Научно-технический журнал
ТЕХНИКА СРЕДСТВ СВЯЗИ
MEANS OF COMMUNICATION EQUIPMENT
Scientific and Technical Journal
№ 1 (173) – 2026

РЕДАКЦИЯ:
Верстка принт-макета: **Тюкинеева Л.В.**
Дизайн обложки: **Шаутин Д.В.**
Поддержка сетевой версии журнала: **Тюкинеева Л.В.**
Секретарь редакции: **Тюкинеева Л.В.**

АДРЕС РЕДАКЦИИ:
197342. Россия. г. Санкт-Петербург, ул. Кантемировская, дом 8,
Телефон: +7(812) 542-90-54; +7(812) 448-95-97; +7(812) 448-96-84
Факс: +7(812) 542-18-49. E-mail: mce-journal@inteltech.ru.
Официальный сайт: www.inteltech.ru; www.mce-journal.ru

Научно-технический журнал
ТЕХНИКА СРЕДСТВ СВЯЗИ
MEANS OF COMMUNICATION EQUIPMENT
Scientific and Technical Journal
№1 (173) – 2026

Научно-технический журнал «Техника средств связи» – это рецензируемое научное издание, в котором публикуются результаты научных исследований специалистов в области современных инфокоммуникационных технологий и автоматизированных систем управления, средств связи и информационной безопасности. Журнал является правопреемником издававшихся с 1959 года Министерством промышленности средств связи СССР всесоюзных журналов «Вопросы радиоэлектроники. Серия: Техника проводной связи» и «Вопросы специальной радиоэлектроники. Серия: Техника проводной связи». С 1975 года журнал издается под названием «Техника средств связи». **Учредитель и издатель журнала:** Публичное акционерное общество «Информационные телекоммуникационные технологии» (ПАО «Интелтех»). **Адрес учредителя и издателя журнала:** 197342, Россия, г.Санкт-Петербург, ул. Кантемировская, д.8.

Адрес типографии: 623102, Свердловская область, г. Первоуральск. пр. Ильича д.26А, АО «Первоуральская типография».

Главный редактор журнала – Председатель редакционного совета – П.А. Будко, Ученый секретарь ПАО «Интелтех», д.т.н., профессор.

Решением ВАК № 222-р от 10.06.2024 научно-технический журнал «Means of communication equipment» («Техника средств связи») включен в перечень рецензируемых научных изданий, в которых должны быть опубликованы основные научные результаты диссертаций на соискание ученой степени кандидата наук, на соискание ученой степени доктора наук и рекомендован ВАК для публикаций основных результатов по научным специальностям:

2.2.13. Радиотехника, в том числе системы и устройства телевидения;
2.2.14. Антенны, СВЧ устройства и их технологии;
2.2.15. Системы, сети и устройства телекоммуникаций;
2.3.1. Системный анализ, управление и обработка информации, статистика;
2.3.5. Математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей; 2.3.6. Методы и системы защиты информации, информационная безопасность (по отраслям науки - технические науки).

Выходит 4 раза в год.
Публикация в журнале является научным печатным трудом.
Основное содержание издания представляет собой научные статьи и научные обзоры.
Возрастное ограничение 12 +
Журнал зарегистрирован как сетевое и печатное издания в Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор).
Свидетельства о регистрации средств массовой информации: ПИ № ФС 77 – 80135 и ЭЛ № ФС 77 – 80136 от 31.12.2020 г.
ISSN (print): 2782-2141; ISSN (online): 2782-2133; РИНЦ (eLIBRARY ID: 77074)
Распространяется по подписке. Подписной индекс журнала-79656. Ссылки для оформления интернет-подписки на журнал:
https://www.akc.ru/itm/means-of-communication-equipment/; https://www.pressa-rf.ru/cat/1/edition/e79656/
Свободная цена
Тираж: 40 экз.
Подписано в печать 18.03.2026. Дата выхода в свет 20.03.2026

СОДЕРЖАНИЕ

CONTENTS

Рубрики журнала: Анализ новых технологий и перспектив развития техники средств связи • Системы управления • • Передача, прием и обработка сигналов • Системы связи и телекоммуникации • Перспективные исследования • • Вычислительные системы • Информационные процессы и технологии. Сбор, хранение и обработка информации • • Моделирование сложных организационно-технических систем • Вопросы обеспечения информационной безопасности • • Интеллектуальные информационные системы • Робототехнические системы • Электронные и радиотехнические системы • • Объекты интеллектуальной собственности и инновационные технологии в области разработки средств телекоммуникаций

ПЕРЕДАЧА, ПРИЕМ И ОБРАБОТКА СИГНАЛОВ

УДК 621.513.6 DOI: 10.24412/2782-2141-2026-1-2-13

Адаптивные алгоритмы пространственно-временной обработки запросных сигналов системы госопознавания

Белов А. С., Чони Ю. И.

Аннотация. ***Постановка задачи.*** *Работоспособность радиоэлектронных систем вторичной радиолокации, в том числе систем государственного опознавания, зависит от помехозащищенности запросного и ответного каналов. Показано, что основные направления исследований должны быть направлены на запросный канал опознавания «свой-чужой». Исследовано использование антенных решеток в приеме сигналов системы государственного опознавания.* ***Объект исследования****. В работе исследуются кольцевые антенные решетки ответчиков государственного опознавания.* ***Предмет исследования.*** *Предметом исследования являются алгоритмы и средства пространственной обработки сигнально-помехового потока, принимаемого антенной решеткой.* ***Цель статьи:*** *формирование методического подхода к построению алгоритмов пространственно-временной обработки запросных сигналов в ответчиках системы государственного опознавания) и оценка потенциальных характеристик компенсатора помех на базе кольцевой антенной решетки. В анализе использованы антенны с диаграммами направленности кардиоидного типа.* ***Используемые методы.*** *Основным методом исследования являются методы компьютерного моделирования антенных решеток в условиях воздействия помех.* ***Результаты.*** *Приведены результаты моделирования диаграмм направленности антенных решеток при воздействии одной, двух и трех помех. Результаты моделирования для конкретных помеховых ситуаций и статистические оценки по множеству случайных ситуаций подтверждают эффективность пространственной обработки, которая при реалистичном сочетании параметров в среднем привносит дополнительное ослабление помех на 25 дБ ÷ 30 дБ.* ***Практическая значимость.*** *Областью применения результатов данной работы являются адаптивные антенные решетки ответчиков системы государственного опознавания, а также других систем вторичной радиолокации и управления воздушным движением.*

Ключевые слова: *адаптация, компенсация помех, помеховая ситуация, пространственно-временная обработка.*

Введение

Совершенствование радиоэлектронных систем вторичной радиолокации, передачи информации и обмена данными зачастую связано с переходом на новые помехозащищенные сигналы и алгоритмы их обработки [1-3]. Однако существует ряд систем, включающий средства, развитие которых требует существенных финансовых и временных затрат. К подобным системам относится и система государственного опознавания (СГО). В данном случае значительный интерес представляет возможность улучшения комплексов СГО по общесистемным характеристикам, и в первую очередь по помехозащищенности, без изменения используемых сигнально-кодовых конструкций.

Запросный канал СГО наиболее подвержен воздействиям внутрисистемного потока и различного рода помех ввиду большей информационной емкости сигналов и использования относительно слабоустойчивой к действию помех импульсной модуляции. Скрытность запросчиков СГО обеспечивается в какой-то степени направленными свойствами их антенн. В то же время, скрытность ответчиков, излучающих ответные сигналы на ненаправленную антенну, может быть улучшена за счет формирования направленного ответа. В данной работе рассматривается возможность построения адаптивных алгоритмов пространственно-временной обработки запросных сигналов в ответчиках СГО с акцентом на компенсацию помех за счет соответствующего весового суммирования сигналов, принимаемых N-элементной антенной решеткой (АР) ответчика.

Исследования соответствующих принципов, алгоритмов и путей их технической реализации стартовали давно [4-8] и продолжаются до сих пор [9-16], составляя предмет разработки компенсаторов помех или, говоря по-другому, адаптивных антенных решеток (ААР). По сути, это одно и то же, но в терминах соотношения сигнала, помехи и шума на выходе компенсатора или в терминах диаграммы направленности (ДН). Нюанс, отличающий эти подходы, состоит лишь в том, что ДН не только отражает реакцию на текущую сигнально-помеховую ситуацию, но и характеризует, что будет происходить при приходе полезного сигнала с произвольных направлений. С системных же позиций этим надо отдельно озаботиться. Учитывая равнозначность обеих точек зрения, будем использовать системный или антенный подход в зависимости от характера обсуждаемого вопроса.

Сущностный фактор, обусловливающий возможность формирования провалов в направлениях на источник помех и в возможной степени сохранения условий приема полезных сигналов, состоит в том, что должны существовать и использоваться в алгоритме адаптации априорные отличия источников помех от полезных сигналов. Применительно к СГО, полезные сигналы которых представляют собой короткие импульсные посылки высокой скважности, фундаментальным отличительным признаком помехи, тем более умышленной, является то, что это низкой скважности сигнал, приходящий с фиксированного или медленно меняющегося[1] направления. В излагаемых ниже компенсаторах помех именно это отличие используется для защиты цепей адаптации от срабатывания на полезные запросы.

Все элементы рассматриваемой кольцевой ААР используются и для формирования круговой ДН в отсутствии помех, и для формирования провалов на источники помех (ААР Аппельбаума [4]). При оценке потенциальных возможностей компенсации помех, не динамика регулирования, а характеристики установившегося режима играют решающую роль. И в этом отношении важна минимизируемая целевая функция. Как показано в [5, 11], известные алгоритмы обращения корреляционной матрицы или градиентного спуска [7] соответствуют ослаблению мощности помех на выходе при минимальном отклонении вектора весовых коэффициентов (ВВК) от его исходного состояния. Предметом оценки будет эффективность компенсации помех при использовании именно этих алгоритмов.

1. Кольцевая антенная решетка

В интересах повышения функциональных и системных характеристик ответчика СГО предлагается использовать кольцевую антенную решетку, структурная схема которой приведена на рис. 1. Схема АР состоит из шести элементов, расположенных равномерно на окружности радиуса a и имеющих радиально ориентированные кардиоидные амплитудные ДН в плоскости решетки и синусоидальные ДН в азимутальных плоскостях по углу θ. Для простоты следующего изложения введем универсальный символ ψ для направления (аргумента ДН), который означает угол φ или совокупность углов (θ, φ) соответственно 2D или 3D вариантам анализа.

Для обоих вариантов рассмотрения (в плоскости АР или в полусфере) индивидуальная ДН n-го элемента (n = 1,…, N) с учетом его выноса из центра системы координат описывается выражениями вида[2]

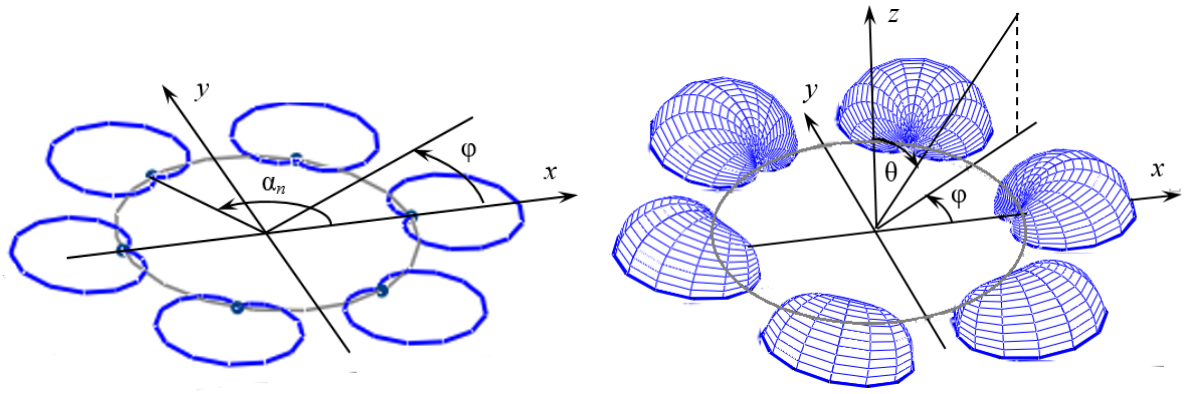
$$f_n(\psi) = \begin{cases} \left[1+\cos\left(\varphi-\alpha_n\right)\right]\exp\left(jka\cos\left(\varphi-\alpha_n\right)\right) \\ \sin(\theta)\left[1+\cos\left(\varphi-\alpha_n\right)\right]\exp\left(jka\sin(\theta)\cos\left(\varphi-\alpha_n\right)\right) \end{cases}, \quad (1)$$

где $k = 2\pi/\lambda$ – волновое число, $\alpha_n = 2\pi(n-1)/N$ – угловая координата элемента.

Если в текущий момент времени ВВК есть $\mathbf{W} = \{W_n\}$ (n = 1, …, N), то с учетом универсальной записи (1) ДН ААР задается выражением

[1] В соответствии с динамикой перемещения источника помехи и/или приемника ответчика.

[2] Не существенный 0.5-множитель, нормирующий кардиоидную зависимость, опущен.



а) *б*)

Рис. 1. Структурная схема шестиэлементной антенной решетки: *а*) Вариант 2*D; б*) Вариант 3*D*

$$F(\psi, \mathbf{W}) = \sum_n W_n \; f_n(\psi) \, . \qquad (2)$$

Естественно полагать, что источники помех и сигналов расположены случайно с постоянной плотностью вероятностей по поверхности верхней полусферы, и вероятность пребывания источника в пределах интервалов $d\theta\, d\varphi$ вокруг направления (θ, φ) пропорциональна величине $dP = \sin\theta\, d\theta\, d\varphi$. Таким образам, источники и помех, и сигналов с наибольшей вероятностью располагаются вблизи меридиональной плоскости, и при оценке эффективности компенсации помех анализ в варианте 2*D* оправдан не только экономичностью расчетов, но и в вероятностном плане.

2. Методические основы адаптации антенной решетки к помеховой ситуации

Среди возможных критериев эффективности адаптации, отражающих функциональные требования к процессу компенсации помех, и при этом допускающих аналитическое решение, выделим [10, 13, 14] критерий минимизации целевой функции $\Phi(\mathbf{W})$ в виде взвешенной суммы

$$\Phi(\mathbf{W}) = P_{\text{вых}}(\mathbf{W}) + \mu \, \|\mathbf{W}_0 - \mathbf{W}\|^2. \qquad (3)$$

Здесь $\mathbf{W}=\{W_n\}$ и $\mathbf{W}_0=\{W_{0n}\}$ это, соответственно, искомый ВВК компенсатора и исходный ВВК, обеспечивающий формирование оптимальной ДН в отсутствии помех; $P_{\text{вых}}(\mathbf{W})$ – мощность помех на выходе; μ – коэффициент штрафа за отклонение текущего ВВК от номинального.

2.1. Алгоритм обращения корреляционной матрицы

Как известно [10, 14], в условиях статистически независимых источников помех, приходящих с M направлений $\{\psi_m\}$, $m = 1,\ldots, M$, интенсивность которых характеризуется мощностью[3] P_m, оптимальный в смысле минимума критерия (3) ВВК $\mathbf{W}_{\text{opt}}$ определяют как

$$\mathbf{W}_{\text{opt}} = \mu \, (\langle \mathbf{R} \rangle + \mu \, \mathbf{E})^{-1} \, \mathbf{W}_0, \qquad (4)$$

где $\mathbf{E}$ – единичная матрица, $\langle \mathbf{R} \rangle$ – эрмитово сопряженная матрица коэффициентов корреляции комплексных огибающих $\{S_n\}$ ($n = \underline{1,\ldots, N}$) помеховых сигналов, принимаемых элементами АР

$$R_{n,k} = \left(S_k \, S_n^*\right) = \sum_m P_m \; f_k(\psi_m) \; f_n^*(\psi_m) \, . \qquad (5)$$

Здесь и далее черта сверху означает усреднение по времени на интервале, превышающем интервал корреляции комплексных огибающих сигналов.

Ясно, что при исходном ВВК (до адаптации) мощность помех на выходе компенсатора составляет величину $P_{0\,\text{вых}} = \sum_m P_m \left|F(\psi_m, \mathbf{W}_0)\right|^2$. В результате адаптации мощность помех на выходе снижается до уровня $P_{\text{вых}} = \sum_m P_m \left|F(\psi_m, \mathbf{W})\right|^2$.

[3] Имеется в виду мощность, принимаемая элементом антенной решетки от источника, расположенного по максимуму диаграммы направленности.

Отношение этих величин

$$\gamma = \frac{\sum_m P_m \left| F(\psi_m, \mathbf{W}) \right|^2}{\sum_m P_m \left| F(\psi_m, \mathbf{W}_0) \right|^2} \qquad (6)$$

характеризует эффективность компенсации помех и, выраженное в децибелах, будет использоваться ниже.

При всей привлекательности целевого функционала (3) очевидно, что в ситуациях, когда АР не способна сформировать глубокие провалы на источники помех, уменьшение первого слагаемого $P_{вых}(\mathbf{W})$ будет достигаться за счет того, что ВВК $\mathbf{W}$ устремится к бесполезному нулевому решению. При этом коэффициент γ будет давать завышенную оценку эффективности компенсации помех, поскольку в нем не учитывается снижение уровня принимаемых полезных сигналов. Этого недостатка нет у ААР с частичной адаптацией [5]: выбирается один из элементов АР и его весовой коэффициент фиксируется W_n = const. В случае кольцевой АР нет логичных оснований для такого выбора. Нам представляется целесообразным достичь той же цели, нормируя решение (4) по исходному ВВК: $\mathbf{W} = \mathbf{W}_{opt} \|\mathbf{W}_0\| / \|\mathbf{W}_{opt}\|$. Именно такой вариант алгоритма адаптации, приводящий к реалистичной оценке эффективности компенсации, используется далее.

2.2. Алгоритм градиентного спуска

Градиентные алгоритмы адаптации по скорости регулирования уступают алгоритмам обращения корреляционной матрицы, но экономнее в вычислительном отношении. Кроме того, они устойчивее по отношению к неконтролируемым отклонениям параметров цепей адаптации, и находят широкое применение на практике. Несложно показать [10] (и из физических соображений это ожидаемо), что вектор градиента $\mathbf{G} = \{\partial P_{вых}(\mathbf{W})/\partial W_n\}$ целевой функции (3) образован коэффициентами корреляции сигналов помех на выходе компенсатора с сигналами помех, принимаемых элементами АР, т. е.

$$G_n = \overline{\left(S_{вых} S_n^* \right)}. \qquad (7)$$

Процесс адаптации, реализующий градиентный спуск в реальном масштабе времени, сходится к минимуму функции (3), и таким образом, величина γ (6) характеризует эффективность компенсации помех в установившемся состоянии и для алгоритма градиентного спуска. На рис. 2 представлена блок схема соответствующего компенсатора помех в цифровом варианте реализации.

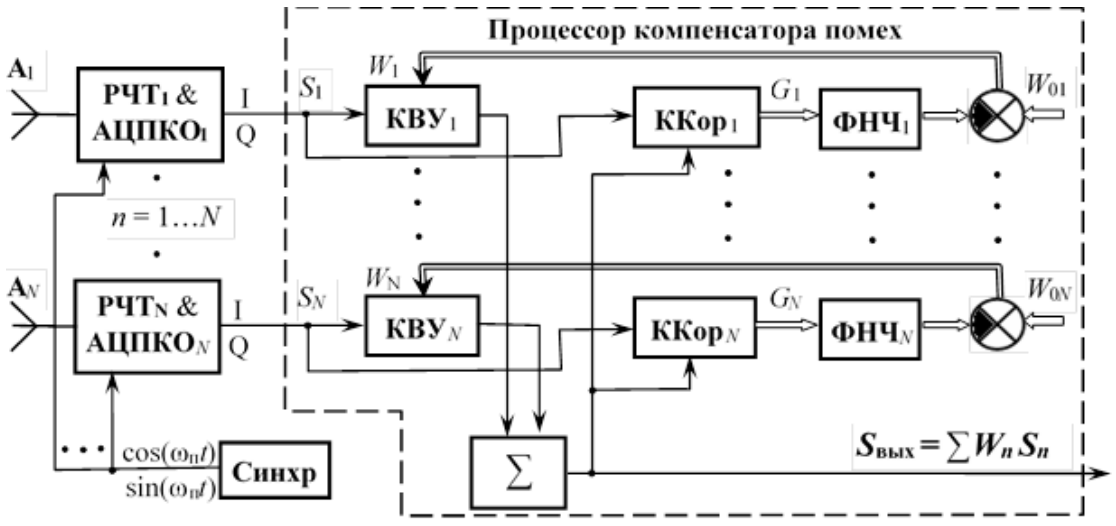


Рис. 2. Структурная схема компенсатора помех

Принятые сигналы: смесь запросных сигналов (ЗС), помех и шумов – после соответствующей фильтрации, усиления в радиочастотном тракте (РЧТ) и переноса на промежуточную частоту $\omega_п$, подвергаются когерентному (от единого синхронизатора) аналогово-цифровому преобразованию комплексных огибающих (АЦПКО) $\{S_n\}$ в формате *I/Q*. Последующая обработка и формирование выходного сигнала как взвешенной комплексными весовыми умножителями (КВУ) суммы

$$S_{вых} = \sum W_n S_n, \qquad (8)$$

осуществляются в цифре соответствующим процессором. Здесь $\mathbf{W} = \{W_n\}$ есть ВВК выработанный в текущий момент времени цепями обратной связи.

В соответствие со схемной реализацией, комплексные корреляторы (ККор) перемножают мгновенные отсчеты сигналов S_n и $S_{вых}$ и выделяют среднее значение[4] на интервале $T_{кор}$, тем самым формируя текущие оценки (7) компонент G_n вектора градиента **G**. Фильтры низких частот (ФНЧ) с большой постоянной времени $T_{фнч}$ играют роль интегратора, изменяющего текущее значение ВВК **W** со скоростью, пропорциональной градиенту со знаком «–»

$$\mathbf{W}(T) = \mathbf{W}_0 - K_ф \int_0^T h_{фнч}(T-\tau)\,\mathbf{G}(\tau)\,d\tau\,. \qquad (9)$$

При значении постоянной $T_{фнч}$, существенно превышающем длительность запросных сигналов[5], их наличие вызывает незначительное и разнонаправленное подрабатывание ВВК (9). В отличие от этого каждый источник помехи создает высокой плотности поток сигналов (хаотических импульсных последовательностей, ложных синхрогрупп, ложных ЗС), приходящих с постоянного направления. Соответственно, регулирование (9) эффективно отрабатывает эти сигналы. В отсутствии помех $G_n(\tau) \approx 0$ и ВВК практически совпадает с $\mathbf{W}_0$.

3. Эффективность компенсации помех кольцевой антенной решеткой

Волновой размер кольца определяет угловую чувствительность АР и тем самым пространственное разрешение компенсатора. Помеховая ситуация – это другой решающий фактор эффективности компенсации. Реальные число, расположение и мощность источников помех случайны, поэтому наиболее значимы статистические оценки параметра γ (6) на состоятельной выборке помеховых ситуаций. Особенности этих статистик отражают поведение компенсатора в частных ситуациях. Ясно, что наличие слабых источников помех облегчает возможность компенсации более мощных. Потому для ужесточения оценок в расчетах задавалась одинаковая мощность всех помех, превосходящая мощность внутреннего шума в десять раз: $P_{пом} = 10\,P_{nois}$.

3.1. 2*D*-вариант, одиночная помеха

На рис. 3 приведены ДН как результат компенсации одиночной помехи, угловая координата β_1 которой отмечена на графиках жирной красной точкой. В подрисуночных подписях приведены значения γ эффективности компенсации помехи (6). В силу периодичности АР зависимость γ от расположения помехи в пределах полуинтервала между соседними элементами АР периодически повторяется для иных углов прихода помехи. Поэтому представлены лишь две ситуации $\beta_1 = 30°$ и $\beta_1 = 60°$. Ясно, что эффективность компенсации почти не зависит от направления прихода помехи.

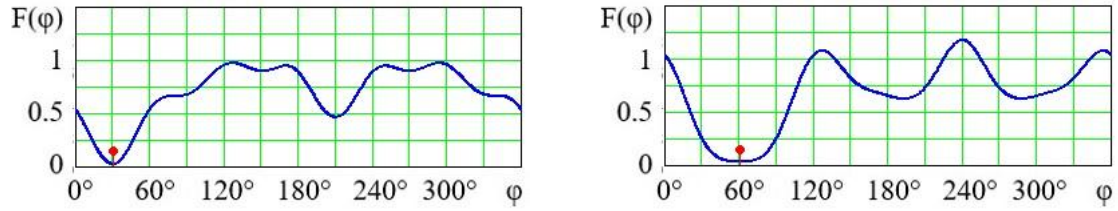
3.2. 2*D*-вариант, две помехи

Естественно, эффективность компенсации двух помех зависит от их взаимного положения. На рис. 4 представлены три ситуации со все возрастающим угловым интервалом между помехами.

---

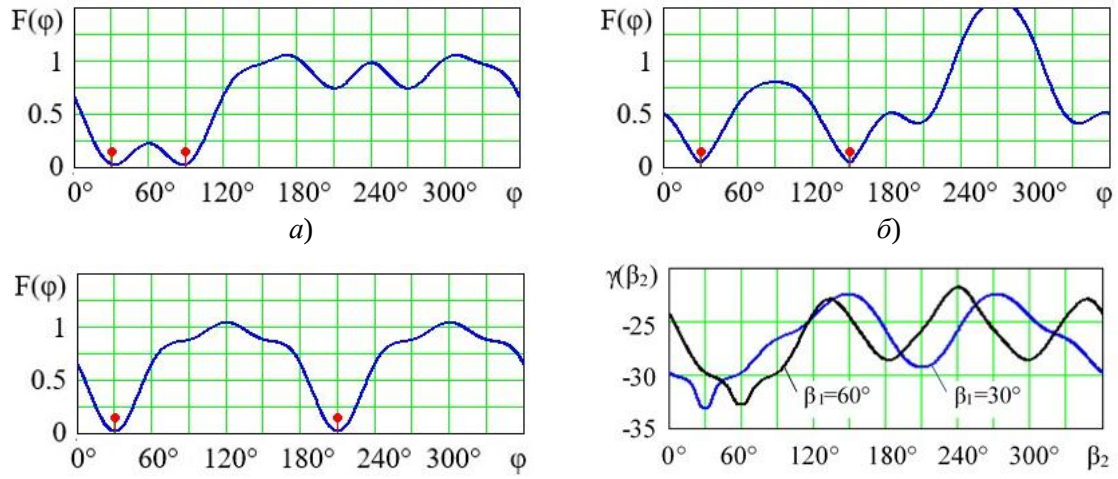
[4] Двойные линии на структурной схеме символизируют медленно меняющиеся сигналы.

[5] В ответчике СГО результат обнаружения полезного ЗС может использоваться еще и для защиты алгоритма адаптации от влияния ЗС.



а) *б*)

Рис. 3. Эффективность компенсации одиночной помехи: *а*) γ = –27.3 дБ; *б*) γ = –26.9 дБ



а) *б*)

в) *г*)

Рис. 4. Эффективность компенсации двух помех: *а*) γ = –26.6 дБ; *б*) γ = –22.4 дБ; *в*) γ = –29.3 дБ; *г*) вторая помеха перемещается

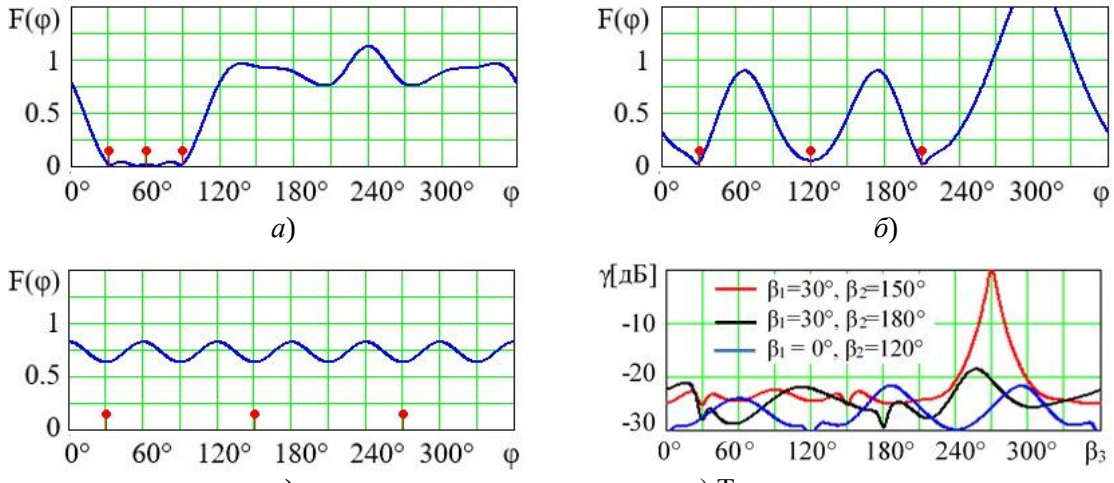
Две близкие помехи, рис. 4 *а*), сродни одной суммарной и потому эффективно компенсируются. При $|\beta_1 - \beta_2| = 180°$ помеховые сигналы на АР ортогональны (отчасти благодаря радиально ориентированным кардиоидам) и компенсируются как две одиночные помехи, рис. 4 *в*). Ситуация по рис. 4 *б*) выделяется тем, что при компенсации помех $\beta_1 = 30°$ и $\beta_2 = 150°$ в направлении $\varphi = 270°$ формируется интенсивный интерференционный максимум. По физическим соображениям ясно, что он может сыграть роковую роль, при появлении третьей помехи с этого направления.

На рис. 4 *г*) показаны зависимости эффективности компенсации двух помех при фиксированном положении одной из помех (в вариантах $\beta_1 = 30°$ и $\beta_1 = 30°$) и при второй помехе, перемещающейся в полных пределах. Представленные данные свидетельствуют о том, что компенсация двух помех возможна на уровне не хуже –22 дБ при любом расположении их источников.

3.3. 2*D*-вариант, три помехи

Аналогично предыдущему, на рис. 5 представлены три ситуации с все возрастающим угловым интервалом между помехами. Естественно, близко расположенные помехи, рис. 5 *а*), легко компенсируются за счет расширенного провала в ДН, а в остальном эффект компенсации зависит от взаимного расположения источников помех. В частности, при угловых координатах помех {30°, 150°, 270°} (рис. 5 *в*) наблюдается критическая ситуация, когда оптимальный ВВК (4), минимизирующий целевую функцию (3), повторяет[6] номинальный ВВК $\mathbf{W}_0$ с весом 0.071. Соответственно, значение коэффициента γ без нормировки составляет формальные –22.98 дБ, а после нормировки истинные 0 дБ, что соответствует факту сохранения исходной ДН.

[6] Интерференционные всплески ДН как физические причины этого упомянуты выше.



а) *б*) *в*) *г*) Третья помеха перемещается

Рис. 5. Эффективность компенсации трех помех: *а*) γ = –30.7 дБ; *б*) γ = –24.5 дБ; *в*) γ = 0 дБ; *г*) третья помеха перемещается

Благоприятным обстоятельством является тот факт, что критические ситуации появляются лишь при специфическом сочетании помеховой ситуации и геометрии АР. Рис. 5 *г*) наглядно демонстрирует это: при смещении третьего источника помехи за пределы $\beta_3 = 270° \pm 30°$ эффективность компенсации помех полностью восстанавливается. То же самое происходит и при смещениях других источников помех.

3.4. 2*D*-вариант, вероятностные оценки

Шестиэлементная АР способна формировать до пяти нулевых провалов не без все возрастающего ущерба для поддержания уровня исходной ДН вне этих провалов. Ситуация с одиночным источником помехи интереса не представляет, поскольку для кольцевой АР степень компенсации γ почти не зависит от направления прихода и, как подтверждают результаты расчетов, рис. 3, составляет величину порядка –27 дБ. Значение это обусловлено глубиной одиночного провала в ДН кольцевой АР, формируемого в результате адаптации на помеху $P_{пом} = 10\ P_{nois}$ при параметре $\mu = 1$ целевой функции (3). Поэтому, будем анализировать эффективность компенсации при числе M от двух до пяти случайно расположенных источников помех. На практике их интенсивности тоже случайны, но в интересах более суровой оценки будем считать, что мощность каждого источника помех ($m = 1,\ldots, M$) в десять раз превосходит мощность шума $P_m = 10\ P_{nois}$.

В табл. 1 приведены статистические параметры min, max, mean (матожидание) и среднеквадратическое отклонение (СКО), которые получены по $Stat = 1500$ случайным ситуациям, когда направление каждой из помех задавалось генератором случайных чисел, равномерно распределенных на интервале $(0 – 2\pi)$.

На рис. 6 представлены распределения вероятностей эффективности γ компенсации помех для тех же случайных ситуаций[7], что и в табл. 1.

Таблица 1 – Статистические показатели эффективности γ компенсации

M	min, дБ	max, дБ	mean, дБ	СКО, дБ
2	–33.0	–21.8	–26.6	2.1
3	–35.3	–0.6	–24.7	3.5
4	–37.6	–3.6	–22.3	4.6
5	–34.8	–2.2	–19.5	5.6

[7] Для трех помех ($M = 3$) была выбрана серия, содержащая почти критическую ситуацию $\gamma_{max} = –0.6$ дБ,

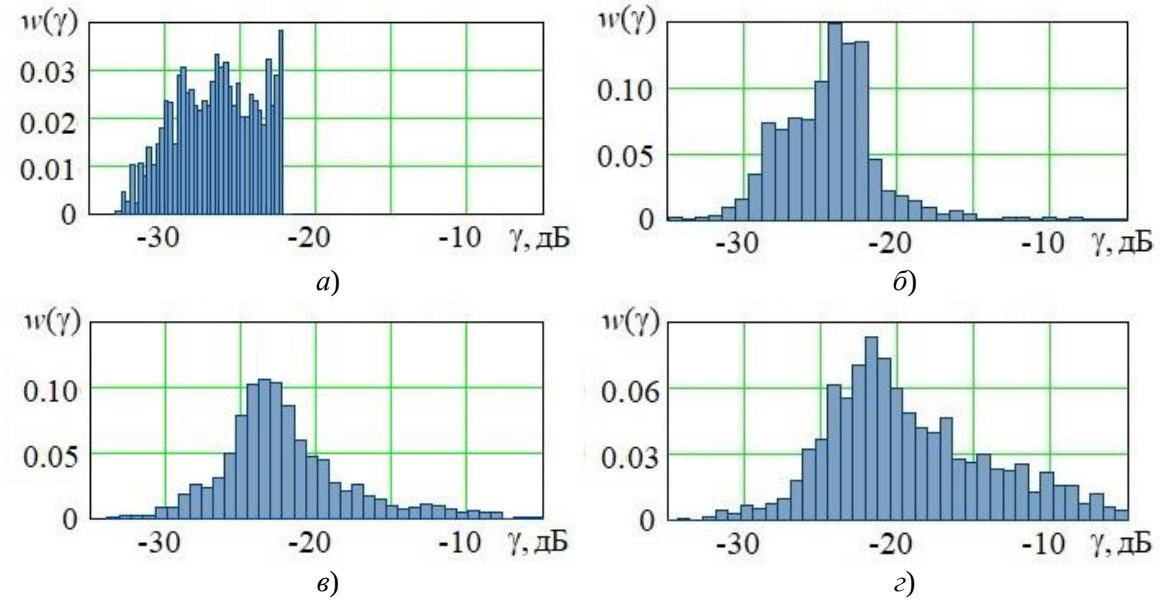


Рис. 6. Распределение вероятностей параметра γ: *а*) $M = 2$; *б*) $M = 3$; *в*) $M = 4$; *г*) $M = 5$

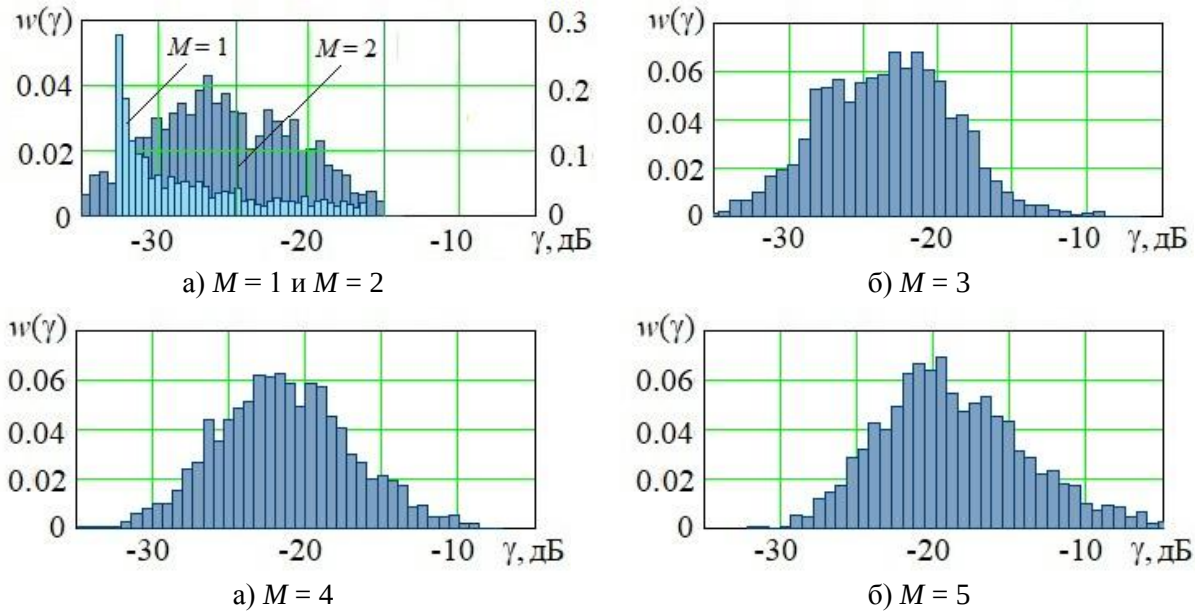
Здесь $w(\gamma)$ это частотность пребывания γ на соответствующем интервале из сорока равных, на которые разбивался полный диапазон (от min до max) разброса значений γ. То есть, если на k-том интервале значение γ наблюдается N_k раз, то $w(\gamma) = N_k / Stat$. Интересно заметить, что, хотя при трех помехах существует критическая ситуация γ = 0 дБ, рис. 5 *в*), однако вероятность возникновения ситуаций не только близких к критической, но даже для таких, которые компенсируются хуже уровня –15 дБ достаточно мала, рис. 6 *б*). Естественно, с ростом числа M источников помех среднематематическое значение уровня компенсации постепенно ухудшается с –27 дБ для одного или пары источников помех до –19 дБ для пяти источников.

3.5. 3*D*-вариант, вероятностные оценки

Изображать объемную ДН с провалами обременительно, а главное – в информационном отношении бессмысленно. Поэтому ограничимся результатами статистического моделирования пространственной обработки при источниках помеховых сигналов, равновероятно возникающих в пределах полусферы. Соответственно, угловые координаты (β_m, θ_m) источников помех задавались генераторами случайных величин, равномерно распределенных на интервале (0, 2π) и распределенных на интервале (0, π/2) с плотностью вероятностей $w(\theta) = \sin(\theta)$, соответственно. Как и в предыдущем подпараграфе, при заданном числе M источников помех статистика набиралась по 1500 ситуациям со случайным их расположением на полусфере. Полученные результаты представлены в табл. 2 и рис. 7. В 3*D* варианте степень компенсации одиночного источника помех зависит от его полярной координаты θ. Поэтому на рис. 7 *а*) приведены две гистограммы, а в табл. 2 добавлена строка $M = 1$.

Таблица 2 – Статистические показатели эффективности γ компенсации

M	min, дБ	max, дБ	mean, дБ	СКО, дБ
1	–33.1	–15.5	–28.0	4.9
2	–37.0	–14.1	–25.9	4.8
3	–35.8	–8.4	–23.9	4.2
4	–36.5	–3.6	–21.7	4.4
5	–33.5	–4.0	–19.0	4.7



а) $M = 1$ и $M = 2$ б) $M = 3$

а) $M = 4$ б) $M = 5$

Рис. 7. Распределение вероятностей параметра γ: *а*) $M = 1$ и $M = 2$; *б*) $M = 3$; *в*) $M = 4$; *г*) $M = 5$

При том, что результаты 3*D* и 2*D* вариантов в общем близки, в варианте 3*D* заметно расширение и смещение вправо зависимостей $w(\gamma)$, т. е. в сторону снижения уровня ослабления. Причина этого ясна. При смещении источника m с экваториальной плоскости, мощность принимаемой от него помехи снижается как $P_m \sin(\theta_m)^2$. *По смыслу целевой функции (3) ясно, что степень ослабления помехи на выходе соответствующего компенсатора тем выше, чем интенсивнее помеха. Поэтому наличие ослабленных «приполярных» источников снижает их вклад в суммарный для M источников эффект компенсации γ. В табл. 2 это проявляется как увеличение дисперсии (значения СКО) по сравнению с табл. 1.

Выводы

1. Обоснована целесообразность применения алгоритма обращения корреляционной матрицы для компенсации помеховых сигналов в ответчике с кольцевой антенной решеткой.

2. Выявлено существование специфических, мало вероятных на практике, комбинаций расположения трех и более источников помех, при которых эффективность пространственной компенсации помех заметно снижается.

3. Предложена нормировка решения как средство повышения реалистичности оценок эффективности компенсации помех.

4. Результаты статистического моделирования установившихся режимов компенсатора помех на базе кольцевой АР из шести кардиоидных элементов подтверждают, возможность ослабления помех в среднем от 27дБ (один или два источника помех) до 19 дБ (пять источников) при соотношении помеха/шум = 10 дБ.

Пространственная компенсация помех достигается за счет формирования в ДН провалов, ориентированных на источники помех. Анализ и оценка вызванного этим сокращения области обнаружения запросных сигналов могут составить предмет наших дальней исследований.

Литература

1. Ирихов А. И., Мармалюков И. М., Москаленко В. И. Отечественные системы и средства государственного опознавания // Вооружение и экономика. 2022. № 3 (61). С. 207-215.

2. Чулюк С. Г. Некоторые аспекты практического применения в радиоэлектронных комплексах вероятностных алгоритмов объединения информации // Радиотехника. 2017. № 8. С. 95-99.

3. Аврамов А. В. Метод и алгоритмы комплексной обработки информации на борту воздушного судна в интересах определения принадлежности целей // Успехи современной радиоэлектроники. 2021. Т. 75, № 1. С. 86-104. DOI 10.18127/j20700784-202101-05.

4. Дардымов А. В., Чони Ю. И. Дофокусировка лучей спутниковой зеркальной антенны при умеренных деформациях рефлектора // Антенны. 2024. № 3. С. 21-28. DOI 10.18127/j03209601-202403-03.

5. Джиган В. И. Цилиндрические адаптивные антенные решетки // Цифровая обработка сигналов. 2023. № 4. С. 18-25.

6. Бойков Т. В., Григорьев Н. С., Тарасенко А. А. Радиоэлектронная борьба над беспилотными летательными аппаратами с воздушного судна // Вестник науки. 2023. Т. 1, № 6 (63). С. 1142-1150.

7. Насонов В. В., Фитасов Е. С., Журавлев И. В. Разработка адаптивных алгоритмов компенсации помех для многофункциональных обзорных радиолокационных станций в условиях воздействия декоррелирующих факторов и нестационарной помеховой обстановки. Ярославль: Ярославский гос. педагогический университет им. К.Д. Ушинского, 2014. 154 с.

8. Метелев С. А. Адаптивная пространственно-временная компенсация помех в каналах радиосвязи: специальность 01.04.03 "Радиофизика": автореф. дисс. … д-ра физ.-мат. наук. Н. Новгород: Научно-исследовательский радиофизический институт.2004. 26 с.

9. Djigan V. "Circular Adaptive Antenna Array," 2021 IEEE East-West Design & Test Symposium (EWDTS), Batumi, Georgia, 2021, pp. 1-5, doi: 10.1109/EWDTS52692.2021.9580987.

10. Семина Е. М., Чони Ю. И. О преобразовании сигнала в комплексно-сопряженный // VII научный форум телекоммуникации: Теория и технологии ТТТ-2024: Материалы XXVI Международной научно-технической конференции, Самара, 06 – 08 ноября 2024 г. – Самара: Поволжский государственный университет телекоммуникаций и информатики, 2024. С. 402-403.

11. Cheng G. and Chen H. "An Analytical Solution for Weighted Least-Squares Beampattern Synthesis Using Adaptive Array Theory," in IEEE Transactions on Antennas and Propagation, vol. 69, no. 9, pp. 6034-6039, Sept. 2021, doi: 10.1109/TAP.2021.3069526.

12. Ganesh A., Charyulu M. L. N. and Kushwah V. S. "Adaptive Space-Air-Ground Integrated Network (SAGIN) Antennas Using Distributed Apertures and AI," 2025 IEEE 17th International Conference on Computational Intelligence and Communication Networks (CICN), Goa, India, 2025, pp. 12-18, doi: 10.1109/CICN67655.2025.11367864.

13. Шилов Н. А. Исследование автокомпенсатора активных шумовых помех // Актуальные исследования. 2021. № 13 (40). С. 6-10.

14. Djigan V. I. "Adaptive Antenna Array for Low Signal-to-Noise Ratio Operation," 2023 Antennas Design and Measurement International Conference (ADMInC), Saint Petersburg, Russian Federation, 2023, pp. 65-68, doi: 10.1109/ADMInC59462.2023.10335198.

15. Tsarik V. I., Bitsulia D. A. and Djigan V. I., "FPGA/ARM Design of Multibeam Adaptive Array for GNSS Receiver," 2024 IEEE East-West Design & Test Symposium (EWDTS), Yerevan, Armenia, 2024, pp. 1-5, doi: 10.1109/EWDTS63723.2024.10873650.

16 He Y., Zhao H., Guo W., Shao S. and Tang Y."Frequency-Domain Successive Cancellation of Nonlinear Self-Interference With Reduced Complexity for Full-Duplex Radios," in IEEE Transactions on Communications, vol. 70, no. 4, pp. 2678-2690, April 2022, doi: 10.1109/TCOMM.2022.3148428.

References

1. Irihov A. I., Marmalyukov I. M., Moskalenko V. I. Otechestvennye sistemy i sredstva gosudarstvennogo opoznavaniya [National systems and means of identification friend-or-foe (IFF)]. *Armament and Economics*, 2022, no. 3 (61), pp. 207-215 (in Russian).

2. Chulyuk S. G. Nekotorye aspekty prakticheskogo primeneniya v radioelektronnykhkompleksakh veroyatnostnykh algoritmov obedineniya informatsii [Some aspects of practical application of probabilistic information fusion algorithms in radio-electronic complexes]. *Radiotekhnika*. 2017. № 8. Pp. 95–99. (In Russian).

3. Avramov A. V. Metod i algoritmy kompleksnoy obrabotki informatsii na bortu vozdushnogo sudna v interesakh opredeleniya prinadlezhnosti tseley [Method and algorithms for integrated information processing on board an aircraft for identifying targets]. *Uspekhi sovremennoi radioelectroniki*, 2021, no. 75 (1), pp. 86-104 (in Russian). DOI: 10.18127/j20700784-202101-05.

4. Dardymov A. V., Choni Yu. I. Dofokusirovka luchey sputnikovoy zerkalnoy antenny pri umerennykh deformatsiyakh reflektora [Refocusing the beams of a satellite reflector antenna under moderate reflector deformations]. *Antenny*, 2024, no. 3 (289), pp. 21-28 (in Russian). DOI: 10.18127/j03209601-202403-03.

5. Dzhigan V. I. Tsilindricheskie adaptivnye antennye reshetki [Cylindrical Adaptive Antenna Arrays]. *Digital Signal Processing*, 2023, no. 4, pp. 18-25 (in Russian).

6. Bojkov T. V., Grigor'ev N. S., Tarasenko A. A. Radioelektronnaya bor'ba nad bespilotnymi letatel'nymi apparatami s vozdushnogo sudna [Airborne electronic warfare against unmanned aerial vehicles (UAVs)]. *Vestnik nauki* [Herald of Science]. 2023, v. 1, no. 6 (63), pp. 1142-1150 (in Russian).

