НАУЧНЫЙ ЖУРНАЛ

СИСТЕМЫ СИНХРОНИЗАЦИИ, ФОРМИРОВАНИЯ И ОБРАБОТКИ СИГНАЛОВ

№3-2026 год

Учредитель:
ООО «ИД Медиа Паблишер»

Номер подписан в печать 30.04.2026 г.

СОДЕРЖАНИЕ

АНАЛИЗ И ПЕРСПЕКТИВЫ РАЗВИТИЯ ТЕХНОЛОГИИ 10G-EPON

Данилов Алексей Николаевич
Московский Технический Университет Связи и Информатики, доцент, к.т.н., Москва, Россия,
alexnicdanilov@yandex.ru

Петрович Никита Русланович
Московский Технический Университет Связи и Информатики, студент группы БСС2201, Москва, Россия
petrowitch.nickita2018@yandex.ru

Аннотация
В работе проводится анализ технологии пассивной оптической сети стандарта 10G-EPON. Рассматриваются основные архитектурные решения, такие как ассиметричный режим работы оптического приемника и проведен сравнительный анализ с технологией предыдущего поколения. Оценены ключевые изменения в области кодирования, переход на новую схему кодирования (64B/66B) и внедрение потокового FEC. Проведен сравнительный анализ интерфейсов GMII и XGMII. Даны оценки перспектив экономического и технологического развития технологии 10G-EPON.

Ключевые слова
10G-EPON, PON, пассивные оптические сети, IEEE 802.3av, кодирование 64B/66B, интерфейс XGMII, обратная совместимость, ассиметричный режим.

Введение

В данной работе произведен анализ технологии 10G-EPON и перспектив ее развития по технологическим, эксплуатационным характеристикам и экономическим показателям.

Прежде всего проведем сопоставительный анализ 10G-EPON с технологией предыдущего поколения 1G-EPON.

1G-EPON, являющийся частью стандарта IEEE 802.3, на 2008 год обеспечивал необходимую полосу пропускания в 1,25 Гбит/сек. Однако проприетарный характер технологических решений EPON, с более высокой скоростью, ограничивал количество поставщиков и совместимость системных агрегаторов при интеграции. Совокупность этих факторов приводила к некоторым экономическим и технологическим трудностям в реализации данной технологии. С ростом требований к пропускной способности, качеству доставки мультимедиа-контента, а также развитием облачных сервисов и Интернета вещей, возникла необходимость развить или заменить существующую 1G-EPON сеть на более скоростную [1].

Появление технологии 10G-EPON было логичным эволюционным шагом, особенно на фоне роста количества мультимедиа-контента, более высоких требований к скорости передачи данных и новым требованиям к оборудованию. 10G-EPON достиг масштабов развертывания, намного превышающих существующие решений PON. 10G-EPON, имеющий скорость, в 10 раз превышающую технологии предыдущего поколения (8,9 Гбит/сек с учетом обязательного прямого исправления ошибок) и обеспечивающий необходимую пропускную способность для приложений нового поколения, имеет эволюционный характер развития. Это подразумевает обратную совместимость. Операторы модифицировали существующее оборудование 1G-EPON, без необходимости полной замены оборудования. Проект 10G-EPON P802.3av является дополнением к технологии EPON, что означает, что стоимость развертывания на одного абонента сравнима с оборудованием 1G-EPON, при этом обеспечивая более высокую плотность абонентов на станции и окупая инвестиции для уже развернутого оборудования [2].

Результаты исследования

Стоит отметить гибкость, с которой был разработан стандарт 10G-EPON. Для повторного использования отдельных элементов, входящих в состав уровней стандарта IEEE 802.3, они подразделяются на несколько подуровней, объединенных стандартизированными интерфейсами. Это позволяет выстраивать проекты, такие как P802.3av, на базе спецификаций предыдущих проектов (например, P802.3ae 10GE или P802.3ah), лишь вводя новые расширения для поддержки новых функций. Модульность спецификаций 802.3 позволяет снизить затраты на разработку и ускорить цикл разработки, применяя технологии и проектные решения из предыдущего поколения устройств (или из других линеек продукции).

Одно из основных отличий технологии 10G-EPON от 1G-EPON заключается в асимметричном режиме

передачи данных. В случае приемника OLT с одной скоростью передачи данных, поддерживающий 1 Гбит/сек или 10 Гбит/сек, приемник может быть оптимизирован для обработки целевой скорости передачи данных в восходящем канале. Однако в случае двухскоростного устройства, приемник становится сложнее. Приемник выполняет регулировку усиления, определяет скорость передачи данных без дополнительной информации, на основе ожидаемой скорости передачи данных восходящих пакетов. Таким образом, приемник принимает пакеты как от ONU 1G-EPON, так и ONU 10G-EPON. Единственный оптический интерфейс принимает оптические сигналы в полосе 1260-1360 нм, исключая все остальные. Приемник OLT разделяет входящий канал на два независимых пути, которые затем передаются на канальный уровень. Основная сложность заключается в разделении сигнала и последующей обработки.

Разделение может происходить двумя разными способами:

- Сигнал разделяется в оптической области и затем передается на два независимых фотодетектора (как показано на рисунке 1а).
- Сигнал может быть обнаружен с помощью одного фотодетектора, а затем разделен в электрической области (как показано на рисунке 1б).

В первом случае электронный блок более простой, так как два приемника могут быть оптимизированы для максимальной чувствительности под каждую скорость (1 Гбит/сек и 10 Гбит/сек). Такой вариант требует большего количества оптических компонентов, где каждый приемник оптимизирован под свою скорость, но разделение в восходящем канале вносит дополнительные потери.

Во втором случае используется только один оптический модуль, но фотодетектор должен автоматически настраиваться на скорость передачи данных, что означает более высокие требования к быстродействию и алгоритмам обработки электронной схемы. Таким образом, электрический блок должен моментально переключаться между пакетами.

На рисунке 1 показаны две архитектурные схемы решения двухскоростного пакетного приемника.

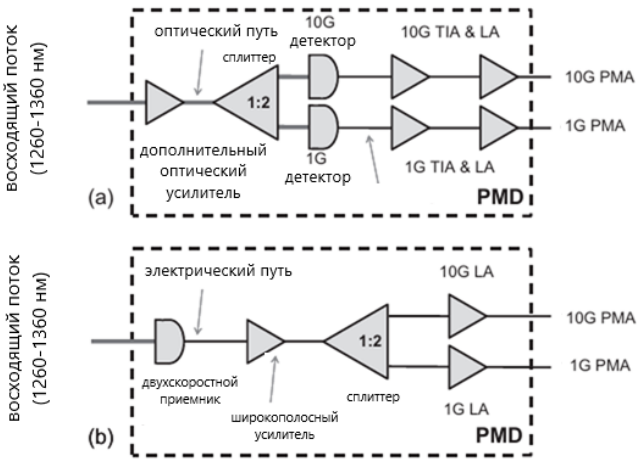


Рис. 1. Схема двухскоростного пакетного приемника

Однако, несмотря на сложности технической реализации асимметричной работы приемника, такой подход обеспечивает обратную совместимость с технологией предыдущего поколения, а также возможность расширить существующую сеть за счет модернизации существующего оборудования. Именно технология асимметричной передачи данных позволила достичь скорости в 10 Гбит/сек. Фактически увеличилась полоса пропускания, восходящий канал теперь не ограничен скоростью в 1 Гбит/сек, что увеличило общую пропускную способность в 10 раз.

Двухскоростной приемник повышает эффективность передачи данных, так как оптический линейный терминал OLT знает, с какой скоростью работает каждый ONU, что позволяет терминалу эффективно выделять временные интервалы под передачу данных.

Рассмотрим главные отличия на подуровне физического кодирования технологий 10G-EPON и 1G-EPON, которые позволили достигнуть скорость передачи данных в 10 Гбит/сек.

Основные новшества касаются метода коррекции ошибок, линейного кодирования и механизмов управления передачи данных.

Главное отличие между технологиями заключается в схемах линейного кодирования.

В случае технологии 1G-EPON применяется схема кодирования 8B/10B. Каждые 8 бит данных преобразуются в 10-битные символы. Такой способ кодирования создает 25%-ную избыточность (на 8 бит полезной нагрузки приходится 2 служебных бита), что снижает эффективную пропускную способность канала [3].

В технологии 10G-EPON используется более эффективная схема кодирования 64B/66B, которая была разработана для высокоскоростных Ethernet стандартов. В такой схеме каждые 64 бита данных кодируются в 66-битные блоки данных, таким образом избыточность составляет около 3%. Такое изменение позволило эффективней использовать полосу пропускания, что увеличило фактическую скорость с 1 Гбит/сек до 8,9 Гбит/сек [4].

В блоке исправления ошибок также произошли радикальные изменения. В стандарте 1G-EPON FEC был опциональным и кадровым. В 10G-EPON используется потоковый FEC, использующий код Рида-Соломона RS (255, 223). Этот код используется как для нисходящих каналов, так и для восходящих. В случае 1G-EPON контрольные байты добавляются в конце каждого кадра. В 10G-EPON биты четности FEC добавляются в непрерывный поток данных после кодирования. В таком потоке блоки данных чередуются с контрольными байтами.

Устройство 10G-EPON, не поддерживающее FEC, не сможет декодировать поток данных, так как не сможет отделить полезные данные от байтов четности.

В стандарте 10G-EPON был внедрен новый механизм управления передачей данных - механизм удаления холостых символов для обеспечения корректной работы FEC. В верхней части PCS происходит удаление избыточных символов IDLE, которые подуровень MAC вставляет между кадрами. В промежутки между кадрами добавляются биты четности FEC.

В восходящем канале 10G-EPON появился детектор данных. Буфер FIFO используется как линия задержки. Его основная задача - управление лазером. Лазер включается для передачи служебных блоков данных перед началом передачи полезной информации и отключается между передачами, чтобы избежать взаимных помех между оптическими сетевыми устройствами ONU.

Комплексная модернизация физического подуровня позволила достичь скорости и увеличить пропускную способность в стандарте 10G-EPON. Переход от схемы кодирования 8B/10B к 64B/66B привел к более эффективному использованию полосы пропускания и уменьшению избыточности кодирования. Потоковый FEC, который стал обязателен в стандарте 10G-EPON, значительно повысил надежность по сравнению со стандартом 1G-EPON. Система управления передачей данных стала более сложной. Все эти технические решения не только привели к увеличению скорости, но и заложили основу для дальнейшего развития оптических сетей.

Изменения претерпели интерфейсы взаимодействия, которые обеспечивают асимметричную работу и обратную совместимость. Одним из важнейших в технологии EPON является интерфейс, не зависимый от среды (xMII), которые является частью стандарта IEEE 802.3. Это - интерфейс общего назначения, который разделяет подуровень MAC от подуровня PHY. Фактически, интерфейс xMII защищает верхние уровни стека от необходимости взаимодействовать со множеством различных типов PHY. Это позволяет производителям создавать универсальные MAC-контроллеры и подключать к ним различные трансиверы через один интерфейс xMII.

В случае симметричной работы (10/10G-EPON) OLT и ONU используют единый интерфейс XGMII для соединения подуровня согласования с подуровнем кодирования.

При асимметричной работе устройство (OLT или ONU) работает с разными скоростями. Например, архитектура OLT 10/1G выглядит так: данные в нисходящем потоке 10 Гбит/сек от MAC передаются через XGMII, а на приеме данные из сети поступают через GMII. В случае ONU 10/1G ситуация обратная, прием данных от OLT идет через XGMII, а передача к OLT – через GMII.

Эволюция интерфейсов в EPON от GMII к XGMII и совместное их использование при асимметричной передаче данных в 10G-EPON показывает эволюционный подход к развитию технологии EPON. Новые интерфейсы позволили обрабатывать большие объемы данных. Гибкость архитектурных решений позволила операторам выбирать наиболее оптимальные сценарии развертывания. Независимые от среды интерфейсы обеспечили необходимый уровень модульности и изолированности отдельных частей систем, что позволило заложить основу сетям нового поколения и развить существующие технологии.

На данный момент стандарт 10G-EPON является доминирующей технологией гигабитного доступа. Ключевым экономическим преимуществом технологии можно назвать возможность интеграции ее в многостандартные экосистемы, без замены волоконно-оптической инфраструктуры, что позволяет операторам максимизировать окупаемость инвестиций.

Наиболее стратегически важной перспективой можно назвать сближение стандартов IEEE и МСЭ-Т. В результате возрастает объем производства аппаратуры, а также снижаются затраты на производство. Так, например, уже существуют мультистандартные OLT, способные поддерживать работу с терминалами как 10G-EPON, так и XGS-PON. Со временем OLT перестанут быть привязаны к одному стандарту и будут поддерживать несколько PON технологий.

Развитие 10G-EPON было направлено не только на рынок частных домов, но и такие сегменты как: мобильный транспорт, где с ростом трафика появилась необходимость в высокой скорости и надежности, и корпоративный сегмент, для подключения офисов и государственных учреждений.

В долгосрочной перспективе стандарт 10G-EPON станет одним из ключевых элементов перехода к следующему поколению PON (25G/50G), сохраняя свою роль в сегментах, где важны экономическая эффективность и совместимость с существующей инфраструктурой.

В современных условиях развития сетей доступа наблюдается тенденция к конвергенции различных стандартов пассивных оптических сетей, что позволяет операторам гибко управлять инфраструктурой. Одним из ключевых направлений является сближение технологий 10G-EPON (стандарт IEEE 802.3av) и XGS-PON (стандарт МСЭ-Т G.9807.1), которые становятся совместимыми на уровне оборудования и управления.

Предпосылки конвергенции обусловлены тем, что оба стандарта обеспечивают скорость передачи данных до 10 Гбит/с в нисходящем и восходящем каналах, но используют различные методы кодирования, структуру кадров и протоколы управления. 10G-EPON основан на архитектуре Ethernet, использует кодирование 64B/66B и потоковый FEC, в то время как XGS-PON применяет кодирование NRZ, кадры GEM и протокол управления OMCI. Однако развитие мультистандартных OLT (Optical Line Terminal) позволяет поддерживать оба стандарта на одной аппаратной платформе за счёт программируемых физических уровней (Programmable PHY) и виртуализации функций доступа (vOLT).

Архитектура мультистандартных OLT строится на возможности одновременной работы с ONU 10G-EPON и XGS-PON на одном оптическом распределительном сети (ODN). Это достигается за счёт динамического распределения длин волн: 10G-EPON использует пару 1577 нм (нисходящий поток)/1270 нм (восходящий поток), а XGS-PON может работать в тех же или дополнительных спектральных окнах (например, 1590 нм), разделяемых с помощью WDM-фильтров в OLT. Кроме того, применение программируемых чипсетов, таких как Broadcom BCM88690, позволяет динамически переключаться между стандартами в зависимости от типа подключённой ONU, а унифицированные системы управления на базе стандартов TR-069 или YANG-моделей обеспечивают централизованное администрирование разнотипных терминалов через единый интерфейс [5].

Эксплуатационные преимущества такой конвергенции включают возможность поэтапной модернизации сети, при которой операторы могут внедрять XGS-PON, сохраняя существующие подключения 10G-EPON без замены оптической инфраструктуры. Это ведёт к значительному снижению капитальных (CAPEX) и операционных (OPEX) затрат за счёт использования единой платформы, сокращения энергопотребления и упрощения обучения персонала. Кроме того, конвергенция обеспечивает гибкость тарифной политики, позволяя предлагать абонентам разные технологии в зависимости от потребностей — например, 10G-EPON для жилых домов и XGS-PON для корпоративных клиентов. Мультистандартные OLT закладывают основу для перехода к следующему поколению сетей, поскольку могут быть программно обновлены до поддержки 25G/50G-PON, что продлевает жизненный цикл оборудования и защищает инвестиции операторов.

Несмотря на преимущества, конвергенция 10G-EPON и XGS-PON сталкивается с рядом технических и организационных вызовов. Одной из ключевых задач является обеспечение совместимости абонентских устройств (ONU). Для этого требуются гибридные модули, способные работать в обоих стандартах, например, XGS-PON ONU с поддержкой эмуляции 10G-EPON. Это усложняет конструкцию терминалов и влияет на их стоимость. Также для эффективного управления ресурсами в конвергентной сети требуется разработка интеллектуальных алгоритмов динамического распределения полосы пропускания между стандартами, что повышает сложность систем управления и планирования. Нормативная и стандартизационная работа также остаётся важным фактором: несмотря на прогресс в рамках IEEE и МСЭ-Т, сохраняется необходимость унификации интерфейсов, протоколов управления и процедур взаимодействия между экосистемами, чтобы обеспечить полную совместимость и снизить риски для операторов при развёртывании гибридных решений.

Заключение

Конвергенция 10G-EPON и XGS-PON представляет собой важный промежуточный этап в эволюции оптических сетей доступа, создающий основу для перехода к более гибким и программно-определяемым архитектурам. В среднесрочной перспективе ожидается развитие полностью конвергентных PON (CPON), в рамках которых один OLT сможет поддерживать широкий спектр стандартов - от EPON и GPON до XG(S)-PON и 25G/50G-PON – с динамическим распределением ресурсов в реальном времени. Это будет сопровождаться внедрением принципов программно-определяемых сетей доступа (SD-Access), где управление физическим уровнем, выделение полосы пропускания и настройка служб будут осуществляться централизованно через программные контроллеры, что повысит гибкость, автоматизацию и экономическую эффективность эксплуатации сетей. Долгосрочной тенденцией станет интеграция PON-технологий в единые инфраструктурные платформы, объединяющие фиксированный и мобильный доступ (Fixed-Mobile Convergence), где 10G-EPON и XGS-PON будут играть роль высокопроизводительного транспортного слоя для сервисов 5G/6G, Интернета вещей и облачных приложений.

Таким образом, конвергенция не только расширяет возможности текущих развёртываний, но и формирует технологический фундамент для сетей следующего поколения, обеспечивая масштабируемость, эффективность и долгосрочную устойчивость решений на основе пассивных оптических сетей.

Литература

1. ITU-T G.9807.1 (02/2023): 10-Gigabit-capable symmetric passive optical network (XGS-PON). Geneva: ITU, 2023. 124 p.

2. Inewski K. (Ed.) Convergence of mobile and stationary next-generation networks. Hoboken, New Jersey: John Wiley & Sons, Inc., 2010. 784 p.

3. *Бертенев М. Б., Горетый М. А., Хмелевский А. В.* Анализ технологий пассивных оптических сетей // Инфокоммуникации и космические технологии: состояние, проблемы и пути решения: сборник научных статей по материалам VII Всероссийской научно-практической конференции. Курск: Юго-Зап. Гос. Ун-т. 2025. С. 123-127.

4. Global Market Report: PON Equipment 2020–2025. Dell'Oro Group, 2024. 45 p.

5. *Oscar J. Ciceri, Carlos A. Astudillo, Zuqing Zhu, Nelson L.S. da Fonseca*. Federated Learning over Next-Generation Ethernet Passive Optical Networks // IEEE Network-January/February 2023. Vol. 37, No. 1, pp. 70-76.

ВЫБОР ОБОРУДОВАНИЯ ДЛЯ ПОСТРОЕНИЯ ФИЗИЧЕСКОГО УРОВНЯ СЕТИ ПЕРЕДАЧИ ДАННЫХ

Каширин Иван Владимирович
МТУСИ, студент группы БСТ2204, Москва, Россия,
sdbereg@gmail.com

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

Аннотация
Одним из основных видов сетей являются оптические сети. За последние четыре года с рынка Российской Федерации ушло большое количество брендов, на место которых претендуют отечественные производители. В работе рассматриваются основные критерии и приводится анализ оборудования этих поставщиков.

Ключевые слова:
Оптические сети, оборудование оптических сетей, архитектурная модель сети, критерии оценивания, параметры оценивания

Введение

Оптические транспортные сети (OTN) остаются одной из важнейших деталей цифровой инфраструктуры России [1-3], обеспечивая передачу растущих объёмов данных в условиях масштабной цифровизации экономики, строительства центров обработки данных и реализации государственных ИТ-инициатив [4-6]. Однако начиная с 2022 года отрасль столкнулась с проблемой: значительная часть западных вендоров — Cisco, Ciena, Nokia, а также частично Huawei – либо полностью покинули российский рынок, либо резко ограничили поставки оборудования, программного обеспечения и технической поддержки. В результате, на смену хорошо совместимым решениям пришли новые вендоры, состоящие из отечественных платформ, оборудованием из дружественных стран и остаточные поставки через «серый рынок».

Сегодня на рынке активно представлены такие игроки, как «Элтекс», «Ситроникс Телеком», «ИНПРОТЕК», «Микран», а также ZTE и ограниченные партии Huawei или бывшего в употреблении Ciena. Каждый из этих вендоров предлагает собственные архитектурные подходы, протоколы управления, разные уровни локализации ПО и разные требования к эксплуатации. Это порождает ситуацию в которой решения формально работают, но их совместимость не гарантируется, а при интеграции часто теряются ключевые функции — например, сквозной мониторинг OTN, поддержка ROADM, эффективная FEC-коррекция.

В таких условиях больше нельзя полагаться на привычные сценарии «plug-and-play» или рекомендации производителей, ориентированные на глобальные рынки. Возникает острая необходимость в методически выверенном подходе к выбору оборудования, основанном не на маркетинговых заявлениях, а на количественных расчётах физических параметров канала (затухание, дисперсия, OSNR), оценке совокупной стоимости владения, надёжности, энергоэффективности и, что особенно важно, реальной совместимости компонентов в условиях российской инфраструктуры.

Цель данной работы – определить подход, который позволяет не просто перечислить доступные решения, а обоснованно выбрать оптимальное оборудование на основе комплексного анализа.

Анализ вендоров

До 2022 года большая часть российского рынка приходилась на западных лидеров. Однако санкционные ограничения привели к радикальному пересмотру этой системы. Из 12 ключевых вендоров, чьи решения активно рассматривались при проектировании OTN-сетей в РФ до 2022 года, 7 были западными компаниями, и все они либо полностью ушли с рынка, либо стали фактически недоступны для новых проектов.

Следующие компании полностью прекратили официальные поставки, техническую поддержку, обновления ПО и гарантийное обслуживание:

- Cisco (США) – полный уход; оборудование доступно только на вторичном рынке.
- Ciena (США/Канада) – прекращены все поставки; б/у решения не имеют поддержки.

- Nokia (Финляндия) – прекращение деятельность на территории РФ.
- Ericsson (Швеция) – не был самым массовым решением, но учавствовал в интегрированных проектах, прекратил деятельность на территории РФ.

Фактически недоступны, несмотря на частичное присутствие:

- Huawei (Китай) – поставки возможны только через «серый рынок» или параллельный импорт, без обновлений ПО и гарантий.
- ADVA (Германия, часть Adtran) – оборудование использовалось в метрополитенских сетях, но сейчас недоступно.
- Infinera (США) – присутствовал в пилотных проектах, но не обеспечивает поддержку.

Итог: 7 западных лидеров – 4 полностью ушли, а 3 остались лишь формально [7]. Их совокупная доля в новых закупках в 2025 году – менее 2 %, преимущественно в виде временных решений.

На смену ушедшим компаниям пришли отечественные производители и вендоры из дружественных стран, которые сегодня обеспечивают более 95 % новых поставок:

- «Элтекс» (Новосибирск) – лидер среди отечественных компаний; полностью импортонезависим, совместим с MSA.
- «Ситроникс Телеком» (в составе «Росэлектроники») – ключевой поставщик для госсектора, сертифицирован по ФСТЭК и ГОСТ Р [8,9].
- «ИНПРОТЕК», «Микран», «Орион Телеком» – нишевые, но надёжные отечественные платформы с 100 % локализацией.
- ZTE (Китай) – единственный крупный иностранный вендор с легальными поставками DWDM/OTN-оборудования (включая 100G/400G).

«Элтекс» и «Ситроникс» – до 2022 года фокусировались на сегменте доступа и госзаказах. Сегодня – основа магистральных и метрополитенских сетей.

ZTE – ранее конкурировал с Cisco/Nokia на равных; теперь стал де-факто стандартом для коммерческих операторов из-за своего баланса между ценой и функциональностью.

Белорусские и турецкие производители («Интеграл», «МСИ», TurkNet, Aselsan) – начали входить на рынок как альтернативные источники, хотя их доля пока не превышает 3-5% и сосредоточена в специализированных проектах.

Предлагаемые архитектурные модели

Проектирование современной оптической транспортной сети (OTN/DWDM) в условиях РФ выходит за рамки классических физических расчётов. Сегодня инженер обязан учитывать три взаимосвязанных группы ограничений: физические, финансовые и климатические. Игнорирование хотя бы одной из них может привести к нестабильной работе, высокой стоимости владения или полной неработоспособности системы в реальных условиях эксплуатации.

В основном используется архитектура, схема которой представлена на рисунке 1:

Базовый уровень проектирования, определяет техническую возможность передачи сигнала:

- Затухание: суммарные потери в волокне, соединителях и пассивных компонентах не должны превышать бюджет мощности транспондера (обычно 25-30 дБ для 100G).
- OSNR (оптическое отношение сигнал/шум): должен быть выше порога чувствительности приёмника (10-12 дБ для 100G DP-QPSK). Недостаточный OSNR приводит к росту BER и потере данных.
- Дисперсия: хроматическая (CD) и поляризационная модовая (PMD) дисперсия ограничивают максимальную длину линии без компенсации. Особенно критична PMD на старых трассах (РЖД, МТС), где её значение может достигать 0.5-1.0 пс/√км.
- Нелинейные эффекты: при плотном DWDM (50 ГГц шаг) и высокой мощности возникают FWM, SPM, XPM, что требует снижения мощности на канал (рекомендуется ≤ +1 дБм).

В условиях санкционной реальности стоимость владения (TCO) становится одним из ключевых факторов [10-12]:

- CAPEX (капитальные затраты): цена оборудования, включая транспондеры, ROADM, EDFA. Западные решения (Cisco, Ciena) формально дешевле на вторичном рынке, но не имеют поддержки ПО.
- OPEX (операционные или текущие затраты): расходы на обслуживание, spare parts, энергопотребление, термоконтейнеры. «Серый рынок»-оборудование не имеет поддержки – OPEX резко возрастает [13-15].

- Риски недоступности: закупка Huawei или Ciena сегодня может означать невозможность масштабирования проекта в будущем.
- Энергопотребление: отечественные платформы («Элтекс», «Микран») потребляют на 15–20 % больше, чем ZTE, что увеличивает эксплуатационные расходы.

