанавливается уникальный идентификатор маршрутизатора (Router ID), служащий для его идентификации в OSPF: network 192.168.1.0 0.0.0.255 area 0. Указываются сети, которые будут участвовать в OSPF, и определяются их маски: network 10.0.0.0 0.255.255.255 area 0.

OSPF использует LSA (Link State Advertisements) для обмена информацией о состоянии соединений между маршрутизаторами. LSA (Link State Advertisements) — это сообщения, используемые в протоколах

маршрутизации для обмена информацией о состоянии соединений между маршрутизаторами в сети. Каждый маршрутизатор строит свою таблицу маршрутизации на основе полученных LSA, используя алгоритм Дейкстры, используемый для нахождения кратчайшего пути от одной вершины графа до всех остальных вершин, для нахождения кратчайшего пути. OSPF поддерживает иерархическую структуру с областями, что позволяет уменьшить объем маршрутизируемой информации и улучшить масштабируемость.

После настройки и активации протоколов было проведено повторное тестирование с использованием утилиты для измерения пропускной способности сетевого соединения. Наблюдалось значительное снижение битрейта, что свидетельствует о влиянии внедренных протоколов на производительность сети (рис. 5).

```
Connecting to host localhost, port 5201
[  5] local ::1 port 34174 connected to ::1 port 5201
[ ID] Interval           Transfer     Bitrate         Retr  Cwnd
[  5]   0.00-1.00   sec  5.61 GBytes  5883857 KBytes/sec    0   1.87 MBytes
[  5]   1.00-2.00   sec  5.60 GBytes  5870139 KBytes/sec    0   2.62 MBytes
[  5]   2.00-3.00   sec  5.64 GBytes  5914824 KBytes/sec    0   3.06 MBytes
[  5]   3.00-4.00   sec  5.62 GBytes  5890071 KBytes/sec    0   3.25 MBytes
[  5]   4.00-5.00   sec  5.57 GBytes  5840044 KBytes/sec    0   3.25 MBytes
[  5]   5.00-6.00   sec  5.50 GBytes  5771872 KBytes/sec    0   3.25 MBytes
[  5]   6.00-7.00   sec  4.93 GBytes  5169496 KBytes/sec    0   3.25 MBytes
[  5]   7.00-8.00   sec  5.60 GBytes  5873409 KBytes/sec    0   3.25 MBytes
[  5]   8.00-9.00   sec  5.58 GBytes  5855830 KBytes/sec    0   3.25 MBytes
[  5]   9.00-10.00  sec  5.59 GBytes  5857022 KBytes/sec    0   3.25 MBytes
- - - - - - - - - - - - - - - - - - - - - - - - -
[ ID] Interval           Transfer     Bitrate         Retr
[  5]   0.00-10.00  sec  55.2 GBytes  5792651 KBytes/sec    0             sender
[  5]   0.00-10.00  sec  55.2 GBytes  5792625 KBytes/sec                  receiver
```

Рис. 5. Проверка с BGP и OSPF

Заключение

Проведенный эксперимент подтвердил, что оптимизация трафика является неотъемлемой частью управления сетевыми ресурсами и должна применяться в целях обеспечения качества обслуживания. Она позволяет не только повысить производительность и надежность сети, но и обеспечить высокий уровень безопасности, что особенно важно в условиях увеличения числа сетевых угроз. На практическом примере была доказана эффективность использования протоколов BGP и OSPF в информационных системах.

В результате решения практической задачи было обнаружено, что при использовании протоколов BGP и OSPF характеристики сетевой производительности значительно улучшились. В первом опыте, где протоколы BGP и OSPF не использовались, средняя скорость передачи данных составила 66238 КБ/с, а ее максимальное значение не превышало 67744 КБ/с. Во втором опыте, в котором были задействованы протоколы BGP и OSPF, средняя скорость передачи данных была равна 579265 КБ/с, а максимальная скорость передачи данных достигла 591482 КБ/с. Оба этих показателя из второго опыта примерно в девять раз выше, чем в первом. Объем переданных данных также существенно различается: в первом опыте за 19 с было передано 13,8 Гб, тогда как во втором за 10 секунд передано 55,2 Гб. На основании этого показателя мы можем сделать вывод о значительном увеличении пропускной способности сети во втором эксперименте по сравнению с первым. То есть, использование протоколов BGP и OSPF позволяет произвести передачу большего объема данных за меньшее время.

В первом эксперименте размер TCP-окна варьировался в диапазоне 1,19-1,37 Мб, а во втором он быстро достиг значения 3,25 МБ и оставался стабильным на этом уровне что свидетельствует о том, что соединение лучше подстраивается под динамически изменяющиеся условия сети и эффективнее использует её возможности. В обоих случаях отсутствуют повторные передачи (Retr = 0), что подтверждает факт стабильности соединения и отсутствия потерь данных. Длительность первого эксперимента составила 19 с, а второго – 10 с. Но несмотря на сокращение времени выполнения, во втором эксперименте удалось передать в четыре раза больше данных благодаря существенно более высокой скорости передачи.

Таким образом во втором опыте произошло значительное увеличение скорости передачи данных, за счет оптимизации параметров TCP-окна и повышения эффективности использования сетевых ресурсов. В то же время результаты первого эксперимента указывают на ограниченную пропускную способность, что может быть обусловлено как особенностями сетевого оборудования, так и конфигурацией сети или параметров настройки протоколов.

Для практического применения результатов исследования рекомендуется использовать протокол OSPF в локальных сетях (LAN), где требуется быстрая адаптация к изменениям топологии и минимизация времени восстановления после сбоев. BGP, в свою очередь, целесообразно применять в глобальных сетях, где необходимо учитывать политику маршрутизации и надежность путей, особенно в условиях множества альтернативных маршрутов.

Кроме того, для достижения максимальной эффективности рекомендуется комбинировать использование этих протоколов с другими методами оптимизации, такими как балансировка нагрузки и сетями доставки контента (CDN) что позволит создать более устойчивую и производительную сетевую инфраструктуру, способную справляться с высокими нагрузками и обеспечивать стабильное качество обслуживания для пользователей и повысить надежность сети [18-27].

Литература

1. *Гадасин Д.В., Вакурин И.С., Цыгулева А.В*. Управление трафиком беспроводной сети с применением сети Петри // Телекоммуникационные и вычислительные системы 2020: Труды международной научно-технической конференции, Москва, 14-17 декабря 2020 г. Московский технический университет связи и информатики. М.: Горячая линия – Телеком, 2020. С. 92-101. EDN WOVZAJ

2. *Кузин И.А., Гадасин Д.В*. Модель контейнера данных для минимизации трафика при передаче субъективных характеристик объектов на изображении трехмерной сцены // Телекоммуникации и информационные технологии. 2021. Т. 8, № 2. С. 96-100. EDN TYFFBH

3. *Шульпина П.Д., Гадасин Д.В., Тремасова Л.А*. Взвешивание признаков как предварительная обработка исходных наборов данных // Системы синхронизации, формирования и обработки сигналов. 2024. Т. 15, № 3. С. 40-47. EDN BIOWRB

4. *Гадасин Д.В., Бессолицын А.Д., Гадасин Д.Д*. Оценка качества данных информационных систем // DSPA: Вопросы применения цифровой обработки сигналов. 2024. Т. 14, № 2. С. 4-12. EDN GYIWJU

5. *Гадасин Д.В., Первухина А.А.* Группировка узлов передачи данных с использованием метода к-средних для создания кластеров // Теория и практика экономики и предпринимательства : Труды XXI Международной научно-практической конференции, Симферополь – Гурзуф, 18-20 апреля 2024 г. Симферополь: ИП Зуева Т. В., 2024. С. 233-236. EDN IAHHLX

6. *Золотарева П.Ю., Гадасин Д.В., Маклачков К.А.* Методы обработки информации в распределенных информационных системах // Тенденции развития Интернет и цифровой экономики : Труды VI Международной научно-практической конференции, Симферополь-Алушта, 01-03 июня 2023 года. Симферополь: ИП Зуева, 2023. С. 187-189. EDN LGONZK

7. *Гадасин Д.В., Шустов С.А.* Исследование эффективности протоколов маршрутизации в условиях сетей с высокой нагрузкой // Теория и практика экономики и предпринимательства: Труды XXI Международной научно-практической конференции, Симферополь – Гурзуф, 18-20 апреля 2024 года. Симферополь: ИП Зуева Т. В., 2024. С. 236-237. EDN WNVEOC

8. *Шведов А.В., Гадасин Д.В., Клыгина О.Г., Тремасова Л.А*. Оптимизация маршрутизации в сети при помощи гамильтонова цикла и марковского процесса принятия решений // DSPA: Вопросы применения цифровой обработки сигналов. 2023. Т. 13, № 3. С. 42-49. EDN BSWDEQ

9. Свидетельство о государственной регистрации программы для ЭВМ № 2023615007 Российская Федерация. Программное приложение «Анализатор актуальности угрозы» ("Threat Relevance Analyzer" – на английском языке) для определения актуальности угроз персональных данных при их обработке в информационных системах персональных данных : № 2023613955 : заявл. 27.02.2023 : опубл. 09.03.2023 / В. А. Докучаев, В. В. Маклачкова, Д. В. Гадасин [и др.] ; заявитель Общество с ограниченной ответственностью Фирма «ТЕЛЕСОФТ». EDN AOOMDG

10. *Гадасин Д.В., Шведов А.В*. Применение транспортной задачи для балансировки нагрузки в условиях нечеткости исходных данных // T-Comm: Телекоммуникации и транспорт. 2024. Т. 18, № 1. С. 13-20. DOI 10.36724/2072-8735-2024-18-1-13-20. EDN WKNPIX

11. *Гадасин Д.В., Вакурин И.С., Тремасова Л.А*. Алгоритм распределения данных между системами хранения на основе свойства самоподобия // Электросвязь. 2024. № 4. С. 44-50. DOI 10.34832/ELSV.2024.53.4.007. EDN BRSLCL

12. *Гадасин Д.В., Кривов Д.А.* Мониторинг трафика в сетях SDN // Телекоммуникационные и вычислительные системы – 2017: Труды международной научно-технической конференции, Москва, 22 ноября 2017 г. М.: Горячая линия – Телеком, 2017. С. 88-89. EDN ZVITBZ

13. *Гадасин Д.В., Шведов А.В., Савкин Д.И*. Проектирование единого информационного пространства в рамках курса лабораторных работ по дисциплине «Принципы построения систем управления базами данных и знаний» // Методические вопросы преподавания инфокоммуникаций в высшей школе. 2023. Т. 12, № 2. С. 14-21. EDN FLOPUM

14. *Пантелеева К.А., Палибза С.А., Гадасин Д.В*. Принципы построения системы управления при возникновении сбоев в ИТ-инфраструктуре // REDS: Телекоммуникационные устройства и системы. 2024. Т. 14, № 2. С. 24-34. EDN MOYCNG

15. *Monkewich O., Sales I., Probert R*. OSPF Efficient LSA Refreshment Function in SDL // Lecture Notes in Computer Science. 2001. Vol. 2078. P. 0300. EDN ATNOHV

16. *Kim Do. H., Tcha D.W*. Scalable domain partitioning in Internet OSPF routing // Telecommunication Systems. 2000. Vol. 15, No. 1-2. P. 113-127. EDN AMSGAX

17. *Гадасин В.А., Гадасин Д.В. Надежность* крупномасштабных сетей связи с аддитивной структурой // Автоматика и телемеханика. 1997. № 1. С. 160.

18. *Гадасин В.А., Гадасин Д.В*. Надежность двухполюсных сетей с аддитивной структурой II. Финальная вероятность связи // Автоматика и телемеханика. 1999. № 10. С. 164-179. EDN OKEMTZ

19. *Яковенко Н.В., Гадасин Д.В., Коцич Л*. Повышение точности коэффициента влияния ошибок в информационных системах с применением метода обратного распространения ошибки // Системы синхронизации, формирования и обработки сигналов. 2024. Т. 15, № 4. С. 35-42. EDN CMFVNH

20. *Гадасин Д.В*. Построение бинарного дерева минимальной цены // T-Comm: Телекоммуникации и транспорт. 2024. Т. 18, № 11. С. 38-44. DOI 10.36724/2072-8735-2024-18-11-38-44. EDN GMCEWG

21. *Гадасин Д.В., Шведов А.В., Кузин И.А.* Трехмерная реконструкции объекта по одному изображению с использованием глубоких свёрточных нейронных сетей // T-Comm: Телекоммуникации и транспорт. 2022. Т. 16, № 7. С. 29-35. DOI: 10.36724/2072-8735-2022-16-7-29-35. EDN: YTLCNW

22. *Shvedov A.V., Gadasin D.V., Alyoshintsev A.V.* Segment routing in data transmission networks // T-Comm: Телекоммуникации и транспорт. 2022. Vol. 16. No. 5, pp. 56-62. DOI: 10.36724/2072-8735-2022-16-5-56-62. EDN: VAYLJQ

23. *Kalmykov N.S., Dokuchaev V.A.* Segment routing as a basis for software defined network // T-Comm: Телекоммуникации и транспорт. 2021. Т. 15. № 7. С. 50-54. EDN: LYVZCV

24. *Dokuchaev V.A., Maklachkova V.V., Statev V.Yu.* Classification of personal data security threats in information systems // T-Comm: Телекоммуникации и транспорт. 2020. Т. 14. № 1. С. 56-60. EDN: QOGYHH

25. *Докучаев В.А., Маклачкова В.В., Статьев В.Ю.* Цифровизация субъекта персональных данных // T-Comm: Телекоммуникации и транспорт. 2020. Т. 14. № 6. С. 27-32. EDN: XVWYJP

26. *Pavlov S.V., Dokuchaev V.A., Mytenkov S.S.* Model of a fuzzy dynamic decision support system // T-Comm: Телекоммуникации и транспорт. 2020. Т. 14. № 9. С. 43-47. EDN: VYFNLB

27. *Гадасин Д.В*., *Тремасова Л.А., Гадасин Д.Д.* Распределение поступающей нагрузки с применением SS-метода // I-methods. 2023. Т. 15, № 3. EDN HQEYTW

ОБЗОР ТЕХНОЛОГИЙ И ПРОТОКОЛОВ ДЛЯ ИНТЕРНЕТА ВЕЩЕЙ

Федькова Александра Александровна
МТУСИ, Москва, Россия,
sashafedkova@gmail.com

Маликова Елена Егоровна
МТУСИ, Кафедра Сетей связи и систем коммутации, к.т.н., доцент, Москва, Россия
e.e.malikova@mtuci.ru

Аннотация
В данной статье проводиться анализ технологий Интернета вещей (IoT), которые в настоящее время нашли широкое применение на различных сетях связи. Описываются основные протоколы передачи данных для данной технологии. Рассмотрены принципы работы датчиков утечки газа. В контексте имитационного моделирования в AnyLogic представлена модель обработки заявок, поступающих от сенсоров.

Ключевые слова
IoT, NFV, SDN, технология ZigBee, протокол MQTT, клиент, сервер, протокол CoAP, датчик утечки газа, элемент, Aqara Smart Natural Gas Detctor, AnyLogic

Введение

В современном мире одним из главных элементов технологического развития – технология Интернет вещей (Internet of Things, IoT) [1, 7, 9], которая состоит из взаимодействующих устройств, включающих датчики, способные на автономную работу. Важным элементом IoT являются датчики, которые играют роль “органов чувств” системы, предоставляя информацию об окружающем мире. Именно датчики помогают предотвратить аварии, защитить здоровье и окружающую среду, обнаруживая отклонения от нормы и сообщая о потенциальных угрозах. Таким образом, обеспечение безопасности становится приоритетной задачей при проектировании и внедрении IoT-решений.

Цель данной статьи – ознакомиться с протоколами взаимодействия устройств и технологий IoT, ознакомиться с принципами работы датчиков утечки газа, а также построить модель в имитационной среде моделирования AnyLogic.

Обзор технологий интернета вещей

Интернет вещей (Internet of Things, IoT) – это сеть, которая объединяет разнообразные информационно-сенсорные устройства и оборудование в единую систему. Эта сеть позволяет осуществлять взаимодействие между людьми, машинами и предметами в любое время и в любом месте. IoT является расширением и экспансией существующей сети, что способствует расширению возможностей Интернета и созданию более сложных и взаимосвязанных систем.

В модели современной сети связи для IoT применяются технологии виртуализации сетевых функций (Network Functions Virtualization, NFV) и программно-определяемых сетей (Software Defined Networks – SDN). Данные технологии реализуют программно-аппаратную абстракцию, обеспечивая динамическую настройку и масштабирование сетевых ресурсов (рис. 1).

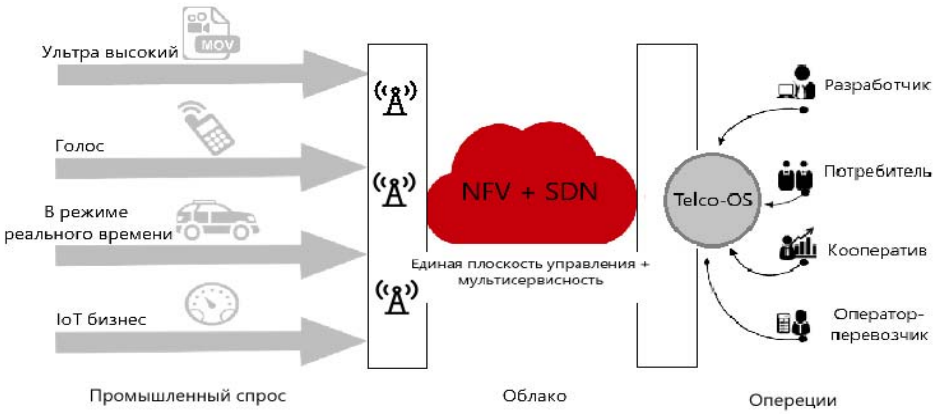


Рис. 1. Модель современной сети связи для IoT и других сервисов

Развитие Интернета вещей характеризуется экспоненциальным ростом разнообразия и количества сервисов, что предъявляет новые требования к сетевой инфраструктуре. Для эффективного управления этой структурой операторы связи все чаще обращаются к NFV и SDN.

NFV, позволяя запускать сетевые функции в виде программного обеспечения на универсальном оборудовании, снижает зависимость от дорогостоящих специализированных устройств и обеспечивает гибкое распределение ресурсов [2, 8]. Этот подход, основанный на аппаратной и программной среде, позволяет оперативно развертывать и масштабировать новые сервисы, в соответствии с меняющимися бизнес-требованиями.

В свою очередь, SDN, представляя инновационную архитектуру на базе протокола OpenFlow, обеспечивает более интеллектуальное и гибкое управление сетевыми ресурсами. Это способствует улучшению управления трафиком и повышению общей эффективности сетевых операций.

В совокупности, эти технологии играют ключевую роль в реализации концепции IoT, представляющей собой динамично развивающуюся сеть, объединяющую различные объекты и обеспечивающую их взаимодействие между собой и с людьми в режиме реального времени.

Развертывание Интернета вещей (IoT) предполагает использование как проводных, так и беспроводных технологий связи [3].

Проводные технологии, основанные на физических кабельных соединениях, обеспечивают передачу данных и электропитания. Примерами таких технологий являются Ethernet, широко применяемый для сетевого подключения вычислительных устройств, и USB, являющийся универсальным интерфейсом для передачи данных и питания периферийных устройств.

Другим типом технологий являются беспроводные, обеспечивающие коммуникацию между устройствами без использования физических кабелей и могут быть классифицированы по дальности действия: технологии дальнего радиуса (например, NB-IoT, LoRa, SigFox) и ближнего радиуса (например, ZigBee, Z-Wave, Bluetooth, Wi-Fi) [4].

Беспроводная связь играет ключевую роль в современной инфраструктуре IoT, позволяя устройствам взаимодействовать на различных расстояниях, обеспечивая гибкость и масштабируемость.