7. Nasonov V. V., Fitasov E. S., Zhuravlev I. V. Razrabotka adaptivnykh algoritmov kompensatsii pomekh dlya mnogofunktsionalnykh obzornykh radiolokatsionnykh stantsiy v usloviyakh vozdeystviya dekorreliruyushchikh faktorov i nestatsionarnoy pomekhovoy obstanovki [Development of adaptive interference compensation algorithms for multifunctional surveillance radar stations under conditions of decorrelating factors and non-stationary interference environment]. Yaroslavl. *Yaroslavskij gosudarstvennyj pedagogicheskij universitet im. K. D. Ushinskogo* [Yaroslavl State Pedagogical University named after K.D. Ushinsky]. 2024. 154 p. (in Russian).

8. Metelev S. A. Adaptivnaya prostranstvenno-vremennaya kompensatsiya pomekh v kanalakh radiosvyazi [Adaptive space-time interference cancellation in radio communication channels. Extended Abstract of D.Sc. Thesis]. Nizhny Novgorod. Research Institute of Radio Physics. 2004. 26 p. (In Russian).

9. Djigan V. I. "Circular Adaptive Antenna Array," 2021 IEEE East-West Design & Test Symposium (EWDTS), Batumi, Georgia, 2021, pp. 1-5, doi: 10.1109/EWDTS52692.2021.9580987.

10. Semina E. M., Choni Yu. I. O preobrazovanii signala v kompleksno-sopryazhennyy [On the conversion of a signal into a complex conjugate]. *VII nauchnyy forum telekommunikatsii: Teoriya i tekhnologii TTT-2024: Materialy XXVI Mezhdunarodnoy nauchno-tekhnicheskoy konferentsii, Samara, 06–08 noyabrya 2024 goda.* [VII Scientific Forum Telecommunications: Theory and Technology TTT-2024: Proceedings of the XXVI International Scientific and Technical Conference, Samara, November 06-08, 2024]. Samara: *Povolzhskij gosudarstvennyj universitet telekommunikacij i informatiki* [Povolzhskiy State University of Telecommunications and Informatics]. 2024. Pp. 402-403 (in Russian).

Cheng G. and Chen H., "An Analytical Solution for Weighted Least-Squares Beampattern Synthesis Using Adaptive Array Theory," in IEEE Transactions on Antennas and Propagation, vol. 69, no. 9, pp. 6034-6039, Sept. 2021, doi: 10.1109/TAP.2021.3069526.

Ganesh A., Charyulu M. L. N. and Kushwah V. S. "Adaptive Space-Air-Ground Integrated Network (SAGIN) Antennas Using Distributed Apertures and AI," 2025 IEEE 17th International Conference on Computational Intelligence and Communication Networks (CICN), Goa, India, 2025, pp. 12-18, doi: 10.1109/CICN67655.2025.11367864.

13. Shilov N. A. Issledovanie avtokompensatora aktivnykh shumovykh pomekh [Study of active noise interference autocompensator]. *Aktualnye issledovaniya* [Actual Research], 2021, no 13 (40), pp.6-10. (in Russian).

Djigan V. I. "Adaptive Antenna Array for Low Signal-to-Noise Ratio Operation," 2023 Antennas Design and Measurement International Conference (ADMInC), Saint Petersburg, Russian Federation, 2023, pp. 65-68, doi: 10.1109/ADMInC59462.2023.10335198.

Tsarik V. I., Bitsulia D. A. and Djigan V. I., "FPGA/ARM Design of Multibeam Adaptive Array for GNSS Receiver," 2024 IEEE East-West Design & Test Symposium (EWDTS), Yerevan, Armenia, 2024, pp. 1-5, doi: 10.1109/EWDTS63723.2024.10873650.

He Y., Zhao H., Guo W., Shao S. and Tang Y. "Frequency-Domain Successive Cancellation of Nonlinear Self-Interference With Reduced Complexity for Full-Duplex Radios," in IEEE Transactions on Communications, vol. 70, no. 4, pp. 2678-2690, April 2022, doi: 10.1109/TCOMM.2022.3148428.

Статья поступила 12 февраля 2026 г.

Информация об авторах

Белов Андрей Сергеевич – соискатель ученой степени кандидата технических наук. Генеральный директор АО «НПО «Радиоэлектроника» им. В.И. Шимко. Область научных интересов: адаптивные антенные решетки; алгоритмы адаптивного приема; фильтры Калмана. Тел.: +7 843 272 55 00. E–mail: info@nposhimko.ru.

Адрес: 420029, Россия, Республика Татарстан, г. Казань, ул. Журналистов, 50.

Чони Юрий Иванович – кандидат технических наук. Профессор кафедры Радиоэлектронных и телекоммуникационных систем Казанского национального исследовательского технического университета им. А.Н. Туполева. Область научных интересов – адаптивные антенные решетки, алгоритмы адаптивного приема, фильтры Калмана. Тел.: +7 843 231 59 14. E–mail: tchoni@rambler.ru.

Адрес: Россия, Республика Татарстан, г. Казань, ул. К.Маркса, 10.

Adaptive algorithms for spatiotemporal processing of request signals of the IFF system

A.S. Belov, Yu.I. Choni

Annotation. Setting the task. *The operability of radio-electronic secondary radar systems, including identification "friend-or-foe" systems, depends on the noise immunity of the request and response channels. It is shown that the main research directions should be directed to the inquiry channel of identification "friend-foe". The use of antenna arrays in receiving signals from the state identification system is investigated.* ***The object of the study.*** *The work examines the ring antenna arrays of the defendants of the state identification.* ***The subject of the study.*** *The subject of the research is algorithms and means of spatial processing of the signal-interference stream received by the antenna array (AR).* ***The purpose of the article*** *is to form a methodological approach to the construction of algorithms for spatiotemporal processing of request signals in the responders of the identification "friend-or-foe" systems and to evaluate the potential characteristics of a noise compensator based on a ring antenna array. Antennas with carotid-type radiation patterns were used in the analysis.* ***The methods used.*** *The main research method is computer simulation of antenna arrays under interference conditions.* ***Results.*** *The results of modeling the radiation patterns of antenna arrays under the influence of one, two and three interference are presented. The simulation results for specific interference situations and statistical estimates for a variety of random situations confirm the effectiveness of spatial processing, which, with a realistic combination of parameters, on average introduces additional interference attenuation by 25dB to 30dB.* ***Practical significance.*** *The scope of application of the results of this article are adaptive antenna arrays of responders of the identification "friend-or-foe" systems, as well as other secondary radar and air traffic control systems.*

Keywords: *interference situation, spatiotemporal processing, adaptation, interference compensation.*

Information about the authors

Andrey Sergeevich Belov – General Director of JSC NPO Radioelectronics named after V.I. Shimko. Field of research – adaptive antenna array, adaptive receive algorithm, Kalman filters. Tel.: +7 843 272 55 00. E–mail: info@nposhimko.ru.

Address: 420029, Russia, Republic of Tatarstan, Kazan, Journalism St., 50.

Choni Yuri Ivanovich – PhD. Professor of the Department of Radioelectronic and Telecommunication Systems of Kazan National Research Technical University named after A.N. Tupolev. Field of research – adaptive antenna array, adaptive receive algorithm, Kalman filters. Tel.: +7 843 231 59 14. E–mail: tchoni@rambler.ru.

Address: 420029, Russia, Republic of Tatarstan, Kazan, K. Marx St., 10.

Для цитирования:

Белов А. С., Чони Ю. И. Адаптивные алгоритмы пространственно-временной обработки запросных сигналов системы госопознавания // Техника средств связи. 2026. № 1 (173). С. 2-13. DOI: 10.24412/2782-2141-2026-1-2-13.

For citation:

Belov A. S., Choni Yu. I. Adaptive algorithms for spatiotemporal processing of request signals of the IFF system. Means of communication equipment, 2026, No. 1 (173), pp. 2-13. (in Russian). DOI: 10.24412/2782-2141-2026-1-2-13.

СИСТЕМЫ СВЯЗИ И ТЕЛЕКОММУНИКАЦИИ

УДК 621.376.9, 004.942, 519.876.5 DOI: 10.24412/2782-2141-2026-1-14-21

Обоснование выбора канального кодера для мультисервисных сверхширокополосных цифровых радиолиний

Деревянкин А. Ю., Путилин А. Н.

Аннотация: *В статье* ***рассматривается задача*** *выбора канального кодера для сверхширокополосных радиолиний, ориентированных на передачу гетерогенного трафика. Анализируются требования к системам кодирования, обусловленные необходимостью одновременной и эффективной передачи потоков данных с различными приоритетами, задержками и требованиями к достоверности (голос, видео, данные датчиков, критичные команды). Проведен сравнительный анализ турбокодов, полярных кодов и кодов с малой плотностью проверок на четность с точки зрения их применимости в мультисервисной среде.* ***Целью работы*** *является обоснование корректности выбора класса квазициклических кодов с малой плотностью проверок на четность как обладающих возможностью перестройки по скоростям кодирования и длинам кодового блока при сохранении большей части структуры алгоритмов кодирования и декодирования, а также формальная постановка задачи выбора оптимальных параметров кодера и декодера квазициклического кода с малой плотностью проверок на четность в зависимости от характеристик используемого канала связи и требований к характеристикам передачи гетерогенного трафика. При* ***моделировании использовался*** *быстрый многопоточный симулятор AFF3CT с библиотекой эффективных алгоритмов цифровой связи, предназначенных для исправления ошибок в цифровом канале связи.* ***Новизна*** *решения состоит в обосновании целесообразности применения структурированных квазициклических кодов с малой плотностью проверок на четность с поддержкой гибридных схем автоматического запроса повторения в силу обеспечения ими гибкости, адаптивности, возможности реализации неравномерной защиты блоков данных.* ***Практическая значимость*** *работы заключается в определении влияния выбора параметров кодера и декодера на ключевые показатели качества обслуживания для различных типов трафика. Результаты работы могут использоваться при разработке аппаратуры передачи данных для радиосвязи.*

Ключевые слова: *качество обслуживания, канальное кодирование, код с малой плотностью проверок на четность, мультисервисный трафик, помехоустойчивость, сверхширокополосный канал.*

Введение

Современные сверхширокополосные (СШП) цифровые радиолинии, занимающие полосу частот от 500 МГц и более [1], все чаще выступают в роли универсальной транспортной среды для широкого спектра приложений: от высокоскоростной передачи файлов и видеоконтента до телеметрии и дистанционного управления робототехническими комплексами. Это формирует мультисервисную среду, где единый физический канал должен обслуживать разнородные потоки данных, каждый из которых предъявляет различные требования к задержке (*latency*), джиттеру, вероятности битовой ошибки (*BER*) и делению потоков данных по приоритетам. В таких условиях выбор канального кодера перестает быть задачей исключительно максимизации помехоустойчивости и становится многокритериальной оптимизационной задачей, решение которой должно учитывать гибкость, адаптивность и возможность дифференцированного обслуживания трафика.

Специфика требований к кодированию в мультисервисных системах передачи данных

Мультисервисный трафик в СШП каналах можно условно разделить на несколько классов, каждый из которых формирует особые требования к системе помехоустойчивого кодирования:

1) Критичный к задержке (ультра-надежный с низкой задержкой): команды управления. Требования: минимальная задержка (до 70 мс), высокая надежность доставки.

2) Чувствительный к пропускной способности: потоковое *HD* видео, телефонная связь, передача больших массивов данных. Требования: высокая или средняя скорость, устойчивость к пакетам ошибок, низкая задержка (видео – до 70 мс, телефон – до 300 мс).

3) Машинный (*IoT/M2M*): данные с датчиков, телеметрия. Требования: низкая скорость обмена, высокая энергоэффективность, возможность работы при низком *SNR*, допускают более высокую *BER*.

Следовательно, идеальный канальный кодер для такой среды должен обладать следующими свойствами:

– гранулярной адаптивностью: возможность плавного и быстрого изменения скорости кодирования (*code rate*) и других параметров в ответ на изменение состояния канала и приоритета текущего потока.
– поддержкой гибридного алгоритма повышения достоверности с переспросом (*HARQ*): эффективная комбинация кодирования с протоколами повторной передачи для баланса между задержкой и надежностью.
– предсказуемой и управляемой задержкой декодирования, особенно для малых длин блоков, критичных для приложений с требованиями по низкому времени задержки.

Сравнительный анализ классов кодеров для мультисервисных систем передачи данных

Несмотря на исторически высокую эффективность, реализованную в стандартах 3*G*/4*G* [2], турбокоды (*turbo codes*) обладают рядом фундаментальных ограничений в контексте мультисервисных СШП систем. Их низкая гибкость, заключающаяся в сложности изменения скорости кода без перестройки структуры интерливера (перемежителя битового потока), затрудняет динамическую адаптацию. Эффект «плато насыщения» ухудшает отдачу при высоких *SNR*, что не оптимально для трафика, требующего экстремально низких *BER*. Задержка декодирования значительна и плохо масштабируется для коротких блоков, а сложность реализации эффективного *HARQ* с инкрементальной избыточностью (*IR-HARQ*) высока.

Полярные коды (*polar codes*), будучи теоретически емкостно – достижимыми и принятыми для каналов управления в 5*G NR* [3], обладают специфическими свойствами. Их врожденная поддержка неравномерной защиты, основанная на принципе поляризации канала, идеально подходит для приоритетной передачи заголовков пакетов и потоков данных с различными требованиями по помехоустойчивости. Однако динамическая адаптация к каналу требует точного и быстрого оценивания *SNR*, что увеличивает общую сложность системы. Производительность для коротких и средних блоков может уступать кодам с низкой плотностью проверок на четность (*LDPC*), что критично для *low-latency* приложений. Существует также компромисс между задержкой и корректирующей способностью: декодирование с последовательным исключением (*SC*) имеет низкую задержку, но умеренную эффективность, тогда как более эффективные списковые декодеры (*SCL*) значительно увеличивают задержку и вычислительную сложность.

Класс *LDPC*-кодов с квазициклической структурой (*QC-LDPC*), ставший доминирующим в стандартах широкополосного беспроводного доступа (*Wi-Fi* 802.11*ac/ax* [4], *DVB-S2*, *DOCSIS* 3.1, а также для каналов данных в 5*G NR* [2]), наиболее полно отвечает вызовам мультисервисности. Их исключительная гибкость обеспечивается стандартизованными семействами кодов, включающими множество предопределенных комбинаций длины блока и скорости кода. Это позволяет мгновенно переключаться между режимами в зависимости от типа трафика. Идеальная совместимость с *IR-HARQ* обусловлена блочной структурой и возможностью генерации дополнительной избыточности «на лету». Ключевым преимуществом является «управляемая задержка декодирования»: количество итераций в итеративном декодере (например, *min-sum*) служит прямым рычагом для компромисса между помехоустойчивостью и

скоростью обработки. Высокая аппаратная эффективность, обеспечиваемая квазициклической структурой, позволяет создавать высокоскоростные конвейерные декодеры на ПЛИС.

Сравнение кодеров по критериям мультисервисной СШП системы передачи данных приведено в табл. 1. На рис. 1 приведена тепловая карта оценок рассматриваемых классов кодов по ключевым критериям. Данные сравнения показывают предпочтительность использования класса *QC-LDPC* кодов для обслуживания мультисервисных потоков данных.

Таблица 1 – Сравнение кодеров по критериям мультисервисной системы передачи данных

Параметр / Критерий	Турбокоды	Полярные коды	*QC-LDPC* коды	Вывод
Эффективность (близость к пределу Шеннона)	Высокая (особенно для средних *SNR*)	Теоретически достижима при бесконечной длине блока	Очень высокая, особенно для длинных блоков и высоких *SNR*	*LDPC* > Турбо ≈ Полярные
Сложность декодера	Высокая (итеративное декодирование с двумя составляющими декодерами, $O(N^2)$.	Зависитот алгоритма: *SC*: $O(N \log N)$, низкая *SCL*: $O(L \cdot N \log N)$, высокая (L – размер списка)	Средняя/Низкая (для *QC-LDPC* благодаря структуре), $O(N \log N)$	*QC-LDPC* < Полярные (*SC*) < Турбо < Полярные (*SCL*)
Задержка декодирования	Высокая (множество итераций, обработка двух составляющих кодов)	*SC*: Низкая (последовательное декодирование) *SCL*: Высокая	Управляемая (зависит от числа итераций, можно сократить для *lowlatency* трафика)	Полярные (*SC*) < *LDPC* < Турбо ≈ Полярные (*SCL*)
Устойчивость к пакетным ошибкам	Средняя/Высокая (зависит от перемежителя)	Низкая/Средняя (чувствительны к структуре ошибок)	Высокая (благодаря длинным блокам и структуре графа Таннера)	*LDPC* > Турбо > Полярные
Гибкость настройки скорости	Низкая (требует изменения структуры кода или интерливера)	Средняя (изменением «замороженных» битов)	Очень высокая (стандартные наборы матриц для разных скоростей, мгновенное переключение)	*LDPC* >> Полярные > Турбо
«Эффект плато» (*error floor*)	Ярко выражен (плато BER при высоких SNR)	Практически отсутствует	Низкий (при правильном дизайне графа)	Полярные > *LDPC* > Турбо
Реализуемость в БМК/ПЛИС	Сложная (требует большой памяти для перемежителя и сложной логики)	*SC*: Простая *SCL*: Сложная (большие списки, память)	Оптимизированная (регулярная структура, конвейерная обработка, готовые IP-ядра)	*LDPC* > Полярные (*SC*) > Турбо > Полярные (*SCL*)

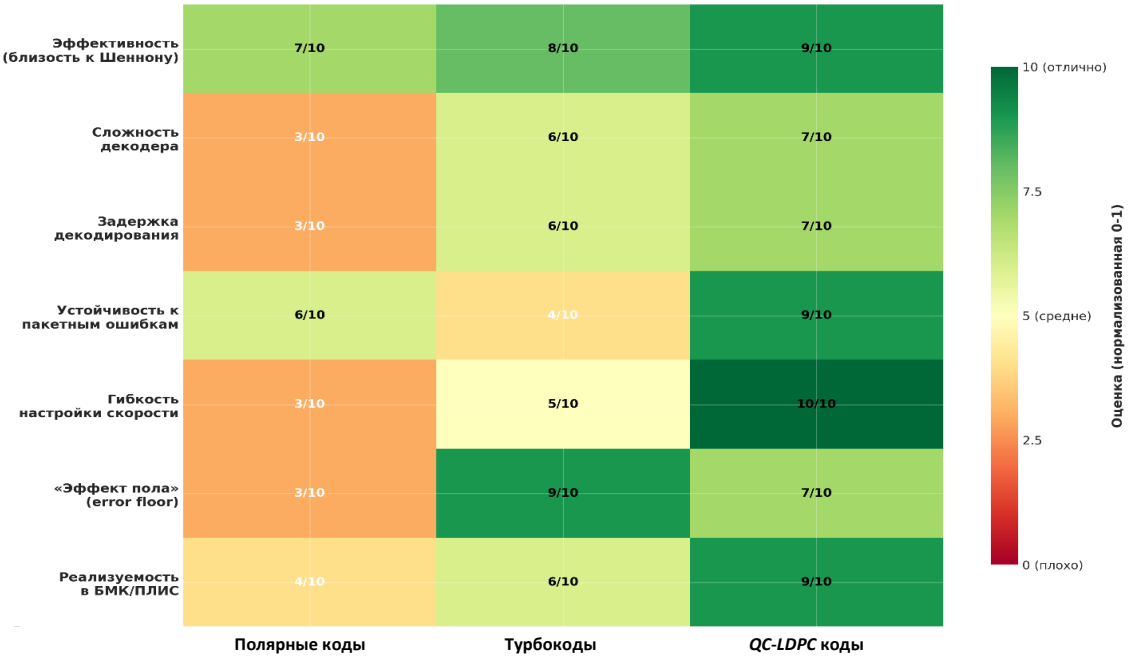


Рис. 1. Тепловая карта оценок классов кодеров для мультисервисных СШП по ключевым критериям

Постановка задачи управления параметрами кодирования и декодирования *QC-LDPC* кода при передаче мультисервисного потока данных и состав стенда моделирования

Рассмотрим систему передачи информации, структура которой отображена в составе стенда моделирования, рис. 2.

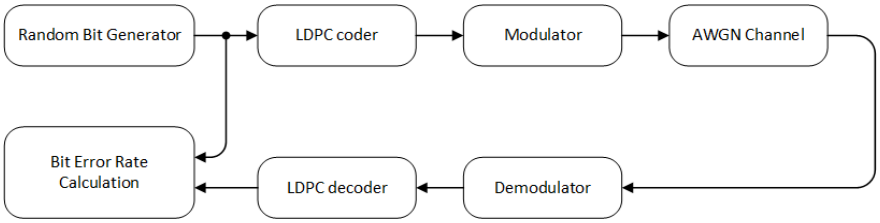


Рис. 2. Структура стенда моделирования рассматриваемой системы передачи данных

В данной структуре реализуется описанный в работе [5] *QC-LDPC* код со следующими параметрами:

n_o – число бит в выходном блоке порождающей матрицы кода;

r – число проверочных бит в порождающей матрице кода;

N – размерность матрицы циклического сдвига кода;

M – размерность перестановочной матрицы кода;

P – размерность базовой единичной матрицы;

B – кратность модуляции, для *QPSK* $B = 2$, для КАМ-16 $B = 4$, для КАМ-64 $B = 6$;

T – длительность посылки сигнала модулятора, с.

Тогда $n = n_oNMP$ – число бит (размер) кодового блока *QC-LDPC* кода;

$K = n - r$ – число (информационных, переменных) бит во входном блоке порождающей матрицы;

$R = k/n = 1 - r/n$ – скорость кода;

$V = BR/T$ – скорость передачи данных.

Обозначим вектор $\bar{a} = (n, r, N, M, P, B, T)$.

Будем полагать, что поток данных передается в канале с белым гауссовским шумом с заданным отношением сигнал/шум *SNR*.

Пусть определены требования по вероятности ошибки на бит P^* и допустимому времени задержки t^* для рассматриваемого сервиса потока данных. Тогда задача управления параметрами кодирования и декодирования *QC-LDPC* кода при передаче данного сервисного потока данных будет формулироваться как задача поиска аргумента

$$\bar{a}^* = \arg\max V(\bar{a}, SNR) \text{ для всех } \bar{a} \in A,$$

где A – область определения вектора $\bar{a}$, при условиях $P(\bar{a}, SNR) < P^*$, $t(\bar{a}, SNR) < t^*$.

Для оценки помехоустойчивости *LDPC* кода в многопоточном симуляторе *AFF3CT* была смоделирована рассматриваемая система передачи данных. Выборка данных для подсчета статистических характеристик рассматриваемой системы составляет 10 000 кодовых блоков. Влияние системы синхронизации не учитывается.

Результаты моделирования

Для мультисервисной СШП системы предлагается архитектура с единым программируемым *QC-LDPC* кодером/декодером, управляемым интеллектуальным диспетчером трафика (*Traffic Shaper/Scheduler*). На основе метаданных потока (класс обслуживания, приоритет) и текущей оценки состояния канала (*CQI*) диспетчер динамически выбирает параметры:

– длину кодового блока (n): короткие блоки (648, 1296) – для *low-latency* трафика; длинные блоки (3888, 15552) – для *high-throughput* трафика;

– скорость кода (*R*) и кратность (вид) модуляции (*QPSK*, 16-*QAM*, 64-*QAM*): адаптивное кодирование и модуляция для максимизации спектральной эффективности;
– число итераций декодирования: минимизация (5-10 итераций) для критичного к задержке трафика; максимизация (20-50 итераций) для трафика, требующего минимальной *BER*.

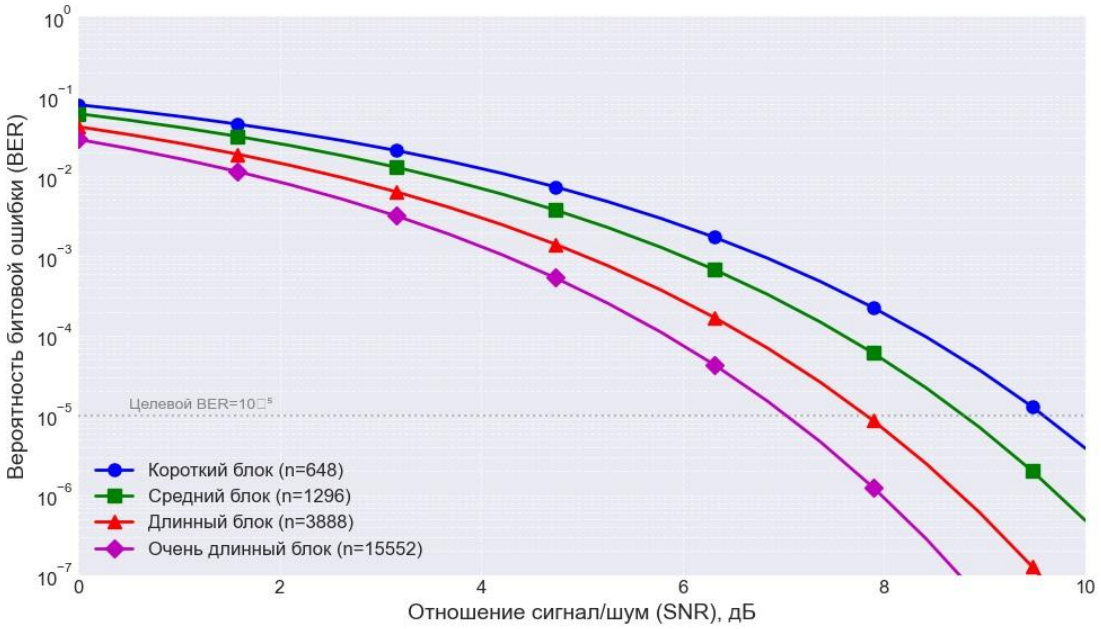


Рис. 3. Влияние длины кодового блока на помехоустойчивость *LDPC*-кодов, *R* = 1/2, *QPSK*

Приведенные на рис. 3 зависимости показывают выигрыш в помехоустойчивости рассматриваемой системы передачи данных при увеличении длины кодового блока. Фактически его длина всегда должна выбираться максимальной при ограничении только двумя факторами: требуемым временем доставки сообщения и возможностью реализации кода на выбранной программно-аппаратной платформе. Приведенные на рис. 4 зависимости подтверждают ключевые преимущества рассматриваемого подхода. Показано, что применение *LDPC*-кодирования обеспечивает выигрыш п помехоустойчивости на 5-7 дБ соответственно смещая пороги переключения кратности модуляции.

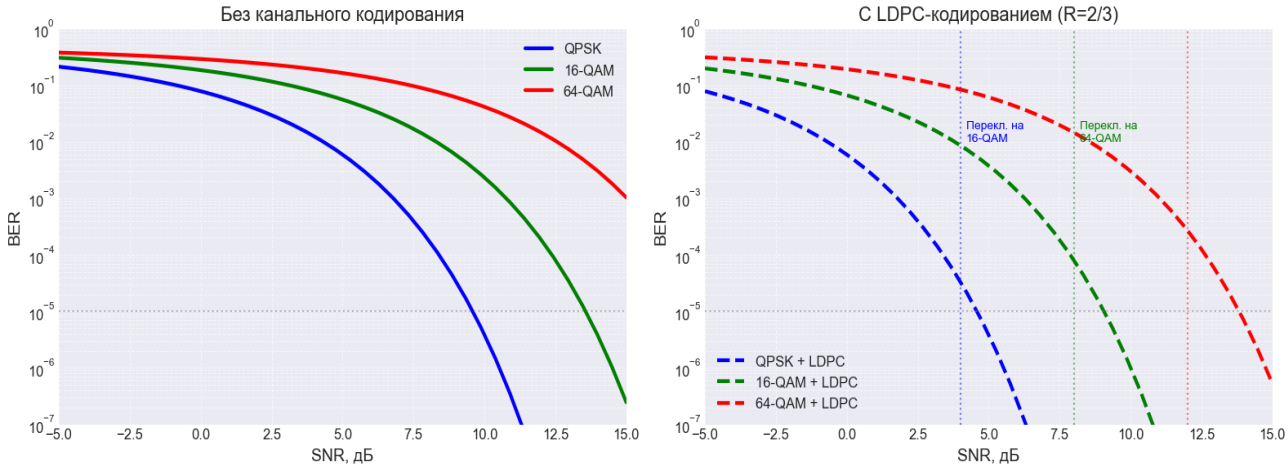


Рис. 4. Помехоустойчивость при различной кратности модуляции с *LDPC* кодом *n* = 1296

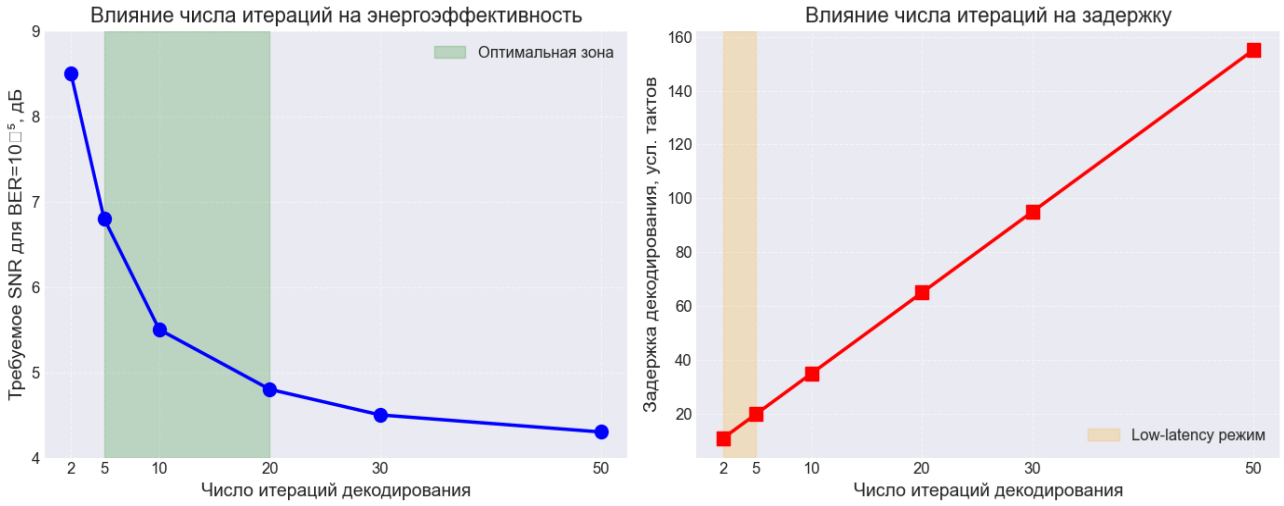


Рис. 5. Компромисс «Задержка декодирования – энергетическая эффективность» для *QC-LDPC* кода при разном числе итераций, n = 1296, R = ¾

На рис. 5 представлен фундаментальный компромисс системы. Для достижения *BER* = 10^{-5} *low-latency* трафик (5 итераций) получает выигрыш в задержке более чем в 2 раза по сравнению с *high-throughput* трафиком (20 итераций), ценой повышения требуемого *SNR* примерно на 1 дБ. Это демонстрирует возможность тонкой настройки кодера под конкретный класс качества обслуживания (*QoS*). Для каждого вида сервиса должна определяться своя точка компромисса.

Аппаратная реализация и производительность

Практическая реализация предложенной архитектуры возможна на современных программируемых системах на кристалле (*SoC*), таких как серия *Zynq UltraScale+ RF SoC* от *AMD*. Наличие специализированного ядра *Soft-Decision Forward Error Correction* (*SD-FEC*) позволяет эффективно реализовать высокоскоростной конвейер декодирования *QC-LDPC* кодов.

Данные табл. 2 показывают, что выбранный подход позволяет достигать информационной скорости декодирования, превышающей 1 Гбит/с, даже для больших кодовых блоков, что соответствует требованиям перспективных СШП систем.

Возможность работы с блоками длиной 15552 бита обеспечивает эффективную передачу пакетов стандартного размера *MTU*.

Таблица 2 – Оценка производительности декодера *QC-LDPC* на платформе *Zynq UltraScale+* (*SD-FEC* 600 МГц, 10 итераций

Длина блока (n)	Скорость (R)	Модуляция	SNR для BER=10⁻⁵	Пропускная способность
648	5/6	64-QAM	9.2 дБ	~1.9 Гбит/с
1296	2/3	16-QAM	6.5 дБ	~1.5 Гбит/с
3888	3/4	64-QAM	7.8 дБ	~2.2 Гбит/с
15552	5/6	256-QAM	11.5 дБ	~2.5+ Гбит/с

Заключение

Проведенный анализ позволяет сделать вывод, что выбор канального кодера для мультисервисной СШП радиолинии должен определяться не только классическими критериями помехоустойчивости, но и комплексом свойств, обеспечивающих гибкое

обслуживание разнородного трафика. Квазициклические LDPC-коды демонстрируют уникальное сочетание высокой корректирующей способности, исключительной адаптивности (реализуемой через мгновенное переключение между предопределенными матрицами), идеальной совместимости с механизмами *IR-HARQ* и управляемой задержкой декодирования. Их способность к динамическому переконфигурированию параметров в реальном времени на основе класса трафика и состояния канала делает их предпочтительным выбором для построения систем, которые должны одновременно удовлетворять противоречивым требованиям *low-latency*, *high-throughput* и *ultra-reliable* коммуникаций в рамках единой СШП радиолинии.

Дальнейшие исследования целесообразно направить на разработку интеллектуальных алгоритмов диспетчеризации, которые на основе машинного обучения будут совместно оптимизировать параметры кодера, модулятора и планировщика, а также на исследование гибридных схем, комбинирующих *QC-LDPC* с иными методами специфических классов трафика.

Литература

1. Галкин В. А. Сверхширокополосные сигналы в цифровой радиосвязи. – Санкт-Петербург: Лань, 2026. – 160 с.

2. IEEE Std 802.11-2020. Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications.

3. 3GPP TS 38.212. NR; Multiplexing and channel coding (Release 17).

4. Richardson T., Kudekar S. Design of Low-Density Parity Check Codes for 5G New Radio // IEEE Communications Magazine. 2018.

5. Путилин А. Н., Шаптала В. С. Выбор системы помехоустойчивого кодирования для сверхширокополосных каналов радиосвязи // Техника средств связи. 2025. № 4. С. 63-37.

References

1. Galkin V. A. Ultra-wideband signals in digital radio communications. St. Petersburg. Lan Publ., 2026, 160 p. (in Russian).

2. IEEE Std 802.11-2020. Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications.

2. 3GPP TS 38.212. NR; Multiplexing and channel coding (Release 17).

3. Richardson T., Kudekar S. Design of Low-Density Parity Check Codes for 5G New Radio. IEEE Communications Magazine. 2018.

5. Putilin, A. N., Shaptala, V. S. Selecting a Noise-Corrective Coding System for Ultra-Wideband Radio Communication Channels. *Means of Communication Equipment*, 2025, No. 4, pp. 63-37 (in Russian).

Статья поступила 20 февраля 2026 г.

Информация об авторах

Деревянкин Андрей Юрьевич – адъюнкт. Военная академия связи им. С.М. Буденного. Область научных интересов: сети передачи данных специального назначения. E-mail: derevjankin-a@mail.ru.

Адрес: 194064, г. Санкт-Петербург, Тихорецкий проспект, д. 3

Путилин Алексей Николаевич – доктор технических наук, профессор, главный научный сотрудник. ПАО «Интелтех». Область научных интересов: передача данных в сетях радиосвязи. Тел.: 8 (812) 448-19-01. E-mail: PutilinAN@inteltech.ru.

Адрес: 197342, Россия, г. Санкт-Петербург, Кантемировская ул., д. 8.

Justification of the choice of a channel coder for multiservice ultra-wideband digital radio lines

A. Y. Derevyankin, A. N. Putilin

Annotation: *This article examines the* ***problem*** *of selecting a channel coder for ultra-wideband radio links designed to transmit heterogeneous traffic. It analyzes the requirements for coding systems, driven by the need to simultaneously and efficiently transmit data streams with different priorities, latencies, and reliability requirements (voice, video, sensor data, critical commands). A comparative analysis of turbo codes, polar codes, and low-density parity-check codes is provided for their applicability in a multiservice environment. The* ***objective*** *of this work is to substantiate the validity of choosing a class of quasi-cyclic low-density parity-check codes capable of varying coding rates and code block lengths while preserving most of the structure of the encoding and decoding algorithms. This work also formally formulates the problem of selecting the optimal encoder and decoder parameters for a quasi-cyclic low-density parity-check code, depending on the characteristics of the communication channel used and the requirements for the transmission characteristics of heterogeneous traffic. The* ***simulation*** *utilized the fast multi-threaded AFF3CT simulator with a library of efficient digital communication algorithms designed to correct errors in a digital communication channel. The* ***novelty*** *of the solution lies in substantiating the feasibility of using structured quasi-cyclic low-density parity-check codes with support for hybrid automatic repeat request schemes due to their flexibility, adaptability, and the ability to implement non-uniform data block protection. The* ***practical significance*** *of this work lies in determining the impact of the choice of encoder and decoder parameters on key quality of service indicators for various types of traffic. The results of this work can be used in the development of data transmission equipment for radio communications.*

Keywords: *ultra-wideband channel, multiservice traffic, channel coding, low-density parity-check code, noise immunity, quality of service.*

Information about the authors

Andrey Yuryevich Derevyankin – postgraduate. Military Academy of Communications. Scientific interests: special-purpose data transmission networks. E-mail: derevjankin-a@mail.ru.

194064, Russia, Saint-Petersburg, Tikhoretsky pr., b. 3.

Aleksej Nikolaevich Putilin – PhD (Tech.), professor, Chief scientific specialist PJSC “Inteltech”, Scientific interests: data transmission in radio network. Tel.: 8(812) 448-19-01 (12-15). E-mail: PutilinAN@inteltech.ru.

Address: Russia, 197342, Saint-Petersburg, Kantemirovskaya st. 8,

Для цитирования:

Деревянкин А. Ю., Путилин А. Н. Обоснование выбора канального кодера для мультисервисных сверхширокополосных цифровых радиолиний // Техника средств связи. 2026. № 1. С. 14-21. DOI: 10.24412/2782-2141-2026-1-14-21.

For citation:

Derevyankin A. Y., Putilin A. N. Justification of the choice of a channel coder for multiservice ultra-wideband digital radio lines. Means of communication equipment, 2026, No. 1 (173), pp. 14-21 (in Russian). DOI: 10.24412/2782-2141-2026-1-14-21.

ВОПРОСЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

УДК 004.056 DOI: 10.24412/2782-2141-2026-1-22-33

Модель функционирования узла связи сети связи общего пользования при возникновении уязвимостей в средствах защиты информации

Черных И. С., Лепешкин О.М.

Аннотация. *Обеспечение устойчивости и безопасности сетей связи общего пользования является ключевой задачей, на решение которой негативно влияют деструктивные программно-аппаратные воздействия, нарушающие нормальное функционирование узлов связи. Традиционно противодействие деструктивным программно-аппаратным воздействиям осуществляется средствами защиты информации и пограничным сетевым оборудованием в момент атаки. Однако эффективность такой защиты снижается, если сами средства защиты или оборудование имеют уязвимости, вызванные некорректной настройкой конфигурации или отсутствием своевременного обновления программных компонентов.* ***Целью работы*** *является разработка модели функционирования узла связи сети связи общего пользования при возникновении уязвимостей в средствах защиты информации открытого сегмента сети передачи данных, позволяющей выявлять уязвимости средств защиты и оборудования, обусловленные ошибками в настройке конфигурации и отсутствием своевременного обновления компонентов, приводящими к ложноотрицательным решениям, рассчитывать траектории перехода узла связи в состояния опасного функционирования для получения вероятностной функции возникновения уязвимостей в средствах защиты и оборудования, проводить количественную оценку вероятности возникновения уязвимостей в открытом сегменте сети передачи данных в процессе функционирования узла связи, а также определять на основе анализа этих траекторий места размещения агентов сетевого контроля.* ***Методы исследования:*** *структурно-функциональный анализ узла связи сети связи общего пользования; имитационное моделирование функционирования узла на основе аппарата сетей Петри; матричный подход исследования структурных свойств графа сети Петри; аппарат линейной алгебры для исследования динамических свойств графа сети Петри с помощью решения задачи достижимости; алгоритм ортогонализации логико-вероятностного метода, преобразующий функции алгебры логики, соответствующие траекториям перехода узла связи в состояния опасного функционирования, в вероятностную функцию возникновения уязвимостей в средствах защиты и оборудовании при функционировании узла связи.* ***Новизна****: использован новый комбинированный подход, объединяющий аппарат сетей Петри и логико-вероятностный метод, для количественной оценки вероятности возникновения уязвимостей средств защиты информации открытого сегмента сети передачи данных узла связи сети связи общего пользования, обусловленных ошибками в настройке конфигурации и отсутствием своевременного обновления компонентов, приводящими к ложноотрицательным решениям средств защиты информации, что позволило получить вероятностную функцию, учитывающую комбинированные сценарии одновременных ложноотрицательных решений нескольких средств защиты.* ***Результат*** *заключается в том, что получены аналитические выражения траекторий перехода узла связи сети связи общего пользования в состояния опасного функционирования при различных комбинациях ложноотрицательных решений средств защиты информации, на основе которых построена вероятностная функция возникновения уязвимостей в открытом сегменте сети передачи данных, позволяющая количественно оценивать защищённость узла связи.* ***Практическая значимость:*** *полученные результаты исследования могут быть использованы для обоснования требований к техническим характеристикам и размещению агентов сетевого контроля при проектировании автоматизированных систем контроля защищенности, а также для поддержки принятия решений должностными лицами служб информационной безопасности.*

Ключевые слова: *вероятностная функция возникновения уязвимости, сеть связи общего пользования, средства защиты информации, траектории перехода в состояния опасного функционирования, узел связи, уязвимость.*

Введение

В современных условиях развития информационно-телекоммуникационной инфраструктуры особую актуальность приобретает проблема обеспечения безопасности сетей связи общего пользования (ССОП). Критически важными элементами сетевой инфраструктуры, обеспечивающими взаимодействие между участниками информационного обмена, являются узлы связи (УС). Уязвимости в системе защиты информации создают серьезные риски для работы сетевых узлов, что может привести к нарушению целостности, конфиденциальности и доступности передаваемых данных. Существующие методы выявления уязвимостей средств защиты информации (СЗИ) зачастую демонстрируют недостаточную эффективность в условиях динамично меняющейся сетевой инфраструктуры и появления новых видов угроз. В виду ряда ограничений традиционные статические подходы к оценке вероятности возникновения уязвимости в системе защиты информации узла фиксируют состояния системы на определённый момент времени, не отражая траекторий перехода узла в состояния опасного функционирования, вызванные цепочками событий или последовательными воздействиями. В связи с этим возникает необходимость в разработке эффективных методов анализа и прогнозирования возможных сценариев перехода сетевого элемента в состояние опасного функционирования. С этой целью требуется разработка модели функционирования УС ССОП при возникновении уязвимости в СЗИ открытом сегменте (ОС) сети передачи данных (СПД).

Постановка задачи

Проанализируем типовую конфигурацию УС, применяемую в ССОП, рис. 1. Подобная архитектура характерна для высококритичных инфраструктур. В их числе — нефтедобыча, промышленные объекты, банки, а также организации госсектора и муниципалитеты. Если рассматривать состав открытого сегмента, то в типовом варианте УС ССОП он формируется из следующего оборудования связи [1, 3, 7]: маршрутизатор *Huawei USG*5520*S*, который обеспечивает подключение узла к *VPN*-сети оператора связи; коммутатор *Ethernet-Huawei CE*6850-*EI Bundle* для включения в сеть оборудования передачи данных открытого сегмента; шлюз *VoIP Yeastar TA*3200,32*FXS* открытого сегмента – для подключения АТС-О к телефонной сети; сервер системы технологического управления *SCADA-SSPI*-2500 выполняющий функции доступа и управления оборудованием ОС; сервер общего назначения открытого сегмента *HPE ProLiant DL*380 *Gen*10 выполняющий технологические функции сервиса времени, домена; АРМ администратора открытого сегмента *HP EliteDesk* 800 *G*6 обеспечивающего возможность настройку оборудования ОС с рабочего места администратора; средства защиты информации, например средство антивирусной защиты (далее САВЗ) *DrWEB Enterprise* для ОСМСВС 3.0, средство защиты от несанкционированного доступа (далее НСД) «КСЗИ от НСД» *Secret Net LSP*, система обнаружения атак (СОА) (изделие СОА-01).

Применение криптомаршрутизатора и межсетевых экранов (МСЭ) позволяет обеспечить высокий уровень криптографической защиты данных, однако для достижения полной безопасности необходимо минимизировать влияние человеческого фактора [1, 2]. Автоматизация процессов в сетях связи не исключает таких рисков, как злоупотребление доверием, внутренние нарушения, внедрение программно-аппаратных закладок и некорректную настройку оборудования [3, 4].

Среди проблем, связанных с функционированием СЗИ, выделяются ложноотрицательные срабатывания — ситуации, при которых реальная угроза не выявляется. Данное явление обусловлено следующими факторами: трудности детектирования ранее неизвестных атак, применение нарушителями методов сокрытия вредоносной активности, а также ограниченные возможности существующих средств анализа угроз [2, 4, 7].

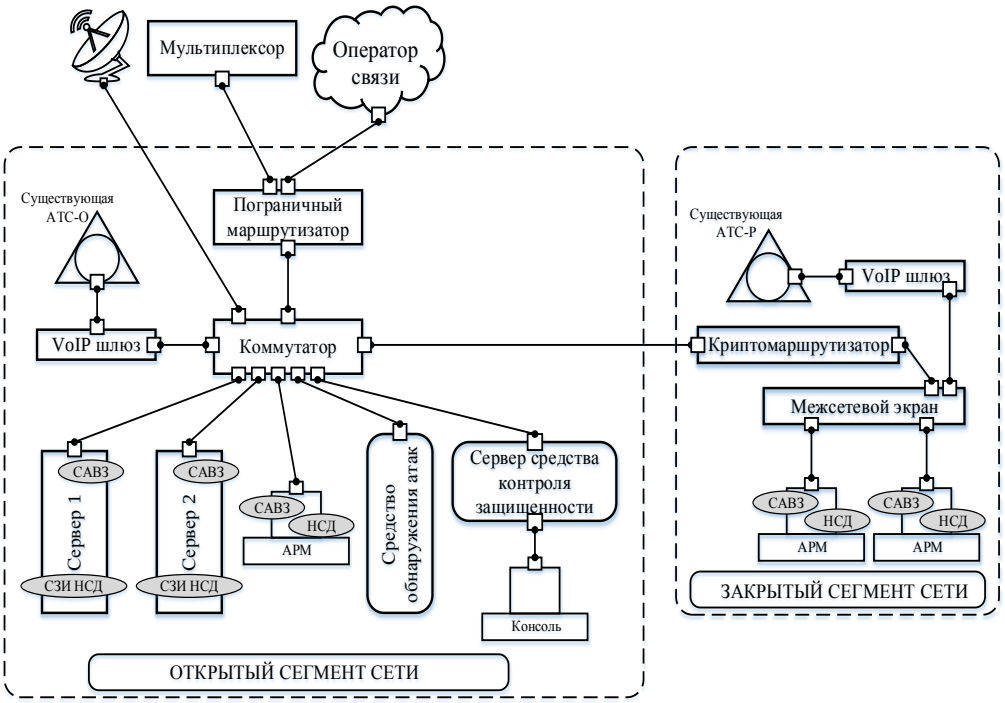


Рис. 1. Узел связи сети связи общего пользования

Особую степень риска несут внутренние нарушители, чьи действия сложно идентифицировать на фоне легитимных операций. В связи с тем, что базовые настройки и алгоритмы функционирования систем устанавливаются людьми, исключить человеческий фактор в полном объеме нельзя [7, 8].

Исходя из всего вышесказанного требуется разработка модели, обеспечивающей формализованный и количественный анализ возможных траекторий перехода УС ССОП в состояния опасного функционирования, для проведения дальнейшего структурно-параметрического синтеза системы контроля защищенности УС от ДПАВ. Вместе с тем позволяющей получить вероятностную функцию возникновения уязвимости, что критически важно для проведения оценки защищенности УС от ДПАВ как объекта критической информационной инфраструктуры (ОКИИ) и в дальнейшем оптимизации его комплекса средств защиты информации [1-3].

2. Описание процесса функционирования узла связи сети связи общего пользования при возникновении уязвимостей в средствах защиты информации открытого сегмента сети передачи данных на первом этапе моделирования в терминах сетей Петри

Выбор сетей Петри в качестве инструмента моделирования на начальном этапе продиктован их способностью к формальному описанию параллельно протекающих и асинхронных процессов, которые являются характерной чертой современных телекоммуникаций [3].