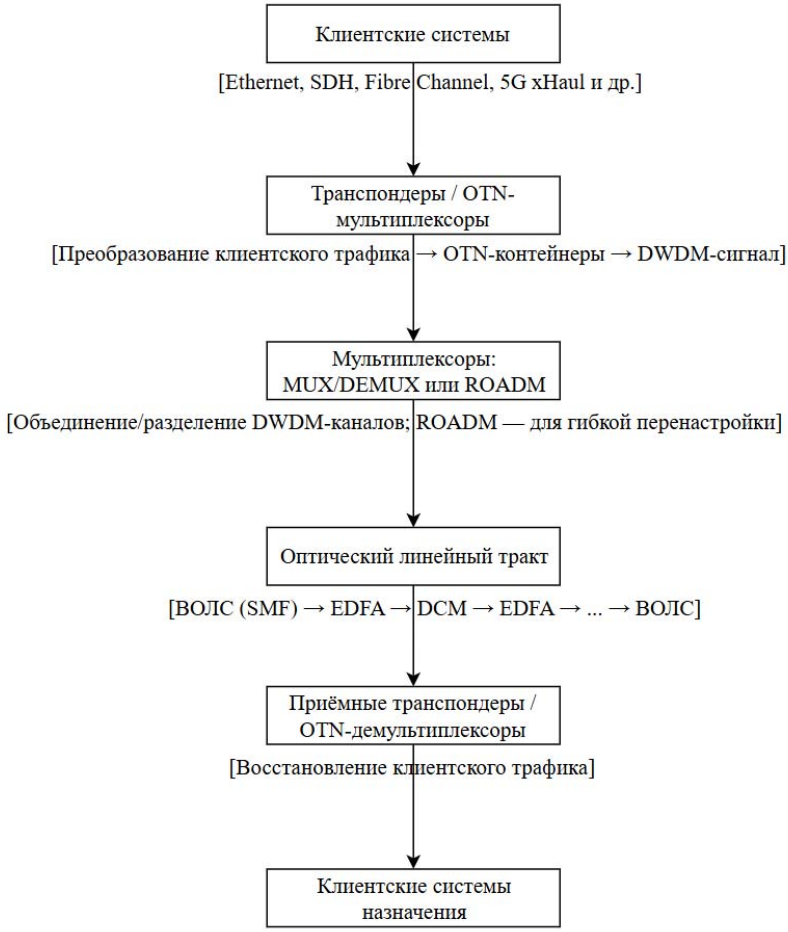


Рис. 1. Пример архитектуры сети

Российская специфика требует обязательного учёта экстремальных условий [16-18]:

- Температурный диапазон: оборудование должно работать при −40…+55 °C.
- Влажность: до 95 % без конденсации.
- Антивандальная защита: IP30 и выше для уличных шкафов.
- Последствия игнорирования:
- ZTE требует термоконтейнеров при T < −25 °C что ведет к +15–20 % к CAPEX.
- «Элтекс», «ИНПРОТЕК» работают «из коробки» нулевые дополнительные затраты.

Таким образом при расчёте параметров оптической сети должен находиться в балансе между физической реализуемостью, экономической целесообразностью и климатической устойчивостью.

Анализ параметров передачи

Минимальный OSNR для корректной работы 100G DP-QPSK системы с SD-FEC (Soft-Decision Forward Error Correction) может быть оценён по формуле 1:

$$\mathrm{OSNR}_{\min} = 10\log_{10}\left(\frac{B_0}{B_n}\right) + \mathrm{SNR}_{\mathrm{req}}, \quad (1)$$

где:

- B_0 = 12.5 ГГц – опорная полоса,
- B_n – полоса канала (например, 37.5 ГГц для 50 ГГц сетки),
- SNR_{req} – требуемое отношение сигнал/шум на входе декодера (обычно 7-9 дБ).
- Для 400G ZR/ZR+ (400G-FR4) требования повышаются до 14-16 дБ OSNR, что накладывает жёсткие ограничения на длину пролёта и количество EDFA.

Хроматическая дисперсия в SMF составляет ~17 пс/(нм·км) на 1550 нм. При скорости 100G (символьная скорость 32 ГБод) максимальная длина без компенсации, расчет представлен в 2:

$$L_{CD} = \frac{1}{D \times \Delta\lambda \times B^2}, \quad (2)$$

Где:

Δ – ширина спектра сигнала. Современные когерентные приёмники позволяют компенсировать до 30 000 пс/нм цифровым способом (в DSP), что эквивалентно ~1700 км SMF.

Бюджет затухания (Power Budget) определяет максимальную допустимую длину участка без усиления:

$$P_{tx} - P_{rx,min} \geq \alpha L + \sum \Delta_{conn} + \Delta_{mux/demux} + \Delta_{margin}, \quad (3)$$

Где:

P_{tx} – выходная мощность транспондера (дБм)

$P_{rx,\,min}$ – чувствительность приёмника (дБм)

α – затухание волокна (дб/км)

L – длина линии (км)

$\sum \Delta_{conn}$ – потери в соединителях (~0.3 дБ на штуку)

$\Delta_{mux/demux}$ – потери в MUX/DEMUX или ROADM (4-6 дБ)

Δ_{margin} – запас на старение и неоднородность волокна (рекомендуется 3-5 дБ в РФ из-за качества вторичного ВОЛС)

Хроматическая дисперсия (CD), рассчитывается по формуле 4:

$$D_{total} = DL, \quad (4)$$

Где:

D = 17 пс/(нм*км)

L – длина линии (км)

Максимальная компенсируемая дисперсия DSP-приёмником:

100G DP-QPSK → до 30 000–40 000 пс/нм (~1700–2300 км)

400G 16QAM → до 10 000–15 000 пс/нм (~600–900 км).

Поляризационная модовая дисперсия (PMD), рассчитывается по формуле 5

$$PMD_{total} = \sqrt{\sum \left(PMD_i\right)^2} \leq PMD_{max}, \quad (5)$$

Где:

PMD_i – PMD i-го участка (пс/$\sqrt{км}$)

Типичное значение для нового волокна: 0.1 пс/$\sqrt{км}$

Для старого волокна (например РЖД, МТС): 0.5-1.0 пс/$\sqrt{км}$

Максимально допустимая PMD:

10G ≤ 10 пс

100G ≤ 10 пс

400G ≤ 4-5 пс

Формула расчета итогового балла 6

$$S_i = \sum_{k=1}^{6} w_k \cdot x_{ik}, \quad (6)$$

Где:

w_k – вес k-го критерия (сумма = 1.0),

x_{ik} – нормированная оценка i-го оборудования по k-му критерию (от 0 до 1, где 1 = 10 баллов по 10 балльной шкале)

Сравнительный анализ оборудования

Для объективного выбора оборудования предложена многокритериальная система оценки [19-21], учитывающая специфику российского рынка. Оценка проводится по шести ключевым параметрам:

Веса определены на основании экспертной оценки исходя из приоритетов российского рынка в 2025 году, где главными стали надёжность, доступность и предсказуемость, а не максимальная производительность или минимальная цена:

- Качество передачи (0.20) – базовое условие работоспособности канала (OSNR, BER, FEC). Без него сеть невозможна.

Таблица 1

Критерии оценки

Критерий	Вес(оценка)	Пояснение
Качество передачи	0.20	Техническая основа – без неё нет канала. Сохраняем высокий вес.
Надёжность	0.20	Включает климатическую устойчивость (−40 °C) – критично для РФ.
Сервис и поддержка	0.20	Гарантия долгосрочной эксплуатации; дефицит после ухода западных вендоров.
Совместимость	0.15	Позволяет избежать «зоопарка», обеспечивает управляемость.
Энергоэффективность	0.15	Влияет на OPEX, но второстепенна по сравнению с отказоустойчивостью.
Цена (CAPEX)	0.10	Снижена, так как дешёвое оборудование без поддержки дороже в TCO.

- Надёжность (0.20) – включает MTBF и соответствие климатическим требованиям РФ. Критично для удалённых узлов.
- Сервис и поддержка (0.20) – наличие локальной техподдержки, spare parts и обновлений ПО. Гарантия долгосрочной эксплуатации.
- Совместимость (0.15) – открытость (MSA, G.709), возможность интеграции в гетерогенную среду, избежание «зоопарка».
- Энергоэффективность (0.15) – влияет на операционные расходы, но второстепенна по сравнению с отказоустойчивостью.
- Цена (CAPEX) (0.10) – дешёвое оборудование без поддержки (например, с «серого рынка») ведёт к росту TCO и рискам простоя.

Сумма весов = 1.0. Акцент сделан на эксплуатационную устойчивость, а не на первоначальную стоимость.

Принципы оценки по критериям представлены в таблице 2.

Таблица 2

Принцип оценки по критериям

Критерий	Высокая оценка (9–10)	Средняя (5–7)	Низкая (1–4)
Качество передачи	OSNR ≤10 дБ, FEC, DSP, BER < 10^{-15}	OSNR 11–12 дБ, базовый FEC	OSNR >13 дБ, нет FEC, grey market
Надёжность	MTBF ≥300 000 ч, работа до −40 °C	MTBF 200–300 тыс. ч, требует термоконтейнер	MTBF <200 тыс. ч, не для улицы
Сервис и поддержка	Локальная поддержка, spare parts, ПО	Ограниченная поддержка (через партнёров)	Grey market, без ПО и spare parts
Совместимость	MSA, G.709, открытые API	Частичная совместимость	Проприетарная система
Энергоэффективность	≤25 Вт/100G	25–35 Вт/100G	>35 Вт/100G
Цена (CAPEX)	≤0.9 млн руб./100G	0.9–1.2 млн руб./100G	>1.2 млн руб./100G

Из всех рассмотренных решений, таблица 3 наиболее сбалансированным и практичным выбором для развёртывания в российских условиях выглядит «Элтекс» LTP-16. Это оборудование демонстрирует высочайший уровень надёжности, полную локальную поддержку, что критически важно для долгосрочной эксплуатации. Несмотря на несколько более высокую CAPEX по сравнению с иностранными аналогами, его предсказуемость, доступность spare parts и совместимость с отечественной инфраструктурой делают его оптимальным решением как для коммерческих операторов, так и для государственных проектов.

ZTE ZXMP M721 и «Ситроникс» ST-OTN-9600 занимают следующую позицию с одинаковым итоговым баллом 0.77. ZTE предлагает привлекательное соотношение цены и технических характеристик, но требует дополнительных мер при эксплуатации в северных регионах (термоконтейнеры) и несёт риски, связанные с зависимостью от внешнего поставщика. «Ситроникс», в свою очередь, обеспечивает отличную надёжность и поддержку, особенно в госсекторе, но имеет более высокую стоимость владения.

Таблица 3

Итоговый расчет оценки

Название оборудования	Качество (0.20)	Надёжность (0.20)	Сервис (0.20)	Совместимость (0.15)	Энергия (0.15)	Цена (0.10)	Итог S_i
«Элтекс» LTP-16	0.8	0.9	0.9	0.8	0.7	0.7	0.82
ZTE ZXMP M721	0.9	0.6	0.7	0.8	0.8	0.9	0.77
«Ситроникс» ST-OTN-9600	0.8	0.9	0.8	0.7	0.7	0.6	0.77
«ИНПРОТЕК» OTN-400	0.7	0.9	0.8	0.6	0.6	0.5	0.71
«Микран» MT-100G	0.7	0.8	0.7	0.6	0.5	0.6	0.67
Huawei OSN 1800	0.8	0.4	0.2	0.3	0.7	0.8	0.51
Ciena 6500 (б/у)	0.9	0.3	0.1	0.2	0.8	0.7	0.48

Наименее подходящим вариантом для постоянного развёртывания остаётся бывшее в употреблении оборудование Ciena WaveServer Ai. Несмотря на выдающиеся технические параметры – низкий порог OSNR, высокую энергоэффективность и плотность размещения – его практическая применимость в текущих условиях крайне ограничена: отсутствие доступа к оригинальному программному обеспечению, сервисной поддержке, гарантийному обслуживанию и запасным частям превращает такие системы в «золотую клетку»: они могут работать безупречно до первого серьёзного сбоя, после которого восстановление может оказаться невозможным. Использование подобных решений оправдано разве что в краткосрочных, тестовых или временных сценариях, где не требуется высокая надёжность и длительная эксплуатация [22, 23].

Заключение

При выборе телекоммуникационного оборудования в условиях современной рыночной и геополитической составляющей недостаточно ориентироваться исключительно на первоначальные капитальные затраты (CAPEX). Важно учитывать совокупную стоимость владения, включающую как стартовые, так и эксплуатационные расходы (OPEX) на протяжении всего жизненного цикла системы [24, 25].

Одним из значимых компонентов OPEX является энергопотребление. Сравнительный анализ показывает, что оборудование ZTE демонстрирует уровень энергопотребления около 25 Вт на 100 Гбит/с, в то время как у российского производителя «Микран» этот показатель составляет приблизительно 33 Вт/100G, что на 30% выше. На масштабах магистральной или метрополитенской сети такая разница может существенно повлиять на ежегодные затраты на электроэнергию.

Важную роль также играет доступность и качество сервисной поддержки. Отечественные вендоры, такие как «Элтекс» и «Ситроникс», обеспечивают круглосуточную техническую поддержку на территории всей Российской Федерации, что способствует оперативному устранению неисправностей. В случае с оборудованием ZTE поддержка предоставляется исключительно через дистрибьюторские каналы, что может увеличивать время решения проблемы при возникновении инцидентов.

Срок службы оборудования также влияет на TCO. Большинство российских платформ поставляются с гарантией 5 лет, тогда как у импортных решений гарантийный срок редко превышает 3 года, особенно в условиях нестабильности поставок. Кроме того, наличие локализованных пользовательских интерфейсов у отечественных систем снижает затраты на обучение персонала и ускоряет процесс ввода оборудования в эксплуатацию.

Согласно проведённой оценке, на горизонте 7 лет совокупная стоимость владения решениями «Элтекс» и ZTE сопоставима. Однако преимущество ZTE проявляется на этапе первоначального развертывания за счёт более низкой закупочной стоимости, что делает его привлекательным для проектов с ограниченным стартовым бюджетом. В то же время при долгосрочном планировании следует учитывать риски, связанные с сервисной поддержкой, доступностью запасных частей и энергоэффективностью.

Санкционные ограничения и массовый уход западных поставщиков заставили пересмотреть проектирование оптических сетей. Сегодня недостаточно опираться лишь на классические физические модели — необходим более целостный подход, в котором технические расчёты дополняются экономическими соображениями и реалиями геополитической обстановки. Предложенная в статье методика как раз и отвечает этой задаче: она позволяет не только корректно учесть такие параметры, как затухание, дисперсия и уровень OSNR, но и выбрать оборудование, способное работать стабильно и предсказуемо именно в условиях российского рынка.

В современных реалиях «лучшее» – это не то, что обладает рекордными характеристиками на бумаге, а то, что реально доступно, поддерживается на месте и не подведёт в критический момент. Напротив, «худшее» – это кажущаяся высокопроизводительность, за которой скрывается хрупкость: отсутствие сервиса, запчастей и обновлений, что делает такие решения рискованными даже при выдающихся технических данных. Современные инженеры всё меньше ориентируется на достижение пиковых показателей и всё больше на обеспечение устойчивой и долгосрочной эксплуатации.

Литература

1. *Gadasin D. V., Shvedov A. V., Klygina O. G.* Organization of Interaction Between the Concept of Fog Computing and Segment Routing for the Provision of IoT Services in Smart Grid Networks // Wave Electronics and Its Application in Information and Telecommunication Systems. 2022. Vol. 5, No. 1, pp. 141-146. EDN: UQSHRH

2. *Гадасин Д. В., Шведов А. В.* Проблемы интеграции концепции "Интернет вещей" и облачных вычислений // Технологии информационного общества: Материалы XIII Международной отраслевой научно-технической конференции, Москва, 20-21 марта 2019 года. Том 2. М.: Издательский дом Медиа Паблишер, 2019. С. 22-23. EDN: MEQRFA

3. *Гадасин Д. В., Шведов А. В., Алексеева Е. А.* Информационная энтропия в стохастических сетях связи // Телекоммуникационные и вычислительные системы 2020: Труды международной научно-технической конференции, Москва, 14-17 декабря 2020 года / Московский технический университет связи и информатики. М.: Горячая линия – Телеком, 2020. С. 108-116. EDN: IOGLQH

4. *Gadasin D. V., Shvedov A. V., Kuzin I. A*. Reconstruction of a Three-Dimensional Scene from its Projections in Computer Vision Systems // 2021 Intelligent Technologies and Electronic Devices in Vehicle and Road Transport Complex, TIRVED 2021 – Conference Proceedings, Moscow, 11-12 ноября 2021 г. Moscow, 2021. DOI: 10.1109/TIRVED53476.2021.9639161 EDN: CKSNPA

5. *Gadasin D. V., Shvedov A. V., Kuzin I. A.* A model for representing the color and depth metric characteristics of objects in an image // 2021 Systems of Signal Synchronization, Generating and Processing in Telecommunications, SYNCHROINFO 2021 – Conference Proceedings, Svetlogorsk, Kaliningrad Region, 30 июня – 02 июля 2021 г. Svetlogorsk, Kaliningrad Region, 2021. P. 9488349. DOI: 10.1109/SYNCHROINFO51390.2021.9488349 EDN: YAYZVP

6. *Гадасин Д. В., Пак Е. В., Коровушкина В. М., Мелькова Е. К.* Предобработка текстовой информации на основе термов естественного языка // REDS: Телекоммуникационные устройства и системы. 2022. Т. 12, № 1. С. 4-11. EDN: PDGAVP

7. *Фокин В. Г.* Исследование развития функциональной гибкости оптических транспортных сетей OTN-OTH // Современные проблемы телекоммуникаций : материалы Всероссийской научно-технической конференции, Новосибирск, 22-25 апреля 2024 года. Новосибирск: Сибирский государственный университет телекоммуникаций и информатики, 2024. С. 31-37. DOI: 10.55648/SPT-2024-1-31 EDN: BFCDUU

8. МСЭ-Т Рекомендация G.709 (2022). Интерфейсы оптических транспортных сетей. Женева: МСЭ, 2022.

9. ГОСТ 28439-90. Аппаратура волоконно-оптических систем передачи по линиям электропередач цифровая. М.: Стандартинформ, 2005.

10. *Попова В. В., Булаев В. Д., Галицкий П. А*. Системный подход к построению комплексной защиты информации на объектах критической информационной инфраструктуры. Создание Единой централизованной федеральной телекоммуникационной сети // Безопасность личности, общества и государства: теоретико-правовые аспекты : Сборник научных статей XVII международной научной конференции обучающихся образовательных организаций высшего образования, проводимой в рамках IV Санкт-Петербургского международного молодежного научного форума "Северная Пальмира: территория возможностей". Санкт-Петербург, 30 мая 2024 г. Санкт-Петербург: Санкт-Петербургский университет МВД РФ, 2024. С. 1694-1703. EDN:AZKLFI

11. *Шевелев С. В.* Анализ требований к телекоммуникационным подсистемам, обеспечивающим бесперебойное функционирование систем оповещения населения // Технологии информационного общества: Сборник трудов XIV

Международной отраслевой научно-технической конференции, Москва, 18-19 марта 2020 г. М.: Издательский дом Медиа Паблишер, 2020. С. 310-312. EDN: AVHGLA

12. *Игнатьев Р. П.* Мультисервисные сети передачи данных: совокупная стоимость владения и проблема дистрибуции точного времени // Инженерные кадры – будущее инновационной экономики России. 2020. № 6. С. 71-74. EDN: VREDIB

13. *Shvedov A. V., Gadasin D. V., Pak E. V.* Application of the Backman Model for the Distribution of Traffic Flows in Networks with Segment Routing // 2022 Systems of Signals Generating and Processing in the Field of on Board Communications, SOSG 2022 – Conference Proceedings, Moscow, 15-17 марта 2022 г. Moscow, 2022. DOI: 10.1109/IEEECONF53456.2022.9744344 EDN: RBMTBQ

14. *Гадасин Д. В., Смальков Н. А., Кузин И. А*. Использование метода роя частиц для балансировки нагрузки в сетях Интернета вещей // Системы синхронизации, формирования и обработки сигналов. 2022. Т. 13, № 2. С. 17-23. EDN: LIUWNT

15. *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

16. *Постников И. Н*. Критерии надежности пассивных оптических сетей нового поколения // T-Comm: Телекоммуникации и транспорт. 2018. Т. 12, № 5. С. 41-46. DOI: 10.24411/2072-8735-2018-10085 EDN: XTLDTN

17. *Gadasin D. V., Shvedov A. V., Yudin A. A*. Clustering methods in large-scale systems // Synchroinfo Journal. 2020. Vol. 6, No. 5, pp. 21-24. DOI: 10.36724/2664-066x-2020-6-5-21-24 EDN: XHNSYV

18. *Gadasin D. V., Shvedov A. V., Koltsova A. V*. Cluster model for edge computing // 2020 International Conference on Engineering Management of Communication and Technology, EMCTECH 2020 : Proceedings, Vienna, 20-22 октября 2020 года. New York: Institute of Electrical and Electronics Engineers Inc., 2020. P. 9261538. DOI: 10.1109/EMCTECH49634.2020.9261538 EDN: FGDLSA

19. *Gadasin D. V., Koltsova A. V., Gadasin D. D*. Algorithm for Building a Cluster for Implementing the 'Memory as a Service' Service in the IoT Concept // 2021 Systems of Signals Generating and Processing in the Field of on Board Communications, Conference Proceedings, Moscow, 16-18 марта 2021 г. Moscow, 2021. P. 9416112. DOI: 10.1109/IEEECONF51389.2021.9416112 EDN: VRPCFG

20. *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 г. Симферополь: ИП Зуева, 2023. С. 187-189. EDN: LGONZK

21. *Gadasin D. V., Shvedov A. V., Vakurin I. S*. Determination of Semantic Proximity of Natural Language Terms for Subsequent Neural Network Training // 2022 Systems of Signals Generating and Processing in the Field of on Board Communications, SOSG 2022 – Conference Proceedings, Moscow, 15-17 марта 2022 г. Moscow, 2022. DOI: 10.1109/IEEECONF53456.2022.9744290 EDN: LASMDY

22. *Zolotukhin P. A., Melkova E. K., Gadasin D. V., Korovushkina V. M*. Using Intelligent Testing as a Tool to Improve the Quality of Transport Information Systems // 2022 Systems of Signals Generating and Processing in the Field of on Board Communications, SOSG 2022 – Conference Proceedings, Moscow, 15-17 марта 2022 г. Moscow, 2022. DOI: 10.1109/IEEECONF53456.2022.9744348 EDN: NOMJLX

23. *Шведов А. В., Гадасин Д. В., Коровушкина В. М., Мелькова Е. К.* Интеллектуальное тестирование как способ повышения качества информационной системы // REDS: Телекоммуникационные устройства и системы. 2022. Т. 12, № 2. С. 43-52. EDN: GOLZGE

24. *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

25. *Гадасин Д. В., Шведов А. В., Мелькова Е. К*. Структурирование данных исходя из центра масс // Актуальные проблемы и перспективы развития экономики: Труды XXI Международной научно-практической конференции, Симферополь-Гурзуф, 20-22 октября 2022 года. Симферополь: Крымский федеральный университет им. В.И. Вернадского, 2022. С. 266-268. EDN: RFCCST

ПРОЕКТИРОВАНИЕ И РЕАЛИЗАЦИЯ СЕТИ АВТОНОМНЫХ LORA-МЕТОК НА БАЗЕ ESP32 И SX1262

Королёв Сергей Александрович
Московский технический университет связи и информатики, студент, Москва, Россия
skorolev2004@mail.ru

Воскресенский Егор Филиппович
Московский технический университет связи и информатики, студент, Москва, Россия
egorvoskres@gmail.com

Пестряков Александр Валентинович
Московский технический университет связи и информатики, д.т.н., профессор, Москва, Россия
a.v.pestriakov@mtuci.ru

Аннотация
В статье рассматривается процесс проектирования и реализации аппаратно-программного комплекса для мониторинга миграции животных на основе технологии LoRa. Представлено обоснование выбора компонентов, описана архитектура встроенного программного обеспечения для радиометок и базовой станции, включая реализацию драйвера радиомодуля. Описан процесс проектирования радиометки, оптимизированной по габаритным показателям.

Ключевые слова
Система мониторинга животных, интернет вещей, телеметрия, микроконтроллер, ESP32, LoRa, базовая станция, радиометка, печатная плата, антенна.

Введение

Современные задачи отслеживания и изучения миграционных путей животных на больших территориях требуют применения глобальных систем сбора телеметрии в регионах, где полностью отсутствует наземные системы связи. Одной из наиболее популярных открытых систем глобального сбора и позиционирования данных является система Argos [1]. Спутники этой системы находятся на полярной орбите на высоте 850 км. Это требует достаточно большой мощности сигнала, излучаемого радиометкой, для обеспечения необходимой энергетики радиолинии. Ограниченный энергетический ресурс радиометок при требованиях малых габаритов не позволяет обеспечить длительное время их работы от одного комплекта батарей. Кроме того, они имеют высокую стоимость (до нескольких тысяч евро), так как до сих пор изготавливаются лишь небольшими партиями для решения конкретных задач мониторинга.

В этой области актуальной является разработка систем с дешёвыми малогабаритными радиометками, которые могли бы обеспечить сбор данных в зоне действия наземной сети с последующей их передачей на специализированные спутниковые системы типа Argos (рис. 1) [2]. В такой гибридной системе радиометки могут иметь существенно меньшие стоимость, массу, габариты и потребляемую мощность.

В данной работе описывается поиск оптимального, для решения вышеописанных задач, протокола интернета вещей (IoT), который будет подходить выдвинутым требованиям [3-9], а также на основании которого можно будет разработать собственную специализированную сеть, адаптировать логику работы под конкретные задачи и интегрировать систему с существующими спутниковыми каналами системы Argos.

Целью данной работы является проектирование и реализация опытного образца радиометки на базе выбранных микроконтроллера и трансивера. В статье подробно освещаются ключевые этапы разработки: от выбора компонентов и создания модульной архитектуры встроенного программного обеспечения (ПО) до проектирования шестислойной печатной платы и выбора подходящей антенны.

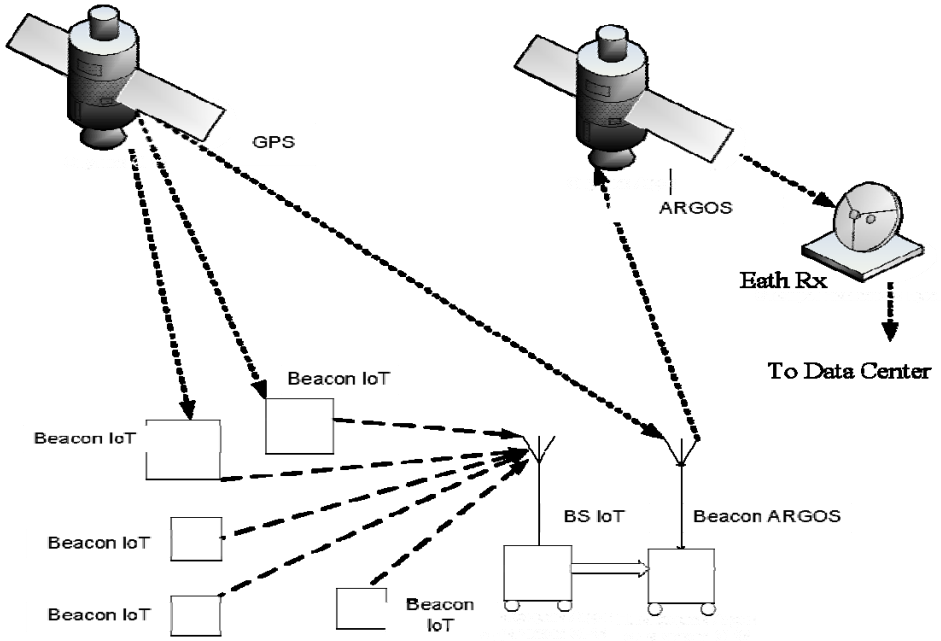


Рис. 1 Гибридная систему глобального мониторинга: Beacon Argos – радиометки системы Argos, Beacon IoT – радиометка сети интернета вещей, BS IoT – базовая станция сети IoT, Earth Rx – спутниковый приёмник системы Argos

Выбор протокола интернета вещей и компонентов для реализации радиометки

Основными требованиями при разработке радиометки были: максимальная дальность связи в различных климатических и территориальных условиях, минимальное энергопотребление и высокая помехоустойчивость при ограниченных массогабаритных показателях. Сравнительный анализ наиболее популярных систем IoT позволил сделать следующие выводы.