В контексте беспроводных технологий ближнего радиуса действия, особое место занимает ZigBee, разработанная ZigBee Alliance и публично представленная в 2004 году. ZigBee основывается на стандарте IEEE 802.15.4, который определяет протокол локальной сети с низким энергопотреблением. Этимологическая основа названия ZigBee заключается в метафоре “танца пчел”, где вибрации и характерные движения используются для передачи информации о местонахождении ресурса.

Типичная сеть ZigBee, как показано на рисунке 2, включает в себя следующие основные компоненты: Концентратор, который выступает в роли координатора и маршрутизатора трафика, а также конечные устройства ZigBee, оборудование, представляющие собой различные датчики или исполнительные механизмы, взаимодействующие по протоколу ZigBee.

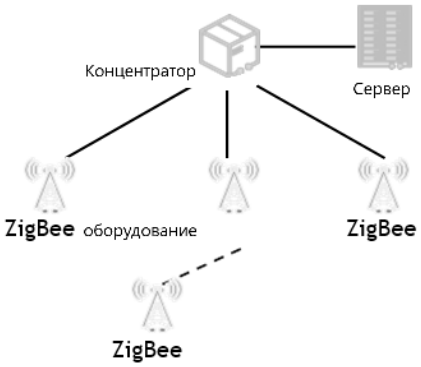


Рис. 2. Схема сети ZigBee

Сеть организована по топологии типа «звезда», где концентратор выступает в качестве центрального узла, а конечные устройства непосредственно подключаются к нему. Концентратор осуществляет управление устройствами, сбор и передачу данных от устройств к другим сетям или системам, обеспечивая тем самым функционирование всей сети.

Технология Zigbee предназначена для обеспечения беспроводного соединения на малых расстояниях, при этом важным фактором является низкое энергопотребление. Архитектура технологии позволяет интегрировать её в различные устройства, что способствует широкому распространению в различных отраслях.

Технологии беспроводной связи ближнего радиуса действия, такие как Wi-Fi, Bluetooth, Z-Wave и

ZigBee, различаются своими техническими характеристиками и целевой направленностью. Выбор наиболее подходящей технологии требует детального анализа требований проекта и условий его реализации. Ключевые факторы, влияющие на выбор, включают дальность действия, пропускную способность, энергоэффективность, стоимость и уровень безопасности. ZigBee отличается от других технологий своей ориентацией на приложения с низким энергопотреблением и малой задержкой, что делает ее предпочтительным выбором для масштабных сенсорных сетей. Wi-Fi, Bluetooth и Z-Wave, напротив, оптимизированы для других сценариев, требующих более высокой пропускной способности или более широкой функциональности.

Протоколы, используемые в технологиях интернета вещей

В контексте Интернета вещей (IoT), где устройства взаимодействуют в гетерогенных сетевых средах, ключевую роль играют протоколы связи, обеспечивающие эффективную передачу данных с учетом ограничений ресурсов и сетевых характеристик. Из часто встречающихся протоколов можно выделить HTTP (Hypertext Transfer Protocol), MQTT (Message Queuing Telemetry Transport), AMQP (Advanced Message Queuing Protocol) и CoAP (Constrained Application Protocol). Каждый из этих протоколов имеет свои индивидуальные характеристики и используются в различных областях, которые соответствуют различным требованиям IoT-приложений.

MQTT и CoAP представляют собой два основных протокола, которые используются в IoT, и характеризуются своими архитектурными особенностями и областями применения.

MQTT (Message Queuing Telemetry Transport) протокол работает на основе транспортного протокола TCP. Применяется для сетей Интернета вещей. MQTT имеет ограниченные вычислительные ресурсы и низкую производительность.

В архитектуре протокола (рис. 3) можно выделить два ключевых элемента: клиент и сервер, который также называют брокером.

Рис. 3. Архитектура «Издатель-Подписчик»

Клиент – это программное обеспечение или устройство, которое использует протокол MQTT для передачи данных. Его ключевые функции:

– установление соединения с сервером;
– публикация данных (в качестве издателя);
– подписка на данные (в роли подписчика);
– отмена подписки;
– завершение соединения с сервером.

Сервер (брокер) функционирует как посредник между клиентами и выполняет следующие функции:

– получение сообщения;
– обработка запросов от клиентов;
– пересылка сообщения на основании подписок;
– завершение подключения.

Для обеспечения гарантированной, безопасной и своевременной доставки информации, сервер задействует систему управления потоками данных в сети MQTT.

Протокол характеризуется простотой реализации, передачей небольшого объема данных, управлением качеством обслуживания (QoS). При этом он не зависим от формата и типа передаваемых данных. Эти принципы обеспечивают гибкость и эффективность протокола в разнообразных сценариях применения.

CoAP (Constrained Application Protocol) является протоколом прикладного уровня, который был создан для работы устройств с ограниченными ресурсами, при этом он обеспечивает низкие накладные расходы и энергопотребляемость. Данный протокол обеспечивает коммуникацию между конечными точками как в пределах одноранговой сети, так и через межсетевое взаимодействие.

CoAP основан на архитектурных принципах REST, но оптимизирован для работы в условиях ограниченных ресурсов. Имеет двоичную систему счисления и многоадресную рассылку по IP-сетям, идеально соответствующий для низко потребляемых приложений.

Схема сети, которая показывает работу устройств с использованием протокола CoAP изображена на рисунке 4. Она разделена на две условные области, изображенные в виде облаков. Первая область включает в

себя два сервера и клиента. Между серверами и клиентом устанавливается соединение по протоколу HTTP, что указывает на использование стандартного веб-протокола в этой части сети. Во второй области расположены сервер, proxy, а также конечные устройства, которые взаимодействуют друг с другом и с другими элементами сети по протоколу CoAP. Устройства представляют собой конечные точки сети, датчики или исполнительные механизмы.

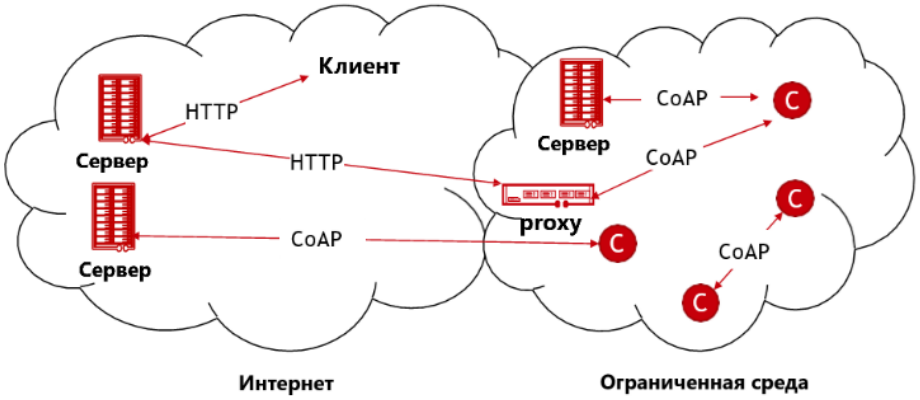


Рис. 4. Схема сети с применением протокола CoAP

Так как современные сети являются гетерогенными, то для разных задач и устройств используются наиболее подходящие протоколы связи.

Принципы работы датчиков утечки газа в интернете вещей

Сенсорные технологии в контексте IoT являются важным элементом в информатизации общества.Технология охватывает разнообразные датчики, предназначенные для измерения параметров окружающей среды, преобразуя полученные данные в унифицированный формат. Затем информация передается на центральный процессор для обработки. Таким образом, системы мониторинга, построенные на основе сенсорных технологий, собирают данные о таких параметрах, как концентрация газов в помещении, температура окружающей среды и влажность воздуха. Данные показатели играют ключевую роль во многих системах управления и мониторинга.

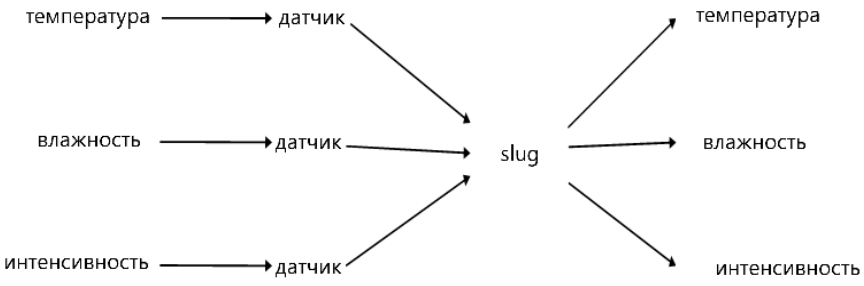


Рис. 5. Схема обработки данных с датчиков в системе мониторинга

Датчики, обладая чувствительными и преобразующими компонентами, осуществляют измерение различных физических параметров в соответствии с установленными алгоритмами, преобразуя их в полезный выходной сигнал. (рис. 6).

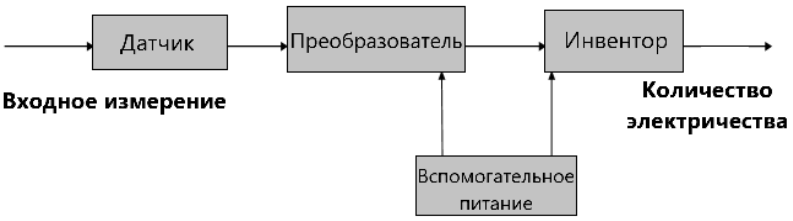


Рис. 6. Схема преобразования сенсорного сигнала

В данной статье мы рассмотрим датчики утечки газа, которые в настоящее время нашли широкое применение на предприятиях общественного питания, больницах, школах и жилых домах. В их функции входит обнаружение повышенных концентраций определенных газов в зданиях и офисах, а также на газопроводах.

Существует множество сенсорных устройств, принципы работы которых отличается от требуемых полученных данных. Так датчики утечки газа можно классифицировать по принципу обнаружения газа.

Рассмотрим основные типы датчиков, которые в настоящее время нашли широкое применение на различных объектах [5]:

1. *Оптические датчики* используют оптические свойства газов для их обнаружения. Например, инфракрасные датчики, которые анализируют спектр поглощения газов в инфракрасном диапазоне. Принцип работы заключается в сравнении интенсивности инфракрасных лучей, прошедших через исследуемую и эталонную среду. Разница в интенсивности пропорциональна концентрации газа.

2. *Термические датчики* используют тепловые эффекты, которые возникают при взаимодействии газа с каталитическими материалами. При контакте газа с катализатором происходит процесс окисление (горения), это приводит к изменению температуры и электрического сопротивления чувствительного элемента.

3. *Электронные датчики* (полупроводниковые) изменяют свои электрические характеристики под воздействием газа. Так, датчики, в составе которых находятся оксиды металлов, благодаря чувствительному элементу, изменяют проводимость при поглощении молекул газа.

Каждый тип датчика обладает различными параметрами чувствительности, точности, скорости срабатывания и устойчивости к внешним воздействиям.

Обычно датчик имеет в своем составе корпус, который защищает его от внешних воздействий, источник питания, чувствительный элемент, измерительный модуль.

Примером датчика, который фиксирует утечку газа и интегрирован в технологию IoT является датчик Aqara Smart Natural Gas Detector [6].

Он использует протокол ZigBee 3.0 для беспроводной связи с центральным хабом или шлюзом умного дома. ZigBee является энергоэффективным и надежным протоколом, что делает его подходящим для применения в сенсорных сетях IoT. Датчик утечки газа, использующий ZigBee, может быть интегрирован с другими устройствами умного дома, что дает возможность создавать автоматизированные системы и повысить уровень безопасности. Основным элементом датчика является чувствительный сенсор, который срабатывает при увеличении концентрации метана в воздухе. Если датчик обнаруживает утечку газа, датчик немедленно активирует встроенную звуковую сирену и мигающий красный светодиод, предоставляя пользователям немедленное предупреждение об опасности.

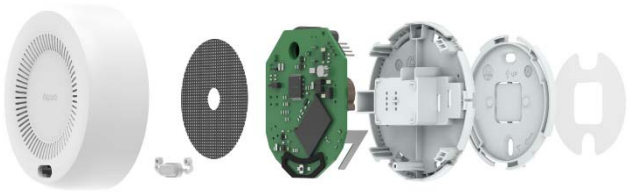


Рис. 7. Датчик Aqara Smart Natural Gas Detector

Моделирование датчиков утечки газа в интернете вещей на примере AnyLogic

Моделирование является важным инструментом для анализа, проектирования и оптимизации сложных систем. AnyLogic, будучи мощной платформой мультиагентного моделирования, предоставляет гибкие возможности для создания реалистичных моделей таких систем.

Рассмотрим конкретный пример создания модели в AnyLogic, где интегрируется структурный и логический анализ, для детального понимания динамики работы системы обнаружения утечки газа.

В качестве примера, модель обработки запросов, поступающих от аварийных датчиков на сервер, где датчики утечки газа, использующие технологию ZigBee и протокол MQTT, передают информацию на центральный координатор. Эта модель наглядно демонстрирует имитацию потока данных от источников до конечных узлов, а также ее пригодность для анализа систем, включающих сложные сетевые взаимодействия.

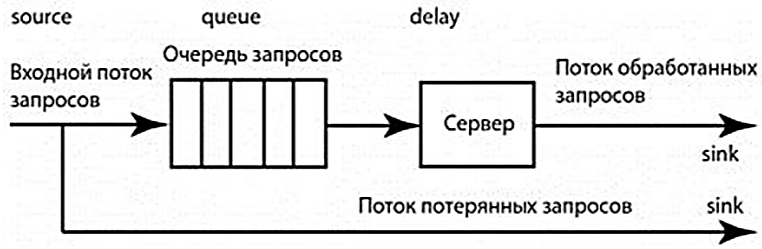


Рис. 8. Структурная схема сети

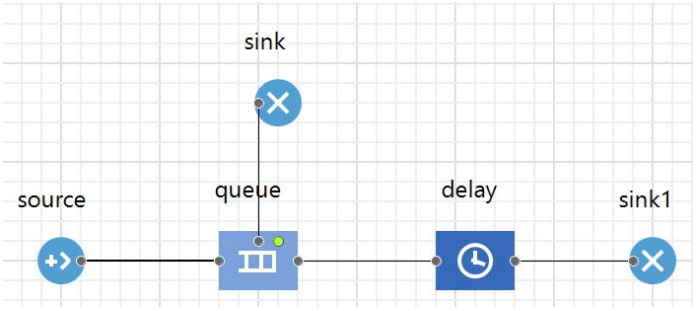


Рис. 9. Логическая схема сети

На рисунке 9 представлена логическая схема работы сети, которая состоит из следующих ключевых элементов:

1. Source (Источник данных): источником данных являются датчики утечки газа, которые передают информацию через определённые временные интервалы. Эти датчики моделируются как генераторы данных, которые регулярно отправляют пакеты, представляющие собой результаты замеров.

2. Queue (Очередь запросов): моделирует буфер, в котором хранятся запросы от датчиков, ожидающие обработки. Это очередь, которая отображает ограниченную пропускную способность системы обработки данных, в частности на этапе маршрутизации.

3. Delay (Задержка обработки): моделирует время, требуемое серверу провайдера для обработки поступивших запросов. Это время включает анализ данных, принятие решения и другие операции на сервере.

4. Sink (Выход данных): Конечная точка в модели, куда поступают обработанные запросы. Запросы, которые не удалось обработать из-за перегрузки или других сбоев, удаляются в “sink”, что моделирует потерю данных в реальной сети.

Использование AnyLogic для моделирования сетей датчиков утечки газа в IoT позволяет интегрировать структурный и логический анализ, создавая реалистичные модели, способные отразить динамику работы системы. Моделирование предоставляет важные сведения для оптимизации архитектуры сети, улучшения производительности, повышения надежности и обеспечения безопасности.

Представим следующую ситуацию: в одном из многоэтажных домов произошла утечка газа, что привело к возгоранию и пожару. Огонь распространился по всему зданию, состоящему из восьми этажей. На каждом этаже установлено по пять датчиков газа, что в общей сложности составляет 40 датчиков, логическая схема представлена на рисунке 10. Эти датчики отправляют пакеты данных каждую секунду.

Сравним работу системы в экстренной ситуации, используя сначала датчики, работающие по технологии Wi-Fi, а затем — датчики, работающие по технологии ZigBee.

С каждого этажа пять датчиков будут отправлять данные по технологии ZigBee объёмом 100 байт. Это означает, что с каждого этажа в секунду будет отправляться пять запросов (агентов). При использовании технологии Wi-Fi длина пакета данных будет 1 килобайт (1000 байт). Это означает, что с каждого этажа(sink) в секунду будет отправляться 50 запросов (агентам).

Блок очереди запросов (queue), ожидающих обработки сервером, может вместить 1000 запросов(агентов). Сервер (delay) обрабатывает 10 запросов(заявок) в секунду.

В ходе первого моделирования будут задействованы датчики умного дома, функционирующие по технологии Wi-Fi. Данные с датчиков будут передаваться напрямую на маршрутизатор без использования хаба. Благодаря оптимизированному для передачи больших объёмов информации технологии Wi-Fi датчики смогут передавать по 50 агентов в секунду с каждого блока source.

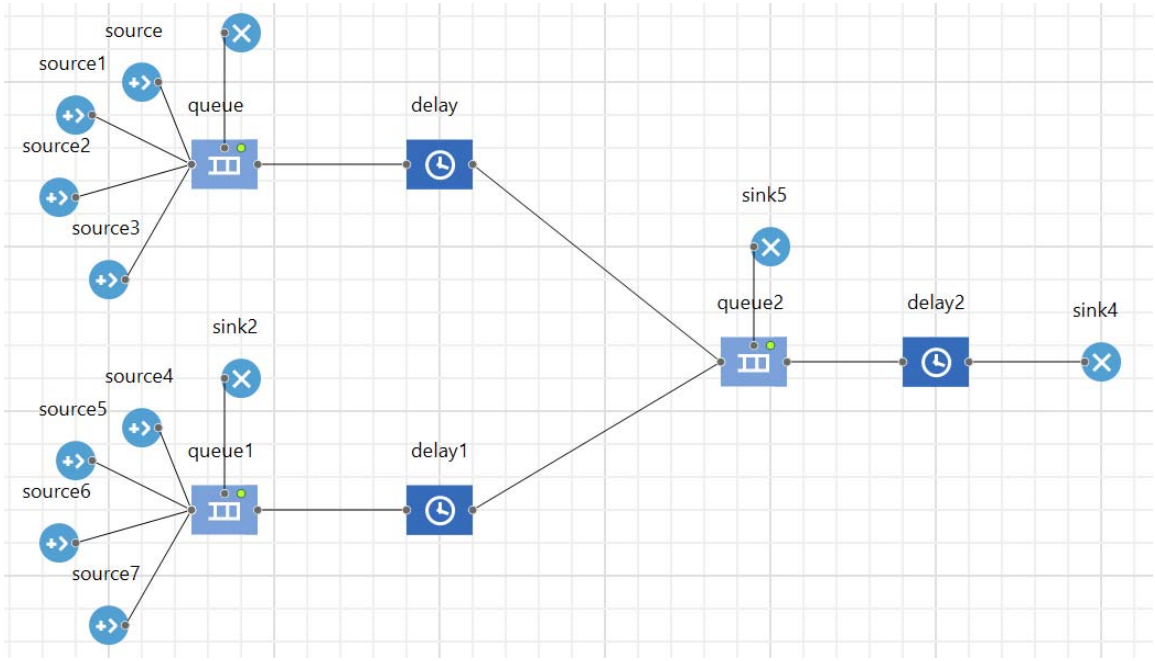


Рис. 10. Итоговая логическая схема

По окончании работы модели, в которой максимально допустимое количество динамически создаваемых агентов составляет 50 000, становится ясно, что сеть перегружена. При достижении 20 000 поступивших агентов сеть теряет способность обрабатывать их в соответствии с увеличением их количества (см. рисунки 11 и 12. Из 50 0027 поступивших заявок обработано 11 000, 6 000 находятся в очереди на обработку, а 33 027 были удалены, что недопустимо в данной ситуации.

