УДК 004.738.2:621.396.2

Лебедев Иван Владимирович

Аспирант первого курса, кафедры отечественные сети магистральной связи, факультет сети и системы связи

Московский технический университет связи и информатики, 111024, РФ, г. Москва, ул. Авиамоторная, д. 8А

АРХИТЕКТУРНЫЕ ПРИНЦИПЫ ПОСТРОЕНИЯ АДАПТИВНОЙ ГИБРИДНОЙ СИСТЕМЫ СВЯЗИ ДЛЯ КОМПЛЕКСОВ ЭКСТРЕННОГО ОПОВЕЩЕНИЯ НАСЕЛЕНИЯ

Аннотация

Статья посвящена исследованию архитектурных принципов построения адаптивных гибридных систем связи, ориентированных на применение в комплексах экстренного оповещения населения при чрезвычайных ситуациях. Актуальность исследования определяется системными недостатками существующих решений, при которых статическая конфигурация каналов связи не позволяет обеспечить требуемые показатели надёжности и оперативности в условиях деградации инфраструктуры. Предложена трёхуровневая модульная архитектура, включающая уровень физических каналов, уровень интеллектуального управления и уровень прикладных сервисов оповещения. Рассмотрены принципы гетерогенного резервирования с минимизацией корреляции отказов, механизмы мониторинга качества обслуживания и алгоритм взвешенного ранжирования каналов. Обоснованы требования к отказоустойчивости, кибербезопасности и масштабируемости системы. Сформулированы направления развития архитектуры в части интеграции с технологиями 5G/6G и сетями IoT.

Ключевые слова: гибридная система связи, экстренное оповещение населения, адаптивное управление каналами, КСЭОН,

качество обслуживания, резервирование, отказоустойчивость, Cell Broadcast, ВОЛС.

Annotation

The article examines the architectural principles for constructing adaptive hybrid communication systems intended for use in emergency public notification complexes during emergency situations. The relevance of the study is determined by systemic shortcomings of existing solutions, where static channel configurations fail to provide the required reliability and operational timeliness under infrastructure degradation conditions. A three-level modular architecture is proposed, comprising a physical channel layer, an intelligent control layer, and an application services layer for notifications. The principles of heterogeneous redundancy with failure correlation minimization, quality-of-service monitoring mechanisms, and a weighted channel ranking algorithm are examined. Requirements for fault tolerance, cybersecurity, and system scalability are justified. Directions for architectural development in terms of integration with 5G/6G technologies and IoT networks are formulated.

Keywords: hybrid communication system, emergency public notification, adaptive channel management, CCEP, quality of service, redundancy, fault tolerance, Cell Broadcast, fiber-optic lines.

Цель исследования – установить и обосновать архитектурные принципы построения адаптивной гибридной системы связи для комплексов экстренного оповещения населения при чрезвычайных ситуациях.

Проблема исследования состоит в том, что обеспечение гарантированного доведения сигнала оповещения до населения в условиях чрезвычайной ситуации является первоочерёдной задачей

национальной безопасности. Вместе с тем практика показывает, что в момент наступления кризисного события физическая инфраструктура связи оказывается под наибольшей нагрузкой или частично выводится из строя именно тогда, когда её роль наиболее критична. Традиционные подходы к построению систем оповещения, опирающиеся на статически заданную конфигурацию приоритетного и резервного каналов, не отвечают этому вызову в полной мере. Переключение по факту обнаруженного отказа неизбежно порождает временной разрыв, несовместимый с требованиями к оперативности, закреплёнными, в частности, в Постановлении Правительства РФ № 1074 [1, 2].

Таким образом, возникает необходимость перехода от реактивной к проактивной парадигме управления каналами связи. Такой переход требует не только новых алгоритмических решений, но и пересмотра самой архитектуры системы — её структурной организации, состава модулей и принципов их взаимодействия. Отсутствие системного описания подобной архитектуры применительно к задачам Комплексной системы экстренного оповещения населения (КСЭОН) и определяет актуальность настоящего исследования [3, 4].

Анализ требований и ограничений к архитектуре системы.

Исходным пунктом для формирования архитектурных принципов служит анализ нормативно закреплённых и технически обусловленных требований к системе. Ключевым нормативным ориентиром выступают Федеральный закон № 68-ФЗ «О защите населения и территорий от чрезвычайных ситуаций» и Постановление Правительства РФ № 1074, устанавливающие иерархическую структуру системы оповещения, охватывающую федеральный, региональный, муниципальный и объектовый уровни [1–3]. Эта иерархия непосредственно транслируется в требования к масштабируемости архитектуры и её способности обеспечивать вертикальную координацию уровней управления.