У протокола NB-IoT дальность (в пределах сотен метров), Sigfox и необходимо наличие сотовой инфраструктуры, Zigbee имеет низкую меет ограниченное покрытие. В то же время LoRa обеспечивает отличную чувствительность приемника (-148дБм), обусловленную особенностями используемой в данном протоколе модуляции. Применительно к решаемой задаче передачи данных, где приоритет отдается помехоустойчивости, нежели скорости передачи, использование LoRa является наилучшим решением.

В качестве трансивера был выбран радиомодуль на основе чипа SX1262 производства компании Semtech, так как на сегодняшний день он обладает наилучшими характеристиками, обеспечивающими более удобную эксплуатацию, проектирование, а также наибольшую дальность связи.

Для управления всей системой был выбран микроконтроллер ESP32, так как для разработки в сфере интернета вещей он имеет наибольший потенциал в сравнении с другими микроконтроллерами, такими как Blue Pill STM32 и Arduino Uno. При сравнительно низкой цене ESP32 значительно обходит своих конкурентов в значениях тактовой частоты, оперативной памяти, а также наличием Wi-Fi, Bluetooth, ЦАП и АЦП с большей разрядностью. При этом работать с ESP32 гораздо проще чем с STM32.

Разработка программного обеспечения

Описание структуры проекта

Для данной работы было создано два проекта: BaseStation_RX и Node_TX, они имеют следующую структуру: проект BaseStation_RX содержит в себе папки BaseStation, BCH, а проект Node_RX - папку BeaconNode, кроме того, данные проекты имеют общие библиотеки такие как LoraSX1262, LoraCalc и файл, описывающий логику работы, Datasheet.md. Каждая папка содержит в себе заголовочный файл, содержащий все переменные и прототипы функций, а также **.cpp** файл, полностью описывающий логику работы каждого метода. Данная структура позволяет грамотно вести и поддерживать проект, а также вносить в него изменения и добавлять новые методы, которые в дальнейшем могут понадобиться пользователям. Также в каждом проекте имеется свой **main.cpp** файл, в котором происходит создание всех объектов и запуск программы.

LoraSX1262

Файлы данной библиотеки являются базовым SPI-драйвером, реализующим основные функции, которые понадобятся для дальнейшей реализации работы устройства. Пример наиболее важных функций, реализованных в данной библиотеке:

1. LoraSX1262() – является конструктором, в котором описываются пины которыми устройство подключается к микроконтроллеру.
2. begin() – проверяет корректность подключения, выполняет базовую настройку модуля, выставляет частоту и параметры модуляции.
3. transmit() – функция, реализующая передачу данных с заданными параметрами.
4. lora_receive_async/blocking() – две версии функции приема, обычная и блокирующая, помимо приема, возвращают объем полученных данных.
5. setTxPower() – позволяет менять выходную мощность.

LoraCalc

Расчет ключевых параметров LoRa для анализа эффективности системы:

1. timeOnAir_ms() – расчитывает время передачи пакета (Time on Air сокращенно ToA) в миллисекундах в зависимости от таких параметров модуляции, как Spreading Factor, Bandwidth, Coding Rate, Low Data Optimizer. Позволяет конечному пользователю оценивать задержки передачи и планировать энергосбережение.
2. energy_mWh() – на основе времени передачи, тока потребления модуля в режиме TX и напряжения питания вычисляет примерное энергопотребление, затрачиваемое на одну передачу.

BeaconNode

Класс описывает всю логику работы конечного устройства (радиометки), он циклически собирает телеметрию или иную необходимую информацию и отправляет её на базовую станцию. Этот класс содержит в себе следующие методы:

1. BeaconNode() – конструктор класса, который принимает в себя уникальные ID ноды, указатель на объект **radio**, а также два объекта для работы с UART протоколом: один для прошивки и отладки, второй для реального ввода-вывода данных.
2. start() – общая инициализация.
3. tick() – главный цикл, вызываемый в loop() файла main.cpp, отвечающий за отправку данных по заданным правилам.
4. preapareNodeData() – осуществляет сбор и подготовку данных для отправки, в зависимости от значения макроса DEBUG_GPS может работать как с тестовыми данными, так и с реальным устройство GPS (ГЛОНАСС) по средствам библиотеки TinyGPSPlus
5. CRC8() – вычисляет контрольную сумму пакета по алгоритму CRC8 для проверки целостности данных на этапе их отправки от метки до базовой станции.
6. ChanelIsBusy и csmaTransmit() – методы, реализующий алгоритм CSMA, который выполняет функцию кратковременной «прослушки» эфира перед отправкой, и введения случайной задержки на отправку данных в случае, если канал передачи занят. Таким образом данный алгоритм позволяет избежать коллизии при передаче данных без введения строгих ограничений на время отправки и различных шлюзов, ожидающих подтверждения освобождения канала. Данный алгоритм позволяет значительно сократить время работы в сети и, следовательно, снизить энергопотребление.
7. distanceKm() – по заранее введенным координатам базовой станции и своих координат, полученных с датчика GPS (ГЛОНАСС), расчитывает расстояние до базовой станции.
8. calcTxPower() – используя заранее известные значения зоны покрытия базовой станции рассчитывает минимальную необходимую мощность передачи (для экономии энергии).
9. applyTxPower() – применяет вычисленную методом calcTxPower() мощность к радиомодулю путем отправки соответствующих SPI-команд.
10. sendData() – формирование и отправка пакета, отладочный вывод в терминал.
11. estimateTineOnAir() – рассчитывает случайную задержку при передачи в зависимости от выбранного пресета.

BaseStation

Данный класс реализует логику работы базовой станции. Устройство принимает пакеты от нодов, а также занимается формированием и отправкой итогового спутникового пакета (в нашем случае вывод в терминал по UART), данный класс содержит следующие методы:

1. BaseStation() – конструктор, принимающий в себя объект радио и UART.
2. start() – проводит инициализацию.
3. tick() – главный цикл постоянно проверяет входящие пакеты и отправляет их по таймеру через определенные промежутки времени, формирует ARGOS-пакет.
4. receiveNodePacket() – принимает пакеты от нод с помощью метода lora_receive_async(). Проверяет корректность пакета с помощью CRC. Обновляет внутренний список nodes (структура NodePacket), содержащий последние данный от каждой ноды. Вычисляет расстояние до каждой ноды и по нему вычисляет энергию, затраченную на передачу.
5. aggregateToArgos() – данные из списка нод переделывает в 18-байтовый пакет. Вычисляет среднии координаты по нодам, проверяет, что все ноды находятся в пределах заданного радиуса зоны обслуживания (ALLOWED_RADIUS_METRES). Формирует два типа пакетов: нормальный (если все метки в пределах заданного радиуса отправляет средние координаты) или аномальный (координаты нод, вышедших за радиус).
6. sendArgosFrame() – отправка финального пакета. На данном этапе данные выводятся в Serial. Здесь же проводится тестовая демонстрация БЧХ.
7. calcTxPower() – вычисляет предполагаемую мощность ноды по полученным координатам.
8. txCurrentFromDbm() – определяет потребляемый ток передатчика в зависимости от установленной мощности.
9. distanceMeters() – вычисление расстояния до ноды, для расчетов и мониторинга энергии передачи.

BCH

Реализация БЧХ кодирования:

1. encode_a_b()/decode_a_b() – функция, которая кодируют и декодируют информацию избыточным кодом **b** байт в **a**, нужным для дальнейшей реализации и выбора конкретной реализации БЧХ кода, например 61,21 или 26,12.
2. injectBitError() – вспомогательная функция тестирования – инжектирует ошибку в заданный бит.

main.cpp

Создают объекты нодов и базовой станции. Логика работы main файла всегда одинаковая, она содержит в себе две функции setup() и loop(), первая проводит всю инициализацию и настройку устройств, а вторая является бесконечным циклом, который полностью осуществляет работу устройства. В данных функциях вызываются методы из описанных выше библиотек.

Datasheet.md

Содержит общую логику работы программы нужную для разработчика, благодаря ему можно узнать распиновку, краткое описание всех методов, форматы передаваемых пакетов, описание ключевых переменных и параметров (интервалы отправки, пресеты и прочее).

Общая логика работы системы "Базовая станция / Ноды"

Работа системы представляет собой циклический асинхронный процесс.

1. Цикл работы Ноды:

- Нода "просыпается" по внутреннему таймеру (например, каждые 10 секунд).
- Собирает данные: считывает GPS-координаты и уровень заряда батареи.
- Формирует пакет фиксированной длины (12 байт), включающий ID, координаты, заряд батареи и CRC.
- Рассчитываем расстояние до базовой станции и на основании этих данных выбираем значение мощности передатчика от 10 до 22 дБм. Мощность вычисляется по формуле $Pwr = P_{min} + \frac{D(P_{max} - P_{min} + 1)}{R}$,

где:

  - Pwr – итоговая мощность;
  - P_{max} – максимально возможная мощность передачи;
  - P_{min} – минимально возможная мощность передачи;
  - D – вычисленное расстояние до базовой станции;
  - R – радиус зоны покрытия в километрах;
- Перед отправкой выполняет CSMA-проверку: «прослушивает» эфир 25 мс. Если эфир свободен, немедленно передает пакет. Если занят, ждет случайное время, зависящее от параметра ToA для данных настроек, и проверяет снова.
- После отправки нода возвращается в режим ожидания следующего цикла.

2. Цикл работы Базовой Станции:

- Базовая станция постоянно находится в режиме приема setModeReceive().

- В фоновом режиме она принимает все пакеты, которые приходят от нод.
- Для каждого принятого пакета:
  - Проверяется CRC. При несовпадении пакет отбрасывается.
  - Пакет разбирается, и его данные обновляются во внутреннем списке активных нод.
  - На основе полученных координат ноды вычисляется затраченная мощность передатчика и как следствие энергозатраты радиометки.
- Параллельно, по другому таймеру (например, каждые 30 секунд), базовая станция выполняет агрегацию:
  - Она берет актуальные данные из своего списка нод.
  - Вычисляет среднюю точку и проверяет, все ли ноды в радиусе.
  - Формирует 18-байтовый ARGOS-совместимый фрейм.
  - Фрейм проходит через процедуру "BCH"-кодирования.
  - Результат (закодированный фрейм) выводится в Serial-порт, имитируя передачу в спутниковый модем.
  - Список нод очищается для сбора новых данных.

Синхронизация

Система асинхронна. Ноды работают по собственному расписанию и не ждут подтверждения от базовой станции. Базовая станция пассивно аккумулирует данные от всех нод в зоне покрытия, что делает систему устойчивой к временным потерям связи с отдельными метками.

Преимущества реализованной логики:

- Масштабируемость – добавление новых нод не требует изменения кода базовой станции.
- Устойчивость к коллизиям – механизм CSMA снижает вероятность одновременной передачи нескольких нод.
- Энергоэффективность – ноды активны только во время сбора данных и короткой сессии передачи.
- Готовность к интеграции формирование ARGOS-фрейма делает систему готовой к подключению к спутниковым сетям передачи данных.

Пример работы всей системы.

Несколько циклов работы всей системы, для примера берем вывод в терминал от разных нод, расположенных на разном расстоянии от базовой станции.

Nodes:

BeaconNode_ID2 (находится на расстоянии ≈ 0.3 км):
Beacon started (longrange preset)
Adaptive TX power ON
Distance to BS: 0.30 km
Setting TX power: 11 dBm
Sent: ID=2 lat=5580070 lon=3761760 bat=90 tx=11 dBm CRC=8C
BeaconNode_ID3 (находится на расстоянии ≈ 2.1 км):
Beacon started (longrange preset)
Adaptive TX power ON
Distance to BS: 2.10 km
Setting TX power: 15 dBm
Sent: ID=3 lat=5580070 lon=3761760 bat=90 tx=15 dBm CRC=8C
BeaconNode_ID4 (находится на расстоянии ≈ 4.8 км):
Beacon started (longrange preset)
Adaptive TX power ON
Distance to BS: 4.80 km
Setting TX power: 22 dBm
Sent: ID=2 lat=5580070 lon=3761760 bat=90 tx=22 dBm CRC=8C

BaseStation:

BaseStation starting…
Radio initialized (longrange)
NodeRecv id=2 lat=5580070 lon=3761760 bat=90
Distance: 0.30 km, assumed TX power: 11 dBm
SF12 ToA=24730.98 ms, I_tx=80.0 mA, energy=1.06838 mWh
NodeRecv id=3 lat=5580070 lon=3761760 bat=90

Distance: 2.10 km, assumed TX power: 15 dBm
SF12 ToA=24730.98 ms, I_tx=95.0 mA, energy=1.26845 mWh
NodeRecv id=4 lat=5580070 lon=3761760 bat=90
Distance: 4.80 km, assumed TX power: 22 dBm
SF12 ToA=24730.98 ms, I_tx=185.0 mA, energy=2.47086 mWh
All nodes within radius -> normal average frame
=== ARGOS 144-bit frame (encoded) ===
22 37 55 0B 23 E4 39 00 03 A5 7C 12 34 56 78 9A BC DE F0
Decoding: A_ok=1 B_ok=1
--- ARGOS frame ready —
Frame bytes: 22 37 55 0B 23 E4 39 00 03 A5 7C 12 34 56 78 9A BC DE F0

Разработка аппаратной части

Устройство должно быть сопоставимо с размерами обычных ушных бирок для крупных животных (коров, лошадей, оленей и т.п.). Ввиду наличия готовых корпусов ушных бирок под размер платы 40мм × 50 мм и типовых размеров аккумуляторов (33мм × 50 мм), габариты печатной платы были выбраны 40мм × 50 мм.

Разработка печатной платы

Для проекта была выбрана шестислойная плата в виду доступности и возможности реализовать отдельные слои для экранирования. На рисунках 2-7 показаны слои печатной платы.

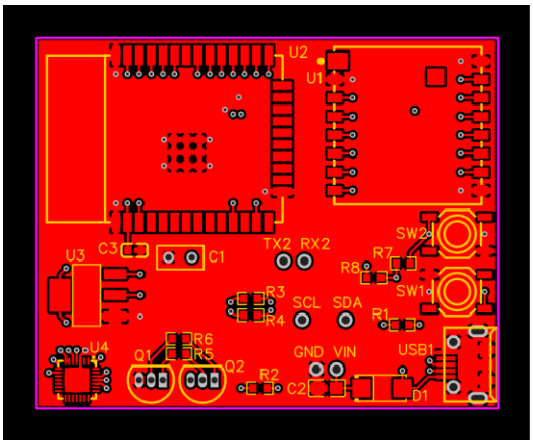


Рис. 2. Верхний слой

На верхнем слое для уменьшения помех расположено минимальное количество дорожек. Также стоит отметить, что под антенным блоком ESP32 на всех слоях отсутствуют дорожки. основная медная область – земля (GND).

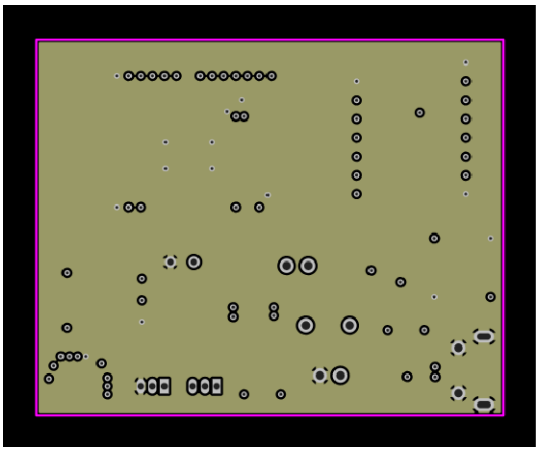


Рис. 3. Первый внутренний слой

Первый внутренний слой – это сплошной слой земли (GND). Это необходимо для экранирования верхнего слоя, что повышает помехоустойчивость.

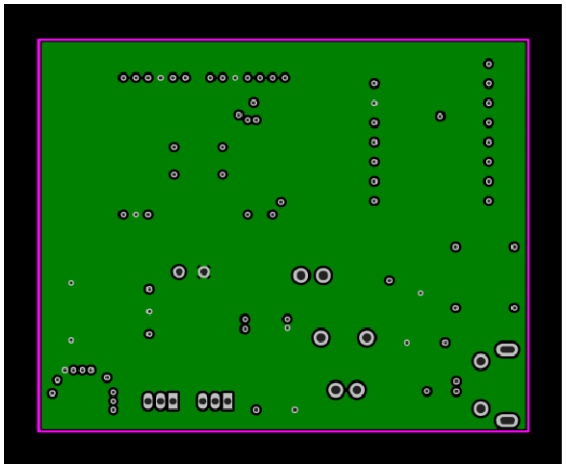


Рис. 4. Второй внутренний слой

Второй внутренний слой – это сплошной слой питания 3.3 вольта (V3.3). Этот слой необходим как для экранирования, так и для подведения питания к элементам на плате.

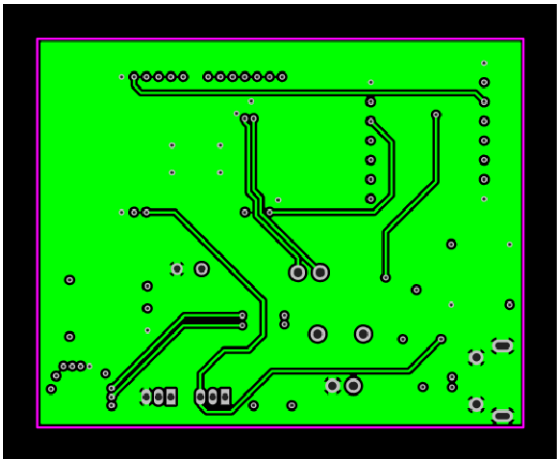


Рис. 5. Третий внутренний слой

Третий внутренний слой содержит сигнальные дорожки. Основная медная область – земля (GND).

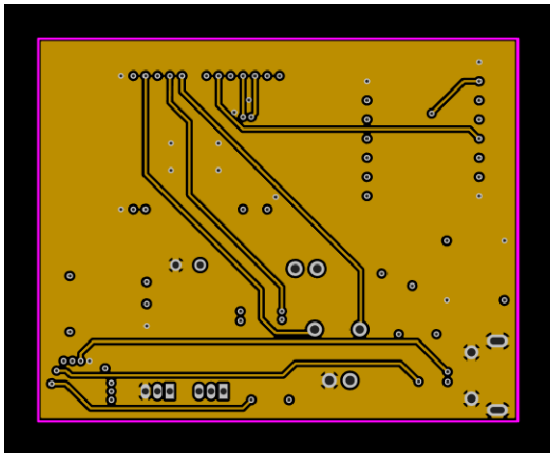


Рис. 6. Четвертый внутренний слой

Четвертый внутренний слой содержит сигнальные дорожки. Основная медная область – земля (GND).

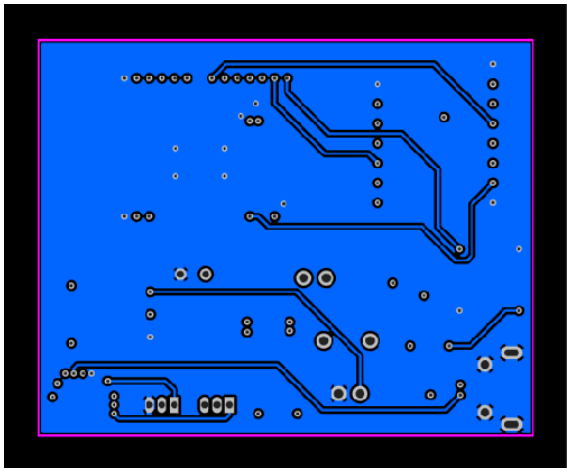


Рис. 7. Нижний слой

Нижний слой содержит сигнальные дорожки. Основная медная область – земля (GND).

Таблица 1

Размеры

Ширина платы	50 мм
Длина платы	40 мм
Толщина платы	1.6 мм
Толщина собранной платы в самом широком месте	6.1 мм

Трехмерная модель

На рисунках 8-9 показано расположение деталей на плате (сверху и снизу).

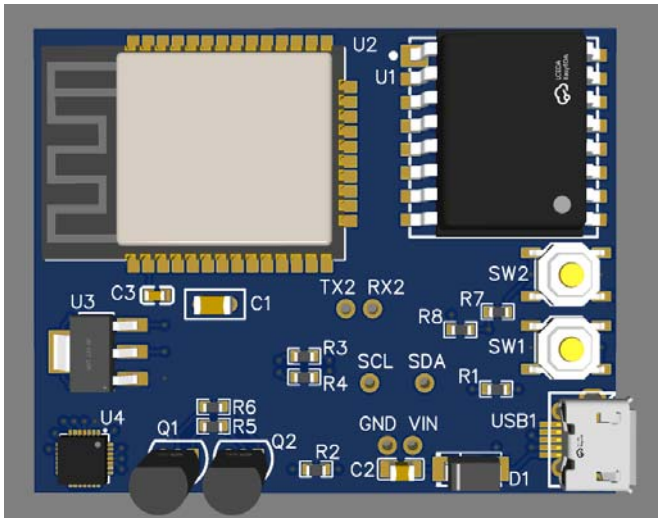


Рис. 8. Плата, вид сверху

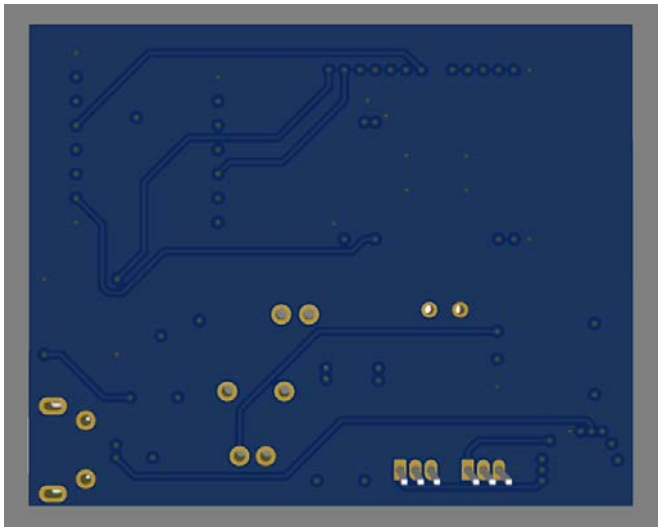


Рис. 9. Плата, вид снизу

Подключение платы, и антенны. Управление платой

- Питание на плату подаётся или через встроенный Micro-USB-B, или через контакты GND и VIN.
- Прошивка устройства производится через встроенный Micro-USB-B. При отладке также могут быть использованы кнопки SW1 (EN) и SW2 (BOOT).
- На плате выведены контакты TX2/RX2 для подключения датчиков по UART (например температуры).
- Также на плате есть контакты SDA/SCL для подключения устройств по протоколу I2C.
- Антенна подключается к разъёму IPEX на чипе RA-01SH-P (U1). Разъём уже согласован.

Фото чипа RA-01SH-P и фото разъёма IPEX:

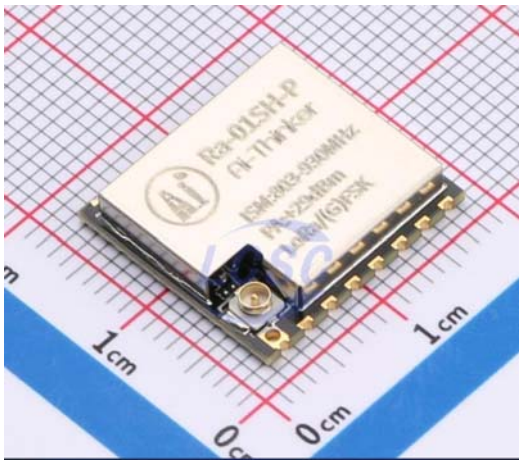


Рис. 10. Фото чипа RA-01SH-P с разъёмом IPEX

Рис. 11. Разъём IPEX

Антенна

Для реализации была выбран антенна в виде монополя ABRACON AEACAC054010-S915 [7], которая подключается через фидер (BAT WIRELESS BWIPX1-SMA-1.13L200) с выводами IPEX-SMA. Она рассчитана на частотный диапазон (803-930), и её размеры идеально подходят для того, чтобы поместить её в корпус метки.

Размеры выбранной антенны идеально подходят под уже готовые корпуса меток, внутренние размеры которых: 40мм x 55мм x 30мм. При необходимости пластиковую защиту монополя можно уменьшить механической обработкой или вовсе удалить.

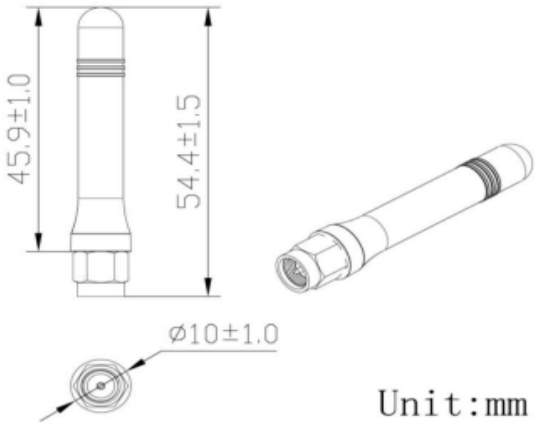


Рис. 12. Габаритные размеры антенны в штатном корпусе

Рис. 13. Фото антенны

Усиление: 2.2 дБи - оптимальное решение по усилению антенны, которое обеспечивает хорошие показатели по всенаправленности, что увеличивает дальность связи в горизонтальной плоскости.

Коэффициент стоячей волны для частоты работы радиометок КСВ равен 1.39 (на основе данных производителя), что является достаточно высоким показателем, обеспечивающим хорошее согласование и эффективную передачу энергии.

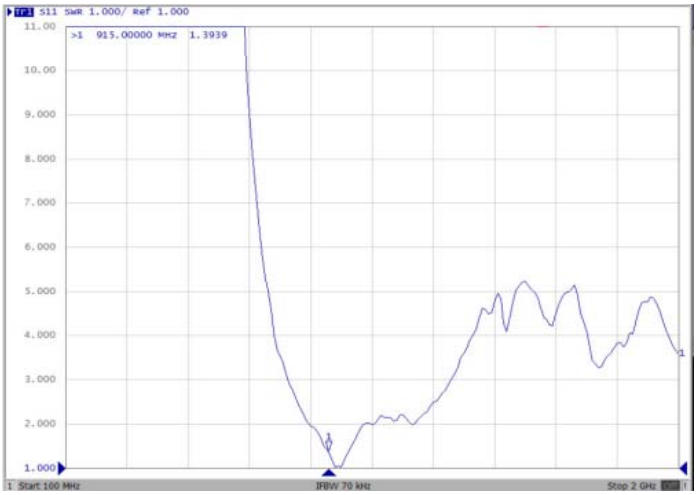


Рис. 14. График коэффициента стоячей волны

Диаграмма направленности в вертикальной плоскости: тороидальная (зенитная). Это увеличивает дальность связи с базовой станцией.