Сбой в системе может привести к травмам или даже гибели людей из-за несвоевременного получения информации.

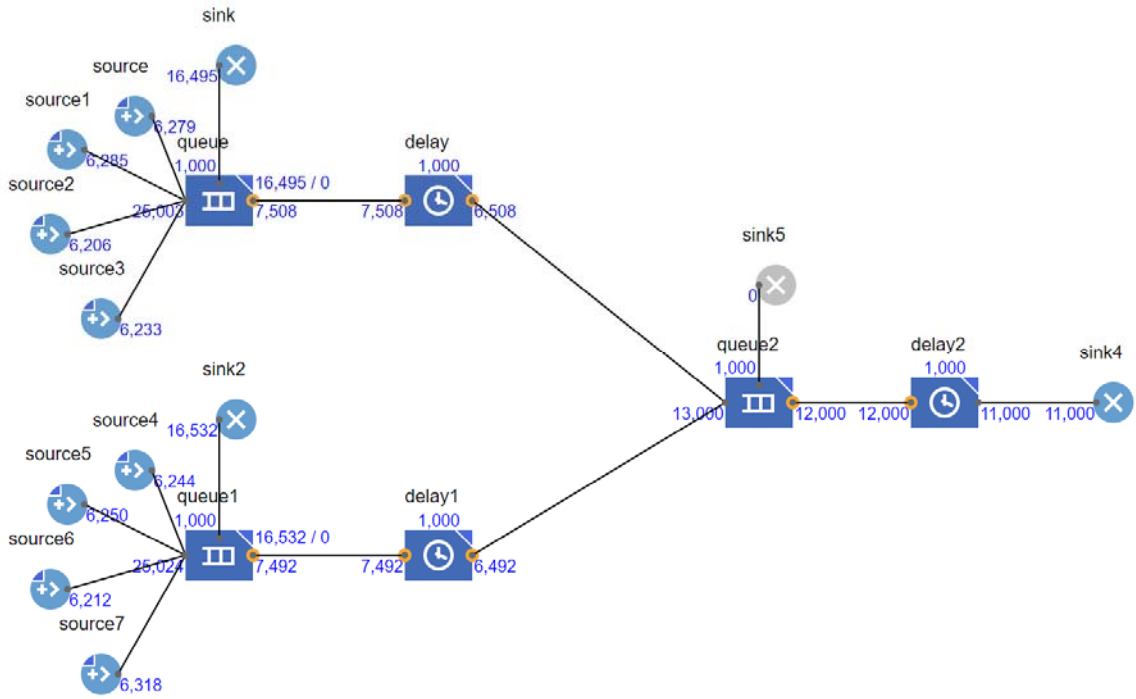


Рис. 11. Работа логической схемы, функционирующая по технологии Wi-Fi

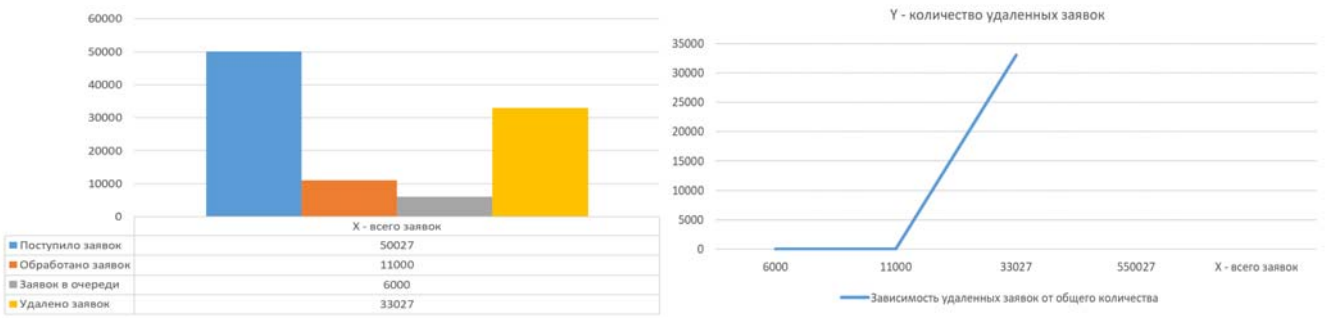


Рис. 12. Результаты моделирования нагрузки на сеть при использовании датчиков, работающих по Wi-Fi технологии

В результате исследования было установлено, что технология Wi-Fi не подходит для использования в системе «умный дом» в многоквартирных зданиях. Из-за большого объёма передаваемой информации сеть может быть перегружена, что может представлять угрозу для безопасности людей.

Второе имитационное моделирование проводилось с использованием датчиков умного дома, работающих по технологии ZigBee. Они передают данные на координатор, который затем отправляет их на маршрутизатор. Благодаря структуре протокола ZigBee, оптимизированного для передачи небольших объёмов информации, датчики будут передавать по пять агентов в секунду с каждого блока source.

После проведения эксперимента с максимальным числом динамических агентов (50 000) становится очевидно, что сеть успешно обрабатывает запросы (рис. 13 и 14). Из общего числа заявок, равных 50 0027, было обработано 49 471, 0 находятся в ожидании обработки и 0 были отклонены.

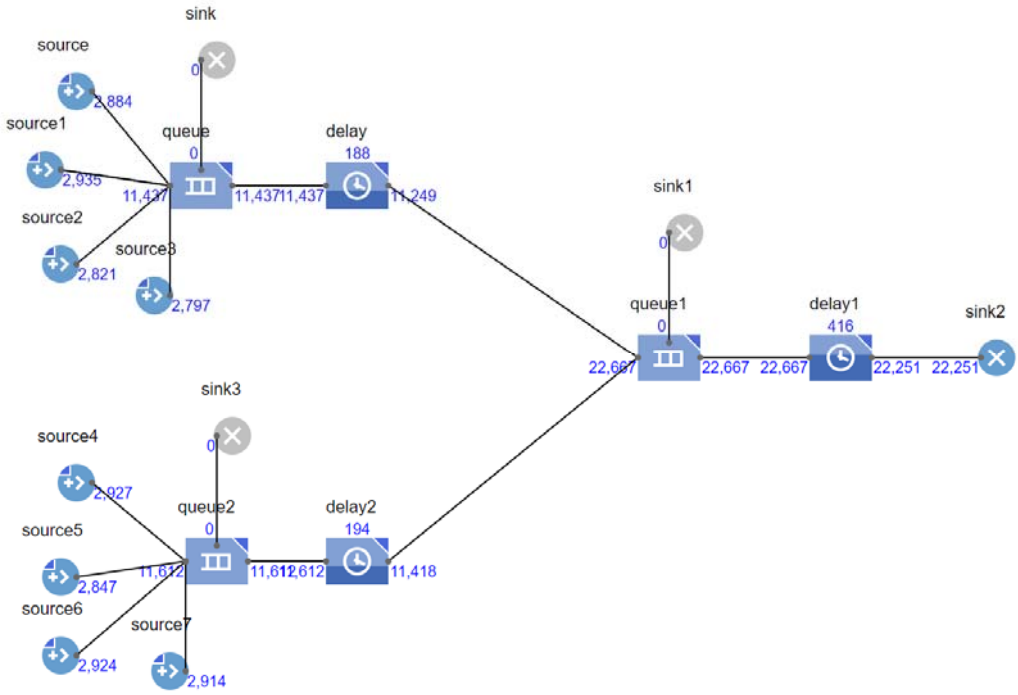


Рис. 13. Работа логической схемы, функционирующая по технологии ZigBee

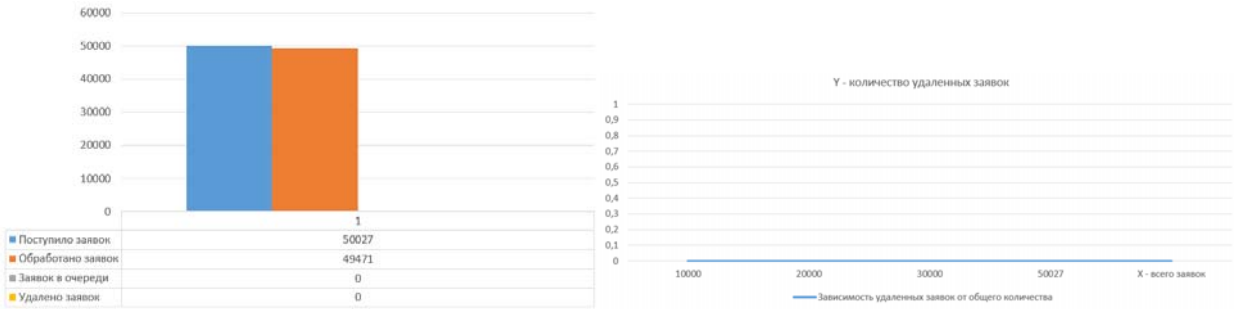


Рис. 14. Результаты моделирования нагрузки на сеть при использовании датчиков, работающих по ZigBee технологии

Моделирование показало, что во втором случае объём полученных данных был таким же, и они были обработаны без потерь.

В связи с этим, учитывая меньшую нагрузку на сеть из-за меньшего объёма передаваемых данных, наиболее эффективным решением будет использование протокола ZigBee. В экстренных ситуациях потеря данных может иметь серьёзные последствия для безопасности людей. Это может привести к несвоевременной реакции экстренных служб и, как следствие, к человеческим жертвам.

Заключение

Интернет вещей (IoT) играет определяющую роль в автоматизации и повышении эффективности производственных процессов, используя разнообразные протоколы обмена данными, которые дают возможность образовывать изменяемые и расширяемые среды, контроль которых может осуществляться в режиме реального времени. Обеспечение безопасности является первостепенным значением в системах IoT, где, в данном контексте, датчики утечки газа играют ключевую роль – являются важным компонентом защиты от аварий. В условиях, где используются горючие и токсичные газы, своевременное обнаружение утечек может предотвратить серьёзные последствия, включая взрывы, пожары и отравления.

Принцип работы датчиков утечки газа основан на использовании сенсорных элементов, реагирующих на уровень концентрации газа, и запуске оповещения при превышении установленного порога.

Для моделирования и анализа работы этих систем применяются специализированные программные инструменты, такие как AnyLogic, что позволяет выявить потенциальные проблемы.

Литература

1. *Ли П.* Архитектура интернета вещей / пер. с анг. М. А. Райтмана. М.: ДМК Пресс, 2019. 454 с.

2. *Смелянский Р.Л.*, *Антоненко В.А*. Концепция программного управления и виртуализации сетевых сервисов в современных сетях передачи данных: учебное пособие. М.: КУРС, 2020. 160 с.

3. *Росляков А.В., Ваняшин С.В., Гребешков А.Ю., Самсонов М.Ю.* Интернет вещей. М.: ПГУТИ, Издательство Ас Гард, 2014. 340 с.

4. *Тихвинский В.О., Коваль В.А., Бочечка Г.С., Бабин А.И.* Сети IoT/M2M: технологии, архитектура и приложения. М.: Издательский дом Медиа Паблишер, 2017. 320 с.

5. Как устроены и работают датчики утечки газа // "Электрик Инфо" URL: https://electrik.info/device/1574-kak-ustroeny-i-rabotayut-datchiki-utechki-gaza.html (дата обращения: 21.01.2025).

6. Умный датчик газа | Aqara Smart Natural Gas Detector // Aqara URL: https://aqara.ru/product/умный-датчик-газа-aqara-smart-natural-gas-detector/ (дата обращения: 21.01.2025).

7. *Боев В.Д.* Компьютерное моделирование: Пособие для практических занятий, курсового и дипломного проектирования в AnyLogic: Спб.: ВАС, 2014. 432 с.

8. *Antonova V.M., Malikova E.E., Stepanov M.S.* Ways of the Asterisk software PBX protection // T-Comm: Телекоммуникации и транспорт. 2023. Т. 17. № 10. С. 52-58.

9. *Antonova V.M., Malikova E.E., Panov A.E., Spichek I.V., Malikov A.Y.* Implementation of IOT technology for data monitoring via cloud services // T-Comm: Телекоммуникации и транспорт. 2021. Т. 15. № 2. С. 46-53.

НОРМИРОВАНИЕ НАДЁЖНОСТИ В ИНФОКОММУНИКАЦИЯХ. ОБЩИЕ ПРИНЦИПЫ И ТИПИЧНЫЕ ОШИБКИ

Нетес Виктор Александрович
МТУСИ, профессор, д.т.н., Москва, Россия
v.a.netes@mtuci.ru

Аннотация
Рассматриваются основные принципы и правила задания количественных требований по надёжности для инфокоммуникационных сетей и систем. Разобраны типичные встречающиеся при этом ошибки. В частности, проанализированы такие вопросы, как определение объекта (предмета рассмотрения), выбор номенклатуры показателей надёжности и норм для них, установление критериев отказа.

Ключевые слова
Инфокоммуникационные сети и системы, нормирование надёжности, стандарты, выбор показателей, коэффициент готовности, коэффициент сохранения эффективности, критерий отказа.

Введение

Важная роль, которую информационные и коммуникационные технологии играют в современном мире, заставляет уделять самое серьёзное внимание обеспечению надёжности соответствующих сетей и систем. Отказы в них могут приводить к весьма тяжким последствиям. Это могут быть значительные экономические потери, угрозы для жизни и здоровья людей. Поэтому в различных нормативных документах устанавливаются требования по надёжности.

Общие принципы и правила задания подобных требований установлены в стандарте [1]. Он входит в систему стандартов «Надёжность в технике» и носит общетехнический (межотраслевой) характер. Поэтому его положения должны применяться и для инфокоммуникационные сетей и систем. К сожалению, в целом ряде документов и публикаций, затрагивающих вопросы нормирования надёжности в инфокоммуникациях, имеют место нарушения установленных этим стандартом правил. Это отражает общее неблагополучное состояние отечественной теории и практики надёжности в настоящее время [2].

Исходя из этого, основные цели этой статьи таковы: привлечь внимание руководителей и специалистов к проблематике нормирования надёжности, сформулировать основные принципы и правила задания требований по надёжности и конкретизировать их применительно к инфокоммуникациям, а также разобрать типичные ошибки в этой области.

Чёткое определение объекта (предмета рассмотрения)

Для предмета рассмотрения в надёжности используется общий термин «объект» [3]. Объект может включать в себя не только аппаратные средства, но и программное обеспечение, и персонал. Детальный анализ этого понятия был представлен в [4]. В инфокоммуникациях объектами могут быть устройства, аппаратура, системы, каналы, тракты, соединения, сети и т.п. Они могут быть не только физическими, но и виртуальными.

При нормировании надёжности в первую очередь следует определять надёжность чего, т.е. какого объекта, рассматривается. При этом должны быть чётко указаны границы этого объекта. Это, казалось бы, очевидное требование, на практике далеко не всегда выполняется, что показывают приведённые далее примеры.

В частности, в [5, 6] приведены требования к коэффициенту готовности для различных типов сетей электросвязи. В их числе сеть междугородной и международной телефонной связи и сеть зоновой телефонной связи. Возникает вопрос: где проходит граница между ними? В самом деле, зоновый узел связи, с одной стороны, является центром зоновой сети, а с другой, при установлении междугородного соединения он выполняет функции междугородного узла связи [7]. Сети передачи данных, как и телефонные сети, могут различаться по масштабу и охватываемой территории. Однако в [5, 6] для них указано только одно требуемое значение коэффициента готовности. Остаётся неясным, к какой ситуации оно относится.

В Стратегии [8] в числе целевых показателей развития отрасли связи присутствует «уровень надёжности (коэффициент готовности) в первичных сетях фиксированной связи». Однако остается непонятным, что имеется под этим в виду. В самом деле, ранее в этом документе отмечается, что первичные сети выделялись в законодательстве, действовавшем до 2003 гола, а в действующих нормативных правовых актах такой объект отсутствует, и это понятие необходимо ввести.

Правда формально продолжает действовать стандарт [9] (хотя он уже, конечно, явно устарел!), и в нём есть понятие первичной сети. При этом выделяются местные первичные сети, внутризоновые первичные сети и магистральная первичная сеть. По всей видимости, показатель в [8] относится к магистральной первичной сети, но явное указание на это отсутствует. Вызывает недоумение также упоминание о фиксированной связи в формулировке показателя. Ведь первичная сеть «образуют транспортную основу для функционирования различных видов сетей связи» [8], в том числе и сетей подвижной связи.

Выбор номенклатуры показателей надёжности

Показатели надёжности служат для количественной оценки свойств, составляющих надёжность. В соответствии с этим они разделяются на показатели безотказности, ремонтопригодности, долговечности и сохраняемости [3]. Кроме того, важную роль играют комплексные показатели, зависящие сразу от нескольких свойств. Таковыми, в частности, являются показатели готовности, зависящие от безотказности и ремонтопригодности. Показатели долговечности и сохраняемости здесь рассматриваться не будут, поскольку применительно к указанным выше видам объектов они имеют смысл только для устройств и аппаратуры.

Основные правила выбора номенклатуры показателей надёжности установлены стандартом [1]. Детальное описание и объяснение лежащих в их основе принципов было дано в [10]. Изложение этих правил приведено в учебном пособии [11]. Однако, несмотря на это, в ряде публикаций и документов встречаются недопустимые отступления от них.

В качестве основного показателя надёжности для объектов непрерывного длительного применения, выполняющих ответственные функции, рекомендуется использовать коэффициент готовности [1]. Большинство объектов, рассматриваемых в инфокоммуникациях, относятся именно к таковым. Поэтому использование коэффициента готовности в [5, 6, 8, 12] вполне оправданно.

Как известно, коэффициент готовности $K_г$ может быть выражен через среднюю наработку на отказ $T_о$, являющуюся показателем безотказности, и среднее время восстановления $T_в$, являющееся показателем ремонтопригодности:

$$K_г = \frac{T_о}{T_о + T_в}. \qquad (1)$$

При этом коэффициент готовности зависит только от отношения $T_в/T_о$, так что одно и то же значение $K_г$ может получаться при различных значениях $T_о$ и $T_в$. Поэтому в дополнение к комплексному показателю ($K_г$) может быть задан один из определяющих его показателей безотказности ($T_о$) или ремонтопригодности ($T_в$). Однако одновременное задание всех трёх показателей не допускается. Это объясняется тем, что любые два показателя, входящие в формулу (1), однозначно определяют значение третьего. К сожалению, автору приходилось видеть документы (технические задания, технические требования, технические условия), в которых были одновременно заданы все три указанных показателя. При этом, что особенно печально, подстановка требуемых значений в (1) иногда не давала верного равенства.

Как обосновано в [10], в дополнение к коэффициенту готовности целесообразно задавать среднюю наработку на отказ, а не среднее время восстановления. Это объясняется тем, что при статистической оценке последнего длительные периоды восстановления могут быть скомпенсированными короткими. Поэтому в случае нормирования $T_в$ разработчик (изготовитель) объекта или поставщик услуги может стремиться сохранять причины отказов, после которых возможно быстрое восстановление. Однако понятно, что это противоречит интересам заказчика (потребителя), которому надо, чтобы отказов было как можно меньше.

Нормируемые показатели надёжности должны выбираться из числа показателей, определения которых приведены в терминологическом стандарте по надёжности. Допускается их конкретизировать и модифицировать, не противореча стандартизированным терминам. Недопустимым является использование в качестве показателей надёжности таких показателей, которые фактически к показателям надёжности не относятся. Такая ошибка допущена, например, в [13]. Это учебное пособие пользуется заслуженной популярностью, за 20 лет было выпущено 6 его изданий. Однако имеющийся в нём небольшой раздел, посвященный надёжности, обладает серьёзными недостатками. В частности, к числу показателей надёжности пакетных сетей там отнесена вероятность потери пакета. Это важный показатель, который действительно надо нормировать, но к числу показателей надёжности он не относится. Заметим, что подобная же ошибка, к сожалению, допущена и в ряде документов международных организаций (МСЭ, 3GPP) [14, 15].