Применение описанного подхода позволяет осуществлять детальное моделирование взаимодействия компонентов УС, определять вероятные траектории смены состояний и выявлять варианты развития событий ведущие к опасному функционированию системы [7, 8].

В ходе начального этапа моделирования было осуществлено графическое представление процесса работы ОС СПД УС ССОП при возникновении уязвимостей в СЗИ. Данное представление реализовано в виде графа сети Петри, рис. 2, с описанием позиций и переходов в табл. 1. В качестве критерия перехода в состояние опасного функционирования приняты ложноотрицательные решения СЗИ ОС СПД УС ССОП [7, 8].

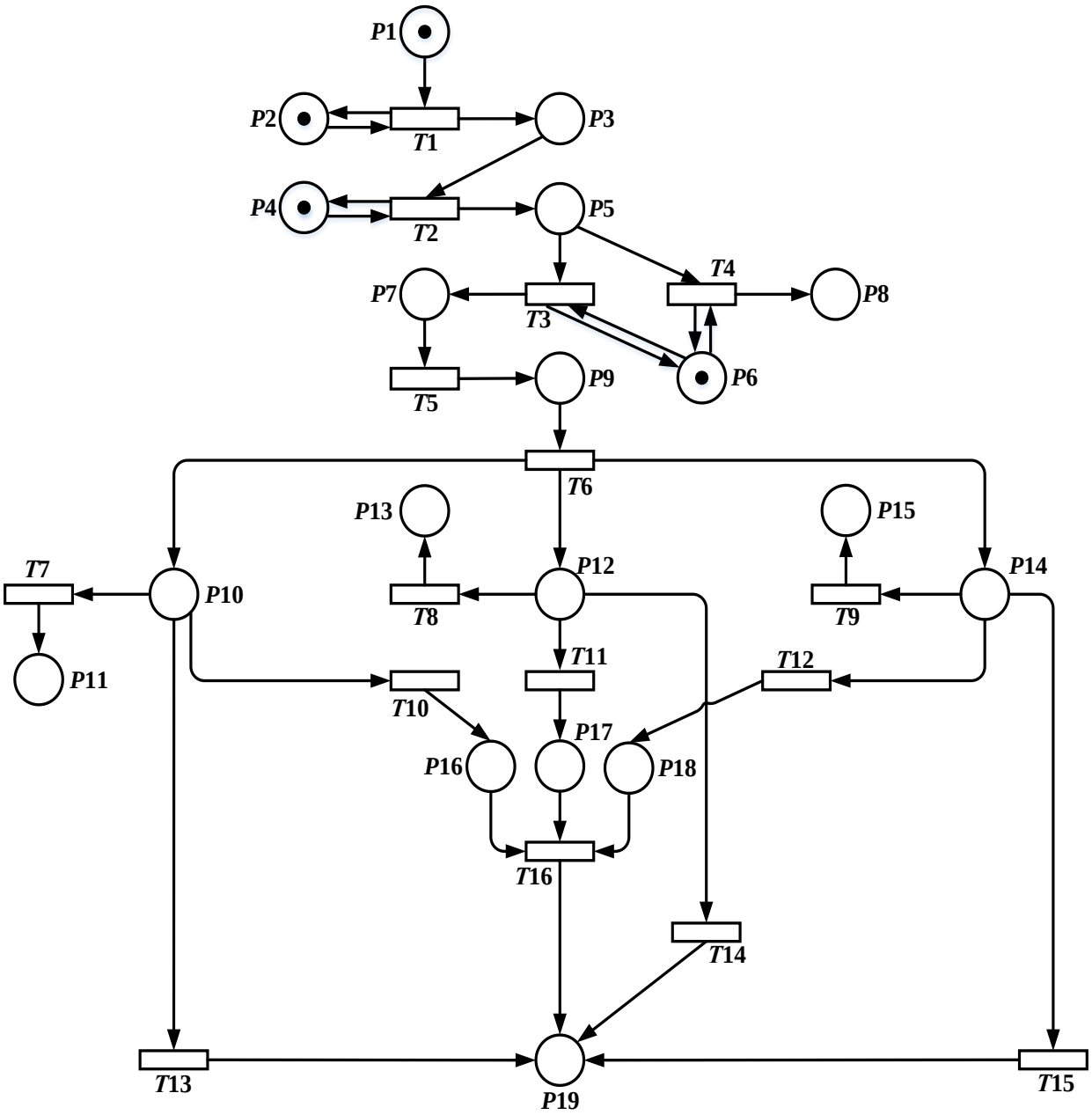


Рис. 2. Формализация процесса функционирования УС ССОП при возникновении уязвимости СЗИ в открытом сегменте сети передачи данных в терминах сетей Петри

Начальное состояние модели функционирования УС ССОП при возникновении уязвимости СЗИ в ОС СПД будет иметь вид:

$$\mu_0=(1101010000000000000). \quad (1)$$

Затем с целью формального представления структуры взаимодействия позиций и переходов топологическая информация, заданная графом, формализуется через матрицу инцидентности (2), которая позволяет выполнить расчет достижимости состояний модели.

В работе использован матричный метод решения задачи о достижимости конечной маркировки [2]. Он опирается на фундаментальное уравнение (3), где $\sigma = t_{j1}\ t_{j2} \ldots t_{jk}$ – вектор срабатываний переходов, обеспечивающий переход от начальной маркировки – μ_k, к итоговой μ_0, C – матрица инцидентности. С его помощью вычислены сценарии развития ОС СПД УС ССОП в опасные режимы функционирования, обусловленные ошибками пропуска угроз со стороны СЗИ.

Таблица 1 – Условия и события возникновения уязвимостей в СЗИ ОС СПД при функционировании УС ССОП

Позиции (условия)	Переходы (события)
*P*1 – наличие соединения ОС к внешней СПД	*T*1 – верификация пакетов на соответствие требованиям
*P*2 – требования фильтрации пакетов установлены	*T*2 – работа агента сетевого контроля
*P*3 – пакет пропущен через предварительную фильтрацию	*T*3 – сопоставление матриц конфигурации МСЭ
*P*4 – сформирована строка матрицы конфигурации	*T*4 – сопоставление матриц конфигурации МСЭ
*P*5 – сформирована матрица текущей конфигурации МСЭ	*T*5 – прохождение трафика в ОС
*P*6 – задана матрица эталонной конфигурации МСЭ	*T*6 – анализ пакета в СЗИ
*P*7 – пакет прошел сравнение конфигураций	*T*7 – отправка пакета в карантин САВЗ
*P*8 – несовпадение матриц (нарушение безопасности связи)	*T*8 – отправка пакета в блокировку СОА
*P*9 – пакет прошел в ОС	*T*9 – блокировка НСД
*P*10 – пакет на анализе в СЗИ САВЗ	*T*10 – принятие правильноотрицательного решения САВЗ
*P*11 – пакет сброшен в карантин СЗИ САВЗ	*T*11 – принятие правильноотрицательного решения СОА
*P*12 – пакет на анализе в СЗИ СОА	*T*12 – принятие правильноотрицательного решения НСД
*P*13 – воздействие обнаружено и заблокировано СЗИ СОА	*T*13 – принятие ложноотрицательного решения САВЗ
*P*14 – попытка НСД	*T*14 – принятие ложноотрицательного решение СОА
*P*15 – попытка НСД заблокирована СЗИ НСД	*T*15 – принятие ложноотрицательного решения СЗИ НСД
*P*16 – правильноотрицательное решение СЗИ АВЗ	*T*16 – правильноотрицательного решение всех трех СЗИ
*P*17 – правильноотрицательное решение СЗИ СОА	
*P*18 – правильноотрицательное решение СЗИ НСД	
*P*19 – пакет прошел проверку СЗИ	

$$C=\begin{Vmatrix}
-1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & -1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & -1 & -1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & -1 & -1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & -1 & -1 & 1
\end{Vmatrix}. \quad (2)$$

$$\mu_k = \mu_0 + \overline{\sigma} C. \quad (3)$$

Присутствие маркеров в позициях *P*10, *P*12, *P*14 сигнализирует о старте обработки поступившего пакета данных СЗИ, что фиксируется соответственно в вершинах графа на рис. 1.

С целью повышения гибкости модели переходы из позиций *P*10, *P*12, *P*14 организованы как независимые узлы ветвления. Из каждой из этих позиций маркер с равной вероятностью направляется по одному из трех маршрутов: к переходам *T*7, *T*8, *T*9, соответствующим сценариям блокировки пакета или его помещения в карантин СЗИ; к переходам *T*10, *T*11, *T*12, представляющим случаи правильноотрицательного решения СЗИ; к переходам *T*13, *T*14, *T*15, соответствующим ситуациям ложноотрицательного решения СЗИ.

Кроме того, модель охватывает все возможные состояния, возникающие в процессе принятия ложноотрицательных и правильноотрицательных решений СЗИ. Для каждого из этих состояний определена соответствующая конечная разметка модели.

В случае, когда всеми тремя СЗИ принимается правильноотрицательное решение, конечная маркировка модели принимает следующий вид (1.1)

$$\mu_1 = (0101000000000000001). \quad (1.1)$$

В случае, когда СЗИ принимает ложноотрицательное решение, конечная маркировка модели принимает следующий вид:

– принятие ложноотрицательного решения САВЗ (1.2)

$$\mu_2 = (0101000000000000111); \quad (1.2)$$

– принятие ложноотрицательного решения СОА (1.3)

$$\mu_3 = (0101000000000001101); \quad (1.3)$$

– принятие ложноотрицательного решения НСД (1.4)

$$\mu_4 = (0101000000000001011); \quad (1.4)$$

– принятие ложноотрицательного решения САВЗ и СОА (1.5)

$$\mu_5 = (0101000000000000102); \quad (1.5)$$

– принятие ложноотрицательного решения САВЗ и НСД (1.6)

$$\mu_6 = (0101000000000000012); \quad (1.6)$$

– принятие ложноотрицательного решения СОА и НСД (1,7)

$$\mu_7 = (0101000000000001002); \quad (1.7)$$

– принятие ложноотрицательного решения НСД, СОА и САВЗ (1,8)

$$\mu_8 = (0101000000000000003). \quad (1.8)$$

3. Применение логико-вероятностного метода на втором этапе моделирования

Подставляя варианты конечных маркировок графа (1.1) – (1.8) в базовое уравнение (3), можно рассчитать траектории перехода ОС УС ССОП в состояния опасного функционирования при ложноотрицательном срабатывании СЗИ. В итоге уравнения принимают следующий вид:

– траектория перехода ОС УС ССОП в состояние опасного функционирования ложноотрицательного решения СЗИ:

$$\overline{\sigma} = t_1 t_2 t_3 t_5 t_6 t_{13} t_{11} t_{12}. \quad (3.1)$$

Чтобы различать траектории, вместо – $\overline{\sigma}$, используем обозначение K_n, тогда запись траектории примет вид:

$$K_1 = t_1 t_2 t_3 t_5 t_6 t_{13} t_{11} t_{12}; \quad (3.2)$$

В ходе дальнейших расчетов траекторий достижения каждой из конечных маркировок (1.3), (1.4), (1.5), (1.6), (1.7), (1.8) получаем:

– вектор последовательности срабатывания переходов в результате ложноотрицательного решения СОА:

$$K_2 = t_1 t_2 t_3 t_5 t_6 t_{14} t_{10} t_{12}; \quad (3.3)$$

– вектор последовательности срабатывания переходов в результате ложноотрицательного решения средством СОА и АВЗ:

$$K_3 = t_1 t_2 t_3 t_5 t_6 t_{13} t_{14} t_{12}; \quad (3.4)$$

– вектор последовательности срабатывания переходов в результате ложноотрицательного решения СЗИ от НСД:

$$K_4 = t_1\, t_2\, t_3\, t_5\, t_6\, t_{15}\, t_{10}\, t_{11}; \quad (3.5)$$

– вектор последовательности срабатывания переходов в результате ложноотрицательного решения средством АВЗ и НСД:

$$K_5 = t_1\, t_2\, t_3\, t_5\, t_6\, t_{13}\, t_{15}\, t_{11}; \quad (3.6)$$

– вектор последовательности срабатывания переходов в результате ложноотрицательного решения средством СОА и НСД:

$$K_6 = t_1\, t_2\, t_3\, t_5\, t_6\, t_{14}\, t_{15}\, t_{10}; \quad (3.7)$$

– вектор последовательности срабатывания переходов в результате ложноотрицательного решения средством АВЗ, СОА и НСД:

$$K_7 = t_1\, t_2\, t_3\, t_5\, t_6\, t_{13}\, t_{14}\, t_{15}. \quad (3.8)$$

4. Получение вероятностной функции возникновения уязвимостей в СЗИ ОС СПД при функционировании УС ССОП на втором этапе моделирования

В качестве математического аппарата для дальнейших расчетов в рамках разрабатываемой модели целесообразно использовать логико-вероятностный метод. Данный метод применительно к анализу структурных отказов, а также к оценке надежности и защищенности технически сложных объектов подробно описан в трудах И. А. Рябинина [1–3].

Благодаря широким возможностям логико-вероятностного метода в части анализа влияния произвольного компонента на надежность, безопасность и защищенность системы в целом, он дает наиболее эффективно применять полученные траектории перехода ОС УС ССОП в состояния опасного функционирования, обусловленные ложноотрицательными срабатываниями СЗИ [4–6].

Полученные аналитические выражения (3.2) – (3.8), используем для получения численного показателя, характеризующего общую вероятность возникновения уязвимости.

Чтобы решить поставленную задачу, используется алгоритм ортогонализации, в основе которого лежит преобразование логических функций в ОДНФ [1, 2].

Отрицание элементарной конъюнкции ранга – r, $K_i = x_1 x_2 \ldots\ldots x_5$ – эквивалентно дизъюнкции члены которой попарно ортогональны (4).

$$K_i = x_1^{a_1'} \vee x_1^{a_1} x_2^{a_2'} \vee \ldots \vee x_1^{a_1} x_2^{a_2} \ldots x_{r\text{-}1}^{a_{r-1}} x_r^{a_r'}. \quad (4)$$

Согласно алгоритму ортогонализации, преобразуем траектории $K_1 - K_7$ к ОДНФ функции с помощью преобразования в матричную форму, она будет иметь вид (4.1):

$$f\left(x_1, x_2, \ldots, x_m\right) = \begin{vmatrix} K_1 \\ K_2 \\ K_3 \\ \ldots \\ K_n \end{vmatrix} = \begin{vmatrix} K_1 \\ K_1' K_2 \\ K_1' K_2' K_3 \\ \ldots \\ K_1' K_2' K_3' K_4' \ldots K_{n\text{-}1}' K_n \end{vmatrix}. \quad (4.1)$$

Исходя из выражения (4.1) определим следующие конъюнкции:

$$K_1' \wedge K_2 = \begin{vmatrix} t_1 t_2 t_3 t_5 t_6 t_{13}' t_{14} t_{10} t_{12} \\ t_1 t_2 t_3 t_5 t_6 t_{13} t_{14} t_{10} t_{11}' t_{12} \end{vmatrix}; \quad (4.2)$$

$$K_1' K_2' \wedge K_3 = \left| t_1 t_2 t_3 t_5 t_6 t_{13} t_{14} t_{10}' t_{11}' t_{12} \right|; \quad (4.3)$$

$$K_1' K_2' K_3' \wedge K_4 = \begin{vmatrix} t_1 t_2 t_3 t_5 t_6 t_{13}' t_{14}' t_{15} t_{10} t_{11} \\ t_1 t_2 t_3 t_5 t_6 t_{13} t_{14}' t_{15} t_{10} t_{11} t_{12}' \\ t_1 t_2 t_3 t_5 t_6 t_{13}' t_{14} t_{15} t_{10} t_{11} t_{12}' \\ t_1 t_2 t_3 t_5 t_6 t_{13} t_{14} t_{15} t_{10} t_{11} t_{12}' \end{vmatrix}; \quad (4.4)$$

$$K_1^{'}K_2^{'}K_3^{'}K_4^{'} \wedge K_5 = \begin{vmatrix} t_1t_2t_3t_5t_6t_{13}t_{14}^{'}t_{15}t_{10}^{'}t_{11}t_{12}^{'} \\ t_1t_2t_3t_5t_6t_{13}t_{14}t_{15}t_{10}t_{11}t_{12}^{'} \end{vmatrix}; \quad (4.5)$$

$$K_1^{'}K_2^{'}K_3^{'}K_4^{'}K_5^{'} \wedge K_6 = \begin{vmatrix} t_1t_2t_3t_5t_6t_{13}t_{14}t_{15}t_{10}t_{11}^{'}t_{12}^{'} \\ t_1t_2t_3t_5t_6t_{13}^{'}t_{14}t_{15}t_{10}t_{11}^{'}t_{12}^{'} \end{vmatrix}; \quad (4.6)$$

$$K_1^{'}K_2^{'}K_3^{'}K_4^{'}K_5^{'}K_6^{'} \wedge K_5 = \left| t_1t_2t_3t_5t_6t_{13}t_{14}t_{15}t_{10}^{'}t_{11}^{'}t_{12}^{'} \right|. \quad (4.7)$$

По формуле суммы вероятностей несовместных событий (5), согласно алгоритму ортогонализации, получим вероятностную функцию (6) возникновения уязвимости в СЗИ ОС СПД при функционировании УС ССОП [1-5].

$$P\left\{ y\left(x_1, ..., x_m \right) = 1 \right\} = R_c = \sum_{i=1}^{s} P\left(W_i \right). \quad (5)$$

где W_i – ортогональные члены функции $y(x_1, x_2, \ldots, x_m)$, записанной в ОДНФ (5.1):

$$y(x_1, x_2, ...x_m) = \bigvee_{i=1}^{n} K_i = \bigvee_{i=1}^{s} W_i, \quad (5.1)$$

$$\begin{aligned} P\{y=1\} = [&R_{13}R_{11}R_{12} + Q_{13}R_{14}R_{10}R_{12} + R_{13}R_{14}R_{10}Q_{11}R_{12} + R_{13}R_{14}Q_{10}Q_{11}R_{12} + Q_{11}Q_{14}R_{15}R_{10}R_{11} + \\ &+ R_{13}Q_{14}R_{15}R_{10}R_{11}Q_{12} + Q_{13}R_{14}R_{15}R_{10}R_{11}Q_{12} + R_{13}R_{14}R_{15}R_{10}R_{11}Q_{12} + \\ &+ R_{13}Q_{14}R_{15}R_{10}R_{11}Q_{12} + R_{13}R_{14}R_{15}Q_{10}R_{11}Q_{12} + R_{13}R_{14}R_{15}R_{10}Q_{11}Q_{12} + \\ &+ Q_{13}R_{14}R_{15}R_{10}Q_{11}Q_{12} + R_{13}R_{14}R_{15}Q_{10}Q_{11}Q_{12}] \times R_1R_2R_3R_5R_6. \end{aligned} \quad (6)$$

5. Определение точности значений вероятности ложноотрицательных решений средствами защиты информации открытого сегмента сети передачи данных узла связи сети связи общего пользования от числа симуляций модели

Если в построенной модели не заданы вероятностные значения для событий (переходов), то, исходя из нормального закона распределения вероятностей, вероятность срабатывания каждого из переходов $T13$; $T14$ и $T15$ составляет 0.16.

С целью установления зависимости точности получения значений вероятности событий принятия ложноотрицательных решений СЗИ (формализованных через срабатывания переходов $T13$; $T14$; $T15$;) от количества симуляций модели составлен график, рис. 3, который показывает, что для практики достаточно 5000 симуляций, что обеспечит статистическую устойчивость результатов вероятностного анализа. Определение количества симуляций разработанной модели, обеспечивающее получение максимально точных значений вероятностей воздействия уязвимостей и срабатывания переходов, дает возможность количественно оценить чувствительность, достоверность, временные характеристики отклика и производительность датчиков при различных сценариях функционирования УС, что обеспечивает объективную верификацию их эффективности в условиях вероятностных воздействий на ОС СПД.

Таким образом, подход, основанный на анализе состояний опасного функционирования объекта при возникновении уязвимостей, траекторий и сценариев перехода в состояния опасного функционирования, а также на установлении зависимости точности получения значений вероятности событий принятия ложноотрицательных решений СЗИ от количества симуляций модели, в дальнейшем позволяет провести структурно-параметрический синтез системы контроля защищенности УС ССОП как объекта критической информационной инфраструктуры от ДПАВ.

Полученная вероятностная функция (6) позволит оценить вероятность возникновения уязвимости в СЗИ ОС СПД при функционировании УС ССОП, до и после применения разработанной в дальнейшем системы контроля защищенности УС ССОП как объекта критической информационной инфраструктуры.

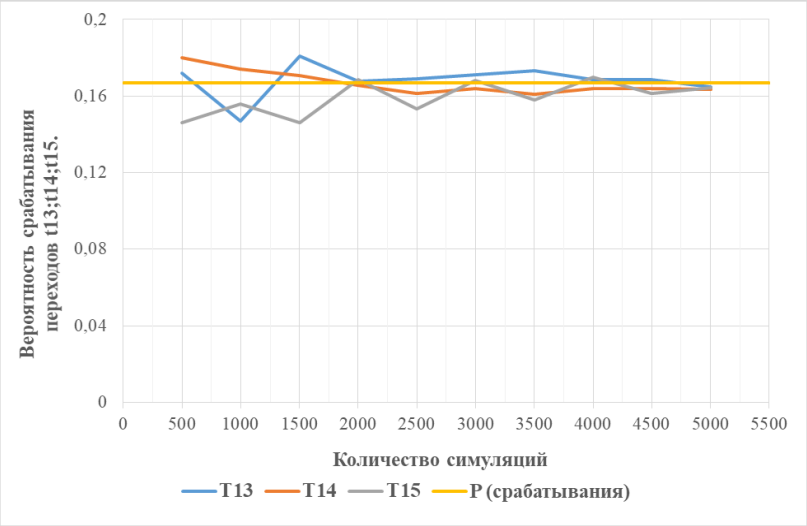


Рис. 3. График зависимости точности значений вероятности ложноотрицательных решений СЗИ от числа симуляций модели

Выводы

В работе содержаться новые научные результаты, обеспечивающие адекватную и теоретически обоснованную оценку вероятности уязвимости объекта защиты с учётом совокупности всех возможных трасс опасного функционирования. Полученные результаты создают основу для повышения эффективности методов анализа и прогнозирования уязвимостей в системах информационной безопасности. Произведена постановка задачи. Предложена модель функционирования УС ССОП при возникновении уязвимостей в СЗИ ОС СПД. Разработанная модель включает в себя несколько этапов моделирования, которые последовательно отражают процесс функционирования объекта защиты при возникновении уязвимостей. На первом этапе осуществляется подробное описание процесса функционирования узла с учётом возможных точек возникновения уязвимостей. На втором этапе производится расчёт траекторий опасного функционирования, что позволяет выявить потенциальные сценарии развития инцидентов. В конечном итоге модель позволяет получить функцию вероятности возникновения уязвимостей, обеспечивая тем самым обратную количественную оценку защищенности узла от ДПАВ. Этот факт будет использован в дальнейшем, для проведения структурно-параметрического синтеза системы контроля защищенности УС ССОП как объекта критической информационной инфраструктуры от ДПАВ.

Полученные результаты могут быть полезны специалистам в области проектирования и оптимизации перспективных систем контроля и мониторинга, обеспечивающих высокий уровень защищенности информационно-телекоммуникационных сетей как объектов критической информационной инфраструктуры от ДПАВ.

Литература

1. Тихонов В. А., Новиков В. А. Верификация систем управления доступом на основе моделирования раскрашенными сетями Петри // Наукоемкие технологии в космических исследованиях Земли. – 2021. – Т.13, №6. – С. 50-59.

2. Рябинин И. А. Надежность и безопасность структурно-сложных систем. СПб.: Политехника, 2000. 248 с.

3. Мараховский В. Б., Розенблюм Л. Я., Яковлев А. В., Моделирование параллельных процессов Сети Петри. СПб.: Профессиональная литература, 2014. 400 с.

4. Burlov V. G., Lepeshkin O. M., Lepeshkin M. O., Gomazov F. A. The control model of safety management systems. IOP Conference Series: Materials Science and Engineering. 8th International Scientific Conference "TechSys 2019" – Engineering, Technologies and Systems. 2019, art. 012088.

5. Пермяков А. С., Лепешкин О. М., Митрофанов М. В. Проблемы защищенности информационно-телекоммуникационных сетей специального назначения // Радиолокация, навигация, связь : сборник трудов XXVI Международной научно-технической конференции. В 6 т. 2020. С. 44-48.

6. Фролов Д. А. Моделирование угроз безопасности в телекоммуникационных сетях средствами сетей Петри // Вестник ЮУрГУ. Компьютерные технологии, управление, радиоэлектроника. 2024. Т. 24, № 4. С. 52-63.

7. Гусев В. Е., Иванов О. Н. Количественная оценка риска информационной безопасности с использованием сетей Петри // Информационные технологии и безопасность. 2023. № 3. С. 112-120.

8. Деньжонков К. А., Чирушкин К. А. Система защиты информации объекта комплексного оснащения узла связи // CyberLeninka: научная электронная библиотека. — URL: https://cyberleninka.ru (дата обращения: 02.02.2026).

9. Kojima Y., Kaji Y., Shioda T. Formal Security Modeling of Cloud Services Using Petri Nets // Proceedings of the 18th International Conference on Network and Service Management. 2024. Pp. 209-214.

10. Deng X., Zhang L., Wang Y., Jiang F. Modeling Analysis of SM2 Construction Attacks in the Open Secure Sockets Layer Based on Petri Net // Sensors. 2022. Vol. 22, no. 4. Art. 1398.

11. Li X., Wang Y., Zhang L. Petri net model for time-delay attack detection in Precision Time Protocol networks // IET Computers & Digital Techniques. 2024. Vol. 18, no. 2. Pp. 157-166.

12. Benabdelhafid M., Merzoug A., Fares M. Hierarchical Colored Petri Nets for Vulnerability Detection in Software Architecture // Proceedings of the 20th International Conference on Informatics in Control Automation and Robotics (ICINCO 2025). 2025. Pp. 345-352.

13. Szpyrka M., Jasiul B. Evaluation of Cyber Security and Modelling of Risk Using Petri Nets for SCADA Systems // Sensors. 2023. Vol. 23, no. 10. Pp. 5421-5438.

14. Jungebloud T., Baumeister D., Schuster R. Model-based structural and behavioral cybersecurity risk analysis via Petri nets // Computers & Security. 2024. Vol. 135. Art. 103283. — DOI: 10.1016/j.cose.2023.103283.

15. Ahmad F., Chaudhry M. T., Jamal M. H., Sohail M. A., Gavilanes D., Vergara M. M., Ashraf I. Formal modeling and analysis of security schemes of RPL protocol using colored Petri nets // PLoS One. 2023. Vol. 18, no. 8. Art. e0285700. — DOI: 10.1371/journal.pone.0285700.

References

1. Tikhonov V. A., Novikov V. A. Verifikatsiya sistem upravleniya dostupom na osnove modelirovaniya raskrashennymi setyami Petri [Verification of Access Control Systems Based on Colored Petri Net Modeling]. *H&ES Research*, 2021, vol. 13, no. 6, pp. 50-59 (in Russian).

2. Ryabinin I. A. *Nadezhnost i bezopasnost strukturno-slozhnykh system* [Reliability and Safety of Structurally Complex Systems]. St. Petersburg. Politekhnika Publ., 2000. 248 p. (in Russian).

3. Marakhovskiy V. B., Rozenblyum L. Ya., Yakovlev A. V. *Modelirovanie parallelnykh protsessov Seti Petri* [Modeling of Parallel Processes. Petri Nets]. St. Petersburg. Professionalnaya literatura Publ., 2014. 400 p. (in Russian).

4. Burlov V. G., Lepeshkin O. M., Lepeshkin M. O., Gomazov F. A. The control model of safety management systems. IOP Conference Series: Materials Science and Engineering: proceedings of the 8th International Scientific Conference "TechSys 2019". *Engineering, Technologies and Systems*, 2019, vol. 618, Art. 012088. — DOI: 10.1088/1757-899X/618/1/012088 (in Russian).

5. Permyakov A. S., Lepeshkin O. M., Mitrofanov M. V. Problemy zashchishchennosti informatsionno-telekommunikatsionnykh setey spetsialnogo naznacheniya [Security Issues of Special-Purpose Information and Telecommunication Networks]. In: *XXVI Mezhdunarodnaya nauchno-tekhnicheskaya konferentsiya "Radiolokatsiya, navigatsiya, svyaz"* [XXVI International Scientific and Technical Conference "Radar, Navigation, Communication"]. In 6 vols. 2020. Pp. 44-48 (in Russian).

6. Frolov D. A. Modelirovanie ugroz bezopasnosti v telekommunikatsionnykh setyakh sredstvami setey Petri [Modeling Security Threats in Telecommunication Networks Using Petri Nets]. *Bulletin of the South Ural State University. Series 'Computer Technologies, Automatic Control, Radio Electronics'*, 2024, vol. 24, no. 4, pp. 52-63 (in Russian).

7. Gusev V. E., Ivanov O. N. Kolichestvennaya otsenka riska informatsionnoy bezopasnosti s ispolzovaniem setey Petri [Quantitative Assessment of Information Security Risk Using Petri Nets]. *Information Technology and Security*, 2023, no. 3, pp. 112-120 (in Russian).

8. Denzhonkov K. A., Chirushkin K. A. Sistema zashchity informatsii ob"ekta kompleksnogo osnashcheniya uzla svyazi [Information Security System of the Integrated Communication Node Facility]. *CyberLenink*a: online repository of scientific publications. Available at: cyberleninka.ru (accessed 02.02.2026) (in Russian).

9. Denzhonkov K. A., Chirushkin K. A. Sistema zashchity informatsii ob"ekta kompleksnogo osnashcheniya uzla svyazi [Information Security System of the Integrated Communication Node Facility]. *CyberLeninka*: scientific electronic library. – URL: https://cyberleninka.ru (accessed: 02.02.2026) (in Russian).

10. Kojima Y., Kaji Y., Shioda T. Formal Security Modeling of Cloud Services Using Petri Nets. *Proceedings of the 18th International Conference on Network and Service Management*, 2024, pp. 209-214.

11. Moradi M., Niknam S., Taheri M. A Petri net model for time-delay attack detection in Precision Time Protocol networks. *IET Computers & Digital Techniques,* 2024, vol. 18, no. 2, pp. 157-166.

12. Benabdelhafid M., Merzoug A., Fares M. Hierarchical Colored Petri Nets for Vulnerability Detection in Software Architecture. *Proceedings of the 20th International Conference on Informatics in Control Automation and Robotics* (*ICINCO* 2025), 2025, pp. 345-352.

13. Szpyrka M., Jasiul B. Evaluation of Cyber Security and Modelling of Risk Using Petri Nets for SCADA Systems. *Sensors*, 2023, vol. 23, no. 10, pp. 5421-5438. — DOI: 10.3390/s23105421.

14. Jungebloud T., Baumeister D., Schuster R. Model-based structural and behavioral cybersecurity risk analysis via Petri nets. *Computers* & *Security*, 2024, vol. 135, Art. 103283. — DOI: 10.1016/j.cose.2023.103283.

15. Ahmad F. Formal modeling and analysis of security schemes of RPL protocol using colored Petri nets. *Computers* & *Security*, 2023, vol. 124, pp. 887-892.

Статья поступила 26 февраля 2026 г.

Информация об авторах

Черных Илья Сергеевич — адъюнкт кафедры безопасности инфокоммуникационных систем специального назначения. Военная академия связи. Область научных интересов: криптографическая защита информации, передаваемой по открытым каналам связи, обеспечение безопасности критически важных объектов систем вязи и управления. SPIN-код автора: 1372-6594. Тел.: +7 911 900 94 34. E–mail: fes90@list.ru.

Лепешкин Олег Михайлович — доктор технических наук, доцент. Профессор кафедры безопасности инфокоммуникационных систем специального назначения. Военная академия связи. Область научных интересов: криптографическая защита информации, передаваемой по открытым каналам связи, обеспечение безопасности критически важных объектов систем вязи и управления. SPIN-код автора: 7916-2190. Тел. +7-905-285-16-49. E–mail: lepechkin1@yandex.ru.

Адрес: 194064, Россия, г. Санкт-Петербург, Тихорецкий проспект, д. 3

Model of Functioning of a Public Communications Network Node under Occurrence of Vulnerabilities in Information Security Tools of the Open Segment of the Data Transmission Network

I. S. Chernykh, O. M. Lepeshkin

Annotation. *Ensuring the stability and security of public communication networks is a key challenge, the solution to which is negatively affected by destructive hardware and software impacts that disrupt the normal functioning of communication nodes. Traditionally, counteraction to destructive hardware and software impacts is carried out by information security tools and edge network equipment at the time of an attack. However, the effectiveness of such protection is reduced if the security tools themselves or the equipment have vulnerabilities caused by incorrect configuration settings or the lack of timely updates of software components.* ***The aim of the work*** *is to develop a model of the functioning of a public communication network node in the event of vulnerabilities in the information security means of the open segment of the data transmission network. The model should allow: identifying vulnerabilities in security means and equipment caused by configuration errors and the lack of timely component updates, leading to false-negative decisions; calculating the transition trajectories of the communication node into states of dangerous operation to obtain a probabilistic function of vulnerability occurrence in security*

means and equipment; conducting a quantitative assessment of the probability of vulnerabilities occurring in the open segment of the data transmission network during the operation of the communication node; and determining, based on the analysis of these trajectories, the placement locations for network monitoring agents. ***Research methods:*** *structural and functional analysis of a public communication network node; simulation modeling of node functioning based on the Petri net apparatus; a matrix approach to studying the structural properties of a Petri net graph; the apparatus of linear algebra for studying the dynamic properties of a Petri net graph by solving the reachability problem; an orthogonalization algorithm of the logical-probabilistic method, which transforms the functions of logic algebra corresponding to the trajectories of the communication node's transition into states of dangerous operation into a probabilistic function of vulnerability occurrence in security means and equipment during the operation of the communication node.* ***Novelty:*** *a new combined approach has been used, integrating the Petri net apparatus and the logical-probabilistic method, for the quantitative assessment of the probability of vulnerabilities occurring in the information security means of the open segment of the data transmission network of a public communication network node. These vulnerabilities are caused by configuration errors and the lack of timely component updates, leading to false-negative decisions of the information security means. This approach has made it possible to obtain a probabilistic function that takes into account combined scenarios of simultaneous false-negative decisions of multiple security means.* ***The result*** *is that analytical expressions have been obtained for the transition trajectories of a public communication network node into states of dangerous operation under various combinations of false-negative decisions of information security means. Based on these expressions, a probabilistic function for the occurrence of vulnerabilities in the open segment of the data transmission network has been constructed, making it possible to quantitatively assess the security of the communication node.* ***Practical significance:*** *the obtained research results can be used to substantiate requirements for the technical characteristics and placement of network monitoring agents when designing automated security control systems, as well as to support decision-making by information security service officials.*

Keywords: *public communications network, communications node, information security tools, vulnerability, trajectories of transition to dangerous functioning states, probabilistic function of vulnerability occurrence.*

Information about the authors

Ilya Sergeevich Chernykh – Postgraduate at the Department of security of special-purpose infocommunication systems. Military Academy of Communications. Research interests: cryptographic protection of information transmitted over open communication channels, ensuring the security of critical objects of communication and control systems. Tel.: +7 911 900 94 34. E-mail: fes90@list.ru

Oleg Mikhailovich Lepeshkin — Dr. habil. Of Engineering Sciences, Docent. Professor of Department of security of special-purpose infocommunication systems. Military Academy of Communications. Research interests: cryptographic protection of information transmitted over open communication channels, ensuring the security of critical objects of communication and control systems. Tel. + 8-905-285-16-49. E-mail: lepechkin1@yandex.ru

Address: 194064, Saint Petersburg, Russia, 3 Tikhoretsky ave.

Для цитирования:

Черных И. С., Лепешкин О. М. Модель функционирования узла связи сети связи общего пользования при возникновении уязвимостей в средствах защиты информации открытого сегмента сети передачи данных // Техника средств связи. 2026. № 1 (173). С 22-33. DOI: 10.24412/2782-2141-2026-1-22-33.

For citation:

Chernykh I. S., Lepeshkin O. M. Model of Functioning of a Public Communications Network Node under Occurrence of Vulnerabilities in Information Security Tools of the Open Segment of the Data Transmission Network. Means of communication equipment, 2026, No. 1 (173), pp. 22-33 (in Russian). DOI: 10.24412/2782-2141-2026-1-22-33.

УДК 004.056.57 DOI: 10.24412/2782-2141-2026-1-34-46

Методика мониторинга нарушений информационной безопасности в компьютерных сетях на основе систематизации множества параметров

Телегин Д. Г., Билятдинов К. З.

Аннотация: *в статье рассматривается оригинальная методика мониторинга нарушений информационной безопасности в компьютерных сетях на основе систематизации множества разнородных параметров, позволяющая повысить точность и оперативность выявления угроз. Актуальность исследования обусловлена стремительным ростом числа кибератак, усложнением их сценариев и необходимостью своевременного обнаружения угроз в условиях динамично изменяющейся сетевой инфраструктуры. Существующие применяемые решения зачастую ориентированы на ограниченный набор индикаторов, что неизбежно снижает эффективность обнаружения комплексных и многоэтапных атак, в том числе направленных на обход традиционных систем защиты.* ***Целью работы*** *является создание алгоритма методики мониторинга нарушений информационной безопасности в компьютерных сетях, позволяющего снизить время выявления потенциальных угроз и нарушений в компьютерных сетях в различных условиях. Комплексная оценка параметров компьютерной сети и формализация процесса мониторинга позволяют повысить точность и оперативность выявления нарушений информационной безопасности. При описании алгоритма методики мониторинга* ***применяется метод*** *анализа. Для достижения цели проведён анализ типовых этапов процесса организации мониторинга нарушений информационной безопасности в компьютерных сетях. Сформирован перечень множеств параметров мониторинга нарушений информационной безопасности, предложена систематизация сформированных множеств параметров, необходимых для мониторинга нарушений информационной безопасности, а также для выявления скрытых взаимосвязей между отдельными организационными этапами мониторинга.* ***Научная новизна*** *исследования заключается в комплексном подходе к систематизации параметров мониторинга нарушений информационной безопасности в компьютерных сетях организации, учитывающем как технические, так и поведенческие факторы.* ***Результат:*** *алгоритм методики мониторинга нарушений информационной безопасности применим для корпоративных и ведомственных сетей, включая объекты критической информационной инфраструктуры и может служить основой для совершенствования систем обнаружения вторжений, SIEM-решений и центров мониторинга информационной безопасности.* ***Практическая значимость*** *алгоритма методики состоит в упорядочении процесса мониторинга нарушений в разнородных, территориально-распределённых компьютерных сетях, находящихся под единым управлением.*

Ключевые слова: *алгоритм методики мониторинга, нарушения информационной безопасности, мониторинг нарушений, систематизация параметров мониторинга, схема алгоритма нарушений.*

Введение

В современных условиях передача данных играет ключевую роль при организации деятельности системы управления органов государственной власти различных уровней и принадлежности. Количественно-качественные показатели правильности, своевременности и актуальности принимаемых управленческих решений во многом зависят от скорости и достоверности массивов данных, передаваемых между управляющими системами, устанавливая требования к недопустимости искажения, хищения или замены информационных потоков [5]. Анализ нормативно-правовых актов, регламентирующих документов и научных публикаций в сфере мониторинга нарушений информационной безопасности (МНИБ) [1 – 23] показал отсутствие методологической основы при организации мониторинга информационной безопасности в компьютерных сетях (КС) органов государственной власти.

Таким образом, *постановка научной задачи исследования* состоит в разработке методики МНИБ в КС (далее – Методика) в интересах обеспечения снижения времени выявления потенциальных угроз и нарушений в компьютерных сетях в различных условиях

путём алгоритмизации организационных процессов и формирования соответствующих требований к специалистам в области защиты информации, отвечающих за процедуры мониторинга и реагирования на нарушения требований информационной безопасности.

Основная часть

Назначение схемы алгоритма методики мониторинга нарушений информационной безопасности (рис.) заключается в упорядочении процессов организации МНИБ в компьютерных сетях, обеспечении снижения времени выявления потенциальных угроз и нарушений в компьютерных сетях в различных условиях путём систематизации множеств параметров мониторинга нарушений информационной безопасности в компьютерных сетях организации (табл.).

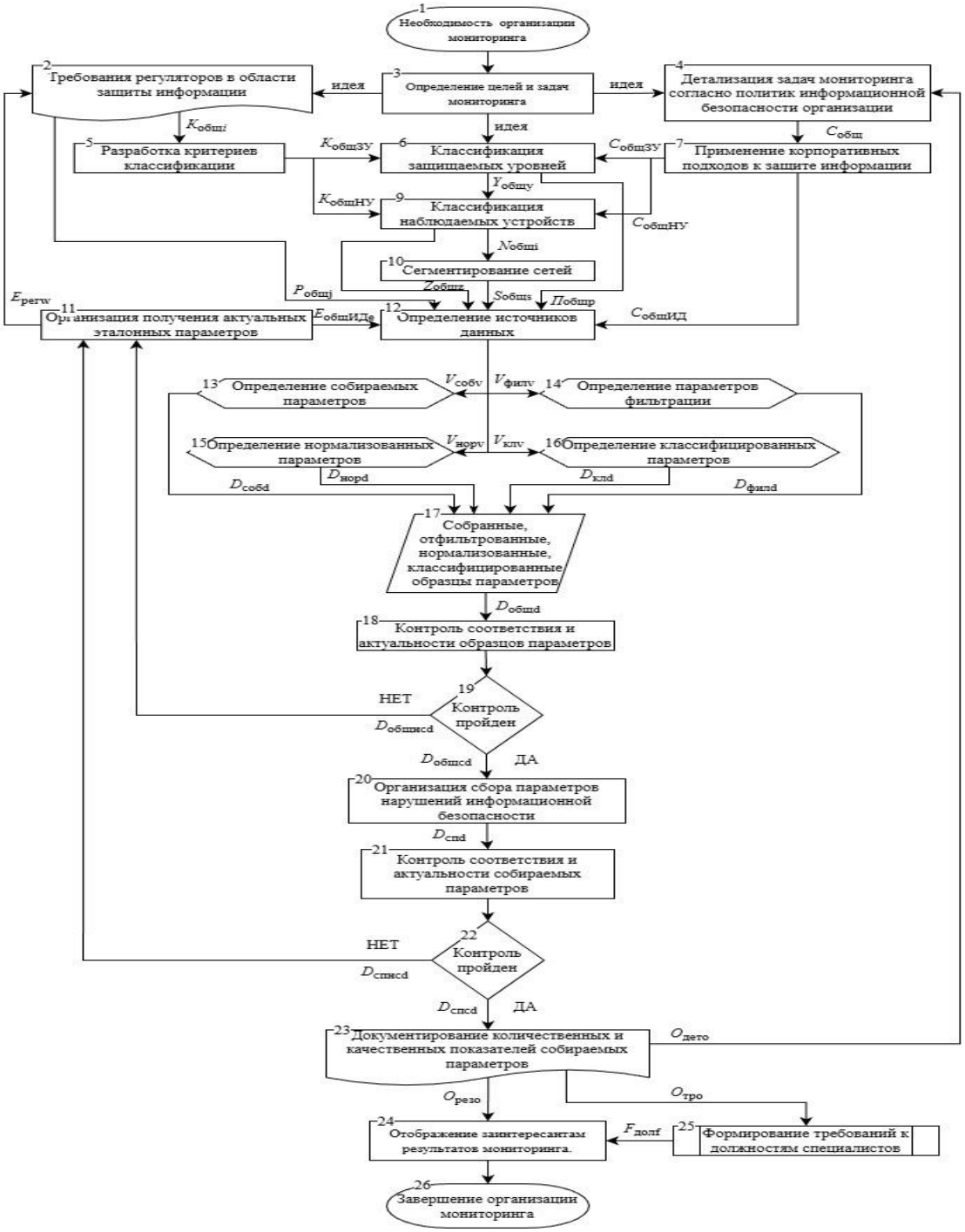


Рис. Схема алгоритма методики мониторинга нарушений информационной безопасности

Таблица – Систематизация множеств параметров мониторинга нарушений информационной безопасности в компьютерных сетях организации

№ п/п	Тип	Наименование	Вход	Выход	Описание
1.	Документ	Требования регуляторов в области защиты информации	Идея	$R_{общ}$	Результат изучения массива документов регуляторов в области защиты информации
				$K_{общi}$	Требования к критериям классификации, сформированные на основание требований регуляторов в области защиты информации
				$P_{общj}$	Требования к источникам данных, сформированные на основание требований регуляторов в области защиты информации
			$E_{регe}$		
2.	Процесс	Разработка критериев классификации	$K_{общi}$	$K_{общЗУ}$	Требования к классификации защищаемых уровней
				$K_{общНУ}$	Требования к классификации наблюдаемых устройств
3.	Процесс	Детализация задач мониторинга согласно политик информационной безопасности организации	Идея	$C_{общ}$	Результат детализации задач мониторинга согласно политик информационной безопасности организации
			$O_{дето}$		
4.	Процесс	Применение корпоративных подходов к защите информации	$C_{общ}$	$C_{общЗУ}$	Требования к классификации защищаемых устройств
				$C_{общНУ}$	Требования к классификации наблюдаемых устройств
				$C_{общИД}$	Требования к определению параметров источников данных
5.	Процесс	Классификация защищаемых уровней	Идея	$L_{общ}$	Ранжирование КС на защищаемые уровни
			$K_{общНУ}$	$Y_{общy}$	Множество устройств защищаемых уровней в КС
			$C_{общЗУ}$	$П_{общp}$	Множество параметров МНИБ защищаемых уровней в КС
6.	Процесс	Классификация наблюдаемых устройств	$K_{общНУ}$	$U_{общ}$	Результат классификации наблюдаемых устройств
			$C_{общНУ}$	$N_{общx}$	Требования к сегментированию КС в зависимости от классификации НУ
			$Y_{общy}$	$Z_{общz}$	Множество параметров МНИБ наблюдаемых в КС устройств
7.	Процесс	Сегментирование сетей	$N_{общx}$	$T_{общ}$	Результат анализа требований к сегментированию КС организации, предъявляемых классификацией ЗУ
				$S_{общs}$	множество параметров МНИБ сегментов КС организации
8.	Процесс	Определение источников данных	$E_{общe}$	$V_{собv}$	Требования к определению собираемых параметров МНИБ в КС организации
			$P_{общj}$	$V_{филv}$	Требования к определению параметров фильтрации
			$Z_{общz}$	$V_{норv}$	Требования к определению нормализованных параметров
			$S_{общs}$		
			$П_{общp}$	$V_{клv}$	Требования к определению классифицированных параметров
			$C_{общИД}$		
9.	Подготовка	Определение собираемых параметров	$V_{собv}$	$D_{собd}$	Собираемые параметры МНИБ в КС организации
10.	Подготовка	Определение параметров фильтрации	$V_{филv}$	$D_{филd}$	Отфильтрованные параметры МНИБ в КС организации
11.	Подготовка	Определение нормализованных параметров	$V_{норv}$	$D_{норd}$	Нормализованные параметры МНИБ в КС организации

№ п/п	Тип	Наименование	Вход	Выход	Описание
12.	Подготовка	Определение классифицированных параметров	$V_{клv}$	$D_{клd}$	Классифицированные параметры МНИБ в КС организации
13.	Данные	Собранные, отфильтрованные, нормализованные, классифицированные образцы параметров	$D_{собd}$ $D_{филd}$ $D_{норd}$ $D_{клd}$	$D_{общd}$	Множество образцов параметров МНИБ в КС организации
14.	Процесс	Контроль соответствия и актуальности образцов параметров	$D_{общd}$	$D_{общсd}$	Множество параметров МНИБ в КС организации, соответствующих образцу
				$D_{общнсd}$	Множество параметров МНИБ в КС организации, несоответствующих образцу
15.	Процесс	Организация сбора параметров нарушений информационной безопасности	$D_{общсd}$	$D_{спd}$	Множество собираемых параметров МНИБ в КС организации
16.	Процесс	Контроль соответствия и актуальности собираемых параметров	$D_{спd}$	$D_{спсd}$	Множество соответствующих и актуальных собираемых параметров МНИБ в КС организации
				$D_{спнсd}$	Множество несоответствующих и (или) неактуальных собираемых параметров МНИБ в КС организации
17.	Процесс	Организация получения актуальных эталонных параметров	$D_{общнсd}$	$E_{общИДе}$	Требования актуальных эталонных параметров к определению источников данных
			$D_{спнсd}$	$E_{регw}$	Требования к запросу актуальных требований регуляторов в области защиты информации
18.	Документ	Документирование количественных и качественных показателей собираемых параметров	$D_{спсd}$	$O_{дето}$	Требования к политикам информационной безопасности организации
				$O_{тро}$	Требования к должностям специалистов в области информационной безопасности организации
				$O_{резо}$	Требования к отображаемым результатам МНИБ в КС организации
19.	Предопределенный процесс	Формирование требований к должностям специалистов	$O_{тро}$	$F_{долf}$	Множество должностных обязанностей специалистов в области информационной безопасности организации

Допущения:

1) в качестве базового состояния информационной безопасности (ИБ) КС рассматривается состояние ИБ КС, при котором отсутствуют угрозы ИБ, воздействующие на систему;
2) в методике рассматривается множество унифицированных, стандартизованных параметров, формируемых устройствами, функционирующими в КС, и устройствами, управляющими КС [1, 3, 4].