С точки зрения функциональных требований определяющими являются следующие. Во-первых, гарантированность доставки: сигнал оповещения должен быть доведён до 100% целевой аудитории вне зависимости от состояния отдельных каналов. Во-вторых, оперативность: нормативный предел — не более трёх минут в городских и пяти минут в сельских условиях согласно Приказу МЧС № 622 [3, 5]. В-третьих, адресность: система должна поддерживать как широкое геолокационное таргетирование (в зону угрозы), так и объектовое оповещение. В-четвёртых, устойчивость к разрушению инфраструктуры: архитектура обязана сохранять работоспособность при выходе из строя любого одного компонента или канала. Наконец, кибербезопасность: несанкционированный запуск оповещения или его блокирование представляют собой угрозы, сопоставимые по последствиям с отказом технических средств [6].

Из совокупности этих требований вытекает ключевое архитектурное ограничение: система должна быть построена по принципу многоканального гетерогенного резервирования, при котором каналы различных физических природ и операторских принадлежностей работают параллельно или в режиме горячего резерва с минимально возможным временем коммутации. Опора на единственный технологический стек, будь то сети подвижной связи или волоконно-оптические магистрали, создаёт недопустимые риски общей точки отказа [4, 7].

Трёхуровневая модульная архитектура.

На основании сформулированных требований предлагается трёхуровневая модульная архитектура адаптивной гибридной системы связи. Её уровни соответствуют трём функциональным задачам: обеспечению физической передачи, интеллектуальному управлению и предоставлению прикладных сервисов оповещения.

Уровень физических каналов является нижним и образован совокупностью гетерогенных средств передачи. В него входят волоконно-оптические линии связи (ВОЛС), формирующие защищённую магистраль с кольцевой топологией и автоматическим переключением по протоколам SDH/OTN; сети подвижной радиотелефонной связи стандартов LTE и перспективных 5G, поддерживающие технологию Cell Broadcast для массового геолокационного оповещения; спутниковые каналы ГЛОНАСС/Inmarsat, обеспечивающие покрытие территорий с деградированной наземной инфраструктурой; радиорелейные линии УКВ-диапазона в качестве оперативного резерва. Принципиальной особенностью данного уровня является его намеренная гетерогенность: каналы, различающиеся по физической природе, географической прокладке и операторской принадлежности, имеют ортогональные, практически некоррелированные профили отказов. Именно это свойство составляет основу системной отказоустойчивости [5, 8].

Уровень интеллектуального управления является ядром архитектуры и включает четыре функциональных модуля. Модуль непрерывного мониторинга реализует как активное зондирование каналов посредством лёгких пробных пакетов, так и пассивный анализ телеметрии от сетевого оборудования. Формируемый им вектор состояния канала включает оценки доступности, сквозной задержки, коэффициента потерь пакетов и джиттера. Модуль прогнозного моделирования обрабатывает временны́е ряды собранных метрик с использованием статистических методов и алгоритмов машинного обучения — в частности, ансамблей на основе решающих деревьев и моделей авторегрессии — для формирования краткосрочного прогноза на горизонте, соответствующем одному управляющему циклу. Модуль принятия решений вычисляет интегральный показатель качества

каждого канала как взвешенную линейную свёртку нормализованных прогнозных значений метрик и осуществляет ранжирование каналов. Выбор резервного канала производится не только по второму по величине показателю, но и с обязательным учётом минимизации корреляции его вероятных отказов с отказами основного. Модуль исполнения реализует принятые решения через взаимодействие с SDN-контроллерами, сетевыми шлюзами и серверами рассылки [7, 9].

Уровень прикладных сервисов обеспечивает непосредственное взаимодействие с конечными потребителями и системами управления. Он включает службу форматирования и маршрутизации сообщений, адаптирующую контент оповещения к требованиям конкретного канала (SMS, Cell Broadcast, голосовое сообщение, push-уведомление), а также программные интерфейсы (API) для интеграции с Едиными дежурно-диспетчерскими службами (ЕДДС) муниципального уровня и с региональными центрами управления в кризисных ситуациях (ЦУКС). Вертикальная координация уровней обеспечивается через защищённый служебный канал управления, изолированный от пользовательского трафика средствами VLAN-сегментации [6, 10].

Принципы функционирования алгоритма выбора канала.