Критерий отказа

Использование показателей безотказности и ремонтопригодности невозможно без задания критерия отказа. В самом деле, как можно говорить о средней наработке на отказ или среднем времени восстановления после отказа, если не определено, что такое отказ. Коэффициент готовности также не имеет смысла в отсутствии критерия отказа. Поэтому в той документации, в которой приведены значения показателей надёжности, следует устанавливать критерии отказов [1]. К сожалению, при задании норм для коэффициента готовности в [5, 6, 12] критерии отказов для различных типов сетей электросвязи и информационных систем не установлены.

С помощью критерия отказа все возможные состояния объекта разделяются на работоспособные и неработоспособные. Во многих Рекомендациях МСЭ-Т их называют состояниями готовности и неготовности соответственно.

Для задания критериев отказа чаще всего используется параметрический подход [16, 17]. Поэтому из двух возможных подходов к определению надёжности (они проанализированы в [18]) в стандарте [3] в качестве основного выбрано параметрическое определение.

При параметрическом задании критерия отказа выбирают один или несколько определяющих параметров, характеризующих функционирование объекта, и для них устанавливаются допустимые области, ограниченные пороговыми значениями. Выход хотя бы одного из параметров за пределы допустимой области означает отказ.

Кроме того, может задаваться и временной порог. В этом случае кратковременный выход параметра за пределы допустимой области не считается отказом [16, 17]. Это позволяет отфильтровать незначительные нарушения в работе объекта. Кроме того, определяющие параметры зачастую имеют статистический характер, поэтому накопление репрезентативной выборки для их оценки требует некоторое время.

Анализ Рекомендаций МСЭ-Т, в которых для различных объектов определены критерии переходов между состояниями готовности и неготовности, т.е. фактически установлены критерии отказа, был предпринят в [19]. Он показал, что во всех Рекомендациях последних лет используется один определяющий параметр и имеется временной порог.

В частности, для пакетных сетей, использующих технологии IP, MPLS и Ethernet, в качестве определяющего параметра берется вероятность потери пакета или кадра. Таким образом, хотя этот параметр, как указывалось выше, сам и не является показателем надёжности, но он используется для задания критерия отказа, необходимого при нормировании надёжности.

В большинстве Рекомендаций МСЭ-Т используется одна и та же схема скользящего 10-секундного окна с односекундной гранулярностью. При этом оценка определяющего параметра осуществляется посекундно, все секунды разделяются на «неплохие», в которых значение параметра является допустимым, и «плохие», в которых значение параметра оказывается недопустимым. Отказом считается появление 10 последовательных «плохих» секунд. Обратный переход (восстановление) фиксируется после 10 последовательных «неплохих» секунд. Применительно к технологии Ethernet эта схема подробно описана в учебном пособии [20].

Надёжность сетей и сложных систем

Особую сложность представляет собой выбор критериев отказа и показателей надёжности для сетей, имеющих много направлений связи. В них возможны ситуации, когда какие-то направления отказали, а остальные остаются работоспособными. Возникает вопрос: как расценивать такие состояния сети? Являются ли они работоспособными или нет? Поэтому может возникнуть вопрос, что же подразумевается под коэффициентом готовности сетей в [5, 6, 8].

В этой связи стоит обратить внимание на стандарт [21]. В нём рассматриваются два сценария оценки надёжности сети и соответственно два варианта определения коэффициента готовности: для отдельных направлений связи (E2E – end-to-end, т.е. из конца в конец по терминологии [21] – между конкретными парами узлов) и для сети в целом. При этом надёжность E2E отражает точку зрения конечных пользователей, а надёжность сети в целом – оператора сети или поставщика услуг на ней.

Поскольку требования к надёжности устанавливаются в интересах конечных пользователей, при этом должен рассматриваться коэффициент готовности для отдельных направлений связи (E2E). В [5] указание на это присутствует, но вот в [6] его нет.

Что же касается определённого в [21] коэффициента готовности сети в целом, то он представляет собой взвешенную сумму коэффициентов готовности для всех направлений связи (пар оконечных узлов). Фактически он является не коэффициентом готовности, а частным случаем другого комплексного показателя надёжности – коэффициента сохранения эффективности [22, 23].

Этот показатель предназначен для оценки надёжности сложных систем, в которых возможны частичные отказы, переводящие систему в состояния промежуточные между полностью работоспособным и неработоспособным [10, 11, 24-27]. При использовании коэффициента сохранения эффективности не требуется формулировать критерий отказа объекта. Вместо этого для него должен быть определён выходной эффект, т.е. полезный результат, получаемый при эксплуатации объекта [1]. Например, при рассмотрении надёжности сети в целом в [21] выходной эффект определяется количеством пользователей, получающих услугу сети.

Вообще, если объект может находиться в частично неработоспособных состояниях, в которые он переходит в результате частичных отказов, и является объектом конкретного назначения, для которого может быть определён выходной эффект, то в соответствии со стандартом [1] основным показателем надёжности для него служит именно коэффициент сохранения эффективности, определение которого приведено в стандарте [3].

Введение этого показателя и разработка для него методов расчёта и оценки – это достижения отечественной школы теории надёжности. В международных стандартах коэффициент сохранения эффективности в общем случае и в явном виде отсутствует. Для некоторых частных случаев он представлен, но, как указывалось выше, в качестве показателя готовности, что не вполне корректно и не раскрывает в полной мере сути этого показателя.

Выбор значений (норм) показателей надёжности

Выбор числовых значений (норм) показателей надёжности должен осуществляться с учётом назначения объекта, достигнутого уровня надёжности и тенденций к его повышению, технико-экономического анализа, реальных возможностей [1]. Для объектов ответственного назначения, отказы которых могут приводить к тяжким последствиям, при выборе норм следует находить разумный компромисс между стремлением иметь очень высокую надёжность и реальными техническими и экономическими возможностями и ограничениями.

В ряде документов международных организаций, принятых в последние годы, (содержание некоторых из них приведено в [7, 28]) задаются очень высокие требования для коэффициента готовности. В некоторых случаях они составляют шесть–восемь девяток. Возможность практического обеспечения и подтверждения столь высокого уровня надёжности вызывает серьёзные сомнения [15, 29].

В российских документах [5, 6, 12] установлены гораздо более низкие требования для коэффициента готовности. Здесь возникают возражения обратного характера, и в некоторых случаях нормы представляются недостаточно высокими [30]. В частности, в [5, 6] норма для сети передачи данных составляет две девятки (0,99). При анализе норм для коэффициента готовности имеет смысл рассматривать соответствующие им значения времени простоя за некоторый период времени: год или месяц. Эти значения можно рассчитать по простым формулам, приведённым, например, в [11]. Для $K_г = 0{,}99$ допустимое время простоя за год составит 87,6 ч, т.е. более 3,5 суток, а за месяц – 7,3 ч, что вряд ли можно считать приемлемым. Отметим, что для других типов сетей электросвязи в [5, 6] заданы более высокие требования – три–четыре девятки.

Норма 0,99 установлена и в [12] для коэффициента готовности информационных систем общего пользования класса I, для менее важных систем класса II она ещё ниже: 0,95. Последнее значение даёт более 18 суток простоя в год или 36,5 ч в месяц. Вряд ли можно считать нормальным, что такая система будет неработоспособна более 2,5 недель за год или более 1,5 суток в месяц.

Заключение

Важная роль, которую инфокоммуникационные сети и системы играют в современном мире, заставляет уделять серьёзное внимание их надёжности. При задании в нормативных документах соответствующих количественных требований необходимо следовать общим правилам, установленным в стандартах системы «Надёжность в технике».

В данной работе эти правила конкретизированы применительно к инфокоммуникациям, проведён анализ действующих документов и публикаций на предмет соответствия им. Основные выводы таковы.

1. Необходимо чётко определять объект, для которого требования устанавливаются. Для него должны указываться границы, условия функционирования и т.п.

2. Показатели надёжности следует выбирать из числа показателей, определенных в терминологическом стандарте по надёжности. Допускается их конкретизация и модификация, не противоречащая сути.

3. Основной показатель надёжности для ответственных объектов непрерывного длительного применения – коэффициент готовности. В дополнение к нему можно задавать среднюю наработку на отказ. Среднее время восстановления при нормировании надёжности использовать не следует.

4. При использовании этих показателей должен быть задан критерий отказа. Для этого целесообразно

использовать однопараметрический критерий с временным порогом.

5. Для сложных систем, в которых могут быть частичные отказы, предпочтительно использовать коэффициент сохранения эффективности. При этом критерий отказа объекта не формулируется, но должен быть выбран выходной эффект.

6. При задании числовых значений показателей важно не допускать их необоснованного занижения или завышения. Для этого надо учитывать как последствия отказов, так реальные возможности и ограничения. При выборе норм для коэффициента готовности стоит рассматривать соответствующие значения времени простоя за год или месяц.

Литература

1. ГОСТ 27.003-2016. Надёжность в технике. Состав и общие правила задания требований по надёжности.

2. *Тарасьев Ю.И., Шпер В.Л.* Мысли о надёжности: в каком состоянии она сегодня // Методы менеджмента качества. 2025. № 1. С. 54-59.

3. ГОСТ Р 27.102-2021. Надёжность в технике. Надёжность объекта. Термины и определения.

4. *Нетес В.А.* Объект в надежности: определение и содержание понятия // Надежность. 2019. Т. 19. № 4. С. 3-7.

5. ГОСТ Р 53111-2008. Устойчивость функционирования сети связи общего пользования. Требования и методы проверки.

6. Требования к организационно-техническому обеспечению устойчивого функционирования сети связи общего пользования. Утверждены приказом Министерства цифрового развития, связи и массовых коммуникаций РФ от 25.11.2021 г. № 1229.

7. *Пшеничников А.П., Росляков А.В.* Будущие сети. Учебник для вузов. М.: Горячая линия – Телеком, 2022. 256 с.

8. Стратегия развития отрасли связи Российской Федерации на период до 2035 года. Утверждена распоряжением Правительства РФ от 24.11.2023 г. № 3339-р.

9. ГОСТ 22348–86. Сеть связи автоматизированная единая. Термины и определения.

10. *Дзиркал Э.В.* Задание и проверка требований к надёжности сложных изделий. М.: Радио и связь, 1981. 176 с.

11. *Нетес В.А.* Основы теории надёжности. Учеб. пособие для вузов. М.: Горячая линия – Телеком, 2019. 102 с.

12. Требования по обеспечению целостности, устойчивости функционирования и безопасности информационных систем общего пользования. Утверждены приказом Министерства связи и массовых коммуникаций РФ от 25.08.2009 г. № 104.

13. *Олифер В., Олифер Н.* Компьютерные сети. Принципы, технологии, протоколы: Юбилейное [6-е] изд. СПб: Питер, 2023. 1008 с.

14. *Netes V.* Modern network technologies and dependability // Proc. of the 3d Intern. Science and Technology Conf. “Modern Network Technologies – 2020”. Moscow, 2020, pp. 104-113.

15. *Netes V.* Ultra-reliable communications: basic concepts, challenges and open issues // Conf. Proc. 2023 Systems of Signals Generating and Processing in the Field of on Board Communications, Moscow, 2023, pp. 1-6.

16. *Нетес В.А.* Критерий отказа и подходы к его определению // Методы менеджмента качества. 2017. № 2. С. 50-54.

17. *Netes V.* Failure criteria and time over thresholds in them // Reliability: Theory & Applications. 2022. Vol. 17. No 4. P. 35-42.

18. *Нетес В.А., Тарасьев Ю.И., Шпер В.Л.* Как нам определить что такое «надёжность» // Надёжность. 2014. № 4. С. 3-25.

19. *Netes V.* Failure criteria and the relationship between quality of service and dependability in telecommunications // Proc. of the 5th Intern. Science and Technology Conf. “Modern Network Technologies – 2024”. Moscow, 2024. P. 109-116.

20. *Нетес В.А.* Ethernet операторского класса. Учеб. пособие для вузов. М.: Горячая линия – Телеком, 2023. 128 с.

21. ГОСТ Р 27.018–2021 (МЭК 62673:2013). Надёжность в технике. Методы оценки и обеспечения надёжности коммуникационной сети.

22. *Нетес В.А.* Надёжность сетей связи в стандартах МЭК // Вестник связи. 2014. № 2. С. 13-15.

23. *Netes V.* Dependability measures for access networks and their evaluation // Proc. of the 26th Intern. Conf. of Open Innovations Association FRUCT. 2020. P. 352–358.

24. *Нетес В.А.* Коэффициент сохранения эффективности – показатель надёжности сложных систем // Надежность. 2012. № 4. С. 14-23.

25. *Нетес В.А.* Использование коэффициента сохранения эффективности для оценки надёжности инфокоммуникационных сетей и систем // Сб. тр. XIV Междунар. отраслевой науч.-техн. конф. «Технологии информационного общества». М.: ИД Медиа Паблишер, 2020. С. 294-296.

26. *Нетес В.А.* Коэффициент сохранения эффективности и его стандартизация // Надёжность. 2021. Т. 21. № 2. С. 3-8.

27. *Netes V.* Effectiveness retention ratio and multistate systems // Reliability: Theory and Applications. 2021. Vol. 16. No 4. P. 94-104.

28. *Росляков А.В.* СЕТЬ 2030: архитектура, технологии, услуги. – М.: ООО «ИКЦ «Колос-с», 2022. 278 с.

29. *Нетес В.А.* Концепция МСЭ-Т «Сеть 2030»: проблемные точки // Сб. тр. XVII Междунар. отраслевой науч.-техн. конф. «Технологии информационного общества». М.: МТУСИ, 2023. С. 137-139.

30. *Нетес В.А.* О нормативных требованиях к надёжности сетей электросвязи // Вестник связи. 2022. № 5. С. 6-9.

АНАЛИЗ СИСТЕМ ГИДРОСФЕРНОЙ СВЯЗИ

Фролов Алексей Андреевич
МТУСИ, доцент кафедры Радиотехнические системы, к.т.н., Москва, Россия
a.a.frolov@mtuci.ru

Томилин Илья Андреевич
МТУСИ, аспирант, Москва, Россия
ilatomilin78@gmail.com

Аннотация
Статья посвящена анализу современных систем гидросферной связи, включая оптические, гидроакустические и гибридные решения. Рассмотрены их преимущества и ограничения, а также перспективы применения в подводной среде. Особое внимание уделено гибридной системе IVA S/W, сочетающей радиосвязь и гидроакустику, которая демонстрирует высокую эффективность в сложных условиях. Обсуждаются технические вызовы, такие как увеличение дальности и скорости передачи данных, минимизация энергопотребления и адаптация к изменяющимся условиям среды. Статья подчеркивает важность дальнейших исследований для развития технологий подводной связи.

Ключевые слова
Гидросферная связь, оптические системы подводной связи, гидроакустическая связь, электромагнитные сигналы, гибридные системы, гидроакустический канал.

Введение

В условиях стремительного развития технологий и возрастающей потребности в надёжных средствах передачи информации в сложных средах, системы гидросферной связи [1-9] приобретают особую значимость. Эти системы, обеспечивающие передачу данных через водную среду, становятся ключевым инструментом в решении задач, где традиционные методы связи оказываются неэффективными или неприменимыми. Актуальность исследований в области гидросферной связи обусловлена не только теоретическим интересом, но и практической необходимостью, связанной с расширением человеческой деятельности в подводных и околоводных условиях.

Гидросферная связь находит широкое применение в различных научных и прикладных сферах. В океанологии она используется для мониторинга состояния морской среды, изучения динамики океанических процессов и анализа биоразнообразия. В подводной робототехнике такие системы обеспечивают управление автономными необитаемыми аппаратами (АНПА), которые применяются для исследования морского дна, поиска полезных ископаемых и проведения спасательных операций. В военно-морской области гидросферная связь является критически важной для координации действий подводных лодок и других подводных объектов.

Рис. 1. Пример использования гидросферной связи

Особое значение системы гидросферной связи приобретают в контексте освоения шельфовых и глубоководных месторождений полезных ископаемых. В условиях растущего спроса на энергоресурсы и минеральное сырьё, разработка технологий, обеспечивающих надёжную связь в подводной среде, становится одной из приоритетных задач. Кроме того, экологические вызовы, такие как загрязнение океанов, изменение климата и разрушение морских экосистем, требуют внедрения современных систем мониторинга, основанных на гидросферной связи.

Однако разработка и внедрение таких систем сопряжены с рядом технических сложностей. К ним относятся затухание сигнала, многолучевое распространение, влияние шумов и ограниченная пропускная способность каналов связи. Эти факторы делают анализ и оптимизацию систем гидросферной связи важной научной задачей, требующей междисциплинарного подхода и применения современных методов моделирования и экспериментальных исследований.

Таким образом, системы гидросферной связи представляют собой не только перспективное направление научных изысканий, но и важный практический инструмент, необходимый для решения широкого круга задач в области освоения водных ресурсов, экологического мониторинга и обеспечения безопасности. Дальнейшее развитие этой области открывает новые горизонты для исследований и технологических инноваций, что подчеркивает её актуальность и значимость в современном научно-техническом ландшафте.

Анализ существующих систем гидросферной связи

Основная часть статьи посвящена детальному анализу современных гидросферных систем связи, которые играют ключевую роль в решении задач передачи данных в подводной среде. Рассматриваются три основных типа систем: оптические, гидроакустические и гибридные. Оптические системы обеспечивают высокую скорость передачи данных на коротких расстояниях, но ограничены затуханием сигнала в мутной воде. Гидроакустические системы, напротив, эффективны на больших дистанциях, но сталкиваются с проблемами задержки и низкой пропускной способности. Гибридные системы, такие как IVA S/W, объединяют преимущества обеих технологий, что позволяет преодолевать ограничения каждой из них. В статье также обсуждаются технические аспекты, результаты испытаний и перспективы развития этих систем.

Оптические системы гидросферной связи

Оптические системы подводной связи используют электромагнитные волны в видимом или ближнем инфракрасном диапазоне для передачи информации. Основными компонентами таких систем являются источник света, модулятор, приёмник и оптическая среда. Источником света обычно служат лазеры или светодиоды (LED), которые генерируют световые сигналы. Лазеры, благодаря своей когерентности и высокой направленности, обеспечивают более высокую эффективность передачи данных на большие расстояния, тогда как светодиоды, обладая меньшей стоимостью и энергопотреблением, чаще применяются в системах с ограниченными ресурсами.

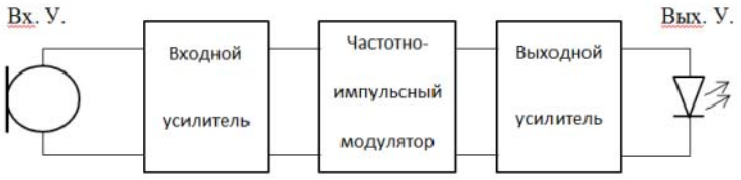


Рис. 2. Упрощенная структурная схема оптического передатчика

Модулятор кодирует информацию в световой сигнал, используя различные методы модуляции, такие как амплитудная (OOK), частотная (FSK) или фазовая (PSK) манипуляция. Приёмник, состоящий из фотодиодов или других детекторов, преобразует световые сигналы в электрические. Оптической средой для передачи сигнала является вода, через которую распространяется свет.

Световые сигналы в воде распространяются с высокой скоростью, что позволяет достичь скоростей передачи данных до нескольких гигабит в секунду (Гбит/с) на коротких расстояниях. Однако распространение света в воде сопровождается значительным затуханием, которое зависит от длины волны, мутности воды и наличия растворённых веществ. Например, в чистой морской воде минимальное затухание наблюдается на длинах волн около 450-550 нм (синий и зелёный свет), что делает эти диапазоны наиболее предпочтительными для подводной оптической связи.

Несмотря на значительные преимущества, оптические системы подводной связи сталкиваются с рядом

серьёзных ограничений. Затухание сигнала в воде, особенно в мутной или насыщенной взвешенными частицами среде, может достигать нескольких децибел на метр, что ограничивает дальность связи до нескольких метров. Например, в прибрежных водах с высокой мутностью затухание может достигать 20-30 дБ/м, что делает передачу данных на расстояния более 10 метров практически невозможной.