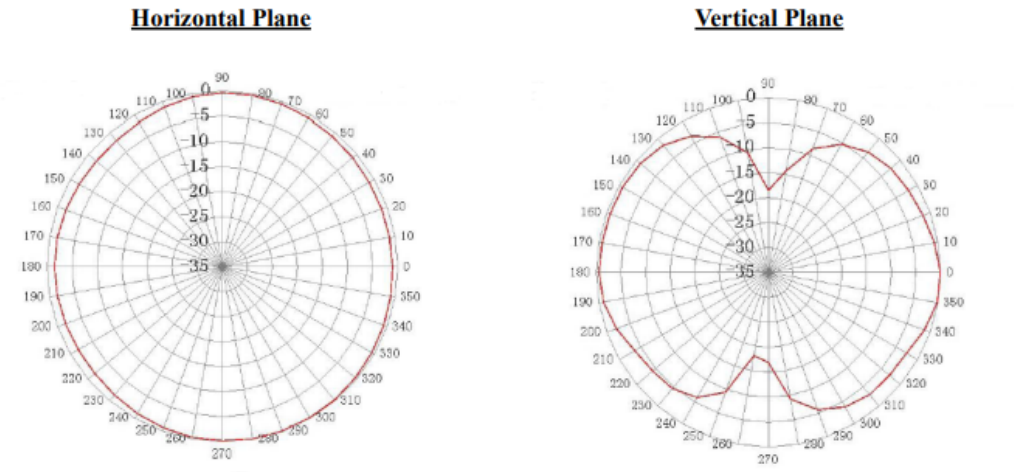


Рис. 15. Диаграммы направленности в горизонтальной и вертикальной плоскостях

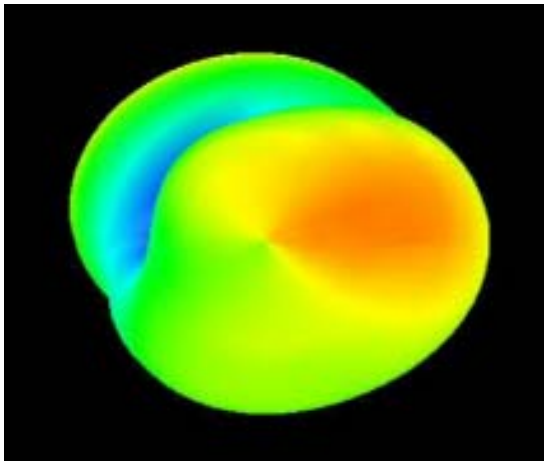


Рис. 16. Трехмерная Диаграмма направленности

Для частоты 915 МГц длина антенны должна составлять λ/4 ≈ 82мм, длина нашей антенны (без корпуса) составляет 41 мм, таким образом коэффициент укорочения равен: $K = \frac{41}{82} = 0.5$. Этим объясняется широкая полоса антенны в зоне более высоких частот, которую можно увидеть на графике КСВ. КПД антенны около 66%. В связи с габаритными ограничениями, данные параметры можно считать удовлетворительными.

Антенна подключается через фидер-переходник (IPEX <=> SMA) BAT WIRELESS BWIPX1-SMA-1.13L200, который имеет затухание около 2 dB/m на заданных частотах, что является хорошим показателем. Фидер через порт IPEX подключается к печатной плате, а через порт SMA к антенне. Это также увеличивает гибкость устройства, так как позволяет подключить любую антенну с входом SMA.

Рис. 17. BAT WIRELESS BWIPX1-SMA-1.13L200

Заключение

Инженерно-экономическое обоснование подтвердило оптимальность выбора связки микроконтроллера ESP32 и трансивера SX1262, обеспечивающей хороший баланс энергопотребления, производительности и стоимости разработки.

Ключевым результатом программной части стала реализация модульной архитектуры ПО. Для радиометок разработан энергосберегающий цикл сбора данных и адаптивный расчет мощности передачи. ПО базовой станции обеспечивает асинхронный прием, работу с большим количеством меток и формирует итоговый пакет, необходимый для передачи радиометкой системы Argos.

Аппаратная реализация базируется на шестислойной печатной плате, оптимизированной по массогабаритным показателям для размещения в корпусе стандартной ушной бирки. Многослойная структура обеспечивает высокую помехозащищенность и целостность сигналов, что критически важно для радиотракта.

Благодаря модульности и масштабируемости, система может быть адаптирована для широкого круга задач глобального мониторинга и интернета вещей, таких как мониторинг миграции животных, исследование окружающей среды или логистики.

Литература

1. *Козлов А.В., Пестряков А.В.* Развитие спутниковой системы позиционирования и сбора данных ARGOS // T-Comm: Телекоммуникации и транспорт. 2012. Т. 6. № 2. С. 36-39.

2. *Пестряков А.В*. Разработка и испытание комбинированной системы глобального мониторинга подвижных объектов // Инфокоммуникационные и радиоэлектронные технологии. 2022. Т. 5. № 2. С. 185-195.

3. *Pestryakov A.V., Dinges S.I.* Development trends of IoT equipment // В сборнике: Systems of Signal Synchronization, Generating and Processing in Telecommunications, SYNCHROINFO 2021 – Conference Proceedings. 2021. С. 9488391.

4. *Sornin N., Luis M., Eirich T., Kramp T., Hersent O.* LoRaWAN™ Specification. 2015. С. 9-34.

5. Решение ГКРЧ при Мининформсвязи России от 07.05.2007 N 07-20-03-001 "О выделении полос радиочастот устройствам малого радиуса действия". С. 37-42.

6. *Васильев А.Н.* Программирование на C++ в примерах и задачах. 2017. С. 158-191.

7. LPWA/ISM External Antenna AEACAC054010-S915, LCSC 2019 [электронный ресурс] URL: https://www.lcsc.com/datasheet/C6123576.pdf.

8. *Пестряков А. В., Дымкова С. С.* Синхронизация. Итоги 50-ти лет развития в СССР и России // T-Comm: Телекоммуникации и транспорт. 2023. Т. 17, № 11. С. 27-34. DOI 10.36724/2072-8735-2023-17-11-27-34. EDN SALXGY.

9. *Микенин А. Э., Прокурат Г. А., Пестряков А. В*. Применение векторного анализатора спектра signalhound SM200C при разработке лабораторного практикума по дисциплине "тестирование радиооборудования систем связи" // Методические вопросы преподавания инфокоммуникаций в высшей школе. 2023. Т. 12, № 2. С. 43-49. EDN XBCSRF.

ИССЛЕДОВАНИЕ ОСОБЕННОСТЕЙ ВИДЕОКОДЕКОВ, ПРЕДНАЗНАЧЕННЫХ ДЛЯ ПЕРЕДАЧИ ПО НИЗКОСКОРОСТНЫМ РАДИОКАНАЛАМ

Косичкина Татьяна Павловна
Московский технический университет связи и информатики,
заведующий кафедрой СиСРТ, кандидат технических наук, доцент, Москва, Россия
t.p.kosichkina@mtuci.ru

Винокуров Алексей Михайлович
Московский технический университет связи и информатики, Москва, Россия
alexvinokurovv@gmail.com

Аннотация
Статья посвящена исследованию особенностей видеокодеков, адаптированных для передачи видео по низкоскоростным радиоканалам. Проводится анализ ключевых параметров современных видеокодеков (H.264, H.265, AV1). Приведены результаты сравнительных тестов, демонстрирующих влияние различных настроек на качество видео и нагрузку на сеть, а также результат их совместной работы. Результаты исследования могут быть использованы при проектировании систем видеопередачи в условиях ограниченной пропускной способности каналов.

Ключевые слова
Видеокодеки, битрейт, сжатие видео, оптимизация видеопотока, H.264/H.265/AV1.

Введение

Видеоданные стали ключевым элементом информационного обмена в системах видеонаблюдения, безопасности и дистанционного управления, в том числе для БПЛА и других подвижных объектов в реальном времени. При передаче по низкоскоростным радиоканалам с пропускной способностью до нескольких мегабит в секунду возникает необходимость в сильном сжатии видеопотока при сохранении приемлемого качества.

Основной задачей работы является анализ характеристик современных видеокодеков H.264, H.265 и AV1 и разработка рекомендаций по их настройке для передачи видео по низкоскоростным и нестабильным радиоканалам в реальном времени. Особое внимание уделяется выбору параметров кодирования, обеспечивающих баланс между эффективностью сжатия, вычислительной сложностью и задержкой видеопередачи.

Основные понятия и термины

Битрейт (bit rate) – скорость передачи или обработки видеоданных, измеряемая в битах в секунду; рост битрейта повышает качество изображения и требования к пропускной способности канала. При слишком низком битрейте возрастает уровень артефактов и шумов, что затрудняет визуальный анализ сцены.

Видеокодек представляет собой программное или аппаратное средство для сжатия и восстановления видеопотока в соответствии с определённым стандартом кодирования. Как правило, используется сжатие с потерями (lossy compression), при котором часть мало заметной зрительно информации удаляется для уменьшения объёма данных.

Пропускная способность. Типичные значения для радиоканалов варьируются от нескольких килобит в секунду (кбит/с) для специализированных мобильных сетей до нескольких сотен кбит/с для 3G/4G сетей и спутниковых каналов. В сравнении с проводными сетями, пропускная способность радиоканалов значительно ниже, что требует использования кодеков с максимальной степенью сжатия.

Требования для использования кодеков

H.264 остаётся самым распространённым видеокодеком благодаря невысоким требованиям к вычислительным ресурсам и широкой аппаратной поддержке, включая устаревшие устройства [1].

H.265 более требователен к техническим характеристикам из-за более сложных алгоритмов сжатия, но его можно увидеть в современных устройствах, хоть и реже, чем H.264 [2].

AV1 один из самых эффективных и одновременно требовательных к вычислительным ресурсам кодеков [3], однако его аппаратная поддержка до сих пор ограничена отдельными современными SoC и специализированными решениями для сетевого видео [4] (например решения от MediaTek [5] или же Axis [6]).

Использование кодеков на основе ИИ в настоящее время, как правило, неприемлемо для задач реального времени из-за высокой вычислительной сложности и низкой доступности специализированных ускорителей.

Настройка и тестирование кодеков

Битрейт – базовый регулируемый параметр любого кодека. Если задать слишком низкое его значение, то качество изображения может сильно ухудшиться, возникнут серьезные артефакты, шумы. Существуют различные рекомендации по выбору среднего значения битрейта в зависимости от сценария (рис. 1).

H.265 Recommended Bit Rate (Approximate Value)(Kbps)

Resolution \ Frame Rate	30 fps	25 fps	20 fps	15 fps	12.5 fps	10 fps	1 fps
12MP(4000×3000)	10240	10240	7680	5120	5120	3840	3840
12MP(4000×3072)	10240	10240	7680	5120	5120	3840	3840
9MP(3072×3072)	8192	8192	6144	4096	4096	3072	3072
9MP(4096×2160)	7680	7680	5760	3840	3840	2880	2880
3840×2160	8192	8192	6144	4096	4096	3072	3072
6MP(3072×2048)	5120	5120	3840	2560	2560	1920	1920
2560×2560	5120	5120	3840	2560	2560	1920	1920
3072×1728	4096	4096	3072	2048	2048	1536	1536
2560×2048	4096	4096	3072	2048	2048	1536	1536
2592×1944	4608	4608	3456	2304	2304	1728	1728
2560×1920	4608	4608	3456	2304	2304	1728	1728
2688×1520	4096	4096	3072	2048	2048	1536	1536
4MP(2560×1440)	4096	4096	3072	2048	2048	1536	1536
QXGA(2048×1536)	3072	3072	2304	1536	1536	1152	1152
1080P(1920×1080)	2048	2048	1536	1024	1024	768	768
1280×960	1024	1024	768	512	512	384	384
720P(1280×720)	1024	1024	768	512	512	384	384
4CIF(704×576)	704	704	512	384	384	256	256
640×360	576	576	384	320	320	192	192
352×288	320	320	192	192	192	128	128

Note 1: This sheet is useful for users who has high reqirement for bit rate settings. If the real environment is more complex, you can increase the bite rate 20%~30% higher than recommend.
Note 2: The above value is suitable for all series IPC and PTZ with new platform.

Рис. 1. Рекомендации по выбору битрейта от компании Hikvision для кодека H.265

При кодировании видеофайла выбор режима управления битрейтом может напрямую повлиять на итоговое качество, эффективность сжатия и стабильность передачи данных. Наиболее распространённые подходы – CBR (Constant Bitrate, постоянный битрейт) и VBR (Variable Bitrate, переменный битрейт). Наряду с ними, в современных программных реализациях кодеков широкое применение нашли такие методы, как CRF (Constant Rate Factor) и его модификация с ограничением пропускной способности – Capped CRF. Рассмотрим каждый подход подробнее:

В режиме CBR битрейт поддерживается примерно постоянным по всему потоку, что упрощает планирование нагрузки на канал, но при сложных сценах может приводить к заметному падению качества.

VBR динамически настраивает битрейт в зависимости от сложности сцены, позволяет улучшить общее качество при той же средней скорости передачи, что оптимизирует передачу и потенциально улучшает общее качество.

Третий метод, CRF, задает целевое качество (значение от 0 до 51, где 0 – наилучшее качество, а 51 – максимальное сжатие), подгоняя под это значение битрейт, чтобы сохранить заданный уровень детализации (рис. 2). Он также, как и VBR позволяет динамически снижать битрейт для статичных сцен, а для динамичных увеличивать [7].

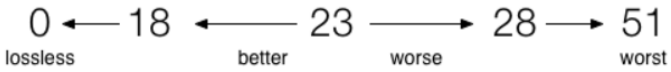
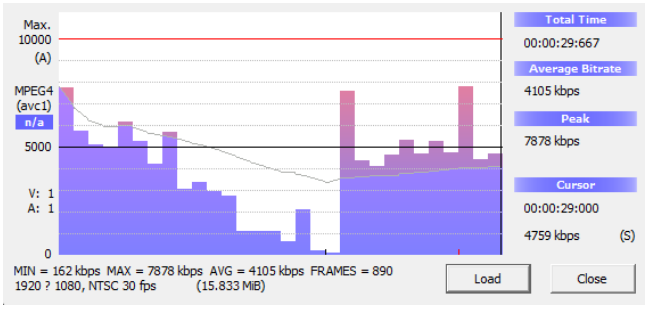


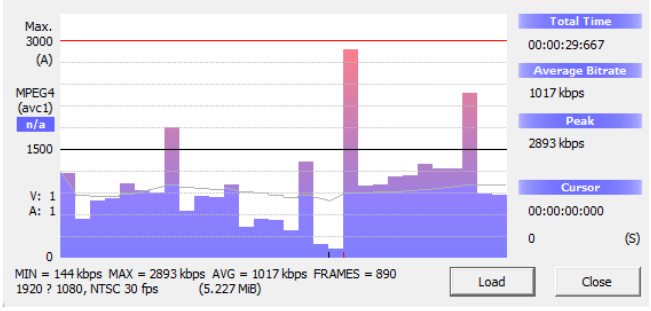
Рис. 2. понятие выбора целевого качества для CRF для H.264/H.265

Для радиоканалов с жесткими ограничениями CRF можно комбинировать с ограничением максимального битрейта (Capped CRF), что позволит предотвратить перегрузку канала в пиковых сценах, сохраняя преимущества адаптивного кодирования. На рисунке 3 изображено сравнение работы режимов управления битрейтов.



а) оригинальное видео

б) CBR (maxrate 2000 кбит/с)



в) VBR (maxrate 3000 кбит/с)

г) CRF (crf 34, maxrate 3000 кбит/с)

Рис. 3. Сравнение CBR, VBR и CRF

Вместе с задачей максимального битрейта необходимо настраивать параметр bufsize (размер видеобуфера, Video Buffering Verifier). Правильная настройка bufsize критична для реального времени, особенно на нестабильных каналах. Рекомендуется выбирать данное значение либо равное, либо в два раза больше, чем maxrate, либо задавать его в соответствии с рекомендациями по настройке VBV в документации FFmpeg [8]. Компромисс между скоростью кодирования и эффективностью сжатия регулируется с помощью опции пресетов. H.264 и H.265 разделяют одинаковые пресеты, в то время как для AV1 используется другая команда, а также значение изменяется от 0 до 6 (значения 7-10 доступны только при активации режима кодирования в реальном времени). Для реального времени необходимо использовать быстрые пресеты (preset ≤ 3).

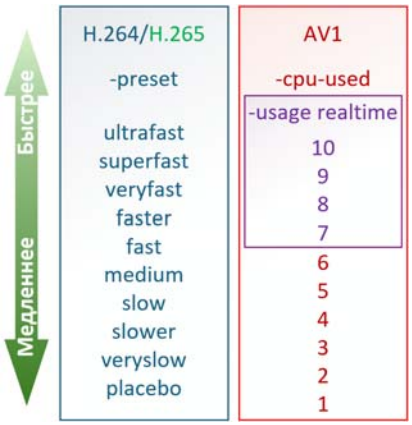
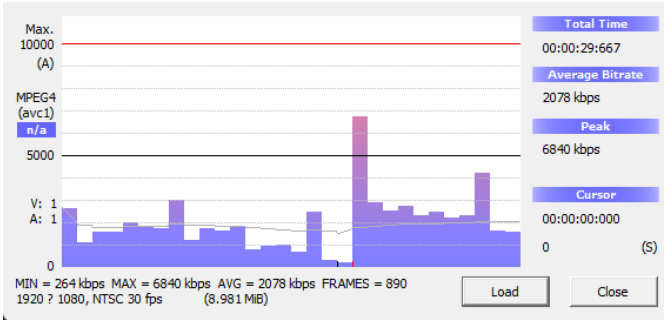


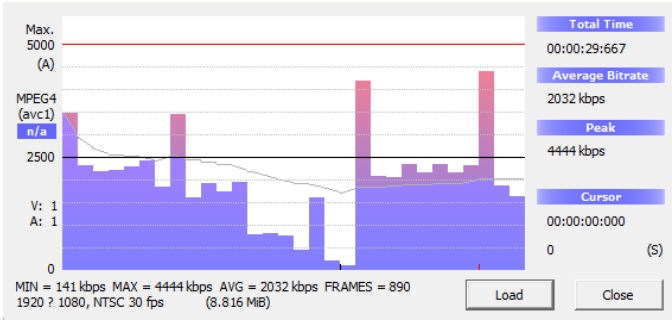
Рис. 4. Пресеты скорости кодирования для H.264, H.265 и AV1

Отдельно для H.264 и для H.265, в дополнение к опции пресетов, можно упомянуть возможность оптимизации кодирования (tune) под конкретные цели. Есть настройки под реальную запись, анимации, статичное изображение и оптимизация для быстрого декодирования.

Кодирование в два прохода улучшает качество при фиксированном размере файла за счёт предварительного сбора статистики по всему видеоролика (рис. 5). Однако для задач реального времени этот подход неприемлем, так как требует существенной буферизации, увеличивает задержку и нагрузку на вычислительные ресурсы.



а) один проход



б) два прохода

Рис. 5. Результаты кодирования с одним проходом и с двумя проходами

Group of Pictures (GoP) – логическая последовательность кадров между двумя ключевыми I-кадрами, определяет структуру зависимостей при межкадровом сжатии. GoP характеризуется двумя ключевыми параметрами: длиной (количеством кадров между I-кадрами) и структурой (порядком следования P- и B-кадров) [9]. Чаще всего изменяют именно длину данной последовательности (рис. 6).

Кодек	Макс. GOP
H.264	250
H.265	1024
AV1	∞ (гибкое разделение кадров)

Рис. 6. Максимальные значения GoP для каждого из кодеков

Пример структуры: I-B-B-P-B-B-P-B-B-I.

Кадры:

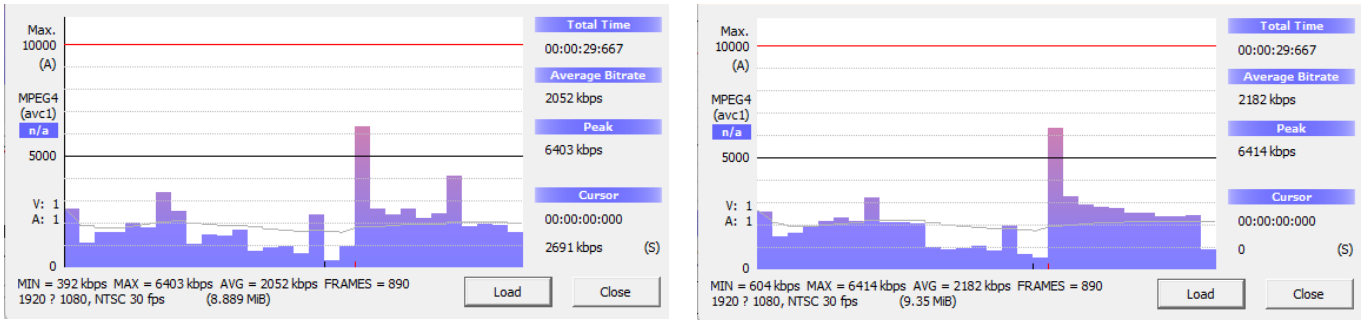
– I-Frame – ключевой (опорный) кадр, использующий только межкадровое предсказание, используется для предсказания P и B кадров.

– P-Frame – кадр, предсказанный на основе предыдущего кадра.

– B-Frame – двунаправленный кадр, который может быть предсказан на основе предыдущего кадра, на основе будущего кадра, предсказан без межкадрового предсказания, а также быть полностью пропущен.

Требует больших вычислительных ресурсов, но его можно отдельно настраивать, для H.264/H.265 от 0 до 16, для AV1 от 0 до ∞.

Размер структуры GoP не оказывает непосредственного влияния на сквозную задержку. Данный параметр влияет исключительно на время ожидания клиента до момента синхронизации с потоком. Для минимизации задержки, как правило, следует исключить использование B-Frame, что позволит декодеру инициировать вывод восстановленных кадров без ожидания, тем самым устраняя задержку, вносимую процессом переупорядочивания кадров в декодере.



а) GoP = 200 б) GoP = 30

Рис. 7. Сравнение работы с высоким значением GoP и низким

Проведем небольшое тестирование с применением всех вышеописанных настроек и конфигураций. В таблице 1 представлены параметры кодирования.

Таблица 1

Параметры кодирования видеофрагмента пролета камеры над горной местностью

Видеофрагмент пролета камеры над горной местностью					
Разрешение видео	Частота кадров	Исходный битрейт	Длительность		
4K (3840x2160p)	25 к/с	61460 кбит/с	00:06.44 (чуть более 6 сек)		
Кодеры, используемые в исследовании					
Кодек	Реализация	Версия	Команда FFmpeg		
H.264/AVC	libx264	164	ffmpeg -c:v libx264		
H.265/HEVC	libx265	3.4+	ffmpeg -c:v libx265		
AV1	libsvtav1	1.7+	ffmpeg -c:v libsvtav1		
Переменные параметры по битрейту. GoP зафиксирован на значении 10 кадров					
Целевой битрейт	H.264 CRF	H.265 CRF	AV1 CRF	maxrate	bufsize
256 кбит/с	26	25	40	320k	512k
400 кбит/с	22	21	30	500k	1000k
600 кбит/с	20	19	24	750k	1500k
1000 кбит/с	18	17	23	1250k	2500k
1500 кбит/с	17	16	22	1850k	3750k
2000 кбит/с	16	15	21	2500k	5000k
3500 кбит/с	15	14	20	4200k	8400k
5000 кбит/с	14	13	19	6000k	12000k

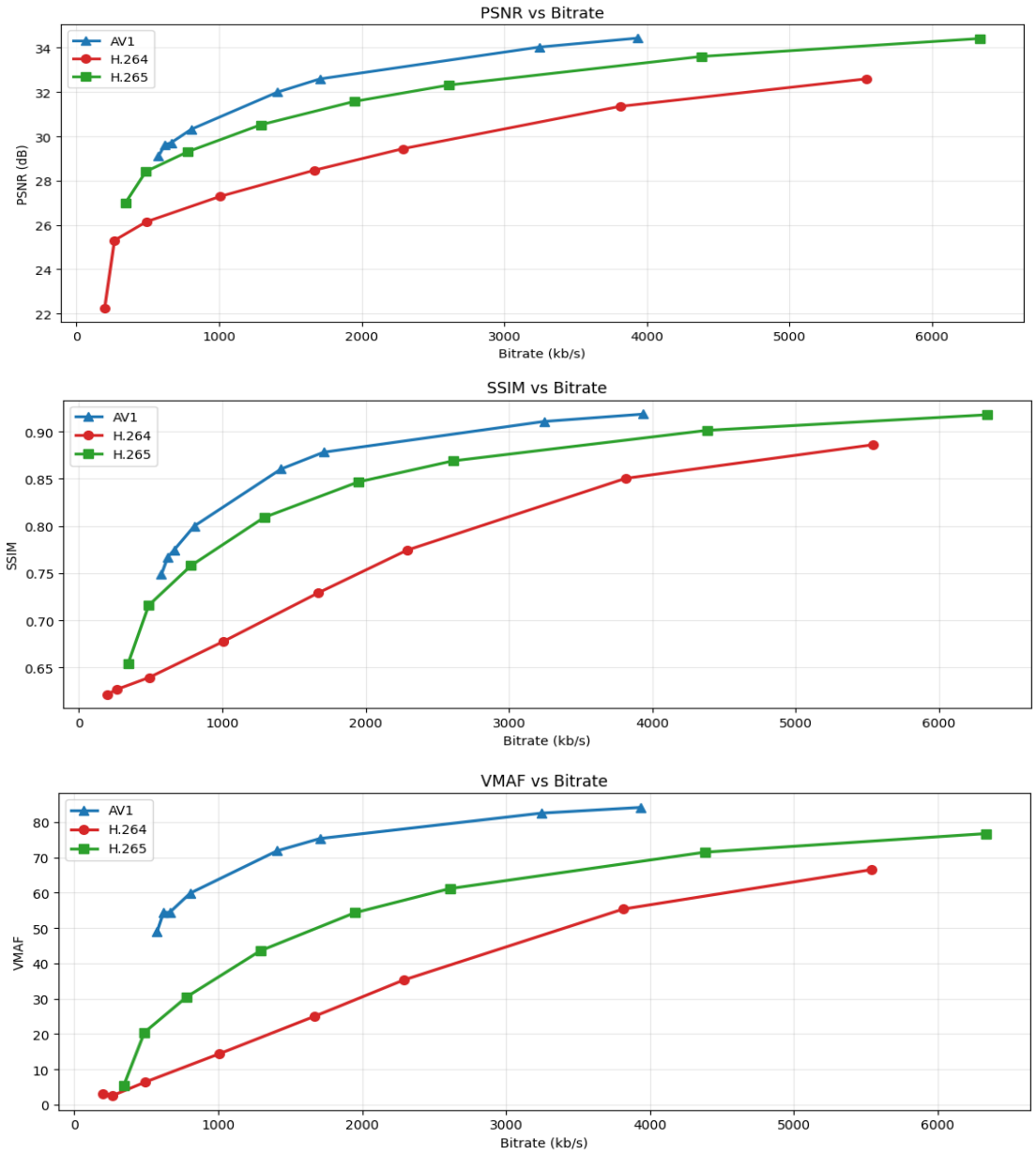


Рис. 8. Итоговое сравнение работы кодеков

Таблица 2

Рекомендации для четырех различных сценариев

Для видео 1080p 30fps	Если канал стабилен (потери <0.5%)	Для нестабильных условий (потери 0.5-5%)	Если задержка критична (<500ms)	Для максимального сжатия и эффективности
Кодек	H.265 (HEVC)	H.264 (более устойчив к ошибкам)	H.264	AV1
Пресет	-preset fast или faster	-preset faster или veryfast	-preset veryfast или ultrafast	-cpu-used 6 -usage-realtime 7
GoP	60	10–30	10–30	10–30
B-кадры	2–3	0–1	0	2–3
Битрейт	1500–2000 кбит/с (VBR с -maxrate 2500k)	2000-3000 кбит/с (CBR с небольшой буферизацией)	выше на 10–20% из-за меньших оптимизаций	1000–1500 кбит/с (Capped CRF с -maxrate 2000k)
Bufsize	5000k	4000k	2×bitrate (минимальный буфер для VBV)	3000k

Анализ полученных экспериментальных данных позволяет сделать вывод о существенном преимуществе современных стандартов кодирования над H.264. При идентичных параметрах битрейта кодеки H.265 и AV1 демонстрируют значительно более высокую эффективность сжатия. Однако выбор между HEVC и решением от AOMedia (AV1) требует учета вычислительной сложности: эксперименты показали кратное увеличение времени кодирования при использовании AV1. Следовательно, применимость данного кодека в задачах реального времени напрямую ограничивается производительностью центрального процессора (CPU).