Ограничения:

1) методика рассматривается применимо к КС организаций, не затрагивая другие сферы ИБ;
2) методика применима для КС организаций, находящихся под единым управлением;
3) методика предполагает сегментирование компьютерных сетей;
4) методика МНИБ не рассматривает проприетарные протоколы производителей сетевых устройств и сетевого оборудования и не акцентируется на специфических параметрах таких устройств;
5) Методика направлена на обеспечение снижения времени выявления потенциальных угроз и нарушений в компьютерных сетях в различных условиях.

Начальным этапом организации процесса МНИБ в компьютерных сетях организаций выступает фаза определения целей и задач мониторинга. Процесс выполнения этапа определения целей и задач мониторинга основывается на изучении требований регуляторов в области защиты информации, таких как ФСТЭК России [12, 13, 16, 17 ,19], ФСБ России [14, 15], ФСО России [8] применительно к компьютерным сетям организации, документально закрепленных в нормативно-правовых актах [6, 7] и иных документах регуляторов в области информационной безопасности и защиты информации (далее — регуляторы). Математически итоговый результат процесса изучения массива документов ($R_{общ}$), утверждающих наборы требований регуляторов, выражается следующим образом (1):

$$R_{общ} = \{K_{общi}, P_{общj}, i = 1, 2, \ldots, I; j = 1, 2, \ldots, J\}, \quad (1)$$

где

$R_{общ}$ – результат изучения массива документов регуляторов в области защиты информации (ЗИ);

$K_{общi}$ – требования к критериям классификации, сформированные на основание требований регуляторов в области ЗИ;

$P_{общj}$ – требования к источникам данных, сформированные на основание требований регуляторов в области ЗИ;

i – количество требований к критериям классификации;

j – количество требований к источникам данных.

Требования к критериям классификации ($K_{общ}$) представляет собой сумму требований к критериям классификации определяемых регуляторами (2):

$$K_{общ} = \sum_{k=1}^{m} K_{1k} + \sum_{k=1}^{m} K_{2k} + .. + \sum_{k=1}^{m} K_{nk}, \quad (2)$$

где K_{1k} – требования к критериям классификация первого регулятора в области ЗИ;

K_{2k} – требования к критериям классификация второго регулятора в области ЗИ;

K_{nk} – требования к критериям классификация n-го регулятора в области ЗИ.

Следовательно, требования предъявляемые к критериям классификации и определённые одним регулятором представляют собой одномерный массив данных (3):

$$[K_1 \quad K_2 \quad \ldots \quad K_k], \quad (3)$$

где K_1 – первое требование, предъявляемое к критериям классификации;

K_2 – второе требование, предъявляемое к критериям классификации;

K_k – k-ое требование, предъявляемое к критериям классификации.

На основании требований к критериям классификации, сформированных согласно требованиям регуляторов в области ЗИ, формируются требования к классификации защищаемых уровней ($K_{общЗУ}$) и требования к классификации наблюдаемых устройств ($K_{общНУ}$).

На втором этапе определения целей и задач мониторинга, независимо от вида или типа организации необходимо детализировать задачи МНИБ согласно политик информационной безопасности, принятых в организации. Результат применения политик информационной безопасности в КС организации имеет следующий вид (4).

$$C_{общ} = \sum_{c=1}^{m} C_{1c} + \sum_{c=1}^{m} C_{2c} + .. + \sum_{c=1}^{m} C_{nc}, \quad (4)$$

где $C_{общ}$ – результат детализации задач мониторинга согласно политик информационной безопасности организации;

C_{1k} – требования первой политики информационной безопасности;

C_{2k} – требования второй политики информационной безопасности;

C_{nk} – требования n-ой политики информационной безопасности.

При этом, требования, предъявляемые одной политикой информационной безопасности к передаче информации внутри КС, выражаются в виде (5):

$$[C_1 \quad C_2 \quad \ldots \quad C_c], \quad (5)$$

где C_1 – первое требование политики информационной безопасности;

C_2 – второе требование политики информационной безопасности;

C_c – c-ое требование политики информационной безопасности.

В результате применения корпоративных подходов по защите информации в компьютерных сетях организаций так же формируются требования к классификации защищаемых уровней ($C_{\text{общЗУ}}$), требования к классификации наблюдаемых устройств ($C_{\text{общНУ}}$) и требования к определению параметров источников данных ($C_{\text{общИД}}$).

Третьим этапом определения целей и задач МНИБ в КС организации выступает процесс классификации защищаемых уровней компьютерных сетей организации. Ранжирование КС на защищаемые уровни ($L_{\text{общ}}$) включает в себя суммарное применение требований к классификации защищаемых уровней сформированных, согласно требований регуляторов в области ЗИ ($K_{\text{общЗУ}}$) и требований к классификации защищаемых уровней, определенных корпоративными подходами к защите информации передаваемой в КС организации ($C_{\text{общЗУ}}$) (6).

$$L_{\text{общ}} = K_{\text{общЗУ}} + C_{\text{общЗУ}} . \quad (6)$$

Результат применения операции сложения вышеуказанных требований классификации защищаемых уровней в КС организации представляется множеством следующего вида (7):

$$L_{\text{общ}} = \{\text{У}_{\text{общ}y}, \text{П}_{\text{общ}p}, y = 1, 2, \ldots, Y; p = 1, 2, \ldots, P\}, \quad (7)$$

где $\text{У}_{\text{общ}y}$ – множество устройств защищаемых уровней в КС;

$П_{\text{общ}p}$ – множество параметров МНИБ защищаемых уровней в КС;

y – количество наблюдаемых устройств защищаемых уровней в КС;

p – количество параметров нарушений информационной безопасности (НИБ) защищаемых уровней в КС.

Классификацию наблюдаемых устройств (НУ) ($U_{\text{общ}}$) необходимо проводить на основании полученных ранее множества и требований, а именно (8):

1) требований к критериям классификации НУ, сформированных согласно требованиям регуляторов, в области ЗИ ($K_{\text{общНУ}}$);
2) требований к критериям классификации НУ, сформированных согласно применения корпоративных подходов к ЗИ ($C_{\text{общНУ}}$);
3) множество устройств защищаемых уровней в КС ($У_{\text{общ}i}$).

$$U_{\text{общ}} = K_{\text{общНУ}} + C_{\text{общНУ}} + \text{У}_{\text{общ}i}. \quad (8)$$

Сформированная классификация наблюдаемых устройств предъявляет соответствующее множество требований последующим процессам (9):

$$U_{\text{общ}} = \{N_{\text{общ}x}, Z_{\text{общ}z}, \ x = 1, 2, \ldots, X; \ z = 1, 2, \ldots, Z\}, \quad (9)$$

где $N_{\text{общ}x}$ – требования к сегментированию КС в зависимости от классификации НУ;

$Z_{\text{общ}z}$ – множество параметров МНИБ наблюдаемых в КС устройств;

x – количество защищаемых сегментов КС;

z – количество параметров НИБ наблюдаемых в КС устройств.

В результате анализа требований к сегментированию КС организации, проведенного на основе классификации наблюдаемых устройств, определятся множество параметров МНИБ сегментов КС (10).

$$T_{\text{общ}} = \{S_{\text{общ}s}, s = 1, 2, \ldots, S\}, \quad (10)$$

где $T_{\text{общ}}$ – результат анализа требований к сегментированию КС организации, предъявляемых классификацией ЗУ;

$S_{\text{общ}s}$ – множество параметров МНИБ сегментов КС организации;

s – количество параметров НИБ сегментов КС организации.

При первоначальном определении источников данных ($V_{\text{общ}}$) для систем мониторинга нарушений ИБ в КС организации необходимо анализировать полученные ранее требования и множества (11):

1) требования к источникам данных, сформированные на основание требований регуляторов в области ЗИ ($P_{\text{общ}j}$);
2) множество параметров МНИБ наблюдаемых в КС устройств ($Z_{\text{общ}z}$);

3) множество параметров МНИБ сегментов КС организации ($S_{общs}$);
4) множество параметров МНИБ защищаемых уровней в КС ($П_{общр}$);
5) требования к определению параметров источников данных, сформированные согласно применения корпоративных подходов к ЗИ ($C_{общИД}$).

$$V_{общ} = P_{общi} + Z_{общz} + S_{общs} + П_{общр} + C_{общИД}. \quad (11)$$

В свою очередь источники данных определяют требования к данным, собираемых ($V_{собv}$), отфильтрованных ($V_{филv}$), нормализованных ($V_{норv}$), классифицированных ($V_{клv}$) параметров МНИБ в КС организации.

Собираемые параметры МНИБ в КС организации ($D_{собd}$) являются суммой параметров мониторинга источников данных в КС организации (12):

$$D_{собd} = \sum_{d=1}^{m} D_{1d} + \sum_{d=1}^{m} D_{2d} + .. + \sum_{d=1}^{m} D_{nd}, \quad (12)$$

где $D_{собd}$ – собираемые параметры МНИБ в КС организации;
D_{1d} – собираемые параметры МНИБ в КС организации первого источника данных;
D_{2d} – собираемые параметры МНИБ в КС организации второго источника данных;
D_{nd} – собираемые параметры МНИБ в КС организации «*n*»-го источника данных.

При этом, собираемые параметры МНИБ в КС от одного источника данных, выражаются одномерным массивом вида (13):

$$[D_1 \quad D_2 \quad .. \quad D_d], \quad (13)$$

где D_1 – первый собираемый параметр МНИБ в КС организации;
D_2 – второй собираемый параметр МНИБ в КС организации;
D_d – *d*-ый собираемый параметр МНИБ в КС организации.

В свою очередь собираемые параметры мониторинга можно представить в виде двумерного массива данных (14):

$$D_{собd} = \begin{bmatrix} D_{11} & D_{12} & .. & D_{1d} \\ D_{21} & D_{22} & & D_{2d} \\ & & & \\ D_{n1} & D_{n2} & & D_{nd} \end{bmatrix}, \quad (14)$$

где D_{11} – первый собираемый параметр МНИБ в КС организации первого источника данных;
D_{21} – первый собираемый параметр МНИБ в КС организации второго источника данных;
D_{n1} – первый собираемый параметр МНИБ в КС организации «*n*»-го источника данных.

Отфильтрованные параметры МНИБ в КС организации ($D_{филd}$) являются произведением фильтрующей функций с суммой собранных параметров МНИБ в КС организации (15):

$$D_{филd} = f_{m-n} * \sum_{d=1}^{m} D_{собd}, \quad (15)$$

где f_{m-n} – функция фильтрации параметров МНИБ в КС организации;
m – конечный параметр фильтрации применяемый при МНИБ в КС организации;
n – начальный параметр фильтрации применяемый при МНИБ в КС организации.

Нормализованные параметры МНИБ в КС организации ($D_{норd}$) являются произведением нормализующей функции с суммой отфильтрованных параметров МНИБ в КС организации (16):

$$D_{норd} = f_{m-n} * \sum_{d=1}^{m} D_{филd}, \quad (16)$$

где f_{m-n} – функция нормализации параметров МНИБ в КС организации;
m – конечный параметр нормализации применяемый при МНИБ в КС организации;
n – начальный параметр нормализации применяемый при МНИБ в КС организации.

Классифицированные параметры МНИБ в КС организации ($D_{клd}$) являются произведением классифицирующей функции с суммой нормализованных параметров МНИБ в КС организации (17):

$$D_{клd} = f_{m-n} * \sum_{d=1}^{m} D_{норd}, \quad (17)$$

где f_{m-n} – функция классификации параметров МНИБ в КС организации;

m – конечный параметр классификации применяемый при МНИБ в КС организации;

n – начальный параметр классификации применяемый при МНИБ в КС организации.

Функции фильтрации, нормализации и классификации определяются требованиями к данным собираемых, отфильтрованных, нормализованных, классифицированных параметров МНИБ в КС организации.

Собранные, отфильтрованные, нормализованные и классифицированные образцы параметров образуют множество образцов параметров МНИБ в КС организации ($D_{\text{общ}d}$) (18).

$$D_{\text{общ}d} = \{D_{\text{соб}d}, D_{\text{фил}d}, D_{\text{нор}d}, D_{\text{кл}d} \;\; d = 1, 2, \dots, D\}, \quad (18)$$

где d – количество образцов параметров МНИБ в КС организации.

Множество образцов параметров МНИБ в КС организации после сбора подвергается процессу контроля на соответствие и актуальность образцам, в результате прохождения которого вышеуказанное множество приобретает вид (19):

$$D_{\text{общ}d} = \{D_{\text{общсd}}, D_{\text{общнсd}}, \;\; d = 1, 2, \dots, D\}, \quad (19)$$

где $D_{\text{общсd}}$ – множество параметров МНИБ в КС организации, соответствующих образцу;

$D_{\text{общнсd}}$ – множество параметров МНИБ в КС организации, несоответствующих образцу.

Множество параметров МНИБ в КС организации, несоответствующих образцу выступает одним из двух факторов, определяющих требования для организации процесса получения актуальных эталонных параметров ($E_{\text{общe}}$).

На основании полученного множества параметров МНИБ в КС организации, соответствующих образцу, выполняется процесс организации сбора параметров НИБ в КС организации, результатом которого является множество собираемых параметров МНИБ в КС организации ($D_{\text{спd}}$).

Сформированное множество собираемых параметров МНИБ в КС организации проходит через процедуру контроля соответствия и актуальности собираемых параметров, результатом которого выступает следующее множество (20):

$$D_{\text{спd}} = \{D_{\text{спсd}}, D_{\text{спнсd}}, \;\; d = 1, 2, \dots, D\}, \quad (20)$$

где $D_{\text{спсd}}$ – множество соответствующих и актуальных собираемых параметров МНИБ в КС организации;

$D_{\text{спнсd}}$ – множество несоответствующих и (или) неактуальных собираемых параметров МНИБ в КС организации.

Множество несоответствующих и (или) неактуальных собираемых параметров МНИБ в КС организации, выступает вторым фактором, определяющим требования для организации процесса получения актуальных эталонных параметров.

Результатом процесса организации получения актуальных эталонных параметров является получение требований актуальных эталонных параметров к определению источников данных ($E_{\text{общИДe}}$) и требований к запросу актуальных требований регуляторов в области ЗИ ($E_{\text{регw}}$) (21):

$$E_{\text{общe}} = \{E_{\text{общИДe}}, E_{\text{регw}}, \;\; e = 1, 2, \dots, E; \; w = 1, 2, \dots, W\}, \quad (21)$$

где e – количество актуальных эталонных параметров МНИБ в КС организации для определения источника данных;

w – количество параметров МНИБ в КС организации для запроса актуальных требований регуляторов в области ЗИ.

Принимая во внимание полученные в ответ на сформированный запрос актуальные требования регуляторов в области ЗИ необходимо изменить требования к критериям классификации, сформированные ранее на их основание. Величина изменения ($\triangle K_{\text{общ}}$) будет определяться разностью между требованиями к критериям классификации полученными от регуляторов в области ЗИ на первичном этапе ($K_{\text{общП}}$) и требованиями к критериям классификации полученными после уточняющего запроса ($K_{\text{общУ}}$) регуляторам в области ЗИ (22):

$$\Delta K_{\text{общ}} = K_{\text{общП}} - K_{\text{общУ}}, \quad (22)$$

Первичные результаты процесса определения источников данных (11) необходимо изменить с учётом полученных требований актуальных эталонных параметров к определению источников данных (23):

$$V_{\text{общ}} = P_{\text{общ}i} + Z_{\text{общ}z} + S_{\text{общ}s} + \Pi_{\text{общ}p} + C_{\text{общИД}} + E_{\text{общИД}e}, \quad (23)$$

Документирование количественных и качественных показателей собираемых параметров своим итогом определяет требования к политикам информационной безопасности организации ($O_{\text{дето}}$), требования к должностям специалистов в области информационной безопасности организации ($O_{\text{тро}}$) и требования к отображаемым результатам МНИБ в КС организации ($O_{\text{резо}}$).

Требования к политикам информационной безопасности организации оказывают изменяющее воздействие на детализацию задач мониторинга, а значит и на результат детализации задач мониторинга согласно политик информационной безопасности организации (4). Величина изменения ($\triangle C_{\text{общ}}$) будет определяться разностью между результатами детализации задач мониторинга согласно политик информационной безопасности организации полученными на первичном этапе ($C_{\text{общП}}$) и результатами детализации задач мониторинга согласно политик информационной безопасности организации полученными после уточнения ($C_{\text{общУ}}$) (24):

$$\Delta C_{\text{общ}} = C_{\text{общП}} - C_{\text{общУ}}, \quad (24)$$

Предопределенный процесс формирования требований к специалистам по информационной безопасности организации зависит от требований к должностям специалистов в области информационной безопасности организации полученных после процесса документирования количественных и качественных показателей собираемых параметров НИБ в КС организации. Результатом выполнения данного предопределенного процесса будет множество должностных обязанностей специалистов в области информационной безопасности организации ($F_{\text{долf}}$).

Отображаемый заинтересантам результат МНИБ в КС организации строится на требованиях к отображаемым результатам МНИБ в КС организации и множеств параметров должностных обязанностей специалистов в области информационной безопасности организации.

Выводы

Разработанная методика МНИБ в КС позволяет обеспечить снижение времени выявления потенциальных угроз и нарушений в компьютерных сетях в различных условиях за счёт алгоритмизации организационных процессов и формирования требований к должностям специалистов в области защиты информации, отвечающих за процедуры мониторинга и реагирования на нарушения требований информационной безопасности.

Проведённая систематизация множеств параметров мониторинга нарушений информационной безопасности в компьютерных сетях организации позволяет оперативно проводить изменения контролируемых параметров учитывая постоянно совершенствующиеся угрозы нарушений ИБ компьютерных сетей [5], повышая их защищенность за счёт снижения времени выявления таких угроз и реагирования на них.

Таким образом, в заключении вполне обоснованно можно сформулировать следующее:

1) Научная новизна Методики основывается на применении систематизации множеств параметров мониторинга нарушений информационной безопасности в компьютерных сетях организации, табл.;
2) Теоретическая значимость Методики состоит в разработке алгоритма мониторинга нарушений информационной безопасности в компьютерных сетях организаций, рис.;
3) Практическая значимость Методики состоит в снижения времени выявления потенциальных угроз и нарушений в компьютерных сетях в различных условиях.

Литература

1. Стригунов В.В. Введение в компьютерные сети. Хабаровск: ТОГУ, 2016. – 103 с.
2. ГОСТ Р 59547-2021 Защита информации. Мониторинг информационной безопасности. – М.: Российский институт стандартизации, 2021. – 14 с.
3. Бородко А. В., Кукунин Д. С. Компьютерные сети передачи данных. Часть 1. Учебн. пособ. – СПб.: СПбГУТ, 2013. – 195 с.
4. Сиротко С. И., Волосевич А. А. Компьютерные сети: учебн. пособ. – Минск: БГУИР, 2006. – 95 с.
5. Aslan Ö., Aktu˘ g. S.S., Ozkan-Okay M., Yilmaz A.A., Akin E. A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions. *Electronics*, 2023, vol. 1333, no. 12, pp. 1-42.
6. Указ Президента Российской Федерации от 22.05.2015 г. № 260 «О некоторых вопросах информационной безопасности Российской Федерации». – URL: http://www.kremlin.ru/acts/bank/39718 (дата обращения: 19.11.2025).
7. Федеральный закон Российской Федерации от 12.07.2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации». – URL: https://www.consultant.ru/document/cons_doc_LAW_220885/ (дата обращения: 18.11.2025).
8. Приказ ФСО России от 07.09.2016 г. № 443 «Об утверждении Положения о российском государственном сегменте информационно-телекоммуникационной сети «Интернет». – URL: http://publication.pravo.gov.ru/document/0001201610170008?index=1 (дата обращения: 20.11.2025).
9. ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения. – М.: Стандартинформ, 2009. – 11 с.
10. ГОСТ 19.701-90 Схемы алгоритмов, программ, данных и систем. Обозначения условные и правила выполнения. – М.: Стандартинформ, 2010. – 158 с.
11. ГОСТ Р ИСО/МЭК 27001-2021 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования. – М.: Российский институт стандартизации, 2021. – 23 с.
12. Методический документ ФСТЭК России. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных: утв. 14.02.2008. – URL: https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodika-ot-14-fevralya-2008-g (дата обращения: 21.11.2025).
13. Методический документ ФСТЭК России. Методика оценки угроз безопасности информации: утвержден 05.02.2021. – URL: https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-5-fevralya-2021-g (дата обращения: 21.11.2025).
14. Приказ ФСБ России от 11 мая 2023 г. № 213 «Об утверждении порядка осуществления мониторинга защищенности информационных ресурсов, принадлежащих федеральным органам исполнительной власти, высшим исполнительным органам государственной власти субъектов Российской Федерации, государственным фондам, государственным корпорациям (компаниям), иным организациям, созданным на основании федеральных законов, стратегическим предприятиям, стратегическим акционерным обществам и системообразующим организациям российской экономики, юридическим лицам, являющимся субъектами критической информационной инфраструктуры Российской Федерации либо используемых ими». – URL: http://publication.pravo.gov.ru/document/0001202306020020 (дата обращения: 19.09.2025).
15. Приказ ФСБ России от 18 марта 2025 г. № 117 «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений, с использованием шифровальных (криптографических) средств». – URL: http://publication.pravo.gov.ru/document/0001202503260008 (дата обращения: 22.11.2025).
16. Приказ ФСТЭК России от 11.02.2013 г. № 7 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах». – URL: https://base.garant.ru/70391358/ (дата обращения: 22.11.2025).
17. Приказ ФСТЭК России от 11.02.2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных». – URL: https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-18-fevralya-2013-g-n-21 (дата обращения: 28.11.2025).

18. Приказ ФСТЭК России от 25.12.2017 г. № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» (в ред. приказов ФСТЭК России от 09.08.2018 г. № 138, от 26.03.2019 г. № 60, от 20.02.2020 г. № 35, от 28.08.2024 г. № 159). – URL: https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-25-dekabrya-2017-g-n-239 (дата обращения: 29.11.2025).

19. Таненбаум Э., Фимстер Н., Эузеролл Д. Компьютерные сети. – СПб.: Питер, 2025. – 992 с.

20. Олифер В. Г., Олифер Н. А. Компьютерные сети. Принципы, технологии, протоколы: юбилейное издание, дополненное и исправленное. – СПб.: Питер, 2025. – 1008 с.

21. Буторин Д. Н., Пак Н. И., Бархатова Д. А., Левин А. А., Панова А. М. Компьютерные сети: учебник для вузов. – СПб.: Лань, 2025. – 304 с.

22. Нечаев А. М., Трубин А. Е., Анисимов А. Ю. Компьютерные сети: учебник и практикум для среднего профессионального образования. – М.: Юрайт, 2025. – 515 с.

23. Максимов Н. В., Попов И. И. Компьютерные сети. Интернет: учебное пособиею – М.: Форум, 2024. – 464 с.

References

1. Strigunov V. V. *Vvedenie v kompyuternie seti* [Introduction to Computer Networks]. Khabarovsk, Pacific National University, 2016. 103 p. (in Russia).

2. State Standard R 59547-2021 Information Protection. Information Security Monitoring. Moscow, Russian Institute of Standardization, 2021. 14 p. (in Russia).

3. Borodko A. V., Kukunin D. S. *Kompyuternie seti peredachi dannikh. Chast 1*. [Computer Data Networks. Part 1]. St. Petersburg, Bonch-Bruevich Saint Petersburg State University of Telecommunications, 2013. 195 p. (in Russia).

4. Sirotko S. I., Volosevich A. A. *Kompyuternie seti* [Computer Networks]. Minsk, Belarusian State University of Informatics and Radioelectronics. 2006. 95 p. (in Russian).

5. Aslan Ö., Aktu˘ g. S.S., Ozkan-Okay M., Yilmaz A.A., Akin E. A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions. Electronics, 2023, vol. 1333, no. 12, pp. 1-42.

6. Decree of the President of the Russian Federation of May 22, 2015 no. 260 «On Certain Issues of Information Security of the Russian Federation». Available at: http://www.kremlin.ru/acts/bank/39718 (accessed 19.11.2025).

7. The federal law of the Russian Federation of July 12, 2017 no. 187-FZ «On the Security of Critical Information Infrastructure of the Russian Federation». Available at: https://www.consultant.ru/document/cons_doc_LAW_220885 (accessed 18.11.2025).

8. Order of the FSO of Russia of September 7, 2016 no. 443 «On Approval of the Regulations on the Russian State Segment of the Information and Telecommunication Network «Internet»». Available at: http://publication.pravo.gov.ru/document/0001201610170008?index=1 (accessed 20.11.2025).

9. State Standard R 53114-2008 Information Protection. Ensuring Information Security in an Organization. Basic Terms and Definitions. Moscow, Standartov Publ., 2009. 11 p. (in Russia).

10. State Standard 19.701-90 Schemes of Algorithms, Programs, Data and Systems. Conditional Designations and Execution Rules. Moscow, Standartov Publ., 2010. 158 p. (in Russia).

11. State Standard R ISO/IEC 27001-2021 Information Technology. Methods and Means of Ensuring Security. Information Security Management Systems. Requirements. Moscow, Russian Institute of Standardization, 2021. 23 p. (in Russia).

12. Methodological Document of FSTEC of Russia. Methodology for Determining Actual Threats to Personal Data Security during their Processing in Personal Data Information Systems. February 14, 2008. Available at: https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodika-ot-14-fevralya-2008-g (accessed 21.11.2025).

13. Methodological Document of FSTEC of Russia. Methodology for Assessing Information Security Threats. February 5, 2021. Available at: https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-5-fevralya-2021-g (accessed 21.11.2025).

14. Order of the FSB of Russia of May 11, 2023 no. 213 «On Approval of the Procedure for Monitoring the Security of Information Resources Belonging to Federal Executive Bodies, Higher Executive Bodies of State Power of the Subjects of the Russian Federation, State Funds, State Corporations (Companies), Other Organizations Created on the Basis of Federal Laws, Strategic Enterprises, Strategic Joint-Stock

Companies and Backbone Organizations of the Russian Economy, Legal Entities that are Subjects of the Critical Information Infrastructure of the Russian Federation or Used by Them». Available at: http://publication.pravo.gov.ru/document/
0001202306020020 (accessed 19.09.2025).

15. Order of the FSB of Russia of March 18, 2025 no. 117 «On Approval of the Requirements for Protecting Information Contained in State Information Systems, Other Information Systems of State Bodies, State Unitary Enterprises, State Institutions, Using Encryption (Cryptographic) Means». Available at: http://publication.pravo.gov.ru/document/0001202503260008 (accessed 22.11.2025).

16. Order of the FSTEC of Russia of February 11, 2013 no. 17 «On Approval of the Requirements for Protecting Information Not Constituting State Secrets Contained in State Information Systems». Available at: https://base.garant.ru/70391358 / (accessed 22.11.2025).

17. Order of the FSTEC of Russia of February 11, 2013 No. 21 «On Approval of the Composition and Content of Organizational and Technical Measures to Ensure the Security of Personal Data during their Processing in Personal Data Information Systems». Available at: https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-18-fevralya-2013-g-n-21 (accessed 28.11.2025).

18. Order of the FSTEC of Russia of December 25, 2017 no. 239 «On Approval of the Requirements for Ensuring the Security of Significant Objects of the Critical Information Infrastructure of the Russian Federation" (as amended by Orders of the FSTEC of Russia of August 9, 2018 no. 138, March 26, 2019 no. 60, February 20, 2020 no. 35, August 28, 2024 no. 159)». Available at: https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-25-dekabrya-2017-g-n-239 (accessed 29.11.2025).

19. Tanenbaum A. S., Fimster N., Wetherall D. *Computer Networks: 6th edition*. London, Pearson, 2020. 944 p.

20. Olifer V. G., Olifer N. A. *Kompyuternie seti. Printsipi, tekhnologii, protokoli: yubileinoe izdanie, dopolnennoe i ispravlennoe* [Computer Networks. Principles, Technologies, Protocols: anniversary edition, revised and updated]. St. Petersburg, Piter Publ., 2025. 1008 p. (in Russia).

21. Butorin D. N., Pak N. I., Barkhatova D. A., Levin A. A., Panova A. M. *Kompyuternie seti* [Computer Networks]. St. Petersburg, Lan Publ., 2025. 304 p. (in Russia).

22. Nechaev A. M., Trubin A. E., Anisimov A. Yu. *Kompyuternie seti* [Computer Networks]. Moscow, Yurait Publ., 2025. 515 p. (in Russia).

23. Maksimov N. V., Popov I. I. *Kompyuternie seti. Internet.* [Computer Networks. Internet]. Moscow, Forum Publ., 2024. 464 p. (in Russia).

Статья поступила 08 января 2026 г.

Информация об авторах

Телегин Данила Григорьевич – адъюнкт. ФГБОУ ВО «Санкт-Петербургский университет государственной противопожарной службы министерства Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий имени Героя Российской Федерации генерала армии Е.Н. Зиничева». Область научных интересов: информационная безопасность, защита информации. E-mail: windowsrt31@mail.ru.

Адрес: 196105, Россия, Санкт-Петербург, Московский пр-кт, д. 149,

Билятдинов Камиль Закирович – доктор технических наук, доцент. Профессор. ФГАОУ ВО «Санкт-Петербургский государственный университет аэрокосмического приборостроения». Область научных интересов: управление сложными системами в условиях неблагоприятных воздействий внешней среды, информационная безопасность отечественных систем связи и автоматизированных систем управления. E-mail: k74b@mail.ru.

Адрес: 190000, Россия, Санкт-Петербург, ул. Большая Морская, д. 67, лит. А,

A methodology for monitoring information security violations in computer networks based on the systematization of a variety of parameters

D. G. Telegin, K. Z Biliatdinov

Annotation: *the article examines an original methodology for monitoring information security violations in computer networks based on the systematization of dissimilar parameters variety, which allows improving the accuracy and efficiency of threat detection. The relevance of the research is due to the rapid growth in the number of cyber-attacks, the increasing complexity of their scenarios, and the need for timely threat detection in a dynamically changing network infrastructure. Existing solutions often focus on a limited set of indicators, which inevitably reduces the effectiveness of detecting complex and multi-stage attacks, including those aimed at bypassing traditional protection systems. The objective of the work is to create a methodology algorithm for monitoring information security violations in computer networks, which allows reducing the time required to detect potential threats and violations in various network conditions. A comprehensive assessment of computer network parameters and formalization of the monitoring process enhance the accuracy and efficiency of detecting information security violations. The methodology monitoring algorithm description employs the analysis method. To achieve the goal, an analysis of typical stages in the organization of information security violation monitoring in computer networks was conducted. A list of information security monitoring parameter sets was formed, and a systematization of these parameters necessary for monitoring information security violations was proposed. This includes identifying hidden relationships between individual monitoring organizational stages. The scientific novelty of the research lies in the comprehensive approach to systematizing information security monitoring parameters in organizational computer networks, taking into account both technical and behavioral factors. The developed information security monitoring methodology algorithm is applicable to corporate and departmental networks, including critical information infrastructure facilities. The proposed methodology can serve as a basis for improving intrusion detection systems, SIEM solutions, and information security monitoring centers. Applying the information security monitoring methodology algorithm will streamline the monitoring organization process in dissimilar, geographically distributed computer networks under unified management.*

Keywords*: information security breaches, monitoring methodology algorithm, monitoring parameters systematization, violation algorithm diagram, violation monitoring.*

Information about the authors

Telegin Danila Grigorievich. — Postgraduate. Saint Petersburg University of State Fire Service of the Ministry of the Russian Federation for Civil Defense, Emergencies and Elimination of Consequences of Natural Disasters named after Hero of the Russian Federation Army General E.N. Zinichev. Research interests: information security, information protection. E-mail: windowsrt31@mail.ru.

Address: Russia, Saint- Petersburg, Moskovsky Avenue, 149, 196105.

Biliatdinov Kamil Zakirovich — Dr. habil. of Engineering Sciences, Docent. Associate Professor at Saint Petersburg State University of Aerospace Instrumentation. Research interests: control of complex systems under adverse environmental conditions, information security of domestic communication systems and automated control systems. E-mail: k74b@mail.ru.

Address: Russia, Saint-Petersburg, Bolshaya Morskaya Street, 67A, 190000.

Для цитирования:

Телегин Д. Г., Билятдинов К. З. Методика мониторинга нарушений информационной безопасности в компьютерных сетях на основе систематизации множества параметров // Техника средств связи. 2026. № 1 (173). С. 34-46. DOI: 10.24412/2782-2141-2026-1-34-46.

For citation:

Telegin D. G., Biliatdinov K. Z. A methodology for monitoring information security violations in computer networks based on the systematization of a variety of parameters. Means of communication equipment, 2026, No. 1 (173), pp. 34-46 (in Russian). DOI: 10.24412/2782-2141-2026-1-34-46.

УДК 621.317 DOI: 10.24412/2782-2141-2026-1-47-55

Повышение эффективности сетевой безопасности систем IP-телефонии за счёт использования алгоритмов анализа трафика и структуры сети

Лежнина Ю. А., Селин А. А., Цуранов А. Ю., Тувыкин М. Д.

Аннотация. *Существующие информационные системы наиболее эффективно выполняют свои функции при оптимальном взаимодействии устройств, образующих сети связи, как транспортную основу для передачи трафика информационных систем. Обеспечение оптимального распределения трафика между узлами сетей является одним из основных задач анализа многокритериальной оптимизации информационно-телекоммуникационных систем. Последняя подразумевает этап моделирования процессов передачи трафика при обеспечении безопасности его передачи в сети. Это, в том числе, означает, что требуется обеспечить невозможность определения характеристик передаваемых сообщений на основе методов математической статистики, что в современных системах ip-телефонии обеспечивается посредством применения асимметричного шифрования. Важной характеристикой современных информационных систем с позиций обеспечения информационной безопасности является их устойчивость к DDOS-атакам. Одним из возможных подходов к снижению негативных последствий таких атак является использование методов, направленных на поиск маршрутов передачи трафика в сети, способных снизить перегрузку информационной инфраструктуры, что требует обращения к методам анализа структуры сетей. Высокие темпы роста сложности современных сетей связи выдвигает повышенные требования к качеству используемых методов оптимизации как структуры сетей, так и управления маршрутами передачи сообщений в них. В настоящее время анализ сетевых структур выполняется с применением подходов, основанных на математическом моделировании, что обеспечивает формализованный подход к решению практических задач. При этом необходимо стремиться, с одной стороны, к снижению сложности сетевых структур в силу значительных потенциальных затрат на их формирование и обслуживание, а с другой – к устойчивости сетей, достигаемой за счет введения структурной избыточности для обеспечения возможности формирования альтернативных маршрутов передачи трафика. Поэтому используемые методы анализа, моделирования и оптимизации структуры сетей должны быть не обособленными, а взаимосвязанными. Одной из важных задач при этом является нахождение такого сочетания методов, которое вместе с повышением эффективности не приводит к необоснованно высокому росту сложности анализа сети. В работе рассмотрен вариант сочетания методов анализа графов, обладающий относительно низкой вычислительной сложностью, применение которого обеспечивает возможность более быстрого выбора оптимальных маршрутов передачи пакетов ip-телефонии, что критично в условиях реализации DDOS – атак.*

Ключевые слова: *алгоритм Флойда-Уоршелла, алгоритм поиска в глубину, ip-телефония, DDOS – атаки, графовые сети, анализ трафика, моделирование сетевых потоков.*

Введение

Проведение анализа трафика любой сети предполагает выделение особенностей взаимодействия её компонентов, характерных для сетей рассматриваемого типа. Для оценки эффективности работы сети важно знать «узкие» места анализируемой сети, в частности какие пропускные способности имеют каналы передачи информации между узлами сети, обеспечивающие информационное соединение технических устройств и их взаимодействие [1-3].

Известно, что, существенным для исследования сетевой безопасности информационной системы, является определение оптимальной структуры сети, с учётом взаимосвязи её компонентов и анализ трафика данной сети [4].

В интересах оценки оптимальной структуры сети целесообразным является использование алгоритма поиска в глубину. Алгоритм поиска в глубину (*DFS*) ориентирован

в первую очередь на нахождение компонент связности и циклов, таким образом, проектирование сети позволяет определять и рассматривать каждый из узлов сети и связи между ними как элементы единой структуры – графа. По своей сути, алгоритм содержит в себе применение рекурсии, а оценка эффективности проводится путём решения рекуррентных соотношений как в общем виде, так и в каждом конкретном случае [5]. По определению использование алгоритма не позволяет выявлять кратчайшие пути, в связи с чем решение оптимизационных задач по распределению трафика с его помощью невозможно. В связи с вышеуказанным, основной функцией алгоритма поиска в глубину является определение оптимальной структуры сети и взаимосвязи её компонентов, что важно как при моделировании новой, так и при реструктуризации уже существующей сети [6].

Представление сети устройств в виде графов и последующее определение его свойств позволяют определённым образом оптимизировать как структуру самой сети, так и распределение трафика между устройствами внутри неё. Анализ трафика сети целесообразно осуществлять на основе моделирования, при этом распределение потоков трафика в любой сети рационально рассматривать с точки зрения математического моделирования [7-10].

1. Оценка алгоритмов поиска в глубину и Флойда-Уоршелла

Для исследования сетевой безопасности информационной системы рассмотрим применение алгоритма поиска в глубину на примере сети, которая представлена в виде дерева на рис. 1. Каждый узел рассматриваемой сети связан рёбрами графа – информационными линиями только с дочерним и материнским относительно такого узла компонентами, одновременно, то есть у дочерних компонентов взаимосвязи отсутствуют.

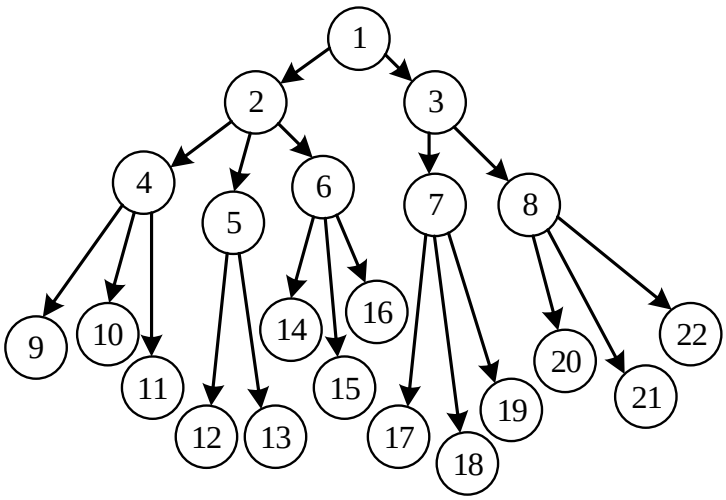


Рис. 1. Структура сети в древовидном виде

Асимптотическая сложность перебора вершин графа рассматриваемого типа определяется рекуррентным соотношением вида

$$f_n = f_{n-1} + f_{n-2} + ... + f_2 + f_1,$$

для решения которого необходимо найти все корни уравнения

$$\alpha^n - \alpha^{n-1} - \alpha^{n-2} - ... - \alpha^2 - \alpha = 0. \quad (1)$$

Очевидно, во внимание принимаются только действительные корни, тогда решение рекуррентного соотношения можно описать следующим образом:

$$f_n = \sum_{k=1}^{n} C_k * \alpha_k^n.$$

Важно отметить, что количество корней не обязательно будет равно *n*, однако тогда некоторое количество слагаемых мы можем представить в виде произведения константы C_k и значения 0^n, что не повлияет на значение f_n, а, следовательно, на оценку асимптотической сложности.

Рассмотрим представленный выше граф и оценим асимптотическую сложность его обхода f_n с помощью алгоритма поиска в глубину и рекурсивным подходом.

Заметим, что каждый из узлов имеет либо 2, либо 3 дочерних. Пусть также:

$$g_n = g_{n-1} + g_{n-2} \quad (2)$$

– нижняя оценка, при которой каждый узел имеет 2 дочерних, а

$$j_n = j_{n-1} + j_{n-2} + j_{n-3} \quad (3)$$

– верхняя оценка, при которой каждому узлу соответствует 3 дочерних.

Тогда:

$$g_n \le f_n \le j_n .$$

Как известно, рекуррентное соотношение (2) задаёт последовательность чисел Фибоначчи, а

$$g_n \approx C_1 * 1{,}618^n + C_2 * (-0{,}618)^n .$$

Ответ получается путём решения уравнения (1) для случая полинома второй степени

$$\alpha^2 = \alpha + 1 .$$

Теперь решим соотношение (3), составив для него характеристическое уравнение:

$$\alpha^3 = \alpha^2 + \alpha + 1,$$

$$\alpha^3 - \alpha^2 - \alpha - 1 = 0 .$$

Методом половинного деления получаем:

$$\alpha \approx 1{,}839 .$$

Таким образом:

$$j_n \approx A_1 * 1{,}839^n .$$

В итоге получаем:

$$C_1 * 1{,}618^n + C_2 * (-0{,}618)^n \le f_n \le A_1 * 1{,}839^n .$$

Более строгая оценка имеет вид:

$$f_n = O(1{,}839^n) ,$$

где *n*, высота дерева графа.

Также, путём математической индукции доказывается факт, что когда база рекурсии имеет чётное количество элементов

$$f_1 = p_1;\ f_2 = p_2 \ldots f_n = p_n;\ \{n = 2k \mid k \in N\},$$

решение рекуррентного соотношения имеет два корня – отрицательный и положительный.

В противном случае, будет один положительный корень, который растёт с увеличением значения *n*.

Перейдём к анализу сетей, в которых непосредственно могут содержаться циклы, а граф данной сети будет неориентированным и невзвешенным.

Рассмотрим граф, представленный на рис. 2, в качестве примера типичного графа, содержащего циклы.

Для удобства также пронумеруем вершины в порядке их обхода, как показано на рис. 2. Рекурсия имеет одно повторение. Первый обход содержит узлы 1-2-3-4-5, а второй обход – узлы 4-6-7-8-9-10-11.

Стоит отметить, что разветвление необходимо производить именно с вершины 4, как того требует алгоритм. Вершина 4 стала точкой разветвления, иначе говоря граф, полученный из исходного путём применения алгоритма поиска в глубину однозначно

представим в виде дерева. Из графа были удалены два цикла: 3-4-6-3 и 2-3-4-5-2, тем самым мы получили новую модель реорганизации существующей сети. Необходимо оптимально произвести построение модели сети, так как её структура будет определять дальнейшее взаимодействия устройств.

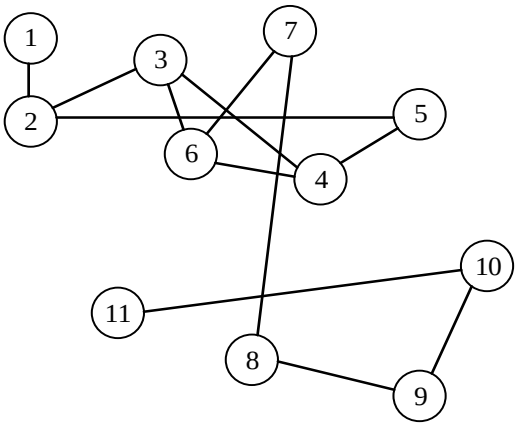


Рис. 2. Структура сетевого графа и его обход по алгоритму *DFS*

Удаляя все циклы, производим обход всего графа в глубину, что также соответствует приведённой ранее рекуррентной оценке согласно формуле (2).

Стоит учитывать, что в любой сети скорости и времена передачи информации между узлами не будут постоянными ввиду наличия задержек, обусловленных различными факторами. Тогда, если можно приближённо описать функцию $U_{\Pi}(\tau)$ зависимости скорости передачи данных U_{Π} от времени τ, то объём информации V определяется интегралом

$$V = \int U_{\Pi}(\tau) d\tau .$$

При фиксированном значении $V = V_k$ можно аналитически вычислить интервал времени, выразив объём передаваемых данных через определённый интеграл функции от времени

$$V_{\text{К}} = \int_{\tau_0}^{\tau_1} U_{\Pi}(\tau) d\tau .$$

При нахождении значения параметра τ_1, как правило, полагают $\tau_0 = 0$. Тогда, при нахождении значений первообразных функции скорости передачи, останется решить уравнение относительно τ_1. Если условия, создающие задержки, могут быть определённо точно оценены и учтены в функции скорости, то чем больше их, тем большую неопределённость это вносит в оценку времени. Некоторые причины задержек могут вообще не оказывать влияния на временной интервал. Как правило, это факторы, влияние которых на значение функции меняется довольно резко и не может быть вычислено даже приблизительно. В таких случаях необходимо выявить временные интервалы, на которых влияние этих причин минимизировано или отсутствует полностью и анализировать характер функции исходя только из них.

Интегральное вычисление объёма информации имеет следующие аналоги: данные о скорости передачи информации представляются в виде частичной суммы ряда

$$U = \sum\nolimits_{i(t)} U_i .$$

За начальное время, то есть момент, с которого мы начинается анализ трафика, принимается t_0, скорость U_i считается постоянной на заранее определённом промежутке

времени. Величина этого промежутка будет зависеть от того, насколько точно требуется вычислить объём информации.

В информационной системе работа алгоритма предусматривает сведение действий к рекурсивным операциям. При решении задач оптимизационного характера для произвольной сети, рекурсии будут содержать непосредственно функциональные последовательности, каждая из которых в некоторых случаях может быть задана с помощью интеграла, поскольку речь не идёт о каких-либо конкретных числовых значениях. Особенно важно в такой ситуации учитывать характер функции, так как решение задачи по большей части заключается в сравнении численных значений путей и выбора минимального из рассматриваемых двух, что возможно только однозначным определением минимального из двух интегралов. Таким образом, сравнение весов рёбер в общем виде будет схоже с задачей упорядочивания по величине значений интегралов, а $V_К$ в большинстве случаев потребуется взять таким, чтобы этот объём информации мог быть передан минимум за один период анализа трафика канала.

2. Оптимизация анализа трафика сети путём совмещения алгоритмов

Строгое комбинирование алгоритмов поиска в глубину и Флойда-Уоршелла с точки зрения теории графов является довольно трудной задачей. Однако, при их использовании в контексте трафика систем *ip*-телефонии, имеется возможность снять некоторые ограничения, которые действовали бы с формально математической точки зрения.

Совмещение алгоритмов предлагается организовать следующим образом. Формируется граф сети анализируемой информационной системы по следующему принципу – все устройства являются узлами графа, все существующие соединения (предполагается, что связь любых двух компонентов сети двусторонняя и единственная) его рёбрами. С помощью *ping*-запросов определяется скорость передачи данных по каналу. Мы всё ещё не можем с помощью одного лишь *DFS* – алгоритма найти кратчайший путь, однако его рекурсивный характер, а именно, переход от одной вершины к другой «по ребру», позволяет оценить все каналы связи и тем самым построить матрицу смежности и расстояний. В ходе выполнения каждой итерации и проверки канала помимо скорости передачи данных извлекается дополнительная информация, которая зависит от специфики выполняемой задачи, например, тип соединения и его безопасность.