Многолучевое распространение, вызванное отражением света от поверхности воды, дна и других объектов, создаёт множество путей распространения сигнала, что приводит к интерференции и искажениям. Это явление особенно выражено в мелководных районах, где отражения от дна и поверхности воды создают сложную интерференционную картину.

Прозрачность воды, наличие планктона, взвешенных частиц и других факторов значительно влияют на качество связи. Например, в водах, насыщенных фитопланктоном, затухание сигнала может увеличиваться в несколько раз, что делает передачу данных крайне затруднительной.

$$L(h) = L_0 \exp(-\varepsilon h)$$

где L_0 – интенсивность оптического луча в начальный момент времени; ε – коэффициент затухания, представляющий собой сумму показателя рассеяния и показателя поглощения водной среды, $м^{-1}$; h – расстояние, пройденное оптическим лучом, м.

Ограниченная дальность связи является одной из основных проблем оптических систем. В чистой морской воде дальность оптической связи обычно не превышает 100–200 метров, что делает её непригодной для задач, требующих передачи данных на большие расстояния.

Оптические системы подводной связи находят применение в различных областях, включая подводную робототехнику, научные исследования и военные применения. В подводной робототехнике они используются для управления автономными аппаратами на коротких дистанциях, где требуется высокая скорость передачи данных. В научных исследованиях оптические системы применяются для передачи данных с подводных датчиков и камер в режиме реального времени. В военных целях они обеспечивают скрытную связь между подводными объектами.

Например, в 2019 году исследователи из Массачусетского технологического института (MIT) разработали систему подводной оптической связи, которая смогла предавать необходимые данные при скорости 2,2 Мбит/с на рсстояние до 10 метров при замутненной воде. В 2021 году компания Sonardyne официально показала систему, которая базируется на методе передачи данных при помощи синего света, BlueComm, обеспечивающую стабильную передачу данных на скорости 10 Мбит/с на внушительное расстояние в 150 метров при условиях чистой водной среды.

Рис. 3. Оптический подводный модем BlueComm

Гидроакустические системы связи

Гидроакустические системы представляют собой сложные технические комплексы, предназначенные для сбора, обработки и передачи информации в подводной среде. Гидроакустические системы демонстрируют уникальные эксплуатационные свойства, детерминированные совокупностью инженерно-технических решений и физическими особенностями акваторий. Ключевыми отличительными чертами выступают повышенные весо-размерные показатели, высокая степень структурной сложности, а также стохастическая локализация модулей на придонных участках. Существенную роль в модификации их функционала играет полиморфизм гидросферы, проявляющийся в вариабельности химического состава, термодинамических параметров, аэродинамических возмущений поверхностного слоя, хаотичности течений и метеоклиматических колебаний, что индуцирует необходимость адаптивного подхода к проектированию.

Прагматическая ценность данных устройств артикулируется их интеграцией в мультидисциплинарные сферы деятельности: организацию подводной телекоммуникации, обеспечение координации перемещений субмарин, проведение батиметрических исследований и создание комплексных мониторингово-аналитических платформ. Экспансия их применения детерминирована способностью преодолевать ограничения, накладываемые непрозрачностью жидкой среды для электромагнитного излучения, что позиционирует гидроакустику как доминирующую технологию в решении задач подводной телеметрии и сбора гидрофизических данных. Эти системы играют ключевую роль в обеспечении эффективного взаимодействия между подводными объектами, а также в решении задач, связанных с исследованием и освоением океанических ресурсов.

Динамика распространения звуковых колебаний в водной толще находится в прямой зависимости от физико-химических параметров окружающей среды, включая её массовую плотность (ρ) и коэффициент упругости (E), а в случае жидких сред — от их способности к деформации под давлением (χ). Среднее значение скорости звука в водной среде приближается к отметке 1500 метров в секунду, однако данный параметр не является постоянным и может отклоняться в пределах от 1450 до 1550 м/с, что обусловлено вариациями таких факторов, как концентрация солей и температурный режим. Плотность морской воды, как правило, стабилизируется на уровне приблизительно 1030 килограммов на кубический метр.

$$c = \sqrt{\frac{E}{\rho}} = \sqrt{\frac{1}{\chi\rho}}$$

В области подводной акустики спектр применяемых частот охватывает интервал от 10 герц до 1 мегагерца, что соответствует временным промежуткам от 0,1 секунды до 1 микросекунды. Определение оптимальной частоты обусловлено спецификой решаемых задач и регулируется двумя ключевыми аспектами: степенью поглощения звуковых колебаний, которая возрастает с увеличением частоты, и характером отражения сигнала от объекта, который теряет свою интенсивность при уменьшении габаритов цели по сравнению с длиной акустической волны.

На скорость распространения звука в водной среде существенное влияние оказывают такие параметры, как уровень минерализации (солёность) и температурные условия. Увеличение солёности приводит к росту плотности воды и снижению её сжимаемости, что, в свою очередь, увеличивает скорость звука. Например, изменение солёности на 1 % вызывает увеличение скорости звука примерно на 1,3 м/с. Температура также играет важную роль: при температуре 5°C увеличение температуры на 1°C приводит к росту скорости звука на 4,5 м/с. Эти параметры необходимо учитывать при проектировании и эксплуатации гидроакустической аппаратуры.

Подводный акустический канал передачи данных функционирует как среда распространения сигналов, несущих информацию. В архитектуре современных цифровых коммуникационных систем выделяют базовые элементы: генератор исходных данных, модуль преобразования сигналов, излучатель, физическую среду передачи и приёмный комплекс. Устройство-источник генерирует сведения, которые могут быть представлены в аналоговой или цифровой форме. Тем не менее, вне зависимости от формата, требуется конвертация данных в высокоэффективный цифровой код для минимизации потерь при транспортировке. После этапа компрессии и кодирования информация поступает в излучатель, где осуществляется формирование устойчивого к помехам сигнала через процедуры помехоустойчивого кодирования и модуляции. Канал передачи, будучи физическим проводником, подвергает сигнал воздействию множества деструктивных факторов: аддитивных шумовых помех, наложения символов (ISI) и амплитудного затухания, что провоцирует деградацию и частичную утрату данных. На стороне приёмника реализованы алгоритмы синхронизации и демодуляции, обеспечивающие реконструкцию исходного сообщения.

Гидроакустический канал связи характеризуется рядом специфических особенностей:

1. Суженный спектр частот, благодаря чему достигается дальнодействие коммуникации, но ограничивается пропускная способность.

2. Выраженные доплеровские эффекты, проявляющиеся даже при незначительном смещении объектов относительно траектории сигнала.

3. Минимальная частотная когерентность, создающая барьеры для передачи сигналов с широким спектром.

4. Низкая временная стабильность канала, вынуждающая внедрять механизмы частой ресинхронизации.

5. Динамическая рефракция волн, сочетающаяся с рассеиванием энергии, что усиливает деформацию и фрагментацию сигнала.

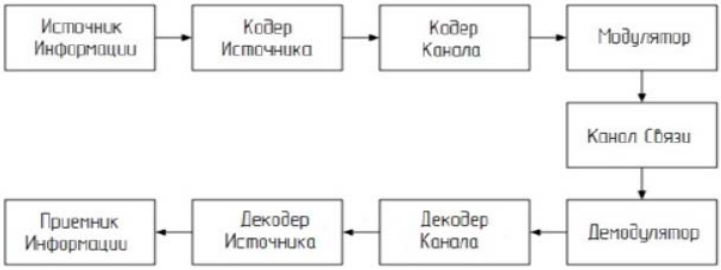


Рис. 4. Простейшая схема функционирования гидроакустического канала связи

Синтез гидроакустической и оптической систем связи представляет собой инновационный подход к решению задач передачи данных в подводной среде. Такая гибридная система объединяет преимущества обеих технологий, компенсируя их недостатки, и создаёт универсальное решение для широкого спектра применений. Гидроакустические технологии, несмотря на свою способность передавать информацию на значительные расстояния, сталкиваются с ограничениями в скорости передачи данных и высокой задержкой. Оптические системы, напротив, обеспечивают высокую скорость передачи данных и низкую задержку, но их эффективность снижается на больших расстояниях и в условиях мутной воды. Гибридная система, сочетающая в себе преимущества обоих подходов, позволяет использовать оптический канал для высокоскоростной передачи на коротких дистанциях и гидроакустический – для передачи данных на большие расстояния, что делает её универсальной и эффективной в различных условиях.

Гибридная система гидросферной связи

Гибридная система связи состоит из нескольких функциональных блоков, которые взаимодействуют между собой для обеспечения надёжной передачи данных. Основные блоки включают источник информации, блок обработки данных, передатчик, канал связи, приёмник, блок синхронизации и обработки сигналов, а также блок помехоустойчивого кодирования. Устройство, генерирующее данные, создаёт информационный поток, который может быть представлен как в дискретной, так и в непрерывной форме. Вне зависимости от исходного формата, данные подвергаются преобразованию в цифровой вид для последующей обработки. Блок обработки информации выполняет сжатие данных и их подготовку к передаче, а также определяет, какой канал связи (оптический или гидроакустический) будет использоваться в зависимости от условий окружающей среды и характеристик передаваемых данных.

Передатчик включает два модуля: оптический и гидроакустический. Оптический модуль использует лазеры или светодиоды для генерации световых сигналов, а данные модулируются с использованием методов, таких как амплитудная (OOK) или фазовая (PSK) манипуляция. Гидроакустический модуль преобразует данные в акустические сигналы с использованием частотной (FSK) или фазовой (QPSK) модуляции. Канал связи представляет собой физическую среду (воду), через которую передаются сигналы. Оптический канал используется для передачи данных на короткие расстояния, а гидроакустический — для передачи на большие дистанции.

Приёмник также включает два модуля: оптический и гидроакустический. Оптический модуль использует фотодиоды для приёма световых сигналов и их демодуляции, а гидроакустический модуль использует гидрофоны для приёма акустических сигналов и их демодуляции. Блок синхронизации и обработки сигналов обеспечивает синхронизацию между передатчиком и приёмником, а также выполняет обработку сигналов для компенсации искажений, вызванных затуханием, многолучевым распространением и шумами. Блок помехоустойчивого кодирования использует коды, такие как коды Рида-Соломона или коды Голея, для исправления ошибок, возникающих при передаче данных, что повышает надёжность передачи, особенно в условиях сильных помех.

Функционирование системы начинается с генерации и подготовки данных. Источник информации генерирует данные, которые поступают в блок обработки. Данные сжимаются и преобразуются в цифровой формат. Затем блок обработки анализирует условия среды (прозрачность воды, расстояние, уровень шумов) и определяет, какой канал связи будет использоваться. Если условия позволяют, данные передаются через оптический канал для обеспечения высокой скорости и низкой задержки. Если оптический канал недоступен (например, из-за мутности воды), данные передаются через гидроакустический канал. Приёмник получает сигналы через соответствующий модуль (оптический или гидроакустический), а блок синхронизации и обработки сигналов компенсирует искажения и восстанавливает исходные данные. Блок помехоустойчивого кодирования исправляет ошибки, возникшие при передаче данных, что повышает надёжность системы.

Преимущества гибридной системы заключаются в компенсации ограничений каждой технологии. Оптический канал обеспечивает высокую скорость передачи данных на коротких расстояниях, а гидроакустический – передачу на большие дистанции. Это повышает надёжность передачи данных, так как в условиях, где один из каналов может быть нарушен, второй канал обеспечивает резервный путь передачи данных. Система также адаптируется к условиям среды, автоматически переключаясь между каналами в зависимости от условий, что позволяет оптимизировать передачу данных. Эффективное использование ресурсов достигается за счёт использования оптического канала для передачи критически важных данных, а гидроакустического – для менее срочной информации.

С этической точки зрения гибридная система минимизирует экологическое воздействие, используя оптический канал в зонах с высокой чувствительностью к акустическим волнам. Оптические системы также обеспечивают более высокую степень конфиденциальности, так как световые сигналы сложнее перехватить. С экономической точки зрения разработка гибридной системы требует значительных инвестиций, но такие затраты могут быть оправданы за счёт повышения эффективности и снижения эксплуатационных расходов. Гибридная система позволяет снизить затраты на передачу данных за счёт оптимизации использования ресурсов.

Система подводной радиосвязи

Подводная связь, основанная на использовании радиоволн, является активно развивающейся областью исследований, направленной на преодоление ограничений, присущих традиционным гидроакустическим методам передачи данных. В отличие от акустических сигналов, которые подвержены значительному затуханию, многолучевому распространению и зависимости от гидрологических условий, радиоволны, особенно в низкочастотном диапазоне, демонстрируют способность проникать через водную среду с относительно низкими потерями. Однако применение радиоволн в подводной связи сопряжено с рядом технических сложностей, обусловленных высокой проводимостью морской воды, что приводит к существенному затуханию электромагнитных сигналов.

Основной принцип работы подводных радиосистем основан на использовании низкочастотных электромагнитных волн (от 3 до 300 кГц), которые способны проникать через воду на глубину до нескольких десятков метров. В отличие от высокочастотных сигналов, низкочастотные волны меньше подвержены затуханию в проводящей среде, такой как морская вода. Передача данных осуществляется за счёт модуляции сигнала, например, с использованием частотной (FSK) или фазовой (PSK) манипуляции. Приёмник, оснащённый магнитной антенной, регистрирует изменения электромагнитного поля и демодулирует сигнал для восстановления исходных данных.

Важным аспектом является использование магнитной составляющей электромагнитной волны, которая менее подвержена затуханию в воде по сравнению с электрической составляющей. Это позволяет системе работать в условиях, где традиционные методы радиосвязи оказываются неэффективными. Кроме того, магнитные волны способны проходить через границу раздела сред (вода–воздух), что делает их пригодными для связи между подводными и надводными объектами.

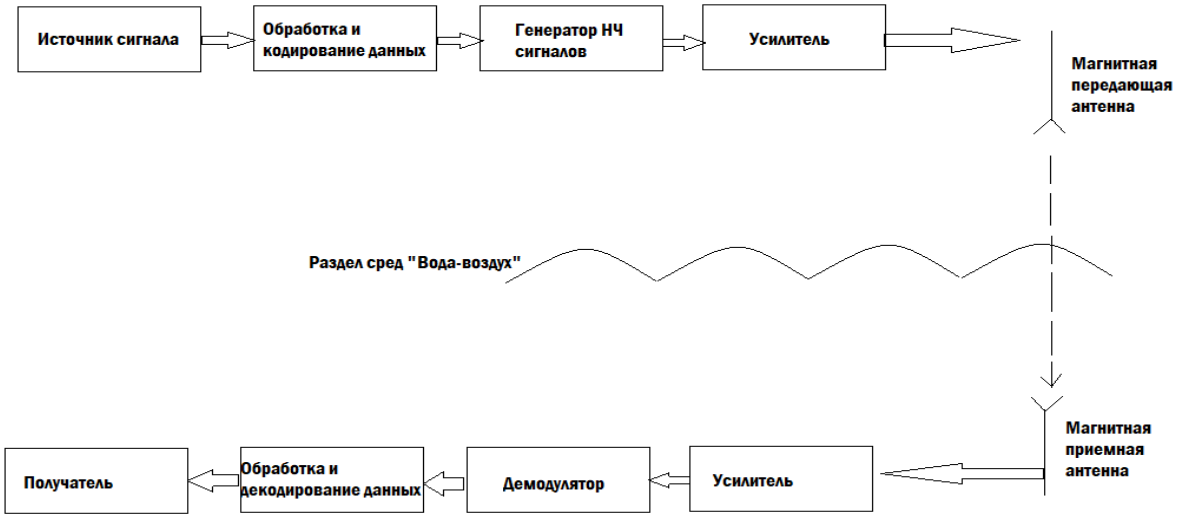


Рис. 5. Принципиальная схема системы подводной радиосвязи

Более современные исследования сосредоточены на использовании низкочастотных (НЧ) и сверхнизкочастотных (СНЧ) волн для передачи данных на меньшие расстояния, но с более высокой скоростью. Например, в работе исследователей из Массачусетского технологического института (MIT) была продемонстрирована возможность передачи данных на частоте 1 МГц на расстояние до 10 метров в морской воде со скоростью до 100 бит в секунду. Эти результаты были достигнуты за счёт оптимизации конструкции антенн и использования современных методов модуляции сигнала.

Ещё одним примером является разработка исследователей из Университета Вашингтона, которые создали систему подводной радиосвязи, работающую на частоте 30 кГц. В ходе экспериментов им удалось достичь скорости передачи данных до 1 кбит/с на расстоянии до 20 метров. Система показала устойчивость к помехам, вызванным движением воды и наличием взвесей, что делает её пригодной для использования в прибрежных зонах.

Гибридная система подводной связи IVA S/W, разработанная компанией IVA Technologies, представляет собой комбинированное решение, объединяющее два принципиально различных метода передачи данных: радиосвязь на основе электромагнитных волн и гидроакустическую связь. Такая комбинация позволяет минимизировать ограничения, присущие каждому из методов в отдельности, и создать универсальную платформу для передачи информации в сложных подводных условиях. Радиосвязь в системе реализована за счёт использования магнитной составляющей электромагнитной волны, которая демонстрирует низкий уровень затухания при прохождении через немагнитные среды, такие как вода, лёд или горные породы. Это свойство обеспечивает возможность передачи данных через границу раздела сред (вода–воздух), а также через подводные препятствия, включая ледовый покров и рифы. Гидроакустический канал, в свою очередь, применяется для передачи информации на большие расстояния в условиях, где радиосигнал может быть ослаблен или недоступен.

Техническая реализация системы включает цифровой приёмопередатчик, гидроакустическую и электромагнитную антенны, контроллеры управления связью и подводную гарнитуру, интегрированную в полнолицевую маску водолаза. Все компоненты системы отличаются компактностью и размещаются на аквалангe, что обеспечивает удобство использования без ограничения подвижности оператора. Время автономной работы системы достигает 8 часов, что позволяет применять её для продолжительных операций.

Рис. 6. Комплект для обеспечения связи под водой IVA S/W

Проведение испытаний системы IVA S/W было осуществлено в акватории Баренцева моря при активном содействии специалистов Военно-морского флота Российской Федерации. В ходе экспериментальных исследований была подтверждена способность системы обеспечивать устойчивую голосовую связь с исключительной чёткостью, достигая расстояния до 2000 метров и функционируя на глубине до 26 метров.

Эти результаты свидетельствуют о высокой эффективности системы в условиях, где традиционные гидроакустические методы связи демонстрируют ограниченную работоспособность. Кроме того, система показала устойчивость к внешним помехам, таким как подводные течения, изменения температуры воды и естественное волнение, что делает её пригодной для использования в сложных условиях, включая загрязнённые водные среды и прибрежные зоны с высоким уровнем акустических шумов.