Центральным алгоритмическим элементом архитектуры является процедура циклического выбора активного канала. Для каждого канала с

i из множества доступных $C = \{c_1, c_2, ..., c_n\}$ состояние в момент t задаётся вектором:

$$S_i(t) = (A_i(t), L_i(t), P_i(t), J_i(t)),$$

где $A_i(t)$ — доступность, $L_i(t)$ — сквозная задержка, $P_i(t)$ — коэффициент потерь пакетов, $J_i(t)$ — джиттер.

Прогнозная модель F на основе исторических данных $H_i(t)$ оценивает ожидаемое состояние на горизонте H:

$$\hat{S}_i(t + H) = F(H_i(t)).$$

Интегральный показатель качества канала вычисляется как взвешенная сумма нормализованных прогнозных значений:

$$Q_i = w_a \cdot \hat{A}_i + w_l \cdot (1 - \hat{L}_i) + w_p \cdot (1 - \hat{P}_i) + w_j \cdot (1 - \hat{J}_i),$$

где $w = (w_a, w_l, w_p, w_j)$ — вектор весовых коэффициентов, определяемый политикой системы для конкретного класса сообщений оповещения, а значения с крышкой представляют собой прогнозные величины, нормализованные к диапазону [0, 1].

Смена основного канала инициируется при выполнении условия превышения порога:

$$Q^*_{ne}w - Q^*_{ol}d > \delta,$$

где δ — гистерезисный порог, препятствующий избыточным переключениям при незначительных флуктуациях метрик. Данный порог является настраиваемым параметром и может быть откалиброван на этапе ввода системы в эксплуатацию на основе статистики переключений в конкретной инфраструктурной среде. Резервный канал выбирается из оставшихся с учётом условия:

$$arg\ max\ Q_j \quad при \quad \rho(f_i, f_j) < \rho max,$$

где $\rho(f_i, f_j)$ — коэффициент корреляции вероятностей отказа основного и резервного каналов, а ρmax — максимально допустимое значение данного коэффициента. Тем самым обеспечивается независимость сбоев двух выбранных каналов, что принципиально важно для устойчивости системы при локализованных воздействиях [9, 11].

Принципы обеспечения устойчивости и кибербезопасности.

Устойчивость системы обеспечивается на нескольких уровнях. На физическом уровне ВОЛС прокладываются по кольцевой топологии с автоматическим восстановлением соединений, а каждый узел управления оснащается источниками бесперебойного питания с

расчётным временем автономной работы, перекрывающим нормативный период ликвидации последствий ЧС. На транспортном уровне применяется пространственное разделение антенных систем радиорелейных линий и географическое разнесение спутниковых наземных станций. В условиях масштабной деградации инфраструктуры система переходит в режим снижения битрейта, при котором приоритет отдаётся доставке критически важных управляющих сигналов за счёт сжатия или временного отключения высокополосных сервисов [6, 10].

Кибербезопасность архитектуры строится на принципах, регламентируемых стандартами ФСТЭК России. Управляющий трафик модуля мониторинга и модуля принятия решений изолируется от общедоступного сегмента сети посредством VLAN-сегментации и двусторонней аутентификации на межсетевых экранах. Все команды управляющих воздействий подписываются цифровой подписью, что исключает их подделку. Модуль принятия решений снабжается механизмом обнаружения аномалий во входящей телеметрии: резкие немотивированные изменения параметров качества рассматриваются как потенциальный признак атаки типа «отравление данных», направленной на вывод системы на неоптимальный канал. В случае обнаружения подобных аномалий система переходит в детерминированный резервный режим с фиксированными приоритетами, реализуя принцип безопасного отказа [6, 8].

Масштабируемость достигается за счёт применения облачной (гибридной) платформы, где виртуальные машины региональных центров обработки информации динамически перераспределяют вычислительную нагрузку. Модульность архитектуры позволяет расширять количество поддерживаемых каналов без изменения базовых алгоритмических компонентов — достаточно добавить новый экземпляр

агента мониторинга и прогнозную модель для соответствующего канала [5, 9].

Интеграция с перспективными технологиями.

Предложенная архитектура изначально проектировалась с учётом перспективы интеграции с технологиями следующего поколения. Внедрение сетей 5G открывает возможности для использования технологии Network Slicing, при которой для трафика оповещения выделяется отдельный сетевой срез с гарантированными параметрами качества обслуживания, не зависящий от нагрузки пользовательского сегмента. Это принципиально меняет модель взаимодействия со сетями подвижной связи: от «лучшего из возможного» до гарантированного качества обслуживания [5, 11].

