

TELECOMMUNICATIONS AND COMMUNICATIONS

№ 5 (14) 2026

DOI: 10.21681/3034-4050

THEME OF THE ISSUE:

INFORMATION CONFRONTATION IN THE MILITARY SPHERE

INCREASING THE STRUCTURAL SECRECY OF DATA TRANSMISSION NETWORKS

BUILDING AN ADAPTIVE COMMUNICATION SYSTEM

ТЕЛЕКОММУНИКАЦИИ и СВЯЗЬ

№ 5 (14) 2026

ТЕМА НОМЕРА:

ИНФОРМАЦИОННОЕ ПРОТИВОБОРСТВО В ВОЕННОЙ СФЕРЕ

ПОВЫШЕНИЕ СТРУКТУРНОЙ СКРЫТНОСТИ СЕТЕЙ ПЕРЕДАЧИ ДАННЫХ

ПОСТРОЕНИЕ АДАПТИВНОЙ СИСТЕМЫ СВЯЗИ

WWW.TELEMIL.RU

DOI: 10.21681/3034-4050



WWW.TELEMIL.RU
EDITOR.TIS@YANDEX.RU



Журнал зарегистрирован Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций. Свидетельство о регистрации ПИ № ФС77-88069 от 16.08.2024

Журнал входит в Российский индекс научного цитирования, публикует статьи по специальностям перечня научных специальностей группы 6.0.0

Главный редактор
ИВАНОВ Василий Геннадьевич, д.в.н., доцент, Москва

Шеф-редактор
МАКАРЕНКО Григорий Иванович, с.н.с., Москва

Попечительский совет
РУБИС Александр Анатольевич, к.т.н., заместитель начальника Главного управления связи ВС РФ по вооружению (председатель)
ПАНКОВ Роман Николаевич, к.ист.н., начальник ФГБУ «16 Центральный научно-исследовательский испытательный институт»
ХАРЧЕНКО Евгений Борисович, к.соц.н., доцент (секретарь)

Редакционная коллегия
АЧКАСОВ Николай Борисович, д.в.н., профессор, Санкт-Петербург
БЫЧКОВ Антон Вячеславович, д.в.н., доцент, Санкт-Петербург
БУЙНЕВИЧ Михаил Викторович, д.т.н., профессор, Санкт-Петербург
ГЛУШАНКОВ Евгений Иванович, д.т.н., профессор, Санкт-Петербург
ГРУДИНИН Игорь Владимирович, д.в.н., профессор, Санкт-Петербург
ИВАНОВ Сергей Александрович, д.т.н., Санкт-Петербург
КОЗАЧОК Александр Васильевич, д.т.н., доцент, Орел
КОСТОГРЫЗОВ Андрей Иванович, д.т.н., профессор, Москва
КУЗИН Павел Игоревич, к.т.н., доцент, Санкт-Петербург
МАКАРЕНКО Сергей Иванович, д.т.н., профессор, Санкт-Петербург
МАРКОВ Алексей Сергеевич, д.т.н., доцент, Москва
НОВИКОВ Евгений Александрович, д.т.н., доцент, Санкт-Петербург
ПРИВАЛОВ Андрей Андреевич, д.в.н., профессор, Санкт-Петербург
ПЫЛИНСКИЙ Максим Валерьевич, д.в.н., профессор, Белоруссия
РЫЖОВ Геннадий Борисович, д.в.н., профессор, Москва
САВИЩЕНКО Николай Васильевич, д.т.н., профессор, Санкт-Петербург
СТАРОДУБЦЕВ Юрий Иванович, д.в.н., профессор, Санкт-Петербург
ФЕДЮНИН Павел Александрович, д.т.н., профессор, Воронеж
ФИНЬКО Олег Анатольевич, д.т.н., профессор, Краснодар
ЦИМБАЛ Владимир Анатольевич, д.т.н., профессор, Серпухов
ЧЕРНЫШОВ Михаил Викторович, д.т.н., профессор, Санкт-Петербург

Учредитель и издатель
ФГБУ «16 Центральный научно-исследовательский испытательный институт Министерства обороны РФ»
(Военно-научный комитет Главного управления связи Вооружённых Сил Российской Федерации)

Над номером работали:
Г. И. Макаренко – шеф-редактор, Н. В. Селезнев – отв. секретарь,
С. С. Игнатов – верстка, А. В. Матюшин – маркетинг и подписка
Подписано к печати 15.10.2026 г.
Общий тираж 120 экз. Цена свободная

Адрес: 141006, г. Мытищи, Московской обл.,
1-й Рупасовский пер.
E-mail: editor.tis@yandex.ru, тел.: +7 (985) 939-75-01
Требования, предъявляемые к рукописям,
размещены на сайте: <https://telemil.ru/>

СОДЕРЖАНИЕ

СИСТЕМНЫЙ АНАЛИЗ СИСТЕМ ВОЕННОГО НАЗНАЧЕНИЯ

ОЦЕНКА ДИНАМИЧЕСКИХ ДАННЫХ В КОНТЕКСТЕ СОВРЕМЕННЫХ МЕТОДОЛОГИЙ

Лукашенко В. И., Паняев А. И., Изотов Д. Ю. 2

РАЗРАБОТКА МЕТОДОЛОГИИ АНАЛИЗА И ПОВЫШЕНИЯ СТРУКТУРНОЙ СКРЫТНОСТИ СЕТЕЙ ПЕРЕДАЧИ ДАННЫХ

Слами Али Юсуф 12

НАПРАВЛЕНИЯ РАЗВИТИЯ И ПРИМЕНЕНИЯ СРЕДСТВ БЕСПРОВОДНОГО ШИРОКОПОЛОСНОГО ДОСТУПА В СИСТЕМЕ СВЯЗИ ТАКТИЧЕСКОГО ЗВЕНА УПРАВЛЕНИЯ

Лукьянчик В. Н., Карташев А. В., Васильева Т. Г. 21

ИНФОРМАЦИОННОЕ ПРОТИВОБОРСТВО В ВОЕННОЙ СФЕРЕ

АНАЛИЗ ЭФФЕКТИВНОСТИ РАБОТЫ Д-СЛОЯ НЕРАЗЛИЧИМОСТИ ФАЗОМАНИПУЛИРОВАННЫХ СИГНАЛОВ, ПРИНИМАЕМЫХ В УСЛОВИЯХ НЕКОГЕРЕНТНОГО ВОЗДЕЙСТВИЯ ПРЕДНАМЕРЕННОЙ ПОМЕХИ

Негурица А. О. 33

ПРЕДЛОЖЕНИЯ ПО ПОСТРОЕНИЮ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ УПРАВЛЕНИЯ СВЯЗЬЮ ТАКТИЧЕСКОГО ЗВЕНА УПРАВЛЕНИЯ

Иванов В. Г., Сорокин А. Ю., Лукьянчик В. Н. 39

ВОЕННЫЕ СИСТЕМЫ УПРАВЛЕНИЯ, СВЯЗИ И НАВИГАЦИИ

ЦИФРОВАЯ ТРАНСФОРМАЦИЯ – НОВЫЕ ТЕХНОЛОГИИ ДЛЯ СЕТЕЙ СВЯЗИ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ. Часть I

Лукашев А. В. 50

ПРИМЕНЕНИЕ РЕКУРРЕНТНЫХ НЕЙРОННЫХ СЕТЕЙ ДЛЯ ВЫЯВЛЕНИЯ СКРЫТЫХ АНОМАЛИЙ В ЖУРНАЛАХ СОБЫТИЙ АВТОМАТИЗИРОВАННЫХ СИСТЕМ ВОЕННОГО НАЗНАЧЕНИЯ

Саенко И. Б., Цыпнятов В. Б., Сажина А. В. 59

СПОСОБЫ ОРГАНИЗАЦИИ ФУНКЦИОНИРОВАНИЯ СИСТЕМЫ ВИДЕОТРАНСЛЯЦИИ В УСЛОВИЯХ СОВРЕМЕННЫХ ВОЕННЫХ ДЕЙСТВИЙ

Лебедев П. В., Живодерников А. Ю. 67

МОДЕЛИРОВАНИЕ ЗАДАЧИ МАРШРУТИЗАЦИИ В СЕТИ ПЕРЕДАЧИ ДАННЫХ ПО ПОКАЗАТЕЛЮ ВЕРОЯТНОСТИ СВОЕВРЕМЕННОЙ ДОСТАВКИ СООБЩЕНИЙ

Курашев З. В. 77

ВОЕННАЯ ЭЛЕКТРОНИКА КОМПЛЕКСОВ ВОЕННОГО НАЗНАЧЕНИЯ

ПАРАМЕТРИЧЕСКИЙ СИНТЕЗ МНОГОВИБРАТОРНОЙ ПОДЗЕМНОЙ АНТЕННЫ, ФУНКЦИОНИРУЮЩЕЙ В ДИССИПАТИВНЫХ СЛОИСТЫХ СРЕДАХ

Леонюк А. С., Юртаев А. С., Исмаил М. М. 83

ИССЛЕДОВАНИЕ ВЛИЯНИЯ ВНЕШНИХ ФАКТОРОВ НА ВЫБОР РАБОЧИХ ЧАСТОТ РАДИОЛИНИЙ КВ-ДИАПАЗОНА

Велигоша А. В., Третьяков Е. А., Юрков В. В. 91

СПОСОБ ОБЕСПЕЧЕНИЯ ВЫБОРА И ОБОСНОВАНИЯ ПЕРСПЕКТИВНЫХ СРЕДСТВ СВЯЗИ ДЛЯ ПОСТРОЕНИЯ АДАПТИВНОЙ СИСТЕМЫ СВЯЗИ ТАКТИЧЕСКОГО ЗВЕНА УПРАВЛЕНИЯ

Слепова В. П. 100

ОЦЕНКА ДИНАМИЧЕСКИХ ДАННЫХ В КОНТЕКСТЕ СОВРЕМЕННЫХ МЕТОДОЛОГИЙ

Лукашенко В. И.¹, Паняев А. И.², Изотов Д. Ю.³

DOI:10.21681/3034-4050-2026-5-2-11

Ключевые слова: динамические данные, временные ряды, энтропийно-робастный подход, энтропия выборки, переносная энтропия, причинность, качество данных, латентность, рекуррентные алгоритмы, техническая диагностика, динамическая оценка жизненного цикла.

Аннотация

Цель работы: на основе анализа ограничений классических статических метрик (корреляция, регрессия, MSE) и существующих методов анализа временных рядов обосновать энтропийно-робастный подход к динамической оценке систем с памятью, нелинейностью и нестационарностью, позволяющий одновременно учитывать неопределённость, причинность, качество входных данных и вычислительные ограничения.

Метод исследования: методология объединяет аппарат теории динамических систем (реконструкция фазового пространства по Такенсу), информационно-теоретические меры (Sample Entropy, Transfer Entropy), робастные статистические процедуры (адаптивные пороги, медианные оценки) и рекуррентные алгоритмы онлайн-обработки. Предложен прогностический тест для верификации оценок в отсутствие эталонной истины. Эффективность подхода продемонстрирована на двух прикладных задачах: раннее обнаружение отказов роторного оборудования по вибрационным сигналам и динамическая оценка жизненного цикла продукции с учётом временной вариативности.

Результаты исследования: обоснован переход от точечных метрик к траекторным оценкам в фазовом пространстве. Показано, что качество данных (полнота, точность, стабильность) и причинность (Transfer Entropy, Convergent Cross Mapping) являются сквозными метриками, без которых энтропийные оценки теряют прикладную достоверность. Разработана вычислительная схема на основе рекуррентных алгоритмов, учитывающая латентность и адаптирующая параметры к текущему потоку. Верификация через прогностический тест позволила снизить долю ложных тревог в диагностике на 30 % по сравнению с фиксированными порогами. В кейсе динамической LCA выявлены сезонные колебания углеродного следа (разброс 18 % против 4 % в статической оценке) и пересмотрены приоритетные факторы влияния.

Научная новизна: впервые энтропийные меры, робастные процедуры и причинностный анализ объединены в целостный методологический подход к динамической оценке, применимый как к физическим (диагностика), так и к организационно-техническим (LCA) системам. Предложен прогностический тест как универсальный способ верификации динамических оценок в отсутствие эталонных меток. Формализовано влияние латентности на энтропийные и причинностные меры и предложены методы её компенсации через адаптивное окно.

Введение

Современные системы генерации данных – от промышленных сенсоров до потоков экологического мониторинга – производят не изолированные наблюдения, а временные ряды, потоки событий и траектории состояний, которые обладают фундаментальными свойствами: нестационарностью, памятью (зависимостью от предыстории), нелинейностью и чувствительностью к порядку поступления данных. Классические методы статистики и машинного обучения, ориентированные на статические выборки, оказываются неадекватными в таких условиях: точка не репрезентирует процесс, а усреднение разрушает динамику.

Предметом исследований в данной статье являются динамические данные. Под динамическими данными понимаются последовательности

наблюдений, упорядоченные во времени, где каждое следующее значение не является независимым от предыдущих. Это могут быть показания датчиков, логи событий, временные ряды экономических показателей или траектории движения. Ключевые свойства – нестационарность (изменение среднего, дисперсии, спектра во времени), наличие памяти (автокорреляция), нелинейность (отсутствие пропорциональности между причиной и следствием) – делают неприменимыми методы, предполагающие независимость и одинаковую распределённость наблюдений.

Анализ существующих методологий и их ограничения

Классические статистические методы (корреляция Пирсона, регрессионные модели) требуют стационарности и независимости ошибок; в динамике они дают смещённые оценки

¹ Лукашенко Василий Ильич, младший научный сотрудник Научно-исследовательского центра Военной академии связи, г. Санкт-Петербург, Россия. E-mail: lukasenokvasilij@gmail.com

² Паняев Алексей Игоревич, старший научный сотрудник Научно-исследовательского центра Военной академии связи, г. Санкт-Петербург, Россия. E-mail: alex.panjaev@gmail.com

³ Изотов Даниил Юрьевич, научный сотрудник Научно-исследовательского центра Военной академии связи, г. Санкт-Петербург, Россия. E-mail: daniil.izotov.1999@mail.ru

и не выявляют нелинейных связей. Методы машинного обучения (случайный лес, нейронные сети) часто игнорируют временную структуру либо требуют больших размеченных выборок, что в реальных процессах (например, предотказное состояние оборудования) недостижимо. Методы теории динамических систем (реконструкция аттрактора, показатели Ляпунова) потенциально адекватны, но разрознены и не объединены в целостный подход, учитывающий качество данных, причинность и вычислительные ограничения онлайн-режима.

1. От статистики к динамике: энтропийно-робастный подход

1.1. Пределы классических метрик в динамических системах

Традиционная статистика и машинное обучение оперируют с выборкой как с множеством независимых наблюдений. Для динамических данных, где очередное значение зависит от предыстории, это приводит к систематическим ошибкам.

Рассмотрим простейший случай – корреляцию Пирсона между двумя временными рядами x_t и y_t :

$$\rho_{xy} = \frac{\sum_{t=1}^N (x_t - \bar{x})(y_t - \bar{y})}{\sqrt{\sum_{t=1}^N (x_t - \bar{x})^2} \sqrt{\sum_{t=1}^N (y_t - \bar{y})^2}}.$$

Эта мера фиксирует линейную синхронную связь. Однако в динамических системах:

1. Нелинейность – зависимость может быть детерминированной, но нелинейной (например, $y_t = x_t^2 + \varepsilon$), где ρ_{xy} будет близок к нулю.

2. Нестационарность – среднее и дисперсия меняются во времени, корреляция становится плохо определённой.

3. Сдвиг во времени – причина и следствие могут быть разделены латентным периодом; синхронная корреляция их не увидит.

Регрессионные модели ($y_t = \beta_0 + \beta_1 x_t + \varepsilon_t$) предполагают фиксированную структуру зависимости. При смене режимов (бифуркации, переключение между аттракторами) коэффициенты перестают быть адекватными.

Статические метрики качества прогноза (MSE, MAE) оценивают ошибку в каждой точке, но не отражают, воспроизводит ли модель динамику – например, правильно ли предсказаны повторяющиеся паттерны, частотные характеристики, время возврата.

Вывод: необходим переход от точечных оценок к траекторным.

1.2. Траекторный подход: от точки к фазовому пространству

Ключевая идея: одно наблюдение x_t не репрезентирует состояние системы. Состояние – это

точка в фазовом пространстве, координаты которой задаются текущим значением и его предысторией.

Для временного ряда $\{x_1, x_2, \dots, x_N\}$ теорема Такенса⁴ утверждает, что при выполнении общих условий (гладкость, невырожденность) можно восстановить динамику, эквивалентную исходной, используя метод запаздывающих координат. Вектор вложения:

$$X_t = (x_t, x_{t-\tau}, x_{t-2\tau}, \dots, x_{t-(m-1)\tau}),$$

где m -размерность вложения (достаточно $m > 2d$, где d – размерность аттрактора), τ – временная задержка (обычно выбирается по первому минимуму взаимной информации).

Теоретические основы применимости метода запаздывающих координат для предсказуемого восстановления системы были недавно усилены в работе Barański и др. [1], где доказана гипотеза Shroer–Sauer–Ott–Yorke о предсказуемости временных задержек. С практической стороны, эффективность вложения Такенса для восстановления пространства состояний в динамических системах, в частности в задачах технической диагностики, подтверждена в исследовании Najera-Flores и Todd [2].

Траектория $\{X_t\}$ в фазовом пространстве становится объектом анализа вместо исходного скалярного ряда.

Вывод: траекторное представление позволяет применить аппарат теории динамических систем и теории информации к реальным данным, преодолеть ограничения статических метрик.

1.3. Энтропия как мера неопределённости динамической системы

Энтропия в динамическом контексте – не просто мера хаоса, а количественная характеристика скорости потери информации о состоянии системы при эволюции.

1. Энтропия Шеннона для дискретного источника:

$$H = -\sum_i p_i \log p_i,$$

где p_i – вероятности символов. В динамике её применяют к символьным последовательностям, получаемым из временного ряда, но она не учитывает порядок.

2. Энтропия Колмогорова–Синай (KSE) – фундаментальный инвариант динамической системы. Она равна сумме положительных показателей Ляпунова и характеризует, насколько быстро расходятся близкие траектории. Прямое вычисление KSE по реальным данным сложно.

3. Практические аппроксимации:

⁴ Takens F. (1981). Detecting strange attractors in turbulence. In *Dynamical Systems and Turbulence, Lecture Notes in Mathematics*, vol. 898, Springer, pp. 366–381

ApEn (Approximate Entropy) – вероятность того, что близкие паттерны останутся близкими на следующем шаге. Чувствительна к размеру выборки.

SampEn (Sample Entropy)⁵ – исключает самосовпадения, более робастна.

$$\text{SampEn}(m, r, N) = -\ln \frac{A}{B},$$

где m – длина сравниваемых эпизодов, r – порог схожести, B – число пар близких эпизодов длины m , A – число пар близких эпизодов длины $m + 1$.

Применение энтропийных статистик для анализа, например сложности сигналов в геофизике продемонстрировано в работе Любушина и др. [3], где энтропия вейвлет-коэффициентов использовалась для обнаружения предвестников сильных землетрясений. Показано, что рост энтропийной сложности сейсмического шума предшествует сейсмическим событиям, что коррелирует с предлагаемым в настоящей статье подходом к диагностике отклонений.

В другой работе [4] показано, что энтропийные характеристики динамических систем, вычисленные на основе реконструкции фазового пространства, обладают свойством инвариантности к определённому классу нелинейных искажений сигнала, что важно для обеспечения робастности оценок в реальных приложениях.

Роль энтропии в оценке:

1. Если энтропия высокая, то система непредсказуема, сложна, и возможно хаотична или стохастична.
2. Если же энтропия низкая, то система периодична и высоко предсказуема.
3. При росте энтропии во времени можно делать вывод о вероятной деградации (отказе) или переходе к хаосу.

1.4. Робастность как требование к оценке

Робастность – это способность оценки сохранять свои свойства при малых отклонениях от идеализированных предположений (шумы, выбросы, пропуски). В динамических системах это требование критично, потому что малое искажение на входе из-за чувствительности к начальным условиям может привести к большой ошибке в реконструкции траектории и энтропийных мерах.

Различие между робастностью и устойчивостью:

- устойчивость (классическая теория динамических систем): траектории, стартовавшие из близких начальных условий, остаются близкими (устойчивость по Ляпунову) – это свойство системы;

- робастность – свойство оценки: оценка не меняется сильно при малых возмущениях данных.

В динамических системах классические энтропийные меры (особенно ApEn) могут быть не робастны к шуму – шум искусственно повышает энтропию. Требуется робастная нормализация и фильтрация.

Энтропийно-робастный подход – это совместное использование:

- энтропийных мер (SampEn, переносной энтропии) для характеристики неопределённости и потока информации;
- робастных статистических процедур (медианные оценки, усечённые средние, адаптивные пороги) для обеспечения устойчивости оценки к возмущениям.

Пример робастной оценки энтропии: вместо фиксированного порога r использовать адаптивный порог, кратный медианному абсолютному отклонению (MAD) вместо стандартного отклонения.

Энтропийно-робастный подход даёт базовый аппарат для перехода от точек к траекториям и количественной оценки неопределённости. Однако для полноценной динамической оценки необходимо ответить на два вопроса:

1. Насколько качественны входные данные, по которым мы строим оценку?
2. Как отличить истинные причинно-следственные связи от ложных корреляций в потоке данных?

Этим вопросам посвящён следующий раздел, где качество и причинность вводятся как две сквозные метрики динамической оценки.

2. Качество и причинность как две сквозные метрики

2.1. Качество входного потока в динамическом контексте

В статическом анализе качество данных обычно сводится к отсутствию пропусков, ограниченному уровню шума и корректной калибровке. В динамике этого недостаточно, потому что качество само эволюционирует во времени, и оценка должна быть чувствительна к этой эволюции.

Выделим четыре компонента качества в динамическом контексте.

Полнота во времени, ведь пропуски данных – это не просто дыры, а разрывы траектории. Даже единичный пропуск разрушает возможность корректно построить вектор вложения Такенса в окрестности этого момента. Меры: доля пропущенных отсчётов на скользящем окне, максимальная длина непрерывной последовательности.

⁵ Richman J. S., Moorman J. R. (2000). Physiological time-series analysis using approximate entropy and sample entropy. American Journal of Physiology-Heart and Circulatory Physiology, 278(6), H2039–H2049.

Точность и уровень шума, так как аддитивный шум увеличивает энтропию выборки (SampEn), имитируя более хаотичное поведение. Это может привести к ложной диагностике «предотказного состояния». Требуется оценка отношения сигнал/шум (SNR) в скользящем режиме, например, методом анализа вейвлет-коэффициентов или по спектру сингулярных чисел.

Стабильность характеристик качества во времени немаловажна. Довольно частый случай – нестационарность качества: сенсор деградирует, канал связи меняет пропускную способность. Это означает, что один раз вычисленный порог энтропии становится не валидным. Динамическая оценка должна включать адаптивный контроль качества: например, оценивать дисперсию шума на участках, где система заведомо стационарна (по внешним признакам).

Латентность, потому как задержка между реальным событием и регистрацией данных искажает фазовый портрет и причинностные связи. Для оценки качества важно знать хотя бы диапазон латентности.

Влияние качества на энтропийные оценки:

- Шум → завышение SampEn, ApEn.
- Пропуски → невозможность вычислить вложение для ряда окон, появление артефактных «схождений» траекторий.
- Нестабильная калибровка → дрейф среднего, что при неосторожном вычитании тренда может удалить реальную динамику.

Вывод: перед любой динамической оценкой должна выполняться верификация качества потока с выдачей метрик доверия для каждого интервала времени.

2.2. От корреляции к причинности: проблема ложных связей

В динамических системах высокая корреляция между двумя рядами x_t и y_t может возникать без какой-либо причинно-следственной связи. Три классических сценария:

1. Общая внешняя причина (общий драйвер), когда x_t и y_t независимы, но оба зависят от z_t (например, температура воздуха влияет и на расход электроэнергии, и на число посетителей парка). Корреляция между x и y будет ненулевой, хотя прямой связи нет.
2. Синхронизация независимых хаотических систем, когда две несвязанные системы с одинаковыми параметрами могут демонстрировать синхронное поведение (эффект, наблюдаемый даже у метрономов на подвижной платформе). Корреляция возникает, но причинность отсутствует.
3. Временное усреднение, т.е. если данные агрегированы по времени, то высокочастотная

независимая динамика может маскироваться, создавая ложную корреляцию на низких частотах.

Если мы строим прогноз или диагностику на основе корреляции, то при изменении внешних условий (отключение общего драйвера) связь разрушится, и модель окажется бесполезной. Причинная связь, напротив, более инвариантна.

2.3. Динамическая причинность: инструменты

Классическая причинность по Грейнджеру основана на VAR-моделях. VAR (Vector Autoregression, Векторная авторегрессия) – это статистическая модель, используемая для анализа взаимосвязей между несколькими временными рядами. Она позволяет понять, как прошлые значения одних переменных влияют на текущие значения других и линейной предсказуемости. В нелинейных динамических системах она часто даёт ложноотрицательные результаты. Используем два современных информационно-динамических инструмента.

2.3.1. Transfer Entropy (TE)

Transfer Entropy (TE, переносимая энтропия)⁶ – это статистическая мера, которая определяет количество информации, переданной от одного случайного процесса к другому. Доказано, что TE может интерпретироваться как динамический каузальный эффект, даже в присутствии скрытых переменных [5]. Простыми словами, она отвечает на вопрос: *насколько знание прошлого переменной X помогает предсказать будущее переменной Y лучше, чем если использовать только прошлое самой Y ?*

TE измеряет направленный поток информации от процесса X процессу Y :

$$TE_{X \rightarrow Y} = \sum p(y_{t+1}, y_t^{(k)}, x_t^{(l)}) \log \frac{p(y_{t+1} | y_t^{(k)}, x_t^{(l)})}{p(y_{t+1} | y_t^{(k)})},$$

где $y_t^{(k)}$ – k предыдущих значений Y , $x_t^{(l)}$ – соответственно l предыдущих значений X .

Альтернативное применение TE для отбора наиболее информативных признаков в задачах машинного обучения предложено в работе Misiorek [6], где показано, что TE-отбор признаков превосходит традиционные корреляционные методы при работе с нелинейными и запаздывающими связями. TE не предполагает линейности и симметрии и обладает следующими важными свойствами:

1. TE > 0 означает, что знание прошлого X снижает неопределенность будущего Y по сравнению с использованием только прошлого Y .
2. TE инвариантна к монотонным нелинейным преобразованиям.

⁶ Schreiber T. (2000). Measuring information transfer. Physical Review Letters, 85(2), 461–464.

3. Вычислительно сложна для непрерывных данных; требуются методы оценки плотности (kNN, ядерные оценки).

Практические аспекты применения Transfer Entropy для выявления причинных связей в нелинейных динамических системах рассмотрены в работе [7], где на модельных и реальных данных показано, что ТЕ позволяет корректно определять направление связи даже при наличии шума и нестационарности, что делает этот метод пригодным для диагностики сложных технических систем.

2.3.2. Convergent Cross Mapping (CCM, конвергентное кросс-отображение)

Метод, разработанный для слабо связанных хаотических систем [8]. Идея: если X влияет на Y , то состояние Y можно восстановить по истории X (и наоборот).

Алгоритм следующий:

1-й шаг – строим фазовые пространства для X и Y методом вложения Такенса.

2-й шаг – для каждого момента времени находим ближайших соседей в пространстве Y , затем смотрим на соответствующие им значения X .

3-й шаг – оцениваем, насколько хорошо по соседям в Y предсказывается X (и наоборот).

4-й шаг – при увеличении длины ряда, ошибка предсказания должна сходиться к нулю, если причинность есть.

В сравнительной таблице 1 продемонстрированы различия между ТЕ и CCM

Сравнительный анализ методов обнаружения причинных связей в временных рядах на обширном наборе модельных систем показал [9], что ТЕ и CCM дополняют друг друга: ТЕ лучше работает при наличии шума, а CCM – при сильной нелинейности и слабой связи. Это наблюдение обосновывает необходимость комбинированного использования обоих методов, что и предлагается в настоящей статье.

Методы обнаружения причинных связей в сложных динамических системах систематизированы по математическим основаниям: информационно-теоретические, основанные на реконструкции аттрактора, байесовские. Практические критерии выбора метода определяются длиной ряда, уровнем шума и характером нелинейности.[10]

CCM требует значительно большей длины временного ряда, чем ТЕ, но при выполнении этого условия позволяет обнаруживать связи, невидимые для информационных мер.[11]

Вывод: ТЕ выбираем для умеренно зашумлённых данных, когда важна направленность и не требуется сверхдлинных рядов.

CCM выбираем для сильно нелинейных, почти детерминированных хаотических систем с длительными записями.

2.4. Связь качества и причинности

Качество данных напрямую влияет на оценки причинности:

Шум $\rightarrow$ ТЕ завышается, если шум в X и Y коррелирован (ложноположительные связи). CCM, наоборот, может недооценивать связь, т.к. шум размывает аттрактор [12].

Пропуски $\rightarrow$ для ТЕ требуются непрерывные последовательности; пропуски приходится интерполировать, что вносит артефакты. Для CCM пропуски разрушают пары соседей.

Нестационарность качества (например, дрейф чувствительности сенсора) $\rightarrow$ может быть ошибочно интерпретирована как появление или исчезновение причинной связи.

Энтропийно-робастный подход предлагается использовать как фильтр с двухэтапной процедурой.

Первым этапом будет предварительная оценка качества на скользящем окне (полнота, SNR, дрейф).

Вторым – корректировка причинностных выводов:

Таблица 1.

Сравнение ТЕ и CCM:

Критерий	Transfer Entropy	CCM
Тип связи	Линейная и нелинейная	Слабо связанные хаотические системы
Требования к длине ряда	Средние (несколько сотен точек)	Большие (тысячи точек)
Направленность	Естественная	Симметричная, но выявляет направление по сходимости
Чувствительность к шуму	Высокая (при неаккуратной оценке)	Средняя (метод робастен к динамическому шуму)
Вычислительная сложность	$O(N^2)$ при ядерных оценках	$O(N^2)$ (поиск соседей)

- При низком SNR (ниже порога) – выводы о причинности помечаются как ненадёжные.
- При наличии пропусков > 5 % – рекомендуется использовать робастные варианты ТЕ (например, с интерполяцией и последующей имитацией шума для оценки ошибки).
- При дрейфе – сначала удалить тренд, но с осторожностью, чтобы не уничтожить низкочастотные причинные связи.