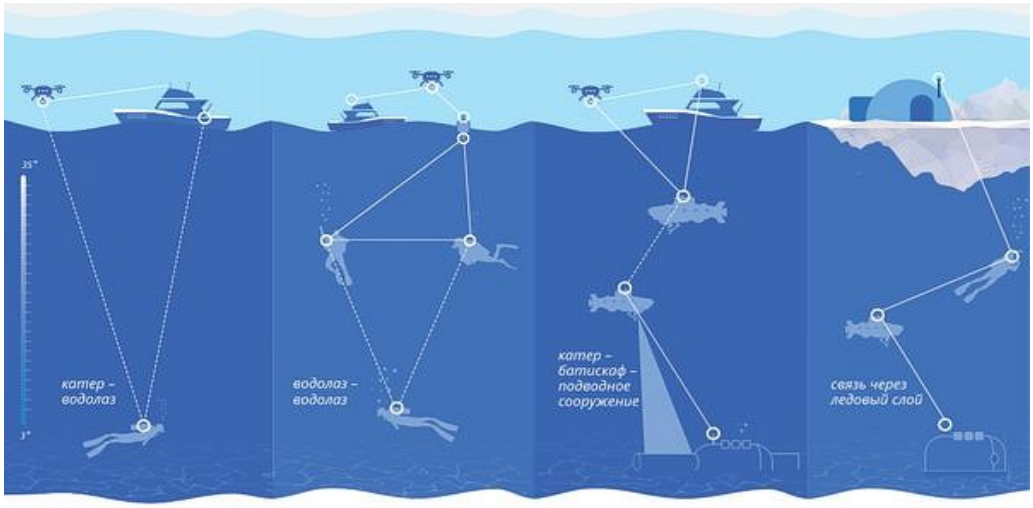


Рис. 7. Возможное применения комплекса связи IVA S/W

Сравнение существующих систем гидросферной связи

Беспроводные системы связи в морской среде традиционно базируются на применении акустических технологий и электромагнитного излучения, охватывающего диапазоны сверхнизких (СНЧ, 30-300 Гц) и очень низких частот (ОНЧ, 3-30 кГц). Акустические системы, активно эксплуатируемые с начала прошлого столетия, отличаются относительной простотой реализации и способностью функционировать на значительных глубинах. Тем не менее, они характеризуются рядом существенных ограничений, включая низкую пропускную способность (например, 62,5 кбит/с на дистанции 300 м для модемов Evologics и 5 кбит/с на 10 км для устройств LinkQuest), высокое энергопотребление, значительные массогабаритные параметры оборудования, низкую устойчивость к внешним помехам и выраженную зависимость от физико-химических характеристик водной среды.

Таблица 1

Аналитическое сравнение систем гидросферной связи

Система	Оптическая	Гидроакустическая	Гибридная
Скорость передачи	До 12,4 Гбит/с	Кбит/с	Высокая на коротких расстояних, низкая на больших
Дальность связи	До 100 – 200 м	До нескольких км	До 2000 м
Преимущества	Высокая скорость, низкая задержка	Большая дальность, устойчивость к мутности	Адаптивность, высокая надежность
Недостатки	Затухание в мутной воде, ограниченная дальность	Низкая скорость, высокая задержка	Сложность реализации, высокая стоимость

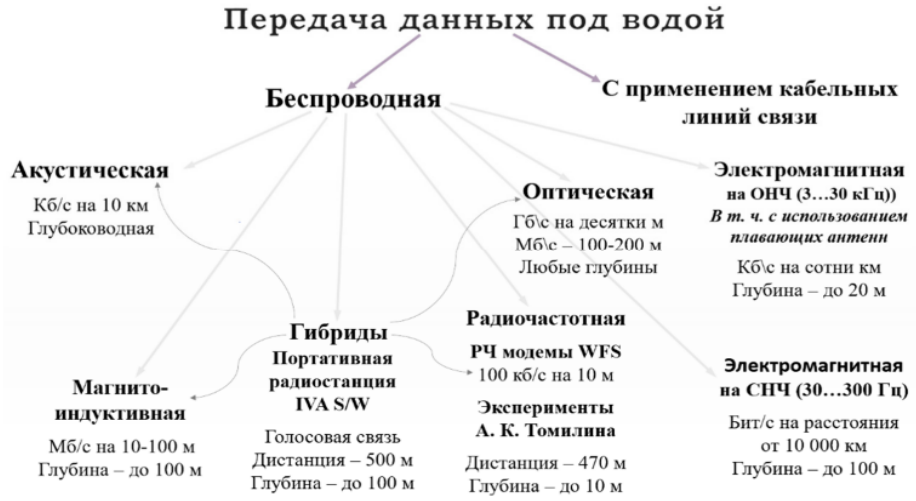


Рис. 8. Способы передачи данных в водной среде

Для обеспечения связи между береговыми объектами и подводными аппаратами преимущественно используются электромагнитные волны ОНЧ-диапазона, однако их применение ограничено малой глубиной проникновения и низкой скоростью передачи данных, не превышающей нескольких килобит в секунду. Волны СНЧ-диапазона, обладая большей глубиной проникновения, обеспечивают крайне низкую скорость передачи информации (порядка 3 символов за 15 минут), а также требуют использования антенных систем километровых размеров и значительных энергетических ресурсов.

Начиная с 2006 года, корпорация Wireless Fibers Systems (WFS) активно развивает направление, связанное с проектированием и производством радиомодемов, специально адаптированных для эксплуатации в водной среде. Одна из их разработок, модель Seatext, демонстрирует возможность передачи информации на скорости до 100 бит в секунду, при этом сохраняя стабильность связи на расстоянии до 30 метров. В свою очередь, модель Seatooth предлагает более высокую пропускную способность – до 100 кбит/с, однако эффективная зона её действия ограничена 10 метрами. Особого внимания заслуживает модификация RAM300, которая, благодаря внедрению акустического режима, существенно расширяет спектр применения устройства. К числу ключевых преимуществ этих радиомодемов можно отнести их исключительную устойчивость к работе в условиях сильного акустического шума, способность преодолевать переходы между различными средами (например, вода-воздух, земля-воздух, лёд), а также высокую эффективность в сложных условиях мелководья и речных водоёмов.

Группа российских учёных во главе с А. К. Томилиным осуществила успешный эксперимент по передаче модулированного коротковолнового радиосигнала в приповерхностном слое морской воды на глубине 4-6 метров. В ходе эксперимента сигнал был передан на расстояние 470 метров с использованием шаровых антенн. Предполагается, что формирование канала связи осуществляется за счёт генерации продольных электромагнитных волн (электроскалярных), способных преодолевать границу раздела сред «морская вода – воздух». Данный подход открывает новые перспективы для разработки высокочастотных систем подводной радиосвязи.

Заключение

Проведённый анализ современных систем гидросферной связи, включая оптические, гидроакустические, системы радиосвязи и гибридные решения, демонстрирует их значительный потенциал для решения задач в подводной среде. Оптические системы обеспечивают высокую скорость передачи данных на коротких расстояниях, но ограничены затуханием сигнала в мутной воде. Гидроакустические системы, напротив, эффективны на больших дистанциях, но сталкиваются с проблемами задержки и низкой скорости передачи. Гибридные системы, такие как IVA S/W, объединяют преимущества обеих технологий, обеспечивая стабильную связь в сложных условиях, включая загрязнённые воды и прибрежные зоны.

Однако разработка и внедрение таких систем по-прежнему сопряжены с рядом вызовов, включая необходимость увеличения дальности и скорости передачи данных, минимизацию энергопотребления и адаптацию к изменяющимся условиям среды. Дальнейшие исследования должны быть направлены на оптимизацию технологий, разработку новых методов модуляции и создание более компактных и энергоэффективных устройств. Развитие систем гидросферной связи открывает новые возможности для освоения водных ресурсов, экологического мониторинга и обеспечения безопасности, что подчеркивает их важность для современной науки и техники.

Литература

1. *Трошина Е.Ю.* Гидроакустический канал передачи данных // Наука без границ. 2020. № 6 (46). С. 101-106.

2. *Farr N., Chave A.D., Freitag L., Preisig J.* Optical modem technology for seafloor observatories // Oceanography. 2010. Vol. 23, no. 1. P. 120-127.

3. *Huang J., Babeau M., Blouin S., Hamm C., Taillefer N.* Simulation and Modeling of Hydro Acoustic Communication Channels with Wide Attenuation and Ambient Noise // International Journal of Parallel, Emergent and Distributed Systems. 2017. No. 2. P. 1-21.

4. Sonardyne International Ltd. BlueComm: Underwater wireless optical communication system. 2021.

5. *Hanson F., Radic S.* High bandwidth underwater optical communication // Applied Optics. 2008. Vol. 47, no. 2. P. 277-283.

6. *Мирошникова Н.Е., Петрухин Г.Д., Щербаков А.А*. Проблемы моделирования гидросферных оптических линий связи // Системы синхронизации, формирования и обработки сигналов. 2019. № 5. С. 29-39.

7. *Томилин А.К., Лукин А.Ф., Гульков А.Н*. Эксперимент по созданию канала радиосвязи в морской среде // Письма в ЖТФ. 2021. Т. 47, № 11. С. 48-50.

8. *Бахур В.* Россияне создали систему беспроводной связи под водой. Аналогов в мире нет. URL: https://www.cnews.ru/news/top/2020-11-10_vmf_rossii_oproboval_podvodnuyu (дата обращения: 22.01.2025).

9. *Павлов И.И., Мышкин В.Ф., Хан В.А.* Организация подводной беспроводной системы связи // T-Comm: Телекоммуникации и транспорт. 2024. Т. 18. № 1. С. 4-12. EDN: ZNJJGQ

АДАПТИВНАЯ НАСТРОЙКА ШИРОКОПОЛОСНОГО РАДИОКАНАЛА ПО RS-ВРЕЗКАМ В OFDM СИГНАЛАХ

Шорин Василий Олегович
МТУСИ, аспирант, магистр, Москва, Россия
shorinvasily23@gmail.com

Аннотация
В статье рассматривается использование референсных сигналов (RS) в системах подвижной радиосвязи 4G и 5G, построенных на OFDM-сигналах. RS обеспечивают корректную демодуляцию данных путем точного учета амплитудно-фазовых искажений радиоканала. Описаны различные типы RS, такие как Cell-specific RS, Sounding RS и Positioning RS, а также их функции: улучшение качества связи, управление модуляцией, мощностью и направленностью антенн. Приведены примеры размещения RS в ресурсных блоках. Указаны перспективы расширения их применения в системах LTE-Advanced и других современных технологиях.

Ключевые слова
Референсные сигналы, OFDM, SC-OFDM, 4G, 5G, LTE, MIMO, MU-MIMO, цифровая модуляция, позиционирование.

Введение

Современные системы подвижной радиосвязи поколений 4G и 5G имеют широкополосный радиоканал, использующий сигналы, построенные на множестве поднесущих. Такие сигналы принято называть OFDM-сигналами (Orthogonal frequency-division multiplexing). При этом каждому активному абоненту для организации подключения к системе по радиоканалу распределяют ресурс нескольких поднесущих, на каждой из которых осуществляется передача (прием) данных. Время разбивают на последовательность тактовых интервалов. На отдельном такте, для каждой из указанных поднесущих передающая сторона устанавливает амплитуду и фазу, путем выбора из множества допустимых состояний, предопределенного выбранным законом цифровой модуляции (например, QPSK, QAM16, QAM64). Чтобы правильно выполнить демодуляцию на приемной стороне необходимо иметь достаточно точную информацию об амплитудно-фазовых искажениях сигнала каждой поднесущей, существующих в радиоканале на текущий момент времени. С этой целью в OFDM (SC-OFDM) на заданных тактах и заданных поднесущих передают референсные сигналы (RS- Reference Signals) обладающие априорно известной структурой с заданными параметрами амплитуды и фазы. Это позволяет в наиболее простой форме выполнять измерения с последующей обработкой для адаптивной подстройки амплитудно-частотной (АЧХ) и фазо-частотной (ФЧХ) характеристик радиоканала на активных поднесущих.

По мере развития функциональности систем подвижной радиосвязи перечень задач, решаемых с помощью *RS* сигналов, стал расширяться. Так в сетях *LTE Release 8* в структуру *OFDM* дополнительно к «исходным» *Cell-specific RS* были введены *RS*-врезки контроля искажений на трассах для сигналов, излучаемых каждым отдельным элементом антенной системы базовой станции (БС), используемые для организации режимов *MIMO, MU-MIMO* и в перспективе – для управления лучами диаграммы направленности, сопровождающими абонентов. В сетях *LTE Release 9* в структуру сигналов *SC-OFDM* (линий «вверх» (*Up-Link*)) были введены дополнительно «зондирующие» *RS*-врезки (*SRS- Sounding Reference Signals*), предназначенные для улучшения: контроля качества радиоканала на отдельных поднесущих линий вверх (*Up-Link*); управления переключением применяемых законов модуляции и управления мощностью трансляции. В линиях «вниз» (*Down-Link*) в структуру *OFDM* были дополнительно введены *RS*-врезки «позиционирования» (*PRS- Positioning Reference Signals*), предназначенные для повышения вероятности правильного обнаружения абонентскими терминалами (*UE- User Equipment*) ближайших БС. На рисунках 1-6 приведены примеры размещения указанных *RS*-врезок в структуре *OFDM*.

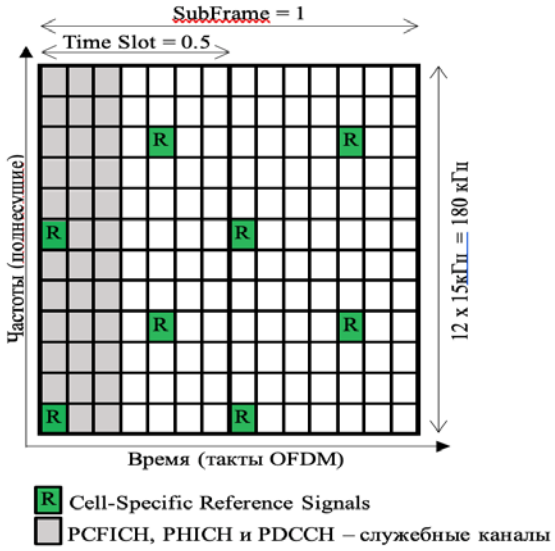


Рис. 1. Размещение «исходных» Cell-specific RS на спаренном ресурсном блоке в OFDM-сигнале LTE

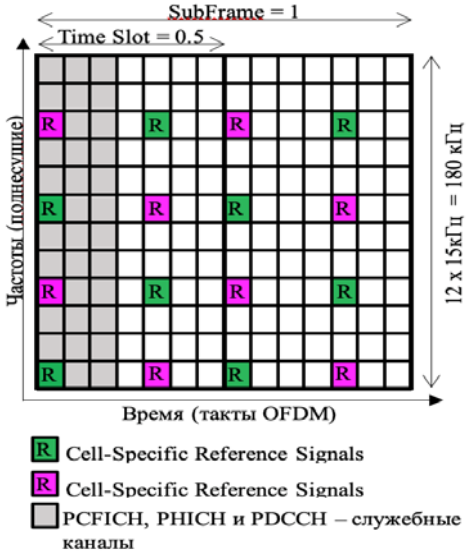


Рис. 2. Размещение Cell-specific RS на спаренном ресурсном блоке OFDM в ситуации сопряжения RS с двумя работающими антеннами БС

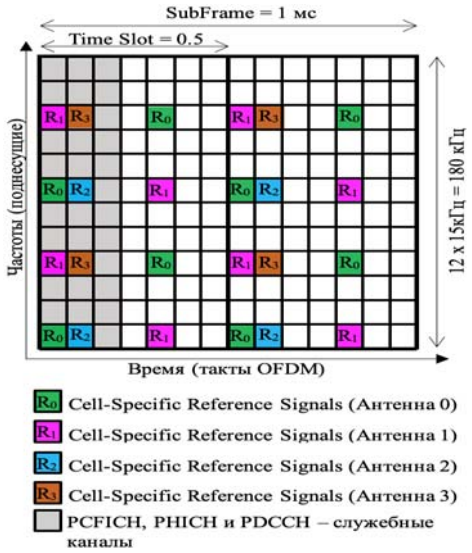


Рис. 3. Размещение Cell-specific RS на спаренном ресурсном блоке OFDM в ситуации сопряжения RS с четырьмя работающими антеннами БС

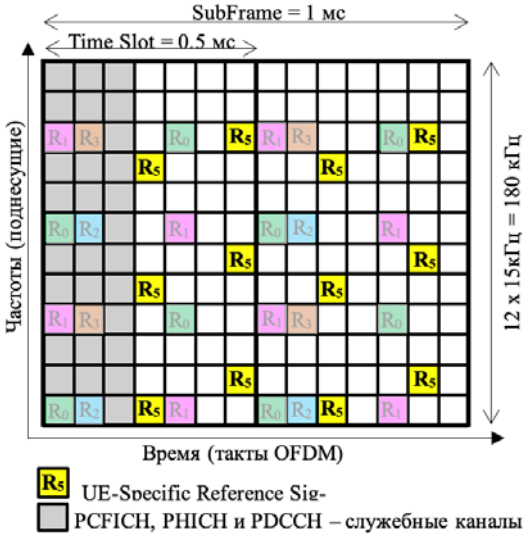


Рис. 4. Размещение UE-specific RS на спаренном ресурсном блоке OFDM, предназначенных для обратной связи при организации режима MIMO в линиях Up-Link в случаях доступа с частотным разделением (FDD)

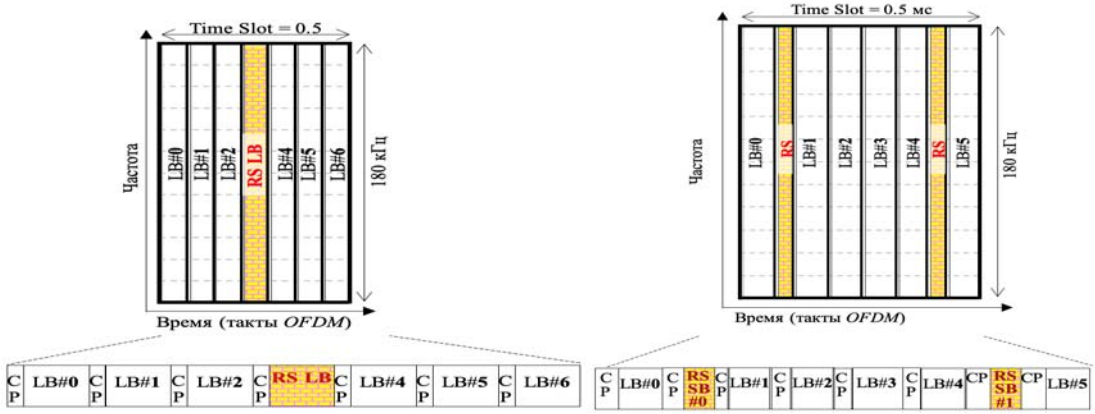


Рис. 5. Размещение RS на одном тайм-слоте сигнала SC-OFDM в линии Up-Link. Случаи с одним длинным блоком (Long Block (LB)) для RS при обслуживании обычных абонентов, и двумя короткими блоками (Short Block (SB)) при обслуживании скоростных абонентов

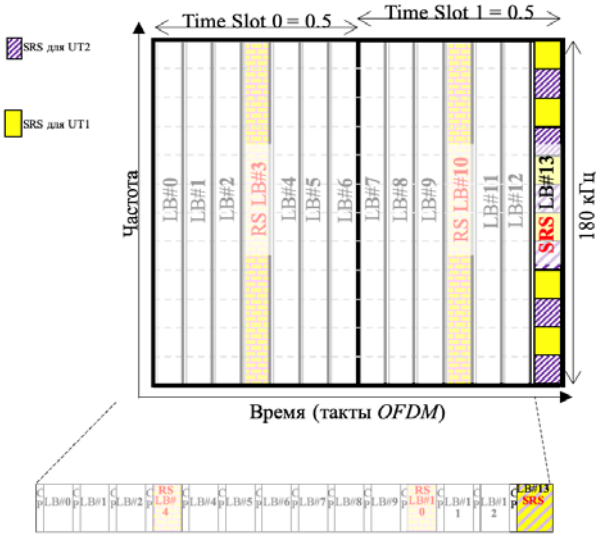


Рис. 6. Размещение «зондирующих» Sounding Reference Signals (SRS) в структуре 2-х тайм-слотов сигнала SC-OFDM линии Up-Link. Случай совместного использования ресурса SRS для двух UT

В сетях стандарта *LTE-Advanced (Release 10)* перечень задач, решаемых на основе *RS*-врезок, еще увеличился, что привело к дополнительному расширению множества применяемых структур. Таким образом, техника *RS*-врезок зарекомендовала себя как весьма эффективный способ решения задач, связанных с адаптивной настройкой радиоканала, в условиях, характерных для работы современных сетей связи и систем широкополосного доступа.