Подобная тенденция роста требований к аппаратным ресурсам при повышении эффективности сжатия подтверждается в недавнем исследовании [10], где проводился комплексный сравнительный анализ эффективности кодеков H.265, AV1 и новейшего стандарта H.266 (VVC). В работе отмечается, что хотя AV1 превосходит H.265 в эффективности сжатия (особенно для HD и FHD разрешений), а H.266 демонстрирует наивысшую степень компрессии среди всех рассмотренных стандартов, это достижение сопряжено с непропорциональным ростом времени кодирования. Таким образом, несмотря на теоретическое превосходство новых алгоритмов, для практических систем реального времени с ограниченными ресурсами H.265 зачастую остается наиболее сбалансированным решением.

В таблице 2 приведены рекомендуемые наборы параметров для четырех различных сценариев использования кодировщиков в реальном времени, которые учитывают состояние канала и требования к задержке.

Заключение

В ходе исследования проведен сравнительный анализ эффективности современных стандартов видеокодирования (H.264, H.265/HEVC, AV1) применительно к передаче видеопотока по низкоскоростным и нестабильным радиоканалам. Экспериментальные данные показали, что переход от стандарта H.264 к H.265 позволяет снизить требования к битрейту на 30–50% при сохранении сопоставимого визуального качества (VMAF/SSIM), что является критическим фактором для узкополосных каналов связи.

Установлено, что, несмотря на максимальную эффективность сжатия кодека AV1, его применение в системах реального времени (Real-Time) ограничено высокими требованиями к вычислительным ресурсам, что делает H.265 оптимальным компромиссным решением для большинства современных мобильных платформ и встраиваемых систем.

Сформированы практические рекомендации по настройке параметров кодирования, включающие использование адаптивного управления битрейтом (VBR с ограничением пиковой скорости или Capped CRF), оптимизацию структуры GoP и корректный расчет буфера видеоданных (bufsize). Показано, что для минимизации задержек в радиоканале необходимо исключать B-кадры и использовать быстрые пресеты кодирования, жертвуя незначительной долей эффективности сжатия ради стабильности потока.

Литература

1. *Wiegand T., Sullivan G. J., Bjøntegaard G., Luthra A*. Overview of the H.264/AVC Video Coding Standard // IEEE Transactions on Circuits and Systems for Video Technology. 2003. Vol. 13, no. 7, pp. 560-576. DOI: 10.1109/TCSVT.2003.815165.

2. *Pastuszak G., Abramowski A*. Algorithm and Architecture Design of the H.265/HEVC Intra Encoder // IEEE Transactions on Circuits and Systems for Video Technology. 2016. Vol. 26, no. 1, pp. 210-222. DOI: 10.1109/TCSVT.2015.2428571.

3. *Han J., Li B., Mukherjee D., Ching-Han Chiang, Grange A., Chen C.* A Technical Overview of AV1 // Proceedings of the IEEE. 2021. Vol. 109, no. 9, pp. 1435-1462. DOI: 10.1109/JPROC.2021.3058584

4. AV1 Decoding and Hardware Ecosystem: The Future of Video Delivery [Электронный ресурс]. URL: https://visionular.ai/av1-decoding-and-hardware-ecosystem-the-future-of-video-delivery/ (дата обращения: 25.12.2025).

5. MediaTek Dimensity 1000 Is the First Smartphone SoC to Support AV1 Hardware Decoding [Электронный ресурс]. URL: https://www.xda-developers.com/mediatek-dimensity-1000-is-the-first-smartphone-soc-to-support-av1-hardware-decoding/ (дата обращения: 02.04.2025).

6. A Win for the Industry: Axis Adds Support for AV1 Encoding Standard [Электронный ресурс]. URL: https://newsroom.axis.com/article/soc-av1-video-encoding-artpec (дата обращения: 03.08.2025).

7. Werner Robitza. CRF Guide (Constant Rate Factor in x264 and x265) [Электронный ресурс]. URL: https://slhck.info/video/2017/02/24/crf-guide.html (дата обращения: 07.04.2025).

8. Limiting the output bitrate [Электронный ресурс]. URL: https://trac.ffmpeg.org/wiki/Limiting%20the%20output%20bitrate (дата обращения: 07.04.2025).

9. Real-World Perspectives on Choosing the Optimal GOP Size [Электронный ресурс]. URL: https://streaminglearningcenter.com/encoding/real-world-perspectives-on-choosing-the-optimal-GoP-size.html (дата обращения: 10.08.2025).

10. *Boumehrez F., Sahour A., Djellab H., Maamri F.* The Efficiency of HEVC/H.265, AV1, and VVC/H.266 in Terms of Performance Compression and Video Content // Indonesian Journal of Electrical Engineering and Informatics. 2024. Vol. 12, № 3, pp. 583-593. DOI: 10.52549/ijeei.v12i3.5336.

РАЗРАБОТКА КОМПЛЕКСА МЕР ДЛЯ ЗАЩИТЫ СИСТЕМ АНАЛИЗА ПЕРСОНАЛЬНЫХ ДАННЫХ С ТЕХНОЛОГИЯМИ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Кудряшова Анастасия Юрьевна
НИУ МАИ, к.т.н., доцент, кафедра 402;
МТУСИ, к.т.н., доцент, кафедра ОТТ, Москва, Россия,
asykka@bk.ru

Кутузов Кирилл Геннадьевич
НИУ МАИ, студент, кафедра 402, гр. М4О-412Б-22, Москва, Россия,
thezelenglobal5454@mail.ru

Аннотация
В условиях внедрения искусственного интеллекта во все сферы деятельности нашей жизнь системы кадровой аналитики не прошли стороной. Эти системы требуют автоматизации процессов, связи с наличием больших объемом данных. Интеллектуальные системы кадровой аналитики значительно облегчают эту работу. Они обеспечивают сбор, обработку и анализ огромных массивов персональных данных сотрудников. Однако использование технологий искусственного увеличивает риск нарушения конфиденциальности, целостности и доступности персональных данных. В связи с этим необходима разработка адекватных мер защиты, приведенных в статье.

Ключевые слова
Системы анализа персональных данных (САПД), искусственный интеллект (ИИ), нарушения конфиденциальности, модель угроз, модель нарушителя, моделирование атак.

Введение

Правовое регулирование обработки персональных данных в Российской Федерации основывается на принципах конституции, федеральных законов и нормативных актов. Основополагающим документом служит Федеральный закон № 152-ФЗ «О персональных данных» [1]. Акт вводит понятие персональных данных и определяет категории субъектов, их права, а также обязанности операторов. Закон устанавливает требования к организационным и техническим мерам по обеспечению безопасности данных при их обработке.

Согласно закону, оператор обязан реализовывать меры, направленные на предотвращение нарушений безопасности персональных данных., на рисунке 1.

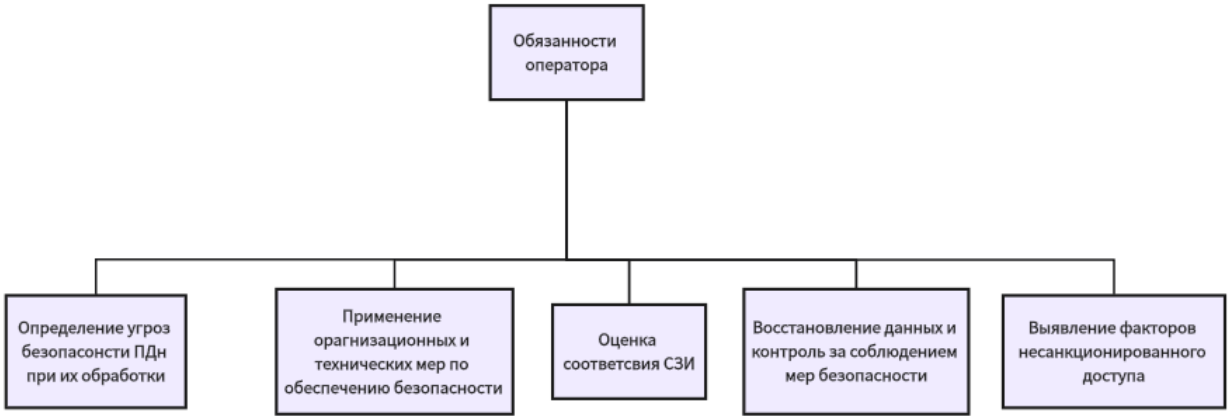


Рис. 1. Обязанности оператора

В С 1 марта 2026 года вступит в силу Приказ ФСТЭК России от 11.04.2025 № 117. Документ впервые вводит профильные требования к защите информации при использовании искусственного интеллекта: контроль данных, моделей, процессов обработки и запрет на передачу ограниченной информации разработчикам моделей. Эти положения актуальны при разработке и эксплуатации интеллектуальных систем кадровой аналитики в государственном и частном секторе.

Дополнением к указанным актам служит методические рекомендации ФСТЭК России по безопасности искусственного интеллекта и стандарты ГОСТ Р, устанавливающие требования к системам на базе машинного обучения. Однако на момент исследования отсутствует специализированный нормативный акт, целиком учитывающий специфику интеллектуальной кадровой аналитики. Это создаёт определённую правовую неопределённость и требует адаптации существующих норм.

Особенности защиты информации систем анализа персональных данных с использованием технологий искусственного интеллекта

Автоматизированная система кадровой аналитики – программно-аппаратный комплекс, предназначенный для сбора, накопления, обработки и анализа персональных данных сотрудников с применением методов машинного обучения, статистики и прогнозирования. Типовая конфигурация представлена на рисунке 2.

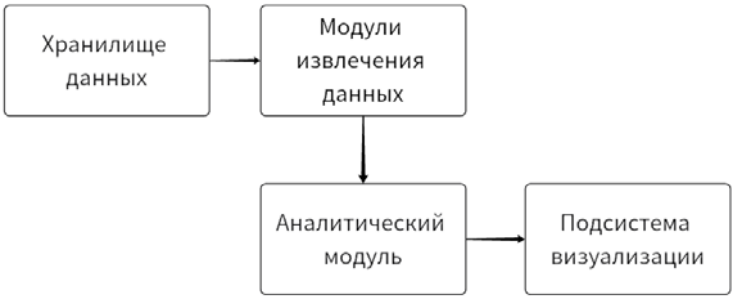


Рис. 2. Типовая конфигурация

Особенность системы - способность обезличиванию персональных данных. При этом требуется сохранить возможность идентификации субъекта.

Кроме того, модели искусственного интеллекта могут содержать скрытые зависимости. Которые дают возможность восстановить исходные данные или получить информацию, превышающую предоставленное субъектом согласие.

Разработка системы ориентирована на предприятия с численностью персонала от нескольких сотен до десятков тысяч человек. Соответственно, обрабатываемые персональные данные требуют строгих мер защиты.

Архитектурные решения, лежащие в основе интеллектуальной системы кадровой аналитики, могут быть соотнесены с положениями ГОСТ Р 71540-2024 «Искусственный интеллект. Эталонная архитектура инженерии знаний» [3]. Стандарт устанавливает эталонную архитектуру для инженерии знаний в сфере искусственного интеллекта. Он фиксирует роли, действия, конструктивные уровни, компоненты и их взаимосвязи как между собой и с другими системами с точки зрения системного пользователя и функциональных моделей.

Анализ нормативной базы определяет ряд требований, которые важно учитывать в процессе разработки, внедрения и использования системы.

Любая операция с персональными данными должны быть определены конкретными, законными целями (ст. 5 Закона № 152-ФЗ) [1]. Использование искусственного интеллекта не должно приводить к обработке данных, выходящей за эти рамки. Данный факт обязывает чётко фиксировать цели обработки в политике оператора и исключать избыточный анализ, способный нарушать права субъектов.

Получение согласия субъекта персональных данных должно быть конкретным, информированным и сознательным (п. 4 ст. 9 Закона № 152-ФЗ) [1]. При эксплуатации интеллектуальных систем необходимо подробно информировать сотрудников о видах обрабатываемых данных, применяемых алгоритмах и целях обработки. Согласно п. 2 ст. 16 этого же закона, исключительное автоматизированная обработка данных возможна только при наличии согласия в письменной форме.

Обработка данных при использовании облачных сервисов за пределами РФ обязует соблюдать требования о локализации баз персональных данных на территории России, что означает обязательное хранение первичных данных сотрудников на российских серверах (ст. 18 Закона № 242-ФЗ, вносящего изменения в Закон № 152-ФЗ) [1].

Оператор обязан создать и утвердить модель угроз безопасности персональных данных согласно базе данных угроз ФСТЭК, методики оценки угроз от 05.02.2021, Приказам ФСТЭК России № 21 и ФСБ России

№ 378 [4]. Интеллектуальный характер системы расширяет спектр угроз и требует подхода, учитывающего особенности искусственного интеллекта.

Организационные ограничения выражаются в необходимости назначения ответственных структурных подразделений или сотрудников за безопасность, проведении внутреннего контроля и регулярных аудитов, обучении персонала с доступом к данным.

В заключении можно обозначить, анализ нормативной базы подтверждает разработку и использование интеллектуальной системы кадровой аналитики только при строгом соблюдении комплекса правовых требований и разработке внутренних организационных документов, в которых учитываются технологические особенности. Отсутствие стандартизированных методов для автоматизированных интеллектуальных систем обязывает разработчиков внимательного и сдержанного интерпретации правил.

После установления правовых и организационных рамок следует перейти к исследованию актуальных угроз. В ходе практики была разработана модель угроз для системы анализа ПДн с использованием технологии искусственного интеллекта. Также сформирован перечень организационных и технических мер для нейтрализации выявленных рисков. В дальнейшем представлены результаты моделирования и комплекс требований, выведенный на их основе.

Для моделирования угроз выбрана интеллектуальная ИСПДн «Система анализа персональных данных с использованием технологий искусственного интеллекта». Основная функция системы - обработка и обезличивания персональных данных сотрудников и корпоративных документов. В состав входят серверы баз данных, серверы приложений, автоматизированные рабочие места, а также сетевое оборудование. Обрабатываемые данные включают общедоступные и иные (те же общедоступные ПДн, но обрабатываемые не в режиме публичности). Основания обработки включают трудовой договор, согласие и федеральные законы.

В ходе практики проведен анализ угроз, основанный на Методике оценки угроз ФСТЭК России от 5 февраля 2021 г. [4], банке данных угроз ФСТЭК и базе MITRE ATT&CK [5,6].

Процесс исследования угроз представляет собой выявление, анализ и оценку возможных опасностей нарушения функционирования системы и конфиденциальности обрабатываемых данных. Данная методология охватывает ряд ключевых элементов:

- Объекты воздействия;
- Виды воздействия;
- Источники угроз;
- Тактики и техники реализации угроз;
- Вероятность реализации угроз;
- Технологии, на которые направлены угрозы;
- Формирование требований к защите.

Анализ также показал, что при оценке актуальности угроз должны рассматриваться только угрозы, которые имеют следующие объекты воздействия:

- Рабочие станции;
- Серверы;
- База данных;
- Защищаемые данные;
- Сетевой трафик;
- Каналы связи (передачи) данных;
- Прикладное программное обеспечение;
- Системное программное обеспечение;
- Аутентификационные данные пользователя;
- Модель искусственного интеллекта;
- Обучающие данные машинного обучения;
- Программное обеспечение (программы), использующее машинное обучение;
- Программное обеспечение (программы), реализующие технологии искусственного интеллекта.

Для определенных информационных ресурсов и компонентов систем и сетей должны быть определены виды воздействия на них, которые могут привести к негативным последствиям [7].

Основными видами таких воздействий представлены на рисунке 3.

Рис. 3. Виды воздействий

Нарушители разделены на внешних (хакеры, конкурирующие организации, бывшие сотрудники) и внутренних (разработчики, администраторы, сотрудники, технический персонал).

Особенность интеллектуальной системы заключается в высокой значимости внутренних нарушителей, способных не только украсть информацию, но и модифицировать алгоритмы или извлечь скрытую информацию из моделей.

Техники и тактики реализации угроз:

В процессе разработки модели угроз для системы анализа ПДн с использованием искусственного интеллекта сценарии реализации угроз безопасности определены в соответствии с требованиями методики оценки угроз безопасности информации.

Основные тактики реализации угроз:

- T01 – Сбор информации о системах и сетях;
- T02 – Получение первоначального доступа к компонентам систем и сетей;
- T03 – Внедрение и исполнение вредоносного программного обеспечения в системах и сетях;
- T04 – Закрепление (сохранение доступа) в системе или сети;
- T05 – Управление вредоносным программным обеспечением и (или) компонентами, к которым ранее был получен доступ;
- T06 – Повышение привилегий по доступу к компонентам систем и сетей;
- T07 – Сокрытие действий и применяемых при этом средств от обнаружения;
- T08 – Получение доступа (распространение доступа) к другим компонентам систем и сетей или смежным системам и сетям;
- T09 – Сбор и вывод из системы или сети информации, необходимой для дальнейших действий при реализации угроз безопасности информации или реализации новых угроз;
- T10 – Несанкционированный доступ и (или) воздействие на информационные ресурсы или компоненты систем и сетей, приводящие к негативным последствиям.

Для каждого сценария были определены тактики и техники, которые могут быть применены нарушителем. Результат моделирования сценариев приведен на рисунке 4, где отражены все техники, применимые для нашей системы.

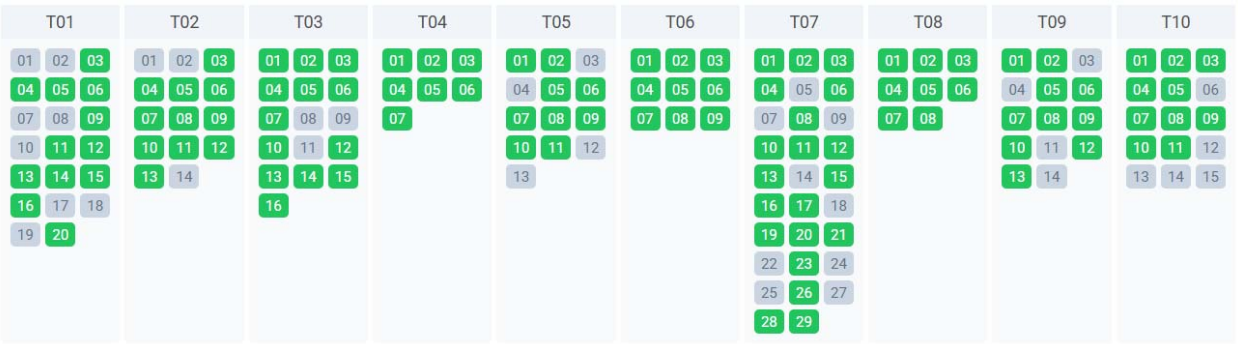


Рис. 4. Актуальные техники для системы анализа ПДн с использованием искусственного интеллекта

Каждая техника была оценена по частоте использования (рис. 5). Чем темнее ячейка, тем чаще данная техника используется в системе.

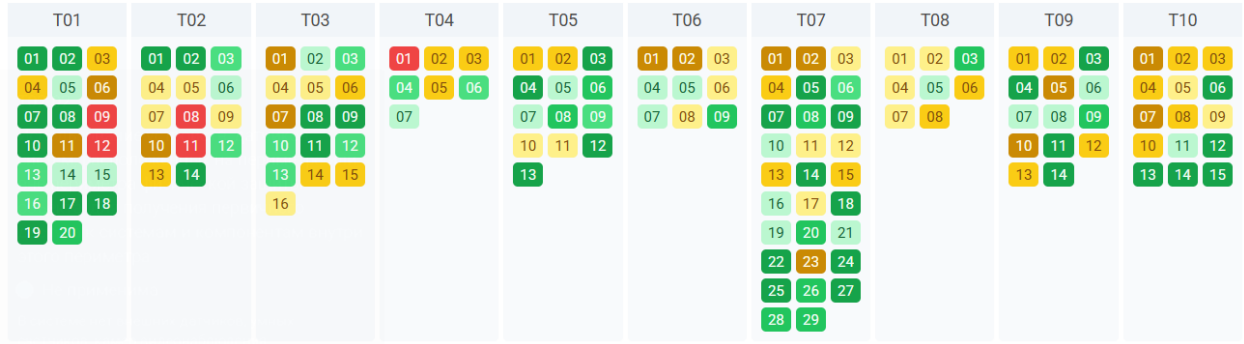


Рис. 5. Градация техник по частоте использования злоумышленником

По итогам оценки был сформирован перечень актуальных угроз. В таблице 1 приведен список основных угроз для данной системы.

Таблица 1

Перечень основных угроз

Тип угроз	Перечень угроз	Вероятность реализации	Уровень последствий
Угрозы, связанные с действиями людей (внешних и внутренних нарушителей)	Угроза несанкционированного копирования защищаемой информации	Высокая	Высокий
	Угроза несанкционированного удаления защищаемой информации	Средняя	Высокий
	Угроза неправомерного ознакомления с защищаемой информацией	Высокая	Средний
	Угроза подмены доверенного пользователя	Средняя	Высокий
	Угроза использования информации идентификации/ аутентификации, заданной по умолчанию	Средняя	Высокий
	Угроза несанкционированного создания учётной записи пользователя	Средняя	Высокий
	Угроза несанкционированного изменения аутентификационной информации	Средняя	Высокий
	Угроза удаления аутентификационной информации	Средняя	Высокий
	Угроза «фишинга»	Высокая	Высокий
	Угроза нецелевого использования вычислительных ресурсов средства вычислительной техники	Средняя	Средний
	Угроза утраты носителей информации	Низкая	Низкий
Угрозы, обусловленные уязвимостями программного обеспечения	Угроза внесения недекларированных (недокументированных) возможностей в прикладном программном обеспечении	Низкая	Высокий
	Угроза повышения привилегий	Средняя	Высокий
	Угроза приведения системы в состояние «отказ в обслуживании»	Средняя	Средний
	Угроза перехвата данных, передаваемых по вычислительной сети	Низкая	Средний
	Угроза перехвата управления информационной системой	Низкая	Высокий
	Угроза несанкционированного использования системных и сетевых утилит	Средняя	Средний
	Угроза использования уязвимых версий программного обеспечения	Средняя	Высокий
	Угроза пропуска проверки целостности программного обеспечения	Низкая	Высокий
	Угроза внедрения кода или данных	Средняя	Высокий
	Угроза подделки записей журнала регистрации событий	Средняя	Высокий
	Угроза использования слабостей протоколов сетевого/локального обмена данными	Низкая	Средний
Специфические угрозы для ИИ-систем	Угроза раскрытия информации о модели машинного обучения	Средняя	Средний
	Угроза хищения обучающих данных	Средняя	Высокий
	Угроза модификации модели машинного обучения путем искажения («отравления») обучающих данных	Низкая	Высокий
	Угроза нарушения функционирования («обхода») средств, реализующих технологии искусственного интеллекта	Низкая	Средний
	Угроза подмены модели машинного обучения	Низкая	Высокий

Каждая из перечисленных угроз была проанализирована с учетом степени вероятности их осуществления и возможных последствий. Для значительной части угроз вероятность реализации и уровень последствий определены как средние или высокие.

Для данной системы актуальны угрозы 1-го типа. Категория обрабатываемых ПДн – иные. Следовательно, согласно Постановлению Правительства РФ № 1119 системе присвоен первый уровень защищённости (УЗ-1) (рис. 6) [8]. Это требует реализации средств защиты не ниже соответствующего класса, включая сертифицированные средства защиты информации. Для соответствия уровню безопасности необходим комплекс организационных и технических мер [9, 10].

Тип ИСПДн	Субъекты ПДн	Объем ПДн	Типы актуальных угроз		
			1 тип	2 тип	3 тип
Специальные	Не сотрудники	Более 100 тыс.	УЗ 1	УЗ 1	УЗ 2
		Менее 100 тыс.	УЗ 1	УЗ 2	УЗ 3
	Сотрудники	Любое	УЗ 1	УЗ 2	УЗ 3
Биометрические	Не сотрудники	Более 100 тыс.	УЗ 1	УЗ 2	УЗ 3
		Менее 100 тыс.	УЗ 1	УЗ 2	УЗ 3
	Сотрудники	Любое	УЗ 1	УЗ 2	УЗ 3
Иные	Не сотрудники	Более 100 тыс.	УЗ 1	УЗ 2	УЗ 3
		Менее 100 тыс.	УЗ 1	УЗ 3	УЗ 4
	Сотрудники	Любое	УЗ 1	УЗ 3	УЗ 4
Общедоступные	Не сотрудники	Более 100 тыс.	УЗ 2	УЗ 2	УЗ 4
		Менее 100 тыс.	УЗ 2	УЗ 3	УЗ 4
	Сотрудники	Любое	УЗ 2	УЗ 3	УЗ 4

Рис. 6. Определение уровня защищённости ПДн согласно ПП РФ №1119 [2]

Для системы анализа ПДн с уровнем защищенности 1 (УЗ-1) последствия утечки ПДн наиболее чувствительны, а вероятность инцидентов выше из-за архитектуры системы и объема данных. Для таких систем требуется максимальный набор организационных и технических мер защиты, контроль доступа и механизмы журналирования событий [11-14].

Согласно Приказу ФСТЭК России № 117 [2], информационным системам присваиваются классы защищённости К1-К3 в зависимости от масштабов и значимости информации (табл. 2).

Таблица 2

Определение класса типовой ИСПДн

Категория ПДн	Менее чем 1000 субъектов ПДн или ПДн субъектов ПДн в пределах конкретной организации	От 1000 до 100 000 субъектов ПДн или раб. в отрасли эк-ки РФ, в органе гос. власти, проживающий в пределах МО	Более чем 100 000 субъектов ПДн или ПДн субъектов ПДн в пределах субъекта РФ или РФ в целом
Обезличенные и(или) общедоступные данные	К4	К4	К4
ПДн, позволяющие идентифицировать субъекта ПДн	К3	К3	К2
ПДн, позволяющие идентифицировать субъекта ПДн и получить о нем доп. информацию	К3	К2	К1
ПДн, касающиеся расовой, национальной принадлежности, полит. взглядов, религиозных и философских убеждений, состояния здоровья и интимной жизни	К1	К1	К1

Для рассматриваемой системы применим уровень К2. Этот класс предполагает реализацию защиты, рассчитанную на высококвалифицированных нарушителей [14].

На основании исследования угроз и нормативных требований был сформирован набор организационных и технических мероприятий. Эти меры направленны на защиту не только традиционных компонентов, но и элементов, связанных с искусственным интеллектом (табл. 3).