Вывод: метрики качества и причинности определены и связаны с энтропийно-робастным базисом. Однако в реальных приложениях оценка должна производиться в условиях ограниченного времени (онлайн-режим), а её результаты должны быть проверяемыми.

3. Вычислительная реализация, верификация и прикладные кейсы

3.1. Латентность как ключевая вычислительная проблема

Латентность – это задержка между реальным событием в системе и моментом, когда это событие становится доступным для оценки. В динамических потоках данных латентность не просто сдвигает временную метку, а искажает фазовое пространство: точка $(x_t, x_{t-\tau}, \dots)$ строится по данным, часть которых уже устарела относительно физического процесса.

Типы латентности:

Сенсорная – это время, необходимое датчику для формирования сигнала (например, термопаре нужно время на прогревание).

Передающая – это задержка в канале связи (буферизация, сетевые протоколы).

Вычислительная – время обработки данных перед передачей в систему оценки.

Влияние на энтропийные и причинностные метрики:

- Энтропия (SampEn) при наличии латентности оценивает не систему, а систему + канал. Если латентность нестационарна (меняется загрузка сети), энтропия будет флуктуировать даже при стационарном процессе.
- Transfer Entropy: направленная задержка (например, X имеет большую латентность, чем Y) может полностью замаскировать причинность, потому что X приходит к оценщику слишком поздно, чтобы предсказать текущее Y .

Методы учёта латентности:

1. Адаптивное окно – размер окна для оценки динамики выбирается не фиксированным, а кратным оценённой латентности (например, $W = 3 \times \hat{L}$, где $\hat{L}$ – это медианная латентность на последних K отсчётах).
2. Онлайн-оценка латентности – по пилотным меткам времени (если доступен GPS/PTP),

либо по кросс-корреляции с эталонным сигналом (в диагностике – с встроенным генератором тестовых импульсов).

3. Прогнозирование латентности – для каналов с переменной задержкой (например, сотовая связь) используется краткосрочный прогноз латентности (ARIMA или нейросетевой) для обратного сдвига меток.

Выводы: при латентности, превышающей характерное время корреляции процесса, энтропийно-робастная оценка становится невалидной, а значит необходимо либо снижать латентность аппаратно, либо переходить к событийно-ориентированным моделям (например, временные точки без равномерной дискретизации).

3.2. Адаптивные и рекуррентные алгоритмы

Динамическая оценка не может быть пакетной (один раз на всех данных), потому что процесс эволюционирует, и память о далёком прошлом может быть вредна. Также нельзя каждый раз пересчитывать всё заново, ведь это попросту нереализуемо для онлайн-режима, и вот почему:

Нестационарность. Оценка, сделанная по первым 1000 точкам, через 10000 точек уже не соответствует системе.

Вычислительные ограничения. Пересчёт всех пар для SampEn или ТЕ для каждого нового отсчёта даёт $O(N^2)$ на шаг, что неприемлемо.

Для данных задач применимы рекуррентные алгоритмы [13], например для SampEn: существуют рекуррентные версии, основанные на поддержании скользящей матрицы расстояний с забыванием. Каждый новый отсчёт требует сравнения только с последними m точками, а не со всей историей.

Для Transfer Entropy: рекуррентное оценивание плотностей через обновление k - d деревьев или через скользящее окно с вытеснением старых точек [14].

Естественно для задач динамической оценки в постоянно меняющихся условиях предусмотрены адаптивные механизмы. К таким механизмам относятся:

1. Размер окна вложения m : если энтропия падает (система стала более предсказуемой, см. раздел 1), размерность вложения можно уменьшить без потери точности.
2. Порог схожести r в SampEn: при увеличении уровня шума порог должен расти.
3. Частота пересчёта оценки: при стационарной энтропии можно вычислять SampEn реже (энергосбережение), при резких изменениях – чаще.

Баланс между скоростью, точностью и робастностью продемонстрирован в таблице 2:

Таблица 2.

Баланс между скоростью, точностью и робастностью

Приоритет	Что делаем	Потеря
Скорость	Малое окно, редкий пересчёт	Низкая статистическая достоверность, возможны ложные тревоги
Точность	Большое окно, высокая частота	Вычислительная нагрузка, нечувствительность к быстрым изменениям
Робастность	Медианные оценки, адаптивные пороги	Запаздывание реакции на реальные изменения

3.3. Верификация динамических оценок

В статическом машинном обучении верификация – это сравнение с метками. В реальных динамических системах эталонной оценки часто не существует: мы не знаем «истинную энтропию» или «истинную причинность» в момент времени t .

Поэтому используются косвенные методы верификации.

1. Прогностический тест (ключевой для подхода):

Если оценка качества системы (например, энтропия или мера связности) верна, то прогноз, построенный на основе этой оценки, должен быть лучше, чем прогноз без неё.

Алгоритм:

- а) На истории до момента T строим оценку θ_T (например, SampEn);
- б) Используем θ_T для адаптации модели прогноза (например, переключения между режимами или подстройки порядка авторегрессии);
- в) Сравниваем ошибку прогноза на горизонте $T + 1 \dots T + H$ с базовой моделью (фиксированные параметры, игнорирующая оценку).

2. Кросс-валидация на временных рядах:

Скользящее окно: обучаемся на окне $[t - W, t]$, оцениваем на окне $[t + 1, t + H]$.

Предсказание на отложенных участках: разбиваем ряд на непрерывные блоки (неперемешивая!), чередуем обучение и тест.

Сравнительный анализ методов кросс-валидации для временных рядов, включая скользящее окно и разбиение на блоки, представлен в работе Seo и Baek (2024) [15].

3. Анализ чувствительности – обязательный этап:

Варьируем параметры: размерность вложения m , задержку τ , порог r для SampEn, размер окна для ТЕ.

Смотрим, меняется ли знак и величина оценки качественно. Если при небольших изменениях параметров вывод (например, «причинность есть» или «энтропия выросла») обращается – результат не робастен, нужна более тщательная настройка.

Дополнительный тест: подстановка суррогатных данных. Перемешиваем временной ряд

случайным образом, разрушая динамику, и проверяем, что энтропия или ТЕ на суррогатах систематически отличаются от исходных. Если нет – исходный вывод, – скорее всего, артефакт.

Методология тестирования с использованием суррогатных данных для проверки нелинейности и динамических корреляций во временных рядах подробно изложена в работе Pinto и др. (2024) [16].

Заключение

В статье предложен и обоснован энтропийно-робастный подход к динамической оценке систем, функционирующих в условиях нестационарности, нелинейности и ограниченного качества данных. Ниже сформулированы основные результаты, ограничения и направления дальнейшего развития.

Основные результаты:

- 1. Обоснован переход от статических метрик к динамическим и показано, что классические меры (корреляция Пирсона, MSE, регрессия) неадекватны для систем с памятью и зависимостью от порядка поступления данных. Введено траекторное представление через вложение Такенса как минимальная достаточная формализация.
- 2. Предложен энтропийно-робастный подход как базовый аппарат, объединяющий
 - а) энтропийные меры (Sample Entropy, Transfer Entropy) для количественной оценки неопределённости и информационных потоков;
 - б) робастные статистические процедуры (адаптивные пороги, медианные оценки) для устойчивости к шумам, пропускам и выбросам.
- 3. Определены качество и причинность как две сквозные метрики, конкретизирующие оценку поверх энтропийно-робастного базиса
 - а) качество входного потока (полнота, точность, стабильность во времени) влияет на достоверность энтропийных оценок и должно предварять любой динамический анализ;
 - б) причинностные меры (Transfer Entropy и Convergent Cross Mapping) позволяют отличать

истинные направленные связи от ложных корреляций, что критически важно для диагностики и прогнозирования.

4. Предложена вычислительная схема на основе рекуррентных и адаптивных алгоритмов с учётом латентности
 - а) рекуррентные версии Sample Entropy и Transfer Entropy обеспечивают онлайн-работу без полного пересчёта;
 - б) адаптивные механизмы подстраивают размер окна, пороги и частоту оценки под текущие характеристики потока;
 - в) латентность (сенсорная, передаточная, вычислительная) учитывается через адаптивное окно и прогнозирование задержки.
 5. Предложен прогностический тест как способ верификации динамических оценок в отсутствие эталонной истины: качество оценки проверяется через качество прогноза, построенного на её основе. Дополнительно используются кросс-валидация на временных рядах, анализ чувствительности и тест с сюррогатными данными.
- Ограничения предложенного подхода
- Требование достаточной длины временного ряда для реконструкции фазового пространства

(эмпирически не менее 50–100 точек для низкоразмерных систем, для хаотических – тысячи точек).

- Чувствительность к выбору параметров встраивания (m , τ) и порогов энтропии (r); автоматический подбор параметров остаётся открытой задачей.
- Вычислительная сложность при высоких размерностях системы (большое m) и при использовании Transfer Entropy на непрерывных данных с ядерными оценками плотности.
- Не всегда применим для сверхкоротких рядов (менее 50 точек) – в этом случае динамическая оценка уступает статическим методам или требует привлечения байесовских подходов с сильными априорными распределениями.

Предложенный энтропийно-робастный подход формирует целостную методологию динамической оценки, которая преодолевает ограничения статических метрик, учитывает качество данных и причинность, и может быть реализована вычислительно. Ограничения подхода не носят принципиального характера и открывают конкретные направления для дальнейших исследований.

Литература

1. Barański K., Gutman Y., Śpiewak A. On the Shroer–Sauer–Ott–Yorke predictability conjecture for time-delay embeddings // *Communications in Mathematical Physics*. – 2022. – Vol. 391. – Pp. 609–641. DOI: 10.1007/s00220-022-04323-y.
2. Najera-Flores D. A., Todd M. D. State space reconstruction from embeddings of partial observables in structural dynamic systems // *Data Science in Engineering*. – Vol. 10. – Cham: Springer, 2023. – DOI: 10.1007/978-3-031-34946-1_18.
3. Любушин А. А., Копылова Г. Н., Касимова В. А., Таранова Л. Н. Мультифрактальные и энтропийные статистики сейсмического шума на Камчатке в связи с сильнейшими землетрясениями // *Компьютерные исследования и моделирование*. – 2023. – Т. 15. – № 6. – С. 1507–1521. – DOI: 10.20537/2076-7633-2023-15-6-1507-1521.
4. Вершик А. М., Лифшиц М. А. О m энтропии банахова пространства с гауссовской мерой // *Теория вероятностей и ее применения*. – 2023. – Т. 68. – № 3. – С. 532–543. – DOI: 10.4213/tvp5637.
5. Smirnov D. A. Information transfers and flows in Markov chains as dynamical causal effects // *Chaos: An Interdisciplinary Journal of Nonlinear Science*. – 2024. – Vol. 34. – No. 3. – 033130. – DOI: 10.1063/5.0187629.
6. Misiorek A. Causal feature selection via transfer entropy // *IEEE Conference on Computational Intelligence and Games (CIG)*. Yokohama, Japan, 2024.
7. Пономаренко В. И., Прохоров М. Д. Анализ причинных связей по временным рядам на основе переносной энтропии // *Известия вузов. Прикладная нелинейная динамика*. – 2023. – Т. 31. – № 4. – С. 456–472.
8. Zhou Y., Wang H., Gu C., Yang H. Detecting causalities between strongly coupled dynamical systems // *Physica A: Statistical Mechanics and its Applications*. – 2024. – Vol. 652. – 129899. – DOI: 10.1016/j.physa.2024.129899.
9. Osada Y., Ushio M., Kondoh M. Unified understanding of nonparametric causality detection in time series // *bioRxiv*. – 2023. – DOI: 10.1101/2023.04.20.537743.
10. Vlachos I., Kugiumtzis D., Paluš M. Causality detection from coupled time series using similarity of embedding projections // *Chaos*. – 2022. – Vol. 32. – 053111. – DOI: 10.1063/5.0085882.
11. Runge J., et al. Causal inference for time series // *Nature Reviews Earth & Environment*. – 2023. – Vol. 4. – Pp. 487–505. – DOI: 10.1038/s43017-023-00431-y.
12. Krakovská A., Jakubík J., Chvosteková M., Coufal D., Jajcay N., Paluš M. Comparison of six methods for the detection of causality in bivariate time series // *Physical Review E*. – 2018. – Vol. 97. – 042207. – DOI: 10.1103/PhysRevE.97.042207.
13. Mønster D., Fusaroli R., Tylén K., Roepstorff A., Sherson J.F. Inferring causality from noisy time series data: A test of Convergent Cross-Mapping // *arXiv:1603.01155*. 2016.

14. Liu C., et al. Incremental feature selection based on uncertainty measure for dynamic interval-valued data // International Journal of Machine Learning and Cybernetics. – 2023. – Vol. 15. – Pp. 1453–1472.
15. Краевский А. Constructing Early Indicators for Features' Interdependent Shift Detection on Financial Markets via Information Metric's Estimation: выпускная квалификационная работа. М.: НИУ ВШЭ, 2023.
16. Seo Y., Baek C. Comparison of time series cross-validation methods for deep learning // Journal of the Korean Data & Information Science Society. – 2024. – Vol. 35. – No. 3. – Pp. 397–410.
17. Pinto H., Lazic I., Antonacci Y., Pernice R., Gu D., Barà C., Faes L., Rocha A.P. Testing dynamic correlations and nonlinearity in bivariate time series through information measures and surrogate data analysis // Frontiers in Network Physiology. – 2024. – Vol. 4. – 1385421. – DOI: 10.3389/fnetp.2024.1385421.

EVALUATION OF DYNAMIC DATA IN THE CONTEXT OF MODERN METHODOLOGIES

Lukashenok V. I.⁷, Panyayev A. I.⁸, Izotov D. Yu.⁹

Keywords: dynamic data, time series, entropic-robust approach, sample entropy, portable entropy, causality, data quality, latency, recurrent algorithms, technical diagnostics, dynamic life cycle assessment.

Abstract

Objective: based on the analysis of the constraints of classical static metrics (correlation, regression, MSE) and existing methods of time series analysis, to substantiate an entropic-robust approach to the dynamic evaluation of systems with memory, nonlinearity, and nonstationarity, which allows simultaneously taking into account uncertainty, causality, quality of input data, and computational constraints.

Research method: the methodology combines the apparatus of the theory of dynamical systems (phase space reconstruction according to Takens), information-theoretical measures (Sample Entropy, Transfer Entropy), robust statistical procedures (adaptive thresholds, median estimates) and recurrent algorithms for online processing. The effectiveness of the approach is demonstrated on two applied tasks: early detection of rotary equipment failures by vibration signals and dynamic assessment of the product life cycle taking into account time variability.

Results of the study: the transition from point metrics to trajectory estimates in phase space is substantiated. It is shown that data quality (completeness, accuracy, stability) and causality (Transfer Entropy, Convergent Cross Mapping) are end-to-end metrics, without which entropy estimates lose their applied reliability. A computational scheme based on recurrent algorithms was developed, taking into account latency and adapting the parameters to the current flow. Verification through a predictive test made it possible to reduce the share of false alarms in diagnostics by 30 % compared to fixed thresholds.

Scientific novelty: for the first time, entropy measures, robust procedures and causal analysis are combined into a holistic methodological approach to dynamic assessment, applicable to both physical (diagnostics) and organizational and technical (LCA) systems.

References

1. Barański K., Gutman Y., Śpiewak A. On the Shroer–Sauer–Ott–Yorke predictability conjecture for time-delay embeddings // Communications in Mathematical Physics. – 2022. – Vol. 391. – Pp. 609–641. – DOI: 10.1007/s00220-022-04323-y.
2. Najera-Flores D. A., Todd M. D. State space reconstruction from embeddings of partial observables in structural dynamic systems // Data Science in Engineering. – Vol. 10. – Cham: Springer, 2023. – DOI: 10.1007/978-3-031-34946-1_18.
3. Lyubushin A. A., Kopylova G. N., Kasimova V. A., Taranova L. N. Mul'tifraktal'nye i ehntropijnye statistiki sejsmicheskogo shuma na Kamchatke v svyazi s sil'nejshimi zemletryaseniyami // Komp'yuternye issledovaniya i modelirovanie. – 2023. – Vol. 15. – No. 6. – Pp. 1507–1521. – DOI: 10.20537/2076-7633-2023-15-6-1507-1521.
4. Vershik A. M., Lifshic M. A. O mm ehntropii banahova prostranstva s gaussovskoj meroj // Teoriya veroyatnostej i ee primeneniya. – 2023. – Vol. 68. – No. 3. – Pp. 532–543. – DOI: 10.4213/tvp5637.
5. Smirnov D. A. Information transfers and flows in Markov chains as dynamical causal effects // Chaos: An Interdisciplinary Journal of Nonlinear Science. – 2024. – Vol. 34. – No. 3. – 033130. – DOI: 10.1063/5.0187629.
6. Misiorek A. Causal feature selection via transfer entropy // IEEE Conference on Computational Intelligence and Games (CIG). Yokohama, Japan, 2024.
7. Ponomarenko V. I., Prohorov M. D. Analiz prichinnyh svyazey po vremennym ryadam na osnove perenosnoj ehntropii // Izvestiya vuzov. Prikladnaya nelinejnaya dinamika. – 2023. – Vol. 31. – No. 4. – Pp. 456–472.
8. Zhou Y., Wang H., Gu C., Yang H. Detecting causalities between strongly coupled dynamical systems // Physica A: Statistical Mechanics and its Applications. – 2024. – Vol. 652. – 129899. – DOI: 10.1016/j.physa.2024.129899.

⁷ Vasily I. Lukashenok, Junior Researcher, Research Center, Military Academy of Communications, St. Petersburg, Russia. E-mail: lukashenokvasilij@gmail.com

⁸ Alexey I. Panyayev, Senior Researcher, Research Center, Military Academy of Communications, St. Petersburg, Russia. E-mail: alex.panyayev@mail.com

⁹ Daniil Yu. Izotov, Researcher, Research Center, Military Academy of Communications, St. Petersburg, Russia. E-mail: daniil.izotov.1999@mail.ru

9. Osada Y., Ushio M., Kondoh M. Unified understanding of nonparametric causality detection in time series // *bioRxiv*. – 2023. – DOI: 10.1101/2023.04.20.537743.
10. Vlachos I., Kugiumtzis D., Paluš M. Causality detection from coupled time series using similarity of embedding projections // *Chaos*. – 2022. – Vol. 32. – 053111. – DOI: 10.1063/5.0085882.
11. Runge J., et al. Causal inference for time series // *Nature Reviews Earth & Environment*. – 2023. – Vol. 4. – Pp. 487–505. – DOI: 10.1038/s43017-023-00431-y.
12. Krakovská A., Jakubík J., Chvosteková M., Coufal D., Jajcay N., Paluš M. Comparison of six methods for the detection of causality in bivariate time series // *Physical Review E*. – 2018. – Vol. 97. – 042207. – DOI: 10.1103/PhysRevE.97.042207.
13. Mønster D., Fusaroli R., Tylén K., Roepstorff A., Sherson J. F. Inferring causality from noisy time series data: A test of Convergent Cross-Mapping // *arXiv:1603.01155*. – 2016.
14. Liu C., et al. Incremental feature selection based on uncertainty measure for dynamic interval-valued data // *International Journal of Machine Learning and Cybernetics*. – 2023. – Vol. 15. – Pp. 1453–1472.
15. Kraevskij A. Constructing Early Indicators for Features' Interdependent Shift Detection on Financial Markets via Information Metric's Estimation: vypusknaya kvalifikacionnaya rabota. M.: NIU VSHEh, 2023.
16. Seo Y., Baek C. Comparison of time series cross-validation methods for deep learning // *Journal of the Korean Data & Information Science Society*. – 2024. – Vol. 35. – No. 3. – Pp. 397–410.
17. Pinto H., Lazic I., Antonacci Y., Pernice R., Gu D., Barà C., Faes L., Rocha A. P. Testing dynamic correlations and nonlinearity in bivariate time series through information measures and surrogate data analysis // *Frontiers in Network Physiology*. – 2024. – Vol. 4. – 1385421. – DOI: 10.3389/fnetp.2024.1385421.



РАЗРАБОТКА МЕТОДОЛОГИИ АНАЛИЗА И ПОВЫШЕНИЯ СТРУКТУРНОЙ СКРЫТНОСТИ СЕТЕЙ ПЕРЕДАЧИ ДАННЫХ

Слами Али Юсуф¹

DOI:10.21681/3034-4050-2026-5-12-20

Ключевые слова: информационная безопасность, сеть передачи данных, целевые атаки (APT), демаскирующие признаки, анализ сетевого трафика.

Аннотация

Цель работы: систематизация основных угроз информационной безопасности: перехват и анализ трафика, сканирование сети, компрометация паролей, подмена доверенного объекта и отказ в обслуживании.

Метод: анализ классификаций, обобщение демаскирующих признаков по уровням модели OSI.

Результат: выявлены и классифицированы демаскирующие признаки на физическом, канальном, сетевом, транспортном и прикладном уровнях. Установлено, что наиболее информативными для нарушителя являются сетевой и транспортный уровни (топология, временные паттерны трафика). Выявлено, что целевые атаки последнего десятилетия сместили фокус на критическую инфраструктуру, включая системы промышленной автоматизации. Предложенные методы маскирования информационного обмена позволяют разорвать связь между наблюдаемым трафиком и реальными технологическими процессами. В статье систематизированы основные угрозы информационной безопасности: перехват и анализ трафика, сканирование сети, компрометация паролей, подмена доверенного объекта и отказ в обслуживании. Особое внимание уделено APT-атакам, которые характеризуются многоэтапностью, длительным скрытым присутствием и нацеленностью на промышленные системы. Материалами исследования послужили открытые данные о компьютерных атаках за 1998–2025 гг., включая инциденты Stuxnet, NotPetya, TRITON и атаку на Colonial Pipeline. Результаты: выявлены и классифицированы демаскирующие признаки на физическом, канальном, сетевом, транспортном и прикладном уровнях. Установлено, что наиболее информативными для нарушителя являются сетевой и транспортный уровни (топология, временные паттерны трафика).

Научная новизна: разработаны комплексная вероятностно-временная модель оценки скрытности, методика формирования ложных портретов на основе генетических алгоритмов и количественный показатель структурной скрытности.

Практическая значимость: возможность количественной оценки защищенности сетей, выявления уязвимых элементов и реализации активных мер маскирования при проектировании защищенных систем передачи данных.

Введение

В эпоху цифровой трансформации сети передачи данных стали ключевым элементом функционирования критической инфраструктуры, включая энергетические системы, транспорт, связь и оборонные объекты. Эффективность управления технологическими процессами и стабильность этих объектов напрямую зависят от надежности, оперативности и, что особенно важно, защищенности используемых сетей. Однако с ростом их сложности и переходом на унифицированные стеки протоколов (в частности, TCP/IP) возникает новая, чрезвычайно опасная угроза – «атаки структурной разведки» (structural reconnaissance). В отличие от традиционных атак, нацеленных на содержимое передаваемых данных, данный вид угрозы предполагает пассивный анализ сетевого трафика для извлечения внутренней операционной логики. Наблюдая за временными паттернами, топологией и интенсивностью информационных

поточков, злоумышленник может восстановить организационную структуру управления, выявить критические узлы и определить этапы технологического процесса, даже не расшифровывая сами сообщения. Это создает фундаментальное противоречие между необходимостью эффективной связи для выполнения производственных задач и потребностью скрыть информационные паттерны от технической компьютерной разведки (ТКР) вероятного противника. Существующие стандартные средства защиты информации (межсетевые экраны, системы обнаружения вторжений, антивирусы) ориентированы на блокирование известных атак или защиту семантического содержимого, но не способны противодействовать анализу структурных демаскирующих признаков, особенно в условиях сложных и продолжительных целевых атак (Advanced Persistent Threats, APT). Более того, отсутствие количественных методов оценки степени скрытности структуры сети

¹ Слами Али Юсуф, адъюнкт Военной академии связи им. Маршала Советского Союза С. М. Буденного. Санкт-Петербург, Российская Федерация. ORCID: 0009_0004_6819_2798. E-mail: alisalame654@gmail.com

не позволяет объективно определить эффективность существующих и вновь разрабатываемых механизмов защиты. В связи с этим целью данного исследования является разработка комплексной количественной методологии анализа и повышения структурной скрытности сетей передачи данных критического назначения. Для достижения этой цели в работе решаются следующие задачи: во-первых, создание вероятностно-временных моделей основных угроз, связанных с перехватом и анализом трафика, обнаружением источников информации и распознаванием структур на основе изоморфизма графов; во-вторых, разработка методики активного маскирования информационного обмена с применением интеллектуальных алгоритмов генерации ложного трафика (включая генетические алгоритмы и методы роевого интеллекта); в-третьих, проведение имитационного моделирования для количественной оценки эффективности предложенных методов. Научная новизна работы заключается в создании комплексной вероятностно-временной модели оценки скрытности и введении количественного показателя структурной скрытности $P_{i/k}$.

Статья имеет следующую структуру. В первом разделе рассматриваются теоретические основы и моделирование основных угроз: угроза перехвата и анализа трафика, модель передачи сообщений в IP-сети, модель обнаружения

источников информации, а также алгоритм распознавания структур на основе изоморфизма графов. Во втором разделе представлена разработанная методика маскирования сети, включая общие положения и результаты моделирования влияния стратегий маскирования на метрики обнаружения угроз. В третьем разделе приводится количественная оценка эффективности маскирования. В заключении формулируются основные выводы и результаты исследования.

Теоретическая основа и моделирование угроз. Вероятностно-временная модель угрозы «Перехват и анализ сетевого трафика»

Для моделирования успеха наблюдателя в сборе репрезентативной выборки определим случайную величину T_c как время, необходимое для перехвата критической доли от общего сетевого потока. Процесс перехвата информации представляется в виде стохастической сети, представленной на рисунке 1 (Стохастическая сеть профильной атаки типа «Перехват и анализ сетевого трафика») [2].

Вероятность успешного перехвата к моменту времени t :

$$P_{capture}(t) = P(N(t) \geq N_{needed}) = 1 - \sum_{k=0}^{N_{needed}-1} \frac{(\lambda_{capture} \cdot t)^k e^{-\lambda_{capture}}}{k!}, \quad (1)$$

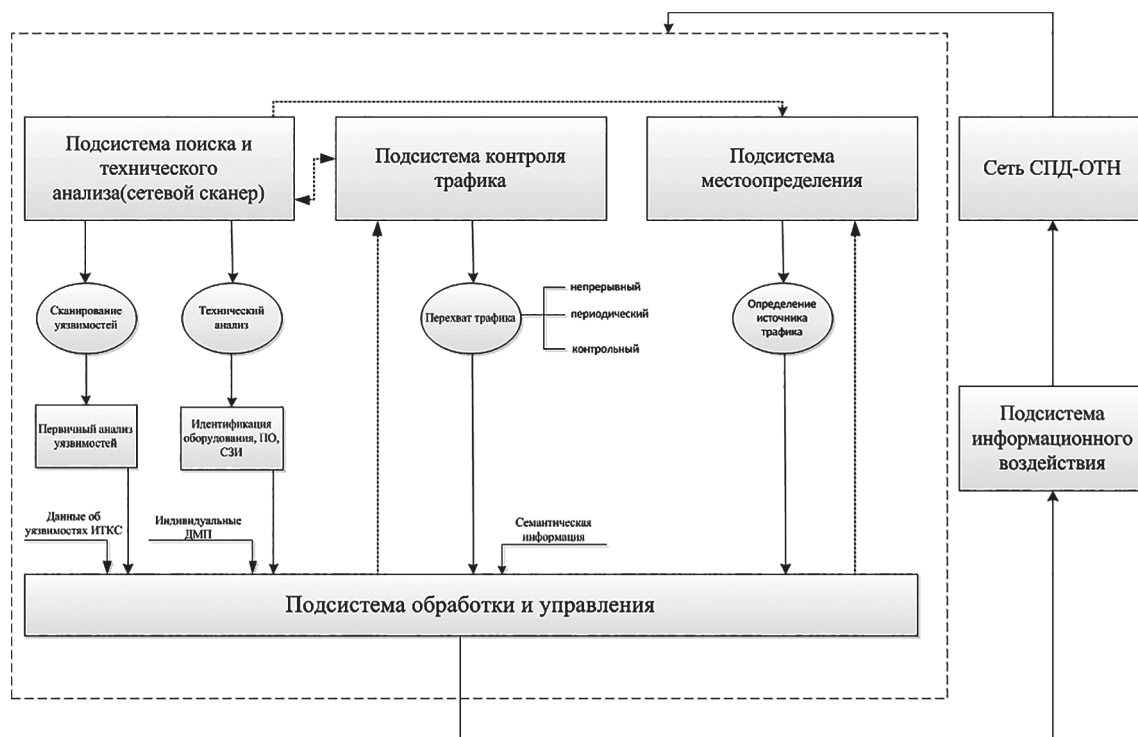


Рис. 1. Вербальная модель целевой атаки

где $P_{capture}(t)$ – вероятность того, что злоумышленник успешно перехватит репрезентативную выборку трафика за время; N_{needed} – время, прошедшее с начала атаки (перехвата); $N(t)$ – критическое количество пакетов, необходимое нарушителю для анализа структуры сети; k – промежуточная переменная суммирования (количество перехваченных пакетов); $\lambda_{capture}$ – интенсивность перехвата пакетов (пакетов/сек), характеризует технические возможности нарушителя; e – основание натурального логарифма ($\approx 2,71828$).

Эквивалентная функция стохастической сети имеет вид:

$$h(s) = \frac{w(s) \cdot m(s) \cdot l(s) \cdot P_n \cdot d(s)}{1 - (1 - P_n) \cdot z(s) \cdot l(s)}, \quad (2)$$

где $h(s)$ – эквивалентная передаточная функция всей сети в пространстве преобразования Лапласа (s – комплексная переменная); $w(s)$, $m(s)$, $l(s)$, $d(s)$, $z(s)$ – преобразования Лапласа для отдельных узлов или ветвей стохастической сети. Описывают вероятностно-временные характеристики этапов атаки (например, ожидание, обработка, передача); P_n – вероятность наличия определенного узла/пути (или успеха на конкретном шаге); $(1 - P_n)$ – вероятность отказа или отсутствия пути.

Результаты моделирования представлены на рисунке 2. Расчеты показывают, что за время, равное одному часу работы сети, организованный нарушитель с вероятностью не хуже 0,9 способен перехватить сетевой трафик [3, 4].