Развитие Интернета вещей (IoT) создаёт принципиально новый пласт оконечных устройств — уличные информационные киоски, светодиодные экраны, интеллектуальные громкоговорители, — которые могут быть интегрированы в систему оповещения как управляемые терминалы по протоколам MQTT/CoAP. Уровень прикладных сервисов предложенной архитектуры предусматривает соответствующие адаптеры для работы с такими устройствами. Помимо этого, данные с IoT-датчиков — сенсоров задымления, вибрации, уровня воды — могут использоваться модулем прогнозного моделирования как дополнительные признаки для оценки вероятности деградации отдельных сегментов инфраструктуры [10, 12].

Применение рекуррентных нейронных сетей архитектуры Long Short-Term Memory для прогнозирования временны́х рядов метрик качества рассматривается как перспективное направление развития модуля прогнозного моделирования. В сравнении с ансамблями решающих деревьев данные архитектуры способны улавливать долгосрочные зависимости в динамике сетевых показателей, что

особенно важно для прогнозирования деградационных сценариев, разворачивающихся в течение нескольких часов. Вместе с тем их применение предъявляет повышенные требования к вычислительным ресурсам, что обусловливает необходимость оценки компромисса между точностью прогноза и накладными расходами на инференс [7, 11].

Таким образом, в ходе проведённого исследования разработана и обоснована трёхуровневая модульная архитектура адаптивной гибридной системы связи для комплексов экстренного оповещения населения. Предложенная архитектура строится на принципах гетерогенного резервирования с минимизацией корреляции отказов, непрерывного прогностического мониторинга качества обслуживания и взвешенного динамического ранжирования каналов. Показано, что именно совокупность этих принципов, а не улучшение отдельных характеристик отдельных каналов, обеспечивает качественный скачок в надёжности системы — исключение не только средних задержек, но и хвостовых экстремальных задержек, несовместимых с требованиями оперативности. Разработанная архитектура формирует практическую основу для модернизации существующих КСЭОН, допуская поэтапное внедрение без полной замены действующей инфраструктуры. Дальнейшее её развитие связывается с углублённой интеграцией методов глубокого обучения, адаптацией к возможностям сетей 5G/6G и формализованной верификацией кибербезопасности предложенных решений.

Литература

1. О защите населения и территорий от чрезвычайных ситуаций природного и техногенного характера : Федеральный закон от 21.12.1994 № 68-ФЗ (ред. от 11.06.2021) // Собрание законодательства РФ. – 1994. – № 35. – Ст. 3648.

2. Об утверждении Положения о системах оповещения населения : постановление Правительства РФ от 01.03.2019 № 1074 (ред. от 23.10.2021) // Собрание законодательства РФ. – 2019. – № 10. – Ст. 1028.

3. ГОСТ Р 22.1.12-2020. Безопасность в чрезвычайных ситуациях. Единая система экстренного оповещения населения. Общие требования. – Введ. 2021-07-01. – М. : Стандартинформ, 2020. – 24 с.

4. Максимов И. А., Краснокутский А. В., Удилова И. Я., Сулима Т. Г. Современный этап развития, тенденции и проблемы функционирования систем оповещения и информирования населения в системе гражданской обороны и защиты от чрезвычайных ситуаций // Научные и образовательные проблемы гражданской защиты. – 2013. – № 4. – URL: https://cyberleninka.ru/article/n/sovremennyy-etap-razvitiya-tendentsii-i-problemy-funktsionirovaniya-sistem-opovescheniya (дата обращения: 11.01.2026).

5. Уктамов Н. П., Гафуров Н. Н. Современные средства оповещения населения при угрозах возникновения чрезвычайных ситуаций // Universum: технические науки. – 2020. – № 6 (75). – URL: https://7universum.com/ru/tech/archive/item/9639 (дата обращения: 11.01.2026).

6. Ахмедова Х. М. Организационно-правовое регулирование информирования и оповещения населения при угрозе и возникновении чрезвычайных ситуаций природного или техногенного характера // Молодой учёный. – 2022. – № 38 (433). – С. 87–89.

7. Соколов Ю. И. К вопросу организации оповещения населения при возникновении чрезвычайной ситуации // Проблемы анализа риска. – 2019. – № 1. – URL: https://cyberleninka.ru/article/n/k-voprosu-organizatsii-opovescheniya-naseleniya-pri-vozniknovenii-chrezvychaynoy-situatsii (дата обращения: 11.01.2026).