Таблица 1

Набор организационных и технических мер защиты системы

Требования	Меры
Организационные требования	Назначение администратора системы и ответственных за безопасность данных
	Разработку и утверждение модели угроз с обязательным обновлением не реже одного раза в три года или при изменениях архитектуры
	Формирование перечня мероприятий по нейтрализации угроз с учетом криптографической защиты
	Создание внутренних политик, регламентирующих процедуры получения согласий, обезличивания, хранения и реагирования на инциденты
	Регулярное обучение сотрудников с доступом к системе с учетом особенностей интеллектуальных систем
	Организация периодического аудита и контроль эффективности мер защиты с анализом журналов и проведением тестирования на проникновение
Технические требования	Управление доступом на основе ролевой модели, применение двухфакторной аутентификации для привилегированных пользователей и регистрация всех операций с данными и моделями
	Криптографическая защита данных в базах и при передаче с использованием сертифицированных СЗИ
	Внедрение антивирусных средств и систем обнаружения и предотвращения вторжений (IDS/IPS) на всех серверах и рабочих станциях
	Периодическая оценка рисков, анализ уязвимостей и своевременное обновление компонентов
	Развертывание сетевых и локальных средств обнаружения вторжений, адаптированных к атакам на API и системы искусственного интеллекта
	Обеспечение резервного копирования и отказоустойчивости с хранением копий в защищённых условиях
Требование к защите модели ИИ и обучающих данных	Ограничение доступа к моделям ИИ и обучающим данным по принципу минимально необходимых привилегий
	Внедрение механизмов мониторинга запросов к моделям, включая ограничение частоты запросов и выявление аномалий для защиты от атак по извлечению данных
	Применение при обучении методов дифференциальной приватности с целью снижения вероятности восстановления исходных данных
	Обеспечивается целостность моделей посредством контроля версий и использования электронной подписи

В соответствии с пунктом 60 Приказа ФСТЭК России № 117 [2], при функционировании интеллектуальной системы кадровой аналитики необходимо исключить: несанкционированный доступ к наборам данных и моделям, запретить передачу информации разработчикам моделей, определить шаблоны запросов и ответов, разработать критерии для выявления недостоверных ответов искусственного интеллекта и обеспечить соответствующие меры реагирования.

Заключение

В ходе анализа требований был сформирован итоговый перечень условий, необходимых для создания подсистемы защиты персональных данных в рамках системы анализа ПДн.

Данный перечень включает:

- Перечень нормативных и методических документов, которым должна соответствовать система (152-ФЗ, ПП РФ №1119, Приказы ФСТЭК №21, №239, Приказ ФСБ №378, Приказ ФСТЭК России № 117, ГОСТ Р 71540–2024);
- Классификация обрабатываемых персональных данных с определением уровня защищённости;
- Утвержденная модель угроз;
- Перечень организационных и технических мер по нейтрализации актуальных угроз;
- Разработка организационно-распорядительные мер согласно методической рекомендации по разработке нормативных правовых актов;
- Технические меры защиты на различных уровнях (сетевом, приложений, данных, моделей);

- Сертифицированные средства защиты информации, согласно ФСТЭК России или ФСБ России;
- Регламент оценки эффективности, включающий периодичность контроля и методы тестирования.

Данный комплекс требований был представлен руководству профильной компании и принят для использования при проектировании демонстрационной версии интеллектуальной системы кадровой аналитики для одного из ключевых заказчиков. Реализация изложенных требований позволит обеспечить соответствие системы действующему законодательству и повысить эффективность нейтрализации выявленных угроз безопасности персональных данных.

Литература

1. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» [Электронный ресурс] // Контур Норматив. Режим доступа: https://normativ.kontur.ru/document?moduleId=1&documentId=501173 (дата обращения: 03.04.2026).

2. Приказ ФСТЭК России от 11.04.2025 № 117 «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений» [Электронный ресурс] // Контур Норматив. Режим доступа: https://normativ.kontur.ru/document?moduleId=1&documentId=500478 (дата обращения: 05.04.2026).

3. Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» [Электронный ресурс] // Контур Норматив. Режим доступа: https://normativ.kontur.ru/document?moduleId=1&documentId=370164 (дата обращения: 03.04.2026).

4. ГОСТ Р 71540-2024. Искусственный интеллект. Эталонная архитектура инженерии знаний [Электронный ресурс] // Интернет и право – Режим доступа: https://internet-law.ru/gosts/gost/83867/ (дата обращения: 06.04.2026).

5. Банк данных угроз безопасности информации [Электронный ресурс] // ФСТЭК России. Режим доступа: https://bdu.fstec.ru (дата обращения: 03.04.2026).

6. База данных векторов компьютерных атак MITRE ATT&CK [Электронный ресурс] // Матрица ATT&CK для предприятий. Режим доступа: https://attack.mitre.org (дата обращения: 03.04.2026).

7. *Кузнецов М. А., Кузнецова Н. С., Кудряшова А. Ю*. Разработка пользовательского инструмента для выбора способа построения сети // Современная педагогика и научные исследования в образовательной организации высшего образования : Сборник докладов очно-заочной научно-методической конференции, Кострома, 16 февраля 2025 года. Кострома: Военная академия радиационной, химической и биологической защиты им. Маршала Советского Союза С.К. Тимошенко, 2025. С. 271-284. EDN GJTBIB.

8. Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» [Электронный ресурс] // ГАРАНТ.РУ. Режим доступа: https://base.garant.ru/70252506/ (дата обращения: 03.04.2026).

9. *Кудряшова А. Ю., Юшко А. Ю.* Исследование способов представления данных в вычислительных системах // DSPA: Вопросы применения цифровой обработки сигналов. 2025. Т. 15, № 4. С. 41-46. EDN XYROEB.

10. *Сафронов К. О., Кудряшова А. Ю., Молодцова Ю. В*. Исследование взаимосвязи галлюцинаций ИИ, длины промптов и логических парадоксов: роль сложности Колмогорова и семантического анализа в обеспечении целостности информационных систем // REDS: Телекоммуникационные устройства и системы. 2025. Т. 15, № 3. С. 22-26. EDN WOPNND.

11. *Timoshenkov A. I., Kudryashova A. Y.* A study of SGD and ADAM approaches to training an LSTM artificial neural network for malicious traffic recognition // Synchroinfo Journal. 2025. Vol. 11, No. 4, pp. 9-14. DOI 10.36724/2664-066X-2025-11-4-9-14. EDN YZOHWD.

12. *Zakharova V. A., Kudryashova A. Y.* The digital twin of the cyber-study enterprise: new methods for simulating the most complex attacks // Synchroinfo Journal. 2025. Vol. 11, No. 5, pp. 18-27. DOI 10.36724/2664-066X-2025-11-5-18-27. EDN GTRZUM.

13. *Кудряшова А. Ю., Захарова В. А.* Разработка мер информационной безопасности предприятий ОПК для реализации политики «Цифровая экономика 2030» // Телекоммуникации и информационные технологии. 2024. Т. 11, № 2. С. 45-51. EDN QUIWOG.

14. *Кудряшова А. Ю., Хорошун В. В*. Разработка автоматизированных средств тестирования системы управления коммутационным оборудованием // REDS: Телекоммуникационные устройства и системы. 2024. Т. 14, № 4. С. 21-26. EDN AGCFMD.

15. *Поборчая Н. Е., Кудряшова А. Ю.* Анализ нерекуррентных алгоритмов детектирования сигнала 4-qam в системе с MIMO с разным количеством антенн в условиях Релеевского канала с доплеровским расширением спектра // Наукоемкие технологии в космических исследованиях Земли. 2024. Т. 16, № 5. С. 35-41. DOI 10.36724/2409-5419-2024-16-5-35-41. EDN JWYYLD.

РАЗРАБОТКА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ДЛЯ ИМИТАЦИОННОГО МОДЕЛИРОВАНИЯ СИСТЕМ СИНХРОНИЗАЦИИ ШКАЛЫ ВРЕМЕНИ

Лоховин Владимир Александрович
АО «ЦЭНКИ», г. Москва, Россия,
vladimir.lokhovin@yandex.ru

Шварц Михаил Львович
МТУСИ, Москва, Россия, mschwartz@smsync.ru

Аннотация
Сегодня имеется необходимость в дальнейшем развитии технологий частотно-временного обеспечения (ЧВО) с использованием наземных каналов связи с целью снижения зависимости от глобальных навигационных спутниковых систем (ГНСС). Исходя из имеющихся задач в области исследования систем ЧВО и с учетом возрастающей сложности телекоммуникационных систем в целом авторами выбрано направление имитационного моделирования систем синхронизации и совершенствовании методов моделирования с целью прогнозирования устойчивости систем синхронизации к воздействиям со стороны внутренних и внешних факторов. В статье представлена общая концепция имитационной модели, проведен краткий обзор результатов моделирования структуры системы на основе агентного подхода с использованием карт состояний, а также результаты разработки программного обеспечения для оценки состояния параметров синхронизации в зависимости от состояния работоспособности имитируемой системы.

Ключевые слова
Имитационное моделирование, сети связи, частотно-временное обеспечение, синхронизация, разработка программного обеспечения, Java, SQL.

Введение

Недостатком технологии сличения шкал времени (ШВ) пользователей со шкалами национальных стандартов по сигналам различных глобальных спутниковых навигационных систем (ГНСС), таких как ГЛОНАСС, GPS, Galileo, BeiDou, является ее зависимость от электромагнитной обстановки, солнечной активности и других факторов, сопутствующих технологиям передачи сигналов по радиоканалам. Помимо классических задач навигации и высокоточного сличения шкал времени, ГНСС также применяется для решения задач метрологии, геодезии, калибровки средств измерений и иных приложений.

Поэтому сегодня среди основных исследований в области ЧВО можно выделить работы, направленные на снижение зависимости от спутниковых систем, усиление защиты от внешнего влияния на сигналы ГНСС, повышение качества и надежности распространения сигналов точного времени по наземным волоконно-оптическим системам передачи (ВОСП) с высокой точностью, повышение доступности услуг ЧВО для широкого круга потребителей мультисервисных сетей благодаря развитию технологий передачи такой информации в сетях электросвязи [1-8].

В качестве одного из решений проблемы предлагается обратить внимание на альтернативу спутниковым системам в лице перспективных когерентных сетей связи общего пользования (КССОП), построенных на базе наземных волоконно-оптических систем передачи (ВОСП), концепция которых подробно описана в работах [9-13, 25, 26].

Исходя из имеющихся задач авторами выбрано направление имитационного моделирования систем синхронизации с целью оценки их устойчивости к воздействиям со стороны внутренних и внешних факторов, оценки эксплуатационных параметров, в том числе прогнозирования дрейфа ШВ и расчета бюджета ошибки времени, а также сравнения существующих и перспективных способов сличения шкал времени пользователей с национальными стандартами.

Результаты исследования

1. Концепция и задача имитационного моделирования

По задумке авторов разрабатываемая имитационная модель строится вокруг идеи о совмещении подходов к анализу устойчивости функционирования системы (заключающейся, например, в расчёте коэффициента готовности) и оценке эксплуатационных параметров, среди которых – качество передаваемых сигналов, скорость выхода системы на режим нормальной работы, время автономного удержания шкалы вре-

мени в заданных пределах, устойчивость к влиянию внешних помех, стоимостные показатели. Такой подход основан на исследовании системы через призму выполняемых функций, детальный анализ её структуры и часто именуется функциональным или структурно-функциональным анализом [14-16].

Применительно к области телекоммуникаций структурно-функциональный анализ позволяет рассматривать сложные системы как совокупность отдельных функциональных групп, каждая из которых выполняет определенную роль. Это позволяет расставлять приоритеты на основе оценки критичности выполняемых функций, уточнять требования к отдельным функциональным группам, выявлять слабые звенья внутри отдельных функциональных групп, принимать решения по усилению или устранению структурной избыточности. При структурно-функциональном анализе оцениваются различные показатели эффективности работы оборудования и программного обеспечения, изучаются алгоритмы технологических процессов, происходящих внутри системы, логика информационного взаимодействия между компонентами систем [17-19]. Такой подход позволяет формулировать интегральные показатели эффективности системы, которые не искажают результаты имитационного моделирования и не приводят к ошибочной интерпретации полученных данных.

В этом смысле разрабатываемая модель должна решать широкий круг задач, которые непосредственно следуют из задач частотно-временного обеспечения. С одной стороны, поддержание точности шкалы времени потребителя достигается только при осуществлении всех видов синхронизации (по частоте, фазе и времени). С другой стороны, выполнение функций ЧВО напрямую зависит от устойчивости системы и её компонентов.

Таким образом, основной задачей является моделирование дрейфа шкалы времени ведущих часов в зависимости от состояния работоспособности моделируемой системы и ее компонентов, в том числе моделирование дрейфа при нормальном режиме работы, при спуфинговых атаках, в режиме холдовера и т.д. Здесь и далее под системой будем понимать весь комплекс оборудования, участвующий в передаче информации о шкале времени от государственных эталонов времени и частоты к пользователям мультисервисных сетей.

2. Моделирование системы при помощи карт состояний

Первым шагом на пути к созданию имитационной модели была разработка небольшой модели на основе агентного моделирования, использующего карты состояний агентов модели для описания происходящих в имитируемой системе событий и оценки ее работоспособности. В публикации [20] продемонстрированы структура модели линии передачи информации о ШВ, принцип работы и результаты моделирования.

Для создания исходной модели в качестве среды моделирования было выбрано готовое решение (AnyLogic). На первоначальном этапе это позволило отказаться от разработки собственного кода, обеспечило легкую масштабируемость, наглядность переходов между состояниями и встроенные инструменты отладки и логирования.

В ходе моделирования оценка состояния имитируемой системы проводится по трем интегральным состояниям: 1. Пользователю передаются точные синхросигналы; 2. Передаются неточные синхросигналы; 3. Сигналы не передаются. На рис.1 представлен фрагмент разработанной модели линии синхронизации, имитирующий ведущие часы (в модель внесены корректировки).

Внутри каждого компонента модели (агента) находится собственная аналитическая модель. Конкретная модель расчета и входные параметры выбираются в зависимости от стадии жизненного цикла, на котором проводится моделирование, а также от топологии и сложности компонента [21]. К примеру, как показано на рис. 1, переход компонента «PRTC» (Primary Reference Time Clock, первичный эталонный источник времени и частоты) модели линии синхронизации из рабочего (PRTCon) в нерабочее (PRTCdown) состояние может быть связан с заложенными в модель параметрами: вероятность безотказной работы компонента или системы, ограничение времени нахождения в определенном режиме (например, в режиме холдовера), расчетное время восстановления и т.п.

В публикации была показана целесообразность дальнейшего развития модели, насыщения её дополнительным функционалом для сравнения различных топологий и способов сличения шкал времени пользователей с национальными стандартами, моделирования работы элементов КССОП и их взаимодействия, учета влияния происходящих в системе синхронизации событий на ход шкалы времени.

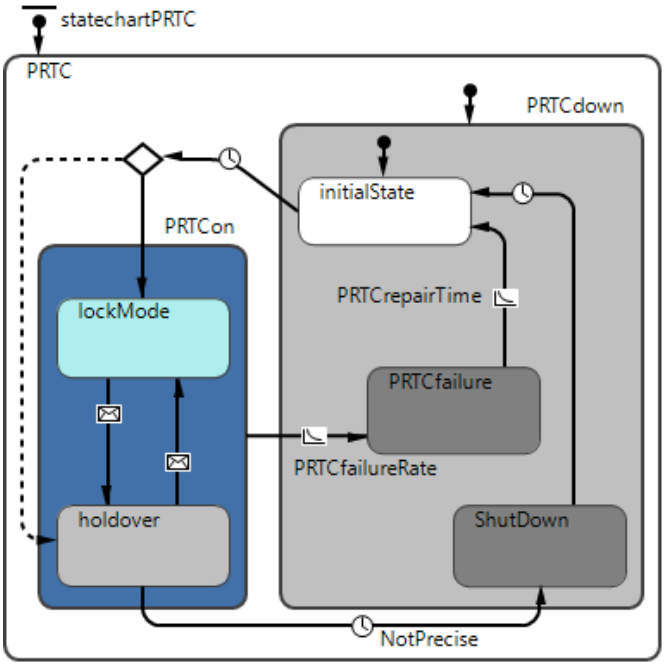


Рис. 1. Фрагмент имитационной модели линии синхронизации

3. Моделирование дрейфа шкалы времени, разработка программного обеспечения

Следующим этапом был выбор способа моделирования дрейфа шкалы времени. Для этого осуществлены:

– выбор стека технологий для создания модели ШВ (язык программирования, тип базы дынных);

– выбор способа взаимодействия с моделью структуры системы;

– выбор входных и выходных параметров, описание граничных условий для оценки характеристик моделируемой шкалы времени;

– разработка исходной версии программного обеспечения, отладка.

Изначально проведение расчетов планировалось осуществлять непосредственно в среде имитационного моделирования, поэтому в качестве языка программирования был выбран язык Java, который является внутренним языком реализации в AnyLogic. В процессе разработки по мере расширения функционала, учитывая сложность задачи, а также для большей независимости от проприетарных приложений, было принято решение применить гибридный подход и вынести вычисления функциональной части модели во внешние модули, разработав собственное ПО. При этом язык Java был сохранен, так как в контексте имитационного моделирования и будущих задач по развитию модели у Java имеются специфические преимущества перед остальными языками программирования, в особенности узкоспециализированными. Среди наиболее актуальных:

– поддержка объектно-ориентированного подхода для моделирования сложных систем как набора взаимодействующих объектов;

– кроссплатформенность;

– наличие специализированных Java-библиотек для имитационного моделирования;

– возможность легкой контейнеризации и масштабирования;

– сохранение обратной совместимости с предыдущими версиями JVM;

– наличие решений по настройке многопоточных вычислений, моделированию распределённых систем.

Таким образом, разработан программный комплекс, представляющий собой инструмент для оценки влияния событий, происходящих в имитируемой системе синхронизации, на параметры формируемой шкалы времени. Структура программного комплекса приведена на рис. 2.

Входные данные для вычислений дрейфа ШВ содержатся в лог-файле Excel среды моделирования. В таблицах 1 и 2 приведены фрагменты листов лог-файла, формируемого в среде моделирования, где зафиксированы такие параметры, как время входа и время выхода из состояния, среднее и общее время пребывания агента в состоянии. Представленные таблицы лог-файлов сформированы в ходе моделирования сценария с частыми переходами между состояниями, что применялось для наглядности и удобства работы на этапе разработки и отладки взаимодействия компонентов комплекса.

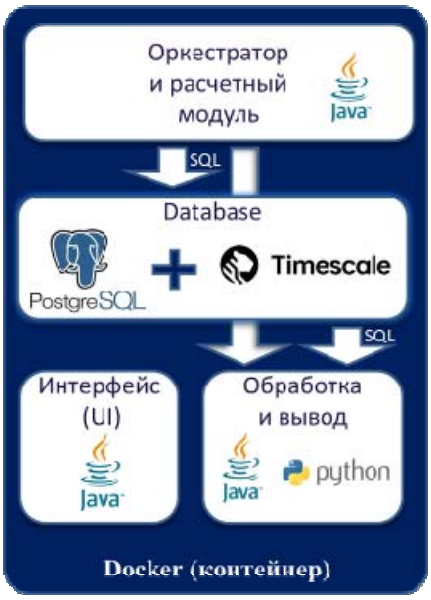


Рис. 2. Структура программного обеспечения

Таблица 1

Фрагмент лог-файла
(время входа и время выхода из состояния)

state	entry date	exit date
InitialState	24.10.2025 15:06:44	24.10.2025 15:21:44
PRTCon	24.10.2025 15:21:44	24.10.2025 15:25:06
PRTCdown	24.10.2025 15:25:06	24.10.2025 15:26:51
InitialState	24.10.2025 15:26:51	24.10.2025 15:41:51
PRTCon	24.10.2025 15:41:51	24.10.2025 16:40:11

Таблица 2

Фрагмент лог-файла.
(среднее и общее время пребывания в состоянии)

state	mean seconds	total seconds	n entries
InitialState	611513,727	413,727	680
PRTCdown	116,002623	78765,781	679
PRTCon	1210,127271	821676,417	679

Расчетный модуль комплекса производит построчное считывание данных из лог-файла и подготовку данных. Продолжительность нахождения системы в состояниях рассчитывается в секундах путем сравнения времени входа и выхода.

Вычисляются динамические параметры с последующей пакетной записью массива значений, включающего результаты и параметры вычислений, в базу данных. Использована реляционная база данных PostgreSQL.

На первоначальном этапе была предпринята попытка фиксировать результаты вычислений в файле Excel. Однако данный способ показал свою бесперспективность ввиду резкого снижения производительности с ростом объема данных при том, что одной из задач является моделирование в масштабе жизненного цикла системы (например, моделирование работы системы на дистанции в 1 год с шагом 1 секунда требует около 32 млн. строк). Причинами выбора PostgreSQL стали: открытая лицензия и бесплатное распространение, поддержка стандартных и хорошо задокументированных SQL-запросов и возможностью установки специального расширения TimescaleDB, которое позволяет значительно увеличить производительность при записи, считывании и анализе больших объемов данных временных рядов, что подробно описано в работах [22-24].

Для последующего расширения функционала имитационной модели, в том числе для имитации воздействия на эталонную ШВ и исследования реакции подсистемы автоподстройки частоты ведущих часов, процессы вычисления ШВ эталона и ШВ ведущих часов сделаны независимыми.

По причине постоянного уточнения требований, существенных трудозатрат на разработку и минимального вклада в достижение задач научного исследования решено приостановить разработку пользовательского интерфейса, сформировав лишь требования к нему.

Отметим, что каждому состоянию имитируемой системы соответствует своя логика расчета параметров шкалы времени. При этом основным ориентиром послужили определения параметров сигналов шкалы времени, данные в рекомендации ITU-T G.810 (08/96) «Definitions and terminology for synchronization networks». Использовано, например, уравнение модели временных отклонений (**1**) из раздела I.3 «Time error model» приложения I (Appendix I). Для каждой итерации расчета формируется строка в базе данных, содержащая входные и выходные значения, в том числе начальные значения задержек и текущие значения девиации частоты, шумовых составляющих, параметры фазы. Строки также содержат уникальный идентификатор, штамп времени (включая значение даты), значения текущей секунды, текущее состояние.

$$x(t) = x_0 + (y_0 - y_{0,ref})t + \frac{(D - D_{ref})}{2}t^2 + \frac{f(t) - f_{ref}(t)}{2\pi V_{nominal}} \quad (1)$$

где:

– x(t) – абсолютная задержка сигнала относительно эталонного значения; x0 – начальная постоянная задержка;

– $(y_0 - y_{0,ref})\cdot t$ – линейная составляющая отклонения, связанная с начальной частотой и смещением частоты относительно эталона;

– $((D - D_{ref})/2)t^2$ – квадратичный вклад задержки, связанный с ускорением фазы (частоты), обусловленный изменением частотной нестабильности;

– $(f(t) - f_{ref}(t))/2\pi V_{nominal}$ – периодический шум или регулярная составляющая, зависящая от текущего мгновенного изменения частоты f(t) относительно номинальной частоты ($V_{nominal}$).

В функционал комплекса входит визуализация расчетных данных. Модуль визуализации также реализован на Java. На рис. 3 и 4 представлены небольшой фрагмент базы данных, сформированной в результате работы расчетного модуля, и пример формируемых графиков.

4. Перспектива

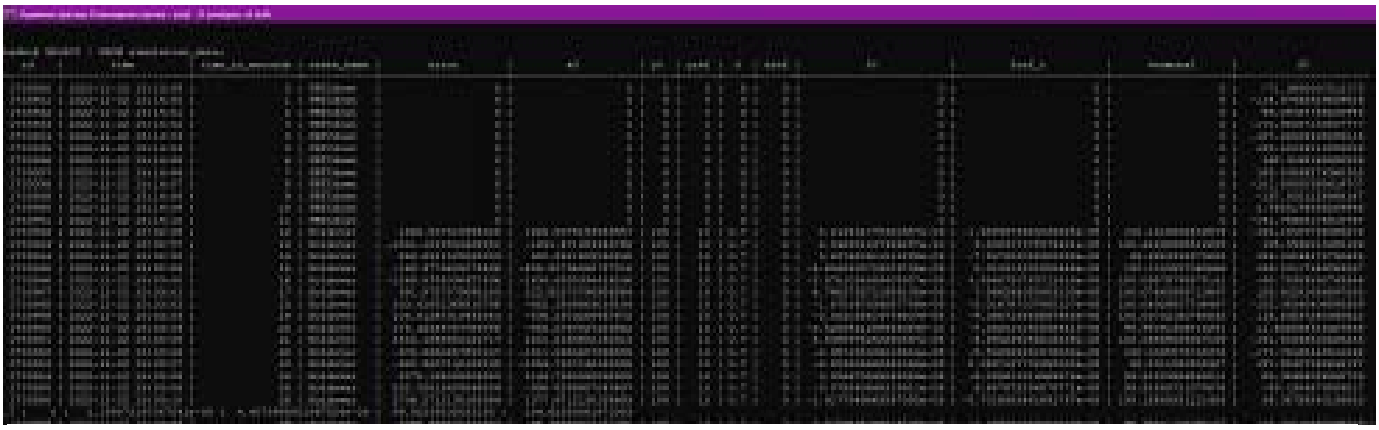


Рис. 3. Фрагмент сформированной базы данных

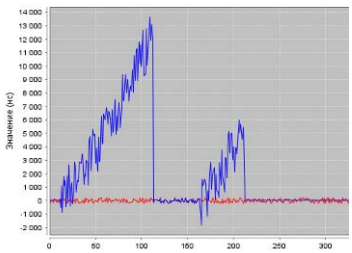


Рис. 4. Примеры формируемых графиков (сформированы в режиме отладки)

Важной задачей, выполняемой в рамках научной работы, является исследование перспективных КССОП. Сложность таких сетей заключается в том, что развитая КССОП может состоять из множества пространственно-разнесенных узлов, взаимосвязанных наземными ВОЛС. Их информационное взаимодействие основано на принципах формирования группового стандарта времени и частоты, формируемого каждым узлом КССОП на основе сигналов от внутренних и внешних источников.

Сейчас ведется работа по исследованию соответствующих математических алгоритмов и их программной реализации. Среди первоочередных задач:

– разработка имитационной модели сетевого элемента КССОП на основе представленного в данной работе структурно-функционального анализа;

– разработка полноценной модели когерентной сети, состоящей из нескольких сетевых элементов, применение существующих или разработка новых математических моделей, максимально точно имитирующих поведение подобных систем синхронизации;

– детальный анализ концепции когерентных сетей связи общего пользования, их перспективности и востребованности в будущем. Проведение экспериментов, направленных на исследование отказоустойчивости, обнаружение уязвимостей, исследование реакции системы на изменения структуры, в том числе топологии сети и количества узловых элементов;

– уточнение требований к когерентным сетям связи общего пользования, описание граничных условий для оценки параметров отказоустойчивости и, по возможности, формирование интегральных показателей такой оценки.

Выводы

В разработанной имитационной модели объединяются подходы к анализу функциональной и структурной устойчивости систем синхронизации шкал времени.

Основываясь на предыдущих результатах по имитационному моделированию, линии синхронизации разработан программный комплекс для расчета параметров, отражающих качество синхронизации и зависящих от состояния работоспособности системы, имитируемой в среде моделирования (на основе агентного моделирования). Комплекс обеспечивает автоматизацию процесса сбора данных из лог-файлов Excel, обработку, расчет и визуализацию в Java-приложении, интеграцию с системой хранения данных (свидетельство о регистрации программы для ЭВМ «Программный комплекс для имитационного моделирования систем синхронизации шкалы времени в сетях связи общего пользования» от 3 декабря 2025 года № 2025694023).