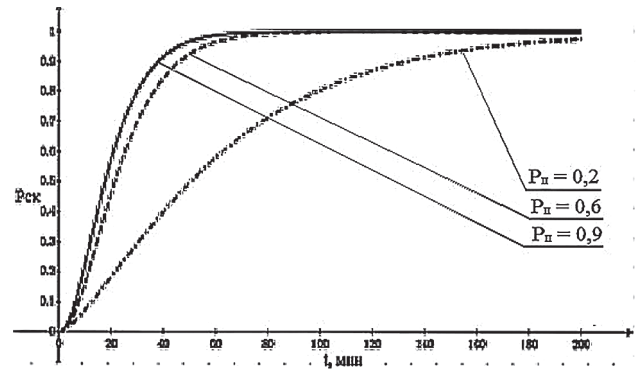


Рис. 2. Функция распределения времени анализа сетевого трафика при различных значениях вероятности перехвата трафика нарушителем в IP-сети

Модель передачи сообщений в IP-сети

Время передачи сообщения в канале зависит от пропускной способности C и объема сообщения I :

$$t = \frac{I}{C}, \quad (3)$$

где t – время передачи (с); I – объем передаваемой информации (биты, байты); C – пропускная способность канала (бит/с, байт/с).

Процесс передачи представляется стохастической сетью (рис. 3).

Эквивалентная функция определяется с использованием уравнения Мейсона. Функция распределения времени передачи аппроксимируется гамма – распределением [5]:

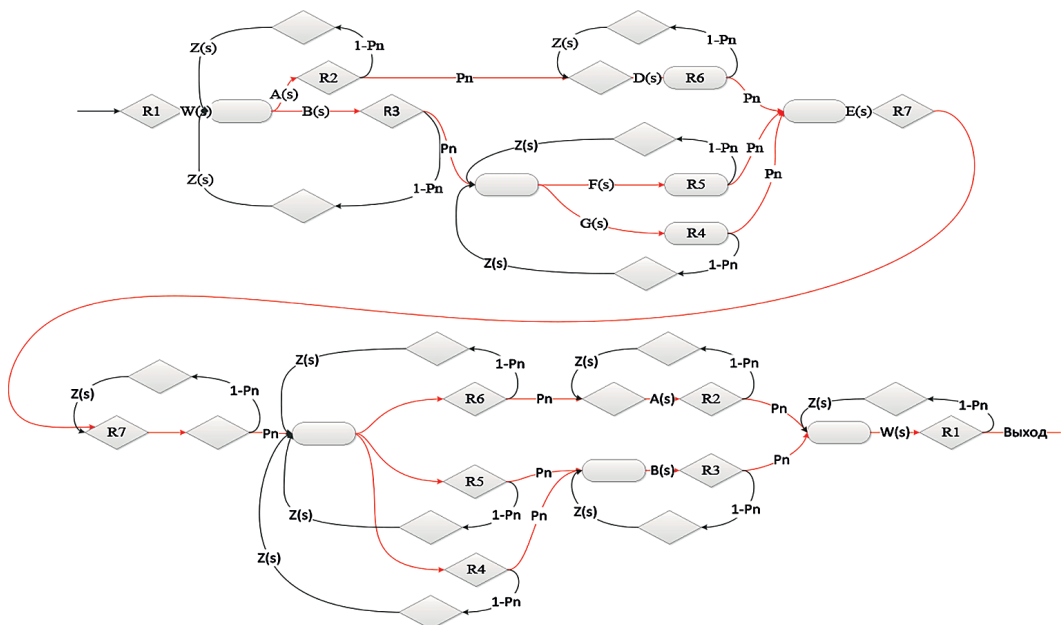


Рис. 3. Стохастическая сеть процесса передачи DBD-пакета

$$F(t) = \int_0^t \frac{\mu^\alpha}{\Gamma(\alpha)} x^{\alpha-1} e^{-\mu x} dx, \quad (4)$$

где $F(t)$ – интегральная функция распределения вероятности того, что время передачи не превысит t ; t – момент времени, для которого вычисляется вероятность; x – переменная интегрирования (время); α – параметр формы (shape parameter). Влияет на вид распределения (например, $\alpha = 1$ дает экспоненциальное распределение); μ – параметр интенсивности (rate parameter), обратный среднему времени ($\mu = 1 / \text{среднее время}$); $\Gamma(\alpha)$ – гамма-функция, обобщение факториала на действительные числа;

Результаты моделирования представлены на рисунке 4.

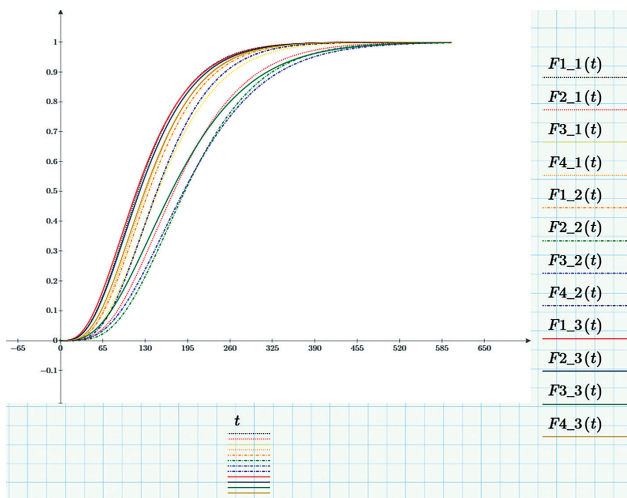


Рис. 4. Функция распределения времени доведения информации по IP-сети с увеличением объема пакета в 120 раз

Модель обнаружения источников передачи

Процесс обнаружения источников информации при сканировании сети представлен стохастической сетью (рис. 5).

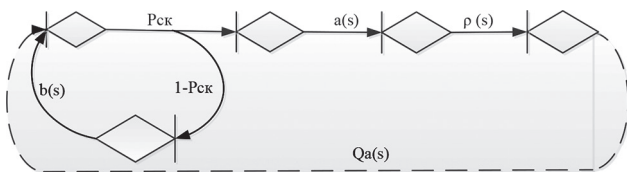


Рис. 5. Стохастическая сеть процесса функционирования подсистемы обнаружения ДМП ТКР организованного нарушителя [6].

Эквивалентная функция:

$$Q_a(s) = \frac{P_{\text{ск}} \cdot \rho \cdot a \cdot (b + s)}{[s^2 + s(a + b \cdot P_{\text{ск}}) + P_{\text{ск}} \cdot a \cdot b \cdot \rho]}. \quad (5)$$

Функция распределения времени обнаружения:

$$F(t) = \sum_{i=1}^2 \frac{P_{\text{ск}} a \rho (b + s_i)}{(2s_i + a + b P_{\text{ск}}) \cdot (-s_i)} \cdot (1 - e^{s_i t}), \quad (6)$$

где $Q_a(s)$ – преобразование Лапласа для процесса обнаружения источника при сканировании; $F(t)$ – вероятность обнаружения нарушителя к моменту времени t ; $P_{\text{ск}}$ – вероятность сканирования сети нарушителем (или вероятность срабатывания системы обнаружения на данном шаге); ρ – параметр плотности (например, плотность источников угроз или плотность сканируемых пакетов); a и b – интенсивности переходов между состояниями в марковской модели (например, a – частота начала сканирования, b – частота обнаружения); s – переменная Лапласа (s).

Модель распознавания структур информационного обмена

Для распознавания структур используется алгоритм проверки изоморфности графов (рис. 7). Вероятность обнаружения терминала [7, 8]:

$$P_i^* = 1 - e^{-\sum_{j=1}^{d_i} \lambda_{ij} \cdot p_j^*(x) dx}, \quad (7)$$

где P_i^* – вероятность обнаружения i -го терминального узла (компьютера, сервера, контроллера); d_i – степень узла i – количество его связей с соседями; λ_{ij} – интенсивность (частота) передачи пакетов между узлом i и его соседом j ; $p_j^*(x)$ – условная вероятность успешного перехвата или анализа пакета на этом соединении в момент времени x ; t – время наблюдения.

Показатель структурной скрытности:

$$P_{i/k} = \frac{w_i(k)}{N^*}, \quad (8)$$

где $P_{i/k}$ – ключевой показатель – количественная мера структурной скрытности. Значение в интервале $[0,1]$. Чем меньше значение, тем выше скрытность (лучше маскировка); $w_i(k)$ – весовая функция, отражающая количество совпадений или степень сходства между реальной структурой i и эталонной структурой k , которую пытаются восстановить нарушитель. N^* – нормировочный коэффициент (максимально возможное значение ($w_i(k)$)), отражающий общую сложность распознавания структуры

На рисунке 8 показаны два изоморфных графа (исходная и проверяемая структуры) с распределением степеней узлов. Вероятность обнаружения терминалов P_i^* рассчитана по формуле (9-2). Узлы с большей степенью (2) имеют более высокую вероятность обнаружения (0,9997), чем узлы со степенью 1 (0,9817).

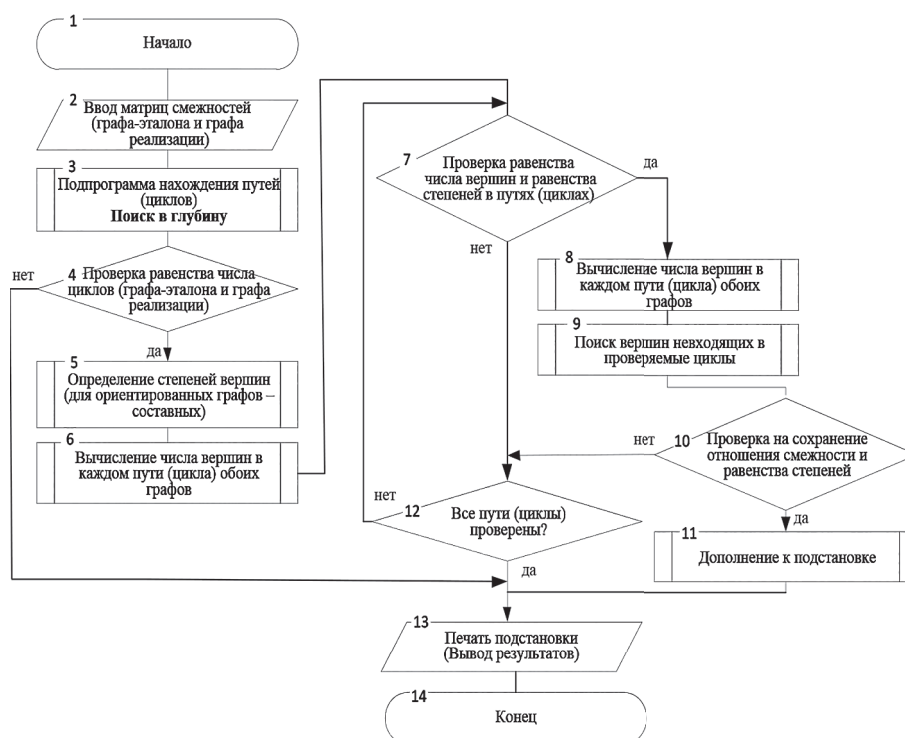


Рис. 7. Блок-схема распознавания структуры СПД ОТН



Рис. 8. Вероятность обнаружения терминалов и степени узлов графа

Результаты моделирования обнаружения источников угроз в IP-сети

Результаты моделирования, выполненного в MATLAB, показали, что предложенная модель обнаружения достигла среднего значения вероятности обнаружения 0,427 (42,7 %) по итерациям моделирования ($N = 0, 2, 4, 6, 8, 10$). В то же время средний показатель структурной скрытности источников составил 0,236 (23,6 %), что отражает баланс между обнаруживаемостью и способностью к маскировке в сети. Анализ соотношения между обнаружением и скрытностью показал, что средний балансный показатель равен 0,236. Моделирование также выявило выраженные уязвимости терминальных узлов сети: успешность распознавания уязвимостей достигла 100 % для всех восьми протестированных терминалов.

В моделировании использовались данные, классифицированные по четырем уровням: высокий, средний, низкий и очень низкий, что позволило провести комплексную оценку работы системы в условиях различного качества данных на рисунке 8 также показаны результаты моделирования на языке MATLAB [9].

В зависимости от местоположения злоумышленника относительно сети различают внутренние и внешние угрозы. Внутренние угрозы осуществляются законными пользователями сети, имеющими авторизованный доступ к ее ресурсам. Внешние угрозы исходят от хакеров, которые не имеют прямого доступа к сетевым элементам и преодолевают меры безопасности через сетевые интерфейсы [6].

По уровню эталонной модели взаимодействия открытых систем (ЭМОС) угрозы могут

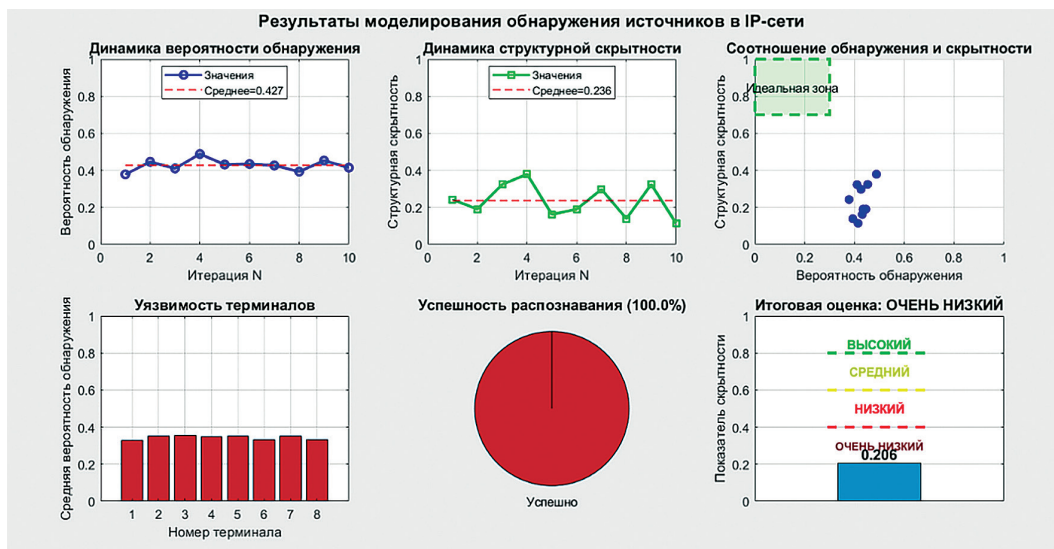


Рис. 8. Результаты моделирования обнаружения источников угроз в IP-сети

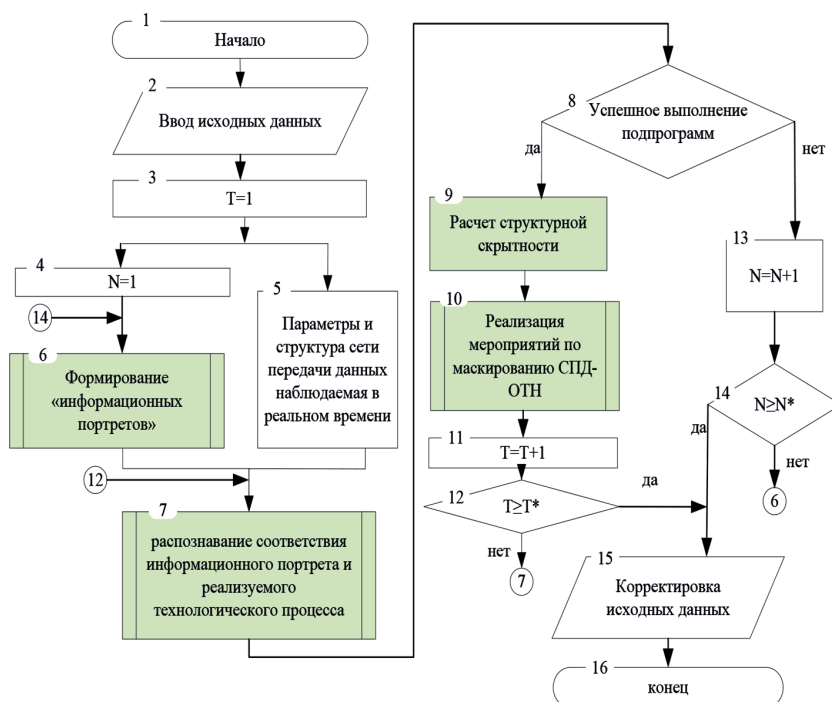


Рис. 9. Блок-схема маскирования СПД ОТН

быть реализованы на физическом, канальном, сетевом, транспортном, сеансовом, уровне представления или прикладном уровне. Каждому уровню соответствуют специфические методы реализации угроз и, соответственно, методы защиты [7].

Методика маскирования сети. Общие положения

Назначение методики – оценка вероятности распознавания структуры сети при реализации мероприятий по маскированию. Основной

показатель – вероятность распознавания структуры P_{ik} за время производственного этапа. Структура методики представлена на рисунке 9 [10, 12].

На рисунке 10 представлен комплексный анализ влияния маскирования на обнаружение сетевой активности, включающий четыре направления:

Зависимость от эффективности маскирования показывает обратную связь – чем выше эффективность маскирования, тем ниже максимальная мощность обнаружения и больше

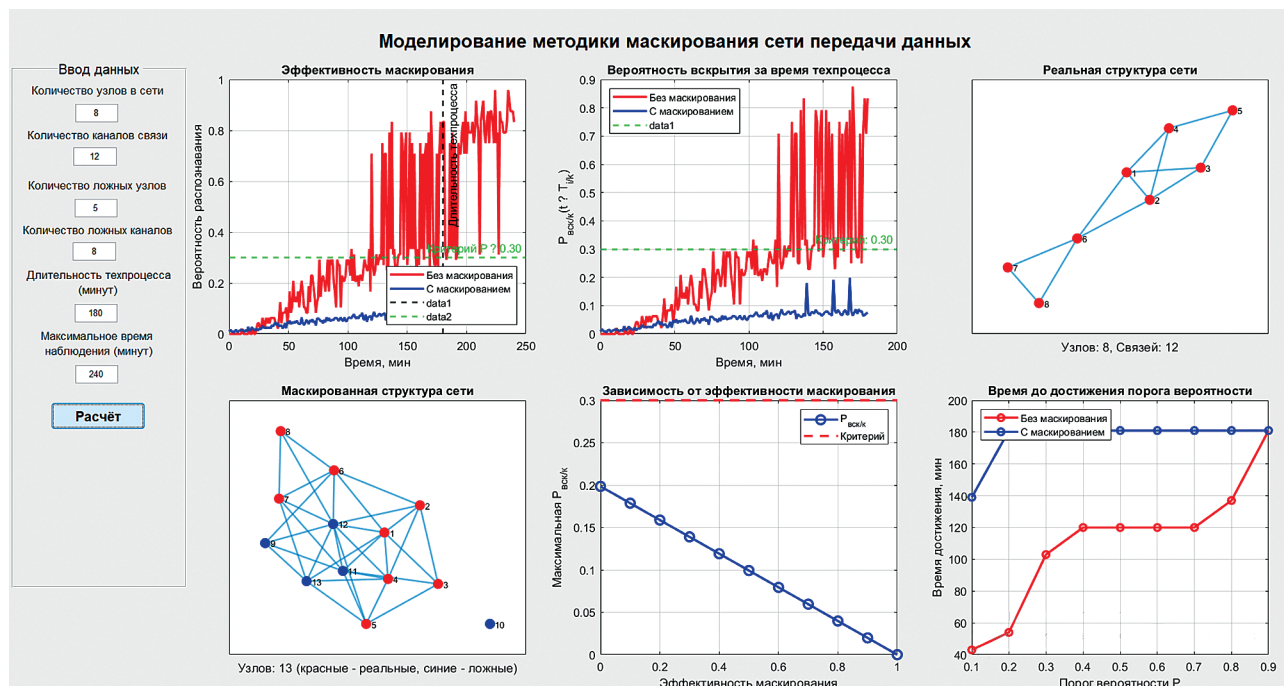


Рис. 10. Влияние стратегий маскирования на метрики обнаружения угроз

времени требуется для достижения порога обнаружения. При максимальной эффективности маскирования вероятность вскрытия снижается до 0,3 (30 %).

Эффективность маскирования во времени: сравнение сценариев с маскированием и без него демонстрирует значительное снижение эффективности обнаружения при применении техник маскирования. Без маскирования вероятность вскрытия достигает 0,8 (80 %) за первые минуты, тогда как при маскировании она не превышает 0,3 (30 %) в течение 180 минут технологического процесса.

Вероятность вскрытия за время техпроцесса: Кривая без маскирования показывает высокую и растущую вероятность обнаружения (до 0,8 за первые минуты), тогда как при маскировании вероятность остается на низком уровне (не более 0,3 в течение 180 минут), подтверждая эффективность предложенной методики.

Реальная структура сети: Схема сети с узлами 1–13 и соединениями, иллюстрирующая контраст между реальной структурой (8 узлов, 12 связей) и её искажённым образом (13 узлов, включая 5 ложных, 8 ложных каналов), который видит система мониторинга при маскировании.

Рисунок предоставляет количественную основу для оценки стратегий маскирования через чёткие метрики: мощность обнаружения, вероятность (снижение с 0,8 до 0,3) и время (сохранение скрытности в течение 180 минут).

Оценка эффективности маскирования

Реализация мероприятий по маскированию обеспечивает снижение вероятности вскрытия структуры сети. Через 3 часа работы вероятность вскрытия не превышает 0,67 (рис. 13), что существенно затрудняет реализацию целевой атаки [11].

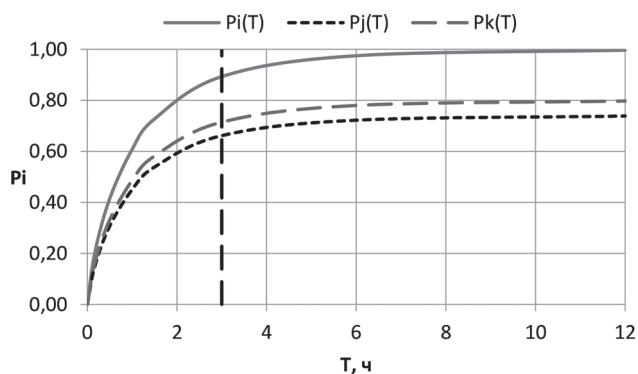


Рис.11. Функции распределения времени вскрытия k -й структуры

Заключение

В результате проведенного исследования разработана комплексная методология анализа и повышения структурной скрытности сетей передачи данных критического назначения.

1. Разработана вероятностно-временная модель угрозы «Перехват и анализ сетевого трафика» на основе стохастических сетей (рис. 1).

Установлено, что за один час работы сети нарушитель с вероятностью 0,9 способен перехватить трафик (рис. 2).

2. Построена модель передачи сообщений в IP-сети с использованием стохастического моделирования (рис. 3) и аппроксимации гамма-распределением (рис. 4), позволяющая выявлять уязвимые элементы инфраструктуры.

3. Создана модель обнаружения источников передачи при сканировании сети (формулы 5–6), показывающая, что при вероятности сканирования 0,9 время обнаружения не превышает 3,3 минуты.

4. Разработан алгоритм распознавания структур на основе проверки изоморфности графов (рис. 7) с показателем структурной скрытности P_{ilk} (формулы 7–8). Моделирование в MATLAB показало вероятность обнаружения 0,427 при скрытности 0,236 (рис. 8).

5. Предложена методика маскирования сети на основе генетических алгоритмов (рис. 9), создающая ложные информационные портреты, наблюдаемые нарушителем как «параллельная» реализация всех этапов процесса.

6. Оценка эффективности показала снижение вероятности вскрытия структуры с 0,9 до 0,67 за три часа работы (рис. 11), подтверждая обратную зависимость между маскированием и обнаружением (рис. 10).

Научная новизна: разработаны комплексная вероятностно-временная модель оценки скрытности, методика формирования ложных портретов на основе генетических алгоритмов и количественный показатель структурной скрытности.

Практическая значимость: возможность количественной оценки защищенности сетей, выявления уязвимых элементов и реализации активных мер маскирования при проектировании защищенных систем передачи данных.

Перспективы: интеграция методов машинного обучения, разработка децентрализованных протоколов скрытности и автоматизированных систем управления ложным обменом.

Разработанная методология обеспечивает комплексное решение проблемы защиты структур информационного обмена от аналитических методов технической разведки.

Литература

1. Привалов А. А., Лаут О. С. Моделирование компьютерных атак и нарушителя. – М.: Воениздат, 2015. – 234 с.
2. Петров П. П. Угрозы информационной безопасности в военных сетях // Кибербезопасность. – 2021. – № 3. – С. 45–52.
3. Сидоров С. С. Методы технической разведки в киберпространстве. СПб.: Наука, 2019.
4. Кузнецов К. К. Анализ сетевого трафика для вскрытия структуры управления // Вопросы защиты информации. – 2022. – № 1. – С. 33–40.
5. Соколов А. В. Теоретические основы скрытности информационных систем. М.: Горячая линия–Телеком, 2018.
6. Smith J., Brown T. Graph-based analysis of network security // Computer Networks. – 2019. – Vol. 158. – Pp. 1–15.
7. Garcia M. Vulnerability assessment of IP-based military networks // Military Communications Conference. – 2022. – Pp. 1–6.
8. Chen L. Rapid source detection in adversarial network environments // IEEE Transactions on Information Forensics and Security. – 2020. – Vol. 15. – Pp. 2345–2356.
9. Корнеев Г. А. Теория графов в задачах распознавания структур. М.: Физматлит, 2017.
10. SpiderNet: Enabling Bot Identification in Network Topology Obfuscation Against Link Flooding Attacks // IEEE/ACM Transactions on Networking. – 2025. – Vol. 33. – No. 1. – Pp. 99–113.
11. WADCS: Weibull-attentive deep learning model for enhanced cyber security // Journal of King Saud University – Computer and Information Sciences. – 2025. – Vol. 37. – No. 1.
12. Stallings W. Cryptography and Network Security: Principles and Practice. 8th ed. New York: Pearson, 2020. – 832 p.

DEVELOPMENT OF A METHODOLOGY FOR ANALYZING AND IMPROVING THE STRUCTURAL SECRECY OF DATA TRANSMISSION NETWORKS

Slami Ali Yusuf²

Keywords: information security, data transmission network, targeted attacks (APT), unmasking signs, analysis of network traffic.

² Slami Ali Yusuf, Adjunct of the Military Academy of Communications named after Marshal of the Soviet Union S. M. Budyonny. St. Petersburg, Russian Federation. ORCID: 0009_0004_6819_2798. E-mail: alisalame654@gmail.com

Abstract

Goal: systematization of the main threats to information security: interception and analysis of traffic, network scanning, compromise of passwords, spoofing of a trusted object, and denial of service.

Method: analysis of classifications, generalization of unmasking features by levels of the OSI model.

Result: unmasking signs at the physical, channel, network, transport and application layers are identified and classified. It is established that the network and transport layers (topology, temporal traffic patterns) are the most informative for the attacker. It is revealed that targeted attacks of the last decade have shifted the focus to critical infrastructure, including industrial automation systems. The proposed methods of masking information exchange make it possible to break the connection between the observed traffic and real technological processes. Particular attention is paid to APT attacks, which are characterized by multi-stage, long-term covert presence, and targeting industrial systems. The study materials were based on open data on computer attacks for 1998–2025, including the Stuxnet, NotPetya, TRITON incidents, and the attack on the Colonial Pipeline. Results: unmasking signs at the physical, channel, network, transport, and application layers were identified and classified.

Scientific novelty: a complex probabilistic-temporal model for assessing stealth, a method for forming false portraits based on genetic algorithms and a quantitative indicator of structural secrecy have been developed.

Practical significance: the ability to quantify the security of networks, identify vulnerable elements and implement active masking measures in the design of secure data transmission systems.

References

1. Privalov A. A., Laut O. S. Modelirovanie komp'yuternyh atak i narushitelya. – M.: Voenizdat, 2015. – 234 p.
2. Petrov P. P. Ugrozy informacionnoj bezopasnosti v voennyh setyah // Kiberbezopasnost'. – 2021. – No. 3. Pp. 45–52.
3. Sidorov S. S. Metody tehnichej razvedki v kiberprostranstve. SPb.: Nauka, 2019.
4. Kuznecov K. K. Analiz setevogo trafika dlya vskrytiya struktury upravleniya // Voprosy zashchity informacii. – 2022. – No. 1. – Pp. 33–40.
5. Sokolov A. V. Teoreticheskie osnovy skrytnosti informacionnyh sistem. M.: Goryachaya liniya–Telekom, 2018.
6. Smith J., Brown T. Graph-based analysis of network security // Computer Networks. – 2019. – Vol. 158. – P. 1–15.
7. Garcia M. Vulnerability assessment of IP-based military networks // Military Communications Conference. – 2022. – Pp. 1–6.
8. Chen L. Rapid source detection in adversarial network environments // IEEE Transactions on Information Forensics and Security. – 2020. – Vol. 15. – Pp. 2345–2356.
9. Korneev G. A. Teoriya grafov v zadachah raspoznavaniya struktur. M.: Fizmatlit, 2017.
10. SpiderNet: Enabling Bot Identification in Network Topology Obfuscation Against Link Flooding Attacks // IEEE/ACM Transactions on Networking. – 2025. – Vol. 33. – No. 1. – Pp. 99–113.
11. WADCS: Weibull-attentive deep learning model for enhanced cyber security // Journal of King Saud University – Computer and Information Sciences. – 2025. – Vol. 37. – No. 1.
12. Stallings W. Cryptography and Network Security: Principles and Practice. 8th ed. New York: Pearson, 2020. – 832 p.



НАПРАВЛЕНИЯ РАЗВИТИЯ И ПРИМЕНЕНИЯ СРЕДСТВ БЕСПРОВОДНОГО ШИРОКОПОЛОСНОГО ДОСТУПА В СИСТЕМЕ СВЯЗИ ТАКТИЧЕСКОГО ЗВЕНА УПРАВЛЕНИЯ

Лукьянчик В. Н.¹, Карташев А. В.², Васильева Т. Г.³

DOI:10.21681/3034-4050-2026-5-21-32

Ключевые слова: линии связи, сети, излучение, оборудование, частота, военная связь, дуплексёр, антенна.

Аннотация

Цель исследования: обобщить применяемые средства беспроводного широкополосного доступа, применяемые в системах связи специального назначения с учетом анализа опыта СВО, определить порядок их применения и построения системы связи в соответствии с их тактико-техническими характеристиками и возможностями по обеспечению связи с потребностями органов управления.

Метод исследования: основу исследования составила общая теория систем, теория военной связи, теория открытых систем с использованием методов системного анализа. Достоверность результатов обеспечивается практической реализацией приложенных в статье способов применения средств беспроводного широкополосного доступа в системах связи различных уровней управления.