Система широкополосного доступа ГОСТ Р 58166-2018 (технология МАКВИЛ) не является исключением. У нее в структуре *OFDM*-сигналов также применяются *RS*-врезки априорно установленного формата, предназначенные для решения задач подключения абонентов, адаптации к параметрам радиоканала, осуществления режима расширения спектра и реализации пространственно-временной обработки в антенных системах.

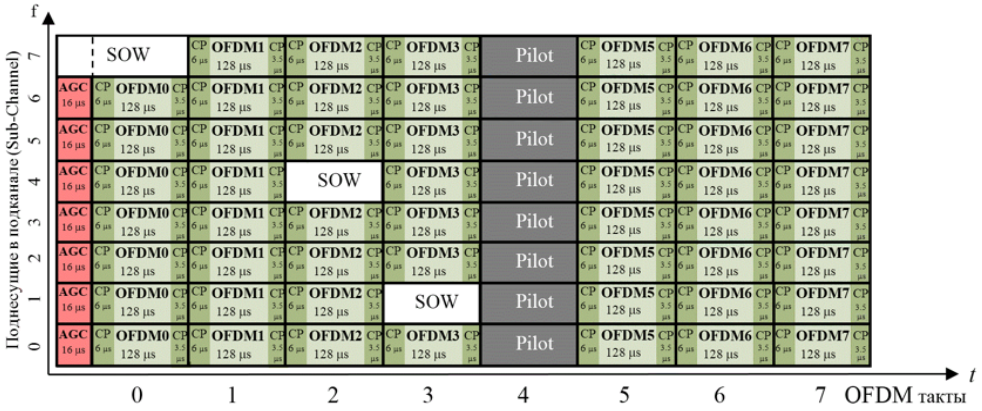


Рис. 7. Размещение Pilot-врезок (аналог RS) на ресурсном блоке в OFDM-сигнале МАКВИЛ, в каналах связи стационарных абонентов

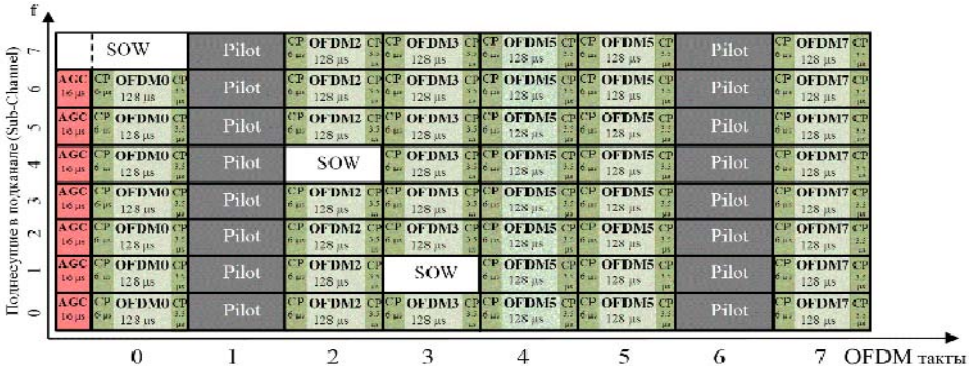
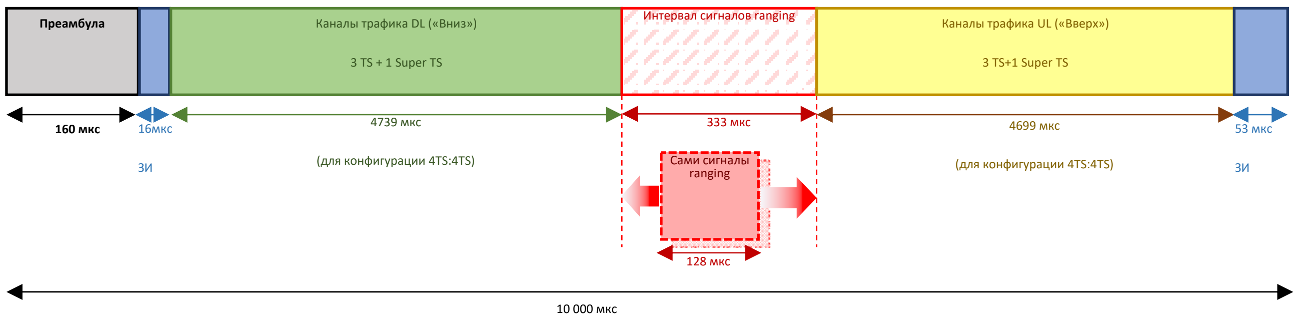


Рис. 8. Размещение Pilot-врезок (аналог RS) на ресурсном блоке в OFDM-сигнале МАКВИЛ, в каналах связи мобильных абонентов

Кроме того, в МАКВИЛ используются сигналы «Преамбула», которые являются аналогом *Cell-specific RS* врезок в *LTE*. Эти сигналы предназначаются для идентификации БС и подключения к сети МАКВИЛ абонентов. По «преамбулам» осуществляется первичная синхронизация приемного тракта *UT* МАКВИЛ по параметрам частоты и задержки. На рисунке 9 показана структура отдельного кадра (Frame) системы МАКВИЛ и размещение на ней сигнала «Преамбула». На рисунке 10 показана частотно-временная структура самих сигналов «Преамбула» в привязке к идентификаторам БС.



Sequence ID	Кодовая последовательность преамбулы
0	1,-1,1,1,-1,-1,1,-1,1,1,-1,1,-1,1,1,1,-1,1,1,1,1,-1,-1,1,1,-1,-1,-1,1,-1,1,-1,1,-1,-1,1,1,1,1,1,1, -1,1,-1,-1,-1,-1,-1,1,1,1,-1,-1,-1,-1,1,-1,-1,1,-1,-1,-1,1,1
1	1,1,1,1,1,-1,1,-1,-1,-1,-1,-1,1,1,1,-1,-1,-1,-1,1,-1,-1,1,-1,-1,-1,1,1,-1,1,1,-1,-1,1,-1,1,1,-1,1, -1,1,1,1,-1,1,1,1,1,-1,-1,1,1,-1,-1,-1,1,-1,1,-1,1,-1,-1,1,1
2	-1,1,-1,1,-1,1,-1,-1,1,1,1,1,1,1,-1,1,-1,-1,-1,-1,-1,1,1,1,-1,-1,-1,-1,1,-1,-1,1,-1,-1,-1,1,1,-1, 1,1,-1,-1,1,-1,1,1,-1,1,-1,1,1,1,-1,1,1,1,1,-1,-1,1,1,-1,-1,-1
3	1,-1,1,-1,1,1,1,-1,1,1,1,1,-1,-1,1,1,-1,-1,-1,1,-1,1,-1,1,-1,-1,1,1,1,1,1,1,-1,1,-1,-1,-1,-1,-1, 1,1,1,-1,-1,-1,-1,1,-1,-1,1,-1,-1,-1,1,1,-1,1,1,-1,-1,1,-1,1,1
⋮	⋮
15	-1,-1,1,-1,-1,1,-1,-1,-1,-1,-1,-1,-1,-1,1,-1,1,1,-1,-1,-1,1,1,1,1,-1,-1,1,1,1,-1,1,1,1,-1,-1,-1, 1,1,-1,-1,1,1,1,1,1,1,-1,1,-1,-1,-1,1,-1,1,-1,-1,-1,1,-1,1,1,1,-1

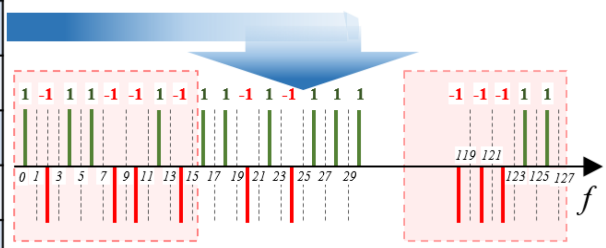


Рис. 9. Структура отдельного кадра (Frame) системы МАКВИЛ и размещение на ней сигнала «Преамбула»

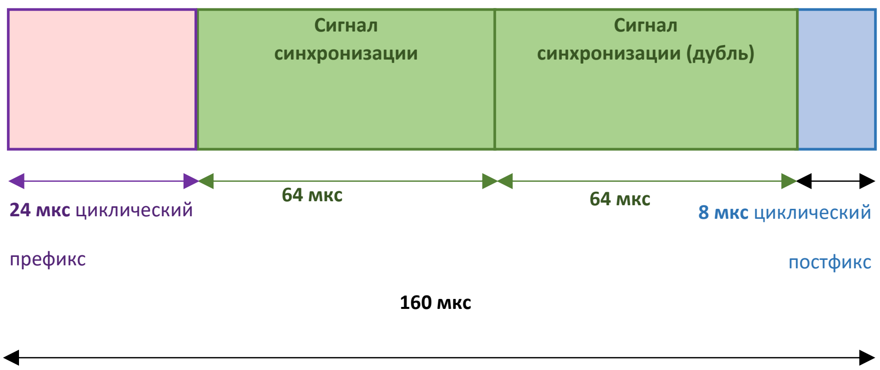


Рис. 10. Частотно-временная структура сигналов «Преамбула» в привязке к идентификаторам БС (Sequence ID)

Следует отметить, что в *LTE* и *LTE-Advance* для режима *TDD* установлены такие же размеры кадра (*Frame*), как и в МАКВИЛ (10 мс). На рисунках 11 и 12 приведены структуры указанных кадров LTE для ситуаций с различными установками соотношений ресурсов линий *Down* и *Up* для 5 и 10 мс соответсвенно.

Если работа сети *LTE* осуществляется в режиме с *FDD*, то для речевых соединений и соединений низкоскоростного обмена данными используются ресурсы не каждого подкадара (*SubFrame*), а выборочно, с прореженным периодом повторения [1, стр. 113, 194], [2, стр. 447]. Это позволяет избежать избыточности выделенных ресурсов.

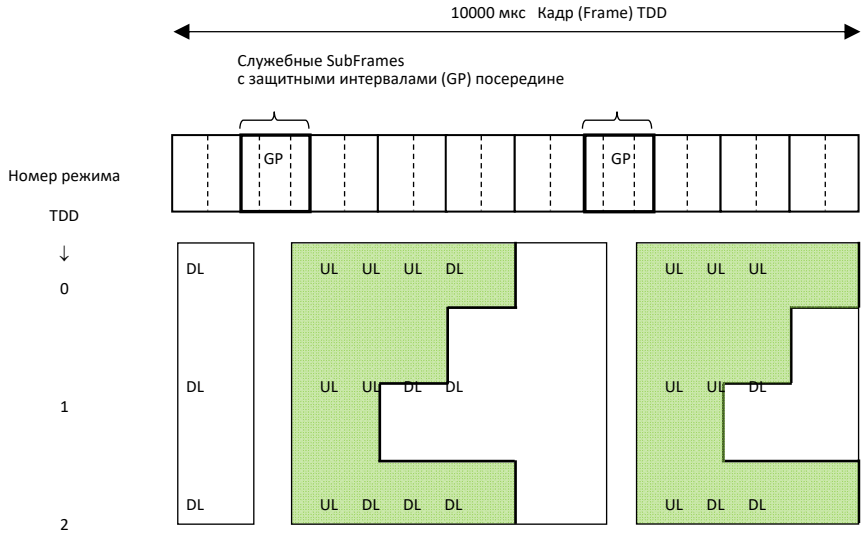


Рис. 11. Кадры TDD LTE при периоде повторения 5 мс

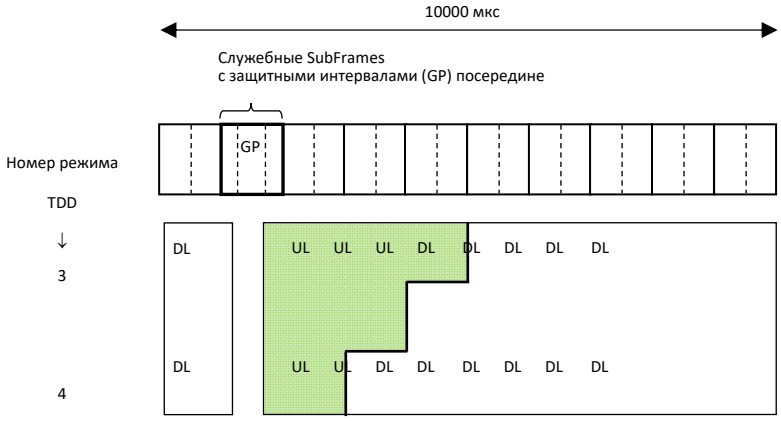


Рис. 12. Кадры TDD LTE при периоде повторения 10 мс

Согласно такой схеме, получившей название «полу-настойчивая» (*SPS- Semi-Persistent Scheduling*), абоненты имеют доступ в канала либо через каждые: 10, 20, 32, 40, 64, 80, 128, 160, 320 или 640 мс. Это означает, что и в режиме с *FDD* между кадрами абоненты могут иметь задержки от 10 мс и более.

Из вышеизложенного следует, что привязки к моментам времени для отсчетов статистических выборок, формируемых из данных *RS* сигналов (*LTE*) и *Pilot*-врезок (МАКВИЛ), в первом приближении можно считать, если не одинаковыми, то, по крайней мере, мало различающимися. Но с точки зрения статистики это совсем не обеспечивает близости или схожести рабочих характеристик на выходах блоков оценок (например, искажений радиоканала). Причиной тому является зависимость указанных рабочих характеристик от множества других параметров, которые в сетях стандарта *LTE* и системе широкополосного доступа технологии МАКВИЛ заметно различаются. В первую очередь это относится к диапазонам рабочих частот. Если для *LTE* на территории РФ основными являются диапазоны 1800 МГц и 2500 МГц, то для МАКВИЛ это 340 МГц и 425 МГц (т.е. примерно в 5-7 раз меньше). Поэтому показатели доплеровских сдвигов, пространственные характеристики областей с замираниями сигнала, длительности интервалов пропаданий сигнала из-за замираний в МАКВИЛ существенно ниже. Следовательно, эффективность показателей для режима накопления данных должна быть выше, чем для *LTE*.

Ситуация усложняется еще тем, что в технической документации, стандартах и доступной литературе не удалось обнаружить сколько-нибудь подробных данных или отчетов об исследованиях, связанных с оценкой эффективности алгоритмов обработки данных *RS*-сигналов с динамическими характеристиками условий работы. Практически вся доступная информация по этому вопросу ограничивается одной единственной фразой о том, что структура с двумя короткими блоками *SB RS* (см. рис. 5) используется при скоростях абонентов от 250 км/ч [1]. При этом совершенно ясно, что в разных условиях потеря качества восстановле-

ния характеристик канала будет сказываться на информационном обмене по-разному. Так при высоких отношениях сигнал/шум даже небольшие неточности восстановления будут заметно снижать эффективный энергетический запас, а может даже и полностью блокировать работу при использовании сложных законов модуляции. Это приведет к потере производительности. А на краях сот, при предельно низких отношениях сигнал/шум, неточности восстановления характеристик радиоканала будут, в первую очередь, приводить к потере чувствительности и сокращению площади покрытия.

Такие разнотипные проявления нужно правильно комбинировать при решении общей целевой задачи достижения максимальной информационной производительности системы широкополосного доступа при заданных ключевых показателях качества работы.

Заключение

В широких полосах частот, занимаемых системами подвижной радиосвязи с *OFDM* сигналами, неизбежно возникают частотно-селективные замирания с динамическим характером поведения. Для отслеживания этих изменений применяются пилот сигналы, функционал которых, с совершенствованием систем, расширяется. Поэтому для увеличения информационной производительности таких системах является весьма актуальным решение задачи слежения за частотно-селективными искажениями сигнала с целью их компенсации.

Литература

1. *Sesia I., Toufik M., Baker*. LTE – the UMTS Long Term Evolution: From Theory to Practice. John Wiley&Sons, 2011, p. 752.

2. 3GPP TS 136.331 version 13.1.0. LTE; Evolved Universal Terrestrial Radio Access (E-UTRA); Radio Resource Control (RRC); Protocol specification 04.2016.

3. *Viholaimen A., Bellanger M., Huchard M.* Prototype filter and structure optimization, Tech. Rep., PHYDYAS. 2008.

4. *Bellanger M*. FBMC physical layer: a primer, Tech. Rep., PHYDYAS. 2010.

5. *Schaich F., Wild T.* Waveform contenders for 5G – OFDM vs FBMC vs. UFMC, in 6th Int. Symp. Commun. Cont. Sig. Proc. (ISCCSP), 2014, IEEE, pp. 457-460.

6. *Нгуен Ван Фе*. Повышение скорости передачи информации при использовании многочастотных сигналов путем использования оптимальных спектральных импульсов / Диссертация на соискание ученой степени кандидата тех. наук, Санкт-Петербургский политехнический университет Петра Великого, СПб, 2018, 112 с.

7. *Vakilian V., Wild T., Schaich T., Stephan ten Brink, Frigon J-F*. Universal-Filtered Multi-Carrier Technique for Wireless Systems Beyond LTE // Globecom 2013 Workshop – Broadband Wireless Access, IEEE, 2013, pp. 223-228.

8. *Ворожищев И.В., Бочечка Г.С., Тихвинский В.О*. Сравнительный анализ использования технологий UFMC и OFDM в сетях 5G // Электросвязь, №11, 2017. С. 46-51.

9. *Бакулин М.Г., Варукина Л.А., Крейнделин В.Б.* Технология MIMO: принципы и алгоритмы. М.: Горячая линия – Телеком, 2014. 244 с.

10. *Ravi Teja, Shakti Raj Chopra*. Review of UFMC Technique in 5G// 2018 International Conference on Intelligent Circuits and Systems, IEEE, 2018, pp. 115-120.

ВОЗДЕЙСТВИЕ РАЗЛИЧНЫХ ОПТИЧЕСКИХ ВОЗМУЩЕНИЙ НА ХАРАКТЕРИСТИКИ КВАНТОВОГО АТМОСФЕРНОГО КАНАЛА СВЯЗИ

Наниджанян Анна Карапетовна
МТУСИ, бакалавр МТУСИ, Москва, Россия
aliberation@ya.ru

Бахус Александр Владимирович
МТУСИ, магистрант МТУСИ, Москва, Россия
sasha.bahus.01@mail.ru

Ярыгин Михаил Александрович
МТУСИ, бакалавр МТУСИ, Москва, Россия
mikhail.yarygin2004@mail.ru

Аннотация
Представлены результаты физического моделирования воздействий возмущений на атмосферную квантовую трассу системы квантового распределения ключей. Протестированы экспериментальные методики для оценки изменения характеристик квантового беспроводного канала связи в атмосфере. Исследована динамика изменения процента квантовых битовых ошибок и скорости генерации квантового ключа при наличии различных возмущений среды.

Ключевые слова
квантовое распределение ключей, атмосферный канал, процент квантовых битовых ошибок, квантовый ключ, скорость выработки квантового ключа, турбулентность.

Введение

Квантовое распределение ключей (КРК) в атмосферных оптических линиях связи (АОЛС) является многообещающей технологией для создания безусловно защищенных коммуникаций [1-3]. Поскольку воспроизводимые измерения параметров квантового канала связи при воздействии различных возмущений на протяженной атмосферной трассе в реальных условиях трудноосуществимы [1, 2], создаются небольшие экспериментальные трассы, на которых и проводят исследования влияния атмосферных возмущений [4]. В ряде работ оптическая линия связи тестировалась с использованием классического источника и квантового оборудования на открытой трассе между двумя зданиями [5, 6]. В [5] тестирования систем КРК проводились на дистанциях 175 м и 135 м. В [6, 7] аналогичные исследования проводились на дистанции 180 м, основной целью работ [6, 7] являлось разработка методик оценивания воздействия различных атмосферных явлений на атмосферный канал связи. При этом исследования [4-7] нельзя назвать вполне законченными, поскольку воспроизводимость результатов страдает непредсказуемостью погодных условий [2]. Поэтому, более удобно моделировать воздействия на оптический канал связи в лабораторных условиях [8-10].