Допустим, скорость передачи информации по каналу передачи информации определяется выражением:

$$U_П(\tau) = \left|\sin\frac{\tau}{5}\right|.$$

Пусть $V_К = 3$ (единицы измерения в данном случае не играют роли), а $\tau_0 = 0$

Поскольку первообразная функции не определена в точке $\tau_0 = 0$, необходимо применить переход к пределу

$$V_К = \lim_{\tau\to 0+}\int_{\tau_0}^{\tau_1} U_П(\tau)d\tau = \lim_{\tau\to 0+}\int_{\tau_0}^{\tau_1} |\sin\frac{\tau}{5}|d\tau = 5 - 5*\frac{\sin(\frac{2\tau_1}{5})}{2*|\sin\frac{\tau_1}{5}|} = 3.$$

Значение первообразной $F(\tau)$ при $\tau_0 \to 0+$, вычисляется путём замены sin(x) на эквивалентные бесконечно малые функции. После основных преобразований получаем:

$$5*\frac{\sin(\frac{2\tau_1}{5})}{2*|\sin\frac{\tau_1}{5}|} = 2.$$

Значение τ_1 будем искать в области первого периода с положительным значением аргумента, поэтому модуль можно опустить.

Тогда

$$5*\frac{2*\sin(\frac{\tau_1}{5})*\cos(\frac{\tau_1}{5})}{2*\sin(\frac{\tau_1}{5})}=2;\ \cos(\frac{\tau_1}{5})=\frac{2}{5}.$$

$$\tau_1 \approx 5,8\,\text{ед.}$$

$$\tau_1-\tau_0 \approx 5,8\,\text{ед.}$$

Подобный анализ каждого канала сети информационной системы используется для определения средней скорости передачи данных в сети.

К построенному графу путём рассмотрения матрицы смежности и расстояний применяется алгоритм Флойда-Уоршелла, однако на каждой его итерации вместо обязательного обновления матрицы предлагается использовать информацию о циклах, полученную из предыдущего пункта. Тем самым определяется, какие именно узлы сети не нужно учитывать при рекурсивном вычислении минимального расстояния. В случае, когда на каком-то участке сети обнаружены потенциальные или действующие задержки, например, как показано на рис. 3, интенсивность передачи трафика по нему следует снижать.

Рассмотрим граф сети, представленный на рис. 3, для которого выполнены вышеуказанные этапы анализа

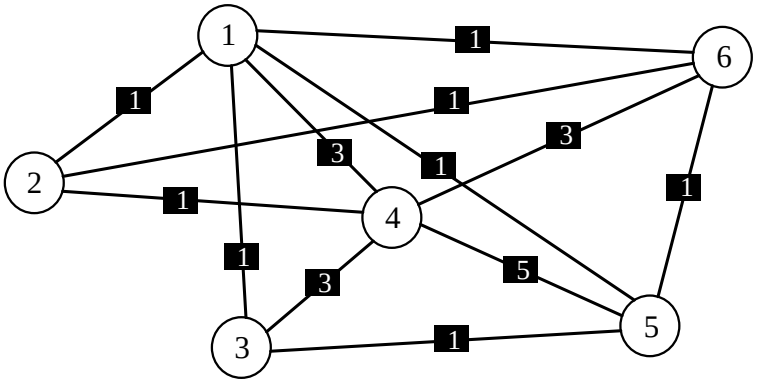


Рис. 3. Структура графа сети с перегруженным узлом

Для такого графа применение алгоритма поиска в глубину приводит к определению обхода графа (одного из оптимальных путей трафика) относительно узла 4 без циклов: 4-1-2-6-5-3, согласно разработанного варианта совмещения алгоритмов.

Матрица расстояний, полученная в результате применения алгоритма поиска в глубину, имеет вид

$$R_1=\begin{pmatrix}0&1&1&3&1&1\\1&0&1&-&-&1\\1&-&0&3&1&-\\3&1&3&0&5&3\\1&-&1&5&0&1\\1&1&-&3&1&0\end{pmatrix}.$$

При анализе структур сетей с помощью предлагаемого совмещенного алгоритма на этапах обхода и определения кратчайших путей им следует уделять особое внимание. В качестве принятых мер могут быть также найдены альтернативные пути трафика относительно узла 4, потенциально разгружающие систему.

Заключение

В работе рассмотрен вариант комбинирования алгоритмов анализа структур, направленный на моделирование структуры сетей, с целью повышения эффективности анализа маршрутов передачи трафика. Применение быстрых алгоритмов поиска эффективных маршрутов передачи трафика потенциально способно снизить эффективность производимых *DDO*-атак, направленных на перегрузку инфраструктуры инфокоммуникационных систем за счет перераспределения информационных потоков в информационных системах.

Направлением дальнейших исследований является организация натурных и вычислительных экспериментов с моделями информационных систем для оценки качества предложенного алгоритма в условиях внешних атак.

Литература

1. Тонких Е. В., Парамонов А. И., Кучерявый А. Е. Планирование структуры сети интернета вещей с использованием фракталов // Электросвязь. – 2021. – № 4. – С. 55-62.

2. Максуров А. А. Обеспечение информационной безопасности в сети Интернет. – Москва: Общество с ограниченной ответственностью «Научно-издательский центр ИНФРА-М», 2023. – 226 с.

3. Портнов Э. Л., Фатхулин Т. Д. Технологии увеличения пропускной способности в современных системах связи с использованием многосердцевинных оптических волокон // Труды Северо-Кавказского филиала Московского технического университета связи и информатики. – 2016. – № 1. – С. 196-199.

4. Давыдов К. С., Ухов Г. В., Фатхулин Т. Д. Анализ ключевых особенностей технологии программно-конфигурируемых сетей (SDN) // Труды Северо-Кавказского филиала Московского технического университета связи и информатики. – 2019. – № 1. – С. 280-287.

5. Фицов В. В. Применение программного кода для оптимизации числа серверов DPI методом максимального элемента // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2018): VII Международная научно-техническая и научно-методическая конференция. Сборник научных статей. В 4-х томах, Санкт-Петербург, 28 февраля – 01 марта 2018 года / Под редакцией С. В. Бачевского. Том 1. – Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2018. – С. 650-656.

6. Корячко В. П., Перепелкин Д. А. Анализ и проектирование маршрутов передачи данных в корпоративных сетях. Монография. – Москва: Горячая линия-Телеком, 2012. – 236 с.

7. Кобылянский В. Г. Сетевые информационные технологии. Моделирование и основные протоколы компьютерных сетей. – Новосибирск: Новосибирский государственный технический университет, 2021. – 131 с.

8. Стахнов А. А. Сеть для офиса и Linux-сервер своими руками: практ. рук. для начинающего администратора. – Санкт-Петербург: БХВ-Петербург, 2006. – 320 с.

9. Смирнова Е. В., Козик П. В. Технологии современных сетей Ethernet. Методы коммутации и управления потоками данных; под ред. Б. В. Кострова. – Санкт-Петербург: БХВ-Петербург, 2012. – 271 с.

10.Поляк-Брагинский, А. В. Локальная сеть. Самое необходимое / А.В. Поляк-Брагинский. – М.: БХВ-Петербург, 2016. – 576 с.

References

1. Tonkikh E. V., Paramonov A. I., Kucheryavy A. E. Planning the structure of the Internet of Things network using fractalsю. *Elektrosvyaz*, 2021, no. 4, pp. 55-62 (in Russian).

2. Maksurov A. A. Ensuring information security on the Internet. Moscow. Limited Liability Company "Scientific Publishing Center INFRA-M" Publ., 2023, 226 p. (in Russian).

3. Portnov E. L., Fatkhulin T. D. Technologies for increasing throughput in modern communication systems using multi-core optical fibers. *Proceedings of the North Caucasus Branch of the Moscow Technical University of Communications and Informatics*, 2016, no. 1, pp. 196-199 (in Russian).

4. Davydov K. S., Ukhov G. V., Fatkhulin T. D. Analysis of key features of software-defined networking (SDN) technology. *Proceedings of the North Caucasus Branch of the Moscow Technical University of Communications and Informatics*, 2019, no. 1, pp. 280-287 (in Russian).

5. Fitsov V. V. Application of software code for optimizing the number of DPI servers using the maximum element method. *Current Problems of Infotelecommunications in Science and Education* (*APINO* 2018). *VII International Scientific, Technical, and Scientific-Methodological Conference. Collection of Scientific Articles. In 4 vol*., Saint Petersburg, February 28 – March 01, 2018, vol. 1. St. Petersburg. Saint Petersburg State University of Telecommunications named after Prof. M. A. Bonch-Bruevich, 2018. pp. 650-656 (in Russian).

6. Koryachko V. P., Perepelkin D. A. Analysis and Design of Data Transmission Routes in Corporate Networks. Monograph. Moscow. Hot Line – Telecom Publ., 2012. 236 p. (in Russian).

7. Kobylansky V. G. Network Information Technologies. Modeling and Main Protocols of Computer Networks. Novosibirsk. Novosibirsk State Technical University Publ., 2021, 131 p. (in Russian).

8. Stakhnov A. A. Office network and Linux server with your own hands: practical guide for the novice administrator. St. Petersburg. BKhV-Peterburg Publ., 2006, 320 p. (in Russian).

9. Smirnova E. V., Kozik P. V. Technologies of modern Ethernet networks. Switching methods and data flow management. St. Petersburg: BKhV-Peterburg Publ., 2012. 271 p. (in Russian).

10. Polyak-Braginsky A. V. Local network. The essentials. Moscow. BKhV-Peterburg Publ., 2016. 576 p. (in Russian).

Статья поступила 18 февраля 2026 г.

Информация об авторах

Лежнина Юлия Аркадьевна – кандидат технических наук, доцент. Доцент кафедры индустриального программирования. Институт перспективных технологий и индустриального программирования Московского института радиотехники, электроники и автоматики – Российского технологического университета (РТУ МИРЭА). Область научных интересов: разработка новых методов анализа и синтеза элементов систем управления. Тел: +7 (985) 402–94–64, E-mail: lejninau@mail.ru.

Селин Андрей Александрович – кандидат технических наук. Доцент кафедры информационной безопасности. Институт кибербезопасности и цифровых технологий РТУ МИРЭА. Область научных интересов: кибербезопасность, проектирование инфокоммуникационных систем. Тел: +7 (920) 087–11–71, E-mail: selin@mirea.ru.

Тувыкин Михаил Денисович – студент. РТУ МИРЭА. Область научных интересов: проектирование инфокоммуникационных систем и систем связи. Тел: +7 (910) 097–20–56, E-mail: rosomaha1812@mail.ru. Адрес: 119454, Россия, г. Москва, проспект Вернадского, д. 78.

Цуранов Артём Юрьевич – студент. РТУ МИРЭА. Область научных интересов: проектирование инфокоммуникационных систем и систем связи. Тел: +7 (996) 448–89–35, E-mail: artemcuranov526@gmail.com.

Адрес: 119454, Россия, г. Москва, проспект Вернадского, д. 78.

Improving the efficiency of network security for IP-telephony systems by using traffic and network structure analysis algorithms

Y. A. Lezhnina, A. A. Selin, A. Yu. Tsyranov, M. D. Tuvykin

Annotation. *Existing information systems perform their functions most effectively with optimal interaction of devices that make up communication networks, serving as a transport basis for the transmission of information systems traffic. Ensuring optimal traffic distribution between network nodes is one of the main tasks of multicriteria optimization analysis of information and telecommunication systems. The latter implies a stage of modeling traffic transmission processes while ensuring the security of its transmission in the network. This, among other things, means that it is necessary to prevent the possibility of determining the characteristics of transmitted messages using mathematical statistics methods, which in modern IP-telephony systems is ensured through the use of asymmetric encryption. An important characteristic of modern*

information systems from the perspective of information security is their resistance to DDOS attacks. One possible approach to reducing the negative consequences of such attacks is the use of methods aimed at finding traffic routing paths in networks that can reduce the overload of the information infrastructure, which requires resorting to methods of network structure analysis. The high rate of growth in the complexity of modern communication networks imposes increased demands on the quality of the methods used for optimizing both the network structure and the management of message transmission routes within them. Currently, the analysis of network structures is carried out using approaches based on mathematical modeling, which provides a formalized approach to solving practical problems. At the same time, it is necessary to strive, on the one hand, to reduce the complexity of network structures due to the significant potential costs of their formation and maintenance, and on the other hand, to ensure network stability, achieved by introducing structural redundancy to provide the possibility of forming alternative traffic transmission routes. Therefore, the methods used for analyzing, modeling, and optimizing network structure should not be isolated, but interconnected. One of the important tasks in this regard is to find such a combination of methods which, along with increasing efficiency, does not lead to an unreasonably high increase in the complexity of network analysis. The paper considers an option of combining graph analysis methods, which has relatively low computational complexity, the application of which provides the ability to more quickly select optimal IP telephony packet transmission routes, which is critical in the context of implementing DDOS attacks.

Keywords: *Floyd-Warshall algorithm, depth-first search algorithm, IP telephony, DDoS attacks, graph networks, traffic analysis, modeling of network flows.*

Information about the authors

Yulia Arkadyevna Lezhnina– Ph.D., Associate Professor, Associate Professor of the Department of Industrial Programming at the Institute of Advanced Technologies and Industrial Programming of MIREA – Russian Technological University. Research interests: development of new methods for analysis and synthesis of control system elements. Tel: +7 (985) 402–94–64, E-mail: lejninau@mail.ru.

Andrey Aleksandrovich Selin– PhD in Technical Sciences, Associate Professor of the Department of Information Security at the Institute of Cybersecurity and Digital Technologies of MIREA – Russian Technological University. Areas of scientific interest: cybersecurity, design of infocommunication systems. Tel.: +7 (920) 087–11–71, E-mail: selin@mirea.ru.

Mikhail Denisovich Tuvykin– student of MIREA - Russian Technological University. Field of scientific interest: design of infocommunication systems and communication systems. Tel: +7 (910) 097–20–56, E-mail: rosomaha1812@mail.ru.

Artem Yurievich Tsuranov– student of MIREA - Russian Technological University. Field of scientific interest: design of infocommunication systems and communication systems. Tel: +7 (996) 448–89–35, E-mail: artemcuranov526@gmail.com.

Address: 119454, Russia, Moscow, Vernadsky Avenue, 78.

Для цитирования:

Лежнина Ю.А., Селин А. А., Цуранов А. Ю., Тувыкин М. Д. Повышение эффективности сетевой безопасности систем IP-телефонии за счёт использования алгоритмов анализа трафика и структуры сети // Техника средств связи. 2026. № 1 (173). С. 47-55. DOI: 10.24412/2782-2141-2026-1-47-55.

For citation:

Lezhnina Y. A., Selin A. A., Tsyranov A. Yu., Tuvykin M. D. Improving the efficiency of network security for IP-telephony systems by using traffic and network structure analysis algorithms. Means of communication equipment, 2026, № 1 (173), pp. 47-55 (in Russian). DOI: 10.24412/2782-2141-2026-1-47-55.

ЭЛЕКТРОННЫЕ И РАДИОТЕХНИЧЕСКИЕ СИСТЕМЫ

УДК 519.248, 621.384.3 DOI: 10.24412/2782-2141-2026-1-56-62

Обоснование возможности использования солнечных панелей космических аппаратов при проведении испытаний лазерных средств связи и передачи данных

Закутаев А. А., Соколов Е. С., Харченко С. С.

Аннотация. Постановка задачи: *в статье обоснована возможность использования солнечных панелей и ряда других элементов штатной системы электропитания космических аппаратов в качестве бортовой регистрирующей аппаратуры лазерного излучения при проведении испытаний (оценке текущих характеристик) наземных сегментов лазерных средств связи и передачи данных.* ***Целью работы*** *является совершенствование подходов к мишенному обеспечению процесса оценивания характеристик наземных сегментов лазерных средств связи и передачи данных на различных стадиях их жизненного цикла – при проведении испытаний и в условиях штатной эксплуатации.* ***Используемые методы:*** *в статье применены известные общенаучные методы системного анализа, теории эффективности целенаправленных процессов и подходы к организации и проведению испытаний.* ***Новизна:*** *комплексная реализация не декларированных функциональных возможностей элементов штатной системы электропитания из состава бортового комплекса управления космических аппаратов в интересах решения новой задачи – регистрации во времени относительным методом амплитуды лазерного излучения, падающего на поверхность солнечных панелей.* ***Результат*** *заключается в разработке методических основ проведения испытаний (оценки текущих характеристик) наземных сегментов лазерных средств связи и передачи данных с использованием в качестве регистрирующей аппаратуры солнечных панелей и ряда других элементов штатной системы электропитания космических аппаратов.* ***Практическая значимость*** *состоит в возможности реализации предложенного способа с привлечением уже существующих и перспективных космических аппаратах без их доработки и получением результатов проведения испытаний (оценки текущих характеристик) в течение суток, а также существенном расширении номенклатуры мишенного обеспечения при проведении испытаний (оценке текущих характеристик) наземных сегментов лазерных средств связи и передачи данных.*

Ключевые слова: *лазерные средства связи и передачи данных, мишенное обеспечение, испытания, солнечная панель.*

Актуальность

Околоземное космическое пространство все активнее вовлекается в процесс развития различных отраслей народного хозяйства. Наибольшее распространение при этом получили такие направления как связь и передача данных. В настоящее время самыми высокоскоростными космическими средствами связи и передачи данных являются средства лазерного типа (ЛССПД). На процесс развития и внедрения указанных средств влияет множество факторов, связанных прежде всего с уровнем развития тех или иных технологий. При функционировании наземных сегментов ЛССПД важным вопросом, например, является точность наведения и удержания лазерного луча на бортовой приемной аппаратуре, а также стабильность параметров доставляемой к ней излучения [1]. Оценка соответствующих характеристик как на этапе испытания наземных сегментов ЛССПД, так и их подтверждения в процессе эксплуатации невозможна без соответствующего мишенного обеспечения. Наиболее эффективным решением указанной проблемы является создание специализированной бортовой испытательной аппаратуры (ИА) [2]. Основной недостаток подобного решения заключается в высокой стоимости. При размещении ИА на сторонних космических аппаратах (КА) сложности будут заключаться в ограничениях характеристик ИА обусловленных конструкцией КА, а также необходимостью согласования количества и длительностей интервалов времени, в течении которых КА будет выводиться из штатной циклограммы функционирования. Перечисленные альтернативные варианты создания ИА для проведения испытаний и подтверждения текущих характеристик наземных сегментов ЛССПД имеет существенные недостатки, что снижает эффективность процессов создания и эксплуатации последних, а также снижает темпы их

развития в целом. Вместе с тем, в состав практически всех современных КА входят солнечные панели (СП), по сути являющиеся устройствами, реализующими свет-сигнальное преобразование падающего на них оптического излучения. Датчиковая аппаратура, обеспечивающая контроль их функционирования, в том числе регистрирует во времени количество полученной СП энергии. Совместное использование указанных не декларированных возможностей элементов системы энергетического обеспечения КА потенциально может позволить осуществлять ими регистрацию излучения наземных сегментов ЛССПД как самостоятельной специализированной аппаратурой. Таким образом, исследование подходов к мишенному обеспечению наземных сегментов ЛССПД на основе использования СП КА является актуальной научно-технической задачей.

Особенности построения и функционирования солнечных панелей космических аппаратов

В качестве классификационного признака при рассмотрении солнечных панелей (СП) для КА может быть использован материал, из которого они изготовлены. В настоящее время наиболее известными материалами для изготовления СП являются: кремний; арсенид галлия; многопереходные материалы, состоящие из галлия, индия, селенида и др. [3].

СП каждого типа обладают совокупностью преимуществ и недостатков. Сравнительный анализ их основных характеристик представлен в табл. 1 [3-12].

Таблица 1 – Сравнительный анализ основных характеристик основных типов СП

Наименование характеристик	Кремниевые СП	Галлий-арсенидные СП	Многопереходные СП
Используемый материал	Монокристаллический кремний	Тонкие плёнки GaAs на Ge-подложке	Тонкие слои
Технология изготовления	Monocrystalline Silicon или Polycrystalline Silicon	MBE-рост	MOCVD
Сложность производства	Низкая	Средняя	Высокая
Толщина, мкм	~200	~10…50	1…5 – каждый слой
Удельная масса, г/Вт	50…70	30…50	20…40
Жесткость структуры	Жесткая	Гибкая	Жесткая
Внешнее покрытие	Стекло	Кварц	Германий
Спектральная квантовая эффективность	~10-20 % – <400 нм ~80-90 % – 600-900 нм ~10-20 % – >1100 нм	~50 % – <300 нм ~80-95 % – 400-900 нм ~50 % – >1100 нм	80% – 300-600 нм 90% – 600-900 нм 70% – 900-1800 нм
Конверсионная эффективность, %	14…18	20…25	30…39
Скорость деградации покрытия, %/год	~ 1	< 0,5	< 0,3
Удельная стоимость, $/Вт	1…2	3…5	5…10

Процесс функционирования всех вышеуказанных типов СП основан на использовании фотоэффекта и условно представляется следующей последовательностью этапов [13-19]:

- поглощение падающих фотонов, сопровождающееся возбуждением электронов в материале полупроводника и, как следствие, созданием пары электрон-дырка;
- генерация напряжения за счет разделения электронов и дырок электрическим полем;
- съем и передача полученной энергии.

СП являются составной частью системы энергообеспечения КА, в которую в общем случае также входят следующие элементы [13-19]:

- аккумуляторные батареи (АКБ), предназначенные для хранения энергии;
- регуляторы заряда и разряда АКБ;
- конвертеры, используемые для преобразования напряжение;
- подсистема управления и мониторинга (СУМ), состоящая из датчиковой аппаратуры и программного обеспечения;
- распределительная сеть;
- вспомогательные элементы (кабели, разъёмы, теплоотводы, защитные устройства (предохранители, реле) и т. д.).

В свою очередь система энергообеспечения КА в целях обеспечения эффективности своего функционирования взаимодействует с другими служебными системами, основной из которых является система ориентации.

Особенности проведения испытаний и оценки текущих характеристик наземных средств связи и передачи данных лазерного типа

Сущность функционирования наземного сегмента ЛССПД при работе в активном режиме заключается в создании стабильного канала с бортовой приемной аппаратурой в ходе сеанса связи или передачи данных. Указанный процесс с точки зрения проверки соответствия требованиям (оценки параметров) может характеризоваться следующим перечнем параметров:

– среднеквадратической ошибкой наведения ЛИ на объект при его сопровождении;
– плотностью лазерного излучения (ЛИ), доставляемого к объекту.

Очевидно, что оценка указанных параметров должна проводиться комплексно с учетом длительности требуемого интервала времени функционирования ЛССПД. С учетом влияния атмосферы Земли на процесс распространения ЛИ, имеющего вероятностный характер, наибольшая достоверность результатов может быть обеспечена только экспериментальными методами в совокупности с достаточной размерностью статистической выборки.

С точки зрения характеристик самого ЛИ, которые будут определять дополнительные требования к средствам проведения испытаний, можно выделить следующие:

– в наземных сегментах ЛССПД используется импульсно-периодический тип ЛИ;
– длины волн ЛИ в современных ЛССПД находятся в пределах видимого и ближнего инфракрасного (ИК) диапазонов и выбираются с учетом «окон прозрачности» атмосферы;
– мощность ЛИ выбирается исходя из условий гарантированной его регистрации приемной аппаратурой с учетом потерь, возникающих на трассе распространения.

Предложения по порядку использования солнечных панелей для регистрации таргетированного лазерного излучения

Анализ особенностей проведения испытаний (оценки текущих характеристик) наземных сегментов ЛССПД показал, что для их успешной реализации необходима бортовая аппаратура, обеспечивающая регистрацию импульсно-периодического ЛИ в видимом и ближнем ИК диапазонах длин волн мощностью менее единиц Вт/см^2. Длительность регистрации будет определяться исходя из времени нахождения КА в зоне действия наземного сегмента ЛССПД, что для высот орбиты порядка 700 км будет составлять более 2 мин.

Характеристики СП КА и принципы их построения и функционирования потенциально позволяют решать указанную задачу без дополнительных модификаций и доработок. Анализ научно-технической литературы в данной предметной области показал, что ЛИ было успешно использовано для оценивания степени деградации СП. При этом необходимо решить задачи:

– исключения деструктивного влияния ЛИ на СП за счет перегрева;
– определения калибровочной кривой, позволяющей относительным методом сопоставлять показания датчиков подсистемы управления и мониторинга системы энергообеспечения КА (амплитуды силы тока или напряжения) с плотностью падающего на СП ЛИ;
– оценки чувствительности и степени инертности вышеуказанной датчиковой аппаратуры в условиях облучения СП ЛИ;
– определения зависимости КПД СП от фазового угла ЛИ.

Все вышеперечисленные задачи могут быть решены в ходе наземной отработки при помощи известного стендового оборудования. Доработка СПО как системы энергообеспечения, так системы управления КА при этом не потребуется. Показания соответствующей датчиковой аппаратуры входят в состав телеметрической информации, передаваемой с борта КА на наземные пункты управления.

Обзор научно-технической литературы [20-22] в области использования свойств СП по регистрации оптического излучения при решении нецелевых задач показал, что положительный опыт применения СП был получен в ряде космических экспериментов:

– в ходе исследований способов оценки степени их деградации в условиях воздействия факторов космического пространства;
– для наблюдения и регистрации вспышек на Солнце;
– для корректировки сигнала на основе регистрации обратного рассеяния ЛИ.

Еще одной областью применения СП является оценка отражательно-излучательных свойств атмосферы Земли.

Методические основы проведения испытаний (оценки текущих характеристик) наземных средств связи и передачи данных лазерного типа с использованием солнечных панелей космических аппаратов

С учетом перечня характеристик наземных сегментов ЛССПД, которые могут проверяться при помощи СП КА, в качестве оцениваемого может быть комплексный показатель, включающий две составляющих:

– значение тока (напряжения), генерируемого СП в каждом временном отсчете;
– значение интервала времени, в течение которого выполняется проверка.

Тогда в качестве критериальных параметров для принятия решения соответственно будут выступать:

– значение критериального уровня тока (напряжения), генерируемого СП в каждом временном отсчете;
– требуемая длительность сеанса связи или передачи данных.

С учетом принятых допущений проведение испытаний (оценка текущих характеристик) наземных сегментов ЛССПД при помощи СП КА будет сводиться к определению соотношения суммы временных интервалов, в которых значение тока (напряжения), генерируемого СП, превысило значение критериального уровня, к общей длительности проведения i-го сеанса связи или передачи данных. Если указанное соотношение обозначить как Q_i, то рассматриваемая задача может быть представлена в следующем формализованном виде:

$$Q_i = \frac{\sum t_j \Big|_{I_{\text{ЛИ } j} \geq I_{\text{ЛИ крит}}}}{T_{\text{с}}}, \quad (1)$$

где $T_{\text{с}}$ – длительность сеанса связи или передачи данных; t_j – длительность временного интервала, в течение которого значение тока (напряжения), генерируемого СП $I_{\text{ЛИ } j}$ превысило значение критериального уровня $I_{\text{ЛИ крит}}$.

При достаточном наборе статистики наземный сегмент ЛССПД считается прошедшим испытание в случае, если выполняется следующее условие:

$$\frac{\sum n_i}{m} \geq K, \quad (2)$$

где n_i – признак зачетного сеанса связи или передачи данных, определяемый как:

$$n_i = \begin{cases} 1, \text{ при } Q_i = 1, \\ 0, \text{ при } Q_i < 1; \end{cases}$$

m – общее количество сеансов связи или передачи данных, проведенных в рамках испытания; K – критериальное значение.

Если количество испытаний мало, то условие (2) может быть заменено более простым, согласно которому испытание наземного сегмента ЛССПД считается успешным если каждое значение Q_i, при $i = 1{:}m$, будет равно 1.

Выводы

На основе результатов сопоставления требований к мишенному обеспечению при проведении испытаний (оценке текущих характеристик) наземных сегментов ЛССПД и основных характеристик наиболее распространенных типов СП КА была обоснована

техническая возможность применения последних в качестве бортовой аппаратуры регистрации таргетированного ЛИ. С учетом реализации комплексного подхода в части учета внешних воздействующих факторов на процесс функционирования наземных сегментов ЛССПД описаны методические основы проведения их испытаний (оценки текущих характеристик) для различных размеров статистических выборок. В качестве дальнейшего направления исследований может рассматриваться разработка модели канала регистрации таргетированного ЛИ различными типами СП КА, которая позволит оценить границы области применимости предлагаемого способа при проведении испытаний (оценке текущих характеристик) наземных сегментов ЛССПД. Также актуальным вопросом является метрологического обеспечения в части калибровки СП КА как измерительного средства.

Литература

1. Пратт Вильям К. Лазерные системы связи, пер. с англ. под ред. проф. Шереметьева А.Г. – М.: Связь, 1972. – 232 с.

2. Free-Space Laser Communications: Principles and Advances / Под ред. А. Майджумдера и Дж. Риклина. – Springer, 2008. – 418 p.

3. European Space Agency. Spacecraft Solar Arrays: Принципы и сравнение типов, 2020. – URL: https://www.esa.int (дата обращения 23.10.2025).

4. National Renewable Energy Laboratory. Solar Cell Efficiency Tables (Version 62, July 2023): Подробные данные по PCE и EQE для различных типов. NREL, 2023. – URL: https://www.nrel.gov (дата обращения 23.10.2025).

5. Luque, A. Space Solar Cells and Arrays [Технический отчет]. Анализ характеристик для КА, включая радиационную устойчивость и EQE. NASA, 2019. – URL: https://www.nasa.gov (дата обращения 23.10.2025).

6. King, D., et al. High-Efficiency Multijunction Solar Cells for Space Applications. Journal of Applied Physics, 2022. – Vol. 132. – № 4. – Pp. 123-134.

7. European Space Agency. Solar Cells for Space, 2021. – URL: https://www.esa.int (дата обращения 23.10.2025).

8. Würfel, P. Physics of Solar Cells: From Principles to New Concepts. – 2021. – 198 с.

9. NASA. Principles of Solar Cell Operation [Технический меморандум]. NASA, 2018. – URL: https://www.nasa.gov (дата обращения 23.10.2025).

10. Geisz, J. et al. Multijunction Solar Cells for Space: From Concept to Reality. Progress in Photovoltaics. – 2022. – Vol. 30. – № 5. – Pp. 123-135.

11. Liu, X. et al. Flexible GaAs Solar Cells for Space. Journal of Spacecraft and Rockets. – 2023. – Vol. 60. – № 4. – Pp. 890-902.

12. Дебрин А.С., Бастрон А.В., Урсегов В.Н. Обзор солнечных панелей и фотоэлектрических станций отечественных производителей // Вестник КрасГАУ. 2018. № 6 (141). – С. 136-141.

13. NASA. Solar Cell Technologies, 2020. – URL: https://www.nasa.gov (дата обращения 23.10.2025).

14. ESA Report «Photovoltaic Assemblies»: Схемы и материалы, 2021. – URL: https://www.esa.int (дата обращения: 23.10.2025).

15. Würfel, P. Physics of Solar Cells (3rd ed.). Wiley-VCH, 2016. – 498 p.

16. Fortescue, P., et al. Spacecraft Systems Engineering (4th ed.). Wiley. 2011. – 928 p.

17. NASA. Spacecraft Power Systems, 2019. – URL: https://www.nasa.gov (дата обращения 23.10.2025).

18. European Space Agency. Electrical Power Subsystem: Тех. руководство, 2020. – URL: https://www.esa.int (дата обращения 23.10.2025).

19. Zhang, X. et al. Solar Power Systems for Small Satellites. Acta Astronautica, 2022. – Vol. 183. – Pp. 114-127.

20. NASA. NASA Report on Photovoltaic Degradation: Обсуждает лазерные эффекты на GaAs СП 2020. – URL: https://www.nasa.gov (дата обращения: 23.10.2025).

21. European Space Agency. ESA Space Environment Report: Примеры использования СП как датчиков 2021. – URL: https://www.esa.int (дата обращения 23.10.2025).

22. Liu, X. et al. Modeling Laser Impact on Multifunction Solar Cells. IEEE Transactions on Electron Devices, 2023. – Vol. 70. – № 6. – Pp. 1234-1245.

References

1. Pratt William K. Laser Communication Systems, translated from English under the editorship of prof. Sheremetyev A.G. Moscow. Svyaz Publ., 1972. 232 p. (in Russian).
2. Free-Space Laser Communications: Principles and Advances, edited by Arun K. Majumdar and Jennifer C. Ricklin. *Springer*, 2008. 418 p.
3. European Space Agency. Spacecraft Solar Arrays: Principles and Type Comparison, 2020. – URL: https://www.esa.int (accessed 23.10.2025).
4. National Renewable Energy Laboratory. Solar Cell Efficiency Tables (Version 62, July 2023): Detailed PCE and EQE data for various types. NREL, 2023. – URL: https://www.nrel.gov (accessed 23.10.2025).
5. Luque A. Space Solar Cells and Arrays [Technical Report]. Performance Analysis for Spacecraft, Including Radiation Hardness and EQE. NASA, 2019. – URL: https://www.nasa.gov (accessed 23.10.2025).
6. King D., et al. High-Efficiency Multijunction Solar Cells for Space Applications. *Journal of Applied Physics*, 2022, vol. 132, no. 4. pp. 123-134.
7. European Space Agency. Solar Cells for Space, 2021. – URL: https://www.esa.int (accessed 23.10.2025).
8. Würfel P. Physics of Solar Cells: From Principles to New Concepts. 2021. 198 p.
9. NASA. Principles of Solar Cell Operation [Technical Memorandum]. NASA, 2018. – URL: https://www.nasa.gov (accessed: 23.10.2025).
10. Geisz J. et al. Multijunction Solar Cells for Space: From Concept to Reality. *Progress in Photovoltaics*, 2022, vol. 30, no. 5, pp. 123-135.
11. Liu X. et al. Flexible GaAs Solar Cells for Space. *Journal of Spacecraft and Rockets*, 2023, vol. 60, no. 4, pp. 890-902.
12. Debrin A. S., Bastron A. V., Ursegov V. N. Review of solar panels and photovoltaic stations of domestic manufacturers. *Vestnik KrasSAU*, 2018, no. 6 (141), pp. 136-141 (in Russian).
13. NASA. Solar Cell Technologies, 2020. – URL: https://www.nasa.gov (accessed 23.10.2025).
14. ESA Report Photovoltaic Assemblies: Schematics and Materials, 2021. – URL: https://www.esa.int (accessed: 23.10.2025).
15. Würfel P. Physics of Solar Cells (3rd ed.). Wiley-VCH, 2016. 498 p.
16. Fortescue P., et al. Spacecraft Systems Engineering (4th ed.). Wiley, 2011. 928 p.
17. NASA. Spacecraft Power Systems, 2019. – URL: https://www.nasa.gov (accessed: 23.10.2025).
18. European Space Agency. Electrical Power Subsystem: Тех. руководство, 2020. URL: https://www.esa.int (accessed: 23.10.2025).
19. Zhang, X. et al. Solar Power Systems for Small Satellites. *Acta Astronautica*, 2022, v. 183, pp. 114-127.
20. NASA. NASA Report on Photovoltaic Degradation: Обсуждает лазерные эффекты на GaAs СП 2020. – URL: https://www.nasa.gov (accessed: 23.10.2025).
21. European Space Agency. ESA Space Environment Report: Примеры использования СП как датчиков 2021. – URL: https://www.esa.int (accessed: 23.10.2025).
22. Liu X. et al. Modeling Laser Impact on Multifunction Solar Cells. *IEEE Transactions on Electron Devices*, 2023, vol. 70, no. 6, pp. 1234-1245.

Статья поступила 25 января 2026 г.

Информация об авторах

Закутаев Александр Александрович – начальник лаборатории военного института (научно-исследовательского). Военно-космическая академия имени А.Ф. Можайского. Область научных интересов: методы оценивания эффективности функционирования и совершенствования программно-алгоритмического обеспечения оптико-электронных и квантово-оптических средств. Тел. +7 952 355 22 92. E-mail: zakutaev.a@mail.ru.

Адрес: 197198, Россия, г. Санкт-Петербург, ул. Ждановская, д. 13.

Соколов Евгений Сергеевич – начальник лаборатории – заместитель начальника испытательного отдела. Войсковая часть 32103. Область научных интересов: методы оценивания эффективности функционирования и совершенствования программно-алгоритмического обеспечения оптико-электронных и квантово-оптических средств. Тел. +7 925 466 58 80. E-mail: sokolov78@mail.ru.

Адрес: 143090, Россия, Московская обл., г. Краснознаменск, ул. Октябрьская, 3.

Харченко Станислав Сергеевич – заместитель начальника испытательного центра. Войсковая часть 32103. Область научных интересов: методы оценивания эффективности функционирования и совершенствования программно-алгоритмического обеспечения оптико-электронных и квантово-оптических средств. E-mail: romeo.maximir@yandex.ru. Тел.: +7 965 208 64 61.

Адрес: 143090, Россия, Московская обл., г. Краснознаменск, ул. Октябрьская, 3.

Justification of the possibility of using spacecraft solar panels during testing of laser communication and data transmission systems

A. A. Zakutaev, E. S. Sokolov, S. S. Kharchenko

Annotation. Problem statement: *This article substantiates the possibility of using solar panels and a number of other elements of the spacecraft's standard power supply system as onboard recording equipment for laser radiation during testing (evaluation of current characteristics) of ground segments of laser communication and data transmission systems (LCTDS).* ***The aim of the work****: improve approaches to target support for the process of evaluating the characteristics of ground segments of LCTDS at various stages of their life cycle, both during testing and during normal operation.* ***Methods:*** *The article uses well-known general scientific methods of system analysis, theories of the effectiveness of purposeful processes, and approaches to the organization and conduct of tests.* ***Novelty:*** *the comprehensive implementation of undeclared functional capabilities of the elements of the standard power supply system from the onboard control complex of spacecraft in order to solve a new task – registration in time by the relative method of the amplitude of the laser radiation falling on the surface of the solar panels.* ***Result:*** *The development of methodological foundations for conducting tests (evaluation of current characteristics) of ground segments of LCTDS using solar panels and a number of other elements of the regular power supply system of spacecraft as recording equipment.* ***The practical significance*** *lies in the possibility of implementing the proposed method using existing and promising spacecraft without any modifications and obtaining test results (current performance assessments) within a day, as well as significantly expanding the range of target support during tests (current performance assessments) of ground-based LCTDS segments.*

Keywords: *solar panel, laser communication and data transmission systems, target support, testing*

Information about the authors

Alexandr Alexandrovich Zakutaev – Head of the Laboratory of the Military Institute (Research) of Military Space Academy of Mozhaisky. Research interests: methods for evaluating the efficiency of functioning and improving software and algorithmic support of optoelectronic and quantum optical means. Tel: +7 952 355 22 92. E-mail: zakutaev.a@mail.ru.

Address: 197198, Russia, Saint-Petersburg, Zhdanovskaya st., 13.

Evgeny Sergeevich Sokolov– head of the laboratory – deputy head of the testing department of military unit 32103. Research interests: methods for assessing the performance and improving software and algorithmic support for optical-electronic and quantum-optical devices. Tel.: +7 925 466 58 80. E-mail: sokol_ov78@mail.ru.

Stanislav Sergeevich Kharchenko– Deputy Head of the Testing Center of Military Unit 32103. Research interests: methods for assessing the performance and improving software and algorithmic support for optical-electronic and quantum-optical devices. Tel.: +7 965 208 64 61. Email: romeo.maximir@yandex.ru.

Address: 143090, Russia, Moscow region, Krasnoznamensk, Oktyabrskaya st., 3.

Для цитирования:

Закутаев А. А., Соколов Е. С., Харченко С. С. Обоснование возможности использования солнечных панелей космических аппаратов при проведении испытаний лазерных средств связи и передачи данных // Техника средств связи. 2026. № 1 (173). С. 56-62. DOI: 10.24412/2782-2141-2026-1-56-62.

For citation:

Zakutaev A. A., Sokolov E. S., Kharchenko S. S. Justification of the possibility of using spacecraft solar panels during testing of laser communication and data transmission systems. Means of communication equipment, 2026, № 1(173), pp. 56-62 (in Russian). DOI: 10.24412/2782-2141-2026-1-56-62.

ВЫЧИСЛИТЕЛЬНЫЕ СИСТЕМЫ

УДК 621.391 DOI: 10.24412/2782-2141-2026-1-63-75

Нейроморфные вычисления и нейроморфные алгоритмы поиска на ресурсах перспективных дата-центров специального назначения: сущность, проблемы и возможные подходы к реализации

Владимирова Е. С., Салюк Д. В., Паращук И. Б., Цыпнятов В. Б.

Аннотация. Постановка задачи*: комплексный и детальный анализ нетривиальных свойств и особенностей, присущих перспективным нейроморфным программно-аппаратным средствам и процедурам, нацеленным на эффективные вычисления и реализацию поисковых запросов на информационных ресурсах дата-центров специального назначения. Исследование физической сущности, общих и частных аспектов реализации технологии и механизмов нейроморфных вычислений и нейроморфных алгоритмов поиска, архитектуры нейроморфных процессоров, условий применения подобных процедур и программно-аппаратных средств, а также формулировка основных проблем и анализ потенциальных подходов к их преодолению на пути реализации технологии и механизмов нейроморфных вычислений и нейроморфных алгоритмов поиска на ресурсах дата-центров специального назначения.* ***Новизна:*** *состоит в том, что объектом исследования являются перспективные нейроморфные программно-аппаратные средства и процедуры для вычислений и информационного поиска на ресурсах дата-центров, которые, в свою очередь, могут служить инновационной основой для построения и применения новых элементов IT-инфраструктуры критических информационных объектов государства, объектов военно-промышленного комплекса, оборонной сферы и охраны правопорядка.* ***Целью работы*** *является анализ существующих и формулировка новых подходов, ориентированных на построение и применение перспективных нейроморфных программно-аппаратных средств и на реализацию процедур нейроморфных вычислений и нейроморфных алгоритмов поиска на ресурсах дата-центров специального назначения.* ***Результат:*** *заключается в том, что исследованы аспекты, предложены и обоснованы условия построения и применения технологии и механизмов нейроморфных вычислений и нейроморфных алгоритмов поиска, которые в дальнейшем могут лечь в основу формулировки частных и общих требований при проектировании, модернизации и модификации дата-центров, составляющих основу современной и перспективной IT-инфраструктуры страны. Предложены современные и перспективные подходы к применению на практике новых технологических и иных инноваций, ориентированных на нейроморфные вычисления и поиск, и напрямую касающихся тенденций построения и совершенствования объектов такого класса.* ***Практическая значимость****: результаты анализа и предложенные подходы к преодолению ряда теоретических, методологических и практических проблемы проектирования, построения и применения технологии и механизмов нейроморфных вычислений и нейроморфных алгоритмов поиска, с учетом возможных ограничений по элементной базе, с учетом закономерностей, алгоритмов, структуры и условий применения отдельных процедур и программно-аппаратных средств для реализации подобных перспективных нейроморфных инструментов, позволяют по новому, с единых системных позиций, взглянуть на физическую сущность нейроморфных процессов и программно-аппаратных средств для их реализации, позволят более реалистично и подробно сформулировать дальнейшие направления развития IT-инфраструктуры, нацеленной на продолжающуюся цифровую трансформацию государственного и муниципального управления, экономики, оборонной и социальной сферы.*

Ключевые слова*: анализ данных, архитектура, дата-центр, нейроморфные алгоритмы поиска, нейроморфные вычисления, нейроморфный процессор, новые физические принципы.*

Актуальность

В рамках одной из национальных целей развития Российской Федерации на перспективу до 2036 года ключевым трендом развития фактически всех основных направлений цифровой трансформации государственного и муниципального управления, экономики, оборонной и социальной сферы является создание современных высокотехнологичных дата-центров (ДЦ),

способных обеспечить оперативный, непрерывный, безопасный и достоверный анализ Больших Данных, мультимодальных моделей объектов и процессов, их обработку с помощью искусственного интеллекта, а также способных учитывать структуру огромных массивов информации, хранящейся и обрабатываемой в интересах дальнейшего эффективного развития страны [1, 2]. Анализ показывает, что особые требования в рамках проектирования, построения и совершенствования ДЦ, составляющих основу современной *IT*-инфраструктуры страны, могут и, безусловно, должны быть предъявлены к центрам обработки данных специального назначения (СН) – защищенным ДЦ, ориентированным на хранение и обработку информации в интересах объектов критической информационной инфраструктуры государства, объектов военно-промышленного комплекса, оборонной сферы и охраны правопорядка [3-7].

Роль и значимость ДЦ СН в *IT*-инфраструктуре государства переоценить трудно, именно поэтому перспективам их развития в современных условиях уделяется особое внимание. Речь идет и об организационных подходах к построению ДЦ СН и о новых перспективных технологиях и средствах обработки и хранения данных.

При этом направлениями и актуальными (прогрессивными и потенциально многообещающими) технологическими аспектами построения и совершенствования перспективных ДЦ СН (разумеется, с учетом импортозамещения и привлечения технологий искусственного интеллекта) принято считать: новое программное обеспечение (ПО) для ДЦ, квантовые и нейроморфные вычислители, технологии построения систем хранения на основе гелиевых дисков, кварцевых и керамических носителей, твердотельных накопителей (*SSD*) и технологии на основе ДНК, средства и ПО автоматизации бизнеса, автоматизации и управления событиями информационной безопасности и защиты веб-приложений, приложения для видеоконференцсвязи, графики и дизайна, средства и ПО в интересах защищенности ДЦ СН (защита данных, защита конечных точек, защита от утечек данных (*DLP*) и киберграмотность персонала ДЦ СН), клиентские операционные системы, менеджеры паролей доступа к ресурсам ДЦ СН, средства и ПО мониторинга инфраструктуры, сервисы ДЦ СН для работы с мультимедиа (включая облачные платформы) и с локальными и облачными офисными приложениями, с платформами и средами разработки, почтовыми системами и другое.

Иными словами, перспективные ДЦ СН, помимо базовых функций по поиску, хранению и обработке информации, должны работать с различными операционными системами и обладать возможностью развертывания на их основе высокотехнологичных САПР, систем и средств визуализации и виртуализации, возможностью обеспечения безопасности данных и процессов, мониторинга, резервного копирования и быстрого восстановления данных.

Они должны обладать автономными системами оптической связи для обмена данными, управления базами данных, службами каталогов и средствами разработки, должны иметь скоростной терминальный доступ и позволять пользователям управлять *IT*-активами, проектами и процессами, рабочими местами, различными системами виртуализации, должны иметь программно определяемое хранилище (*SDS*) [7-9].

Одним из наиболее обладающих потенциалом подходов к повышению эффективности функционирования перспективных ДЦ СН, по нашему мнению, является подход, ориентированный на нейроморфные вычисления (НМВ) и нейроморфные алгоритмы поиска (НМАП) данных на ресурсах перспективных дата-центров такого класса [10, 11].

В свете этих факторов, особого внимания, на наш взгляд, заслуживают вопросы анализа и детального исследования потенциальных проблем и возможных практических подходов к реализации НМВ и НМАП на ресурсах перспективных ДЦ специального назначения, являющихся, по сути, основой *IT*-инфраструктуры, предназначенной для сложных и нетривиальных задач, к примеру, задач информационного обеспечения обороноспособности и правопорядка в Российской Федерации [12].

Особую актуальность задача анализа, систематизации и детальной формулировки проблем и возможных практических подходов к реализации НМВ и НМАП на ресурсах перспективных ДЦ СН, приобретает в наши дни, когда требования пользователей по своевременности

и достоверности вычислений (оперативной интеллектуальной обработки) больших массивов данных и требования по релевантности реализации поисковых запросов в территориально распределенных хранилищах Больших Данных, довольно высоки.

Формулировка сущности, общих и частных особенностей реализации технологии и механизмов нейроморфных вычислений и нейроморфных алгоритмов поиска на ресурсах дата-центров специального назначения

Анализ существующих подходов, посвященных внедрению отечественных и международных технологий построения отдельных цифровых приборов и компьютерных систем в целом, механизмов обработки, хранения и доступа к данным, позволяет говорить о том, что даже в рамках создания элементной базы для перспективных информационно-вычислительных систем, работающих на новых физических принципах, особые роль и место принадлежит разработке новых императивов и созданию линейки отечественных нейроморфных процессоров и иных систем для сверхбыстрой энергоэффективной обработки и передачи информации, например, на базе эффектов спинтроники и спин-фотоники.

Более того, в «Плане фундаментальных научных исследований на 2021-2035 годы», разработанном Министерством науки и образования РФ и утвержденным Распоряжением Правительства РФ от 31 декабря 2020 года, рассматриваются и уже включены в этапы решения практических задач в нашей стране технологии и средства [13-20]:

- квантовые и нейроморфные вычислительные модули, включая модули и стойки ДЦ;
- нейроморфные фотонные структуры;
- технологии и средства построения 2*D* и 3*D* нейроморфных систем и, так называемых, «мозгоподобных» систем на основе интеллектуальных структур с фазовым переходом;
- технологии и средства нейроморфных наноструктур, например, мемристорный переключатель (кроссбарр) для нейроморфной системы хранения данных, стабильная мемристорная ячейка как элемент цифровой памяти ДЦ и иные технологии и средства.