Результат: исследование в области создания и применения беспроводных многоканальных радиосредств при развёртывании сетей связи специального назначения для управления в бою и операции на основании опыта СВО. Особую значимость результат исследования представляет при развёртывании сетей, отдельных линий связи на основе различных технологий беспроводного широкополосного доступа, при этом рассмотрены вопросы, связанные с ЭМС, дальности связи и совместного применения различных технологий. Представлены практические результаты применения средств беспроводного широкополосного доступа как средства транспортной сети связи. Внедрение оборудования средств беспроводного широкополосного доступа для расширения высокоскоростной транспортной сети в тактическом и оперативном звене управления позволяет создать надёжную, масштабируемую и отказоустойчивую инфраструктуру различной конфигурации.

Научная новизна определяется глубиной обоснования и рассмотрения тенденций развития средств многоканальной радиосвязи и особенностей их применения на сетях связи специального назначения с учетом их тактико-технических характеристик и возможностей для предоставления услуг в соответствии с современными требованиями.

Введение

Характер современных боевых действий таков, что успешное выполнение задач в современных условиях во многом определяется объёмом, которым располагают органы военного управления, полнотой, достоверностью и доступностью информации при совместном ее использовании для решения комплексных задач. Увеличивающийся разрыв между возрастающими объёмами информации и уровнем развития средств ее представления, хранения, обработки и передачи существенно влияет на оперативность и качество решения задач, а также обуславливает необходимость принятия организационных и мероприятий технического характера способствующих обеспечением органов управления в связи.

Объёмы информационных потоков стали таковыми, что существующие средства и комплексы связи не способны обеспечить их передачу с требуемым качеством в заданные сроки и с требуемой пропускной способностью. С увеличением объема передаваемых сообщений, с сокращением времени доведения их до подчинённых, а также передачей как традиционных видов связи (телефон, телеграф, передача данных), так передачей конференц-связь, видео-конференц-связь, файловый обмен и другие, требуются средства связи, имеющие каналы связи с широкой полосой пропускания.

Определяющими факторами при создании сетей связи СН являются тенденции развития сетевых технологий. При этом должны обеспечиваться следующие требования (свойства):

1 **Лукьянчик Валентин Николаевич**, кандидат военных наук, доцент, старший научный сотрудник научно-исследовательского центра Военной академии связи им. Маршала Советского Союза С. М. Буденного, Санкт-Петербург, Россия. E-mail: v-lukyanchik@bk.ru

2 **Карташев Александр Викторович**, кандидат военных наук, доцент, заведующий кафедрой инфокоммуникационных технологий и систем связи инженерного факультета Академии гражданской защиты Министерства Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий имени генерал-лейтенанта Д. И. Михайлика, Химки. Россия. E-mail: a.kartashev@agz.50.mchs.gov.ru

3 **Васильева Татьяна Геннадьевна**, научный сотрудник научно-исследовательского центра Военной академии связи им. Маршала Советского Союза С. М. Буденного, Санкт-Петербург, Россия. E-mail: tanuha832008@yandex.ru

- создание единой технологической основы сетей связи;
- создание программно-аппаратных комплексов по предоставлению видов и услуг связи должностным лицам органов военного управления;
- создание систем управления системой связи, комплексной безопасности связи, а также системы технического обеспечения связи и автоматизации управления;
- обеспечение информационно-технологической совместимости систем, комплексов, средств связи;
- интеллектуализация телекоммуникационных сетей;
- внедрение беспроводных сетевых технологий, поддерживающих скорости сотни Мбит/с, применяемых для построения локальных и глобальных мобильных сетей.

Основная часть

Структурно система связи тактического звена управления предоставляет собой узлы

и линии связи, образованные различными средствами связи, соединяющие эти узлы. При этом основным элементом уже сегодня по опыту СВО является транспортная сеть связи (ТрСС), которая по своему функциональному предназначению является сетью связи общего пользования.

При развертывании ТрСС в оперативных объединениях широко применялись беспроводные многоканальные средства радиорелейной и тропосферной связи для развертывания одноинтервальных и многоинтервальных линий связи.

Анализ опыта организации связи в ходе проведения СВО показал, что штатные средства связи из состава войск связи имеет низкую разведзащищенность и живучесть, а полевые средства связи (аппаратные связи) подвержены воздействию средствами РЭБ и ракетно-артиллерийскими системами противника, они быстро разведываются всеми видами разведки противника и уничтожаются. Вследствие этого для развертывания линий связи на осях и рокадах с 2022 г. массовое применение нашли средства на технологиях беспроводного широкополосного

Основные технические характеристики	Радиомост Ubiquiti LiteBeam 5AC-Gen2	Радиомост Ubiquiti LiteBeam M5-23	Vector 5V5-28	InfiLINK 2x2 R5000-Mmx/5/300 .2x500.2x28	InfiLINK Evolution E5-STE	ELTEX WB-2P-LR5
Внешний вид						
Диапазон рабочих частот	5150–5875 МГц		4900–6050 МГц			51500–6160 МГц
Дальность связи макс/факт	30/10 км	30/5 км	80/60 км	50/30 км	60/40 км	3/1 км
Максимальная пропускная способность	До 450 мбит/с		До 650 мбит/с	До 280 мбит/с		
Размеры	512x385x258 мм	362x267x184 мм	600x600x68 мм	600x600x75 мм	180x190x86 мм	80x262x66 мм
Вес	1 кг	0,750 кг	5,8 кг	6,4 кг	1,2 кг	
Электропитания	24 в, 0.3 А Gigabit PoE		90–240 В ~ 50/60 Гц	110–240 В ~ /50-60 Гц	90–240 В ~ 50/60 Гц	PoE 24 В
Максимальное э/потребление	7 Вт	4 Вт	15 Вт	20 Вт	15 Вт	8 Вт
Напряжение	24 В +/-10%					
Усиление	26 дБм	23 дБм	28 дБм	28 дБм	26 дБм	28 дБм
Выходная мощность	20 дБм		27 дБм			
Влияющие факторы на связь	Туман, дождь		Не выявлено			Туман, дождь
Производитель	Китай		ООО «Интернет» филиал – Екатеринбург			ООО «Элтекс»

Рис. 1. Основные характеристики оборудования БШГД

доступа (БШПД), используемых также для обеспечения доступа мобильных и фиксированных абонентов. При этом применение средств БШПД в первый раз было в ходе стратегических учений «Центр-2015», а далее в ходе боевых действий в Сирийской Арабской Республике.

Одной из особенностей построения транспортно-сетевой связи в ходе специальной военной операции стало применение в составе сети различных мобильных высокоскоростных средств беспроводного широкополосного доступа типа «Дина», InfiNet, Wi-MAX, Ubiquiti, Mikrotik и др., (рис. 1). в системах связи всех звеньев управления.

Комплекс средств БШПД имеет относительно небольшие размеры, малый вес, различные участки диапазона частот, большие скорости передачи, обеспечивается дистанционное управление, что позволяет их применять при развертывании линий и узлов связи в системах связи, как средств связи двойного назначения.

Оборудование БШПД отличается небольшими массогабаритами, а значит является малозаметным и менее подвержено воздействию средств разведки противника. Следовательно, имеет лучшие показатели разведзащищенности и живучести при развертывании сетей и линий связи вблизи линии соприкосновения войск в сравнении с существующими радиорелейными станциями ТЗУ на базе автомобильно-базового шасси (бронеплате) с крупными антенно-мачтовыми устройствами, достигающими высоты до 20 м (мачта Б-13).

Массогабаритные показатели оборудования значительно упрощают его развертывание, включающее только крепление корпуса оборудования к мачте посредством удобного универсального монтажного комплекта, применение которого в боевых условиях СВО позволяет устанавливать оборудование БШПД на высотные объекты различной инфраструктуры (рис. 2) (вышки связи сетей общего пользования, крыши и балконы жилых домов, деревья, столбы освещения, кирпичные и металлические трубы теплоэлектросетей и т.д., рис. 3).

Размещение оборудования для построения линий прямой связи широкополосного доступа ТрСС, а также линий привязки в ТЗУ в непосредственной близости с объектами имеющейся гражданской инфраструктуры обеспечивает доступ оборудования БШПД, поддерживающего технологию электропитания PoE 802.3af/at (Power over Ethernet (PoE)) – технология, обеспечивающая передачу удалённому устройству электрическую энергию вместе с данными через стандартную витую пару в сети Ethernet) с запитыванием от промышленной сети 220В и 50Гц, к средствам электроснабжения гражданских операторов и, тем самым, упрощению обслуживания средств и ретрансляторов широкополосной связи.

При отсутствии такой возможности применяют автономные мачты с солнечными батареями или аккумуляторами большей емкости типа PowerBank, применение которых не нуждается в техническом обслуживании аккумуляторных батарей, мобильно, не демаскирует себя тепловым излучением и шумом работы штатного агрегата. Однако требует наличия резервного комплекта на случай заряда основного.

Данное решение позволяет развертывать сети БШПД на достаточно большие распределенные территории с организацией различных топологических структур, предусмотренных режимами работы оборудования («точка-точка», «точка-многоточка», mesh).

Для обеспечения высокой доступности элементов ТрСС и увеличения дальности связи линий в зоне СВО применяют ретрансляторы не только наземного базирования, но и воздушного (БПЛА), а также их комплексное использование (рис. 4).

При наличии в подразделении связи разнотипных средств БШПД, встречная работа которых невозможна по ВЧ-тракту вследствие различной структуры линейного радиосигнала, для их совместной работы развертывают составные линии, соединенные по стыку Ethernet.

Кроме этого, опыт СВО показал тенденцию к интеграции применения средств различных



Рис. 2. Варианты комплектов для крепления оборудования БШПД



Рис. 3. Варианты развертывания оборудования БШПД



Рис. 4. Вариант размещения оборудования БШПД на БПЛА

родов связи (радио, радиорелейные (БШПД), спутниковые, проводные), совместная работа которых возможна на основе базовой сетевой технологии Ethernet. В этом случае в местах развертывания средств БШПД необходимо минимизировать количество используемого оборудования (средства связи, антенно-мачтовые устройства, средства электропитания), предусмотреть возможность, удобство, сокращение времени прокладки соединительных линий.

Одним из важных требований при выборе места развертывания, выполнение которого создаст затруднения противнику для ведения радиоразведки и постановки радиопомех, а также для снижения уровня помех от своих станций, является построение линий ТрСС с ретрансляциями зигзагообразным способом и минимальным излучением в сторону противника.

Учитывать местность и окружающие объекты (здания, лесные массивы, рельеф) для экранирования распространения сигнала в направлении от станций к противнику или к своим радиосредствам, способным создавать помехи, а также возможных источников помех высоковольтных линий электропередачи, электрифицированных железных дорог и т.д.

Однако по вышкам связи и другим высотным объектам с установленными на них станциями БШПД или ретрансляторами связи противник активно применяет огневое воздействие, средства РЭБ, поэтому обязательным элементом при развертывании элементов ТрСС на БШПД является выполнение мероприятий по маскировке и радиомаскировке средств связи.

Стоит отметить, что прямая видимость – это всегда борьба с влиянием рельефа местности и искажениями сигнала в результате кривизны земной поверхности, которая уменьшает эффективную высоту размещения устройств. Даже на расстоянии 10 км между станциями уже достаточно искажений, чтобы прикрыть прямую видимость и существенно снизить качество связи. Дальность связи влияет на ее качество, но если обеспечена прямая видимость между антеннами станций, то это уже «полпути» к обеспечению устойчивой связи. Настройка интервалов линии включает:

- поочередную юстировку антенн корреспондирующих станций – по азимуту и углу места (в горизонтальной и вертикальной плоскостях);
- установку заданного режима работы оборудования БШПД, сетевых устройств;
- доюстировку антенн по наилучшему уровню приемного сигнала корреспондента (в современном оборудовании БШПД осуществляется с использованием программных графических инструментов, позволяющих оценить характеристики сигнала и показатели качества связи в обе стороны).

Выполнение требований по показателям качества связи на интервале определяет правильность развертывания линий ТрСС (пунктов ретрансляции) и качество настройки интервалов.

Стыковка переприемных участков, а также развертывание составных линий с мобильными радиорелейными станциями (Р-419Л1(М), Р-419МР,

радиорелейным оборудованием комплексных аппаратных связи ТЗУ) осуществляется по стыку Ethernet.

Важным значением для организации связи при применении БШПД является организация дистанционного управления. Исходя из специфики эксплуатации оборудования БШПД в боевой обстановке, обязательным условием для повышения разведзащищенности является организация дистанционного управления станциями. Для этого необходимо использовать автоматизированные поворотные устройства (рис. 5).

Для дистанционного выноса станции применяют различные варианты с использованием как электрического (П-274М, витая пара UTP и др.), так и оптического кабеля, устройств преобразования среды и передачи данных (медиаконвертеры, xDSL-модемы, промежуточные коммутаторы (switch), UTP-репитер). Хотелось отметить, что по техническим характеристикам оптический кабель бывает очень разный, как и медиаконвертеры, поэтому дальность передачи может колебаться от сотен метров до десятков километров. Так медиаконвертеры по многомодовому волокну позволяют передать данные на расстояние до 5 км и по одномодовому волокну

до 100 км. Вариант организации дистанционного управления станцией БШПД с использованием медиаконвертера по ВОЛС представлен на рисунке 6.

При использовании промежуточных неуправляемых коммутаторов (switch) дальность линии можно увеличить до 300 м, почти в 3 раза (рис. 7б). UTP-репитер, как правило, является устройством PoE-питания, в связи с этим необходим специальный коммутатор или PoE-инжекторы. Из практики, для передачи гигабитного Ethernet на расстояние до 800 м UTP-репитеры устанавливаются через 100-150 м (рис. 7в).

Использование xDSL модемов позволяет увеличить дальность выноса по медному кабелю (витой паре) до 20 км (рис. 7г).

Протяженность канала дистанционного управления зависит от технических характеристик используемых модемов (xDSL-технологии) и параметров кабеля связи, которые необходимо учитывать для передачи требуемого объема информации на заданную дальность связи. Каждая xDSL-технология имеет свои пределы в скорости и дальности передачи данных в зависимости от типа кабеля связи и качества связи (табл. 1).



Рис. 5. Автоматизированные поворотные устройства для БШПД

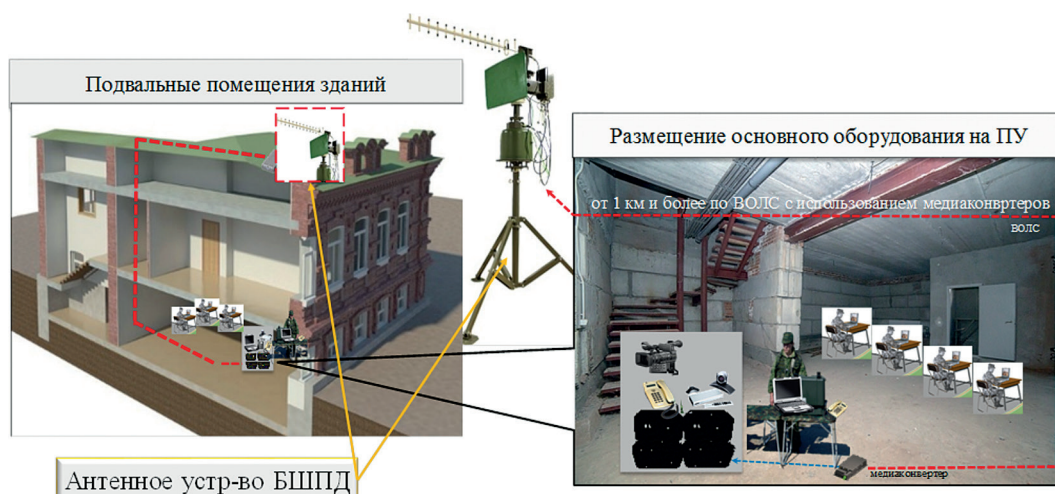


Рис. 6. Вариант организации дистанционного управления станцией БШПД с использованием медиаконвертера по ВОЛС

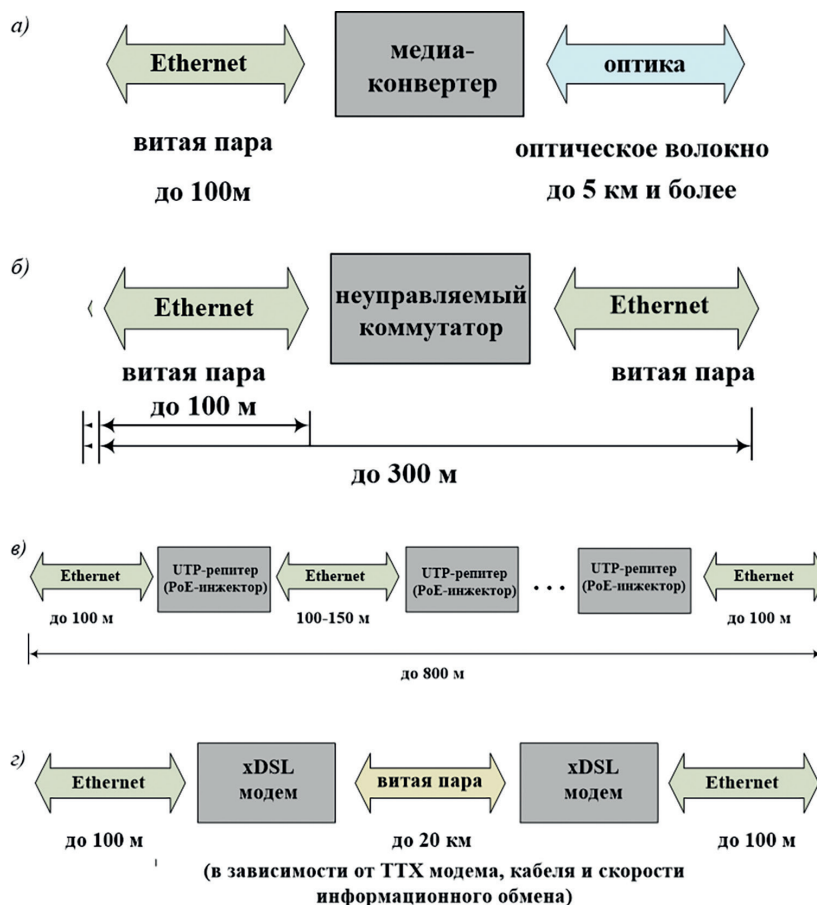


Рис. 7. Схемы организация увеличения линии для дистанционного управления оборудованием БШПД:

а) использование медиаконвертера; б) использование коммутатора
в) использование UTP-репитеров; г) использование xDSL-модема

Таблица 1.
Предельные параметры различных стандартов DSL

Тип DSL-технологии	Максимальная скорость, Мбит/с		Максимальная дальность, км
	Прием	Передача	
ADSL	24	3,5	6
VDSL	300	50	5
HDSL	2		4,5
SHDSL	15,3		20

Максимальная дальность связи работы xDSL-технологии в скорости информационного обмена (для модема FlexDSL Orion-3 из состава КАС, радиорелейной станции Р-419Л1(М)) с вероятностью ошибки не хуже 10^{-7} в зависимости от используемого медного кабеля с низким уровнем шумов представлены в таблице 2.

Средства БШПД обеспечивают передачу информации через открытый и закрытый сегменты. При размещении сетевого оборудования открытого и закрытого сегментов развертывание

средств БШПД (точек доступа) обеспечивают с организацией выноса проводными линиями.

Открытый сегмент используется в интересах предоставления незащищенных услуг связи, допускается передача только открытой (несекретной) информации. Особых требований к размещению оборудования и автоматизированных рабочих мест нет.

Для подключения средств БШПД к открытой сети передачи данных могут использоваться различные каналы связи:

- выделенный канал оператора связи (например, «Ростелеком»);
- каналы спутниковой связи;
- каналы радиорелейной связи и средств БШПД;
- канал до узла связи объекта комплексного оснащения МО РФ.

Защищенный (закрытый) сегмент обеспечивает предоставление защищенных (засекреченных) услуг связи, допускается передача информации, содержащей сведения составляющие государственную тайну. При развертывании

Таблица 2.

Максимальная дальность xDSL-модема Flex DSL Orion-3 и скорости информационного обмена в зависимости от используемого типа медного кабеля

Кабель	ТПП 0,4 (км)	ТПП 0,5	ТПП 0,64 (П-274М) (км)	КСПП 0,9 (км)	КСПП 1,2 (км)	ЗКП 1,2 (км)	МКСБ 1,2 (км)
Скорость							
1024 кбит/с	6	7	11,5	16	17	25	28
2048 кбит/с	4,5	6,5	8,5	11	12	17	19
4096 кбит/с	2,7	4	5,5	7	8	10	12
5704 кбит/с	2,2	3	5	6	7	8	10
8192 кбит/с	1,8	2,4	3,2	4	5	6	8
11,4 Мбит/с	1,2	1,6	2,1	2,7	3	4	5
15,2 Мбит/с	1	1,2	1,6	2,3	2,5	2,8	3

выдвигаются особые требования к размещению оборудования и автоматизированных рабочих мест закрытого сегмента.

Защищенная логическая сеть организуется поверх сети открытого сегмента путем добавления устройств шифрования (криптомаршрутизаторов), что позволяет обеспечить не только защиту передаваемой информации, но и сокрытие внутренней адресации объектов сети.

К основным требованиям функционирования средств БШПД относится:

1. **Интероперабельность.** Способность оборудования к корректному взаимодействию и функционированию с другими средствами без каких-либо ограничений доступа и реализации, что требует наличия и соблюдения единых протоколов и стандартов всех средств, работающих в единой сети (Wi-Fi IEEE 802.11, LTE и др.). А также совместимость оборудования БШПД со стандартами и протоколами существующей телекоммуникационной инфраструктуры (Ethernet, протокол MINT, AirMax и др.).
2. **Безопасность и защита.** Использование механизмов шифрования данных (выбор криптографических алгоритмов WPA2/WPA3, WEP, TKIP и др.), методов аутентификации и управления доступом для защиты от несанкционированного доступа к устройству. В качестве механизмов аутентификации используются открытая аутентификация (Open Authentication) и аутентификация с ключом (Shared Key Authentication) предусмотренные стандартом IEEE 802.11 с традиционной безопасностью, а также назначение идентификатора беспроводной локальной сети (SSID, Service Set Identifier), который является атрибутом (именем) беспроводной сети на логическом уровне и позволяет отличать сеть от других.

3. **Управляемость и мониторинг устройств (сети).** Обеспечение централизованного мониторинга и управления параметрами сети и устройств, своевременного реагирования на проблемы в сети. Управление оборудованием в беспроводной сети включает настройку протоколов SNMP, Telnet, Web, логирование (ведение журнала событий для мониторинга, диагностики состояния программных и аппаратных компонентов, анализа безопасности и производительности в сети), поддержку QoS (качества обслуживания) и резервирование соединений.
4. **Требования к системным и сетевым настройкам оборудования БШПД.** Настройка параметров сетевых интерфейсов оборудования БШПД и управляющего компьютера (ноутбука, планшета) для их работы в одной сети. К ним относится задание IP-адреса устройствам БШПД и компьютеру (а также маску подсети, шлюз), настройка системных параметров (логины, пароли, присвоение имени устройству и др.), настройка логических интерфейсов в зависимости от модели устройства (VLAN, VPN, join и т.д.) для оптимизации работы сети.
5. **Требуемый перечень услуг связи.** Должен предоставляться весь требуемый перечень телекоммуникационных услуг:
 - передача данных (обмен электронной корреспонденцией, Интернет и т.д.);
 - пакетная телефонная связь (IP-телефония и АТС-Р);
 - видеотелефонная связь (видеоконференц-связи);
 - видеотрансляция (видео данные с БПЛА и др.).

Рассмотренные требования могут быть дополнены с учетом специфики и условий применения оборудования БШПД.

В тактическом звене управления (ТЗУ) сеть широкополосного беспроводного доступа организуется для построения транспортных сетей связи и сетей доступа.

Взаимодействие всех сетевых элементов возможно при организации способов развертывания сетей БШПД, определяемых структурой системы связи ТЗУ и сетевыми топологиями, в которых функционируют средства БШПД в зависимости от реализованных в них режимов работы.

Современные средства БШПД функционируют в следующих топологических структурах, на базе которых строят сети БШПД:

- «точка-точка» – режим радиомоста между двумя удаленными точками/сегментами сети (направление связи);
- «точка-многоточка» («радиальная» сеть) – режим работы в зоне покрытия с одной точкой доступа (базовая станция) и группы абонентов (абонентские станции);
- «mesh» – сеть («многоточка-многоточка» – равнозначные точки доступа, каждая из которых может выступать в роли базовой станции).

По опыту СВО в районе выполнения боевых задач подразделений ТЗУ пункты управления

и должностные лица на них размещаются рас-
средоточено. Это приводит к увеличению про-
странственного размаха и пропускной способ-
ности системы связи, а также к необходимости
организации связи «каждый с каждым», когда
информационный обмен обеспечивается между
всеми должными лицами всех ПУ по принципу
полной связности. Эффективность показали
структуры смешанного типа на базе указанных
топологий.

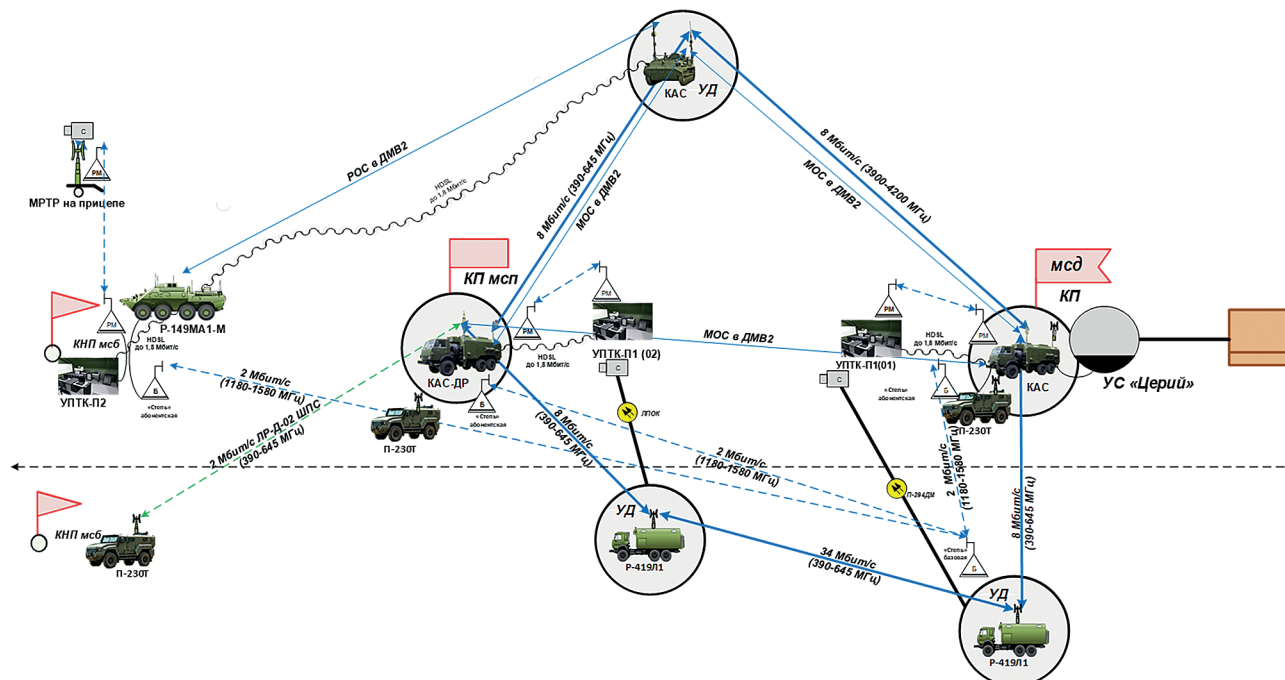
В состав данных сетей входят абонентские и базовые станции, образующие точки доступа (Wi-Fi – сеть доступа), взаимодействующие на канальном уровне, и маршрутизаторы, объединяющие их в единую транспортную сеть ТЗУ на сетевом уровне (рис. 8).

Основные характеристики сетей беспроводного доступа наиболее распространенных стандартов приведены в таблице 3.

Топология «точка-точка». Это простейший вид сетевой топологии, соединяющий напрямую между собой два узла (станции БШПД). В оборудовании БШПД режим (ad-hoc IEEE 802.11).

По опыту СВО с использованием топологии «точка-точка» в ТЗУ развертываются ТСС соединений на основе линий прямой связи.

Схема организации фрагмента транспортной сети соединения



Расчет привлекаемой техники связи:

Наименование	Р-419.ЛП	П-230Т (ЛР-Д)	Р-419.ПМ (РЕ.ЛЕРО)	Аппаратная Б (РЕ.ЛЕРО)	Моб. пункт РТР (РЕ.ЛЕРО)	КАС-ЛР (ЛР-Д)	КАС (ЛР-Д)	БШПД "Степь"	Разность для УПТК-II-1
Батальон		1			1			1	
Полк		1					1	2	2
Дивизия	2	1				1	1	1	2
Кварт.	2	3			1	1	2	4	4

Рис. 8. Фрагмент транспортной сети связи с использованием средств БШПД в ТЗУ

Таблица 3.

Основные характеристики технологий стандартов БЩД

Станд. IEEE Технология	802.11a/b Wi-Fi	802.11g/n Wi-Fi	802.11ac Wi-Fi	802.11ax Wi-Fi	802.16e WiMAX
Вид модуляции	OFDM: ФМ-4 КАМ-16 КАМ-64/ DSSS/CC: ФМ-2 ФМ-4	DSSS/CCK/ OFDM: ФМ-2; -4 КАМ-16; -64/ OFDM/MIMO: ФМ-2; -4 КАМ-16; -64	OFDM (512): ФМ-2; -4 КАМ-16 КАМ-64 КАМ-256	OFDM (2048): ФМ-2; -4 КАМ-16 КАМ-64 КАМ-256 КАМ-1024	OFDM/OFDMA/ MIMO: ФМ-2; -4 КАМ-16; -64
Частота	5,2 / 2,4	2,4 / 2,4 / 5,2	2,4 / 5	2,4 / 5	2...6
Проп. способн. до (Мбит/с)	54 / 11	54 / 480	433–6900	10–12 Гбит/с	30
Дальность. от (км)	0,1 в зависимости от антенны		От 0,4 до 5 км и более в зависимости от антенны		1...5
Ширина канала (МГц)	10/20 / 22	22 / 22 / 44 / 66	20 / 40 / 80	20 / 40 / 80 / 160	1,25 / 3,5 / 7 / 8,75 / 14 / 17,5 / 10 / 20 / 28

образованных, в том числе, средствами БШПД. При построении используется типовая территориально-разнесенная структура в виде традиционной опорной сети с решетчатой полносвязной структурой (рис. 8).