Предлагаются различные способы для моделирования оптических возмущений, это могут быть, как возмущение плотности и температуры воздуха на линии связи [8, 9], так и возмущение специальной физической среды, моделирующей атмосферную трассу [10]. В [8] использовался программируемый жидкокристаллический пространственный модулятор света, позволяющий модулировать фазу и амплитуду светового луча, имитируя различные атмосферные условия на оптической трассе, включая турбулентность и облачность. Однако подход [10] не является универсальным и требуется специальные исследования для строгого обоснования того, что программируемые возмущения жидкокристаллической среды адекватно моделируют атмосферные эффекты при передаче квантовых состояний через атмосферную трассу [1]. В [8, 11] описан более привлекательный подход, где было предложено на лабораторной трассе создавать контролируемые возмущения воздушной среды.

Целью настоящей работы являлось дальнейшее развитие подхода, описанного в [8, 11] и получение экспериментальных данных о характеристиках квантового канала связи через воздушные возмущения, которые могут соответствовать оптическим системам связи с КРК, реализованными через мобильные беспилотные аппараты [12, 13].

Результаты исследования

Для проведения экспериментов по изучению влияния атмосферных турбулентностей на характеристики квантового канала связи был создан экспериментальный стенд, показанный на рисунке 1 [9]. Лабораторный стенд включал в себя следующие компоненты: два коллиматора C40FC-C Thorlabs, разнесенные на расстояние 40 см, одномодовое волокно (SMF-28), EMQOS 1.0, парафиновая свеча, небулайзер JSL-W302, строительный фен REXANT 1600 Вт мощности. На данном стенде реализована двухпроходная система квантового распределения ключей на базе установки EMQOS 1.0 Plug&Play, на которой реализуется квантовый криптографический протокол BB84 [14, 15]. На рисунке 1 схематически показан беспроводной квантовый атмосферный канал, обеспечивающий соединение блоков КРК от установки EMQOS 1.0.

На первоначальном этапе проводилась юстировка коллиматоров под длину волны лазерного излучения 1546,7 нм на расстоянии друг от друга в 40 см. На атмосферной трассе фиксировались потери мощности излучения с точностью до 46%. Потери мощности излучения в атмосферном канале в течение эксперимента могли флуктуировать в диапазоне не более 3,6 дБ. Лазерное излучение подавалось с блока КРК «Боб» через атмосферный канал к блоку КРК «Алиса» и возвращалось обратно к «Бобу», кликая в детекторе одиночных фотонов (ДОФ). Блоки КРК подключались к коллиматорам по одномодовому волокну типа SMF-28. Соответственно, лазерное излучение мощностью 80,1 мкВт, выходящее из схемы блока «Боба», проходило по свободному пространству в схему «Алисы» через коллиматоры, после чего лазерные импульсы возвращались, также проходя атмосферную трассу и схему «Боба», где, в конечном итоге, регистрировались в ДОФ, аналогично [16].

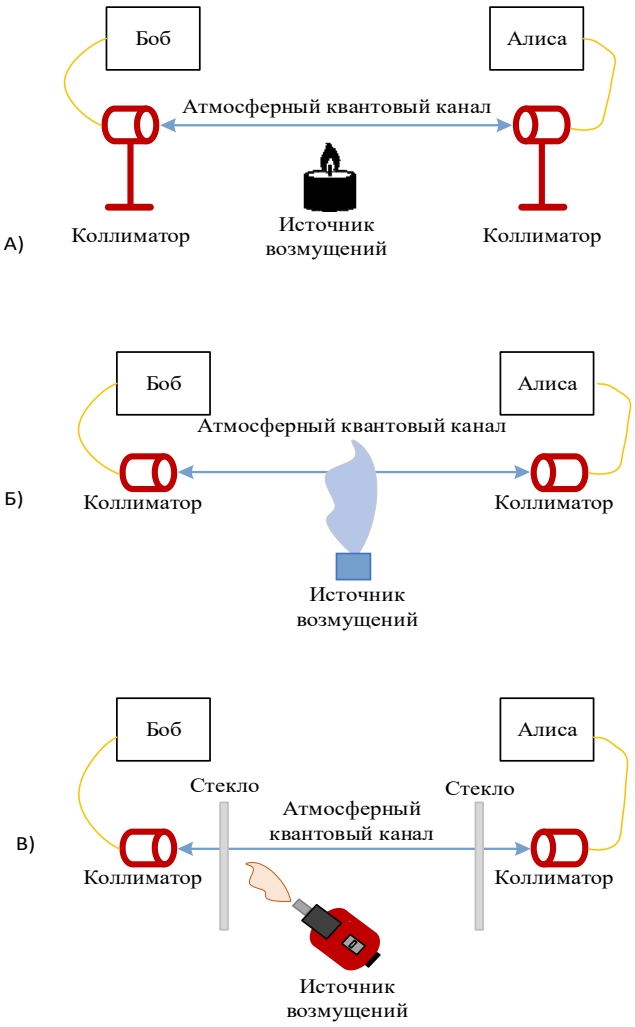


Рис. 1. Схемы экспериментов при введении в атмосферную трассу тепловых возмущений (А); возмущений в виде водного аэрозоля (Б); при нагреве строительным феном стекол (В)

Для реализации криптографической стойкости необходимо добиться отправки квантовых ключей, кодируемых в одиночных состояниях фотонов [14]. Для этого следует провести расчёты количества фотонов в одном посылаемом импульсе:

$$N_{\Phi} = \frac{P \cdot \lambda}{\nu \cdot c \cdot h}, \quad (1)$$

где P – входная мощность лазерного излучения «Боба», λ – длина волны лазера «Боба», ν – частота следования лазерных импульсов, c – скорость света в вакууме, h – постоянная Планка.

Соответственно, для достижения однофотонного режима нужно воспользоваться дополнительными аттенюаторами в схеме, чтобы получить требуемое количество затухания в системе КРК. Для достижения 0,2 фотона на импульс и расчёта затухания необходимо воспользоваться следующей формулой:

$$\alpha = 10 \cdot \lg\left(\frac{N_{\Phi}}{0.2}\right), \quad (2)$$

Проводилось 10 тестов для исследования характеристик квантового канала, а именно: процент квантовых битовых ошибок (QBER, от англ. Quantum Bit Error Rate) и длина просеянного квантового ключа с течением времени. Исследования проходили для трёх различных источников возмущений.

В первом тесте проверялась проходимость квантового ключа в отсутствии искусственно введённых турбулентностей в атмосферной трассе (см. рис. 2а).

В тестах 2-4 изучались характеристики квантового канала при внесении потерь ввиду тепловых возмущений от парафиновой свечи в атмосферный канал. Высота парафиновой свечи составляла 7,1 см и её диаметр – 6,2 см. Три теста проводились с изменением удаленности источника возмущений от каждого из коллиматоров. Для тестов 2, 3, 4 расстояние свечки от коллиматора блока «Боб» составляла 6,8 см, 20 см (середина атмосферной трассы) и 33,2 см соответственно. Представлен результат динамики изменения характеристик квантового канала связи при внесении тепловых возмущений на середину атмосферной трассы (см. рис. 2б). Пунктирной горизонтальной линией отображается уровень QBER, равный 11%, не превышение которого является теоретически доказанным гарантом безопасности передачи квантовых ключей в реализованном криптографическом протоколе системы КРК [3].

В тестах 5-7 изучались характеристики квантового канала при внесении в атмосферный канал водного аэрозоля. Небулайзер, испускающий пары воды с диапазоном воздействия на расстоянии в 30-33 см, устанавливался для тестов 5, 6, 7 на расстоянии от коллиматора, подключённого к «Бобу», 9 см поперек коллиматора, считая с центра линзы коллиматора, и вдоль – 11,2 см, 20 см, 28,8 см соответственно. На рисунке 2. В показан результат изученных характеристик квантового канала связи при небулайзере, находящемся в центре атмосферного канал.

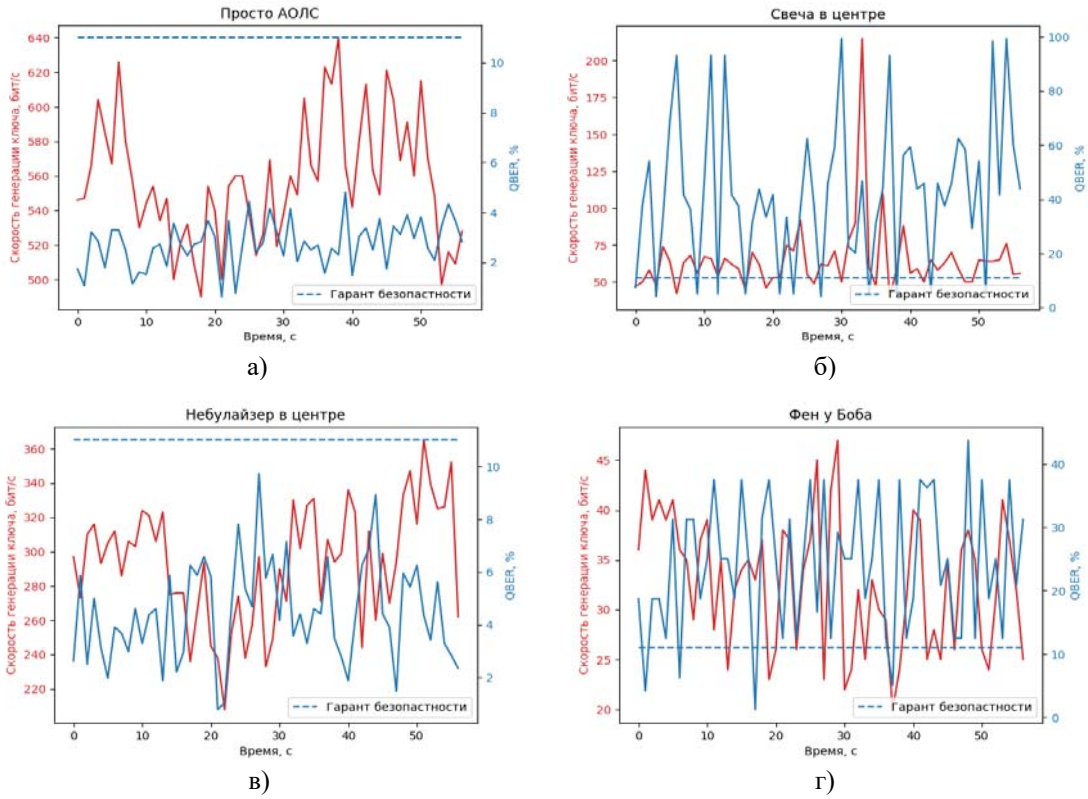


Рис. 2. Зависимость длины просеянного квантового ключа и процент квантовых битовых ошибок от времени при отсутствии возмущений (А), при внесении тепловых возмущений (Б) на середину атмосферной трассы, при воздействии водным аэрозолем (В) на середину атмосферного канала, при нагреве феном стекол коллиматора «Боба» (Г)

В тесте 8 в схему экспериментального стенда были добавлены стёкла напротив обоих коллиматоров, имитирующих защитные обтекатели, которые всегда присутствуют в реальных мобильных оптических системах связи. Набегающий воздушный поток на такой обтекатель может вызывать дополнительные оптические искажения [13]. Квантовый ключ передавался через атмосферную трассу в отсутствии каких-либо турбулентностей. Стёкла находились на расстоянии 6 см от линз коллиматоров.

В тестах 9-10 устанавливался строительный фен на расстоянии 22,5 см от каждого из коллиматора с диапазоном воздействия ≈ 10,5 см. Фен работал в режиме HIGH при температуре 250℃ по направлению к коллиматорам «Боба» и «Алисы» соответственно для тестов 9 и 10. Подверженность влиянию источника возмущений для теста 9 можно рассмотреть на рисунке 2.Г.

В таблице 1 приведены значения средних скорости генерации просеянного ключа ($SPEED_i$) и QBER ($QBER_i$) для каждого из тестов (i – номер теста), а также во сколько раз упал (в случае длины просеянного ключа с течением времени) или вырос (в случае QBER) показатель относительно 1-ого теста ($\Delta SPEED_i$ и $\Delta QBER_i$ соответственно) для каждого из проведенных тестов.

Таблица 1

Глобальные средние значения и коэффициент изменения относительно 1-ого теста для скорости выработки просеянного ключа и QBER

№ теста	$SPEED_i$, бит/с	$\Delta SPEED_i$	$QBER_i$, %	$\Delta QBER_i$
1	558	–	2.77	–
2	41	13.615	37.309	13.468
3	64	8.787	42.649	15.396
4	100	5.563	33.935	12.25
5	290	1.927	6.261	2.26
6	290	1.922	4.42	1.595
7	322	1.732	3.528	1.274
8	96	5.811	6.957	2.511
9	51	11.045	16.494	5.954
10	33	17.054	24.069	8.689

Заключение

Таким образом, экспериментальные методики оценки изменения характеристик квантового атмосферного канала связи были протестированы. В ходе тестирования было выявлено, что наибольшее воздействие на QBER и скорость выработки просеянного ключа есть у парафиновой свечи, имитирующей тепловые возмущения в атмосферной среде [17]. Также было выявлено, что наиболее сильные возмущения характеристик в квантовом атмосферном канале возникали при нахождении источника возмущения рядом с коллиматором «Боба», это, видимо, обусловлено тем, что в блоках КРК, используемых в наших экспериментах источник и приемник фотонов расположен в блоке «Боб».

Очевидно, что оптические искажения вызывающие отклонения лазерного луча вблизи источника излучения приводят к наибольшим оптическим потерям в данной экспериментальной установке. Воздействие от водного аэрозоля на оптической трассе на передачу квантового ключа оказалось не такое значительное, как можно было ожидать из данных [18], но это вызвано в первую очередь малым размером области, где присутствовал аэрозоль, кроме этого, в дальнейшем следует осуществлять контроль размера аэрозольных частиц и их концентрации на трассе.

Экспериментальный стенд, на котором были проведены представленные выше исследования, следует обязательно дополнить устройством, позволяющим контролировать оптические возмущения, создаваемых нами в процессе выполнения тестов. Такое устройство планируется создать на основе датчика волнового фронта на основе эффекта Тальбота [19-22]. Датчик Тальбота позволит визуализировать и измерять возмущения показателя преломления не только воздушной среды, но и в низкотемпературной плазме [22]. Мы планируем в дальнейших работах провести сопоставление изменения параметров квантового канала связи с пространственным изменением показателя преломления воздушной среды, определяемых с помощью Датчика Тальбота [20, 21].

Литература

1. *Pchelkina N.V*. et al. Investigation of the Atmospheric Optical Disturbances Impact on the Free Space Optics Quantum Key Distribution // 2024 Systems of Signal Synchronization, Generating and Processing in Telecommunications (SYNCHROINFO). IEEE, 2024. С. 1-7.

2. *Боев А.А*. и др. Возможность построения модульной системы квантового распределения ключей в атмосфере // Письма в Журнал технической физики. 2022. Т. 48. № 15. С. 15.

3. *Sidhu J.S*. et al. Advances in space quantum communications // IET Quantum Communication. 2021. Т. 2. №. 4. С. 182-217.

4. *Ерохин К.Ю*. и др. Применимость технологии квантового распределения ключей в свободной атмосфере при построении сегментов современных квантовых коммуникационных сетей // Оптический журнал. 2024. Т. 91. № 11. С. 63-70.

5. *Davidson Z.C.M*. et al. AIRQKD: the role of free-space optics quantum key distribution enabling pragmatic secure and scalable communications // IEEE Communications Magazine. 2024. Т. 62. № 10. С. 40-47.

6. *Bolotov D.V*. et al. Modular Facility of Quantum Key Distribution in a Free Space // 2023 Wave Electronics and its Application in Information and Telecommunication Systems (WECONF). IEEE, 2023. С. 1-5.

7. *Бахус А.В., Ерохин К.Ю., Казанцев С.Ю*. Влияние фона на передачу квантового ключа в свободной атмосфере, реализованной на терминалах АОЛС М1-40GE // XIII международная конференция по фотонике и информационной оптике сборник научных трудов. Москва. 2024. Т. 24. С. 465-466.

8. *Наниджанян А.К., Жуковский Д.Д., Казанцев С.Ю*. Аппаратно-программный комплекс для исследования влияния атмосферных возмущений на передачу квантового ключа в свободной атмосфере // Современная педагогика и научные исследования в образовательной организации высшего образования. Материалы Всероссийской научно-методической конференции. Кострома. 2024. С. 32-38.

9. *Наниджанян А.К*. и др. Влияние атмосферных помех на мощность передаваемого сигнала // Инженерные технологии: традиции, инновации, векторы развития. материалы X Всероссийской научно-практической конференции с международным участием. Абакан. 2024. С. 76-77.

10. *Lu Q. H.* et al. Quantum key distribution over a mimicked dynamic-scattering channel // Science China Information Sciences. 2024. Т. 67. № 4. С. 142503.

11. *Жуковский Д.Д., Наниджанян А.К*. Лабораторный стенд для исследования внешних влияний на характеристики атмосферной оптической свзязи // Новые технологии. Наука, техника, педагогика = New Technologies. Science, Engineering, Pedagogics : Материалы Всероссийской научно-практической конференции = Proceedings of the All-Russian scientific-practical conference. 2024. С. 442-448.

12. *Kumar A.* et al. Futuristic view of the internet of quantum drones: review, challenges and research agenda //Vehicular Communications. 2022. Т. 36. P. 100487.

13. *Nzekwu N.J*. et al. A Comprehensive Review of UAV-Assisted FSO Relay Systems // Photonics. MDPI, 2024. Т. 11. №. 3. P. 274.

14. *Бахус А.В*. и др. Измерение квантовой эффективности детекторов одиночных фотонов на EMQOS 1.0 // XII международная конференция по фотонике и информационной оптике. 2023. С. 533-534.

15. *Rabenandrasana J*., et al. Development of a metrological system for measuring the characteristics of single photon detectors based on an educational platform EMQOS 1.0 // Systems of Signals Generating and Processing in the Field of on Board Communications. 2023. Т. 6. № 1. P. 380-383.

16. *Казанцев С.Ю*. и др. Модульная установка квантового распределения ключей в свободной атмосфере // Наука, техника, педагогика в высшей школе. 2023. С. 205-211.

17. *Наниджанян А.К., Жуковский Д.Д*. Воздействие тепловых возмущений в атмосфере на поляризацию лазерного излучения // СНК-2024: материалы LXXIV международной студенческой научной конференции Московского Политеха. 2024. С. 642-647.

18. *Бахус А.В., Ерохин К.Ю., Калюнин А.Д*. Внешние факторы, влияющие на квантовое распределение ключа в атмосферных оптических линиях связи // Новые технологии. Наука, техника, педагогика = New Technologies. Science, Engineering, Pedagogics. Материалы Всероссийской научно-практической конференции = Proceedings of the All-Russian scientific-practical conference. 2024. С. 392-397.

19. *Волкова Л.В.* и др. Датчик волнового фронта широкоапертурных лазерных пучков и его применение // Журнал технической физики. 2022. Т. 92. №. 9. С. 1410.

20. *Казанцев С.Ю., Пчелкина Н.В., Смольский А.А*. Визуализация возмущения оптической плотности среды с помощью датчика волнового фронта на эффекте Тальбота //REDS: Телекоммуникационные устройства и системы. 2023. Т. 13. № 4. С. 4-9.

21. *Касимов К.М., Рабенандрасана Ж., Чижин Д.Д*. Программный анализ изображений датчика волнового фронта на основе эффекта Тальбота // Новые технологии. Наука, техника, педагогика = New Technologies. Science, Engineering, Pedagogics. Материалы Всероссийской научно-практической конференции = Proceedings of the All-Russian scientific-practical conference. 2024. С. 452-459.

22. *Kazantsev S.Y*., et al. Peculiarities of Formation of Plasma Structures in Working Mixtures of Electrochemical HF (DF) Lasers and Methods for Their Study // High Energy Chemistry. 2023. Т. 57. № Suppl 1. P. S91-S94.