Рассматривая вопросы физической сущности нейроморфных вычислений и систем, необходимо отметить, что само понятие «нейроморфный» предопределяет системный и технологический подход, ориентированный на способность систем и процессов на уровне программно-аппаратной реализации максимально точно подражать (симулировать, имитировать) процедурам и алгоритмам работы головного мозга, на способность использовать базовые биологические принципы работы этого важнейшего органа человека.

В идеале, предполагается, что существующие технологические барьеры по скорости, и достоверности обработки Больших Данных в рамках вычислительных систем и систем обработки и хранения информации, например таких, как ДЦ СН, могут и должны быть преодолены с использованием моделей искусственных нейронных сетей, конфигурация и дизайн которых копируют особенности архитектуры и идеологии работы конкретных нейробиологических систем. Это позволяет использовать подобные подходы для современных и перспективных систем искусственного интеллекта, бионики либо робототехники, а также практически везде, где требуется гибкость (адаптивность) технологических и архитектурных решений, в сочетании с высокой производительностью, но, вместе с тем, с невысоким энергопотреблением, что очень характерно для существующих и перспективных ДЦ СН.

Иными словами, речь идет о применении подходов к построению вычислительных систем и процессов, основанных на принципах работы мозга, технологически самостоятельных, но, по сути, заимствованных из биологии.

В рамках проведенного анализа сущности нейроморфных вычислений и нейроморфных систем, важно отметить, что подобная вычислительная концепция представляет собой попытку отказа от классической архитектуры компьютерных вычислений, попытку «ухода» от канонической, традиционной схемы построения компьютера, предложенной, в свое время, Джоном фон Нейманом. Как известно, согласно концепции (принципам) фон Неймана, компьютерные программы, а также исходные и результирующие данные хранятся в одной и той

же памяти и обрабатываются центральным процессором одинаково. В рамках данной архитектуры чтобы суммировать числа, первое из них необходимо взять из ячейки памяти, загрузить его в регистр микрочипа, потом извлечь из другой ячейки памяти второе число, которое помещается в другой микропроцессорный регистр. Результат суммирования загружается уже в третий регистр, откуда перезаписывается обратно в ячейки памяти.

Такие современные многоядерные процессоры, микрочипы с высокой тактовой частотой, построенные на архитектуре фон Неймана, осуществляют подобные операции довольно быстро, но современные задачи, особенно связанные с обработкой и хранением данных для работы с искусственным интеллектом, для вычислений в многослойных нейронных сетях, требуют огромной производительности, значительно происходящей возможности подобных архитектур. Такой производительности сложно добиться на вычислительной архитектуре фон Неймана, поскольку она предполагает быструю обработку большого потока данных, что, в свою очередь, предопределяет постоянное переключение между блоками обработки и блоками памяти. Наличие такой «болевой точки» архитектуры фон Неймана объективно обуславливает необходимость применения новых программно-аппаратных структур и новых реализаций микропроцессоров, способных удовлетворять возросшим требованиям по скорости и достоверности обработки Больших Данных.

Именно поэтому все чаще для решения подобных сложных задач пользователи и разработчики отдают предпочтение архитектуре нейроморфных процессоров, например, отечественных чипов «Алтай» (*AltAI*) [21, 22]. В них (в противоположность традиционной фон Неймановской архитектуре) память и вычислительные ядра расположены очень близко друг к другу, что дает возможность существенно сократить время передачи данных и, соответственно, минимизировать задержки и расход энергии. При этом в нейроморфных процессорах отсутствует необходимость обращаться к регистрам памяти и извлекать оттуда данные, поскольку все эти данные уже изначально хранится в искусственных нейронах. Это позволяет обрабатывать Большие Данные на небольшом и на не энергозатратном пользовательском (конечном) оборудовании, без необходимости привлечения дополнительных вычислительных мощностей и дорогостоящих платформ для хранения и обработки подобных данных.

Практические опыты показывают, что, например, разработанный в России нейроморфный микропроцессор «Алтай» на сравнимых по потребляемой вычислительной мощности задачах, расходует почти в одну тысячу раз меньше энергии, чем классические процессоры с параллельным вычислением и графические ускорители [21].

Эти достоинства, в отличие от традиционных и квантовых вычислений, обусловлены асинхронной и параллельной работой нейроморфных процессоров, копирующих алгоритмы работы нейронов головного мозга, которые обрабатывают не непрерывные сигналы, а подобные всплескам активности между нейронами мозга, краткие импульсы, называемые «спайками». Кроме того, эти преимущества связаны с тем фактом, что исходные и результирующие данные в нейроморфных процессорах записываются и сохраняются напрямик, без «посредников» в элементы, эмулирующие (имитирующие) нейроны головного мозга и связи (синапсы) между этими нейронами, предназначенные для обмена сигналами – спайками [23].

Рассмотренные особенности и достоинства нейроморфных процессоров и иных специализированных электронных компонентов, использующихся для нейроморфных вычислений и имитирующих работу человеческого мозга на уровне аппаратной реализации, их способность решать сложные вычислительные задачи в режиме реального времени с минимальной задержкой и невысокими энергозатратами, делают их применение ярким, востребованным и перспективным направлением в рамках совершенствования классических робототехнических комплексов, биоробототехники, автономного (беспилотного) автомобилестроения, мобильного, носимого оборудования для телекоммуникаций, а также в рамках построения современных ДЦ СН, например, модульных и мобильных (возимых и носимых, «чемоданных») центров обработки данных.

Что касается НМВ и НМАП на ресурсах ДЦ СН, подразумевается, что подобные практические задачи будут решать именно такие системы, способные обрабатывать информацию параллельно, обучаться на опыте и адаптироваться к новым ситуациям, как это делает человеческий мозг. Причем предмет нашего особого внимания – НМАП на ресурсах ДЦ СН, представляется особо перспективной областью практического приложения нейроморфных систем, позволяя существенно повысить оперативность и релевантность реализации поисковых запросов пользователей в огромных массивах хранимых данных, осуществлять сложный и многокритериальный информационный поиск в режиме реального времени и энергоэффективно. Это особенно важно в современных условиях применения ДЦ СН, когда требования к качеству реализации поисковых запросов с учетом нечеткой формулировки критериев качества и предпочтений пользователей, требования к информационно-лингвистическому обеспечению информационного поиска, к своевременности и релевантности процедур поиска на ресурсах стационарных и мобильных центров обработки и хранения такого класса повсеместно и систематически ужесточаются [6, 7, 24-26].

Анализ сущности нейроморфных преобразований, обзор общих и частных особенностей реализации технологии и механизмов НМВ и НМАП на ресурсах ДЦ СН показывают, что некоторые приемы, способы и предложения, связанные с разработкой и эффективной организацией применения таких механизмов и средств, необходимо конкретизировать, изучить и систематизировать проблемы, которые могут проявиться и уже возникают на этом пути, а также искать пути преодоления этих проблем.

Это обусловлено строгой организационной и технологической взаимосвязью предлагаемых новых приемов, способов и инициатив по применению НМВ и НМАП на ресурсах ДЦ СН, всех инновационных нейроморфных вычислительных процедур и процедур информационного поиска с реалиями проектирования и построения перспективных аппаратно-программных механизмов реализации поисковых запросов на ресурсах центров обработки данных будущего. Помимо прочего, это, прежде всего, предопределено тем фактом, что вычислительные процедуры и процессы информационного поиска на ресурсах ДЦ, планируемые к переводу на нейроморфные алгоритмы, определяют эффективность решения сложных расчетных задач, формулируют пути и практические подходы к повышению качества реализации поисковых запросов, к наращиванию реальных значений показателей качества поисковой выдачи и обработки информации.

Проблемы и возможные подходы к реализации технологии и механизмов нейроморфных вычислений и нейроморфных алгоритмов поиска на ресурсах дата-центров специального назначения

Известно, что вычисления в рамках компьютерных (и суперкомпьютерных) программно-аппаратных механизмов, вычислительных центров и центров обработки данных представляют собой процесс определения значений или результатов операций или функций с использованием математических методов и алгоритмов, традиционно включающий выполнение математических операций над числами, символами или другими объектами, обработку больших объемов количественных данных, преобразование числовой и символьной информации, а также решение конкретных задач [27, 28].

Наряду с задачами вычисления, современные и перспективные центры обработки информации, включая и ДЦ СН, осуществляют не менее важную миссию – информационный поиск, под которым понимается целенаправленная совокупность логических и технических операций по реализации поисковых запросов, имеющих конечным ориентиром нахождение конкретных данных и иной информации в форме документов, сведений о них и фактов, релевантных запросу потребителя [29, 30].

Помимо этого, к задачам информационного поиска принято относить реализацию процедур навигации пользователя по фонду (коллекции) документов, сепарацию и фильтрацию этих найденных документов, а также их дальнейшую обработку.

Обе эти базовые функции (вычисления и поиск), реализуемые на ресурсах ДЦ СН, важны и имеют большое значение для пользователей, но мы, в рамках данной статьи, остановимся на одной из них и предпримем попытку проанализировать проблемы и возможные подходы к реализации технологии и механизмов нейроморфных алгоритмов поиска на ресурсах центров обработки данных такого класса.

Известно, что информационный поиск включает несколько последовательных этапов (стадий):

1) Конкретизация (уточнение) информационной потребности пользователя;
2) Формирование (формулировка) запроса;
3) Сортировка, селекция и окончательный выбор источников информации, соответствующих запросу пользователя;
4) Отбор (извлечение) необходимой пользователю информации из информационных массивов, хранящихся на ресурсах ДЦ СН;
5) Оценка результатов реализации поискового запроса [29, 30].

Очевидно, что нейроморфные технологии и механизмы могут и должны сыграть важную роль на каждом из этих этапов (стадий).

Вместе с тем, необходимо признать, что разработка и практическое внедрение нейроморфных алгоритмов поиска информации сталкиваются с рядом проблем:

– проблемы нехватки инвестиций;
– проблемы, вызванные невозможностью использования традиционных стереотипов и традиций (парадигм), языков и опыта программирования для создания программного обеспечения нейроморфных систем и самих нейроморфных алгоритмов поиска: необходимо создавать новые инструменты и методологии для программной разработки таких алгоритмов;
– проблемы, связанные с трудоемкостью и технологической сложностью аппаратной реализации, трудности создания новых нейроморфных компьютерных чипов для имплементации поисковых алгоритмов на ресурсах ДЦ СН: сложность и дороговизна процесса проектирования и производства нейроморфного аппаратного обеспечения, стремящегося точно повторить нейронные сети головного мозга;
– проблемы, обусловленные требованиями по совместимости, по интеграции с существующими поисковыми системами (например, сложности, связанные с ограничениями по передаче данных в рамках нейроморфных алгоритмов поиска);
– проблемы персонала, относящиеся к подготовке программистов и аппаратчиков, обладающих необходимыми специализированными знаниями и навыками для эксплуатации нейроморфного аппаратного обеспечения в интересах информационного поиска;
– этические проблемы, связанные с нейроморфными алгоритмами поиска, похожие на общемировые этические проблемы применения искусственного интеллекта и затрагивающие вопросы моральных норм, сферы применения таких алгоритмов и ответственностью за результаты их работы;
– проблемы правовых норм и стандартов, а также общего законодательного регулирования в сфере нейроморфных систем и алгоритмов.

Более того, при решении этих проблем ключевым вопросом остается необходимость гармонично согласовать, сбалансировать потенциальные плюсы разработки нейроморфных систем и алгоритмов с возможными рисками и угрозами.

Возможные подходы к реализации технологии и механизмов нейроморфных поисковых систем и алгоритмов информационного поиска могут и должны содержать в своей основе:

– создание новых нейроморфных программно-аппаратных архитектур, встраиваемых в подсистемы поиска ДЦ СН,

– использование специальных компонентов и материалов, способных помочь осуществить на практике принципы работы биологических нейронных сетей.
– внедрение инновационных способов и регламентов нейроморфного поиска,

Эти подходы позволят создать энергоэффективные, быстрые и гибкие нейроморфные поисковых системы и алгоритмы информационного поиска, которые могут имитировать сложные поисково-когнитивные функции биологических организмов.

При этом в рамках направления, отвечающего за создание новых нейроморфных программно-аппаратных архитектур, встраиваемых в подсистемы поиска ДЦ СН, должны быть созданы структуры с, так называемым, «массовым параллелизмом», обеспечивающие возможность одновременной и согласованной работы огромного количества поисковых либо вычислительных элементов.

Вторым аспектом в рамках направления, отвечающего за создание новых нейроморфных программно-аппаратных архитектур, является, так называемая технология *IMC* (*In-Memory Computing*) – «вычисления в памяти», обработка, хранение и поиск данных, а также осуществление типовых математических операций непосредственно в месте хранения. Именно это отличает нейроморфные операции и позволяет минимизировать задержки при передаче данных между процессором и памятью [31].

Третьим перспективным аспектом создания и совершенствования нейроморфных программно-аппаратных архитектур для вычислительных и поисковых систем, а также алгоритмов информационного поиска на ресурсах перспективных ДЦ СН, принято считать «разреженные вычисления». Так называют методологию эффективного использования только части (чаще – незначительной части) находящихся в распоряжении и доступных вычислительных и поисковых ресурсов, что существенно сокращает энергопотребление нейроморфных программно-аппаратных архитектур для вычислительных и поисковых систем, в сравнении с цифровыми архитектурами, которые всегда оперируют всеми элементами, независимо от необходимости их задействования [32].

И наконец, четвертым важным аспектом в рамках направления, регулирующего создание новых нейроморфных программно-аппаратных архитектур в интересах поиска информации на ресурсах ДЦ СН, является, поддержка импульсных нейронных сетей. Под этим понимается создание архитектуры, опирающейся на базовый принцип работы биологических нейронных сетей – импульсное кодирование информации, причем данный принцип, помимо прочего позволяет нейроморфным программно-аппаратным архитектурам эффективно работать в реальном времени, обрабатывая данные в рамках поисковых запросов на уровне событий.

Создание и совершенствование нейроморфных алгоритмов информационного поиска, представляющих собой специализированные алгоритмы реализации поисковых запросов на ресурсах ДЦ СН с использованием нейроморфных систем (процессоров), предопределяет наделение их способностью не только обучаться, но и адаптироваться к поисковым запросам пользователей, по аналогии с реальными, «живыми» нейросетями. При этом обучение и адаптация к поисковым запросам пользователей в рамках работы нейроморфных алгоритмов информационного поиска на ресурсах ДЦ СН могут быть осуществлены на основе:

– комбинированного подхода, когда система поиска и поисковые алгоритмы «тренируют» при помощи стандартных алгоритмов обучения, потом параметры нейронной сети записывают в компаративную (эквивалентную) спайковую нейроморфную поисковую систему;
– имитационного подхода, когда система поиска и поисковые алгоритмы обучаются на основе имитации биологических правил (примером могут служить правила синаптического обучения, использующие алгоритм *Spike-Timing-Dependent Plasticity* (*STDP*) – алгоритм регулировки силы синаптических связей между нейронами на основе относительного времени действия их потенциалов (или спайков);
– программный подход к обучению и адаптации нейроморфных алгоритмов информационного поиска на ресурсах ДЦ СН, основанный на использовании алгоритма

обратного распространения ошибки, при воплощении которого в жизнь все вычисления для обновления весов нейронных связей проводятся вне архитектуры нейроморфной поисковой системы.

Важным частным аспектом имплементации возможных подходов к совершенствованию технологии и механизмов нейроморфных систем и реализуемых с их помощью нейроморфных алгоритмов поиска на ресурсах ДЦ СН, является использование новых материалов, в корне отличных, по своим физическим свойствам, например, от традиционной кремниевой основы (кремниевых пластин), на которой производят классические процессоры. Развитие такого направления совершенствования подходов к построению нейроморфных систем и нейроморфных алгоритмов поиска на ресурсах ДЦ СН идет по пути:

– применения мемристоров в качестве основы для создания нейроморфных искусственных нейронов и синапсов, что позволяет создавать элементы, способные «запоминать» количество протекшего через него заряда и в зависимости от этого менять свое сопротивление;
– использования сегнетоэлектрических материалов, что позволяет создавать элементы (твердые диэлектрики), способные стать основой искусственных аналогов нейронов и синапсов.

Применение предложенных подходов, как с точки зрения создания новых программно-аппаратных архитектур поиска, так и с точки зрения подходов к обучению и адаптации подобных алгоритмов, а также использование новых материалов, позволит эффективно использовать нейроморфные вычисления и нейроморфные поисковые алгоритмы для задач реализации сложных поисковых запросов на Больших Данных, где требуются обучение, адаптация и быстрая обработка огромных объемов сложной мультимодальной информации, особенно в условиях ограниченной мощности и конечной (лимитированной) энергии.

При этом огромным достоинством подобных нейроморфных систем и алгоритмов является их способность обучаться «на лету», непосредственно в процессе работы, что, в конечном итоге, делает их гибче и «разумнее», «сообразительнее». Такие нейроморфные системы и алгоритмы способны параллельно и оперативно обрабатывать информацию, поэтому подходят для задач, связанных с поиском и анализом изображений (распознаванием образов), видео и других больших массивов данных, что позволяет говорить об их большом потенциале в рамках создания новых, перспективных технологических и методологических подходов к вычислению и информационному поиску на ресурсах дата-центров специального назначения.

Выводы

Подробный и тщательный анализ сущности, общих и частных особенностей реализации технологии и механизмов НМВ и НМАП на ресурсах ДЦ СН показывает, что это направление развития информационных систем выходит на передовые позиции в науке и практике построения перспективной *IT*-инфраструктуры государства, включая чувствительные элементы критической информационной инфраструктуры. В то же время, нельзя отрицать, что пока не решены на должном законодательном, этическом, теоретическом, методологическом и практическом уровне некоторые проблемы проектирования, построения и применения технологии и механизмов НМВ и НМАП с учетом возможных ограничений по элементной базе, с учетом закономерностей, алгоритмов, структуры и условий применения отдельных процедур и программно-аппаратных средств для реализации подобных перспективных нейроморфных инструментов. С учетом этих обстоятельств, предпринята попытка детально проанализировать современные и перспективные подходы к применению на практике новых технологических и иных инноваций, ориентированных на нейроморфные вычисления, и напрямую касающихся тенденций построения и совершенствования ДЦ СН, причем с учетом импортозамещения и привлечения технологий искусственного интеллекта. Определены и сформулированы предложения по использованию, для построения механизмов НМВ и НМАП, материалов на новых физических принципах,

призванных придать новый импульс развитию процедур и программно-аппаратных средств для имплементации перспективных вычислений и эффективной реализации поисковых запросов.

Ожидается, что результаты этого анализа, сформулированные и обоснованные частные и общие подходы к реализации технологии и механизмов нейроморфных вычислений и нейроморфных алгоритмов поиска, позволят по новому, с единых системных позиций, взглянуть на физическую сущность нейроморфных процессов и программно-аппаратных средств для их реализации, позволят более реалистично и подробно описать дальнейшие инфокоммуникационные направления и вехи цифровой трансформации государственного и муниципального управления, экономики, оборонной и социальной сферы.

Литература

1. Указ Президента РФ от 07.05.2024. № 309 «О национальных целях развития Российской Федерации на период до 2030 года и на перспективу до 2036 года». – М.: Управление делами Президента РФ, 2024. – 13 с.

2. Распоряжение Правительства Российской Федерации от 16.03.2024 г. № 637-р «Об утверждении стратегического направления в области цифровой трансформации государственного управления». – М.: Управление делами Правительства РФ, 2024. – 102 с.

3. Докучаев В. А., Запольских С. В., Маклачкова В. В., Матросов В. М., Шведов А. В., Щербина О. В. Архитектура цифровых платформ для защищенных ЦОД. Общие подходы и используемые технологии: учебное пособие. Ч. 1. – М.: МТУСИ, 2021. – 90 с.

4. Нагорный К. Д., Чеснов А. А., Чирков Т. А. Эксплуатация ЦОД: Практическое руководство. – М.: Альпина ПРО, 2024. – 320 с.

5. Прохоров А. Н., Рахматуллин С. А. Центры обработки данных: анализ, тренды, мировой опыт: корпоративное издание / научное редактирование: К. Королев, И. Дорофеев. – М.: АльянсПринт, 2021. – 414 с.

6. Паращук И. Б., Михайличенко Н. В. Эффективность современных центров обработки данных // III Межрегиональная научно-практическая конференция «Перспективные направления развития отечественных информационных технологий». Материалы конференции. – Севастополь: СевГУ, 2017. С. 24-26.

7. Елизаров В. В., Паращук И. Б., Салюк Д. В. Обоснование требований к программно-аппаратным комплексам специального назначения для сбора и обработки информации на основе методов интеллектуального анализа большого количества разнородных и неструктурированных данных // Техника средств связи. 2024. № 1 (165). С. 76-89.

8. Касумов В. А., Алиева Ш. Х., Гарашлы Т. Д., Асадова М. Я. Современные технологии хранения данных в условиях Industry 4.0 // Доклады БГУИР. 2024. Т. 22, № 5, С. 95-103.

9. Лихачев Н. И., Иванов Д. В. Сравнительный анализ технологий PON систем // Международный журнал информационных технологий и энергоэффективности. 2024. Т. 9, № 5 (43). Ч. 1. С. 5-12.

10. Буряков А. М., Жемеров Е. И., Ильин Н. А. От биологических нейронов к нейроморфным чипам: введение в новые горизонты искусственного интеллекта. Монография. – М.: Мир науки, 2024. [Электронный ресурс]. URL: https://izd-mn.com/PDF/53MNNPM24.pdf (дата обращения: 16.11.2025).

11. Нейроморфные фотонные структуры: сборник научных работ / Под редакцией Г. С. Мельникова. – Ростов-на-Дону: 2022. 280 с.

12. Zhang W., Gao B., Tang J., Yao P., et al. Neuro-inspired computing chips. *Nature Electronics*, 2020, vol. 7, no. 3, pp. 371-82.

13. Kimura M., Shibayama Y., Nakashima Y. Neuromorphic chip integrated with a large-scale integration circuit and amorphous-metal-oxide semiconductor thin-film synapse devices. *Scientific Reports*, 2022, no. 12, v. 1, pp. 3-30.

14. Abdallah A. B., Dang K. N. Neuromorphic Computing Principles and Organization. – Cham: *Springer*. 2022. 436 p.

15. Miller D. Neuromorphic Computing: How Brain-Inspired Chips, Spiking Neural Networks, and Energy-Efficient AI Are Shaping the Future of Technology (Ai, Inventions, Technology, Gadget reviews). NY.: CRC Press. 2025. 122 p.

16. Ежов В. Нейроморфные системы как инструмент реализации искусственного интеллекта // Электроника Наука Технологии Бизнес. 2021. № 2 (00203). С. 82-92.

17. Billaudelle S., Cramer B., Petrovici M. A., Schreiber K., Kappel D., Schemmel J., Meier K. Structural plasticity on an accelerated analog neuromorphic hardware system // Neural Networks, 2021, no. 133, pp. 11-20.

18. Фетисенкова К. А., Рогожин А. Е. Нейроморфные системы: приборы, архитектура и алгоритмы // Микроэлектроника. 2023. Т. 52, № 5. С. 404-422.

19. Морозов В. П., Белоусов В. Е., Мистров Л. Е., Сырин А. И. Свойства и информационные процессы мозга человека для разработки нейроморфных систем // Информационные системы и процессы. 2023. № 5 (74), С.48-55.

20. Moskalenko P. A., Gabdullin E. K. Neuromorphic control systems for distributed energy networks // International Journal of Professional Science, 2025, no. 2 (2), pp. 49-53.

21. Гришанов Н. В., Зверев А. В., Ипатов Д. Е. и др. Нейроморфный процессор «Алтай» для энергоэффективных вычислений // Наноиндустрия. 2020. № 2 (96). С. 531-538.

22. Волков М. Р. Нейроморфный процессор «Алтай»: будущее ИИ по-русски // Технологии. 24 июня 2025. [Электронный ресурс]. URL: https://hightech.fm/authors/mark-volkov (дата обращения: 16.11.2025).

23. Иванов А. И. Малые выборки, нейроморфные вычисления: быстрые алгоритмы оценки энтропии Шеннона-Пирсона квадратичной сложности: справочник. – Пенза: ПГУ, 2023. 32 с.

24. Саяркин Л. А., Паращук И. Б., Владимирова Е. С. Этапы и особенности разработки методики повышения качества информационного поиска на ресурсах современных центров обработки данных с использованием нечетких отношений предпочтения и сравнения альтернатив // Информация и космос. 2024. № 1. С. 38-45.

25. Паращук И. Б., Саяркин Л. А. Аналитическая марковская модель информационного поиска в облачных хранилищах с учетом нечеткой формулировки критериев качества и предпочтений пользователей // Системы управления, связи и безопасности. 2025. № 2. С. 1-17.

26. Владимирова Е. С., Салюк Д. В., Саяркин Л. А., Паращук И. Б. Информационно-лингвистическое обеспечение процедур и программно-аппаратных средств реализации поисковых запросов на ресурсах дата-центров: анализ и формулировка современных требований // Техника средств связи. 2025. № 1 (169). С. 72-83.

27. Гаврилов К. В. Математические методы в компьютерной арифметике. – Новосибирск: Изд-во НГТУ, 2022. 100 с.

28. Саенко И. Б., Паращук И. Б., Авраменко В. С. и др. Информатика. Технологии искусственного интеллекта: учебное пособие. – СПб.: ВАС, 2025. 176 с.

29. Маннинг К., Рагхаван П., Шютце Х. Введение в информационный поиск. М.: Вильямс, 2020. 529 с.

30. Основы информационного поиска // LiveJournal. 14 февраля 2014. [Электронный ресурс]. URL: https://gpib.livejournal.com/30662.html (дата обращения: 16.11.2025).

31. Lepri N., Glukhov A., Cattaneo L., Farronato M., Mannocci P., Ielmini D. In-Memory Computing for Machine Learning and Deep Learning. *IEEE Journal of the Electron Devices Society*, 2023, no. 99, pp. 1-15.

32. Нейроморфные технологии // ООО «Поликетон». – М.: 2024. [Электронный ресурс]. URL: https://memrilab.polyketon.ru/ru/ (дата обращения: 16.11.2025).

References

1. Ukaz Prezidenta RF ot 07 maya 2024 g. № 309 «O nacional`ny`x celyax razvitiya Rossijskoj Federacii na period do 2030 goda i na perspektivu do 2036 goda» [Decree of the President of the Russian Federation of May 7, 2024 No. 309 "On the national development goals of the Russian Federation for the period up to 2030 and for the perspective up to 2036"]. – M.: Upravlenie delami Prezidenta RF, 2024. 13 p. (in Russian).

2. Rasporyazhenie Pravitel`stva Rossijskoj Federacii ot 16.03.2024 g. № 637-r «Ob utverzhdenii strategicheskogo napravleniya v oblasti cifrovoj transformacii gosudarstvennogo upravleniya» [Order of the Government of the Russian Federation dated 16.03.2024 No. 637-r "On approval of the strategic direction in the field of digital transformation of public administration"]. Moscow. Upravlenie delami Pravitel`stva RF, 2024. 102 p. (in Russian).

3. Dokuchaev V. A., Zapolskix S. V., Maklachkova V. V., Matrosov V. M., Shvedov A. V., Shherbina O. V. Arxitektura cifrovy`x platform dlya zashhishhenny`x CzOD. Obshhie podxody` i ispol`zuemy`e texnologii: uchebnoe posobie [Architecture of digital platforms for secure data centers. General approaches and technologies used: a tutorial]. Ch.1. Moscow Technical University of Communication and Informatics (MTUCI). Moscow, 2021. 90 p. (in Russian).

4. Nagornyj K. D., Chesnov A. A., Chirkov T. A. E`kspluataciya CzOD: Prakticheskoe rukovodstvo [Data Center Operation: A Practical Guide]. Moscow. Al`pina PRO Publ., 2024. 320 p. (in Russian).

5. Proxorov A. N., Raxmatullin S. A. Centry` obrabotki danny`x: analiz, trendy`, mirovoj opy`t: korporativnoe izdanie [Data centers: analysis, trends, global experience: corporate publication] nauchnoe redaktirovanie: K. Korolev, I. Dorofeev. Moscow. Al`yansPrint, 2021. 414 p. (in Russian).

6. Parashchuk I. B., Mixajlichenko N. V. E`ffektivnost` sovremenny`x centrov obrabotki danny`x [Efficiency of modern data centers]. III Mezhregional`naya nauchno-prakticheskaya konferenciya "Perspektivny`e napravleniya razvitiya otechestvenny`x informacionny`x texnologij". Materialy` konferencii. Sevastopol`. Sevastopol` State University (SevSU), 2017, pp. 24-26 (in Russian).

7. Elizarov V. V., Parashchuk I. B., Salyuk D. V. Sustification of requirements for special-purpose hardware and software systems for collecting and processing information based on methods of intelligent analysis of large amounts of heterogeneous and unstructured data. *Means of Communication Equipment*, 2024, no. 1 (165), pp. 76-89 (in Russian).

8. Kasumov V. A., Alieva Sh. X., Garashly` T. D., Asadova M. Ya. Sovremenny`e texnologii xraneniya danny`x v usloviyax Industry 4.0 [Modern data storage technologies in the context of Industry 4.0]. *Doklady Belorusskogo gosudarstvennogo universiteta informatiki i radioe`lektroniki*, 2024, vol. 22, no. 5, pp. 95-103 (in Russian).

9. Lixachev N. I., Ivanov D. V. Sravnitel`ny`j analiz texnologij PON sistem [Comparative analysis of PON systems technologies]. *International Journal of Information Technology and Energy Efficiency*, 2024, vol. 9, no. 5 (43), part. 1, pp. 5-12 (in Russian).

10. Buryakov A. M., Zhemerov E. I., Il`in N. A. Ot biologicheskix nejronov k nejromorfny`m chipam: vvedenie v novy`e gorizonty` iskusstvennogo intellekta. Monografiya [From Biological Neurons to Neuromorphic Chips: An Introduction to New Horizons in Artificial Intelligence. Monograph]. Moscow. Mir nauki Pabl., 2024. [E`lektronny`j resurs]. URL: https://izd-mn.com/PDF/53MNNPM24.pdf (data access: 16.11.2025) (in Russian).

11. Nejromorfny`e fotonny`e struktury`: sbornik nauchny`x rabot [Neuromorphic photonic structures: collection of scientific papers]. Pod redakciej G.S. Mel`nikova. Rostov-na-Donu, 2022. 280 p. (in Russian).

12. Zhang W., Gao B., Tang J., Yao P., et al. Neuro-inspired computing chips. *Nature Electronics*, 2020, no. 3, vol.7, pp. 371-382.

13. Kimura M., Shibayama Y., Nakashima Y. Neuromorphic chip integrated with a large-scale integration circuit and amorphous-metal-oxide semiconductor thin-film synapse devices. *Scientific Reports*, 2022, no. 12, vol. 1, pp. 3-30.

14. Abdallah A. B., Dang K. N. Neuromorphic Computing Principles and Organization. Cham. *Springer*, 2022, 436 p.

15. Miller D. Neuromorphic Computing: How Brain-Inspired Chips, Spiking Neural Networks, and Energy-Efficient AI Are Shaping the Future of Technology (Ai, Inventions, Technology, Gadget reviews). NY. CRC Press. 2025. 122 p.

16. Ezhov V. Nejromorfny`e sistemy` kak instrument realizacii iskusstvennogo intellekta [Neuromorphic systems as a tool for implementing artificial intelligence]. E`lektronika Nauka Texnologii Biznes, 2021, no. 2 (00203), pp. 82-92 (in Russian).

17. Billaudelle S., Cramer B., Petrovici M. A., Schreiber K., Kappel D., Schemmel J., Meier K. Structural plasticity on an accelerated analog neuromorphic hardware system. *Neural Networks*, 2021, no. 33, pp. 11-20.

18. Fetisenkova K. A., Rogozhin A. E. Nejromorfny`e sistemy`: pribory`, arxitektura i algoritmy` [Neuromorphic systems: devices, architecture and algorithms]. *Mikroe`lektronika*, 2023, vol. 52, no. 5, pp. 404-422 (in Russian).

19. Morozov V. P., Belousov V. E., Mistrov L. E., Sy`rin A. I. Svojstva i informacionny`e processy` mozga cheloveka dlya razrabotki nejromorfny`x system [Properties and information processes of the human brain for the development of neuromorphic systems]. *Informacionny`e sistemy` i processy`*, 2023, no. 5 (74), pp. 48-55 (in Russian).

20. Moskalenko P. A., Gabdullin E. K. Neuromorphic control systems for distributed energy networks. *International Journal of Professional Science*, 2025, no. 2 (2), pp. 49-53.

21. Grishanov N. V., Zverev A. V., Ipatov D. E. i dr. Nejromorfny`j processor «Altaj» dlya e`nergoe`ffektivny`x vy`chislenij [Neuromorphic processor "Altai" for energy-efficient computing]. *Nanoindustriya*, 2020, no. 2 (96), pp. 531-538 (in Russian).

22. Volkov M. R. Nejromorfny`j processor «Altaj»: budushhee II po-russki [Neuromorphic processor "Altai": the future of AI in Russian]. Texnologii. 24 iyunya 2025. [E`lektronny`j resurs]. URL: https://hightech.fm/authors/mark-volkov (data access: 16.11.2025) (in Russian).

23. Ivanov A. I. Maly`e vy`borki, nejromorfny`e vy`chisleniya: by`stry`e algoritmy` ocenki e`ntropii Shennona-Pirsona kvadratichnoj slozhnosti: spravochnik [Small Samples, Neuromorphic Computing: Fast Algorithms for Estimating Shannon-Pearson Entropy with Quadratic Complexity: A Handbook]. Penza, Penza State University Publ., 2023, 32 p. (in Russian).

24. Sayarkin L. A., Parashchuk I. B., Vladimirova E. S. E`tapy` i osobennosti razrabotki metodiki povy`sheniya kachestva informacionnogo poiska na resursax sovremenny`x centrov obrabotki danny`x s ispol`zovaniem nechetkix otnoshenij predpochteniya i sravneniya al`ternativ [Stages and features of developing a methodology for improving the quality of information retrieval on the resources of modern data processing centers using fuzzy relations of preference and comparison of alternatives]. *Informaciya i kosmos*, 2024, no. 1, pp. 38-45 (in Russian).

25. Parashchuk I. B., Sayarkin L. A. Analytical Markov model of information retrieval in cloud storages taking into account fuzzy formulation of quality criteria and user preferences. *Systems of Control, Communication and Security*, 2025, no. 2, pp. 1-17 (in Russian).

26. Vladimirova E. S., Salyuk D. V., Sayarkin L. A., Parashchuk I. B. Information and linguistic support of procedures and software and hardware for implementing search queries on data center resources: analysis and formulation of modern requirements. *Means of Communication Equipment*, 2025, no. 1 (169), pp. 72-83 (in Russian).

27. Gavrilov K. V. Matematicheskie metody` v komp`yuternoj arifmetike [Mathematical methods in computer arithmetic]. Novosibirsk. NGTU Publ., 2022. 100 p. (in Russian).

28. Saenko I. B., Parashchuk I. B., Avramenko V. S. i dr. Informatika. Texnologii iskusstvennogo intellekta: uchebnoe posobie [Computer Science. Artificial Intelligence Technologies: Tutorial]. St. Petersburg. Military Academy of Communications, 2025. 176 p. (in Russian).

29. Manning K. D., Ragxavan P., Shyutce X. Vvedenie v informacionny`j poisk [Introduction to Information Retrieval]. Moscow. Vil`yams Publ., 2020. 529 p. (in Russian).

30. Osnovy` informacionnogo poiska [Basics of Information Retrieval]. *LiveJournal*. 14.02.2014. [E`lektronny`j resurs]. URL: https://gpib.livejournal.com/30662.html (data access: 16.11.2025) (in Russian).

31. Lepri N., Glukhov A., Cattaneo L., Farronato M., Mannocci P., Ielmini D. In-Memory Computing for Machine Learning and Deep Learning. *IEEE Journal of the Electron Devices Society*, 2023, no. 99, pp. 1-15.

32. Nejromorfny`e texnologii [Neuromorphic technologies]. Moscow. Poliketon Publ., 2024, [E`lektronny`j resurs]. URL: https://memrilab.polyketon.ru/ru/ (data access: 16.11.2025) (in Russian).

Статья поступила 17 января 2026 г.

Информация об авторах

Владимирова Елена Сергеевна – старший преподаватель кафедры (информационных технологий и компьютерных систем). Севастопольский государственный университет. Область научных интересов: анализ качества и эффективности функционирования современных информационных и компьютерных систем. Тел.: +7 978 748 57 43. E-mail: lena_vladimir@mail.ru

Салюк Дмитрий Владиславович – кандидат технических наук, доцент. Начальник отдела ПАО «Интелтех». Область научных интересов: проектирование и разработка автоматизированных систем специального назначения; технологии сбора и обработки информации. Тел.: +7 921 794 10 64. E-mail: salukdv@rambler.ru

Паращук Игорь Борисович – доктор технический наук, профессор, Заслуженный изобретатель Российской Федерации, почетный работник высшего профессионального образования Российской Федерации. Профессор кафедры (автоматизированных систем специального назначения) Военной академии связи им. Маршала Советского Союза С.М. Буденного. Область научных интересов: мониторинг информационных и телекоммуникационных систем; сетевые технологии; комплексы и средства защиты информации. Тел.: +7 911 944 36 88. E-mail: shchuk@rambler.ru.

Цыпнятов Валерий Борисович – кандидат военных наук, доцент, начальник кафедры (автоматизированных систем специального назначения) Военной академии связи им. Маршала Советского Союза С.М. Буденного. Область научных интересов: управление военными информационными и телекоммуникационными системами. Тел.: +7 921 388 65 76. E-mail: zvb097@mail.ru.

Адрес: 197342, Россия, г. Санкт-Петербург, ул. Кантемировская, д. 8.

Neuromorphic computing and neuromorphic search algorithms on the resources of promising special-purpose data centers: essence, problems and possible approaches to implementation

E. S. Vladimirova, D. V. Salyuk, I. B. Parashchuk, V. B. Tsypnyatov

Annotation: Task statement: *a comprehensive and detailed analysis of non-trivial properties and features inherent in promising neuromorphic software, hardware and procedures aimed at efficient computing and implementation of search queries on the information resources of special-purpose data centers. Study of the physical essence, general and specific aspects of the implementation of the technology and mechanisms of neuromorphic computing and neuromorphic search algorithms, the architecture of neuromorphic processors, the conditions for using such procedures and software and hardware, as well as the formulation of the main problems and analysis of potential approaches to overcoming them on the way to implementing the technology and mechanisms of neuromorphic computing and neuromorphic search algorithms on the resources of special-purpose data centers.* ***Novelty:*** *consists in the fact that the object of the study is promising neuromorphic software, hardware and procedures for computing and information retrieval on the resources of data centers, which, in turn, can serve as an innovative basis for the construction and application of new elements of the IT-infrastructure of critical*

information facilities of the state, military-industrial complex facilities, the defense sphere and law enforcement. ***The purpose*** *of the work is to analyze existing and formulate new approaches aimed at building and using promising neuromorphic software and hardware and at implementing neuromorphic computing procedures and neuromorphic search algorithms on the resources of special-purpose data centers.* ***The result:*** *consists in the fact that aspects have been studied, conditions for building and using the technology and mechanisms of neuromorphic computing and neuromorphic search algorithms have been proposed and substantiated, which in the future can form the basis for formulating private and general requirements for designing, modernizing and modifying data centers that form the basis of the modern and promising IT-infrastructure of the country. Modern and promising approaches to the practical application of new technological and other innovations focused on neuromorphic computing and search, and directly related to the trends in the construction and improvement of objects of this class, are proposed.* ***Practical significance:*** *the results of the analysis and the proposed approaches to overcoming a number of theoretical, methodological and practical problems of designing, building and applying the technology and mechanisms of neuromorphic computing and neuromorphic search algorithms, taking into account possible limitations on the element base, taking into account the patterns, algorithms, structure and conditions of application of individual procedures and software and hardware for the implementation of such promising neuromorphic tools, allow us to take a new look, from a unified systemic position, at the physical essence of neuromorphic processes and software and hardware for their implementation, will allow us to more realistically and in detail formulate further directions for the development of IT-infrastructure aimed at the ongoing digital transformation of state and municipal administration, the economy, defense and social spheres.*

Keywords*: architecture, data analysis, data center, neuromorphic computing, neuromorphic search algorithms, neuromorphic processor, new physical principles.*

Information about the authors

Elena Sergeevna Vladimirova – Senior Lecturer of the Department (Information Technologies and Computer Systems) of the Federal State Autonomous Educational Institution of Higher Professional Education "Sevastopol State University". Research interests: analysis of the quality and efficiency of modern information and computer systems. Tel.: +7 978 748 57 43. E-mail: lena_vladimir@mail.ru

Dmitry Vladislavovich Salyuk – Candidate of Technical Sciences, Associate Professor. Head of the Department of PJSC «Inteltech». Research interests: design and development of automated systems for special purposes; technologies for collecting and processing information. Tel.: +7 921 794 10 64. E-mail: salukdv@rambler.ru

Igor Borisovich Parashchuk – Doctor of Technical Sciences, Professor, Honored Inventor of the Russian Federation. Professor of the Department (Automated Special purpose Systems) of the Military Academy of Communications named after Marshal of the Soviet Union S.M. Budyonny. Research interests: monitoring of information and telecommunication systems; network technologies; complexes and means of information protection. Tel.: +7 911 944 36 88. E-mail: shchuk@rambler.ru

Valery Borisovich Tsypnyatov – Candidate of Military Sciences, Associate Professor, Head of the Department (Automated Systems for Special Purposes) at the Marshal of the Soviet Union S.M. Budyonny Military Academy of Communications. Research interests: management of military information and telecommunications systems. Tel.: +7 921 388 65 76. E-mail: zvb097@mail.ru.

Address: Russia, 197342, Saint-Petersburg, Kantemirovskaya St. 8.

Для цитирования:

Владимирова Е. С., Салюк Д. В., Паращук И. Б., Цыпнятов В. Б. Нейроморфные вычисления и нейроморфные алгоритмы поиска на ресурсах перспективных дата-центров специального назначения: сущность, проблемы и возможные подходы к реализации // Техника средств связи. 2026. № 1 (173). С. 63-75. DOI: 10.24412/2782-2141-2026-1-63-75.

For citation:

Vladimirova E. S., Salyuk D. V., Parashchuk I. B., Tsypnyatov V. B. Neuromorphic computing and neuromorphic search algorithms on the resources of promising special-purpose data centers: essence, problems and possible approaches to implementation. Means of communication equipment, 2026, № 1 (173), Pp. 63-75 (in Russian). DOI: 10.24412/2782-2141-2026-1-63-75.

МОДЕЛИРОВАНИЕ СЛОЖНЫХ ОРГАНИЗАЦИОННО-ТЕХНИЧЕСКИХ СИСТЕМ

УДК 621.396.2 DOI: 10.24412/2782-2141-2026-1-76-85

Модели и алгоритмы повышения точности оценки расстояния между объектами с помощью устройств поддерживающих стек BLE

Рахманин Д. С., Боровцов Е. Г., Крючкова Е. Н.

Аннотация. Постановка задачи: *рассмотрена актуальная проблема повышения точности оценки расстояния между устройствами в беспроводных сетях Bluetooth Low Energy (BLE) на основе измерений уровня принимаемого сигнала. Уделено основное внимание влиянию на точность оценки факторов, которые приводят к существенным ошибкам в стандартных логарифмических моделях потерь на трассе.* ***Целью работы*** *является разработка и экспериментальная верификация метода оценки расстояния между BLE-устройствами, обеспечивающего снижение влияния шумов и выбросов в измерениях уровня принимаемого сигнала при ограниченных вычислительных ресурсах.* ***Используемые методы:*** *применена медианная фильтрация временных рядов уровня принимаемого сигнала, пригодная для энергоэффективных IoT-устройств. Параметры модифицированной логарифмической модели затухания определены методом наименьших квадратов. Статистическая значимость корреляции уровня принимаемого сигнала с расстоянием верифицирована коэффициентами Пирсона и Спирмена, а также корреляцией с логарифмом расстояния; достоверность подтверждена малыми значениями p-value во всех трех вариантах расчета. Расчеты выполнены в среде Jupyter Notebook с использованием математических библиотек Python.* ***Новизна*** *состоит в том, что в отличие от существующих подходов, в работе совмещены медианная предобработка сигнала и калибровка модели по натурным данным, что обеспечивает применимость метода на ресурсоограниченных встраиваемых платформах.* ***Результат*** *заключается в том, что откалиброванная модель обеспечила низкую среднеквадратическую ошибку. Медианная фильтрация позволила сократить разброс сырых измерений. Анализ остатков подтвердил, что отклонения между модельными и медианными значениями уровня принимаемого сигнала на дистанциях от 5 до 120 м не превышают ± 6,5 dB.* ***Практическая значимость*** *заключается в том, что предложенный метод рекомендован для применения в системах навигации в помещениях, отслеживания объектов и маршрутизации в ячеистых BLE-сетях, где требуется разумный компромисс между точностью оценки расстояния и ограничениями по энергопотреблению и вычислительным ресурсам.*

Ключевые слова*: Bluetooth Low Energy, оценка расстояния, логарифмическая модель затухания, медианная фильтрация, навигация в помещениях, позиционирование, уровень принимаемого сигнала.*

Введение

Bluetooth Low Energy (*BLE*) представляет собой широко распространенную радиотехнологию, предназначенную для взаимодействия между устройств Интернета вещей и поддержки приложений ближней связи [1]. Эта технология получила широкое распространение благодаря низкому энергопотреблению и встроенной поддержке на различных мобильных платформах. В ряде практических сценариев, включая системы обнаружения местоположения, отслеживания объектов, навигацию в помещениях, поиск наиболее удачного маршрута передачи данных между узлами ячеистой *BLE* сети, требуется оценка расстояния между устройствами [2-5].

Стек *BLE* предоставляет данные об уровне принимаемого сигнала – *Received Signal Strength Indicator* (*RSSI*) в качестве индикатора, что полезно для мониторинга качества канала связи и оценки близости между устройствами [6]. Вместе с тем, в спецификации *BLE* допускается определенная вариативность в методах измерения и калибровки *RSSI*, применяемых различными производителями оборудования, что влияет на абсолютные значения *RSSI*, регистрируемые различными устройствами [7].

RSSI представляет собой логарифмическую величину, выражаемую в децибелах относительно милливатта (dBm) и отражающую мощность сигнала, принимаемого устройством [3]. Типичные значения *RSSI* для слабых сигналов находятся в диапазоне от −100 до −80 dBm, в то время как сильные сигналы могут достигать значений от −40 до −30 dBm. Важно отметить, что чем «меньше по модулю» значение *RSSI* (то есть, чем ближе оно к нулю), тем сильнее принимаемый сигнал [8]. Несмотря на то, что *RSSI* отражает уровень мощности сигнала, он не является прямым показателем расстояния. На значение *RSSI* оказывают влияние мощность передатчика, характеристики антенн, особенности среды распространения радиоволн и алгоритмы измерения, используемые в конкретной модели *BLE* модуля [2, 9].

Существующие методы и подходы к использованию технологии *BLE* позволяют решать задачи позиционирования и оценки расстояния за счет измерения *RSSI*, однако воздействие внешний факторов, таких как шум, специфика затухания и распространения сигнала в среде и прочее, приводит к ошибкам в моделях типа *log-distance path loss* [8, 10, 11].

В данной работе предлагается метод оценки расстояния на основе медианного сглаживания *RSSI*-измерения в *BLE*-сетях с использования оборудования *Nordic Semiconductor NRF54L*15 *DK*, который минимизирует влияние шумов и выбросов, улучшая аппроксимацию эмпирических данных. Разработана модифицированная модель оценки расстояния по уровню сигнала *BLE* с параметрами, полученными в *Jupyter Notebook*, показывающая среднеквадратическую ошибку менее 4 dB на дистанциях до 120 м.