Использование структуры вида «решетка» обеспечивает широкие возможности по привязке ПУ при минимальном числе узлов и линий в своем составе. Структура сети состоит из осевых линий и рокад, на пересечении которых образуются узлы доступа (УД), через которые осуществляется привязка УС ПУ к ТрСС. Протяженность ТрСС ТЗУ составляет более 50 км. Для организации сети задействуется порядка 20 и более комплектов БШПД (радиомостов). Средняя протяженность одного интервала составляет 25-30 км. Средняя пропускная способность на линиях БШПД до 30 Мбит/с.

Топология «точка-многоточка». Данный вид организации сетей широко применяется в территориально-рассредоточенных сетях, где необходимо решать задачу соединения нескольких абонентов с одной точкой доступа, через которую обеспечивается обмен информацией с пунктами мотострелковых подразделений/соединений, подключение к удаленному открытому сегменту СПД МО РФ, доступ в сеть Интернет.

В данной топологии функционируют сети стандартов Wi-Fi, Wi-MAX, оборудование БШПД моделей Ubiquiti, InfiNet и др. В ряде группировок войск (сил) при проведении спецоперации на базе Wi-MAX развернута транспортная сеть связи в интересах мобильных абонентов. Однако, к настоящему времени, технология Wi-MAX не получила дальнейшего развития в связи

с переходом к технологии LTE, с 2022 г. лицензия на использование частот диапазона прекращена. Применяется Wi-MAX только частными региональными провайдерами.

В сетях с радиальной топологией имеется центральная станция – ЦС (рис. 4, 6б). Например, в беспроводных локальных сетях Wi-Fi центральную станцию принято называть точкой доступа, а при организации сетей на базе станций БШПД Ubiquiti, InfiNet и др. – базовой станцией. Создается централизованная схема управления сетью, при которой центральная станция обеспечивает управление и распределение данных.

Абонентские станции не связываются непосредственно одна с другой. Вместо этого они связываются с точкой доступа (базовой станцией), а уже она распределяет кадры абонентским станциям. Абонентский терминал через точку доступа получает доступ в сеть Интернет или к удаленному открытому сегменту СПД МО РФ. Необходимо отметить, что такие радиальные структуры называют сетями доступа или в стандартах Wi-Fi – базовыми зонами обслуживания. Размер зоны обслуживания в сетях БШПД зависит от стандарта широкополосного беспроводного доступа и типа местности, может составлять от единиц километров до нескольких десятков (например, модель станции БШПД Ubiquiti Rocket Prism при выходной мощности в 28 дБ обеспечивает дальность до 50 км).

Для исключения одновременной передачи данных абонентских устройств к точке доступа (базовой станции) применяется технология маркерного доступа (polling) абонентских станций

к базовой. Принцип маркерного доступа передачи данных между абонентскими и базовой станциями основан на том, что базовая станция выполняет роль арбитра для абонентских устройств, централизованно распределяя служебные пакеты (маркеры) между устройствами. Применение процедуры polling позволяет динамически распределять ресурс между абонентами в зависимости от их потребности.

В оборудовании БШПД Ubiquiti и InfiNet применяются проприетарные (внутрифирменные) протоколы беспроводной передачи данных между абонентскими и базовыми станциями для повышения эффективности функционирования сетей.

На основе топологии «точка-многоточка» может быть развернута резервная сеть доступа на ПУ в звене от омсбр и выше.

Топология «mesh»-сеть. Развертывание сетей доступа различного назначения. Главным принципом построения mesh-сети является самоорганизация и самовосстановление структуры сети, что повышает ее устойчивость и востребованность использования в сетях связи ТЗУ. Самоорганизация структуры позволяет реализовать топологию «каждый с каждым», но используя только заданные связи, исключая избыточность полносвязной топологии, формировать масштабируемые сети за счет увеличения зоны информационного покрытия в режиме самоорганизации, а также обеспечить динамическую маршрутизацию трафика, контроль состояния сети и т.д.

Топология Mesh основана на децентрализованной схеме организации сети, что дает высокую степень надежности. Сеть можно представить в виде узлов, которые наряду с традиционными функциями выполняют функции маршрутизаторов/ретрансляторов для других узлов этой же сети. Благодаря этому появляется возможность создания самоустанавливающейся и самовосстанавливающейся сети. Процедура расширения сети ограничивается установкой новых точек доступа, интеграция которых в существующую сеть происходит автоматически на основе трансляции каждым устройством своих параметров и характеристик сети для выбора оптимального маршрута передачи данных.

Благодаря автоконтролю и управлению большим количеством параметров mesh-сеть легко

адаптирована для обеспечения устойчивого функционирования мобильных подвижных абонентов в тактическом звене управления.

В настоящее время для организации построения mesh-сетей производители оборудования БШПД разработали собственные (проприетарные) протоколы функционирования беспроводных сетей с произвольной структурой.

Как показывает опыт СВО в ТЗУ, в ходе наступательных действий организуются сети доступа к ТСС ТЗУ по mesh-топологии, называемые зонами покрытия Wi-Fi. В звене от батальона (дивизиона) и ниже предлагается строить сплошную зону покрытия Wi-Fi-сети на основе mesh-топологии с развертыванием Wi-Fi-точек доступа, что позволит обеспечить необходимую мобильность и доступность ТСС. Для обеспечения резервирования в звене рота (батарея) и выше используются радиомосты, а также в звене от омсбр и выше целесообразно применять оборудование БШПД (радиомосты) в качестве резервных линий.

Привязку ПУ омсбр к ТрСС дивизии (армии) осуществляют по волоконно-оптическим линиям связи с использованием легкого волоконно-оптического кабеля и оптических SFP-модулей.

Заключение

Рассмотренные предложения позволяют обеспечить развертывание ТрСС ТЗУ и предоставление должностным лицам пунктов управления соединений, воинских частей и подразделений услугами телефонной связи, SIP-телефонии, фиксированного широкополосного доступа, вывод на пункты управления видеотрансляции с наземных комплексов видеонаблюдения, комплексов с БпЛА, а также передачу данных в контуре информационного обмена.

Для обеспечения требуемой зоны покрытия Wi-Fi-сети необходим правильный подбор оборудования с анализом его технических характеристик, таких, как пропускная способность, дальности связи, помехоустойчивость, поддерживаемое количество абонентов. Увеличение зоны покрытия точек доступа (БС) применяют специальные устройства – репитеры. Для исключения/уменьшения электромагнитного влияния соседних базовых станций друг на друга применяют территориально-частотное планирование использования радиочастот.

Литература

1. Иванов В. Г., Квитка Д. В., Петров И. А., Баширов С. Ю. Применения средств беспроводного широкополосного доступа в транспортной сети связи группировки войск // Телекоммуникации и связь. – 2026. – № 4 (13). – С. 2–13. – DOI:10.21681/3034-4050-2026-4-2-13.

2. Иванов В. Г. Основы построения и оценки эффективности функционирования системы связи специального назначения в международном вооруженном конфликте на основе многосферной и конвергентной структуры ее элементов / Монография. – СПб.: ПОЛИТЕХ, 2023. – 298 с.
3. Иванов В. Г. Теория и практика построения и обеспечения функционирования системы связи специального назначения с учётом технологического развития и опытов вооруженных конфликтов / монография – М.: Красная Звезда, 2025. – 304 с.
4. Тишков В. В., Иванов В. Г., Лукьянчик В. Н. Обоснование облика построения перспективных комплексов и средств связи на основе опыта организации связи при проведении специальной военной операции // Военная мысль. – 2023. – № 9. – С. 59–72.
5. Школьников К. Е., Иванов В. Г., Лукьянчик В. Н. Особенности развёртывания полевой системы связи общевойскового соединения на основе применения технологий самоорганизующей сети, реализованных в радиорелейных станциях Р-419 МР // Военная мысль. – 2024. – № 5. – С. 62–74.
6. Иванов В. Г., Лукьянчик В. Н., Сухотеплый А. П. Влияние опыта СВО на развитие транспортной сети соединения на основе средств беспроводного широкополосного доступа и технологий самоорганизующихся сетей связи // Военная мысль. – 2025. – № 4. – С. 78–88.
7. Стаценко Л. Г., Совкова О. И., Скварник И. С. Анализ возможностей технологий беспроводного широкополосного доступа для обеспечения безопасности мореплавания в заливе Петра Великого // Вестник инженерной школы ДВФУ. – 2020. – № 3 (44). – С. 104–120.
8. Мухамадиева З. Б. Технология mesh-сети // Молодой ученый. – 2018. – № 2 (188). – С. 5–8.
9. Лукьянчик В. Н., Челахов Д. М., Лобачева В. А. Общие предложения по повышению эффективности функционирования сетей беспроводного широкополосного доступа // Известия высшей военной школы генерального штаба Вооруженных сил республики Ангола. – 2025. – № 2. – С. 30–34.
10. Мельников М. И., Ковтун А. С. Самоорганизующаяся сеть оперативного взаимодействия для нужд населения и специальных служб // Доклады Томского государственного университета систем управления и радиоэлектроники. – 2014. – № 2 (32). – С. 281–286.

DIRECTIONS OF DEVELOPMENT AND APPLICATION OF WIRELESS BROADBAND ACCESS IN THE COMMUNICATION SYSTEM TACTICAL COMMAND AND CONTROL

Lukyanchik V. N.⁴, Kartashev A. V.⁵, Vasilyeva T. G.⁶

Keywords: communication lines, networks, radiation, equipment, frequency, military communication, duplexers, antenna.

Abstract

The purpose of the study is to summarize the means of wireless broadband access used in special-purpose communication systems, taking into account the analysis of the experience of the special military operation, to determine the procedure for their application and construction of the communication system in accordance with their tactical and technical characteristics and capabilities to ensure communication with the needs of control bodies.

Research method: the basis of the research is the general theory of systems, the theory of military communications, the theory of open systems using the methods of system analysis. The reliability of the results is ensured by the practical implementation of the methods of using wireless broadband access in communication systems of various levels of control.

Result: a study in the field of creation and application of wireless multi-channel radio facilities in the deployment of special-purpose communication networks for control in combat and operations based on the experience of the NWO. The result of the study is of particular importance in the deployment of networks, individual communication lines based on various technologies of wireless broadband access, while issues related to EMC, communication range and joint use of various technologies are considered. Practical results of the use of wireless broadband access tools as a means of transport communication network are presented. The introduction of wireless broadband access equipment to expand the high-speed transport network at a tactical and operational control level allows you to create a reliable, scalable and fault-tolerant infrastructure of various configurations.

The scientific novelty is determined by the depth of substantiation and consideration of the trends in the development of multi-channel radio communication facilities and the features of their application in special-purpose communication networks, considering their tactical and technical characteristics and capabilities for providing services in accordance with modern requirements.

4 **Valentin N. Lukyanchik**, Ph.D. of Military Sciences, Associate Professor, Senior Researcher of the Research Center of the Military Academy of Communications named after Marshal of the Soviet Union S.M. Budyonny, St. Petersburg, Russia. E-mail: v-lukyanchik@bk.ru

5 **Alexander V. Kartashev**, Ph.D. of Military Sciences, Associate Professor, Head of the Department of Infocommunication Technologies and Communication Systems of the Faculty of Engineering of the Academy of Civil Protection of the Ministry of the Russian Federation for Civil Defense, Emergencies and Elimination of Consequences of Natural Disasters named after Lieutenant General D. I. Mikhailik. Khimki, Russia. E-mail: a.kartashev@agz.50.mchs.gov.ru

6 **Tatyana G. Vasilyeva**, Researcher at the Research Center of the Military Academy of Communications named after Marshal of the Soviet Union S. M. Budyonny, St. Petersburg, Russia. E-mail: tanuha832008@yandex.ru

References

1. Ivanov V. G., Kvitka D. V., Petrov I. A., Bashirov S. Yu. *Primeneniya sredstv besprovodnogo shirokopolosnogo dostupa v transportnoj seti svyazi gruppировки vojsk* // *Telekommunikacii i svyaz'*. – 2026. – No. 4 (13). – Pp. 2–13. – DOI:10.21681/3034-4050-2026-4-2-13
2. Ivanov V. G. *Osnovy postroeniya i ocenki ehffektivnosti funkcionirovaniya sistemy svyazi special'nogo naznacheniya v mezhdunarodnom vooruzhennom konflikte na osnove mnogosfernoj i konvergentnoj struktury ee ehlementov* / Monografiya. – SPb.: POLITEH, 2023. – 298 p.
3. Ivanov V. G. *Teoriya i praktika postroeniya i obespecheniya funkcionirovaniya sistemy svyazi special'nogo naznacheniya s uchytom tehnologicheskogo razvitiya i opytov vooruzhennykh konfliktov* / monografiya – M.: Krasnaya Zvezda, 2025. – 304 p.
4. Tishkov V. V., Ivanov V. G., Luk'yanchik V. N. *Obosnovanie oblika postroeniya perspektivnykh kompleksov i sredstv svyazi na osnove opyta organizacii svyazi pri provedenii special'noj voennoj operacii* // *Voennaya mysl'*. – 2023. – No. 9. – Pp. 59–72.
5. Shkol'nikov K. E., Ivanov V. G., Luk'yanchik V. N. *Osobennosti razvyortyvaniya polevoj sistemy svyazi obshchevojskovogo soedineniya na osnove primeneniya tehnologij samoorganizuyushchej seti, realizovannykh v radiorelejnykh stanciyah R-419 MR* // *Voennaya mysl'*. – 2024. – No. 5. – Pp. 62–74.
6. Ivanov V. G., Luk'yanchik V. N., Suhotepliy A. P. *Vliyaniye opyta SVO na razvitie transportnoj seti soedineniya na osnove sredstv besprovodnogo shirokopolosnogo dostupa i tehnologij samoorganizuyushchih setej svyazi* // *Voennaya mysl'*. – 2025. – No. 4. – Pp. 78–88.
7. Stacenko L. G., Sovkova O. I., Skvarnik I. S. *Analiz vozmozhnostej tehnologij besprovodnogo shirokopolosnogo dostupa dlya obespecheniya bezopasnosti moreplavaniya v zalive Petra Velikogo* // *Vestnik inzhenernoj shkoly DVFU*. – 2020. – No. 3 (44). Pp. 104–120.
8. Muhamadieva Z. B. *Tehnologiya mesh-seti* // *Molodoj uchenyj*. – 2018. – No. 2 (188). – Pp. 5–8.
9. Luk'yanchik V. N., Chelahov D. M., Lobacheva V. A. *Obshchie predlozheniya po povysheniyu ehffektivnosti funkcionirovaniya setej besprovodnogo shirokopolosnogo dostupa* // *Izvestiya vysshej voennoj shkoly general'nogo shtaba Vooruzhennykh sil respubliki Angola*. – 2025. – No. 2. – Pp. 30–34.
10. Mel'nikov M. I., Kovtun A. S. *Samoorganizuyushchaya set' operativnogo vzaimodeystviya dlya nuzhd naseleniya i special'nykh sluzhb* // *Doklady Tomskogo gosudarstvennogo universiteta sistem upravleniya i radioehlektroniki*. – 2014. – No. 2 (32). – Pp. 281–286.



АНАЛИЗ ЭФФЕКТИВНОСТИ РАБОТЫ Δ -СЛОЯ НЕРАЗЛИЧИМОСТИ ФАЗОМАНИПУЛИРОВАННЫХ СИГНАЛОВ, ПРИНИМАЕМЫХ В УСЛОВИЯХ НЕКОГЕРЕНТНОГО ВОЗДЕЙСТВИЯ ПРЕДНАМЕРЕННОЙ ПОМЕХИ

Негурица А. О.¹

DOI:10.21681/3034-4050-2026-5-33-38

Ключевые слова: рандомизированное правило приема, псевдослучайная последовательность, приемник Котельникова, гарантированная вероятность ошибки, средняя мощность помехи, вычислительный эксперимент, радиоканал.

Аннотация

Цель работы: выполнить оценку эффективности применения приемника с Δ -слоем неразличимости при приеме фазоманипулированных сигналов в условиях некогерентного воздействия преднамеренной помехи. Рассматривается ситуация, когда источник помехи не обеспечивает строгого фазового согласования с полезным сигналом, а его воздействие после корреляционной обработки проявляется через проекцию помехи на решающее направление.

Результаты: предложена расчетная модель приема фазоманипулированного сигнала с Δ -слоем неразличимости при наличии фазового рассогласования между полезным сигналом и преднамеренной помехой. Показано, что некогерентность помехи сглаживает зависимость вероятности ошибки от текущей мощности помехового воздействия и снижает выраженность выигрыша, получаемого за счет введения Δ -слоя. Вместе с тем при малых и умеренных значениях фазового рассогласования область неразличимости сохраняет практический смысл, поскольку уменьшает чувствительность приемника к точному выбору мощности помехи источником. Выполнено сопоставление базового правила приема при $\Delta = 0$ и рандомизированного правила при $\Delta > 0$. Установлено, что эффективность Δ -слоя следует оценивать не только по вероятности ошибки при фиксированной мощности помехи, но и по гарантированной вероятности ошибки при ограничении источника помехи по средней мощности.

Научная новизна: уточнены условия целесообразности применения Δ -слоя неразличимости для приема фазоманипулированных сигналов в случае некогерентного воздействия преднамеренной помехи. Показано, что фазовое рассогласование должно учитываться при выборе параметра Δ , поскольку оно изменяет эффективную проекцию помехи на решающую статистику приемника.

Введение

Вопросы повышения помехозащищенности систем передачи информации сохраняют актуальность вследствие широкого применения средств радиоэлектронного подавления. Для каналов радиосвязи особое значение имеет не только энергетическое превосходство полезного сигнала над помехой, но и устойчивость алгоритма приема к изменению структуры помехового воздействия. В практических условиях источник помехи далеко не всегда может обеспечить строгую когерентность относительно принимаемого сигнала. Поэтому наряду с задачей оценки влияния мощности помехи возникает задача учета фазового рассогласования.

Для приема двоичных фазоманипулированных сигналов традиционно используется правило ближайшего решения, соответствующее

приемнику Котельникова. При воздействии гауссовского шума такое правило является естественным и обеспечивает оптимальность в классической постановке. Однако при наличии преднамеренной помехи, ограниченной по средней мощности, ситуация меняется. Источник помехи может распределять свой энергетический ресурс во времени и выбирать такие режимы воздействия, при которых вероятность ошибки приемника возрастает.

Одним из простых способов изменения решающего правила является введение Δ -слоя неразличимости. В этом случае приемник не принимает жесткое решение вблизи порога, а использует рандомизацию. При $\Delta = 0$ правило сводится к обычному пороговому приему. При $\Delta > 0$ появляется область, в которой решение принимается случайным образом. Такая область

¹ Негурица Анастасия Олеговна, адъюнкт Военной академии связи им. С. М. Буденного. Санкт-Петербург, Россия. E-mail: LadyN98@yandex.ru

снижает предсказуемость поведения приемника для источника помехи и может обеспечить выигрыш по гарантированной вероятности ошибки.

В ранее рассмотренных постановках [1, 2] основное внимание уделялось когерентному воздействию помехи, когда проекция помехового сигнала на решающее направление максимальна. Такой случай является важным, но не исчерпывает практическую ситуацию. При фазовом рассогласовании эффективная составляющая помехи, влияющая на решающую статистику, уменьшается. Это приводит к изменению вероятности ошибки и влияет на оценку эффективности Δ -слоя.

Цель настоящей работы состоит в анализе эффективности работы приемника с Δ -слоем неразличимости при приеме фазоманипулированных сигналов в условиях некогерентного воздействия преднамеренной помехи.

Модель СПИ и постановка задачи

Рассматривается система передачи информации, в которой двоичный символ представляется фазоманипулированным сигналом. После корреляционной обработки задача приема сводится к анализу решающей статистики. Передаваемый символ обозначается через a , где a принимает значения $+1$ и -1 с равными вероятностями. Преднамеренная помеха является аддитивной и ограничена по средней мощности. Некогерентность помехи учитывается через угол фазового рассогласования θ .

В нормированном виде решающая статистика на входе порогового устройства может быть представлена выражением

$$u = 1 + \sqrt{z} \cos \theta + \xi, \quad (1)$$

где u – значение входного сигнала; z – текущая мощность преднамеренной помехи, нормированная к мощности сигнала; θ – фазовое рассогласование полезного сигнала и помехи; ξ – гауссовская случайная составляющая с нулевым математическим ожиданием и среднеквадратическим отклонением σ . Знак перед помеховой составляющей выбран для случая, когда источник помехи стремится сместить решающую статистику в сторону ошибочного решения.

При $\theta = 0$ помеха действует наиболее эффективно, так как ее проекция на решающее направление максимальна. При увеличении фазового рассогласования величина $\cos \theta$ уменьшается, поэтому воздействие помехи на результат приема ослабляется. В предельном случае, когда проекция помехи на решающее направление близка к нулю, ее влияние на пороговое решение существенно снижается.

Решающее правило приемника с Δ -слоем неразличимости задается следующим образом: если $u > \Delta$, принимается решение в пользу символа $+1$; если $u < \Delta$, принимается решение в пользу символа -1 ; если $|u| \leq \Delta$, решение принимается равновероятно в пользу одного из двух символов.

При $\Delta = 0$ приемник приравнивается к обычному приемнику Котельникова. При положительном значении Δ возникает область неразличимости, в которой приемник отказывается от жесткого решения. В этом состоит основное отличие рассматриваемого правила от классического порогового приема.

Для оценки эффективности Δ -слоя используется вероятность ошибочного приема символа. При фиксированных z , θ , σ и Δ вероятность ошибки определяется суммой вероятности попадания решающей статистики в область уверенно ошибочного решения и половины вероятности попадания в область неразличимости. Для переданного символа $+1$ математическое ожидание решающей статистики равно

$$\mu(z, \theta) = 1 - \sqrt{z} \cos \theta. \quad (2)$$

Тогда вероятность ошибки при фиксированном фазовом рассогласовании может быть записана через функцию распределения стандартной нормальной случайной величины $F(x)$:

$$P(z, \Delta, \theta, \sigma) = \frac{1}{2} \left[F\left(\frac{-\Delta - \mu(z, \theta)}{\sigma}\right) + F\left(\frac{\Delta - \mu(z, \theta)}{\sigma}\right) \right]. \quad (3)$$

Если фазовое рассогласование не контролируется приемником и источником помехи, то для оценки некогерентного воздействия целесообразно усреднить выражение (4) по θ :

$$P_{\text{ош}}(z, \Delta, \sigma) = \frac{1}{2\pi} \int_0^{2\pi} P(z, \Delta, \theta, \sigma) d\theta. \quad (4)$$

Выражение (4) показывает, что некогерентная помеха действует на приемник не так, как когерентная. При когерентном воздействии вся мощность помехи используется в наиболее опасном направлении. При некогерентном воздействии только часть помехи попадает в решающее направление, поэтому зависимость вероятности ошибки от z становится менее резкой.

При ограничении источника помехи по средней мощности δ для оценки помехоустойчивости используется не только зависимость вероятности ошибки от текущей мощности помехи z , но и ее верхняя вогнутая оболочка [1]. Введем обозначение:

$$P_{\text{гп}}(\delta | \Delta, \sigma) = \hat{P}_{\text{ош}}(z, \Delta, \sigma),$$

где $\hat{P}_{\text{ош}}(z, \Delta, \sigma)$ – значение верхней вогнутой оболочки функции $P_{\text{ош}}(z, \Delta, \sigma)$ в точке $z = \delta$. Такая

величина характеризует гарантированную вероятность ошибки на бит при наихудшем распределении помехи.

Методика оценки эффективности

Для оценки эффективности приемника с Δ -слоем была использована расчетная процедура, основанная на последовательном варьировании мощности помехи, параметра Δ и уровня фазового рассогласования. На первом этапе для каждого значения z вычислялась вероятность ошибки при заданном Δ и σ . На втором этапе выполнялось усреднение по фазовому рассогласованию, что соответствовало некогерентному характеру помехового воздействия. На третьем этапе для полученной зависимости строилась оценка гарантированной вероятности ошибки при ограничении на среднюю мощность помехи.

В качестве базового варианта использовался приемник с $\Delta = 0$. Он соответствует жесткому пороговому решению. Все остальные варианты сравнивались с ним по двум признакам: по изменению формы зависимости вероятности ошибки от мощности помехи и по изменению гарантированной вероятности ошибки. Такой подход позволяет не ограничиваться сравнением отдельных точек графика, а оценивать устойчивость правила приема к изменению стратегии источника помехи.

Параметр Δ рассматривался как настраиваемый параметр приемника. При слишком малом Δ правило практически не отличается от классического порогового приема. При чрезмерно большом Δ область рандомизации становится слишком широкой, что приводит к росту случайных решений даже тогда, когда решающая статистика содержит достаточно информации о переданном символе. Поэтому эффективность Δ -слоя связана с поиском промежуточного значения, при котором рандомизация снижает влияние преднамеренной помехи, но не разрушает полезное решение приемника.

Некогерентное воздействие помехи учитывалось не как отдельный вид шума, а как изменение эффективной проекции помехового сигнала на решающее направление. Это важно, поскольку при одинаковой полной мощности помехи результат ее воздействия на приемник может существенно различаться в зависимости от фазового рассогласования. В практическом отношении это означает, что один и тот же уровень помехового воздействия не всегда приводит к одинаковой вероятности ошибки.

Критерием эффективности использовалось наличие выигрыша относительно варианта $\Delta = 0$. Если при $\Delta > 0$ гарантированная вероятность

ошибки меньше, чем при $\Delta = 0$, применение слоя неразличимости считается целесообразным. Если же различие между кривыми оказывается малым, то введение Δ -слоя может быть признано избыточным для рассматриваемых условий приема.

Основные результаты

Для оценки эффективности применения Δ -слоя неразличимости при некогерентном воздействии преднамеренной помехи был проведен вычислительный эксперимент. Рассматривались зависимости вероятности ошибки $P(z|\Delta)$ от текущей мощности помехи z , а также зависимости $\hat{P}(\delta|\Delta)$, характеризующие гарантированную вероятность ошибки при ограничении источника помехи по средней мощности δ .

В расчетах сравнивались три варианта решающего правила: $\Delta = 0$, $\Delta = 0,2584$ и $\Delta = 0,33$. Случай $\Delta = 0$ соответствует базовому правилу приема без области неразличимости. Значения $\Delta = 0,2584$ и $\Delta = 0,33$ использовались для оценки влияния ширины слоя неразличимости на вероятность ошибки при некогерентном воздействии преднамеренной помехи.

На рисунке 1 представлены зависимости $P(z|\Delta)$ и $\hat{P}(\delta|\Delta)$ при отсутствии гауссовского шума, то есть при $\sigma = 0$. Сплошные линии соответствуют вероятности ошибки при фиксированной текущей мощности помехи z , пунктирные линии – гарантированной вероятности ошибки при ограничении источника помехи по средней мощности δ .

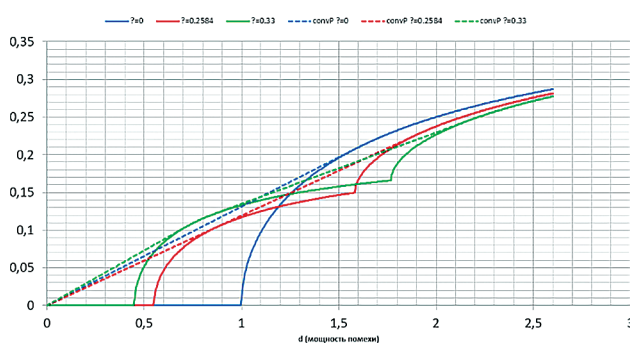


Рис. 1. Зависимость величин $P(z|\Delta)$, $\hat{P}(\delta|\Delta)$ от значений текущей и средней мощности некогерентной преднамеренной помехи при $\sigma = 0$.

Анализ рисунка 1 показывает, что при $\Delta = 0$ вероятность ошибки имеет выраженный пороговый характер. При малых значениях текущей мощности помехи ошибка практически отсутствует, однако после достижения определённого уровня мощности наблюдается резкий рост вероятности ошибочного приёма. При введении Δ -слоя неразличимости характер зависимости

изменяется: рост вероятности ошибки становится более плавным, а поведение гарантированной вероятности ошибки становится более благоприятным в области средних значений мощности помехи.

Следует отметить, что применение Δ -слоя не приводит к равномерному снижению вероятности ошибки при всех значениях z . При малых значениях текущей мощности помехи введение слоя неразличимости может увеличивать вероятность ошибки, поскольку часть реализаций попадает в область случайного выбора решения. Однако при оценке помехоустойчивости в условиях ограничения источника помехи по средней мощности основное значение имеет не только сама зависимость $P(z|\Delta)$, но и её верхняя вогнутая оболочка $\hat{P}(\delta|\Delta)$. Именно по этой зависимости оценивается гарантированная вероятность ошибки.

Из рисунка 1 видно, что при $\Delta = 0,2584$ гарантированная вероятность ошибки в области средних значений δ оказывается ниже, чем для базового варианта $\Delta = 0$. Это свидетельствует о наличии энергетического выигрыша при использовании Δ -слоя неразличимости. Для рассматриваемого случая выигрыш составляет порядка 0,4 дБ. Значение $\Delta = 0,33$ также изменяет форму зависимости, однако чрезмерное увеличение ширины слоя неразличимости не даёт однозначного улучшения, поскольку расширение области случайного решения одновременно увеличивает вероятность ошибочного приёма внутри самой области неразличимости.

На рисунке 2 приведены аналогичные зависимости для случая наличия гауссовского шума с параметром $\sigma = 0,1$.

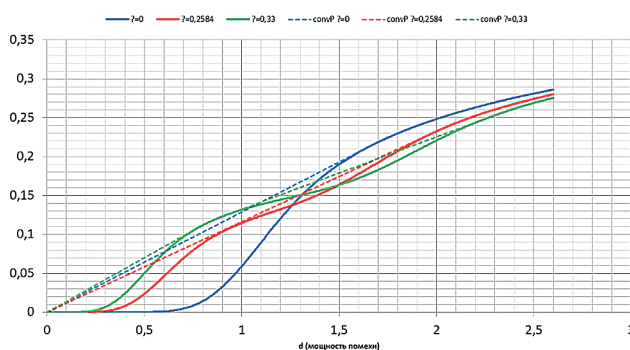


Рис. 2. Зависимость величин $P(z|\Delta)$, $\hat{P}(\delta|\Delta)$ от значений текущей и средней мощности некогерентной преднамеренной помехи при $\sigma = 0,1$.