8. Шарахутдинов Р. Б., Черкесов В. В. Анализ современных технологий и технических средств оповещения и информирования населения о чрезвычайных ситуациях // Пожарная и техносферная безопасность: проблемы и пути совершенствования. – 2020. – № 2 (6). – С. 485–489.

9. Цуриков А. Н., Ракитская Е. А. Мобильные приложения для оповещения об экстренных ситуациях // Научное обозрение. Технические науки. – 2018. – № 5. – С. 30–36.

10. Новиков А. С. Роль волоконно-оптических линий связи в обеспечении отказоустойчивости систем управления при чрезвычайных ситуациях // Вестник связи. – 2022. – № 3. – С. 18–25.

11. Леонова А. Н., Леонова Е. М. О комплексных системах экстренного оповещения населения // Столыпинский вестник. – 2023. – № 1. – URL: https://cyberleninka.ru/article/n/o-kompleksnyh-sistemah-ekstrennogo-opovescheniya-naseleniya (дата обращения: 11.01.2026).

12. Информационно-коммуникационные технологии обеспечения безопасности жизнедеятельности: монография / МЧС России [под общ. ред. П. А. Попова]. – М. : ФГУ ВНИИ ГОЧС (ФЦ), 2009. – 272 с.

References

1. On the Protection of the Population and Territories from Natural and Man-Made Emergencies: Federal Law No. 68-FZ of 21.12.1994 (as amended on 11.06.2021) // Collection of Legislation of the Russian Federation. – 1994. – No. 35. – Art. 3648.

2. On Approval of the Regulation on Public Warning Systems: Decree of the Government of the Russian Federation No. 1074 of 01.03.2019 (as amended on 23.10.2021) // Collection of Legislation of the Russian Federation. – 2019. – No. 10. – Art. 1028.

3. GOST R 22.1.12-2020. Safety in Emergencies. Unified Emergency Public Warning System. General Requirements. – Introduced 2021-07-01. – Moscow: Standartinform, 2020. – 24 p.

4. Maksimov I. A., Krasnokutsky A. V., Udilova I. Ya., Sulima T. G. The Current Stage of Development, Trends and Problems of Functioning of Public Warning and Notification Systems in the Civil Defense and Emergency Protection System // Scientific and Educational Problems of Civil Protection. – 2013. – No. 4. – URL: https://cyberleninka.ru/article/n/sovremennyy-etap-razvitiya-tendentsii-i-problemy-funktsionirovaniya-sistem-opovescheniya (accessed: 11.01.2026).

5. Uktamov N. P., Gafurov N. N. Modern Means of Public Warning in the Event of Emergency Threats // Universum: Technical Sciences. – 2020. – No. 6 (75). – URL: https://7universum.com/ru/tech/archive/item/9639 (accessed: 11.01.2026).

6. Akhmedova Kh. M. Organizational and Legal Regulation of Public Information and Warning in the Event of a Threat or Occurrence of Natural or Man-Made Emergencies // Young Scientist. – 2022. – No. 38 (433). – P. 87–89.

7. Sokolov Yu. I. On the Issue of Organizing Public Warning in the Event of an Emergency // Risk Analysis Problems. – 2019. – No. 1. – URL: https://cyberleninka.ru/article/n/k-voprosu-organizatsii-opovescheniya-naseleniya-pri-vozniknovenii-chrezvychaynoy-situatsii (accessed: 11.01.2026).

8. Sharakhutdinov R. B., Cherkesov V. V. Analysis of Modern Technologies and Technical Means of Public Warning and Notification about Emergencies // Fire and Technosphere Safety: Problems and Ways of Improvement. – 2020. – No. 2 (6). – P. 485–489.

9. Tsurikov A. N., Rakitskaya E. A. Mobile Applications for Emergency Notification // Scientific Review. Technical Sciences. – 2018. – No. 5. – P. 30–36.

10. Novikov A. S. The Role of Fiber-Optic Communication Lines in Ensuring Fault Tolerance of Control Systems in Emergency Situations // Bulletin of Communications. – 2022. – No. 3. – P. 18–25.

11. Leonova A. N., Leonova E. M. On Integrated Emergency Public Warning Systems // Stolypin Bulletin. – 2023. – No. 1. – URL: https://cyberleninka.ru/article/n/o-kompleksnyh-sistemah-ekstrennogo-opovescheniya-naseleniya (accessed: 11.01.2026).

12. Information and Communication Technologies for Life Safety: Monograph / EMERCOM of Russia [under the general editorship of P. A. Popov]. – Moscow: FGU VNII GOChS (FTs), 2009. – 272 p.