На текущий момент реальные возможности разработанного программного комплекса ограничены необходимостью внесения корректировок, однако уже сейчас имеется программная платформа, играющая роль лабораторного стенда для более детального исследования моделей систем синхронизации.

К главным задачам по улучшению имитационной модели можно отнести доработки, связанные с моделированием переходных процессов, неизбежно возникающих в реальных системах при смене состояний, разработка механизмов для исследования спуфинговых атак.

Стоит также отметить, что предпринятые меры по оптимизации работы комплекса позволили значительно снизить скорость проведения цикла операций от считывания лог-файла до записи в базу данных и визуализации.

Литература

1. *Zhong Minghan, Li Wenhao, Lu Minguan, Li Hong.* Feedback Node Aided Distributed Spoofing System for Global Navigation Satellite System Time Synchronisation Attack // IET Radar, Sonar & Navigation. 19. 2025. DOI: 10.1049/rsn2.70088.

2. *He Y., Zhuang X., Xu B.* Sparse Decomposition-Based Anti-Spoofing Framework for GNSS Receiver: Spoofing Detection, Classification, and Position Recovery // Remote Sens. 2025, 17, 2703. https://doi.org/10.3390/rs17152703.

3. *Radoš K., Brki´c M., Beguši´c D.* Recent Advances on Jamming and Spoofing Detection in GNSS // Sensors 2024, 24, 4210. https://doi.org/10.3390/s24134210

4. *Kriezis Argyris, Chen Yu-Hsuan, Akos Dennis, Lo Sherman, Walter Todd*. GNSS Jamming and Spoofing Monitoring Using Low-Cost COTS Receivers. 2025. 10.48550/arXiv.2509.13600.

5. *Zmysłowski Dariusz, Kryk Michał, Kelner Jan.* Testing GNSS receiver robustness for jamming // Aviation and Security 2023. Issues. 4, pp. 139-155. 10.55676/asi.v4i2.64.

6. *Ghanbarzade Ali, Soleimani Hossein*. GNSS/GPS Spoofing and Jamming Identification Using Machine Learning and Deep Learning. 2025. DOI: 10.48550/arXiv.2501.02352.

7. *Lubbers B*. GNSS Accuracy Under White Gaussian Noise Jamming // Eng. Proc. 2025, 88, 26. https://doi.org/10.3390/engproc2025088026

8. *Hussain Zawar, Majal Arslan, Chughtai Aamir, Nadeem Talha*. Dictionary-Based Contrastive Learning for GNSS Jamming Detection. 2025. DOI: 10.48550/arXiv.2512.07512.

9. *Рыжков А.В., Шварц М.Л*. Предпосылки создания когерентной сети связи общего пользования - основы сквозных цифровых технологий // T-Comm: Телекоммуникации и транспорт. 2021. Том 15. №7. С. 14-22. – DOI 10.36724/2072-8735-2021-15-7-14-22. – EDN HQBBNJ

10. *Лоховин В.А., Шварц М.Л., Рыжков А.В.* Перспективные направления развития систем связи и синхронизации сложных инфраструктурных объектов // T-Comm: Телекоммуникации и транспорт. 2024. Том 18. №11. С. 30-37. – DOI 10.36724/2072-8735-2024-18-11-30-37. – EDN UZQBNC.

11. *Lokhovin V. A., Schwartz M. L., Ryzhkov A. V., Aladin V. M*. Communication & Synchronization Systems of Complex Infrastructure Facilities. Directions for Future Development // 2024 Systems of Signal Synchronization, Generating and Processing in Telecommunications (SYNCHROINFO), Vyborg, Russian Federation, 2024, pp. 1-5, doi: 10.1109/SYNCHROINFO61835.2024.10617652.

12. МСЭ-Т G.8275 (01/2024), Architecture and requirements for packet-based time and phase distribution.

13. МСЭ-Т G.8272.2 (01/2024). Timing characteristics of coherent network primary reference time clocks.

14. *Глебов И. В., Митрюхин А. Д.* О функциональной надёжности регенерационных систем жизнеобеспечения пилотируемых космических аппаратов. // Инженерный журнал: наука и инновации, 2020, вып. 6. DOI: 10.18698/2308-6033-2020-6-1987

15. *Подкопаев А. В., Подкопаев И. А.* Централизованный адаптивный алгоритм оценки безопасности сложных технических систем различной энтропии // Надёжность и качество сложных систем. 2020. №3 (31). С. 20-27. DOI 10.21685/2307-4205-2020-3-3

16. *Антошина В. М., Якимов В. Л.* Описание статистики отказов конструктивных элементов многофункциональных радиолокационных станций по экспериментальным данным // Известия ТулГУ. Технические науки, 2018, вып. 12. С. 396-404.

17. *Киселев Ю.В., Мотиенко А.И., Басов О.О., Саитов И.А*. Структурно-функциональная модель интеллектуальной инфокоммуникационной системы // Научно-технический вестник информационных технологий, механики и оптики. 2018. Т. 18. № 6. С. 1034–1046. DOI: 10.17586/2226-1494-2018-18-6-1034-1046.

18. *Салухов В. И., Солдатенко В. С*. Структурно-функциональная модель и методика решения задачи обоснования модернизации телекоммуникационных систем // Труды СПИИРАН, 2015. № 6(43). С. 210-227. https://doi.org/10.15622/sp.43.12

19. *Dzaferagic Merim, Kaminski Nicholas, Macaluso Irene, Marchetti Nicola.* A Functional Complexity Framework for the Analysis of Telecommunication Networks // Journal of Complex Networks. 2016. 6. 10.1093/comnet/cny007.

20. *Lokhovin V. A., Schwartz M. L.* Simulation Modeling of Reference Time Scale Transmission Line // 2025 Systems of Signal Synchronization, Generating and Processing in Telecommunications (SYNCHROINFO), Tyumen, Russian Federation, 2025, pp. 1-6, DOI: 10.1109/SYNCHROINFO65403.2025.11079389.

21. *Vinay Kumar, Lalit Singh, Anil K.* Tripathi Reliability analysis of safety-critical and control systems: a state-of-the-art review IET Softw., 2018, Vol. 12 Iss. 1, pp. 1-18. The Institution of Engineering and Technology 2017 DOI: 10.1049/IET-SEN.2017.0053

22. *Иванова Е.В., Цымблер М.Л.* Обзор современных систем обработки временных рядов // Вестник ЮУрГУ. Серия: Вычислительная математика и информатика. 2020. Т. 9, № 4. С. 79-97. DOI: 10.14529/cmse200406.

23. *Grzesik P., Mrozek D*. Comparative analysis of time series databases in the context of Edge computing for low power sensor networks // Proceedings of the 20th International Conference on Computational Science, ICCS 2020 (Amsterdam, The Netherlands, June, 3-5, 2020). Part V. 2020, pp. 371-383. DOI: 10.1007/978-3-030-50426-7_28.

24. *Платонова А. И.* Сравнение производительности PostgreSQL и ее расширения TimescaleDB. Современные инновации, системы и технологии – Modern Innovations, Systems and Technologies, 2024, no. 4(3), pp. 0121-0133. https://doi.org/10.47813/2782-2818-2024-4-3-0121-0133

25. *Шварц М. Л., Богданов Е. А., Рыжков А. В., Аладин В. М*. Особенности построения систем единого и точного времени в сетях связи электроэнергетики // T-Comm: Телекоммуникации и транспорт. 2024. Т. 18, № 12. С. 27-33. DOI 10.36724/2072-8735-2024-18-12-27-33. EDN MLHRQT.

26. *Медведев С. Ю., Мишагин К. Г., Рыжков А. В.* и др. Формирование шкалы времени в когерентной сети связи общего пользования // T-Comm: Телекоммуникации и транспорт. 2023. Т. 17, № 12. С. 29-35. DOI 10.36724/2072-8735-2023-17-12-29-35. EDN DBWHRP.

РАЗРАБОТКА И ИССЛЕДОВАНИЕ SDN-МОДЕЛИ ПЕРЕДАЧИ МУЛЬТИСЕРВИСНОГО ТРАФИКА В LEO-СЕТЯХ СПУТНИКОВОЙ СВЯЗИ

Степанов Михаил Сергеевич
к.т.н., доцент кафедры ССиСК, МТУСИ, Москва, Россия
m.s.stepanov@mtuci.ru

Домингуш Санка Валтер
студент МТУСИ, Москва, Россия
sancawalter@gmail.com

Аннотация
Статья посвящена разработке и имитационному исследованию модели передачи мультисервисного трафика в низкоорбитальных спутниковых сетях связи (LEO). Актуальность обусловлена быстрым ростом созвездий LEO и необходимостью обеспечения гарантированного качества обслуживания (QoS) для сервисов, чувствительных к задержке. Цель работы – построение модели, учитывающей динамику топологии LEO (частые хэндоверы) и дифференцированное обслуживание четырех классов трафика: реального времени с жесткими (RT1) и мягкими (RT2) требованиями, интерактивного (INT) и фонового (BE). Модель основана на принципах программно-определяемых сетей (SDN), использовании приоритетных дисциплин обслуживания и механизмах управления очередями. Эффективность решений проверена с помощью дискретно-событийного имитационного моделирования в симуляторе ns-3 с последующей обработкой результатов в MATLAB. Показано, что по сравнению с базовой FIFO-схемой предложенный подход существенно снижает задержки и потери пакетов для трафика реального времени при различных уровнях нагрузки LEO-сети.

Ключевые слова
низкоорбитальная спутниковая сеть, LEO, мультисервисный трафик, QoS, SDN, handover, NS-3, FlowMonitor.

Введение

Современный мультисервисный сетевой трафик (голос, видео в реальном времени, стриминговые сервисы, облачные приложения, IoT и др. [9, 10]) требует от сетей связи гарантированного качества обслуживания даже при неравномерном распределении нагрузки. Спутниковые системы на низкой околоземной орбите (LEO) [1, 11, 12] рассматриваются как перспективная платформа для глобального широкополосного покрытия, интегрируемого в инфраструктуру 5G/6G, благодаря существенно меньшей задержке распространения сигнала по сравнению с геостационарными (GEO) спутниками. Так, время распространения сигнала в LEO (порядка нескольких миллисекунд в одну сторону) на порядок ниже, чем в GEO (~120 мс), что делает LEO-сети пригодными для интерактивных сервисов и облачных приложений. Однако снижение высоты орбиты достигается ценой высокой динамичности топологии: каждый LEO-спутник находится в зоне видимости наземного пользователя лишь считанные минуты, после чего связь должна быть передана следующему спутнику. В LEO-сетях хэндовер происходит регулярно (каждые несколько минут), затрагивая множество активных сеансов, что накладывает повышенные требования на устойчивость протоколов, алгоритмов маршрутизации и механизмов QoS. Существующие решения обеспечения QoS в спутниковых сетях и их интеграции с наземными (например, применение мультиканальных очередей, приоритизация, дублирование трафика) широко исследованы, однако динамичная природа LEO-констелляций требует новых подходов [2].

Одним из перспективных направлений развития спутниковых сетей является переход к централизованным SDN-архитектурам. Программно-определяемые сети позволяют отделить плоскость управления от плоскости передачи данных и на уровне контроллера получать глобальное представление о состоянии сети (топологии, нагрузке каналов, очередях). За счет этого открывается возможность оперативно адаптировать маршрутизацию и распределять ресурсы в соответствии с текущими условиями, что особенно важно при частых хэндовер и переменных условиях в LEO-сети. В сочетании с механизмами дифференцированного обслуживания (DiffServ) централизованное SDN-управление предоставляет гибкие средства поддержания требуемых параметров QoS для разных классов трафика даже в условиях быстро меняющейся топологии. В данной работе предложена SDN-ориентированная модель LEO-сети, реализующая классификацию и приоритизацию трафика по классам, динамическую маршрутизацию с учетом ограничений QoS и управление передачей при хэндовере. Ниже описаны используемые методы моделирования, архитектура и основные компоненты модели, а также приведены результаты имитационных экспериментов по оценке эффективности подходов [4].

Методы

Архитектура модели. Разрабатываемая модель LEO-сети включает две плоскости: плоскость данных содержит пользовательские узлы и узлы передачи, а плоскость управления представлена централизованным SDN-контроллером. В топологии модели выделены основные узлы: абонентский терминал UE, два низкоорбитальных спутника (Sat1, Sat2), наземный шлюз (GW) и сервер приложений (Server). Каждый узел плоскости данных работает как коммутатор с поддержкой IP-маршрутизации и многоочередной обработки трафика. SDN-контроллер соединен с узлами выделенным логическим каналом управления и обладает глобальной информацией о состоянии сети (положении спутников, загрузке каналов, очередях), что позволяет ему вычислять оптимальные маршруты и распределять ресурсы для поддержания QoS. В частности, контроллер обновляет правила маршрутизации при событиях хэндовер, заблаговременно переназначая потоки на новый маршрут и корректируя приоритеты, чтобы минимизировать влияние переключения спутника на критичные сервисы. Логическая топология фрагмента сети и взаимодействие компонентов представлены на рисунке 1.

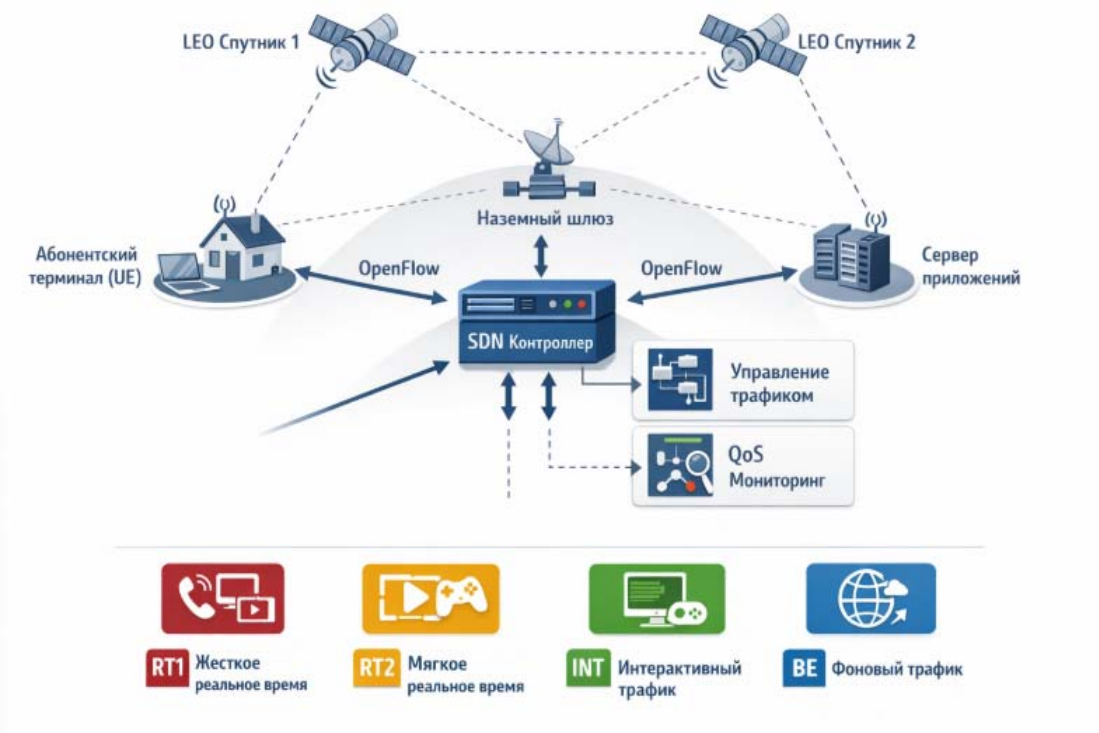


Рис. 1. Логическая топология фрагмента LEO-сети с SDN-контроллером и четырьмя классами трафика (RT1, RT2, INT, BE)

Механизмы QoS. Для обеспечения дифференцированного обслуживания трафик разделяется на четыре класса: RT1 – сервисы реального времени с жесткими требованиями по задержке (например, голос), RT2 – реальное время с умеренными требованиями (например, видео), INT – интерактивные сервисы (веб, транзакции) и BE – фоновые потоки без гарантий (best effort). На спутниковых узлах и шлюзе для каждого класса выделена отдельная очередь (многоканальная система очередей). Очередь класса RT1 обслуживается по строгому приоритету с минимальной задержкой (Low Latency Queue), очереди RT2 и INT имеют гарантированную долю пропускной способности (взвешенное круговое обслуживание, например Weighted Round Robin), а очередь BE обслуживается по остаточному принципу и оснащена механизмом активного управления буфером (RED/WRED). Все очереди подключены к общему планировщику, который выбирает пакеты согласно приоритетам и весам. Такая комбинация дисциплин соответствует DiffServ-модели и нацелена на снижение задержки и потерь для чувствительных классов за счет ограничения фонового трафика [3]. Подобный подход ранее зарекомендовал себя в наземных и спутниковых сетях для улучшения качества TCP-трафика с использованием механизма Differentiated Services. В нашей модели SDN-контроллер централизованно настраивает параметры очередей и планировщика на каждом узле (приоритеты, веса, лимиты буфера) в соответствии с политикой QoS. Это позволяет оперативно перераспределять ресурсы между классами при изменении нагрузки и предотвращать перегрузку высокоприоритетных очередей [5].

Имитационное моделирование. Для оценки эффективности предложенных решений разработан программный комплекс на базе сетевого симулятора ns-3. Данный дискретно-событийный симулятор поддерживает реалистичную модель протоколов IP, маршрутизацию, очереди и планировщики трафика, а также модуль FlowMonitor для сбора статистики QoS. В модели реализована указанная выше топология LEO-сети (UE – Sat1/Sat2 – GW – Server) с параметрами каналов, близкими к реальным: для радиолинии UE–Sat учтены задержка распространения (десятки миллисекунд) и ограниченная полоса пропускания, для каналов Sat–GW – типичные характеристики спутникового канала Земля–космос, для сегмента GW–Server – высокоскоростное наземное соединение с малой задержкой. SDN-контроллер заложен как отдельный логический объект, управляющий маршрутизацией трафика между узлами через интерфейсы управления. Генерация трафика выполняется встроенными приложениями ns-3: для каждого класса RT1, RT2, INT, BE создаются потоки с заданными интенсивностями и распределением пакетов (моделируются Poisson и самоподобные ON/OFF процессы для различного трафика). Метрики QoS (средняя end-to-end задержка, доля потерянных пакетов, средняя пропускная способность) по каждому трафик-потоку регистрируются с помощью FlowMonitor в ходе симуляции. Для обработки результатов используются Python-скрипты (парсинг XML-логов FlowMonitor и агрегирование статистики по классам в CSV-файлы) и пакет MATLAB – на этапе постобработки вычисляются усредненные показатели по каждому сценарию и строятся графики распределения задержек, потерь и throughput [6]. Последовательность конфигурации, сборки и запуска имитационной модели приведена на рисунке 2. Процедура формирования отчётов FlowMonitor и подготовки данных для последующей постобработки показана на рисунке 3.

Рис. 2. Компиляции и запуска имитационной модели в ns-3

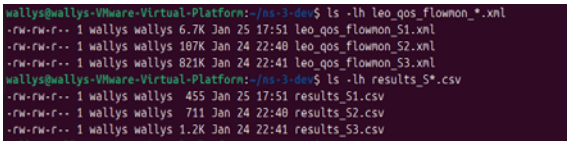


Рис. 3. Формирования отчётов FlowMonitor и подготовки данных для постобработки

Сценарии и эксперименты. Проведена серия экспериментов в трех характерных сценариях нагрузки. Сценарий S1 соответствует умеренной загрузке сети – суммарный битрейт всех потоков не превышает ~50% пропускной способности узких каналов, события хэндовер редки. Этот режим имитирует относительно благоприятную ситуацию для проверки базового распределения ресурсов между классами. Сценарий S2 – повышенная нагрузка: интенсивность интерактивного и фонового трафика возрастает, общее использование канала достигает 60–80% от пропускной способности. Здесь проверяется способность модели удерживать приемлемое QoS для RT-трафика при усилении фоновой нагрузки. Сценарий S3 – стрессовый режим: сеть работает близко к насыщению, канал UE–Sat загружен почти на 100%, а хэндовер происходят часто. Этот сценарий выявляет пределы устойчивости предложенного механизма при перегрузках. В каждом эксперименте имитация выполнялась в течение заданного времени (десятки секунд моделируемого времени); для S3 планировалось несколько событий хэндовер с интервалом в несколько секунд, тогда как для S1 – не более одного переключения за все время. По завершении каждого прогона фиксировались средние значения метрик QoS по каждому классу и сценарию. Кроме того, для проверки преимущества модели проведено сравнение с FIFO: для стрессового сценария S3 отдельно моделировалась работа сети при простой FIFO-дисциплине (одна общая очередь без приоритизации), чтобы сопоставить показатели задержки реального времени с предлагаемой схемой QoS [7].

Результаты

Результаты имитационного моделирования подтверждают эффективность предложенной модели дифференцированного обслуживания в LEO-сети. На умеренной нагрузке (S1) все классы трафика достигают невысоких задержек и пренебрежимо малых потерь. Критичные классы RT1 и RT2 имеют

минимальную среднюю задержку (<20–30 мс), интерактивный трафик INT – несколько выше, но в допустимых пределах, а фоновый BE использует оставшуюся полосу, практически не влияя на приоритетные потоки. При повышенной нагрузке (S2) наблюдается рост задержки и потерь для INT и BE, однако классы реального времени удерживают приемлемое качество: средняя задержка RT1 остается существенно ниже 100 мс, потери единичны. В стрессовом режиме (S3), когда суммарный трафик близок к пропускной способности канала, разработанная модель демонстрирует устойчивое поведение. Ухудшение QoS в первую очередь затрагивает наименее приоритетный трафик: задержка и процент потерь пакетов для класса BE резко возрастают, частично деградирует также INT, тогда как для трафика RT1/RT2 показатели остаются в допустимых пределах. Таким образом, при перегрузке сеть автоматически жертвует производительностью фоновых сервисов, сохраняя обслуживание критичных потоков реального времени на приемлемом уровне, что соответствует заданной политике приоритизации. Сопоставление средней задержки по классам трафика для сценариев S1–S3 приведено на рисунке 4. Оценка вероятности потерь по классам трафика для тех же сценариев представлена на рисунке 5.

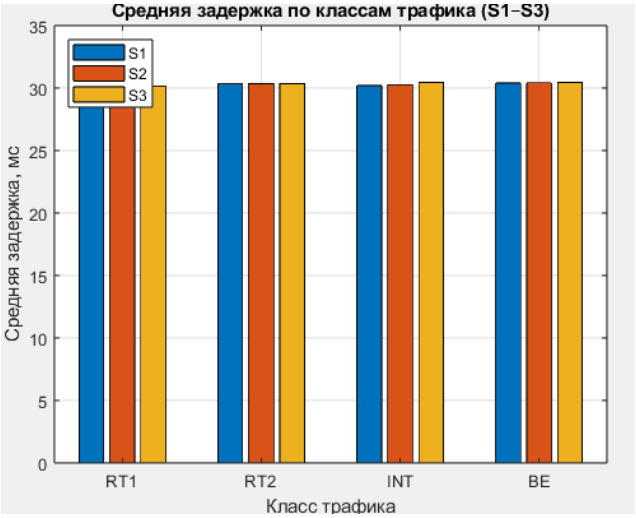


Рис. 4. Средняя задержка по классам трафика в сценариях S1-S3

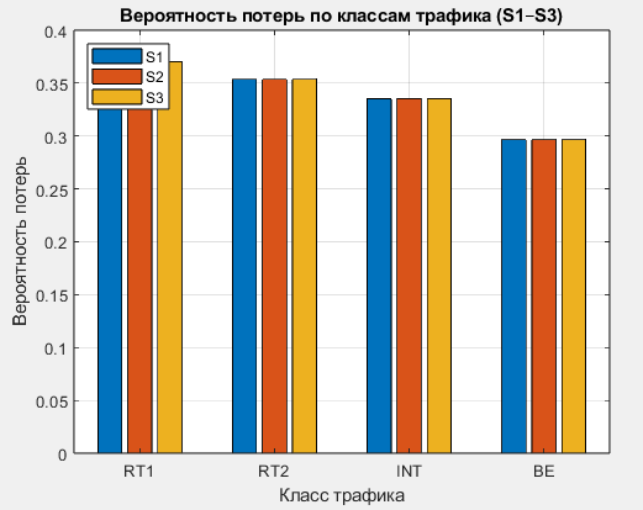


Рис. 5. Вероятность потерь по классам трафика в сценариях S1-S3

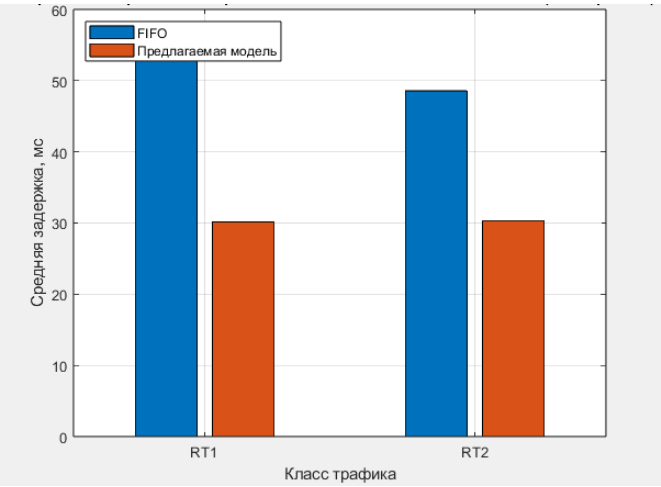


Рис. 6. Сравнение средней задержки RT1/RT2 для FIFO и предлагаемой модели (сценарий S3)

Ключевым результатом является заметное улучшение показателей RT-трафика по сравнению с отсутствием дифференциации (FIFO). В сравнительных экспериментах для сценария S3 средняя задержка пакетов класса RT1 в нашей модели оказалась значительно ниже, чем при FIFO-обслуживании (выигрыш составил десятки миллисекунд), для класса RT2 также зафиксировано уменьшение задержки, хотя и менее выраженное. Это наглядно иллюстрируется графиком на рисунок 6 : переход от FIFO к предлагаемой модели приводит к существенному снижению задержки высокоприоритетного трафика за счет введения приоритетной очереди и гарантированной доли ресурса. Вероятность потерь пакетов для RT1/RT2 при использовании QoS-модели также ниже, чем в FIFO-схеме, поскольку механизм очередей с приоритетом предотвращает вытеснение критичных пакетов из буфера при перегрузке. Общая пропускная способность канала при этом используется более эффективно: высокий приоритет не приводит к «простаиванию» ресурса, поскольку невостребованная полоса отдаётся менее приоритетным классам. В совокупности данные показывают, что SDN-управление с дифференцированными очередями позволяет достичь требуемого QoS для важных сервисов без выделения избыточных резервов пропускной способности.

Дополнительные эксперименты исследовали влияние хэндовер на параметры трафика. В моменты переключения обслуживающего спутника наблюдались кратковременные всплески задержки для затронутых потоков (в основном RT2 из-за перенастройки маршрута) и снижение throughput для некоторых BE-пакетов, однако за счет проактивного управления на уровне контроллера эти эффекты быстро затухали и не приводили к длительной деградации качества. Диаграммы временных рядов показали, что после события хэндовер задержка возвращается к стабильному уровню в пределах нескольких десятков миллисекунд, подтверждая корректность заложенного механизма переназначения потоков. Таким образом, даже при частых хэндовер (сценарий S3) предложенная архитектура сохраняет преимущества дифференцированного обслуживания.