Анализ факторов, влияющих на распространение радиосигнала

Для аппроксимации зависимости уровня сигнала от расстояния обычно применяется логарифмическая модель потерь на трассе (*log-distance path loss model*) [8, 10]:

$$RSSI(d) = RSSI(d_0) - 10n\log_{10}\left(\frac{d}{d_0}\right) + X_\sigma, \quad (1)$$

где: $RSSI(d)$ – средний уровень сигнала на расстоянии d; $RSSI(d_0)$ – уровень сигнала на опорном расстоянии d_0; n – показатель затухания среды (*path loss exponent*); X_σ – случайная компонента (обычно моделируется как нормальная с нулевым средним и стандартным отклонением σ в dB), учитывающая теневое затухание и флуктуации.

Важно отметить, что данная модель описывает среднее затухание сигнала. На практике, реальные измерения *RSSI* на одном и том же расстоянии демонстрируют значительную дисперсию, обусловленную многолучевым распространением сигнала и быстрыми флуктуациями [9]. Следовательно, прямое применение этой формулы без статистической обработки данных может приводить к существенным ошибкам в оценке расстояния.

На предсказуемость *RSSI* в зависимости от расстояния оказывают влияние следующие основные факторы [2, 9-11]:

- многолучевое распространение сигнала: интерференция между прямым и отраженными сигналами приводит к быстрым колебаниям уровня сигнала;
- теневое затухание: физические препятствия, такие как стены или крупные объекты, создают долговременные отклонения в уровне сигнала;
- антенны и ориентация устройств: конструкция и поляризация антенн, а также положение устройства (например, в кармане или сумке), оказывают существенное влияние на *RSSI*;
- аппаратные различия: различия в моделях чипов и аналоговой части оборудования могут приводить к смещениям и различиям в шкалах измерения *RSSI*;
- интерференция в диапазоне 2,4 ГГц: наличие других устройств, работающих в диапазоне 2,4 ГГц (например, *Wi-Fi* роутеров, радиомостов, микроволновых печей и прочее), создает помехи и искажает показания *RSSI*.

Предлагаемые методы снижения ошибок при оценке расстояния по *RSSI*

Для снижения ошибок и повышения информативности корреляционного анализа могут быть применены следующие практические подходы:

- калибровка: проведение измерений $RSSI(d_0)$ и подбор параметров n и σ для выражения (1), полученных в контрольных точках (например, на расстояниях 1 м, 2 м, 5 м) для конкретной среды [10];
- фильтрация временных рядов: использование методов фильтрации, таких как скользящее среднее, медианный фильтр или фильтр Калмана, позволяет снизить влияние быстрых колебаний сигнала [9];
- агрегация данных: вместо использования единичных измерений, применяются усредненные значения *RSSI*, полученные за определенный период времени или по нескольким пакетам данных [12];
- метод радиокарт: создание базы данных *RSSI*-векторов для известных координат в помещении и последующее сопоставление текущих измерений с данными из базы. Этот метод снижает зависимость от простых моделей распространения сигнала, но требует предварительного сбора данных [13];
- комбинирование источников данных: использование дополнительных сенсоров (акселерометр, магнитометр), данных от нескольких приемников (триангуляция/мультиантенные системы) или методов машинного обучения для построения более устойчивых моделей оценки расстояния [14];
- статистическая отчетность: при представлении результатов необходимо указывать доверительные интервалы для средних значений *RSSI* на каждом расстоянии, а также приводить распределение остатков регрессии для оценки адекватности логарифмической модели [15].

Важно разделять корреляционную связь (статистическую зависимость) между *RSSI* и расстоянием и практическую пригодность *RSSI* в качестве инструмента для оценки расстояния, которая определяется допустимой погрешностью для конкретного приложения [16].

Испытательный стенд и методика проведения эксперимента

Для изучения характера зависимости между *RSSI* и расстоянием в сетях *BLE*, были задействованы две отладочные платы, произведённые компанией *Nordic Semiconductor*, *NRF*54*L*15 *DK*. Они предоставляют надежную и стабильную работу *BLE*-стека, а также дают возможность для детального контроля параметров радиоканала и достаточно часто используются в исследовательских и прикладных проектах [17, 18].

Первая плата настраивалась как *BLE*-маяк. Задача маяка заключалась в регулярной передаче рекламных пакетов, содержащих служебную информацию. Вторая плата выполняла функцию *BLE*-сканера. Её задачей был активный приём рекламных пакетов *BLE*-маяка и фиксация соответствующих уровней сигнала *RSSI*, позволяющих судить об интенсивности принимаемого радиосигнала.

Эксперимент проводился следующим образом:

- *BLE*-маяк и *BLE*-сканер размещались на ранее определённом расстоянии друг от друга;
- для каждой выбранной дистанции осуществлялся сбор данных об уровне сигнала *RSSI*;
- сканер замерял уровень сигнала маяка с интервалом в 200 мс, что соответствовало частоте дискретизации 5 Гц.

Для каждого расстояния фиксировалось около 20 последовательных измерений *RSSI*, формирующих своего рода временной снимок уровня сигнала в конкретной точке.

Расстояние между устройствами менялось ступенчато от 1 метра до 120 метров. После завершения серии замеров на текущем расстоянии устройства переносились в следующую точку, и процесс повторялся. Результаты проведенных измерений приведены в рис 1.

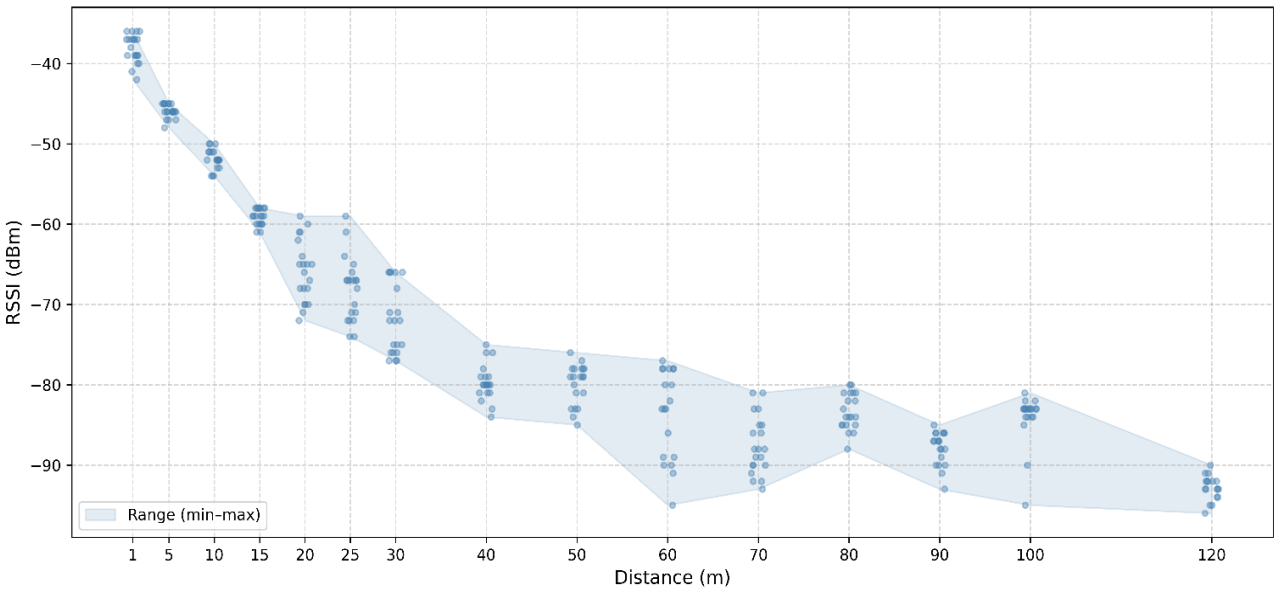


Рис. 1. Результаты измерения *RSSI* при различных расстояниях диапазона 1-120 м

Экспериментальные данные представляли собой набор временных рядов *RSSI*, полученных для различных значений расстояния. Такой формат позволял использовать методы статистического анализа для выявления закономерностей [19].

Методика эксперимента была разработана с целью:

– собрать достаточный объём данных об уровне сигнала *RSSI* для каждого заданного расстояния;
– изучить стабильность показаний *RSSI* во времени;
– найти статистическую связь между расстоянием и уровнем принимаемого сигнала;
– сравнить полученные экспериментальные данные с предсказаниями теоретической модели затухания радиосигнала.

Предварительная обработка результатов эксперимента

Значения *RSSI* в *BLE*-системах могут сильно меняться из-за многолучевого распространения радиоволн, помех в диапазоне частот 2,4 ГГц и погрешностей в работе измерительной аппаратуры. Из-за чего отдельные измерения могут давать неверные результаты.

Для сглаживания шумов применен медианный фильтр, который среди аналогичных методов выделяется низкой вычислительной сложностью $O(n \log n)$, что критично для энергоэффективных *IoT*-устройств на микроконтроллерах [20].

Медианное значение *RSSI* для каждого расстояния d вычислялось по формуле:

$$RSSI_{median}(d) = median\{RSSI_1(d), RSSI_2(d), RSSI_3(d), ..., RSSI_n(d)\}, \quad (2)$$

где: d – расстояние в метрах, n – порядковый номер измерения, $RSSI_n(d)$ – значение для n-го в dBm для расстояния d, $RSSI_{median}(d)$ – результат применения медианного фильтра для расстояния d.

Медиана является более устойчивой оценкой по сравнению со средним значением и менее восприимчива к случайным выбросам, что делает её полезной при анализе радиосигналов.

Результат применения медианного фильтра приведен на рис. 2.

Для количественной оценки взаимосвязи между расстоянием и уровнем сигнала был проведён анализ корреляции между расстоянием d и медианным значением *RSSI* [21]. Использовались следующие показатели корреляции:

– коэффициент корреляции Пирсона, определяющий степень линейной зависимости;

– коэффициент ранговой корреляции Спирмена, отражающий монотонную связь и менее чувствительный к отклонениям от линейности и выбросам.

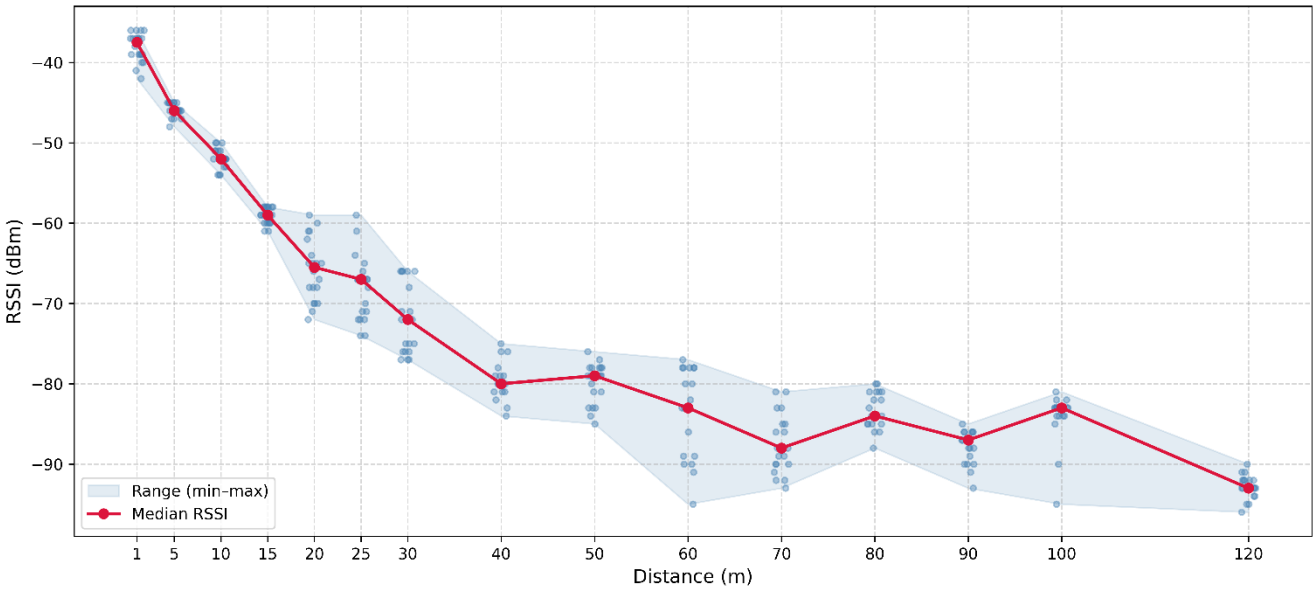


Рис. 2. Результаты применения медианной фильтрации к исходным данным *RSSI*

Был рассмотрен вариант корреляции между *RSSI* и логарифмом расстояния $\log_{10}(d)$, что соответствует предположениям о логарифмическом характере затухания радиосигнала.

Для оценки надёжности полученных значений корреляции используем *p*-значения [22].

Следует отметить, что между *RSSI* и расстоянием обычно наблюдается отрицательная корреляция: чем больше расстояние, тем ниже уровень *RSSI*.

Расчеты были выполнены с помощью инструмента *Jupyter Notebook* и математических библиотек на языке Python. Результаты расчетов приведены на рис. 3.

```
Загружено 15 точек измерений.
Корреляция между расстоянием и медианным RSSI:
  Pearson r = -0.8846 (p = 1.187e-05)
  Spearman rho = -0.9580 (p = 1.998e-08)
  Pearson (RSSI vs log10(distance)) r = -0.9702 (p = 2.203e-09)
```

Рис. 3. Результаты расчетов корреляций

Поскольку расчетное значение *p* получилось достаточно маленькое во всех трех расчетах, можно считать, что вероятность случайности мала и корреляция статистически значима [21, 22].

Аппроксимация экспериментальных данных моделью затухания

Для математического описания зависимости *RSSI* от расстояния математическую модель (1) приведем к следующему виду:

$$RSSI(d) = RSSI(1m) - 10n\log_{10}(d), \quad (3)$$

где: $RSSI(d)$ – средний уровень сигнала на расстоянии d; $RSSI(1m)$ – уровень сигнала на опорном расстоянии 1 метр; n – показатель затухания среды (*path loss exponent*).

Случайную экспоненту компонента X_σ и дробную часть логарифма учтем в константе $RSSI(1m)$, поскольку при применении математической модели в реальных условия получение

данных числовых значений затруднено и не имеет практического смысла, для определения расстояния между устройствами.

Параметры модели *RSSI*(1*m*) и *n* определим с использованием метода наименьших квадратов на основе имеющихся данных. Для оценки точности аппроксимации применим коэффициент детерминации R^2 и среднеквадратическую ошибку (*RMSE*) [23]. Расчеты произведем в *Jupyter notebook*, результаты приведены на рис. 4.

Сопоставление модели (2) и медианных точек приведены на рис. 5.

```
Параметры модели log-distance:
  RSSI(1 m) = -29.772 ± 3.102 dBm
  path-loss exponent n = 2.873 ± 0.199
  R^2 = 0.9413, RMSE = 3.917 dB
```

Рис. 4. Результаты расчетов параметров модели

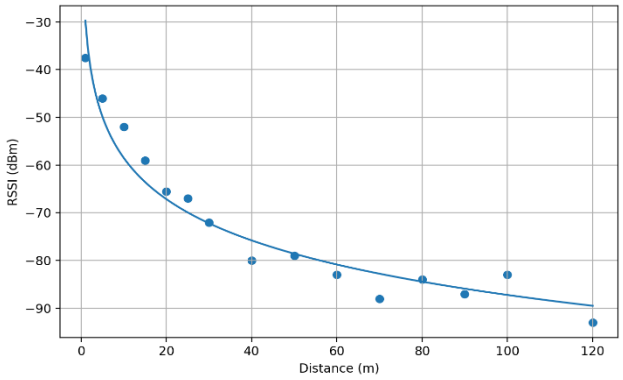


Рис. 5. Сопоставление модели и медианных точек *RSSI*

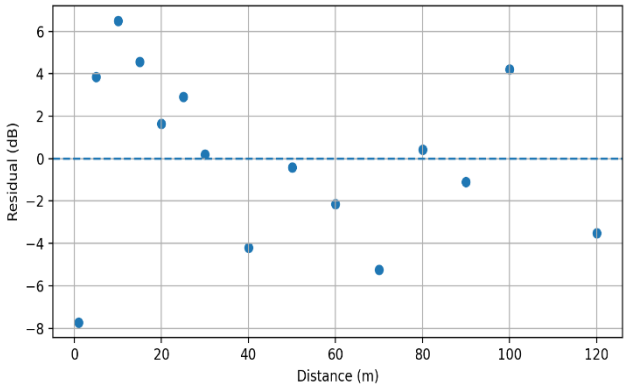


Рис. 6. Рассчитанные остатки на координатной плоскости

Расчет и анализ остатков, интерпретация результатов

Определив параметры модели (2), сопоставим значения между измеренными значения *RSSI* с применением медианного фильтра и значениями, которые были получены с помощью математической модели затухания. Разность между значениями запишем, как остаточная дисперсия. Результаты приведены на рис. 6.

Присутствие остаточной дисперсии может быть объяснено влиянием многолучевого распространения, экранированием сигнала различными объектами и невысокой точностью *RSSI* как измерительного параметра [24].

Выводы

В работе предложен и экспериментально верифицирован метод оценки расстояния между *BLE*-устройствами, основанный на медианной фильтрации измерений *RSSI* и аппроксимации логарифмической моделью затухания с параметрами, определёнными методом наименьших квадратов. Результаты подтверждают применимость подхода для диапазона расстояний от 1 до 120 м на оборудовании *Nordic Semiconductor NRF*54*L*15 *DK*.

Применение медианного фильтра позволило устранить случайные выбросы в сырых данных *RSSI*, разброс которых на отдельных дистанциях достигал 14–16 dB (например, от –59 до –72 dBm на 20 м и от –59 до –74 dBm на 25 м), и получить стабильные медианные значения для каждой контрольной точки.

Таким образом, предложенный метод медианной фильтрации в сочетании с калиброванной логарифмической моделью представляет собой практически обоснованное

решение для оценки расстояния по *RSSI* в *BLE*-системах. Полученные результаты позволяют рекомендовать данный подход для задач навигации в помещениях, отслеживания объектов и маршрутизации в ячеистых *BLE*-сетях, где требуется баланс между точностью оценки расстояния и ограничениями по энергопотреблению и вычислительным ресурсам.

Литература

1. Wang Z., Song P., Liu H. B. Research on Multipoint Mobile Network Positioning Technology Based on Bluetooth Mesh // Proceedings of the 2024 International Conference on Advanced Robotics, Automation Engineering and Machine Learning. 2024. Pp. 23-27. – DOI:10.3390/s23041826.

2. Assayag Y. et al. Adaptive path loss model for BLE indoor positioning system // IEEE Internet of Things Journal. 2023. V. 10. No. 14. Pp. 12898-12907. – DOI:10.1109/jiot.2023.3253660.

3. Guo G. et al. Multichannel and multi-RSS based BLE range estimation for indoor tracking of commercial smartphones // IEEE Sensors Journal. 2023. V. 23. No. 24. Pp. 30728-30738. – DOI:10.1109/jsen.2023.3328711.

4. Shah H. V. et al. Sustainable hardware and software design challenges for Green IoT devices // Design and Analysis of Green and Sustainable IoT Technologies for Future Wireless Communications. Academic Press, 2026. Pp. 53-70. – DOI:10.1016/B978-0-44-333000-1.00008-0.

5. Porter J., Borra V., Li F. Internet of Things Solutions for Data Acquisition from Custom Bluetooth Low Energy Peripherals //2025 IEEE World AI IoT Congress (AIIoT). IEEE, 2025. Pp. 976-981. – DOI: 10.1109/AIIoT65859.2025.11105267.

6. Arif S., Khan M. A., Rehman S. A Lightweight Received Signal Strength Indicator Estimation Model for Low-Power Internet of Things Devices in Constrained Indoor Networks //Applied Sciences. 2025. V. 15. No. 7. Pp. 3535. – DOI:10.3390/app15073535

7. Ayub A. et al. Comparative Analysis of Machine Learning Algorithms for BLE-Based Indoor Localization System // IEEE Access. 2025. V. 13. Pp. 167120-167138. – DOI:10.1109/access.2025.3609464.

8. Szyc K., Nikodem M., Zdunek M. Bluetooth low energy indoor localization for large industrial areas and limited infrastructure // Ad Hoc Networks. 2023. V. 139. Pp. 103024. – DOI: 10.1016/j.adhoc.2022.103024.

9. Janczak D. et al. Accuracy analysis of the indoor location system based on Bluetooth low-energy RSSI measurements // Energies. 2022. V. 15. No. 23. Pp. 8832. – DOI: 10.3390/en15238832.

10. Bencak P., Hercog D., Lerher T. Indoor positioning system based on bluetooth low energy technology and a nature-inspired optimization algorithm // Electronics. 2022. V. 11. No. 3. Pp. 308. – DOI:10.3390/electronics11030308.

11. Wu C. et al. Experimental Study of Bluetooth Indoor Positioning Using RSS and Deep Learning Algorithms // Mathematics. 2024. V. 12. No. 9. Pp. 1386. – DOI:10.3390/math12091386.

12. Subhan F. et al. Experimental analysis of received signals strength in Bluetooth Low Energy (BLE) and its effect on distance and position estimation // Transactions on Emerging Telecommunications Technologies. 2022. V. 33. No. 2. Pp. e3793. – DOI:10.1002/ett.3793.

13. Zholamanov B. et al. RSSI Fingerprint-Based Indoor Localization Solutions Using Machine Learning Algorithms: A Comprehensive Review // Smart Cities. 2025. V. 8. No. 5. Pp. 153. – DOI: 10.3390/smartcities8050153.

14. Ariante G., Ponte S., Del Core G. Bluetooth low energy based technology for small UAS indoor positioning // 2022 IEEE 9th international workshop on metrology for AeroSpace (MetroAeroSpace). IEEE, 2022. Pp. 113-118. – DOI: 10.1109/MetroAeroSpace54187.2022.9856321.

15. Pimentel A. A., Baldovino R. G. IoT indoor localization using design of experiment analysis and multi-output regression models // 2022 IEEE International Power and Renewable Energy Conference (IPRECON). IEEE, 2022. Pp. 1-5. – DOI:10.1109/IPRECON55716.2022.10059563.

16. Vo H. et al. Advance path loss model for distance estimation using LoRaWAN network's Received Signal Strength Indicator (RSSI) // IEEE Access. 2024. V. 12. Pp. 83205-83216. – DOI: 10.1109/ACCESS.2024.3412849.

17. Kozhubaev Y. et al. Energy efficient indoor wireless communication techniques based on BLE technology // E3S Web of Conferences. EDP Sciences, 2023. V. 389. Pp. 07011. – DOI:10.1051/e3sconf/202338907011.

18. Groth M. et al. Low-Cost Bluetooth-Based Testbed for Wireless Connectivity Testing // 2025 19th European Conference on Antennas and Propagation (EuCAP). IEEE, 2025. Pp. 1-5. – DOI: 10.23919/EuCAP63536.2025.10999268.

19. Liu X. et al. A wireless signal correlation learning framework for accurate and robust multi-modal sensing //IEEE Journal on Selected Areas in Communications. 2024. V. 42. No. 9. Pp. 2424-2439. – DOI: 10.1109/JSAC.2024.3413986.

20. Wu J. The Tiny Median Filter: A Small Size, Flexible Arbitrary Percentile Finder Scheme Suitable for FPGA Implementation // arXiv preprint arXiv:2412.05320. 2024.

21. Bocianowski J. et al. Comparison of Pearson's and Spearman's correlation coefficients for selected traits of Pinus sylvestris L // Biometrical Letters. 2024. V. 61. No. 2. Pp. 115-135. – DOI: 10.2478/bile-2024-0008.

22. Максимова О. В. Роль частного коэффициента корреляции в статистических выводах // Экологический мониторинг и моделирование экосистем. 2025. Т. 36. №. 3-4. С. 133-151. – DOI: 10.21513/0207-2564-2025-3-4-133-151.

23. Каличкин В. К. и др. Сравнение предиктивной способности моделей машинного обучения с использованием различной структуры данных // Известия Тульского государственного университета. Технические науки. 2024. №. 8. С. 395-400. – DOI: 10.24412/2071-6168-2024-8-395-396.

24. Asparouhov T., Muthén B. Residual structural equation models //Structural Equation Modeling: A Multidisciplinary Journal. 2023. Т. 30. №. 1. С. 1-31. – DOI: 10.1080/10705511.2022.2074422.

References

1. Wang Z., Song P., Liu H. B. Research on Multipoint Mobile Network Positioning Technology Based on Bluetooth Mesh. *Proceedings of the 2024 International Conference on Advanced Robotics, Automation Engineering and Machine Learning*, 2024, pp. 23-27. – DOI: 10.3390/s23041826.

2. Assayag Y. et al. Adaptive path loss model for BLE indoor positioning system. *IEEE Internet of Things Journal*, 2023, vol. 10, no. 14, pp. 12898-12907. – DOI: 10.1109/jiot.2023.3253660.

3. Guo G. et al. Multichannel and multi-RSS based BLE range estimation for indoor tracking of commercial smartphones. *IEEE Sensors Journal*, 2023, vol. 23, no. 24, pp. 30728-30738. – DOI: 10.1109/jsen.2023.3328711.

4. Shah H. V. et al. Sustainable hardware and software design challenges for Green IoT devices. *Design and Analysis of Green and Sustainable IoT Technologies for Future Wireless Communications*. – Academic Press, 2026, pp. 53-70. – DOI: 10.1016/B978-0-44-333000-1.00008-0.

5. Porter J., Borra V., Li F. Internet of Things Solutions for Data Acquisition from Custom Bluetooth Low Energy Peripherals. *2025 IEEE World AI IoT Congress* (*AIIoT*). IEEE, 2025, pp. 976-981. – DOI: 10.1109/AIIoT65859.2025.11105267.

6. Arif S., Khan M. A., Rehman S. A Lightweight Received Signal Strength Indicator Estimation Model for Low-Power Internet of Things Devices in Constrained Indoor Networks. *Applied Sciences*, 2025, vol. 15, no. 7, p. 3535. – DOI: 10.3390/app15073535.

7. Ayub A. et al. Comparative Analysis of Machine Learning Algorithms for BLE-Based Indoor Localization System. *IEEE Access*, 2025, vol. 13, pp. 167120-167138. – DOI: 10.1109/access.2025.3609464.

8. Szyc K., Nikodem M., Zdunek M. Bluetooth low energy indoor localization for large industrial areas and limited infrastructure. *Ad Hoc Networks*, 2023, vol. 139, p. 103024. – DOI: 10.1016/j.adhoc.2022.103024.

9. Janczak D. et al. Accuracy analysis of the indoor location system based on Bluetooth low-energy RSSI measurements. *Energies*, 2022, vol. 15, no. 23, p. 8832. – DOI: 10.3390/en15238832.

10. Bencak P., Hercog D., Lerher T. Indoor positioning system based on bluetooth low energy technology and a nature-inspired optimization algorithm. *Electronics*, 2022, vol. 11, no. 3, p. 308. – DOI: 10.3390/electronics11030308.

11. Wu C. et al. Experimental Study of Bluetooth Indoor Positioning Using RSS and Deep Learning Algorithms. *Mathematics*, 2024, vol. 12, no. 9, p. 1386. – DOI: 10.3390/math12091386.

12. Subhan F. et al. Experimental analysis of received signals strength in Bluetooth Low Energy (BLE) and its effect on distance and position estimation. *Transactions on Emerging Telecommunications Technologies*, 2022, vol. 33, no. 2, p. e3793. – DOI: 10.1002/ett.3793.

13. Zholamanov B. et al. RSSI Fingerprint-Based Indoor Localization Solutions Using Machine Learning Algorithms: A Comprehensive Review. *Smart Cities*, 2025, vol. 8, no. 5, p. 153. – DOI: 10.3390/smartcities8050153.

14. Ariante G., Ponte S., Del Core G. Bluetooth low energy based technology for small UAS indoor positioning. *2022 IEEE 9th International Workshop on Metrology for AeroSpace* (*MetroAeroSpace*). IEEE, 2022, pp. 113-118. – DOI: 10.1109/MetroAeroSpace54187.2022.9856321.

15. Pimentel A. A., Baldovino R. G. IoT indoor localization using design of experiment analysis and multi-output regression models. *2022 IEEE International Power and Renewable Energy Conference* (*IPRECON*). IEEE, 2022, pp. 1-5. – DOI: 10.1109/IPRECON55716.2022.10059563.

16. Vo H. et al. Advance path loss model for distance estimation using LoRaWAN network's Received Signal Strength Indicator (RSSI). *IEEE Access*, 2024, vol. 12, pp. 83205-83216. – DOI: 10.1109/ACCESS.2024.3412849.

17. Kozhubaev Y. et al. Energy efficient indoor wireless communication techniques based on BLE technology. *E3S Web of Conferences*. *EDP Sciences*, 2023, vol. 389, p. 07011. – DOI: 10.1051/e3sconf/202338907011.

18. Groth M. et al. Low-Cost Bluetooth-Based Testbed for Wireless Connectivity Testing. *2025 19th European Conference on Antennas and Propagation* (*EuCAP*). IEEE, 2025, pp. 1-5. – DOI: 10.23919/EuCAP63536.2025.10999268.

19. Liu X. et al. A wireless signal correlation learning framework for accurate and robust multi-modal sensing. *IEEE Journal on Selected Areas in Communications*, 2024, vol. 42, no. 9, pp. 2424-2439. – DOI: 10.1109/JSAC.2024.3413986.

20. Wu J. The Tiny Median Filter: A Small Size, Flexible Arbitrary Percentile Finder Scheme Suitable for FPGA Implementation. arXiv preprint arXiv:2412.05320. – 2024.

21. Bocianowski J. et al. Comparison of Pearson's and Spearman's correlation coefficients for selected traits of Pinus sylvestris L. *Biometrical Letters*, 2024, vol. 61, no. 2, pp. 115-135. – DOI: 10.2478/bile-2024-0008.

22. Maksimova O. V. The role of the partial correlation coefficient in statistical inference. *Ecological Monitoring and Ecosystem Modelling*, 2025, vol. 36, no. 3-4, pp. 133-151. – DOI: 10.21513/0207-2564-2025-3-4-133-151 (in Russian).

23. Kalichkin V. K. et al. Comparison of the predictive ability of machine learning models using different data structures. *Izvestiya Tula State University. Technical Sciences*, 2024, no. 8, pp. 395-400. – DOI: 10.24412/2071-6168-2024-8-395-396 (in Russian).

24. Asparouhov T., Muthén B. Residual structural equation models. *Structural Equation Modeling: A Multidisciplinary Journal*, 2023, vol. 30, no. 1, pp. 1-31. – DOI: 10.1080/10705511.2022.2074422.

Статья поступила 12 марта 2026 г.

Информация об авторах

Рахманин Данила Сергеевич – аспирант кафедры «Прикладная математика». Алтайский государственны технический университет им. И.И. Ползунова. Область научных интересов: разработка встраиваемых систем; методы построения ячеистых сетей. SPIN-код: 9722-4060, AuthorID: 1220366. E-mail: daniel.radist@gmail.com.

Боровцов Евгений Геннадьевич – кандидат технических наук, заведующий кафедрой «Прикладная математика». Алтайский государственный технический университет им. И.И. Ползунова. Область научных интересов: архитектура вычислительных систем, сети и телекоммуникации. РИНЦ AuthorID: 529678. E-mail: egb3@mail.ru.

Крючкова Елена Николаевна – кандидат физико-математических наук, профессор кафедры «Прикладная математика». Алтайский государственный технический университет им. И.И. Ползунова. Область научных интересов: искусственный интеллект, методы анализа текстов. SPIN-код: 2162-8713, AuthorID: 793489. E-mail: kruchkova_elena@mail.ru.

Адрес: Россия, 656038, г. Барнаул, Проспект Ленина, д. 46.

Models and algorithms for improving the accuracy of distance estimation between objects using devices supporting the BLE stack

D. S. Rakhmanin, E. G. Borovtsov, E. N. Kryuchkova

Annotation. Problem statement: *The relevant problem of improving the accuracy of distance estimation between devices in Bluetooth Low Energy (BLE) wireless networks based on Received Signal Strength Indicator (RSSI) measurements is considered. Primary attention is given to the impact of factors that introduce significant errors into standard logarithmic path loss models.* ***The aim of the work*** *is to develop and experimentally verify a distance estimation method for BLE devices that reduces the influence of noise and outliers in RSSI measurements under constrained computational resources.* ***Methods:*** *Median filtering of RSSI time series, suitable for energy-efficient IoT devices, is applied. The parameters of a modified logarithmic path loss model are determined by the least squares method. The statistical significance of the RSSI–distance correlation is verified using Pearson and Spearman coefficients and the correlation with the logarithm of distance; reliability is confirmed by low p-values in all three calculation variants. Computations are performed in Jupyter Notebook using Python mathematical libraries.* ***Novelt****y consists in the fact that, unlike existing approaches, the study combines median signal preprocessing with empirical model calibration, making the method applicable on resource-constrained embedded platforms.* ***Result:*** *The calibrated model showed a low root mean square error (RMSE). Median filtering reduced the spread of raw measurements. Residual analysis confirmed that deviations between model and median RSSI values do not exceed ±6.5 dB at distances from 5 to 120 m.* ***Practical relevance:*** *The proposed method is recommended for use in indoor navigation systems, asset tracking, and routing in BLE mesh networks where a reasonable trade-off between distance estimation accuracy and energy and computational constraints is required.*

Keywords: *Bluetooth Low Energy, distance estimation, logarithmic path loss model, median filtering, indoor navigation, positioning, received signal level.*

Information about the authors

Danila Sergeevich Rakhmanin – Postgraduate at the Department of Applied Mathematics, Polzunov Altai State Technical University. Research interests: embedded systems development; mesh network construction methods. SPIN code: 9722-4060, AuthorID: 1220366. E-mail: daniel.radist@gmail.com

Evgeny Gennadyevich Borovtsov – PhD, Head of the Department of Applied Mathematics, Polzunov Altai State Technical University. Research interests: computer systems architecture, networks and telecommunications. RSCI AuthorID: 529678. E-mail: egb3@mail.ru

Elena Nikolaevna Kryuchkova – PhD, Professor at the Department of Applied Mathematics, Polzunov Altai State Technical University. Research interests: artificial intelligence, text analysis methods. SPIN code: 2162-8713, AuthorID: 793489. E-mail: kruchkova_elena@mail.ru

Address: 656038, Russia, Barnaul, 46 Lenin ave.

Для цитирования:

Рахманин Д. С., Боровцов Е. Г., Крючкова Е. Н. Модели и алгоритмы повышения точности оценки расстояния между объектами с помощью устройств поддерживающих стек BLE // Техника средств связи. 2026. № 1 (173). С. 76-85 DOI: 10.24412/2782-2141-2026-1-76-85.

For citation:

Rakhmanin D. S., Borovtsov E. G., Kryuchkova E. N. Models and algorithms for improving the accuracy of distance estimation between objects using devices supporting the BLE stack. Means of communication equipment, 2026, No. 1 (173), pp. 76-85 (in Russian). DOI: 10.24412/2782-2141-2026-1-76-85.

ОБЪЕКТЫ ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ И ИННОВАЦИОННЫЕ ТЕХНОЛОГИИ В ОБЛАСТИ РАЗРАБОТКИ СРЕДСТВ ТЕЛЕКОММУНИКАЦИЙ

УДК 621.391 DOI: 10.24412/2782-2141-2026-1-86-94

Метод повышения достоверности приема информации в условиях воздействия случайных и преднамеренных помех

Катанович А. А., Шеремет А. В., Густов А. А., Цыванюк В. А.

***Аннотация. Постановка задачи**: задача повышения показателей достоверности, помехоустойчивости и помехозащищенности приема радиосигналов в каналах системы радиосвязи с расширением частотного спектра радиосигнала может быть решена на основе совершенствования способов приёма и обработки радиосигнала. Можно выделить три основных метода расширения спектра в узкополосной системе радиосвязи: линейная частотная модуляция, метод прямого расширения спектра и метод псевдослучайной перестройки рабочей частоты. В системах связи ограниченно используется комбинированный метод прямой последовательности и псевдослучайной перестройки рабочей частоты, представляющий собой последовательное применение двух методов расширения спектра. Затруднения, возникающие при повышении достоверности приема информации в условиях случайных и преднамеренных помех могут быть решены при внедрении всех возможных комбинаций базовых методов расширения спектра, включая тройные комбинации: метода прямой последовательности, линейной частотной модуляции и псевдослучайной перестройки рабочей частоты. Такой подход позволяет достичь совместного эффекта в повышении помехозащищённости. **Цель работы:** повысить достоверность приема информации в условиях воздействия случайных и преднамеренных помех при многолучевом распространении радиоволн и ограниченной энергетики линии радиосвязи за счет комбинированного применения методов расширения спектра: метода прямой последовательности, линейной частотной модуляции и псевдослучайной перестройки рабочей частоты. **Новизна:** в работе получены результаты, показывающие, что комбинированное применение методов расширения спектра создает многоступенчатую защиту сигнала от различных видов помех, причём каждый метод вносит аддитивный вклад в общий выигрыш при его обработке. **Практическая значимость:** разработан комбинированный метод расширения спектра методом прямой последовательности, линейной частотной модуляции и псевдослучайной перестройки рабочей частоты, который обеспечивает достижение технического результата, выражающегося в повышении помехозащищенности и достоверности приема информации в условиях сложной помеховой обстановки, включая воздействие случайных и преднамеренных помех, многолучевого распространения радиоволн и ограниченной энергетики радиолинии. Технический результат достигается за счет совместного применения трех методов расширения спектра с индивидуальной оптимизацией параметров линейно частотно-модулированных импульсов для каждого элемента псевдослучайной последовательности.*

***Ключевые слова:** метод линейной частотной модуляции, метод прямой последовательности, метод псевдослучайной последовательности, метод псевдослучайной перестройки рабочей частоты, помехозащищенность, случайные и преднамеренные помехи.*

Ведение

Одним из фундаментальных подходов к обеспечению помехозащищённости при передаче информации по радиоканалу является расширение спектра информационного сигнала, под которым понимается увеличение его базы. Расширение спектра позволяет снизить спектральную плотность мощности сигнала, затрудняя его обнаружение и перехват, а также обеспечивает возможность селекции полезного сигнала на фоне помех благодаря использованию согласованной обработки.

В радиосвязи известны три базовых метода расширения спектра: метод прямой последовательности (МПП), при котором информационный сигнал перемножается с псевдослучайной последовательностью (ПСП), имеющей широкий спектр; метод псевдослучайной перестройки рабочей частоты (ППРЧ), заключающийся в быстрой смене несущей частоты по псевдослучайному закону; а также метод линейной частотной модуляции (ЛЧМ), при котором частота несущей линейно изменяется в пределах импульса, что также

приводит к расширению спектра. Каждый из указанных методов обладает собственными достоинствами и недостатками, а их выбор зависит от конкретных условий применения [1, 2].

Анализ тенденций развития помехозащищённой связи свидетельствует, что потенциальные преимущества отдельных методов расширения спектра могут быть в полной мере реализованы лишь при их комплексном и комбинированном применении. Такой подход позволяет достичь совместного эффекта в повышении помехозащищённости. В системах связи ограниченно используется комбинированный метод МПП – ППРЧ, представляющий собой последовательное применение двух методов расширения спектра. В научно-технической практике активно проводятся исследования [1, 2], направленные на внедрение всех возможных комбинаций базовых методов расширения спектра, включая тройные комбинации МПП – ЛЧМ – ППРЧ. В частности, изучаются вопросы оптимизации параметров таких сигналов для достижения наилучших корреляционных характеристик и минимизации уровня боковых лепестков автокорреляционной функции (АКФ).

Перспективным направлением является применение комбинированных методов модуляции и расширения спектра для достижения предельных показателей помехоустойчивости. Примером реализации такого подхода служит технология *ELRS/LR-FHSS* (*ExpressLRS* / *Long Range-Frequency Hopping Spread Spectrum*), получившая массовое распространение в системах управления *FPV*-БПЛА [3]. Данная технология основана на комбинировании метода ППРЧ с протоколом *LoRa* (производным от ЛЧМ) и демонстрирует исключительную устойчивость к воздействию средств радиоэлектронных помех благодаря частотно-временному разнесению сигнала и высокой энергетике ЛЧМ-символов.

В [4] представлена система помехозащищенной передачи данных по радиоканалу с кодовым уплотнением и стеганографической защитой сообщений. В системе каждому биту информации ставится в соответствие ортогональная двоичная последовательность, что обеспечивает повышение помехоустойчивости за счёт кодового разделения каналов. Недостатком является отсутствие комбинированного расширения спектра с использованием ЛЧМ-сигналов, что ограничивает его помехозащищённость в условиях воздействия структурных помех и не позволяет достичь низких уровней боковых лепестков АКФ.

В [5] описан способ передачи информации с широкополосной несущей. Способ позволяет сформировать широкополосную несущую в виде произвольного случайного процесса, которую модулируют путём изменения многомерной функции распределения вероятностей в соответствии с информационным сигналом и нормируют по дисперсии. На приёмной стороне демодуляцию осуществляют путём измерения многомерной функции распределения вероятностей. Недостатком данного способа является сложность практической реализации и высокие требования к вычислительным ресурсам при обработке многомерных функций распределения, что ограничивает применение способа в системах реального времени.

Также известна система передачи данных ортогональными кодами [6]. Данная система содержит регистр сдвига передатчика, сумматоры по модулю два, формирователь ортогональных двоичных последовательностей, формирователи полярного кода, суммирующее устройство, формирующий фильтр, амплитудно-импульсный модулятор, генератор несущего колебания, демодулятор радиосигнала, корреляционные декодеры, формирователь ортогональных двоичных последовательностей в полярном коде и регистр сдвига приемника. Недостатками этих систем и способов является то, что:

- использование амплитудно-импульсной модуляции ограничивает помехоустойчивость системы, так как не позволяет реализовать когерентный приём сигнала в целом и обеспечить тактовую самосинхронизацию принимаемого сигнала;
- отсутствует механизм компенсации уровня боковых лепестков автокорреляционной функции, что снижает достоверность приёма в условиях многолучевого распространения и воздействия структурных помех;
- применяемые ортогональные последовательности имеют фиксированные параметры и не адаптируются к текущей помеховой обстановке;
- не используется потенциал ЛЧМ-сигналов для улучшения корреляционных свойств и повышения энергетической скрытности передачи.

Решение проблемы

Для повышения достоверности приема информации в условиях воздействия случайных и преднамеренных помех предлагается метод помехозащищенной передачи данных по радиоканалу на основе комбинированного способа расширения спектра сигнала. Этот метод включает формирование информационного сигнала, его расширение по спектру и передачу в эфир. Каждый информационный бит кодируют псевдослучайной последовательностью способом прямого расширения спектра, обладающим корреляционными свойствами классов последовательностей Баркера, Голда или *M*-последовательности.

При этом информационный сигнал перемножается с ПСП, имеющей широкий спектр. Каждый элемент (чип) указанных последовательностей представляют в виде линейно-частотно-модулированного импульса, причем частота несущей линейно изменяется в пределах импульса. Это приводит к расширению спектра. Каждому значению элемента последовательности ставят в соответствие ЛЧМ-импульс с определенным направлением изменения частоты (восходящий или нисходящий), промодулированного по фазе в соответствии с ПСП.

В составе пачки информационных битов индивидуально задают их параметры по длительности, начальной и конечной частоте. Указанные параметры выбирают отличными для различных ЛЧМ-импульсов. В пачке информационных битов дополнительно осуществляют быструю псевдослучайную перестройку несущей частоты передаваемого сигнала по заданному закону, обеспечивающему подавление многолучевости. При этом моменты смены несущей частоты синхронизируют с границами информационных битов или с границами пачек ЛЧМ-импульсов. На приемной стороне сигнал подвергают корреляционной обработке с использованием компенсации уровня боковых лепестков опорного сигнала, сформированного аналогично переданному. Причем в опорном сигнале используют те же индивидуальные параметры ЛЧМ-импульсов, что и в переданном сигнале [7].

Пример схемной реализации метода формирования и приема сигналов, модулированных комбинированным методом МПП – ЛЧМ – ППРЧ в системе помехозащищенной связи, приведен на рис. Функциональная схема комплекса содержит: генератор МПП расширения спектра сигнала 1, генератор ЛЧМ-чипов 2, блок формирования параметров ЛЧМ 3, комбинированный модулятор МПП – ЛЧМ 4, генератор МПП – ЛЧМ сигнала 5, генератор ППРЧ 6, синтезатор частот ППРЧ 7, смеситель 8, усилитель мощности 9, передающий комплекс 10, малошумящий усилитель 11, смеситель 12, блок синхронизации 13, генератор ППРЧ 14, генератор ЛЧМ-чипов 15, генератор МПП расширения спектра сигнала 16, синтезатор частот ППРЧ 17, блок формирования параметров ЛЧМ 18, комбинированный модулятор 19, генератор опорного МПП – ЛЧМ сигнала 20, комбинированный коррелятор 21, решающее устройство 22, приемный комплекс 23.

Генератор МПП расширения спектра сигнала 1 формирует ПСП (например, Баркера, Голда, *M*-последовательность) заданной длины, которой кодируется каждый бит информации и символы которой принимают значения +1/–1 (или 0/1 с последующим преобразованием).

Генератор ЛЧМ-чипов 2 создает ЛЧМ-импульсы с индивидуально задаваемыми параметрами для каждого чипа ПСП: длительностью, начальной и конечной частотой. Направление изменения частоты (восходящее или нисходящее) определяется знаком соответствующего элемента ПСП (например, для «+1» – восходящий ЛЧМ, для «–1» – нисходящий). Параметры могут быть фиксированными или адаптивно изменяться в зависимости от помеховой обстановки.

Блок формирования параметров ЛЧМ 3 хранит или вычисляет оптимальные значения длительности, начальной и конечной частоты для каждого чипа. Оптимизация производится по критерию минимизации уровня боковых лепестков АКФ результирующего сигнала (например, путем подбора параметров так, чтобы максимумы боковых лепестков АКФ одних импульсов компенсировались минимумами других). При адаптивном режиме блок может получать информацию о качестве канала от приемного комплекса по обратному каналу.

Комбинированный модулятор МПП – ЛЧМ 4 перемножает ЛЧМ-чипы с символами ПСП. В простейшем случае каждый чип модулируется по фазе: для «+1» ЛЧМ-импульс

передается без изменения, для «–1» – с инверсией фазы (что эквивалентно умножению на –1). В результате формируется сигнал, представляющий собой последовательность ЛЧМ-импульсов, модулированных по фазе в соответствии с ПСП.

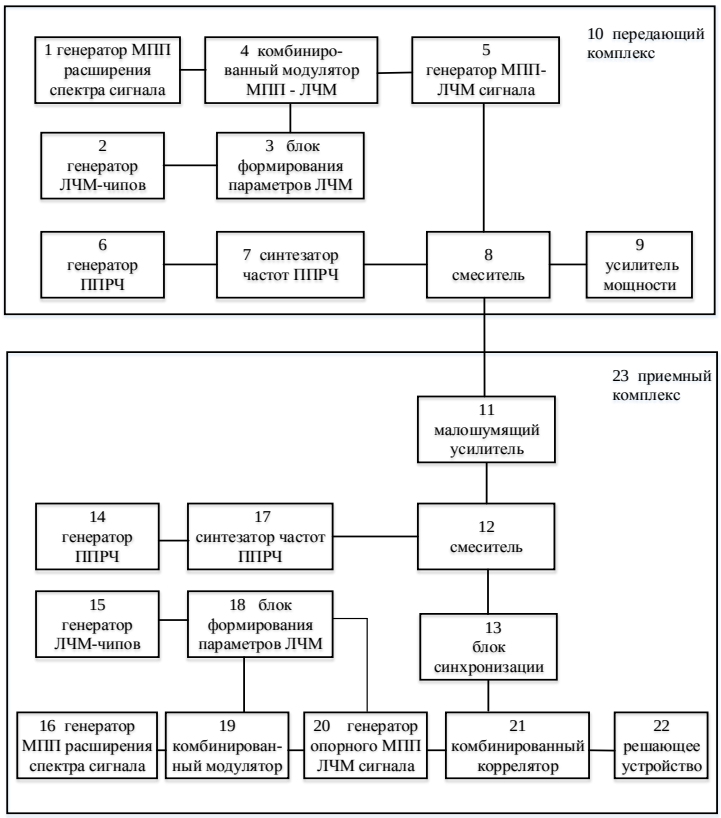


Рис.– Функциональная схема технической реализации метода формирования и приема сигналов, модулированных комбинированным методом МПП – ЛЧМ – ППРЧ в системе помехозащищенной связи

Генератор МПП – ЛЧМ сигнала 5 формирует полный сигнал, соответствующий одному информационному биту (пачка из N ЛЧМ-импульсов с заданными параметрами). На выходе – модулирующий сигнал (на промежуточной частоте).