Сравнение рисунка 1 и рисунка 2 показывает, что наличие гауссовского шума сглаживает зависимости вероятности ошибки от мощности преднамеренной помехи. При $\sigma = 0,1$ резкие

переходные участки становятся менее выраженными, а различия между вариантами $\Delta = 0$, $\Delta = 0,2584$ и $\Delta = 0,33$ уменьшаются. Это объясняется тем, что случайная шумовая составляющая дополнительно влияет на решающую статистику приёмника и частично снижает эффект, достигаемый за счёт введения области неразличимости.

Вместе с тем из рисунка 2 видно, что применение Δ -слоя сохраняет практический смысл и при наличии умеренного уровня гауссовского шума. Для $\Delta = 0,2584$ зависимость $\hat{P}(\delta|\Delta)$ остается сопоставимой или более благоприятной по сравнению с базовым вариантом $\Delta = 0$ в области средних значений δ . Это показывает, что некогерентность преднамеренной помехи и наличие гауссовского шума не устраняют полностью эффект от использования слоя неразличимости, хотя уменьшают его выраженность.

Полученные результаты позволяют сделать вывод, что эффективность Δ -слоя неразличимости необходимо оценивать не только по вероятности ошибки при фиксированной текущей мощности помехи z , но и по гарантированной вероятности ошибки $\hat{P}(\delta|\Delta)$, учитывающей ограничение источника помехи по средней мощности. Такой подход позволяет корректно сравнивать базовое правило приёма и приёмник с Δ -слоем в условиях некогерентного воздействия преднамеренной помехи.

Таким образом, вычислительный эксперимент подтверждает, что применение Δ -слоя неразличимости может обеспечивать повышение помехоустойчивости приёма фазоманипулированных сигналов при некогерентном воздействии преднамеренной помехи. Наиболее выраженный эффект наблюдается при отсутствии или умеренном уровне гауссовского шума. При увеличении шумовой составляющей выигрыш сокращается, что должно учитываться при выборе параметра Δ и оценке целесообразности применения такого решающего правила в реальных радиоканалах.

Заключение

В работе выполнен анализ эффективности работы Δ -слоя неразличимости при приеме фазоманипулированных сигналов в условиях некогерентности преднамеренных помех. Показано, что фазовое рассогласование изменяет эффективную мощность помехи, действующую на решающую статистику приемника, и поэтому должно учитываться при оценке целесообразности применения Δ -слоя.

Основной достигнутый эффект состоит в уточнении условий применения рандомизированного решающего правила. Установлено, что Δ -слой

наиболее полезен при малом и умеренном фазовом рассогласовании, когда помеха сохраняет заметную проекцию на решающее направление. При сильной некогерентности выигрыш уменьшается, поскольку сама помеха становится менее опасной для порогового решения.

В научной области теории помехоустойчивого приема полученные результаты позволяют связать выбор параметра Δ не только с мощностью помехи, но и с фазовыми условиями ее воздействия. Практическая достоверность

предложенных решений подтверждается расчетной процедурой, основанной на вычислении вероятности ошибки, усреднении по фазовому рассогласованию и сравнении гарантированной вероятности ошибки для случаев $\Delta = 0$ и $\Delta > 0$.

Дальнейшее развитие работы может быть связано с учетом нестационарного фазового рассогласования, многолучевого распространения, ошибок синхронизации и переходом от приема одиночных символов к оценке эффективности Δ -слоя при обработке кодовых блоков.

Литература

1. Чуднов А. М., Сазонов В. В., Бикбулатов В. Р. Оптимизация области неразличимости приемником двоичных сигналов, передаваемых по каналу с преднамеренной помехой // Проблемы передачи информации. – 2025. – Т. 61. – № 1. – С. 47–59.
2. Chudnov A. M., Sazonov V. V., Bikbulatov V. R. Optimization of the decisive rule for a receiver with a Δ -layer of indistinguishability of binary signals in a channel with intentional interference // Problems of Information Transmission. – 2025. – Vol. 61. – No. 1. – Pp. 41–55.
3. Чуднов А. М., Сапунова Л. П., Бикбулатов В. Р. Модель канала передачи данных с обратной связью в условиях воздействия преднамеренных помех с ограниченной средней мощностью // Известия ТулГУ. Технические науки. – 2025. – Вып. 2. – С. 243–249.
4. Чуднов А. М., Кирик Д. И., Ермакова Е. М. Оптимизация параметров кода и режима обработки сигналов в условиях преднамеренных помех // Труды учебных заведений связи. – 2019. – Т. 5. – № 4. – С. 79–86. – DOI: 10.31854/1813-324X-2019-5-4-79-86.
5. Чуднов А. М. Теоретико-игровые задачи синтеза алгоритмов формирования и приема сигналов // Проблемы передачи информации. – 1991. – Т. 27. – № 3. – С. 57–65.
6. Чуднов А. М. О минимаксных алгоритмах формирования и приема сигналов // Проблемы передачи информации. – 1986. – Т. 22. – № 4. – С. 49–54.
7. Жодзишский Ю. И. Максимальная гарантированная помехоустойчивость приема сигналов при ограничении средней мощности мешающих воздействий // Радиотехника. – 1986. – № 10. – С. 56–57.
8. Савищенко Н. В. Помехоустойчивость когерентного приема многопозиционных сигналов КАМ и ФМ при неидеальной синхронизации // Информационно-управляющие системы. – 2010. – № 1 (44). – С. 53–63.
9. Nguyen B. V., Nguyen M. T., Jung H., Kim K. Designing Anti-Jamming Receivers for NRDCSK Systems Utilizing ICA, WPD, and VMD Methods // IEEE Transactions on Circuits and Systems II: Express Briefs. – 2019. – Vol. 66. – No. 9. – Pp. 1522–1526. – DOI: 10.1109/TCSII.2019.2891254.
10. Chen Y., Yuan W., Xu T. Coding Split and Adjustment to Defend OFDM-IM Against Jamming Attacks // IEEE Communications Letters. – 2023. – Vol. 27. – No. 2. – Pp. 457–461. – DOI: 10.1109/LCOMM.2022.3224381.
11. Негурица А.О. Оценка эффективности использования Δ -слоя неразличимости двоичных сигналов, принимаемых в условиях случайных и преднамеренных помех // Телекоммуникации и связь. – 2025. – № 4 (07). – С. 22–27.

ANALYSIS OF THE EFFICIENCY OF THE Δ -LAYER OF INDISTINGUISHABILITY OF PHASE-SHIFT KEYED SIGNALS RECEIVED UNDER NONCOHERENT INTENTIONAL INTERFERENCE

Neguritsa A. O.²

Keywords: randomized reception rule, pseudorandom sequence, Kotelnikov receiver, guaranteed error probability, average interference power, computational experiment, radio channel.

Abstract

The purpose of the work: to evaluate the efficiency of applying a receiver with a Δ -layer of indistinguishability for the reception of phase-shift keyed signals under noncoherent deliberate interference. The case is considered in which the interference source does not provide strict phase alignment with the useful signal, and its effect after correlation processing is manifested through the projection of the interference onto the decision direction.

² Anastasia O. Neguritsa, adjunct of the Military Academy of Communications named after S. M. Budyonny. St. Petersburg, Russia. E-mail: LadyN98@yandex.ru

Results: a computational model for the reception of a phase-shift keyed signal using a Δ -layer of indistinguishability in the presence of phase mismatch between the useful signal and deliberate interference is proposed. It is shown that the no coherence of the interference smooths the dependence of the error probability on the current interference power and reduces the pronounced nature of the gain achieved by introducing the Δ -layer. At the same time, for small and moderate values of phase mismatch, the indistinguishability region retains practical significance, since it reduces the receiver sensitivity to the exact choice of interference power by the source. A comparison is performed between the basic reception rule at $\Delta = 0$ and the randomized rule at $\Delta > 0$. It is established that the efficiency of the Δ -layer should be evaluated not only by the error probability at a fixed interference power, but also by the guaranteed error probability under a constraint on the average power of the interference source.

Scientific novelty: the conditions for the expediency of applying a Δ -layer of indistinguishability for the reception of phase-shift keyed signals under noncoherent deliberate interference are refined. It is shown that phase mismatch should be taken into account when choosing the parameter Δ , since it changes the effective projection of the interference onto the receiver decision statistic.

References

1. Chudnov A. M., Sazonov V. V., Bikbulatov V. R. Optimizatsiya oblasti nerazlichimosti priemnikom dvoichnyh signalov, peredavaemyh po kanalu s prednamerennoy pomehoj // Problemy peredachi informatsii. – 2025. – V. 61. 2 No. 1. – Pp. 47–59.
2. Chudnov A. M., Sazonov V. V., Bikbulatov V. R. Optimization of the decisive rule for a receiver with a Δ -layer of indistinguishability of binary signals in a channel with intentional interference // Problems of Information Transmission. – 2025. – Vol. 61. – No. 1. – Pp. 41–55.
3. Chudnov A. M., Sapunova L. P., Bikbulatov V. R. Model' kanala peredachi dannyh s obratnoj svyaz'yu v usloviyah vozdeystviya prednamerennyh pomekh s ogranichennoj srednej moshchnost'yu // Izvestiya TulaGU. Tehnicheskie nauki. – 2025. – Vyp. 2. – Pp. 243–249.
4. Chudnov A. M., Kirik D. I., Ermakova E. M. Optimizatsiya parametrov koda i rezhima obrabotki signalov v usloviyah prednamerennyh pomekh // Trudy uchebnyh zavedenij svyazi. – 2019. – V. 5. – No. 4. – Pp. 79–86. – DOI: 10.31854/1813-324X-2019-5-4-79-86.
5. Chudnov A. M. Teoretiko-igrovye zadachi sinteza algoritmov formirovaniya i priema signalov // Problemy peredachi informatsii. – 1991. – V. 27. – No. 3. – Pp. 57–65.
6. Chudnov A. M. O minimaksnyh algoritmah formirovaniya i priema signalov // Problemy peredachi informatsii. – 1986. – V. 22. – No. 4. – Pp. 49–54.
7. Zhodzishskij Yu. I. Maksimal'naya garantirovannaya pomehoustojchivost' priema signalov pri ogranichenii srednej moshchnosti meshayushchih vozdeystvij // Radiotekhnika. – 1986. – No. 10. – Pp. 56–57.
8. Savishchenko N. V. Pomehoustojchivost' kogerentnogo priema mnogopozitsionnyh signalov KAM i FM pri neideal'noj sinhronizatsii // Informatsionno-upravlyayushchie sistemy. – 2010. – No. 1 (44). – Pp. 53–63.
9. Nguyen B. V., Nguyen M. T., Jung H., Kim K. Designing Anti-Jamming Receivers for NRDCSK Systems Utilizing ICA, WPD, and VMD Methods // IEEE Transactions on Circuits and Systems II: Express Briefs. – 2019. – Vol. 66. – No. 9. – Pp. 1522–1526. – DOI: 10.1109/TCSII.2019.2891254.
10. Chen Y., Yuan W., Xu T. Coding Split and Adjustment to Defend OFDM-IM Against Jamming Attacks // IEEE Communications Letters. – 2023. – Vol. 27. – No. 2. – Pp. 457–461. – DOI: 10.1109/LCOMM.2022.3224381.
11. Negurica A. O. Ocenka ehffektivnosti ispol'zovaniya Δ -slova nerazlichimosti dvoichnyh signalov, prinimaemyh v usloviyah sluchajnyh i prednamerennyh pomekh // Telekommunikatsii i svyaz'. – 2025. – No. 4 (07). – Pp. 22–27.



ПРЕДЛОЖЕНИЯ ПО ПОСТРОЕНИЮ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ УПРАВЛЕНИЯ СВЯЗЬЮ ТАКТИЧЕСКОГО ЗВЕНА УПРАВЛЕНИЯ

Иванов В. Г.¹, Сорокин А. Ю.², Лукьянчик В. Н.³

DOI:10.21681/3034-4050-2026-5-39-49

Ключевые слова: система связи, эффективность системы, управление связью, элементы системы связи, цифровые модели, модель Деминга.

Аннотация

Цель работы: выработка практических предложений по построению автоматизированной системы управления связью тактического звена управления на основе опыта организации связи и управления связью в боевых действиях.

Метод исследования: основу исследования составила общая теория систем, теории военного управления, теории менеджмента, теория военной связи, теория открытых систем с использованием методов системного анализа.

Результаты исследования: выработаны и обоснованы требования к автоматизированной системы управления связью тактического звена управления, на основе требований предъявляемых к системам управления военного назначения и системам военной связи. Предложена структура, состав и взаимосвязь основных элементов автоматизированной системы управления связью, обеспечивающих выполнения задач по управлению связью на различных циклах модели Деминга.

Представлены основные задачи, решаемые с помощью подсистем автоматизированной системы управления связью.

Научная новизна: заключается в разработке обоснованных продолжений по построению и организации функционирования автоматизированной системы управления связью тактического звена управления. Представлена практическая реализация выработанных предложений в демонстрационном макете программы.

Введение

Основная цель управления связью – эффективное использование потенциальных возможностей органов управления связью, системы и войск связи при выполнении поставленных им задач в операциях (боевых действиях) в установленные сроки [1, 2]. На уровне оперативно-технического управления целью является обеспечение контроля состояния и изменение структуры сетей связи и управление качеством связи, то есть выполнение заданных требований [1, 2]. Опыт организации связи в ходе специальной военной операции показывает, что элементы системы связи тактического звена управления (ТЗУ) постоянно находится под воздействием средств противника (огневым, физическом с применением беспилотных летательных аппаратов (БПЛА)), РЭБ и т.д). Следовательно, для обеспечения их функционирования необходимо обеспечить непрерывное, оперативное управление.

Управление системой связи должно обеспечивать: постоянную готовность системы связи к выполнению задач связи; своевременное и скрытое развертывание элементов системы связи, ее перестроение и наращивание в ходе боевых действий; гибкого маневра маршрутами доставки сообщений, линиями, каналами и средствами связи в соответствии со складывающейся обстановкой, оперативное восстановление связи, а также боеспособности воинских частей и подразделений связи [3].

Основная часть

Учитывая сложность структуры системы связи, разнотипность применяемых средств связи, высокую динамичность современных боевых действий и возможность выхода из строя личного состава и элементов системы, оперативно-техническое управление занимает значительную часть управленческой деятельности органов управления, особенно в ходе боевых

¹ **Иванов Василий Геннадьевич**, доктор военных наук, доцент, профессор кафедры информационных систем и технологий инженерного факультета Академии гражданской защиты Министерства Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий имени генерал-лейтенанта Д.И. Михайлика. Химки, Россия. E-mail: v.ivanov@agz.50.mchs.gov.ru

² **Сорокин Алексей Юрьевич**, кандидат технических наук, преподаватель кафедры информатики и вычислительной техники инженерного факультета Академии гражданской защиты Министерства Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий им. генерал-лейтенанта Д. И. Михайлика. Химки, Россия. E-mail: a.sorokin@amchs.ru

³ **Лукьянчик Валентин Николаевич**, кандидат военных наук, доцент, старший научный сотрудник научно-исследовательского центра Военной академии связи им. Маршала Советского Союза С. М. Буденного, г. Санкт-Петербург, Россия. E-mail: v-lukyanchik@bk.ru

действий. На уровне оперативно-технического управления осуществляется контроль состояния и изменение структуры сетей связи, управление качеством предоставления видов и услуг связи. Оперативное управление осуществляется, как правило, должностными лицами дежурных смен пунктов управления связью и составляет второй уровень управления после организационного.

Основными задачами управления связью ТЗУ являются [1, 2]:

- непрерывное добывание, сбор, обработка, изучение, обобщение и анализ данных по связи;
- оценка и отображение данных обстановки и состояния связи;
- определение и доведение задач связи до подчиненных;
- планирование системы связи;
- организация и проведение мероприятий по всестороннему обеспечению применения подразделений связи и средств связи;
- руководство подготовкой подчиненных органов управления связью и подразделений связи к применению;
- организация, осуществление контроля и оказание помощи подчиненным органам управления связью и войскам связи;
- непосредственное оперативное управление системой связи и действиями подразделений связи и их личным составом при выполнении ими поставленных задач;
- управление информационным обменом в системе связи и качеством предоставляемых видов (услуг) связи;
- управление восстановлением системы связи, ее элементов и боеспособности подразделений связи.

Требования к системе управления связью предъявляются такие же, как и системе связи: по боевой готовности устойчивости, мобильности, пропускной способности, разведзащищенности, управляемости, доступности [2, 4].

Выполнение приведенных требований осуществляется комплексом мероприятий организационного и технического характера способствующих их поддержанию в заданных пределах.

Основными требованиями к принятию решения и планированию связи на операцию (бой) являются: обоснованность (адекватность), своевременность (оперативность) и скрытность, в совокупности определяющие качество планирования связи.

Обоснованность (адекватность) – соответствие принимаемых решений и документов планирования сложившейся обстановке, потребностям управления и допустимым затратам сил,

средств и времени на их разработку и реализацию.

Своевременность (оперативность) принимаемых решений и планирования связи определяется допустимой продолжительностью их выполнения, определяемой оперативными условиями сложившейся обстановки.

Скрытность принимаемых решений и планирования связи диктуется необходимостью исключения возможности получения противником данных о структуре системы и группировке войск связи, содержании разрабатываемых документов по связи и компрометации принимаемых решений.

Наряду с названными требованиями при принятии решения и планировании связи должны учитываться **реальная осуществимость и эффективность** (техническая, экономическая, организационная выполнимость в установленные сроки и требуем качеством) принимаемых решений и разрабатываемых планов; **четкость и непротиворечивость формулировок** (логичность всех предусмотренных решением действий при выполнении задачи, отсутствие противоречивых установок и взаимоисключающих требований); **адаптивность** (качество решения, позволяющее подчиненным делать необходимый маневр, корректировать свои действия в соответствии с изменившимися обстоятельствами) [1, 4].

Кроме того к решению предъявляются требования по соответствию его формы содержанию, учету возможных отрицательных последствий, возможности контроля выполнения решения и др.

Для выполнения этих требований принятие решения на организацию связи и планирование связи должны осуществляться на основе четкого уяснения задачи, объективной и всесторонней оценки обстановки, проведения необходимых расчетов, учета количественных и качественных показателей применяемых сил и средств, влияющих факторов на создаваемую систему связи и конкретных исходных данных. Выполнение указанных задач и требований может быть достигнуто, прежде всего, при условии четкой организации работы каждого органа управления связью.

Главным должностным лицом в соединении ответственным за организацию связи является начальник связи соединения. Как показал опыт организации связи в СВО начальнику связи необходимо решать значительно больше задач чем предписано руководствами, наставлениями и инструкциями. Например при развёртывании системы связи на территории РФ или в глубоком тылу, где существуют константные условия

обстановки, основная задача начальника связи дивизии (полка, батальона), в техническом плане сводится к текущей эксплуатации его инфраструктуры связи.

При развертывании системы связи для обеспечения связи с воюющими подразделениями задачи значительно расширяются, где вопросы организации связи между подразделениями и их должностными лицами превращаются в чрезвычайно сложные задачи, которые обусловлены изменяющимися условиями ведения боевых действий.

Концептуальная разница выявляется при рассмотрении процесса управления связью в ТЗУ через модель Деминга (PDCA) [5,6]. Модель рассматривает процесс управления как циклически повторяющиеся этапы планирования, реализации, контроля и анализа, результаты которого являются основой для планирования на следующей итерации. Ключевым моментом модели является время одной итерации цикла управления, и именно это время является существенным отличием в задачах начальника связи (НС) в зависимости от ситуационных обстоятельств в данный период времени.

Итерация цикла управления связью длится ровно столько, сколько актуально выработанное решение в начале итерации. Другими словами, исходя из текущих условий ведения боевых действий, наличия сил и средств, НС оперативно изменяет состояние системы связи. При этом критериями определяющие ее состояние могут быть разные (например: обеспечение максимальной доступности услуг связи и с минимальным

использованием средств связи; обеспечение максимальной развед- и помехозащищенности без экономии средств связи и т.д.). При изменении условий начального планирования или при выявлении ошибок в реализованном решении цикл переходит на следующую итерацию. Таким образом, если подразделения на передовой находится в обороне, то условия будут в большей части зависеть от действий противника. Если же подразделение на передовой находится в наступлении и движется вперед, то условия будут изменяться по мере продвижения своих войск и будут также зависеть от действий противника.

Опираясь на вышеприведенное, можно сказать, что НС в тылу будет заниматься текущей эксплуатацией элементов системы связи, а НС на передовой помимо текущей эксплуатации будет заниматься еще и адаптацией систем связи под изменяющиеся условия. С научной точки зрения, автоматизация процессов текущей эксплуатации действующих систем связи в константных условиях не представляет сложную задачу, более того, уже разработаны и успешно применяются системы управления средствами связи. Но вместе с этим автоматизация процессов адаптации действующих элементов системы связи под изменяющиеся условия боевых действий на сегодняшний день представляет проблему.

Разрабатываемые в настоящее время специальные программные средства (СПО) «домашним» способом, такие как «Волна», «Гроза», «RadioPlanner» (рис. 1) и т.д., заявляются раз-

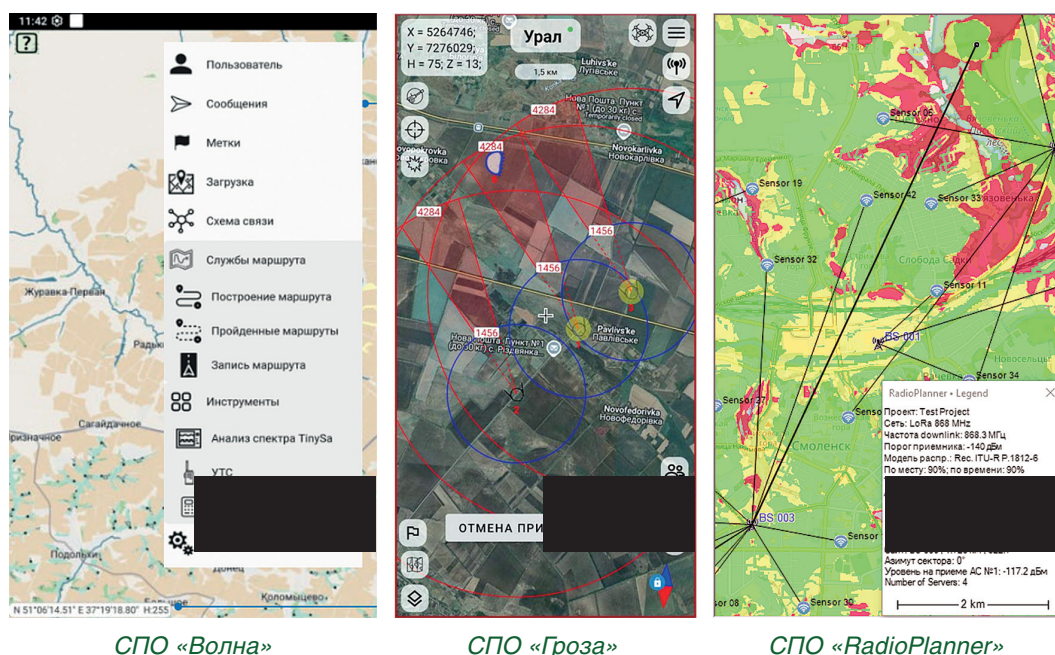


Рис. 1. Специальные программные средства применяемые в ходе планирования связи

решения начальниками связи подразделений ТЗУ, но в сущности представляют собой простые автоматизированные средства для решения информационных и расчетных задач (например, определение условий прямой видимости, построение профиля радиоинтервала и зоны покрытия, формирование документов и т.д.).

Этот функционал в рамках цикла управления является подспорьем для этапа планирования, при этом остальные этапы управления упускаются, что в значительной степени сужает область их применения.

Адаптация системы связи под изменяющиеся условия – это процесс выработки и реализации новых решений по реорганизации системы связи в подразделении или режимах ее работы. Такой процесс требует оперативного сбора разнообразной информации и ее последующего глубокого анализа. На сегодняшний день адаптация систем связи под изменяющиеся условия имеет догоняющий характер, поскольку отсутствуют необходимые организационно-технические условия для обеспечения данного процесса.

Для того, чтобы адаптация системы связи приобрела опережающий характер, необходимо, чтобы скорость определения тенденций изменения условий ведения боевых действий опережала их фактическое изменение. Другими словами, речь идет о прогнозировании условий в будущие моменты времени и об оценке адекватности этим условиям текущего решения по организации системы связи.

В данном тезисе сокрыта еще одна проблема. Возможности по адаптации в рамках воюющего подразделения, прежде всего, ограничены номенклатурой имеющихся средств связи и их ТТХ. Разработка перспективных средств связи также должна осуществляться с учетом прогнозирования будущих условий, что, к сожалению, пока также имеет догоняющий характер. Это обусловлено скоростью и достоверностью информации о состоянии связи в низовых подразделениях, которая уходит на высшие уровни управления войсками. Это важно, потому что информация от высших органов управления ложится в основу технических заданий на перспективную разработку средств связи, несвоевременный учет каких-либо условий порождает в последствии неэффективное производство.

Таким образом, практика управления связью в условиях интенсивного воздействия противника требует технологии прогнозирования условий ведения боевых действий, оценки адекватности текущих решений предполагаемым условиям, оперативного и достоверного доведения информации о состоянии элементов системы связи.

Одним из путей создания управляющих систем является разработка интеллектуальной автоматизированной системы управления связью (ИАСУС) [1, 2, 3].

Структура системы связи, состав ее сети связи в соединении, уже сегодня характеризуется наличием магистральных узлов связи, узлов доступа, узлов связи пунктов управления и ретрансляционных пунктов на которых установлено различное оборудование связи. На таких объектах располагаются ретрансляторы радиосетей, оборудование беспроводного широкополосного доступа (БШПД), которые являются основным средством создания высокоскоростных каналов связи, средства оптико-электронной связи, каналы данных средств выделяются в отдельные логические каналы под соответствующие услуги связи.

Следовательно, НС соединения (полка, батальона) необходимо решать следующие задачи:

Первая задача – это планирование системы связи и сетей связи. Исходными данными для такой задачи являются:

- 1) перечень абонентов, с которыми необходимо обеспечить связь;
- 2) требования к построению сетей на различных средствах связи;
- 3) требования к пропускной способности каналов для планируемых сетей;
- 4) номенклатура и тактико-технические характеристики (ТТХ) средств связи, имеющихся в подразделении;
- 5) места дислокации абонентов, которых необходимо связать;
- 6) данные о физико-географических условиях в районе развертывания элементов системы связи и сетей связи;
- 7) данные об инфраструктуре в районе;
- 8) данные о сети электроснабжения в районе развертывания элементов системы связи и сетей связи;
- 9) данные о наземных объектах которые могут быть использованы при организации связи;
- 10) данные о маршрутах перемещения подразделений в районе развертывания элементов системы связи и сетей связи;
- 11) предполагаемые режимы установления связи в различных сетях;
- 12) сведения об частотной и электромагнитной обстановке в районе развертывания элементов системы связи и сетей связи;
- 13) сведения о применяемых средствах РЭБ в районе развертывания;
- 14) сведения характере огневого воздействия противника.

Данные сведения – это база, которая позволяет сформировать качественное решение по построению системы связи и сетей связи ТЗУ. Однако в настоящее время начальники связи планирующие развертывание в новом районе, полнотой этих сведений не обладают. В результате пока боевые подразделения соединения разворачиваются и занимают позиции согласно боевому распоряжению, начальник связи делает временную радиосеть для оперативной связи и при этом приступает к сбору необходимой информации. Сведения о местности собираются путем осмотра занимаемого района, также в рамках объездов формируется представление об уровне электрификации и точках возможного подключения, выбираются опорные объекты. Данные об электромагнитной обстановке могут быть также получены в ходе объездов путем замеров. В свою очередь, полнота сведений о частотах и характере огневого воздействия противника формируется внутри соединения, полка, батальона исходя из его действий. Вполне естественно, что при таком объеме мероприятий эффективная система связи и сети связи разворачиваются небыстро, и с различными организационно-техническими ошибками. И как правило критерии формирования системы связи сводятся к обеспечению трех составляющих: доступность связи для абонентов, защищенность каналов связи от разведки противника и возможность осуществления текущей эксплуатации элементов системы связи (узлов связи, ретрансляторов и средств связи) в местах развертывания.

С точки зрения военной и технической науки формирование решения по построению системы связи и сетей связи – это сложная многокритериальная оптимизационная задача, качественное и быстрое решение которой является невозможным без применения средств вычислительной техники. Таким образом, задача планирования системы связи может и должна быть автоматизирована. Прежде всего, автоматизировать возможно следующее:

- формирование цифровой модели района развертывания системы связи и передачи данных, которая включала бы в себя исчерпывающие данные о местности, объектах инфраструктуры и электрификации;
 - выбор опорных объектов инфраструктуры для формирования на их базе элементов системы связи (магистральных и зональных узлов связи, ретрансляционных пунктов, ложных элементов системы связи и т.д.);
 - постановку и решение задачи обоснования проекта системы связи с учетом имеющихся сведений;
 - моделирование функционирования системы связи и сетей связи с учетом известных условий ведения боевых действий.
- Вторая задача** – это контроль текущего состояния системы связи и ее элементов. Исходными данными для такой задачи будут:
- 1) номенклатура и количество функционирующих средств связи в составе сетей связи;
 - 2) частота и причины отказов по каждому устройству в составе сетей связи;
 - 3) показатели качества связи на абонентских устройствах;
 - 4) конфигурации по каждому устройству.
- Данные сведения позволяют дать оценку работоспособности оборудования и корректности его работы в составе сети. Своевременное выявление и устранение неполадок – залог качественной связи. На текущий момент данные сведения формируются ручным способом. Технические средства учитываются в таблицах Excel или в журналах, отдельно учитываются их конфигурации. Контроль функционирования устройств осуществляется дежурными телефонистами на пунктах управления. Они, в лучшем случае, фиксируют в журнале возникающие неполадки и передают эти сведения на пункты управления связью для дальнейшего разбора. Фактически информация существует в бумажном виде и глубокому анализу не подвергается.
- Применительно к данной задаче автоматизации подлежат:
- для сетевых устройств может быть реализован автоматический контроль и регистрация параметров состояния в цифровом журнале;
 - для радиостанций и ретрансляторов может быть реализован автоматизированный контроль и регистрация параметров состояния в цифровом журнале, осуществляемый дежурным телефонистом;
 - учет причин отказа по каждому оборудованию, осуществляемый дежурным по пункту управления связью с фиксацией времени на устранение неисправности;
 - анализ и формирование сводного отчета по состоянию системы связи и передачи данных с детализацией до отдельных устройств.
- Третья задача** – это организация обслуживания и проведения аварийно-восстановительных работ при отказах в системе связи и передачи данных. По сути, это подзадача контроля, но в рамках условий ведения боевых действий выделяется в отдельную задачу. Исходными данными для такой задачи будут:

- 1) номенклатура и количество средств связи, находящихся в резерве у подразделений связи и боевых подразделений;
- 2) состояние сил и средств дежурной смены пункта управления связью (дежурный и аварийный расчет);
- 3) уровни опасности на маршрутах перемещения (наличие БПЛА противника в небе, воздействие артиллерии и т.д.);
- 4) показатели состояния элементов системы связи и средств связи при отказах;
- 5) состояние промышленной электросети в местах развертывания элементов системы связи и средств связи.