Заключение

В работе представлена SDN-ориентированная модель передачи мультисервисного трафика для низкоорбитальных спутниковых сетей, включающая централизованное управление маршрутизацией и QoS с классификацией трафика на четыре класса. Разработан программно-имитационный комплекс на базе ns-3 и MATLAB, реализующий предложенную архитектуру и позволяющий проводить серии экспериментов в воспроизводимых сценариях нагрузки. Имитационное исследование подтвердило, что сочетание дифференцированных очередей (LLQ, WRR/CBWFQ, RED) и глобального SDN-управления эффективно решает проблему обеспечения QoS в LEO-сети с динамичной топологией. По сравнению с традиционной FIFO-схемой, модель обеспечивает явное преимущество для трафика реального времени: при росте нагрузки и появлении частых хэндовер задержки и потери для классов RT1/RT2 остаются существенно ниже, чем для INT/BE, а суммарная пропускная способность канала используется более рационально. Перегрузка в первую очередь сказывается на фоновых сервисах, тогда как критичные потоки сохраняют приемлемое качество обслуживания – это соответствует целям приоритизации и подтверждает работоспособность выбранных алгоритмов.

Таким образом, предложенная модель позволяет адекватно описывать процессы передачи мультисервисного трафика в LEO-сети и обеспечивать требуемый уровень QoS за счет комбинации

дифференцированной обработки пакетов и учета динамики спутниковой инфраструктуры. Полученные результаты могут быть использованы при проектировании спутниковых систем нового поколения, интегрированных с наземными сетями, а также послужить основой для дальнейшего развития модели. В частности, перспективами продолжения работы являются углубленное исследование алгоритмов многокритериальной QoS-маршрутизации и адаптивного управления ресурсами в LEO-сетях на базе предложенного подхода.

Литература

1. *Kodheli O., Lagunas E., Maturo N.* et al. Satellite communications in the new space era: A survey and future challenges // IEEE Commun. Surveys & Tutorials. 2021. Vol. 23, No 1, pp. 70-109.

2. *Niephaus C., Kretschmer M., Ghinea G.* QoS provisioning in converged satellite and terrestrial networks: a survey of the state-of-the-art // IEEE Commun. Surveys & Tutorials. 2016. Vol. 18, No 4, pp. 2415-2441.

3. *Durresi A., Kota S., Goyal M.* et al. Achieving QoS for TCP traffic in satellite networks with differentiated services. NASA Technical Report 20050019511, 2001.

4. *Chowdhury P.K., Atiquzzaman M., Ivancic W.* Handover schemes in satellite networks: state-of-the-art and future research directions // IEEE Commun. Surveys & Tutorials. 2006. Vol. 8, No 4, pp. 2-14.

5. *Rizvi M.E.K*. QoS Provisioning for Multi-Class Traffic in Wireless Networks: PhD Thesis. Norfolk, VA: Old Dominion Univ., 2004.

6. *Leland W.E.* et al. On the Self-Similar Nature of Ethernet Traffic // IEEE/ACM Trans. on Networking. 1994. Vol. 2, No. 1, pp. 1-15.

7. *Li Y., Liu L., Li H.* et al. Stable Hierarchical Routing for Operational LEO Networks // Proceedings of the 30th Annual International Conference on Mobile Computing and Networking (ACM MobiCom '24). New York, NY, USA: Association for Computing Machinery, 2024, pp. 296-311. DOI: 10.1145/3636534.3649362.

8. *Durresi A.* et al. Achieving QoS for TCP Traffic in Satellite Networks with Differentiated Services. NASA Tech. Rep. 20050019511, 2001.

9. *Степанов М. С., Давуд Т., Степанов С. Н.* Преодоление барьеров внедрения AR/VR в образовании // Методические вопросы преподавания инфокоммуникаций в высшей школе. 2025. Т. 14, № 4. С. 45-50. EDN UJAWHJ.

10. *Давуд Т., Степанов М. С., Степанов С. Н*. Сравнительный анализ технологий дополненной и виртуальной реальности (AR/VR) при использовании в современных образовательных процессах // Методические вопросы преподавания инфокоммуникаций в высшей школе. 2025. Т. 14, № 4. С. 51-56. EDN SXQPFI.

11. *Dawood T., Stepanov M. S*. Cellular internet of things modeling: the literature review // T-Comm: Телекоммуникации и транспорт. 2024. Vol. 18, No. 8, pp. 68-76. DOI 10.36724/2072-8735-2024-18-8-68-76. EDN EWAXDW.

12. *Маслов А. А., Себекин Г. В., Степанов М. С.* и др. Моделирование процессов обслуживания трафика реального времени в мультисервисных широкополосных сетях спутниковой связи на базе космических аппаратов на низких и средних круговых орбитах // T-Comm: Телекоммуникации и транспорт. 2025. Т. 19, № 12. С. 4-15. DOI 10.36724/2072-8735-2025-19-12-4-15. EDN DVDQIJ.

РЕШЕНИЕ ЗАДАЧИ ПРОГНОЗИРОВАНИЯ ОТКАЗОВ В ВЕДОМСТВЕННЫХ СЕТЯХ СВЯЗИ

Фатхулин Тимур Джалилевич
Московский технический университет связи и информатики, доцент кафедры ИАД, к.т.н., Москва, Россия
t.d.fatkhulin@mtuci.ru

Сазыкин Сергей Владимирович
Московский технический университет связи и информатики, студентка группы МБД2332, Москва, Россия

Сахарова Анастасия Михайловна
Московский технический университет связи и информатики, студентка группы БФИ2202, Москва, Россия

Рулев Денис Владиславович
Московский технический университет связи и информатики, студент группы БСТ2201, Москва, Россия

Аннотация
В работе проведено исследование методов прогнозирования отказов в ведомственных сетях связи. Цель работы – определение наиболее эффективного метода прогнозирования отказов в сетях связи такого типа. Актуальность работы обусловлена тем, что рост сложности сетевой архитектуры при одновременной гетерогенности каналов передачи, протокольных стеков и сервисных уровней увеличивает долю ситуаций, где отказ проявляется через комбинацию событий и телеметрии, а обнаружение ранних признаков требует анализа многомерных временных рядов и журналов событий.

Ключевые слова
Метод, алгоритм, машинное обучение, метрика, эффективность, показатель, сеть связи

Введение

Ведомственные сети связи обеспечивают обмен информацией внутри органов государственного управления, силовых структур и организаций критической инфраструктуры, поэтому требования к непрерывности обслуживания, контролю доступа и устойчивости к отказам формируют задачу прогнозирования инцидентов как прикладную задачу информационных технологий [5, 15].

Практика эксплуатации показывает, что ручной анализ сигналов мониторинга и постфактум разбор аварийных случаев приводит к запаздыванию управляющих воздействий и к перерасходу ресурсов сопровождения, поэтому внедрение методов машинного обучения для прогнозирования отказов рассматривается как средство повышения оперативности реагирования и снижения масштаба последствий [12, 16-19].

Постановка задачи прогнозирования отказов в ведомственной сети связи сводится к построению модели машинного обучения, которая по совокупности признаков, сформированных из журналов и описаний объектов сети, относит наблюдение к одному из 3 уровней fault_severity, при этом основной интерес представляет корректное распознавание редкого уровня 2 на фоне доминирования уровня 0 [15].

Выбор датасета для исследования

Выбор датасета Telstra Recruiting Network [1, 2, 4] задает формат исходных данных, где сведения распределены между основной таблицей train и четырьмя вспомогательными таблицами, поэтому корректная интерпретация задачи требует явного описания связей по id и анализа плотности записей в каждом источнике. Практическая специфика задачи определяется тем, что один объект идентифицируется единственным id в train, однако получает множественные описания через события, ресурсы, уровни серьезности и логовые признаки, поэтому дальнейшие эксперименты по алгоритмам опираются на агрегированное представление на уровне id [1].

Состав датасета и размерности таблиц по результатам Python-анализа представлены в таблице 1.

Таблица 1

Состав датасета

Таблица	Размерность	Столбцы
train	(7381, 3)	id, location, fault_severity
event_type	(31170, 2)	id, event_type
log_feature	(58671, 3)	id, log_feature, volume
resource_type	(21076, 2)	id, resource_type
severity_type	(18552, 2)	id, severity_type

Данные таблицы 1 показывают распределение информации по нескольким источникам. Таблица train содержит минимальный набор идентификационных и целевых полей, а основная часть полезных данных размещена во вспомогательных таблицах, где для одного id может быть много связанных строк.

Размер таблиц log_feature и event_type говорит о высокой активности событий. Поэтому если напрямую соединять все таблицы по id, число строк резко увеличивается, и структура данных разрушается. В этом случае правильнее использовать свёртку и объединение данных на уровне id.

Особого внимания требует таблица severity_type с размером (18552, 2). Количество строк здесь близко к общему числу идентификаторов, поэтому признаки, основанные на severity_type и статистике логов, стоит вычислять для всего набора id, а потом применять к обучающей выборке train, не меняя исходное распределение данных.

Характеристика таблицы train, полученная при анализе в Python, показывает отсутствие пропусков по всем трём столбцам и уточняет тип данных [6, 14]: id и fault_severity – целые числа, а location – строковая метка формата location N. Для алгоритмов машинного обучения колонку location нужно перевести в числовой вид с помощью кодирования. Диапазон id в train – от 1 до 18550, а целевой признак fault_severity принимает значения 0, 1 и 2, что делает задачу многоклассовой классификацией с упорядоченными уровнями серьёзности.

Распределение целевой переменной неравномерное, поэтому ещё на этапе описания данных становится ясно, что при обучении нужно учитывать редкие случаи. Пример первых строк таблицы train, полученный в Python (табл. 2), подтверждает формат идентификаторов, обозначение локаций и показывает, что в данных присутствуют все три уровня fault_severity.

Таблица 2

Пример первых строк таблицы «train»

fault_severity	Число наблюдений	Доля от train, %
0	4784	64.82
1	1871	25.35
2	726	9.84
Итого	7381	100.00

По данным таблицы 2 видно, что уровень 0 занимает 64.82% выборки и является основным, тогда как уровень 2 встречается лишь в 9.84% случаев. Поэтому, если оптимизировать модель только по общей точности, возникает риск смещения в сторону самого частого класса и снижения способности модели находить редкие, но важные случаи отказов.

Доля уровня 1 равна 25.35% и формирует промежуточный класс, который влияет на стабильность границ между уровнями 0 и 2. Ошибки между соседними уровнями происходят чаще, поэтому важно подбирать признаки и методы обучения, устойчивые к такому перекосу.

Распределение данных также показывает, что при проверке модели стоит использовать стратифицированное разделение. Без него возможны фолды, не отражающие реальные пропорции классов, что приведёт к искажённой оценке точности для уровня 2.

Сравнительный анализ эффективности современных алгоритмов машинного обучения

Сравнительный анализ алгоритмов машинного обучения для прогнозирования отказов в ведомственных сетях связи опирается на структуру выборки Telstra, где целевая переменная fault_severity принимает 3 значения, а распределение классов задается реальными частотами 4784, 1871, 726 при общем объеме train 7381.

Наличие связанной событийной и ресурсной информации, представленной отдельными таблицами event_type, log_feature, resource_type, severity_type, требует сопоставления алгоритмов не только по итоговым метрикам, но и по устойчивости к разреженным признакам, чувствительности к дисбалансу и способности корректно интерпретировать редкий класс 2. Процедура сравнения строится на единых правилах формирования признаков, одинаковых разбиениях выборки и одинаковом наборе метрик, поскольку любые вариации протокола обучения создают некорректные различия между моделями.

Сопоставление алгоритмов в данных условиях ориентируется на практическую пригодность к задаче прогнозирования отказов, где наибольшую ценность несет корректное обнаружение класса 2 при сохранении приемлемой точности по классам 0 и 1 (табл. 3).

Таблица 3

Метрики, применяемые в исследовании

Метрика	**Уровень расчета**	**Назначение в задаче**	**Чувствительность к дисбалансу**	**Риск искажения при доминировании класса 0**
Accuracy	выборка	контроль общей доли верных ответов	высокая	высокий
Macro F1	класс, усреднение	баланс качества по всем классам	низкая	низкий
Recall по классу 2	класс	контроль пропусков тяжелых отказов	низкая	низкий
Precision по классу 2	класс	контроль ложных тревог тяжелых отказов	средняя	средний
Log loss	выборка	контроль качества вероятностных прогнозов	низкая	низкий

Разбиение выполняется однократно по схеме train/test 80/20 со стратификацией по fault_severity, поэтому доли классов 0, 1, 2 сохраняются в обеих частях и сравнение алгоритмов опирается на сопоставимый состав наблюдений, включая редкий класс 2. Масштабирование MaxAbs применяется только для логистической регрессии, поскольку линейная оптимизация чувствительна к диапазонам признаков, тогда как Random Forest и XGBoost сохраняют устойчивость к масштабу и обучаются на немасштабированных значениях агрегированных объемов log_feature и бинарных индикаторов событий и ресурсов [3, 7-11, 13].

Визуальная интерпретация различий между моделями представлена на рисунке 1, где представлены значения ключевых метрик на тестовой выборке.

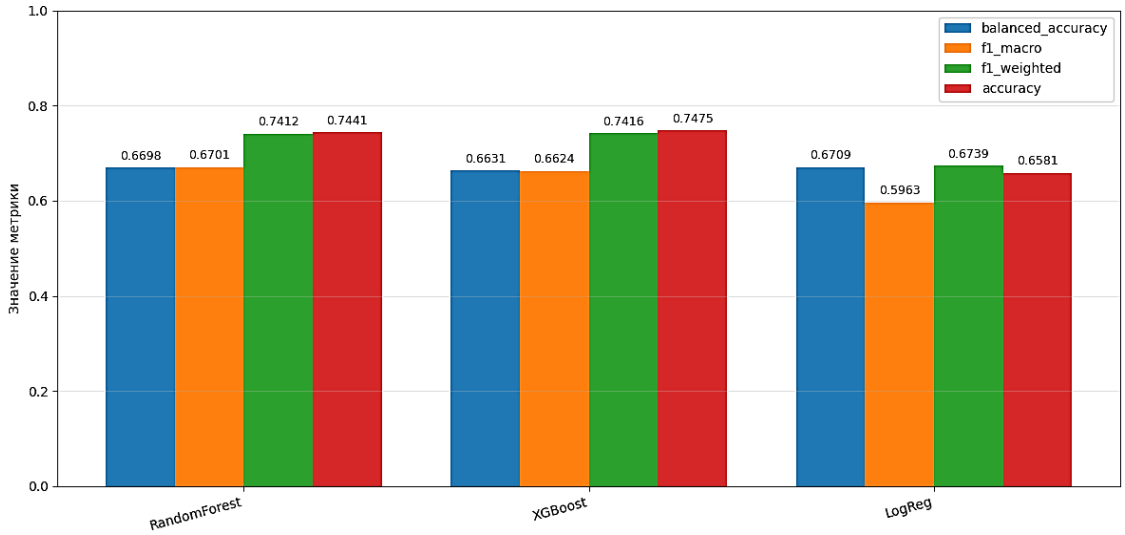


Рис. 1. Сравнение LogReg, RandomForest и XGBoost по метрикам на тестовой выборке Telstra Recruiting Network

Сопоставление по balanced_accuracy и f1_macro используется как основной критерий качества при дисбалансе, поскольку доминирование класса 0 способно завышать accuracy и f1_weighted, а эксплуатационное применение требует сохранения качества по классам 1 и 2 при минимизации пропусков тяжелых событий.

Интерпретация logloss в таблице 2.10 дополняет анализ, поскольку задача прогнозирования отказов в ведомственной сети связи предполагает дальнейшее использование вероятностей для ранжирования инцидентов и настройки порогов реагирования, а некорректная калибровка снижает устойчивость решений при изменении профиля локаций. Качественная структура ошибок раскрывается через матрицы ошибок на рисунке 2.

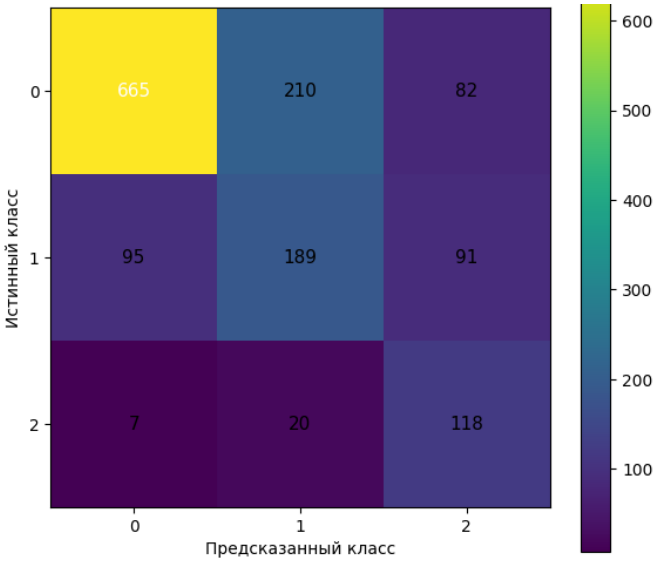


Рис. 2. Матрица ошибок классификации для модели LogReg на тестовой выборке Telstra Recruiting Network

Выбор базового алгоритма для дальнейшего совершенствования

Выбор базового алгоритма для последующего совершенствования выполняется на основании совокупности полученных оценок качества и устойчивости, а также на основании технологической пригодности модели к расширению признакового пространства и к внедрению дополнительных механизмов контроля дисбаланса.

Прикладной характер задачи прогнозирования отказов в ведомственной сети связи задает приоритет корректному выделению редких и тяжелых состояний при сохранении приемлемого уровня ложных срабатываний, поэтому модель рассматривается как элемент эксплуатационной цепочки поддержки решений, а не как средство формального достижения высокой общей точности. Дополнительным ограничением выступает необходимость интерпретируемого управления поведением модели при изменении режимов сети,

когда политика реагирования опирается на вероятностные оценки и на стабильность ранжирования инцидентов.

Кандидатные модели оцениваются по нескольким независимым группам критериев, среди которых выделяются качество многоклассовой классификации при дисбалансе, устойчивость при вариации обучающей подвыборки, пригодность вероятностных выходов для пороговых решений, а также вычислительная реализуемость в режиме регулярного дообучения и оперативного прогнозирования.

Линейная модель рассматривается как ориентир по скорости и простоте внедрения, однако ограниченная выразительная способность при разреженном представлении признаков приводит к слабой способности моделировать сложные сочетания событий и ресурсов. Ансамбль bagging обеспечивает конкурентное качество за счет нелинейности, однако управляемость процедуры обучения и тонкая настройка баланса ошибок для редкого класса требуют существенно более трудоемких приемов, а вариативность результатов при изменении обучающих данных затрудняет эксплуатационное сопровождение. Градиентный бустинг по деревьям демонстрирует наилучшее сочетание качества и управляемости, поскольку допускает целенаправленную регуляризацию, контролируемую сложность деревьев, настройку темпа обучения и механизмы адаптации к дисбалансу без разрушения базового пайплайна подготовки данных.

Критерии выбора базового алгоритма для последующей модификации и ожидаемые направления улучшений представлены в таблице 4.

Таблица 4

Критерии выбора базового алгоритма для последующей модификации

Критерий выбора	**Требование прикладной эксплуатации в ведомственной сети связи**	**Диагностический признак по результатам сравнения**	**Направление улучшения**
Устойчивость качества при дисбалансе классов	Сохранение качества по редким состояниям при доминировании штатных случаев	Сохранение высоких значений макро усредненных метрик при сопоставимых разбиениях	Взвешивание классов, корректировка функции потерь, настройка порогов вероятности
Стабильность при изменении обучающей подвыборки	Предсказуемое поведение модели при смене состава наблюдений и локаций	Низкая вариативность оценок по фолдам при повторяемых экспериментах	Регуляризация, ограничение глубины, контроль темпа обучения, ранняя остановка через callback
Пригодность вероятностных выходов	Использование вероятностей для ранжирования инцидентов и пороговых политик реагирования	Низкие значения логарифмической потери и корректная дифференциация классов	Калибровка вероятностей, настройка objective, отбор признаков, устранение шумовых индикаторов
Масштабируемость обучения и прогнозирования	Возможность периодического переобучения без чрезмерных затрат времени	Приемлемое время обучения и предсказания на фиксированной матрице признаков	Оптимизация параметров, снижение размерности через отбор,

Решение о выборе базового алгоритма принято в пользу XGBoost, так как градиентный бустинг по деревьям объединяет высокую точность, гибкость настройки и поддержку функций, важных для задач с дисбалансом классов. Возможности регуляризации и ограничения глубины деревьев помогают уменьшить переобучение, сохраняя чувствительность к слабым зависимостям, которые возникают при редких сочетаниях событий и ресурсов, характерных для серьёзных отказов.

Поддержка механизмов callback и встроенных инструментов контроля метрик делает процесс обучения воспроизводимым и облегчает переход к расширенной схеме, где можно улучшать качество признаков и уточнять модель по практическим критериям. Преимущество выбранного подхода также заключается в том, что добавление новых признаков или изменение функции потерь не требует пересмотра основного процесса подготовки данных. Это позволяет напрямую сравнивать базовую и улучшенную версии модели при одинаковых условиях обучения и оценки.

Заключение

Проведенное исследование современных алгоритмов машинного обучения для прогнозирования отказов в сетях связи позволило уточнить практическую постановку задачи и зафиксировать требования к корректному сравнению методов на данных Telstra, где целевая переменная задает многоклассовую структуру, а исходная информация распределена по нескольким взаимосвязанным таблицам, отражающим событийные, ресурсные и телеметрические признаки состояния объекта.

Анализ структуры исходных данных подтвердил необходимость перехода от реляционного представления к единой матрице признаков на уровне идентификатора, поскольку только такое представление обеспечивает сопоставимость экспериментов, воспроизводимость протокола обучения и возможность формализовать единые правила контроля утечек информации при построении моделей.

Литература

1. *John D. Kelleher*, Deep Learning. The MIT Press Essential Knowledge series, MIT Press, 2019.

2. *Simon J.D. Prince*, Understanding Deep Learning. MIT Press, 2023.

3. *Фатхулин Т. Д., Юдин А. Д.* Методики оптимизации загрузки изображений в web-приложениях // Труды Северо-Кавказского филиала Московского технического университета связи и информатики. 2025. № 1. С. 105-110. EDN TXTWFG.

4. *Фатхулин Т. Д., Фатхулина Г. Г., Рахматова А. А.* Интеграция технологии больших языковых моделей в образовательный процесс высшей школы // Труды Северо-Кавказского филиала Московского технического университета связи и информатики. 2025. № 2. С. 107-110. EDN FOGQPZ.

5. *Киреев А. А., Фатхулин Т. Д.* Анализ средств автоматизированного выбора конфигурации сети // Труды Северо-Кавказского филиала Московского технического университета связи и информатики. 2025. № 1. С. 15-19. EDN ETSHKC.

6. *Фатхули Т. Д., Чепенко К. А.* Анализ технологий обнаружения дефектов фасадов зданий // Труды Северо-Кавказского филиала Московского технического университета связи и информатики. 2025. № 1. С. 78-82. EDN BYMEPU.

7. *Леохин, Ю. Л., Фатхулин Т. Д., Кожанов М. С.* Анализ и исследование применения нейросетевых технологий для генерации программного кода // Вестник Рязанского государственного радиотехнического университета. 2024. № 87. С. 41-53. DOI 10.21667/1995-4565-2024-87-41-53. EDN HKEOFX.

8. *Леохин Ю. Л., Фатхулин Т. Д., Ментус М. В*. Разработка и применение методов распознавания зашумленных аудиофайлов посредством нейросетевых технологий // Вестник Рязанского государственного радиотехнического университета. 2024. № 88. С. 65-73. DOI 10.21667/1995-4565-2024-88-65-73. EDN NMXASI.

9. *Мяличева А. А., Фатхулин Т. Д.* Анализ методов машинного обучения для прогнозирования дефектов в исходном коде // Труды Северо-Кавказского филиала Московского технического университета связи и информатики. 2024. № 2. С. 16-19. EDN IVJCZF.

10. *Маслов К. В., Фатхулин Т. Д., Иванов Д. А*. Анализ технологий автоматизации бизнес-процессов и разработки программного обеспечения с использованием low-code платформ // Труды Северо-Кавказского филиала Московского технического университета связи и информатики. 2024. № 1. С. 6-11. EDN HDBOYM.

11. *Фатхулин Т. Д., Исаев А. В*. Анализ моделей arima и lstm, используемых для прогнозирования криптовалют и определения портфеля инвестиций // Труды Северо-Кавказского филиала Московского технического университета связи и информатики. 2024. № 2. С. 20-25. EDN ODWOPA.

12. *Леохин Ю. Л., Фатхулин Т. Д.* Разработка методов и алгоритма формализации текстового запроса к онлайн-сервисам, генерирующим изображения посредством нейросетевых технологий // Вестник Рязанского государственного радиотехнического университета. 2023. № 85. С. 82-95. DOI 10.21667/1995-4565-2023-85-82-95. EDN PZWYZV.

13. *Фатхулин Т. Д., Лушин Е. А*. Анализ развития автоматической генерации кода для web-сервисов // Труды Северо-Кавказского филиала Московского технического университета связи и информатики. 2023. № 1. С. 128-132. EDN JUEGXP.

14. *Митрофанов А. О., Степанов М. Н., Фатхулин Т. Д.* Анализ нейросетевых методов генерации изображения по текстовому запросу // Труды Северо-Кавказского филиала Московского технического университета связи и информатики. 2022. № 1. С. 19-23. EDN CWRLQA.

15. *Фатхулин Т. Д., Хорикова С. Г., Щитов В. М.* Анализ ключевых особенностей технологии программно-конфигурируемых оптических сетей (SDON) // Труды Северо-Кавказского филиала Московского технического университета связи и информатики. 2021. № 1. С. 29-34. EDN SMTDAF.

16. *Леохин Ю. Л., Дымкова С. С., Фатхулин Т. Д*. Методы машинного обучения в прикладных задачах прогнозирования динамично изменяющихся данных // T-Comm: Телекоммуникации и транспорт. 2025. Т. 19, № 8. С. 49-63. DOI 10.36724/2072-8735-2025-19-8-49-63. EDN ULVCHG.

17. *Леохин Ю. Л., Фатхулин Т. Д., Занегин А. В*. Модификация метода градиентного усиления для прогнозирования спроса на отдельные виды товаров // Наукоемкие технологии в космических исследованиях Земли. 2025. Т. 17, № 2. С. 32-41. DOI 10.36724/2409-5419-2025-17-2-32-41. EDN PNUPKY.

18. *Леохин Ю. Л., Фатхулин Т. Д., Маслов К. В*. Разработка методов системного анализа бизнес-процессов в банковской сфере для принятия решений о кредитовании различных организаций // Наукоемкие технологии в космических исследованиях Земли. 2025. Т. 17, № 5. С. 59-71. DOI 10.36724/2409-5419-2025-17-5-59-71. EDN VXBFTH.

19. *Леохин Ю. Л., Дымкова С. С., Фатхулин Т. Д., Зозуля И. С.* Методы и алгоритмы интеллектуальной поддержки принятия управленческих решений в организационных системах торговых компаний // T-Comm: Телекоммуникации и транспорт. 2025. Т. 19, № 12. С. 44-50. DOI 10.36724/2072-8735-2025-19-12-44-50. EDN XXFTQJ.