Генератор псевдослучайной перестройки рабочей частоты 6 вырабатывает ПСП, управляющую перестройкой несущей частоты. Код ПСП определяет номер частотного канала для каждого бита (или для каждой пачки импульсов).

Синтезатор частот псевдослучайной перестройки рабочей частоты 7 – по коду ПСП формирует соответствующую несущую частоту ППРЧ с требуемой точностью и скоростью перестройки.

Смеситель 8 переносит сигнал МПП – ЛЧМ на несущую частоту, заданную синтезатором ППРЧ. В результате формируется радиочастотный сигнал.

Усилитель мощности 9 усиливает радиочастотный сигнал до уровня, необходимого для излучения в эфир.

Передающий комплекс 10 формирует и излучает в радиоканал сигнал с комбинированным расширением спектра.

Малошумящий усилитель 11 усиливает слабый сигнал, минимизируя собственный шум.

Смеситель 12 переносит принятый сигнал на промежуточную частоту путем перемножения с сигналом гетеродина. Частота гетеродина формируется синтезатором ППРЧ приемного комплекса и должна точно соответствовать частоте переданного сигнала в данный момент времени (с учетом синхронизации).

Блок синхронизации 13 обеспечивает синхронизацию приемного комплекса с передающим по времени, частоте и псевдослучайным последовательностям (как для ППРЧ, так и для МПП). Включает системы поиска и слежения за задержкой, частотой и фазой.

Генераторы опорных сигналов приемного комплекса формируют опорный сигнал, идентичный переданному (с учетом синхронизации). Они состоят из:

- генератора псевдослучайной перестройки рабочей частоты 14;
- генератора ЛЧМ-чипов 15 с теми же индивидуальными параметрами для каждого чипа (информация о параметрах либо заранее известна, либо передается служебным каналом, либо восстанавливается по принятому сигналу);
- генератора МПП расширения спектра сигнала 16;
- синтезатора частот псевдослучайной перестройки рабочей частоты 17;
- блока формирования параметров ЛЧМ 18;
- комбинированного модулятора 19 приемного комплекса, аналогичного передающему комплексу;
- генератора опорного МПП – ЛЧМ сигнала 20.

Комбинированный коррелятор 21 вычисляет взаимную корреляцию между принятым сигналом (после переноса на промежуточную частоту) и опорным сигналом. Выход коррелятора представляет собой функцию, имеющую острый пик в момент окончания пачки (бита).

Решающее устройство 22 анализирует выход коррелятора, выделяет пиковые значения и принимает решение о переданном бите (например, сравнивая амплитуду пика с порогом).

Приемный комплекс 23 принимает из радиоканала сигнал с комбинированным расширением спектра и восстанавливает переданную информацию.

Заявленный метод помехозащищённой передачи данных реализуют следующим образом.

На передающей стороне информационный бит поступает в генератор ПСП метода прямого расширения спектра сигнала 1, который формирует псевдослучайную последовательность заданной длины N (например, код Баркера длиной 5: +1, +1, +1, –1, +1). Параллельно генератор ЛЧМ-чипов 2 создаёт ЛЧМ-импульсы, параметры которых (длительность, начальная частота и конечная частота) для каждого k-го чипа индивидуально задаются блоком формирования параметров ЛЧМ 3. При этом для чипов со значением «+1» формируется восходящий ЛЧМ-импульс, а для чипов со значением «–1» – нисходящий.

В комбинированном модуляторе МПП – ЛЧМ 4 происходит перемножение ПСП и ЛЧМ-импульсов: каждый ЛЧМ-импульс умножается на соответствующий символ ПСП (+1 или –1), что эквивалентно фазовой манипуляции. В итоге формируется радиосигнал, представляющий собой пачку из N следующих друг за другом ЛЧМ-импульсов, промодулированных по фазе в соответствии с ПСП. Этот сигнал поступает в генератор МПП – ЛЧМ сигнала 5, формирующий полный радиосигнал, соответствующий одному информационному биту.

Одновременно генератор ПСП ППРЧ 6 вырабатывает псевдослучайную последовательность, управляющую синтезатором частот ППРЧ 7. Синтезатор формирует несущую частоту, которая изменяется скачкообразно от бита к биту (или от пачки к пачке) по псевдослучайному закону. В смесителе 8 происходит перенос радиосигнала МПП – ЛЧМ на несущую частоту. Полученный сигнал усиливается в усилителе мощности РПДУ 9 и излучается в радиоканал. Радиоканал – среда распространения, в которой сигнал подвергается затуханию, многолучевому распространению, аддитивному и мультипликативному шуму, а также воздействию случайных и преднамеренных помех.

На приёмной стороне принятый сигнал, поступает на малошумящий усилитель 11 приёмного комплекса, где производится его малошумящее усиление, фильтрация и, при необходимости, преобразование частоты. Усиленный сигнал подаётся на первый вход смесителя 12. На второй вход смесителя подается сигнал гетеродина, формируемый синтезатором частот ППРЧ 17, который управляется генератором псевдослучайной перестройки рабочей частоты 14. Частота гетеродина должна точно соответствовать несущей частоте переданного сигнала в данный момент времени, что обеспечивается синхронизацией генератора ПСП ППРЧ приёмного с передающим комплексами. В смесителе 12 происходит перенос принятого сигнала на промежуточную частоту. На выходе смесителя формируется сигнал промежуточной частоты, содержащий полезную составляющую МПП – ЛЧМ, а также шумы и помехи.

Далее сигнал поступает на вход комбинированного коррелятора 21, преназначенный для вычисления взаимной корреляции между принятым сигналом и опорным сигналом, который должен быть идентичен переданному. Опорный сигнал формируется следующим образом:

- генератор ПСП МПП расширения спектра сигнала 16 приёмного комплекса воспроизводит ту же псевдослучайную последовательность, что и в передающем комплексе (с учётом синхронизации по времени);
- генератор ЛЧМ-чипов 15 приёмного комплекса создаёт ЛЧМ-импульсы с параметрами (длительность, начальная и конечная частоты), которые для каждого чипа задаются блоком формирования параметров ЛЧМ 18. Эти параметры должны точно совпадать с параметрами, использованными в передатчике для соответствующих чипов. Информация о параметрах может быть заранее известна (например, храниться в памяти приёмника), передаваться по служебному каналу или восстанавливаться в процессе синхронизации;
- сформированные ЛЧМ-импульсы и ПСП поступают в комбинированный модулятор 19, идентичный модулятору передатчика. На выходе модулятора 19 получается опорный сигнал МПП – ЛЧМ, который подаётся на генератор опорного МПП – ЛЧМ сигнала 20, формирующий полный опорный сигнал (соответствующий одному информационному биту), который подаётся на второй вход коррелятора 21.

Выход коррелятора 21 анализируется решающим устройством 22. Оно выделяет максимальное значение АКФ за период, равный длительности бита, сравнивает его с заданным порогом и принимает решение о значении переданного бита. В двухканальной схеме (для различения битов «0» и «1») используются два коррелятора с опорными сигналами для «0» и «1» (например, на основе прямой и инверсной ПСП). В этом случае решающее устройство выбирает тот канал, на котором выходной сигнал больше.

Важным для работы приёмного комплекса является синхронизация его генераторов с передающим комплексом. Эту функцию выполняет блок синхронизации 13. Он подключён к выходу коррелятора 21 и анализирует положение и амплитуду главного пика. На основе этого анализа блок синхронизации формирует управляющие сигналы для:

- подстройки временной задержки опорного сигнала (чтобы главный пик приходился точно на момент окончания пачки);
- подстройки частоты гетеродина (синтезатор частот псевдослучайной перестройки рабочей частоты 17) для точного совпадения с несущей частотой;
- синхронизации генераторов ПСП (МПП и ППРЧ) по фазе и тактовой частоте.

Блок синхронизации 13 может содержать системы фазовой автоподстройки частоты, схемы поиска и слежения за задержкой (например, ранний – поздний дискриминатор) и логику захвата сигнала. В режиме поиска блок синхронизации сканирует временной диапазон и перебирает возможные фазы ПСП и частоты ППРЧ до обнаружения устойчивого корреляционного пика. После захвата синхронизации поддерживается режим слежения, обеспечивающий непрерывную работу при медленных изменениях параметров канала.

Комбинированный метод расширения спектра МПП – ЛЧМ – ППРЧ гарантирует достижение технического результата, выражающегося в повышении помехозащищенности и достоверности приема информации в условиях сложной помеховой обстановки, включая воздействие случайных и преднамеренных помех, многолучевого распространения радиоволн и ограниченной энергетики радиолинии. Указанный технический результат достигается за счет совместного применения трех методов расширения спектра с индивидуальной оптимизацией параметров ЛЧМ-импульсов для каждого элемента ПСП.

Комбинирование методов расширения спектра создает многоступенчатую защиту сигнала от различных видов помех, причём каждый уровень вносит аддитивный вклад в общий выигрыш обработки.

Защита от узкополосных помех с помощью метода прямого расширения спектра сигнала осуществляется следующим образом. Метод прямой последовательности основан на перемножении информационного сигнала с широкополосной ПСП, имеющей скорость следования символов (чипов), значительно превышающую скорость передачи информации. В

результате спектр сигнала расширяется до ширины, определяемой тактовой частотой ПСП. На приемной стороне производится корреляционное сжатие (свертка) принятого сигнала с опорной ПСП, что приводит к восстановлению исходного информационного сигнала.

Выигрыш обработки для МПП определяется отношением ширины спектра расширенного сигнала к ширине спектра информационного сигнала и численно равен длине ПСП (количеству чипов на бит). Благодаря этому выигрышу узкополосная помеха, попадающая в полосу сигнала, после корреляционной обработки подавляется по мощности, что эквивалентно снижению ее спектральной плотности до уровня шума. Таким образом, МПП обеспечивает эффективную защиту от сосредоточенных по частоте помех (например, от работающих в том же диапазоне радиостанций или преднамеренных постановщиков узкополосных помех).

Защита от широкополосных шумовых помех с использованием ЛЧМ заключается в том, что каждый информационный чип представляет собой импульс, частота которого линейно изменяется во времени. ЛЧМ-сигнал обладает важным свойством: при прохождении через согласованный фильтр в приемном комплексе происходит его сжатие во времени. В результате кратковременная мощность сигнала в момент сжатия существенно возрастает, в то время как шумовая помеха, не имеющая такой структуры, сжатию не подвергается и остаётся на прежнем уровне. Благодаря этому эффекту отношение сигнал/шум на выходе коррелятора увеличивается пропорционально произведению длительности импульса на ширину его спектра. Чем больше это произведение (чем шире полоса качания частоты и чем длиннее импульс), тем сильнее подавляется шумовая помеха.

Заключение

Таким образом, включение ЛЧМ-модуляции в комбинированный метод расширения спектра гарантирует эффективное подавление широкополосных шумовых помех, что особенно важно при работе в условиях интенсивного радиоэлектронного противодействия в каналах с низким отношением сигнал/шум. Применение ППРЧ производится для защиты от частотно-селективных помех и перехвата сигнала, который в каждый момент времени занимает узкую полосу равную полосе МПП – ЛЧМ сигнала, но эта полоса скачкообразно перемещается по широкому диапазону. Это дает следующие преимущества:

- обеспечивается устойчивость к узкополосным помехам, так как помеха фиксированной частоты может поразить только те биты (или пачки), которые передавались на этой частоте;
- затрудняется перехват и имитация сигнала, так как перехватчик, не знающий закона перестройки, не может отследить сигнал;
- производится подавление многолучевости при быстрой перестройке частоты так, как все частотные каналы не могут быть одновременно подвержены глубоким замираниям, характерным для многолучевых каналов.

Литература

1. Макаренко С. И. Помехозащищенность систем связи с псевдослучайной перестройкой рабочей частоты. – СПб.: Свое издательство, 2013. – 166 с.

2. Гантмахер В. Е., Быстров Н. Е., Чеботарев Д. В. Шумоподобные сигналы. Анализ, синтез, обработка. – СПб.: Наука и техника, 2005. – 400 с.

3. Сорокин А. В., Рылов Е. А., Гольдибаев К. В., Галузов Е. В. Исследование комбинированных методов широкополосной модуляции цифровых сигналов // Научно-техническая конференция Санкт-Петербургского НТО РЭС им. А.С. Попова, посвященная Дню радио. – 2025. – № 1 (80). – С. 100-103.

4. Система передачи данных с кодовым уплотнением и стеганографической защитой сообщений. Патент RU 2826448C2 от 11.09.2024.

5. Способ передачи информации с широкополосной несущей. Патент RU 2309547 от 27.10.2007.

6. Система передачи данных ортогональными кодами. Патент RU 2714606C2 от 18.02.2020.

7. Катанович А.А. и др. Способ помехозащищенности передачи данных по радиоканалу на основе комбинированного метода расширения спектра. Заявка на изобретения РФ № 2025107167 от 24.03.2025.

References

1. Makarenko S. I. Interference immunity of communication systems with pseudo-random frequency shifting. St. Petersburg. Svoe izdatelstvo Publ., 2013. 166 p. (in Russian).

2. Gantmakher V. E., Bystrov N. E., Chebotarev D. V. Noise-like signals. Analysis, synthesis, processing. St. Petersburg. Nauka i Tekhnika Publ., 2005. 400 p. (in Russian).

3. Sorokin A. V., Rylov E. A., Goldibaev K. V., Galuzov E. V. Research of Combined Methods of Broadband Modulation of Digital Signals // Scientific and Technical Conference of the St. Petersburg NTO of Radio Engineering and Communications named after A.S. Popov, dedicated to Radio Day. 2025, no. 1 (80), pp. 100-103 (in Russian).

4. Data transmission system with code compression and steganographic protection of messages. Patent RU 2826448C2 dated 11.09.2024 (in Russian).

5. Method of transmitting information with a broadband carrier. Patent RU 2309547 dated 27.10.2007 (in Russian).

6. Data transmission system using orthogonal codes. Patent RU 2714606C2 dated 18.02.2020 (in Russian).

7. Katanovich A. A. and others. A method for noise immunity of data transmission over a radio channel based on a combined spectrum expansion method. Application for Inventions of the Russian Federation, no. 2025107167 dated 03.24.2025.

Информация об авторах

Катанович Андреи Андреевич – доктор технических наук, профессор. Заслуженный деятель науки Российской Федерации. Заслуженный работник связи Российской Федерации. Заслуженный изобретатель Российской Федерации. Главный научный сотрудник. Научно-исследовательский институт оперативно-стратегических исследований строительства Военно-Морского Флота Военного учебно-научного центра Военно-морского флота «Военно-морская академия» (НИИ ОСИС ВМФ ВУНЦ ВМФ ВМА). Область научных интересов: системы телекоммуникаций ВМФ. Тел.: +7 921-318-46-07. E-mail: andrei.katanovitch@yandex.ru.

Адрес: Россия,198516, г. Санкт-Петербург, Петергоф, ул. Разводная, д. 17.

Шеремет Александр Витальевич – начальник научно-исследовательского центра. НИИ ОСИС ВМФ ВУНЦ ВМФ ВМА. Область научных интересов: телекоммуникационные системы Военно-Морского Флота. Тел.: +7 967-769-61-37. E–mail: sheremet_a.1974@mail.ru.

Адрес: Россия,198516, г. Санкт-Петербург, Петергоф, ул. Разводная, д. 17.

Густов Александр Александрович – доктор военных наук, профессор. Заместитель директора научно-исследовательского центра по научной работе. Публичное акционерное общество «Информационные телекоммуникационные технологии», Область научных интересов: системы и устройства телекоммуникаций. Тел.: +7 911-917-47-15. E-mail: a.gustov@inteltech.ru.

Адрес: Россия,197342. г. Санкт-Петербург, ул. Кантемировская, д. 8.

Цыванюк Вячеслав Александрович – кандидат военных наук. Почетный изобретатель Министерства обороны Российской Федерации. Старший научный сотрудник. НИИ ОСИС ВМФ ВУНЦ ВМФ ВМА. Область научных интересов: телекоммуникационные системы Военно-Морского Флота. Тел.: +7 911 267 38 27. E-mail: ciwoniuk@mail.ru.

Адрес: Россия, 198516, г. Санкт-Петербург, Петергоф, ул. Разводная, д. 17.

A method of increasing the reliability of information reception under the influence of accidental and intentional interference

A. A. Katanovich, A. V. Sheremet, A. A. Gustov, V. A. Tsyvanyuk

Annotation. *Problem statement: the task of increasing the reliability, noise immunity and noise immunity of receiving radio signals in the channels of the radio communication system with the expansion of the frequency spectrum of the radio signal can be solved by improving the methods of receiving and processing the radio signal. There are three main methods of spectrum expansion in a narrowband radio communication system: linear frequency modulation, direct spectrum expansion method, and pseudorandom frequency tuning method. In communication systems, the combined method of direct sequence and pseudorandom adjustment of the operating frequency is used to a limited extent, which is a sequential application of two methods of spectrum expansion. The*

difficulties that arise when increasing the reliability of information reception in conditions of accidental and intentional interference can be solved by implementing all possible combinations of basic spectrum expansion methods, including triple combinations: direct sequence method, linear frequency modulation and pseudorandom frequency tuning. This approach allows us to achieve a joint effect in increasing noise immunity. ***The purpose of the work:*** *to increase the reliability of information reception under the influence of knocking and deliberate interference during multipath propagation of radio waves and limited radio line energy through the combined use of spectrum expansion methods: direct sequence method, linear frequency modulation and pseudorandom tuning of the operating frequency.* ***Novelty:*** *the results obtained in the work show that the combined use of spectrum expansion methods creates multi-stage protection of the signal from various types of interference, and each method makes an additive contribution to the overall gain in its processing.* ***Practical significance:*** *a combined method of spectrum expansion using the direct sequence method, linear frequency modulation and pseudorandom adjustment of the operating frequency has been developed, which ensures the achievement of a technical result, expressed in increased noise immunity and reliability of information reception in a complex interference environment, including exposure to accidental and intentional interference, multipath propagation of radio waves and limited radio line energy. The specified technical result is achieved through the combined use of three spectrum expansion methods with individual optimization of the parameters of linearly frequency-modulated pulses for each element of the pseudorandom sequence.*

Keywords: *linear frequency modulation method, direct sequence method, pseudorandom sequence method, pseudorandom frequency chift method, noise immunity, random and intentional interference.*

Information about the authors

Andrey Andreevich Katanovich – PhD (Tech.), Professor. Honored Scientist of the Russian Federation. Honored Communications Worker of the Russian Federation. Honored Inventor of the Russian Federation. Chief Scientific Officer. The Scientific Research Institute of Operational and Strategic Studies of the construction of the Navy of the Military Training and Scientific Center of the Navy "Naval Academy" (SRI OSSC NMT SCN NA). Research interests: telecommunication systems of the Navy. Tel.: +7 921 318 46 07. E-mail: andrey.katanovitch@yandex.ru.

Address: Russia, 198516, Saint-Petersburg, Peterhof, Razvednaya str., 17.

Sheremet Alexander Vitalievich – Head of the Scientific Research Center. SRI OSSC NMT SCN NA. Research interests: telecommunication systems of the Navy. Tel.: +7 9677696137. E-mail: sheremet_a.1974@mail.ru.

Address: Russia, 198516, Saint-Petersburg, Peterhof, Razvednaya str., 17.

Gustov Alexander Alexandrovich – PhD (Mil.), Professor. Deputy Director of the Scientific Research Center for scientific work. Information Telecommunication Technologies Public Joint Stock Company (PJSC Inteltech), Research interests: telecommunication systems, networks and devices. Tel.: +7 911-917-47-15. E-mail: a.gustov@inteltech.ru

Address: Russia, 197342. Saint Petersburg, Kantemirovskaya st.,8.

Tsyvanyuk Vyacheslav Aleksandrovich – Ph.D. of Millitary Sciences. Honorary Inventor of the Ministry of Defense of the Russian Federation. Senior Researcher. The Scientific Research Institute of Operational and Strategic Studies of the construction of the Navy of the Military Training and Scientific Center of the Navy "Naval Academy". Research interests: telecommunication systems of the Navy. Tel.: +7 911-267-38-27. E-mail: ciwoniuk@mail.ru.

Address: Russia, 198516, Saint-Petersburg, Peterhof, Razvednaya str., 17.

Для цитирования:

Катанович А. А., Шеремет А. В., Густов А. А., Цыванюк В. А. Метод повышения достоверности приема информации в условиях воздействия случайных и преднамеренных помех // Техника средств связи. 2026. № 1 (173). С. 86-94. DOI: 10.24412/2782-2141-2026-1-86-94.

For citation:

Katanovich A. A., Sheremet A. V., Gustov A. A., Tsyvanyuk V. A. A method of increasing the reliability of information reception under the influence of accidental and intentional interference. Means of communication equipment, 2026, no. 1 (173), pp. 86-94 (in Russian). DOI: 10.24412/2782-2141-2026-1-86-94.

РОБОТОТЕХНИЧЕСКИЕ СИСТЕМЫ

УДК 621.396.93 DOI: 10.24412/2782-2141-2026-1-95-99

Обеспечение устойчивого доведения команд управления до беспилотных транспортных систем за счет комплексного использования радиочастотного спектра

Будко Д. Д.

Аннотация. Цель работы: *повышение оперативности и устойчивости доведения команд управления до глобально перемещающихся беспилотных транспортных систем в условиях сложной помеховой обстановки за счет применения многочастотных сигналов.* ***Новизна*** *исследования состоит в комплексном использовании каналов связи различных диапазонов радиочастотного спектра.* ***К методам*** *реализации цели можно отнести достижения в развитии технологий программно-определяемого радио когнитивных радиосистем, активных антенных систем, а также алгоритмы синтеза многочастотных сигналов в декаметровом диапазоне волн, приема и цифровой обработки командной информации по параллельным каналом связи.* ***Результат:*** *переход к режиму реального времени в процедуре управления беспилотными транспортными системами, что важно при недопущении аварийных ситуаций на высоких скоростях их перемещения, а также повышение помехоустойчивости каналов управления за счет когнитивного выбора свободных от помех участков диапазона волн.* ***Практическая значимость:*** *обеспечение помехоустойчивого доведения команд управления до беспилотных транспортных систем на основе алгоритма побитовой мажоритарной обработки поступающей по параллельным каналам информации в нескольких полосах частот, включая и область оптимальных рабочих частот, без знания в бортовом комплексе связи сведений об ионосферном мониторинге и их краткосрочных прогнозов.*

Ключевые слова: *активная антенная система, беспилотная транспортная система, комплексное использование каналов связи, многочастотный сигнал, радиочастотный спектр, сосредоточенная помеха.*

Введение

Сегодня на фоне активного внедрения в повседневную жизнь общества автономных и беспилотных транспортных систем (БТС) различного назначения одной из приоритетных задач транспортной отрасли страны [1] ставится обеспечение их устойчивыми каналами и трактами управления при функционировании в труднодоступных регионах страны с неполным охватом сетью базовых станций основных операторов связи, включая морские акватории Арктики, а также в условиях индустриальных помех мегаполисов и логистических центров.

Одним из решений такой задачи является построение в Министерстве транспорта РФ перспективной системы интеллектуального управления БТС в интересах федеральных агентств Росморречфлот, Росавтодор, Росавиация и Росжелдор с параллельной трансляцией их команд управления (КУ), для чего комплексно использовать диапазоны радиочастотного спектра (РЧС).

Решение вопросов интероперабельности БТС в различных средах, а также объединение предложенных универсальных технологических решений (алгоритмов) с их технической реализацией направлена, прежде всего, на создание «...системы одновременного управления любым количеством автономных объектов, т. е. к бесшовному «цифровому небу», когда воздушные, наземные, водные БТС и космические аппараты интегрированы в единую сеть» [1].

Цель статьи: рассмотрение вопросов комплексного использования РЧС в различных диапазонах частот с параллельной передачей команд управления, позволяющей обеспечить их устойчивое доведение до БТС в условиях сложной помеховой обстановки и наличии замираний в ионосферном канале, полностью исключающих (блокирующих) прохождение радиоволн.

Выбор диапазонов частот для построения бортового коплекса связи БТС

В работе [2] отмечалось, что применение БТС различных типов базирования на глобальных расстояниях от пунктов и ситуационных центров управления (ПУ и СЦУ) сопряжено с использованием радиоканалов разных диапазонов волн, подверженных в свою очередь деструктивному влиянию помех и иных внешних деструктивных факторов (ДФ).

Основными трактами управления при этом традиционно считаются радиолинии (РЛ) на базе спутниковых, сверхдлинноволновых, декаметровых и ультракоротковолновых (СДВ, ДКМВ, УКВ) радиоканалах. Безусловно, спутниковые каналы передачи КУ до БТС по скорости и помехозащищенности в этом перечне размещены на первом месте. В тоже время, применение того или иного диапазона РЧС определяется проектировщиком исходя из условий эксплуатации, заданной дальности функционирования радиолиний (РЛ) управления, а также возможности размещения на борту глобально перемещающегося БТС антенно-фидерных подсистем (АФП).

Действительно, в условиях заливания антенны водой при сильном волнении моря, при нахождении автономного БТС в подледном или погруженном положении эффективность применения спутниковой связи весьма проблематична. А учитывая необходимость доведения КУ в интересах безэкипажных судов (БЭС) Росморречфлота в дальнюю морскую и океанскую зоны возникает необходимость в задействовании резервных каналов управления диапазонов СДВ и ДКМВ с дальностью до 12 тыс. км и более. При этом ДКМВ РЛ обеспечивают более высокую скорость доведения КУ при меньшей мощности излучения, нежели в СДВ радиоканале. Причем по качеству радиосвязи ДКМВ каналы справедливо относят к каналам с переменными параметрами (с высоким коэффициентом ошибок). Открытость ДКМВ РЛ влиянию ДФ в виде сосредоточенных помех и мультипликативных замираний ионосферы, рис. 1, 2, требует поиска новых путей формирования и обработки сигнально-кодовых конструкций (СКК) КУ в обеспечении режима реального времени высокоскоростных БТС [3].

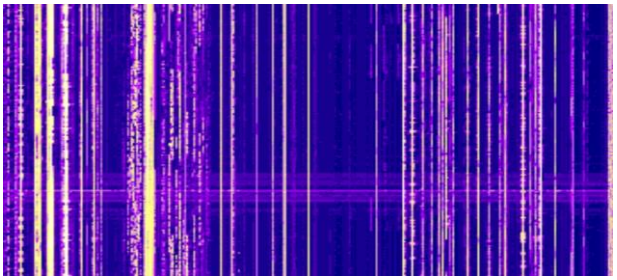


Рис. 1. Фрагмент загрузки декаметрового диапазона волн помехами в области оптимальных рабочих частот

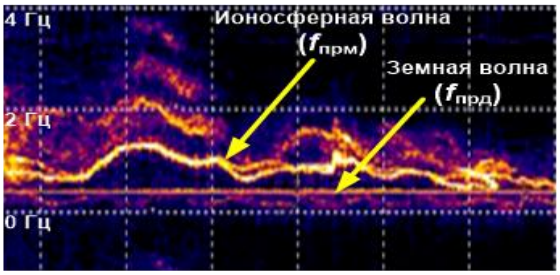


Рис. 2. Спектрограмма «Ионосферной» и «Земной» волн в ДКМВ диапазоне частот

Таким образом, для обеспечения устойчивого доведения КУ в интересах БТС, функционирующих на глобальные расстояния, в его бортовом комплексе связи (БКС) должно быть предусмотрено резервирование каналов по диапазонам волн, а также наличие широкополосных (многодиапазонных) приемных антенн, типа активных антенных систем (ААС), позволяющих достигать устойчивого приема при динамическом диапазоне 120 ÷ 230 дБ и чувствительности 0,1÷0,5 мкВ без дополнительных настроек в полосе СДВ-ДКМВ диапазонов частот. Например, активная штыревая антенна *Rohde&Scharz HE*-010 с динамическим диапазоном до 120 дБ обеспечивает устойчивый прием в полосе 20 кГц ÷ 30 МГц при малой высоте $h = 1$ м. Отечественная ААС подобного класса К-625 в диапазоне 60 кГц ÷ 80 МГц по своей чувствительности эффективнее пассивной штыревой антенны с высотой $h = 6$ м. Плоскосные ферриовые ААС имеют меньшую чувствительность чем у штыревых, но в силу геометрических свойств являются основными для приема СДВ сигналов под водой (льдом) [4].

Комплексное использование радиочастотного спектра в интересах повышения оперативности и устойчивости управления беспилотными транспортными системами

Существенное повышение оперативности и помехоустойчивости управления БТС подтверждается в работе [1] на примере модели формирования многочастотных сигналов команд управления БТС для условий сложной помеховой обстановки. В настоящее время уже имеется возможность использования мегаканальных возбудительных (ВУ) и приемных радиоустройств (РПУ), построенных на основе технологий программно-определяемого радио (*SDR*), для

процедуры параллельного излучения и приема бит КУ при назначении рабочих частот по псевдослучайному закону (ППРЧ) за счет достижений когнитивного радио (*CRS*).

Из рис. 3 видно, что параллельная передача многочастотного сигнала позволяет даже при низкой скорости трансляции одного бита $T_б$ повысить оперативность и достичь режима реального времени в доведении всей команды управления в целом, $T_{ку}$, за счет того, что $T_{ку} = T_б$.

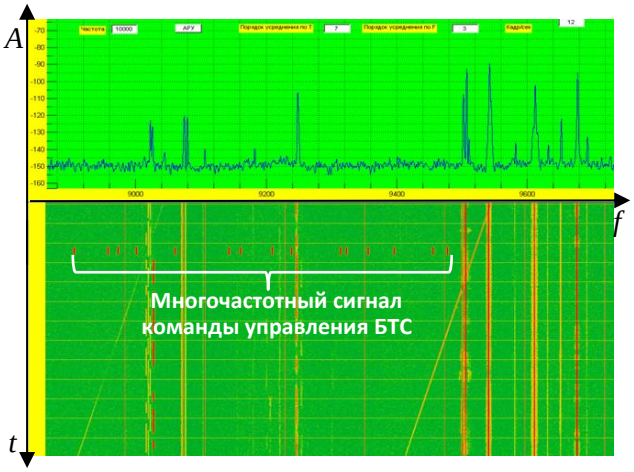


Рис. 3. Спектрограмма многочастотного сигнала, с законом выбора частот по ПСП (режим ППРЧ)

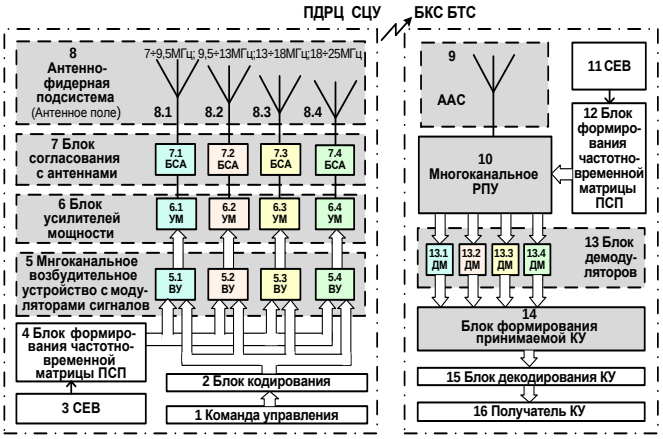


Рис. 4. Структурная схема командной радиолинии в направлении «СЦУ – БТС»

При этом в случае отсутствия возможности на удаленном БТС в режиме реального времени получать сведения о загрузке РЧС, рис. 1, возникновении неподдающихся прогнозу локальных замираниях в ионосфере, рис. 2, а также об оптимальных рабочих частотах (ОРЧ), что характерно для протяженный командных РЛ, представляется весьма целесообразным вести трансляцию команды управления с ПУ или СЦУ ведомства в широком диапазоне, дублируя передачу КУ в нескольких частотных полосах, например от 7 до 25 МГц. Вариант построения ДКМВ РЛ БТС с реализацией помехоустойчивого приема приведен на рис. 4.

Примечание: известно, что в данном диапазоне эффективность передающей антенны крайне низка без дополнительных настроек в блоке согласования с антенной (БСА), чего обеспечить не представляется возможным при параллельной передаче бит КУ в широкой частотной полосе. Добиться высокого КПД в таком случае возможно при использовании сразу нескольких антенн резонансного типа, работающих с коэффициентом частотного перекрытия $f_{верх}/f_{нижн} \approx 1{,}3 \div 1{,}4$. Это техническое решение фактически способно обеспечить трансляцию эквивалентного суммарной КУ в области ОРЧ за счет использования мажоритарного принципа сложения одинаковых битовых элементов с максимальным КПД, применяя менее мощные усилители мощности (УМ) передающего радиоцентра (ПДРЦ) СЦУ.

На передающей стороне КУ закрывается помехоустойчивым кодом в блоке кодирования 2 и далее поступает на вход многоканального ВУ с модуляторами сигналов 5, синтезируя многочастотный сигнал [1] с установкой рабочих частот, задаваемых блоком формирования набора рабочих частот 4. С выходов ВУ биты КУ поступают на сопряженные с каждым из них усилители мощности (УМ) 6.1 – 6.4, далее на БСА 7.1 – 7.4 и в антенны 8.1. – 8.4 АПФ ПДРЦ.

На приемной стороне в БКС БТС применена малогабаритная широкополосная ААС 9, с которой принятый сигнал поступает в многоканальное РПУ 10 [1] и в блок демодуляторов (ДМ) 13.1 – 13.4, после чего – на обработку в блок формирования принятой КУ 14, где в соответствии с заданным на передающей стороне методом кодирования реализуется тот или иной алгоритм совместной обработки принятых по параллельным каналам бит КУ (позначное или поэлементное весовое сложение, либо прием КУ «в целом» и др.). Для недопущения потерь бит КУ в связи с несовпадением рабочих частот в данный момент времени с областью ОРЧ во всех диапазонах параллельной передачи формируют частотно-позиционную последовательность, соответствующая структуре псевдослучайной последовательности (ПСП) изменения комплектов *I – IV* совместимых рабочих частот (КСРЧ) в режиме ППРЧ, как показано в структуре на рис. 5.

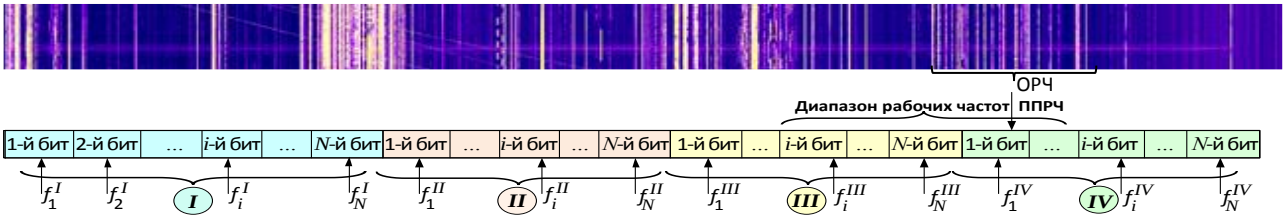


Рис. 5. Структура формирования КСРЧ передаваемой в параллельном режиме команды управления БТС

Заявленный способ построения командной РЛ БТС обеспечивает снижение пакетирования ошибок, что в свою очередь повышает исправляющую способность СКК при корректировке результатов приема КУ. При этом переход на низкую скорость ее побитовой передачи может в дальнейшем способствовать полному отказу от системы единого времени (СЕВ), чего ранее в РЛ подобного назначения не наблюдалось. В данном случае, также возможен отказ от предварительной трансляции перед началом КУ синхронизирующих групп, которые традиционно применяются в режиме т. н. быстрой побитной ППРЧ. Поскольку в этом случае рассинхронизация перестройки частот, в связи с конечностью скорости распространения радиосигнала (около 10 мс на дальности в 3000 км) между удаленными ПДРЦ и приемным БКС БТС фактически не окажет влияние на эффективность приема бит КУ длительностью более 1 с.

Выводы

1) Представленная на рис. 5 структура формирования КСРЧ в поддиапазонах РЧС, а также применение параллельной обработки выстроенных в постоянной ПСП (ППРЧ) бит КУ позволит восстановить доводимую до БТС информацию при любом перемещении области ОРЧ по поддиапазонам *I – IV*. Поскольку при совместной оптимальной обработке принятых бит КУ в блоке весового сложения будут задействованы все принятые ее элементы на одноименных позициях КУ с принятием решения по результату поэлементного (позначного) весового сложения.

2) Низкая энергия излучения каждого бита КУ, а также использование для этого узких полос частот должна обеспечить высокую электромагнитную совместимость БКС на борту БТС.

3) Внедрение подобных командных РЛ с комплексным использованием поддиапазонов РЧС с побитной параллельной передачей КУ в каждом из них в режиме ППРЧ позволит снизить требования к системе синхронизации на распределенных системах управления БТС ведомства, а также повысит устойчивость процесса управления и устранит межсимвольную интерференцию принимаемых бит команды управления за счет частотно-пространственного разноса.

Литература

1. Будко Д. Д., Каретников В. В. Модель формирования многочастотных сигналов команд управления беспилотных транспортных систем в условиях помех // Системы управления, связи и безопасности. 2026. № 1. С. 182-218. DOI: 10.24412/2410-9916-2026-1-182-218.

2. Будко Д. Д., Будко П. А., Клименко А. Д., Рыжкова Д. Н. Модель выбора полосы частот в интересах формирования декаметровых радиолиний управления беспилотными транспортными системами // Техника средств связи. 2025. № 4 (172). С. 74-83 DOI: 10.24412/2782-2141-2025-4-74-83.

3. Будко Д. Д., Будко П. А., Зацепин Т. А., Клименко А. Д. Метод управления беспилотными транспортными системами на основе помехоустойчивых сигнально-кодовых конструкций в условиях сосредоточенных и шумовых помех // Системы управления, связи и безопасности. 2025. № 4. С. 143-178. DOI: 10.24412/2410-9916-2025-4-143-178.

4. Николашин Ю. Л., Мирошников В. И., Будко П. А., Жуков Г. А. Обеспечение устойчивого обмена данными с автономными необитаемыми подводными аппаратами // Морская радиоэлектроника. 2016. № 1. С. 44-49.

References

1. Budko D. D., Karetnikov V. V. A model for generating multi-frequency control command signals for unmanned transport systems under interference conditions. *Systems of Control, Communication and Security*, 2026, no. 1, pp. 182-218 (in Russian). DOI: 10.24412/2410-9916-2026-1-182-218.

2. Budko D. D., Budko P. A., Klimenko A. D., Ryzhkova D. N. A frequency band selection model for the formation of decameter radio control lines for unmanned transport systems. *Means of communication equipment*, 2025, N. 4 (172), pp. 74-83 (in Russian) DOI: 10.24412/2782-2141-2025-4-74-83.

3. Budko D. D., Budko P. A., Zatsepin T. A., Klimenko A. D. A method for controlling unmanned transport systems based on noise-resistant signal-code structures in conditions of concentrated and noisy interference. Systems of Control, Communication and Security, 2025, no. 4, pp. 143-178 (in Russian). DOI: 10.24412/2410-9916-2025-4-143-178.

4. Nikolashin Yu. L., Miroshnikov V. I., Budko P. A., Zhukov G. A. Support of a steady data exchange by the autonomous unmanned underwater vehicles. *Marine Radio Electronics*, 2016, no. 1, pp. 44-49.

Статья поступила 07 марта 2026 г.

Информация об авторах

Будко Дмитрий Дмитриевич – аспирант. Государственный университет морского и речного флота имени адмирала С. О. Макарова. Область научных интересов: методы управления беспилотными транспортными системами. E-mail: budd.85@yandex.ru.

Адрес: Россия,198035, Санкт-Петербург, ул. Двинская, 5/7.

Ensuring sustainable delivery of control commands to unmanned transport systems due to integrated use of radio frequency spectrum

D. D. Budko

Annotation. The purpose of the work: *to increase the efficiency and stability of bringing control commands to globally moving unmanned transport systems in a complex interference situation due to the use of multi-frequency signals.* ***The novelty*** *of the study lies in the complex use of communication channels of various ranges of the radio frequency spectrum.* ***The methods*** *for realizing the goal include achievements in the development of software-defined radio technologies of cognitive radio systems, active antenna systems, as well as algorithms for synthesizing multi-frequency signals in the decameter wavelength range, receiving and digital processing of command information over parallel communication channels.* ***Result:*** *transition to real-time mode in the procedure for controlling unmanned transport systems, which is important in preventing emergencies at high speeds of their movement, as well as increasing the noise immunity of control channels due to the cognitive choice of noise-free sections of the wave range.* ***Practical significance:*** *providing noise-resistant transmission of control commands to unmanned transport systems based on the algorithm of bitwise majority processing of information received over parallel channels in several frequency bands, including the area of optimal operating frequencies, without knowledge in the on-board communication complex of information about ionospheric monitoring and their short-term forecasts.*

Keywords: *active antenna system, unmanned transport system, complex use of communication channels, multi-frequency signal, radio frequency spectrum, concentrated interference.*

Information about the authors

Dmitry Dmitrievich Budko – Postgraduate. State University of the Sea and River Fleet named after Admiral S.O. Makarov. Research interests: methods of managing unmanned transport systems. E-mail: budd.85@yandex.ru. Address: 198035, Russia, Saint-Petersburg, st. Dvinskaya, bldg. 5/7.

Для цитирования:

Будко Д. Д. Обеспечение устойчивого доведения команд управления до беспилотных транспортных систем за счет комплексного использования радиочастотного спектра // Техника средств связи. 2026. № 1 (173). С. 95-99. DOI: 10.24412/2782-2141-2026-1-95-99.

For citation:

Budko D. D. Ensuring sustainable delivery of control commands to unmanned transport systems due to integrated use of radio frequency spectrum. Means of communication equipment. 2026. № 1 (173). С. 95-99 (in Russian). DOI: 10.24412/2782-2141-2026-1-95-99.

29 декабря 2025 года подписан Указ Президента Российской Федерации о проведении в России первой Недели космоса, приуроченной к празднованию 65-летия первого полёта человека в космос. С 2026 года **Неделя космоса в России будет проходить ежегодно 6-12 апреля**

В целях развития механизмов активной государственной политики по привлечению молодежи в сферу науки и технологий, вовлечение исследователей и разработчиков в решение важных задач для страны и общества в десятилетие науки и технологий, профессиональной адаптации, выявления и максимального использования творческого потенциала молодых интеллектуальных кадров, стимулирования научной деятельности и привлечения их к решению научно-технических задач, повышающих качество текущих научно-исследовательских и опытно-конструкторских работ в ПАО «Интелтех» объявляется проведение **Конкурса на лучшую научную работу молодых ученых и специалистов, посвященный 65-летию первого полета человека в Космос:**

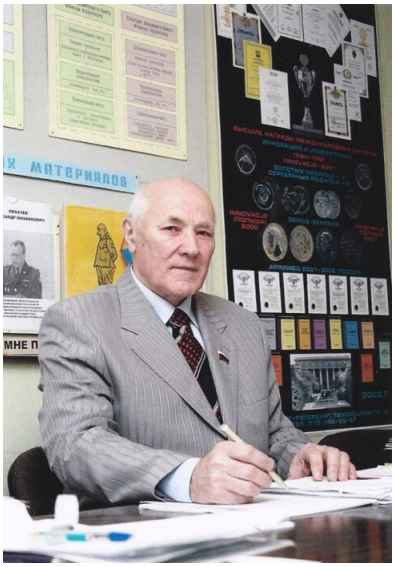
I этап (заочный тур):
до 12.04.2026 сдача научных работ (проектов) в конкурсную комиссию;
до 30.04.2026 предварительная экспертная оценка научных работ, представление проектов для участия в XVI Национальной научно-технической конференции (СоюзМаш);
II этап (очный тур):
с 01.05. 2026 по 19.05.2026 – рецензирование проектов Конкурса на лучшую научную работу молодых ученых и специалистов ПАО «Интелтех»;
III этап (защита проектов):
20.05.2025 – защита конкурсных работ на ежегодной молодежной научно-технической конференции ПАО «Интелтех».

Номинации Конкурса:
«Телекоммуникационные системы и сети»;
«Системы управления»;
«Информационная безопасность»;
«Робототехника».

Информационный спонсор Конкурса на лучшую научную работу молодых ученых и специалистов ПАО «Интелтех» и ежегодной молодежной научно-технической конференции ПАО «Интелтех» – научно-технический журнал «Means of communication equipment» («Техника средств связи»).

Редакция журнала приглашает победителей Конкурса на лучшую научную работу молодых ученых и специалистов к публикации материалов своих научных работ на страницах журнала.

ЗАСЛУЖЕННОМУ ДЕЯТЕЛЮ НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ АНДРЕЮ АНДРЕЕВИЧУ КАТАНОВИЧУ
85 лет



20 апреля 2026 г. известный ученый в области оптических многоканальных телекоммутационных систем, средств и автоматизированных комплексов связи, Заслуженный деятель науки Российской Федерации, главный научный сотрудник Научно-исследовательского института оперативно-стратегических исследований строительства Военно-морского флота (НИИ ОСИС ВМФ), член ученного совета ВУНЦ ВМФ «ВМА» с начала его основания, а также член редакционного совета журнала «Техника средств связи» Андрей Андреевич КАТАНОВИЧ отмечает 85-летний юбилей.

В НИИ ОСИС ВМФ Андрей Андреевич пришел в 1975 году по окончании Военной академии связи и за эти полвека прошел этапы становления военного ученого от младшего до главного научного сотрудника института. А до этого были 561-я мореходная школа специалистов рядового плавсостава (1959) и военное училище связи (1964), командные и инженерные должности в подразделениях специальной разведки ВМФ.

В 1982 году защитил кандидатскую, а в 1998 – докторскую диссертации. Доктор технических наук, профессор, капитан первого ранга в отставке А.А. Катанович за этот период жизни, всецело посвящённой науке, подготовил более 1060 научных трудов (в числе которых – 29 научных монографий) и получил 480 патентов на изобретения. В 1996 году он создал научную школу, исследующую проблемы создания волоконно-оптических систем и комплексов связи Военно-Морского Флота, которая вошла в реестр научных школ ВУНЦ ВМФ «ВМА» и Санкт-Петербурга. Эту школу прошли более 60 адъюнктов и соискателей ученых степеней.

В 2014 году как лучший изобретатель России награждён золотой медалью Всемирной организации интеллектуальной собственности. Участник многочисленных международных и всероссийских выставок и конференций, на которых завоевал 10 Гран-при, 113 золотых и серебряных медалей. Также Андрей Андреевич за заслуги в укреплении обороноспособности страны имеет ряд почётных званий: «Заслуженный деятель науки РФ», «Заслуженный работник связи и информатизации РФ», «Заслуженный изобретатель РФ», «Почётный работник науки и техники РФ», «Почётный радист РФ», «Почётный изобретатель Санкт-Петербурга».

Андрей Андреевич стоял у истоков создания и внедрения оптоэлектроники в комплексы и системы связи Военно-Морского Флота. Разработал теорию построения системы подводно-кабельной связи ВМФ, сформулировал принципы построения и использования специальных судов для прокладки подводных кабельных линий связи в Арктике, предложил целый комплекс инженерно-технических решений для практического использования теоретических предложений по повышению эффективности подводных кабельных систем связи ВМФ.

Несмотря на почтенный возраст, А. А. Катанович продолжает активно и продуктивно трудиться на благо Военно-морской науки. Его энтузиазму могут позавидовать многие. В течение последних лет он ведет масштабную работу и научные изыскания в области развития систем связи Военно-Морского Флота, результатом которых стали 6 научных монографий, которые были признаны лучшими научными трудами в Министерстве обороны РФ. Именно за эти фундаментальные труды в канун своего юбилея научной деятельности Андрей Андреевич награжден премией Конкурса на лучшую научную работу Вооружённых Сил РФ. При этом лауреатом престижного Конкурса военных ученых он становится уже в шестой раз (2012, 2019, 2022, 2023, 2024, 2025 г.г.).

НИИ ОСИС ВМФ ВУНЦ ВМФ «ВМА», а также редакция журнала «Техника средств связи» искренне поздравляет Андрея Андреевича с 85-летним юбилеем на благо военно-морской науки, а также победой в престижных конкурсах! Желаем крепкого здоровья, интересных проектов в его научной деятельности и новых творческих побед!