Приводимая номенклатура сведений позволяет своевременно выявить неполадки средств связи, дать оценку ее причинам и принять решение о порядке дальнейших действий. Своевременное выявление и принятие правильных решений сокращают время устранения неисправности и сохраняет жизни аварийного расчета дежурной смены. На текущий момент большой сложностью является диагностика возникающих неполадок. Очень многое решает уровень компетентности дежурной смены телефонистов и дежурного на пункте управления связью. Прежде, чем дать команду аварийному расчету куда-либо выдвигаться, необходимо как можно точнее установить причину неполадки и место, где она возникла, а также необходимо удостовериться, что движение аварийного расчета к указанной точке является возможным. Последнее достигается через запрос информации с соответствующих пунктов, что тоже занимает время.

Применительно к данной задаче автоматизации подлежат:

- для сетевых устройств – автоматическая диагностика неполадки;
- для радиостанций и ретрансляторов – автоматизированная диагностика по скриптам;
- для магистральных узлов и узлов доступа – автоматический контроль электропитания и переключения на автономные источники питания за счет интеграции программируемых ip-контроллеров;
- сбор информации о действиях противника и пролетах БПЛА с пунктов управления с учетом этих данных и отображением на пункте управления связью;
- автоматизированный сбор сведений о погоде (температура, туман, осадки);
- автоматизированный сбор и анализ частотной обстановки.

Четвертая задача – анализ динамики условий в районе и оценка эффективности функционирования текущей системы связи и сетей связи. Исходными данными для такой задачи будут:

- 1) информация об огневом воздействии противника;
- 2) данные радиомониторинга в районе функционирования системы связи;
- 3) предполагаемые изменения в боевых порядках своих войск;
- 4) сведения о функционировании действующих элементов системы связи, частота отказов оборудования по каждой номенклатуре и время устранения этих отказов;
- 5) уточненная цифровая модель местности, включая уточненные данные по состоянию лесополос и отдельных сооружений;
- 6) данные о применении средств РЭБ своими войсками.

Данные сведения позволяют дать оценку реализованным организационно-техническим решениям и техническим средствам, а также определить динамику изменения условий ведения боевых действий. Результаты такого анализа позволяют выработать управленческие решения которые повышают устойчивость системы связи и сетей связи к факторам обусловленных ведением боевых действий. К сожалению, в настоящее время данная задача в подразделениях даже не рассматривается. Обусловлено это тем, что, с одной стороны, не накапливаются в необходимом виде исходные данные для постановки такой задачи, а, с другой стороны, должностные лица не владеют необходимыми математическими методами анализа такой информации. В результате задача совершенствования текущего организационно-технического состояния элементов системы связи возникает только тогда, когда элементы перестают функционировать надлежащим образом.

Применительно к данной задаче автоматизации подлежат:

- уточнение цифровой модели района функционирования элементов системы связи и сетей связи в части отражения в ней изменений и новых сведений, являющихся значимыми для планирования;
- радиомониторинг за счет применения штатных средств и ip анализаторов спектра;
- прогнозирование динамики условий ведения боевых действий, на основе собранных данных за предыдущий период;
- формирования цифровой модели текущей системы связи;

Таблица 1.

Подсистемы автоматизированной системы управления связью

№ п/п	Наименование подсистемы	Функциональная задача подсистемы
1	Подсистема создания цифровой модели местности	Подсистема предназначена для сбора информации о местности и ее преобразования в редактируемую ГИС БД
2	Подсистема актуализации цифровой модели местности	Подсистема предназначена для актуализации информации по объектам инфраструктуры цифровой модели, а также внесения в нее дополнительной информации о местности
3	Подсистема учета средств связи	Предназначена для ведения баланса технических средств связи, отражения их реального состояния, а также отражения их ТТХ для использования в системе
4	Подсистема планирования системы связи	Предназначена для создания проекта сети связи с опорой на имеющиеся исходные данные
5	Подсистема контроля состояния инфраструктуры связи и передачи данных	Предназначена для автоматического контроля исправности сетевых устройств и автоматизированного контроля несетевых средств связи, а также автоматизированного учета аварийно-восстановительных мероприятий
6	Подсистема контроля электропитания на	Предназначена для автоматического или автоматизированного контроля состояния электропитания на элементах системы связи и управления им (переключение с действующей электросети на автономные источники)
7	Подсистема мониторинга электромагнитной и метеорологической обстановки	Предназначена для автоматического сбора, накопления и отображения данных об электромагнитной и метеорологической обстановке на элементах системы связи
8	Подсистема диагностики отказов средств связи	Предназначена для автоматизированного определения причин отказов средств связи
9	Подсистема учета огневых воздействий противника	Предназначена для автоматизированного учета мест и средств огневого воздействия со стороны противника
10	Подсистема формирования цифрового двойника системы связи	Предназначена для создания цифровой модели действующей системы связи
11	Подсистема прогнозирования условий ведения боевых действий относительно управления связью	Предназначена для аккумуляирования сведений о динамике изменений электромагнитной и метеорологической обстановки, применении РЭБ, перебоях электроснабжения и об огневых воздействиях противника с последующим построением прогностических моделей во времени и формирования будущего облика условий ведения боевых действий
12	Подсистема моделирования состояния системы связи	Предназначена для прогнозирования функциональных показателей работы текущей системы связи в прогнозируемых условиях ведения боевых действий или задаваемых условий, задаваемых в ручном режиме
13	Подсистема классификации типовых технических решений, их учета и оценки их эффективности	Предназначена для автоматического сбора и хранения информации о тактике и эффективности применяемых средств связи на фоне условий их эксплуатации

- моделирование функционирования системы связи в прогнозируемых условиях ведения боевых действий.

Описание четвертой задачи замыкает цикл Деминга [5, 6] на уровне подразделения, однако собираемые и обрабатываемые данные представляют большую ценность и для других подразделений, а также и для органов управления связью объединения. Подобная информация, с одной стороны, содержит сведения о реализуемых технических решениях и показателях функционирования в конкретных условиях; с другой стороны, она содержит сведения об эффективности применения конкретных технических средств и о подлинном их состоянии связи в подразделении. Масштабирование таких средств автоматизации по подразделения и подключение их к общей базе данных, куда будет отправляться вся информация, позволяет получить уникальный функциональный эффект. Начальники связи подразделений ТЗУ получают доступ к опыту друг друга в практике обеспечения связью, что позволит, с одной стороны, не делать уже совершенные ошибки, а, с другой стороны, масштабировать наиболее эффективные решения. В свою очередь, органы управления связью объединения получат возможность оперативной и достоверной оценки текущего состояния связи в ТЗУ, что также положительно скажется на своевременности и качестве принимаемых решений.

Рассмотрим предлагаемую архитектуру автоматизированной системы управления связью и входящие в ее состав подсистемы.

В настоящее время на пунктах управления размещается различное серверное оборудование соединённое между собой высокоскоростными каналами связи. Следовательно, целесообразно проектировать автоматизированную систему управления связью на базе веб-сервера устанавливаемого на соответствующее серверное оборудование, который будет функционировать в изолированной локальной сети соединения (полка) [7]. Соответственно, клиентская часть системы будет реализована в веб-браузере. В рамках такого подхода все требовательные к вычислительным мощностям процедуры можно реализовать на серверной части.

Предлагаемый состав подсистем АСУС представлен в таблице 1.

С учетом предлагаемых подсистем сформирована схема функционирования АСУС (рис. 2).

С учетом организации работы должностных лиц в процессе управления связью и схемы функционирования подсистем АСУС, приведенную на рисунке 1, сформирована взаимодействия автоматизированной системы управления связью ТЗУ (рис. 3).

Из схемы, представленной на рисунке 3, видно, что АСУС имеет архитектуру клиент-серверной системы с удаленным хранением отдельной категории данных. На схеме условными обозначениями «Л1»–«Л3» характеризуются линии обмена данными в АСУС.

Л1 – линия автоматического управления, которая представляет собой отдельный канал обмена данными функционального состояния сетевых устройств, устройств управления

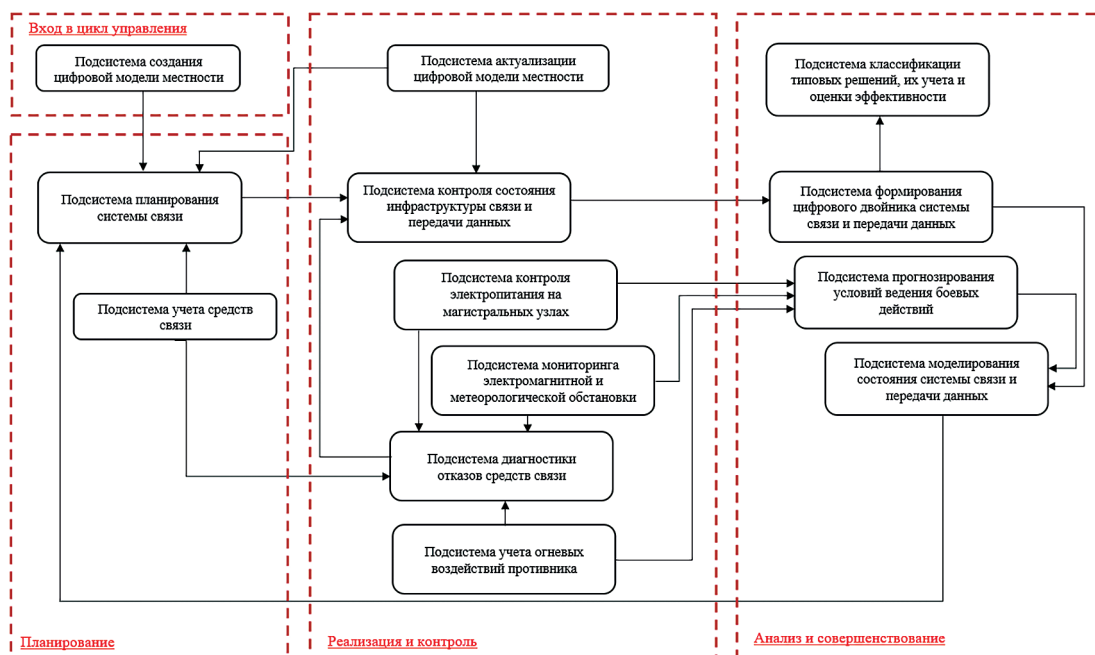


Рис. 2. Схема функционирования подсистем в АСУС

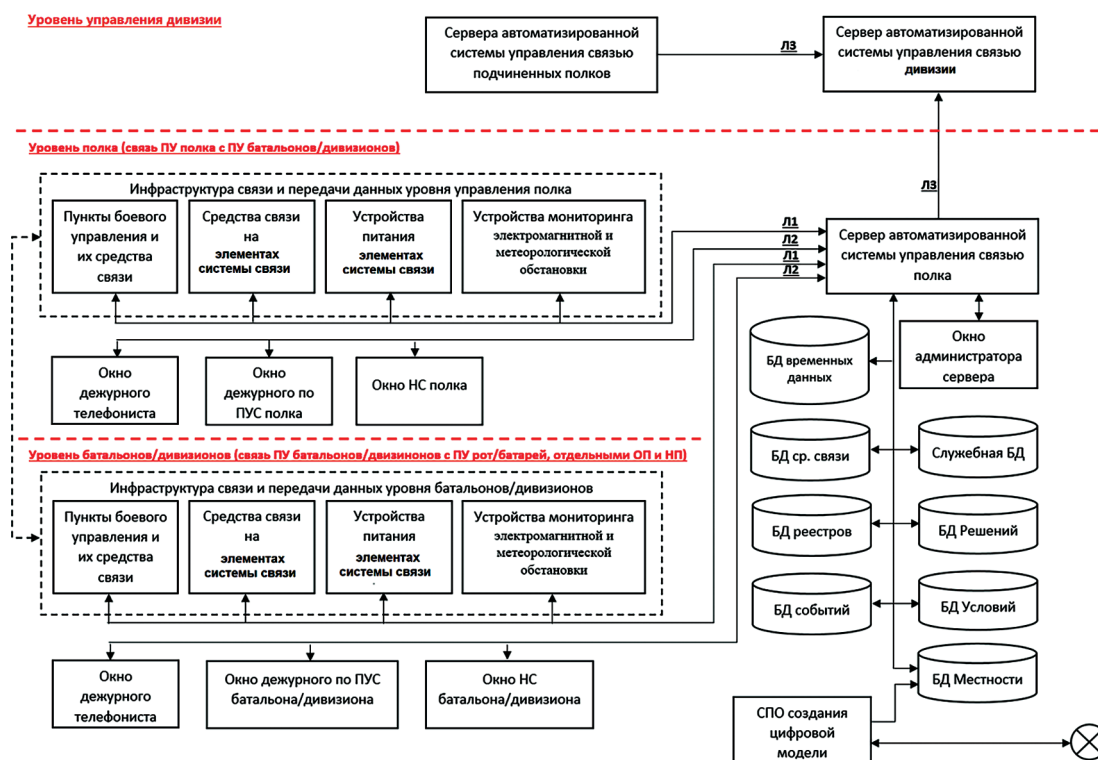


Рис. 3. Структурная организации взаимодействия АСУС ТЗУ

электропитанием и средств мониторинга метеорологической и электромагнитной обстановки;

Л2 – линия автоматизированного управления, которая представляет собой отдельный канал обмена данными между операторскими клиентами и сервером. Для каждого типа должностного лица, исходя из его функции, предусматривается отдельное окно с соответствующим функциональным наполнением;

ЛЗ – линия передачи данных на сервер вышестоящего уровня. Предполагается, что по данной линии будет реализован поток данных по реализуемым решениям организации системы связи и передачи данных, а также условиям, в которых она функционирует.

Стоит отметить, что такой подход позволяет масштабировать систему на различных уровнях управления. Достижимый положительный

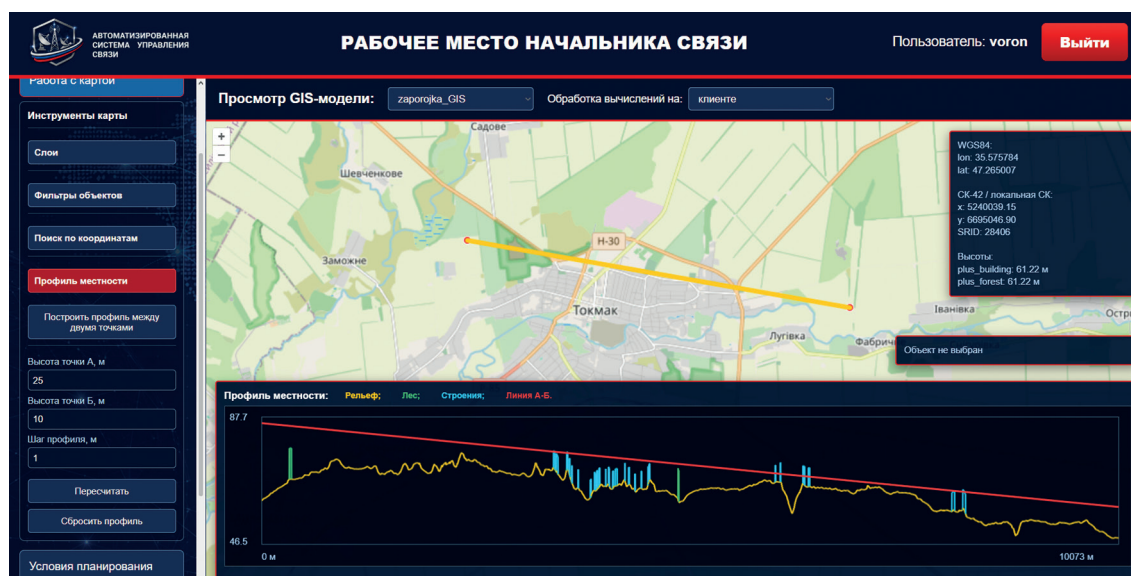


Рис. 4. Построение профиля местности в АСУС ТЗУ

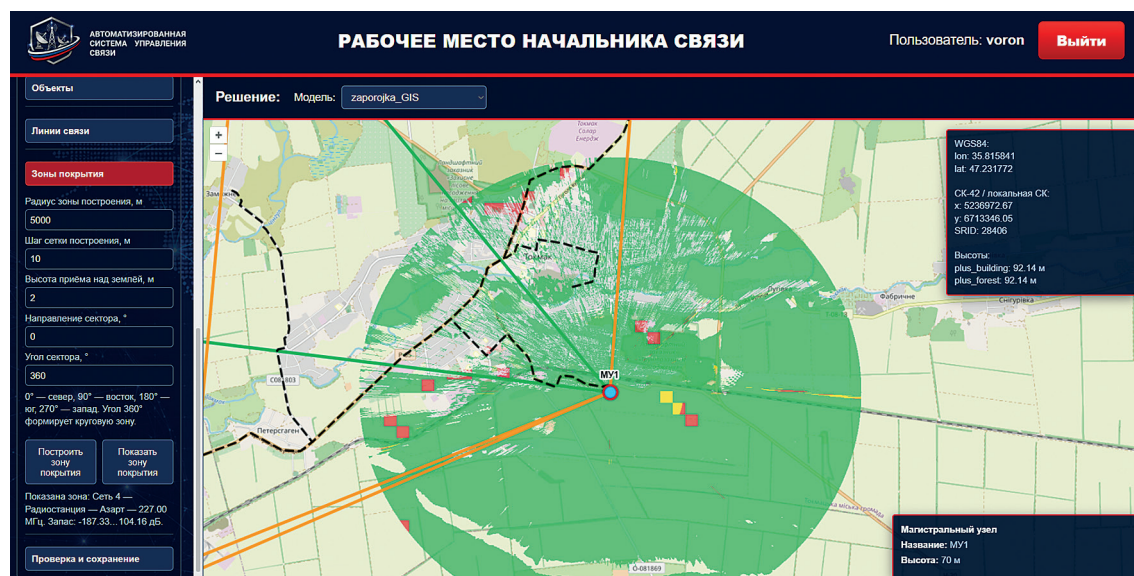


Рис. 5. Редактор определения зоны покрытия и оценки по показателю SINR (сигнал/помеха + шум)

эффект такого масштабирования – детальная осведомленность вышестоящих должностных лиц о состоянии связи в подчиненных подразделениях.

На основе разработанных предложений подготовлен действующий макет АСУС (рис. 4–5) и осуществляется подготовка первой версии АСУС ТЗУ для ее дальнейшей апробации в соединениях группировок войск.

В рамках планирования связи предусмотрены следующие типы сетей: проводная телефонная, радиосеть и ЛВС. Реализован автоматический расчет проекта решений для режима работы Р-187П1 (МПР) и для БШПД.

Серверная часть АСУС реализована под Астролинукс 1.7 с подсистемой администрирования и актуализации цифровой модели местности.

Заключение

Создание эффективной автоматизированной системы управления связью обеспечит решение задач по управлению связью с учетом постоянно развивающихся технологий связи, сетей связи различных родов связи. При этом для ускорения процесса принятия решений и повышения их точности в АСУС необходимо использовать модули работа которых основана на технологиях искусственного интеллекта [8, 9]. Применение данных модулей обеспечит повышении скорости проведения вычислений и качество принимаемых решений, что особенно важно для управления в условиях неопределенности под воздействием внутренних условий и внешних факторов.

Литература

1. Иванов В. Г. Основы построения и оценки эффективности функционирования системы связи специального назначения в международном вооруженном конфликте на основе многосферной и конвергентной структуры ее элементов: монография. – СПб.: ПОЛИТЕХ. – 2023. – 298 с.
2. Иванов В. Г. Теория и практика построения и обеспечения функционирования системы связи специального назначения с учётом технологического развития и опытов вооруженных конфликтов: монография – М.: Красная Звезда. – 2025. – 304 с.
3. Иванов В. Г., Корякин Д. Д., Панихидников С. А. Автоматизированные системы управления связью. Труды учебных заведений связи. – 2016. – Т. 2. – № 4. – С. 56–62.
4. Иванов В. Г., Корякин Д. Д. Особенности функционирования современных автоматизированных систем мониторинга телекоммуникационных сетей // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2017): сборник научных статей VI международной научно-технической и научно-методической конференции (в 4 томах) / под ред. С. В. Бачевского. – 2017. – С. 353–356.
5. Кунаков Е. П. Применение новых подходов к циклу деминга // Вестник Магнитогорского государственного технического университета им. Г. И. Носова. – 2022. – № 1 (1). С. 61–70.
6. Деминг Э. Выход из кризиса: Новая парадигма управления людьми, системами и процессами. – М.: Альпина Паблишер. – 2012. – 419 с.
7. Яковлев Ю. А. Внедрение информационных технологий для повышения эффективности связи / Ю. А. Яковлев, П. В. Трепалин, С. А. Константинов // Вестник информационных технологий. Россия и Африка. – 2026. – № 4. – EDN NEXCLA.

8. Кокошин А. А. Перспективы развития военной техносферы – будущее войн и боевого применения военной силы // Вестник Академии военных наук. – 2019. – № 2. – С. 26–29.
9. Малыгин И. Г., Тарабаев А. А., Аванесов М. Ю. Интеграция искусственного интеллекта в коммуникационные сети и услуги // Информация и космос. – 2019. – № 4. – С. 6–11.

PROPOSALS FOR THE CONSTRUCTION OF AN AUTOMATED COMMUNICATION CONTROL SYSTEM FOR THE TACTICAL CONTROL LEVEL

Ivanov V. G.⁴, Sorokin A. Yu.⁵, Lukyanchik V. N.⁶

Keywords: communication system, system efficiency, communication management, elements of the communication system, digital models, Deming model.

Abstract.

The purpose of the work is to develop practical proposals for the construction of an automated communication control system of the tactical control level based on the experience of organizing communications and managing communications in combat operations.

Research method: the basis of the research is the general theory of systems, the theory of military management, the theory of management, the theory of military communications, the theory of open systems using the methods of system analysis.

Results of the study: the requirements for the automated communication control system of tactical control are developed and substantiated, based on the requirements for military control systems and military communication systems. The structure, composition and interconnection of the main elements of the automated communication control system that ensure the performance of communication control tasks on various cycles of the Deming model are proposed.

The main tasks solved with the help of subsystems of the automated communication control system are presented.

The scientific novelty consists in the development of substantiated continuations for the construction and organization of the functioning of the automated communication control system of the tactical control link. The practical implementation of the developed proposals in the demonstration model of the program is presented.

References

1. Ivanov V. G. Osnovy postroeniya i ocenki ehffektivnosti funkcionirovaniya sistemy svyazi special'nogo naznacheniya v mezhdunarodnom vooruzhennom konflikte na osnove mnogosfernoj i konvergentnoj struktury ee ehlementov: monografiya. – SPb.: POLITEH. – 2023. – 298 p.
2. Ivanov V. G. Teoriya i praktika postroeniya i obespecheniya funkcionirovaniya sistemy svyazi special'nogo naznacheniya s uchyotom tehnologicheskogo razvitiya i opytov vooruzhennykh konfliktov: monografiya – M.: Krasnaya Zvezda. – 2025. – 304 p.
3. Ivanov V. G., Koryakin D. D., Panihidnikov S. A. Avtomatizirovannye sistemy upravleniya svyaz'yu Trudy uchebnykh zavedenij svyazi. – 2016. – V. 2. – No. 4. – Pp. 56–62.
4. Ivanov V. G., Koryakin D. D. Osobennosti funkcionirovaniya sovremennykh avtomatizirovannykh sistem monitoringa telekommunikacionnykh setej // Aktual'nye problemy infotelekkommunikacij v nauke i obrazovanii (APINO 2017)»: sbornik nauchnykh statej VI mezhdunarodnoj nauchno-tehnicheskoy i nauchno-metodicheskoy konferencii (v 4 tomah) / pod red. S. V. Bachevskogo. – 2017. – Pp. 353–356.
5. Kunakov E. P. Primenenie novykh podhodov k ciklu deminga // Vestnik Magnitogorskogo gosudarstvennogo tehnikeskogo universiteta im. G. I. Nosova. – 2022. – No. 1 (1). – Pp. 61–70.
6. Deming Eh. Vyhod iz krizisa: Novaya paradigma upravleniya lyud'mi, sistemami i processami. – M.: Al'pina Publisher. – 2012. – 419 p.
7. Yakovlev Yu. A. Vnedrenie informacionnykh tehnologij dlya povysheniya ehffektivnosti svyazi / Yu. A. Yakovlev, P. V. Trepalin, S. A. Konstantinov // Vestnik informacionnykh tehnologij. Rossiya i Afrika. – 2026. – No. 4. – EDN NEXCLA.
8. Kokoshin A. A. Perspektivy razvitiya voennoj tehnosfery – budushchee vojn i boevogo primeneniya voennoj sily // Vestnik Akademii voennykh nauk. – 2019. – No. 2. – Pp. 26–29.
9. Malygin I. G., Tarabaev A. A., Avanesov M. Yu. Integraciya iskusstvennogo intellekta v kommunikacionnye seti i uslugi // Informaciya i kosmos. – 2019. – No. 4. – Pp. 6–11.

⁴ **Vasily G. Ivanov**, Dr.Sc. of Military Sciences, Associate Professor, Professor of the Department of Information Systems and Technologies of the Faculty of Engineering of the Academy of Civil Protection of the Ministry of the Russian Federation for Civil Defense, Emergencies and Elimination of Consequences of Natural Disasters named after Lieutenant General D. I. Mikhailik. Khimki, Russia. E-mail: v.ivanov@agz.50.mchs.gov.ru

⁵ **Alexey Yu. Sorokin**, Ph.D. of Technical Sciences, Lecturer of the Department of Informatics and Computer Engineering, Faculty of Engineering, Academy of Civil Protection of the Ministry of the Russian Federation for Civil Defense, Emergencies and Elimination of Consequences of Natural Disasters named after Lieutenant General D. I. Mikhailik. Khimki, Russia. E-mail: a.sorokin@amchs.ru

⁶ **Valentin N. Lukyanchik**, Ph.D. of Military Sciences, Associate Professor, Senior Researcher of the Research Center of the Military Academy of Communications named after Marshal of the Soviet Union S. M. Budyonny. St. Petersburg, Russia. E-mail: v-lukyanchik@bk.ru

ЦИФРОВАЯ ТРАНСФОРМАЦИЯ – НОВЫЕ ТЕХНОЛОГИИ ДЛЯ СЕТЕЙ СВЯЗИ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ. Часть I

Лукашев А. В.¹

DOI:10.21681/3034-4050-2026-5-50-58

Ключевые слова: опыт специальной военной операции, операционное пространство, архитектура телекоммуникационной сети, динамичная сетевая маршрутизация, бесшовный информационный обмен, гибридная архитектура вычислений, программно-определяемая сеть, маршрутизация по меткам, межсетевая интеграция сетей связи.

Аннотация

Цель работы: работа посвящена актуальной теме цифровой трансформации системы связи – научному обоснованию необходимости внедрения новых технологий построения сетей связи специального назначения, обеспечивающих устойчивый и безопасный информационный обмен в сложных условиях современных операций на основе приобретенного опыта боевого применения системы связи в специальной военной операции.

Метод исследований: анализ мирового опыта развития сетей связи, его теоретическое обобщение с целью выявления закономерностей развития сетевых технологий с целью научного обоснования способов цифровой трансформации отечественных сетей связи путем внедрения современных виртуальных и программно-определяемых сетевых технологий с встроенными механизмами безопасности и искусственного интеллекта.

Результаты исследований: предложен новый подход к цифровой трансформации сетей связи специального назначения с учетом опыта мирового, в первую очередь, США и Китая, на основе научно обоснованного ее содержания и отличия от типовой модернизации (совершенствования, обновления и пр.). На основе анализа текущих предложений о применении существующих протоколов информационного обмена для перспективных сетей связи обосновано предостережение об ограничении применимости протокола IP/MPLS, продвигаемого некоторыми разработчиками, по основаниям его морального и программно-технического устаревания при обеспечении эволюционного перехода на новый, высший, технологический уровень.

Созданы модели сетевых технологических решений, табличные методики сравнения подходов и представлены научно-обоснованные предложения цифровой трансформации сетей связи в интересах обеспечения безопасного информационного обмена.

Научная новизна: научно обоснованное определение единой цифровой платформы специального назначения; новые для отечественных сетей способы применения технологий виртуализации (NFV, SD-WAN и, программно-определяемых сетей (SDN); рекомендации органам военного управления по содержанию этапов построения единой цифровой платформы специального назначения, а также срокам создания единой цифровой платформы специального назначения; новые для отечественных сетей связи подходы к обеспечению безопасности на основе встроенных сетевых механизмов с применением элементов искусственного интеллекта и минимизации участия человека в управленческих процессах.

Введение

Происходящая в мире третья цифровая революция является закономерным этапом исторического развития сетей связи. И не только сетей связи. С середины XX века параллельно зародились и стали внедряться технологии обработки информации на принципах биологических систем. Так появился первый нейрон, так появились нейросети. Впоследствии, в последней трети прошлого столетия искусственные нейроны обрели новое содержание, приблизившись к биологическому образцу. Так появились нейроморфные системы.

Вряд ли кто-то предполагал, что новая отрасль науки – квантовые вычисления, могут оказать влияние на технологии связи и информатики. Но такое влияние, хоть и косвенное,

возникло. И оказало «давление» на системы информационного обмена в форме угроз криптографическим системам. Квантовый компьютер хорошо справляется с задачами факторизации. Причем настолько хорошо, что существующие системы асимметричного шифрования могут оказаться беззащитными перед его могуществом. При этом технологии квантовых вычислений должны использоваться в сетях связи, поскольку они переводят их на принципиально новый уровень эффективности в аспекте скорости передачи информации, решения задач информационного обмена и его безопасности на новом, квантовом уровне.

Таким образом, история развития этих трех смежных направлений привела к их логическому объединению, интеграции, породив

¹ Лукашев Анатолий Викторович, кандидат военных наук, старший научный сотрудник научно-исследовательского центра Военной академии связи им. С. М. Буденного. Санкт-Петербург, Российская Федерация. E-mail: lukasheff@mail.ru

принципиально новые методы инфокоммуникационного обеспечения систем управления, а также других высокотехнологичных систем обработки информации и связи.

Новизна настоящей работы состоит в детальном научном обосновании путей построения сетей связи специального назначения путем их цифровой трансформации, единого утвержденного взгляда, который только начинает внедряться в среду научных исследований. Принцип единства гетерогенных сетей связи, объединяемых единой цифровой платформой на основе широкого внедрения элементов искусственного интеллекта, приобретает качественно новый облик.

Различные взгляды на построение перспективных сетей связи в рамках единой цифровой платформы целесообразно привести к общему пониманию ее облика в результате цифровой трансформации. При этом сроки создания данной платформы должны быть привязаны к быстро развивающейся негативной геополитической ситуации.

Происходит слияние трех технологий в единый информационно-коммуникационно-вычислительный организм – единую цифровую платформу, облик которой во многих источниках пока представляется туманным. Надеемся, что к концу данного труда туман может поредеть, чтобы окончательно рассеяться в ближайших исследованиях.

Другим фактором, определяющим необходимость глубокой цифровой трансформации, следует считать появление квантовых компьютеров, представляющих угрозу криптографическим системам, что ведет к пересмотру требований к сетевой безопасности на принципиально новых, инновационных, технологиях. Полноценный квантовый компьютер, внедрение которого не за горами, способен дешифровать перехваченные сообщения в реальном времени, даже, если они зашифрованы современными криптографическими системами гарантированной стойкости.

Пока же, «недружественные страны» внедряют системы «*Save now, hack later*» («Сохрани сейчас, взломай потом»)².

Это требует принятия решения о защите данных «еще вчера». Ведь существуют сведения, сроки свободного доступа к которым отложены на десятилетия.

Поэтому сверхзадача данной работы состоит в том, чтобы побудить читателя к глубокому осознанию сути и содержанию происходящего перехода развитых стран к новому, шестому, постиндустриальному, технологическому укладу

и присоединению к этому процессу России с целью недопущения потери национального суверенитета.

Почему не IP-MPLS или предотвращение тупиковой ветви развития

В настоящее время в среде разработчиков перспективных сетевых технологий для сетей передачи данных превалирует решение на протоколе *IP/MPLS (Multi-Protocol Label Switching)*, сеть передачи данных с коммутацией по меткам. Целесообразно отметить перечень особенностей и недостатков данного подхода³.

Информация по сетям связи передается, как правило, способом пакетных данных. При этом пакет не содержит данных вне IP-адреса назначения. Так же не существует инструкций о способе доставки пакета данных по назначению. Локальный сетевой маршрутизатор выполняет вычисления и принимает решение об отправке пакета по сети для каждого пакета, руководствуясь метками, содержащимися в заголовке сетевого уровня пакета. Таким образом, каждый раз, когда пакет прибывает на маршрутизатор, он должен осуществить вычисления о дальнейшем маршруте пакета и отправить его дальше, руководствуясь сложными таблицами маршрутизации, которые создаются сетевым администратором (человеком). В случае деструктивного воздействия с выходом из строя участка (фрагмента) сети таблица маршрутов обновляется, как правило, вручную. К этому следует добавить, что такие вычисления вносят свою лепту в рост задержек доставки пакетов, а, следовательно, непосредственно влияют на обеспечение требований по своевременности связи, что по опыту специальной военной операции (СВО) становится критически недопустимым фактором для системы управления в условиях современного боя в тактическом звене управления.

Данный протокол обладает высокой стоимостью внедрения и обслуживания, сложностью настройки (требует высокопрофессионального персонала) и управления, а также проблемы с масштабируемостью и гибкостью, особенно в облачных средах и при работе с удаленными узлами на выделенных операционных направлениях. Протокол менее гибок, чем современные протоколы, например, наиболее популярный *SD-WAN (Software-Defined Wide Area Network)* – технология управления корпоративной WAN-сетью через программные методы в системах передачи данных развитых зарубежных стран.

Высокая стоимость обусловлена необходимостью специализированного оборудования

2 The Intercept: Расследования Э. Сноудена о теневом бюджете АНБ, включая информацию о строительстве дата-центра в штате Юта. – URL: https://theintercept.com/nsa-black-budget/?spm=a2ty_o01.29997173-0.0.33135171rXl4DI (Дата обращения 13.01.2024).

3 Сетевой мир, Интернет ресурс: Многопротокольная коммутация меток надежна, но дорога, что приводит к тому, что предприятия дополняют ее более дешевыми и гибкими SD-WAN // – URL: <https://www.networkworld.com/article/829388/what-is-mpls.html>.

и программного обеспечения, требующего специальной сертификации.

Это ведет к дороговизне при развертывании и обслуживании.

Настройка и управление MPLS-сетью требует специальных знаний и больших трудозатрат (а значит, времени), что осложняет работу в сложных условиях, в том числе, в военное время.

Масштабирование сети является сложным и дорогостоящим, особенно на выделенных направлениях, например, в арктических сценариях. Это обусловлено централизованной маршрутизацией, реализуемой на технической базе, что приводит к задержкам, а также требует дополнительных затрат на развертывание и настройку квалифицированным персоналом. Людские потери в среде обслуживающего персонала, даже одного специалиста могут привести к потере связи на удаленном направлении.

Кроме того, сеть на протоколе MPLS требует использования специализированных протоколов, например, LDP и RSVP-TE, что усложняет настройку системы и управление сетью. К этому следует добавить необходимость постоянной связи с поставщиком оборудования, что ограничивает выбор оптимальных с экономической точки зрения решений и их гибкости, что критически важно для военных систем коммуникаций, требующих оперативного восстановления при деструктивных воздействиях и изменения ситуационной обстановки.

В сети MPLS могут возникать проблемы с адресацией, особенно в больших сетях и особенно при межсетевой интеграции.

Сеть MPLS чувствительна к характерным для военных сетей связям, что может привести к прерыванию соединения и нарушению работы всей сети. Это также ведет к вероятным нарушениям специальных требований к системе связи в части своевременности, достоверности и актуальности переноса трафика в интересах органов управления войсками и оружием.

С учетом изложенного, требуются наиболее современные решения в организации и эксплуатации сетей связи, свойства и характеристики которых отвечают специальным требованиям⁴.

Ниже (табл. 1) представлены сравнительные характеристики существующей сети на протоколе MPLS и сети SD-WAN.

- 4 ■ Alaettinoglu C. – Проблемы мультисервисных сетей. – URL: <https://www.factorgroup.ru/blogs/news/strukturnyy-razbor-dannyh-sdn-vse-delo-v-analitike?ysclid=mfmtj7cnn0695632275>. (Дата обращения сентябрь 2025).
- Enhancing IP-MPLS Networks: Overcoming Challenges and Embracing SDN Advancements. – URL: <https://5gnetworkarchitecture.com/enhancing-ip-mpls-networks-overcoming-challenges-and-embracing-sdn-advancements> (Дата обращения сентябрь 2025).
- Daniel x.: – URL: https://www.academia.edu/38878253/Chapter_1_Introduction_to_MPLS_and_SDN (Дата обращения сентябрь 2025).
- Sam K. Aldrin.: – SDN and MPLS in DataCenters. – URL: https://www.sanog.org/resources/sanog23/SANOG23_SDN_and_MPLS_in_DC.pdf (Дата обращения сентябрь 2025).
- David Jacobs, The Jacobs Group: With MPLS-TP and SDN, a simpler dynamic control plane. – URL: <https://www.techtarget.com/searchnetworking/tip/With-MPLS-TP-and-SDN-a-simpler-dynamic-control-plane>
- Seremet I., Čaušević S.: Advancing IP/MPLS with Software Defined Network in Wide Area Network. // September 2019. – URL: https://www.researchgate.net/publication/335691420_Advancing_IPMPLS_with_Software_Defined_Network_in_Wide_Area_Network_Conference_FOAN-8th_INTERNATIONAL_CONFERENCE_ON_FIBER_OPTICS_IN_ACCESS_NETWORKSAt_Sarajevo (Дата обращения сентябрь 2025).

Таблица 1.

Сравнение MPLS vs SD-WAN (типовой вариант)

Параметр	MPLS	SD-WAN
Время восстановления при сбое	5–10 с (при наличии динамической маршрутизации)	<1 с
Поддержка нескольких видов каналов связи	Только MPLS	LTE, Интернет, VSAT, Wi-Fi mesh
Latency (задержка)	10-50 мс	10-80 мс (в зависимости от типа канала)
Jitter (колебание задержки)	Низкий	Средний, компенсируется политиками QoS (контроля качества связи)
Packet loss (потери пакетов)	<0,1%	0,1–2%
Автоматизация управления	Ограниченная	Полная (через приложение)
Управление политиками маршрутизации	Локальное или через провайдера	Централизованное через оркестратор
Шифрование точка-точка	Дополнительно	Интегрировано (IPsec, DTLS)
Поддержка мобильных узлов	Нет	Да (например, БПЛА, самолеты)
Количество одновременных путей между узлами	1 (LSP)	До 5 (LTE + Интернет + спутниковый канал и др.)
Возможность масштабирования	Сложно (из-за ограничений MPLS-сети)	Просто (любое количество новых или резервных узлов)

Сравнение качественных характеристик, существующих морально устаревших решений на протоколе MPLS и сети SD-WAN позволяет однозначно отдать предпочтение последнему решению.

Обоснование принципов цифровой трансформации сетей связи

В целях более глубокого понимания сути цифровой трансформации сетей связи, прежде всего, специального назначения, ниже (табл. 2), приводятся основные отличия типовой модернизации технических систем от цифровой трансформации, как она понимается (и осуществляется) мировыми технологическим лидерами.

Следует отметить, что логичным путем развития гетерогенных сетей силовых ведомств, государственных ведомственных сетей, Единой сети электросвязи страны (ЕСЭ) является их интеграция путем создания *единой цифровой платформы национального масштаба*, поэтому исходным пониманием цели и сути цифровой трансформации является установление отличий базовых понятий цифровой трансформации от типовой модернизации.

На текущем этапе планирования развития системы связи мероприятия по повышению

безопасности информационного обмена не включают новые угрозы, например, со стороны уже массово применяемых ИИ-агентов, способных имитировать поведение человека, находить уязвимости в сетях связи, внедряться в их внутреннюю структуру, подменить данные, передавать шпионские данные в скрытом фоновом режиме для их обработки противостоящей стороной. В ближайшей перспективе такая обработка будет осуществляться в реальном масштабе времени с помощью квантовых компьютеров. Поэтому в создаваемой единой цифровой платформе (ЕЦП) должны применяться встроенные механизмы защиты, самовосстановления, за счет которых сети обеспечивают устойчивость к внешним и внутренним воздействиям: кибератакам, природным катастрофам, ошибкам персонала и техническим отказам в мили- и микросекундном масштабе времени, где оператор-человек бессильен в борьбе с современными атаками на сетевую безопасность.

Таким образом, цели цифровой трансформации, ее принципиальные отличия от типовой (стандартной) модернизации сформулированы и предложены условия, в которых цифровая трансформация должна осуществляться.

Следует выделить следующие основные принципы формирования ЕЦП:

Таблица 2.

Основные отличия стандартной модернизации информационных и коммуникационных систем от цифровой трансформации

Стандартная модернизация	Цифровая трансформация
Замена старого оборудования на новое, более эффективное, без изменения принципов работы	Системные изменения, затрагивающие всю инфраструктуру и процессы взаимодействия между участниками экосистемы
Локальные изменения, направленные на улучшение конкретных параметров, корректировки общих и частных требований	Фундаментальное изменение архитектуры, технологий и подходов к управлению сетью. Программно-определяемые сети (SDN) позволяющие управлять сетью через программное обеспечение, что делает ее гибкой и масштабируемой
Ограниченная автоматизация, основная роль остается за человеком	Повсеместное внедрение ИИ для самовосстановления и ликвидации сбоев в сети в мили- и микросекундном масштабе времени, управление и оптимизация ресурсов, персонализация услуг, снижение зависимости от человеческого фактора
Обновление оборудования и программного обеспечения без изменения парадигмы функционирования. Сеть остаётся жестко структурированной и недостаточно гибкой	Переход от иерархических структур к распределённым инвариантным моделям управления. Сеть становится гибкой, масштабируемой и способной адаптироваться к меняющимся условиям в реальном времени по внешним условиям и внутреннему потенциалу
Мероприятия по повышению безопасности информационного обмена осуществляются персоналом соответствующих служб с ограниченным применением искусственного интеллекта и не включают защиту от новых угроз кибернетической войны – ИИ-агентов и квантовых компьютеров	Встроенные механизмы защиты, самовосстановления, за счет которых сети обеспечивают устойчивость к внешним воздействиям: кибератакам, природным катастрофам

1. Новые системы должны создаваться на принципе двойного применения – для гражданской и специальной областей.
2. Сети информационного обмена должны использовать единое для всех ведомств программное обеспечение. Оно должно быть модульным, предусматривающим установку дополнительных блоков, обеспечивающих реализацию требований безопасности в сетях специального назначения.
3. Оборудование должно быть унифицированным, с двойным применением и возможностью доукомплектования дополнительными аппаратными средствами для обеспечения специальных требований.
4. Стек протоколов информационного обмена должен быть единым, при этом выполняется принцип разграничения прав доступа. Заметим, что по запросу, должно обеспечиваться сквозное (бесшовное) взаимодействие ведомственных сетей в целях предоставления информационных услуг с заданным качеством – они должны быть своевременными, достоверными, актуальными и обеспечивать безопасный информационный обмен.

Следование данным принципам системой информационного обмена служит основанием *нового*, более высокого технологического уровня предоставляемых органам управления информационных и телекоммуникационных услуг.

Цифровая трансформация сетей связи – это процесс кардинального изменения архитектуры, функциональности и управления сетями на основе единых правил и цифровых технологий, что позволит не только модернизировать их, но и создать принципиально новые возможности для взаимодействия между людьми, устройствами и системами. Это качественный скачок, который выходит за рамки простой модернизации или обновления оборудования.

Для формирования определения ЕЦП следует учесть все факторы, определяющие ее *сущность*. Сущность нового облика данной платформы должна учитывать:

1. *Главный принцип*: «Внедряются только самые передовые, мирового уровня, технологии информационного обмена при условии взаимодействия новых систем с существующими путём интегрирования «старых» сетей в сети нового уровня с помощью аппаратных и программных средств (эволюционный подход)».
2. *Основное предназначение*: предназначение единой цифровой платформы основано на отечественном, в том числе, негативном, и мировом опыте создания больших инфокоммуникационных сетей (платформ),

включающих разнородные сети, принадлежащие различным ведомствам, органам управления, многочисленным организациям и предприятиям.

3. *Общее назначение*: возможность простого доступа любого пользователя, с любого устройства, из любого местоположения к *доверенной* среде единой платформы.
4. *Конечную цель* обеспечения (уже бесшовного) информационного обмена. Пользователям передаваемые сообщения различной природы (речь, медиа контент, передача данных, телеметрическая информация и пр.) должна быть предоставлена в форме услуги. При этом в существующем положении вещей предоставление услуг может быть существенно затруднено или вообще невозможно в силу несовместимости окончного оборудования и программных компонентов. Отсюда – окончное оборудование и программное обеспечение должны быть *унифицированы* по функциональности и распределено по кластерам для всех участников информационного обмена, являющихся участниками единой цифровой платформы.
5. *Доставка сообщений* платформа должна обеспечивать *актуальность* доставляемой информации. Этого можно добиться снижением задержек при обработке и передаче сообщений об изменении ситуации и новых событий. Опыт внедрения подобных решений в мировой практике показывает эффективность *гибридную архитектуру вычислений*, осуществляемых в сетях. Термин гибридной архитектуры вычислений подразумевает комплексно-распределенную организацию вычислений⁵.
Часть вычислений, наиболее сложную, следует осуществлять в специализированных центрах обработки данных (ЦОДах). Обычно такой способ вычислений называется «облачным». При этом, базы знаний и оперативных данных различных ведомств, имеющих ресурсы в ЦОД, должны содержать непротиворечивые сведения. В целях ускорения прохождения сообщений, уменьшения задержек, могут применяться граничные (на стыках сетей) или конечные вычисления (непосредственно на рабочем месте пользователя). Таким образом, единая цифровая платформа должна использовать *гибридную архитектуру вычислений*.
6. *Обеспечение бесшовного* взаимодействия гетерогенных сетей возлагается на единую цифровую платформу. Следовательно, для

5 Былин А., ГК «Ланит»: Распределенные вычисления и надежность гибридных сред. – URL: <https://www.iksmmedia.ru/articles/5851462-Raspredelennye-vychisleniya-i-nadezh.html?ysclid=mffr4bc2kk704260919>. (Дата обращения сентябрь 2025).

присоединения к ней разнородных сетей должен использоваться единый стек протоколов, исключающий трудности взаимодействия данных сетей.

7. *Большие данные.* Современные системы информационного обмена характеризуются большим объемом передаваемых данных, которые собираются из различных источников. В данной ситуации возможности человека не соответствуют объему задач по обработке такого объема данных. Поэтому большие данные обрабатываются с помощью нейросетей (если они «не очень большие», т.е. частные) или генеративными нейроморфными системами искусственного интеллекта (языковыми моделями), если данные имеют достаточно большой объем, а требования по времени их обработки критически малое. При этом персонал Министерства обороны РФ должен иметь доступ к языковым моделям в целях обеспечения обработки данных в реальном масштабе времени. Таким образом, в ЕЦП для обработки должны использоваться *системы искусственного интеллекта*.
8. *Качество услуг* единой цифровой платформы. Внедрение единой цифровой платформы подразумевает повышение ее эффективности практически по всем показателям предъявляемых пользователями различного ранга. Повышение эффективности, в частности, может быть обеспечено за счет *самоорганизации и самовосстановления* сетей связи, в том числе, и самой ЕЦП. Такие свойства также достигаются применением искусственного интеллекта для управления сетями связи. Другим способом повышения эффективности предоставляемых услуг, является *инвариантный доступ* пользователя к сети (линии) связи, обеспечивающей наиболее эффективное предоставление услуги (ресурса) пользователю, абоненту по ситуационному состоянию сетей и ЕЦП.
9. *Сроки* создания единой цифровой платформы. На создание ЕЦП, на фоне геополитической обстановки, которая приобретает угрожающие формы для национальной безопасности России, целесообразно отвести не более 4–5 лет [1, 2]. Обеспечить это возможно, по зарубежному опыту наиболее развитых стран, использованием средств, систем и программного обеспечения двойного назначения и коренным пересмотром регулирования отрасли [3]. Существующее положение характеризуется ведомственным подходом – каждое силовое ведомство, госкорпорация, и даже местная платформа государственных услуг разрабатываются

собственными или привлеченными подрядными командами. Отсюда беспрецедентный расход финансовых, материальных и интеллектуальных ресурсов из-за параллелизма разработок, которые, в итоге, трудно или вообще никак не стыкуются. Развитые страны уже много лет применяют подход *двойного применения (назначения)* разрабатываемых средств и систем⁶. Предприятия ОПК страны, принадлежащие различным ведомствам, при таком подходе, могли бы объединиться в единый научно-промышленный комплекс.

10. *Структура трафика.* Передаваемая в сетях информация разнородна по видам и назначению. Отсюда логически вытекает необходимость внедрения *многоуровневой архитектуры* трафика. В некоторых источниках такой подход называют «многослойностью». Основными уровнями (слоями) могут быть: уровень доступа, уровень транспорта, уровень вычислений, уровень управления. При необходимости можно организовать и другие уровни, например, IoT (интернет вещей) и пр.
11. *Приоритетность.* В сетях постоянно циркулируют информационные потоки. Они порождаются пользователями (абонентами). Пользователи имеют различный *статус*, в соответствии со своим служебным положением. Поэтому пользователям должен присваиваться определенный владельцем сети *ранг*. Присвоенный ранг по отношению к информационному обмену, должен иметь соответствующий *приоритет*. Другая часть информации представляет собой *большие данные* от разнородных датчиков и систем обмена информацией между устройствами, это – интернет вещей, IoT. Здесь приоритеты устанавливаются в соответствии с важностью информации, ее категорией. Поэтому приоритеты такой информации отображаются в *категориях срочности сообщений, общими* для всех ведомств, учреждений и корпораций.
12. *Цифровые двойники.* Цифровой двойник изделия, согласно ГОСТ Р 57700.37-2021, (следует читать «и программного компонента») применяется на всех стадиях жизненного цикла, п. 3.24. Это означает, цифровой двойник (ЦД) должен разрабатываться на этапе проектирования (разработки) изделия, системы, ЦД должен широко использоваться в процессе приемных испытаний (сокращение сроков принятия на вооружение), а также,

⁶ Techniques for satellite communications. November 2020. – URL: [https://irp.fas.org/16_Joint_Publication_1-02_\(15.12.2023_г.\)](https://irp.fas.org/16_Joint_Publication_1-02_(15.12.2023_г.)). (Дата обращения декабрь 2023).

что важно для сетей и систем обмена информацией, прогнозирования отказов, угроз и немедленной передаче сообщения о возможном инциденте управляющему ИИ для предотвращения отказа и нивелирования угрозы.

Итак, основными факторами, определяющими создаваемую единую цифровую платформу, являются:

1. *Приоритет* новейших мировых достижений при планировании создания ЕЦП в форме цифровой трансформации сетей связи.
2. *Бесшовный* информационный обмен.
3. Унифицированное конечное и сетевое оборудование.
4. *Гибридная* архитектура вычислений.
5. *Единый* стек протоколов информационного обмена.
6. Системы искусственного интеллекта для обработки больших данных.
7. Система поддержки принятия решений (СППР) должна трансформироваться в интеллектуальную СППР.
8. *Самоорганизация и самовосстановление* сетей с автоматизацией вхождения в связь.
9. *Инвариантный* доступ пользователей к сетям, обеспечивающих наиболее эффективное предоставление запрошенной услуги (ресурса). При этом перспективные автоматизированные рабочие места и инструменты пользователей должны исполняться с применением эргономичного подхода – применением промышленного дизайна рабочей среды должностных лиц.
10. Внедрение принципа *двойного применения* (назначения) разрабатываемых средств и систем.
11. *Многослойная* (многоуровневая) архитектура трафика в соответствии с приоритетностью передаваемых сообщений и рангом пользователей. Очевидно, что «слоистость» трафика будет иметь *динамический* характер. Это также предопределяет применение SDN сетей в платформе.
12. *Цифровой двойник* ЕЦП, создающийся на этапе ее проектирования и внедрения, обеспечивающий устойчивость системы связи в целом.

На основании вышеизложенных аргументов, изучения компонентов шестого технологического уклада, признаков цифровой трансформации (табл. 1) и ее принципов, а также выявленных факторов, влияющих на функциональность единой цифровой платформы, можно сформировать подход к определению сущности

платформы, вытекающий из выше проведенного анализа.

Определение. *Единая цифровая платформа есть комплекс инфокоммуникационных технологий, реализуемый сетевыми программно-аппаратными средствами под управлением искусственного интеллекта с гибридной архитектурой вычислений, объединяющий и оптимизирующий ресурсы присоединяемых сетей различной принадлежности по единому стеку протоколов.*

Единая цифровая платформа предназначена для устойчивого информационного обеспечения органов государственного и специального управления, пользователей различного ранга путем сквозного бесшовного взаимодействия гетерогенных сетей различной принадлежности в целях предоставления унифицированных услуг с инвариантным доступом.

Кратко опишем функциональную структуру и принцип действия создаваемой платформы.

Функционально ЕЦП может включать два сегмента – виртуальный и физический. Виртуальный сегмент представляет собой временные соединения для предоставления услуг по запросу пользователей. От окончного оборудования до транспортной сети вычисления оптимального пути обеспечиваются конечными вычислителями на объекте пользователя. На стыке канала с транспортной сетью осуществляются граничные вычисления оптимального маршрута внутри данной сети. Далее, на границе транспортной сети и сети, которой принадлежит вызываемый пользователь, осуществляется коммутация и сообщение, в форме распределенных пакетов, доставляется по адресу. Совокупность соединений представляют собой программно-определяемую сеть (SDN), которая непрерывно изменяет собственную структуру без участия человека.

В случае запроса пользователем услуги вычислений при использовании системы поддержки принятия решения, может использоваться гибридная архитектура вычислений – конечные и облачные вычисления, если принятие решения основано на обработке больших данных. В этом случае пользователь считается приоритетным и ему предоставляется канал (с резервированием) наивысшего качества и удовлетворяющий требованию по пропускной способности.

Виртуальный сегмент опирается на сегмент физический, который, в зависимости от масштаба сети, может включать космический, воздушный (авиационный и/или беспилотный) и наземный (стационарный и /или полевой) компоненты гетерогенных (принадлежащих разным ведомствам и различающиеся по технологиям) сетям,

а все вместе представляющие собой транспортную сеть общего пользования.

Наземный компонент может использовать средства радиосвязи, интегрированные с линиями сети космической связи (используются низкоорбитальные спутники), стационарные и полевые медные (постепенно изживающие себя) и волоконно-оптические проводные линии связи.

Транспортная сеть должна обеспечивать, в том числе, мобильных абонентов, для чего может применяться мобильная связь *5G-BH*, в перспективе *6G-BH*, которые обеспечивают высокие скорости передачи данных и ультранизкие задержки.

Воздушный компонент беспилотных средств может быть основан на роевой структуре, когда группа беспилотных летательных аппаратов (БПЛА) различной численности, «зависает» над определенной территорией, непрерывно псевдохаотично перемещаясь в пространстве на расстоянии доступа к ближайшим аппаратам. При этом рой обладает близкой к полносвязности структурой. При выработке ресурса двигателя БПЛА автоматически возвращается на базу, а ему на замену направляется подменный аппарат. База, с которой осуществляются запуски участников роя, должна быть подвижной с обеспечением радио привода по местоположению. При уничтожении участников воздушного роя они заменяются резервными аппаратами, заранее запрограммированными на выполняемую задачу. Каждый аппарат роя должен обладать компонентом общей нейросети, обучающейся в процессе боевого применения. В рое компоненты объединяются в нейросеть, обладающую искусственным разумом.

Авиационный ретранслятор функционирует по классическому формату, обеспечивая связь на более высоком иерархическом уровне системы управления.

Как виртуальный, так и физический компоненты являются гибкими – они предоставляют свой ресурс пользователям по запросу, в том числе, способом инвариантного доступа (независимо от иерархической и ведомственной принадлежности) и это тоже SDN, пришедшая на смену отслужившей свой век сервис-ориентированной архитектуры.

Для предлагаемой архитектуры требуется разработка специальных требований, разграничивающих пользователей по статусу, рангу, а также по приоритетам сообщений или услуг в соответствии с решаемыми системой (органами) управления задачами. Данная задача выходит за рамки статьи и будет решаться в предстоящих исследованиях.

Для доступа к ЕЦП пользователь использует унифицированное оборудование требуемого вида, в соответствии с запрашиваемой услугой. Это может быть голосовой вызов (смартфон, планшет, настольный терминал), видеосвязь (ноутбук и т. п.), передача данных (ноутбук, персональный компьютер, портативный вычислитель, контроллер и пр.), а также аппаратура шифрования. При создании единой цифровой платформы, в предвидении создания полноценного квантового компьютера, шифрование должно обеспечиваться постквантовыми алгоритмами шифрования с эволюционным внедрением систем квантового распределения ключей.

Продолжение следует.

Литература

1. Bahnasse A., Ezzahraa Louhab F., Khiat A., Badri A., Talea M., Pandey B.: Springer. – 2020. – Pp. 1107–1131. – URL: <https://link.springer.com/article/10.1007/s11277-020-07411-1>.
2. Лукашев А., Лаута О., Чаднов А. В ожидании российской квантовой революции в военной сфере // Военная мысль. – 2024. – № 4. – С. 140–147.
3. Dr. Mosks M., Dr. Piani M. – Quantum Threat Timeline report 2022 // Global Risk Institute, Toronto, Canada, December 2022. – Pp. 1–67.
4. Айзексон У., Илон Маск. – М.: АСТ, 2023 г. – 720 с. – ATP 6–02.54.

DIGITAL TRANSFORMATION – NEW TECHNOLOGIES FOR SPECIAL-PURPOSE COMMUNICATION NETWORKS. Part I

Lukashev A. V.⁸

Keywords: *experience of a special military operation, operational space, telecommunications network architecture, dynamic network routing, seamless information exchange, hybrid computing architecture, software-defined networking, label routing, and internetwork integration of communication networks.*

7 RSA and Diffie-Hellman Cryptosystems. – URL: <https://www.moodyanalitics.com/articles/2023/rsa-and-diffie-hellman-cryptosystems-under-threat-sooner-than-previously-thought> (Дата обращения 15.10.2024).

8 **Anatoly V. Lukashev**, Ph.D. of Military Sciences, Senior Researcher of the Research Center of the Military Academy of Communications named after S. M. Budenny. St. Petersburg, Russian Federation. E-mail: lukasheff@mail.ru

Abstract

The purpose of the work: the work is devoted to the topical topic of digital transformation of the communication system – the scientific substantiation of the need to introduce new technologies for building special-purpose communication networks that provide stable and secure information exchange in the difficult conditions of modern operations based on the acquired experience of combat use of the communication system in a special military operation.

Research method: analysis of the world experience in the development of communication networks, its theoretical generalization in order to identify the patterns of development of network technologies in order to scientifically substantiate the methods of digital transformation of domestic communication networks through the introduction of modern virtual and software-defined network technologies with built-in security and artificial intelligence mechanisms.

Research results: a new approach to the digital transformation of special-purpose communication networks is proposed, considering the experience of the world, primarily the USA and China, based on its scientifically based content and difference from standard modernization (improvement, updating, etc.). Based on the analysis of current proposals for the use of existing information exchange protocols for promising communication networks, a warning is substantiated about the limitation of the applicability of the IP/MPLS protocol, promoted by some developers, on the grounds of its moral and software-technical obsolescence while ensuring an evolutionary transition to a new, higher, technological level.

Models of network technological solutions, tabular methods for comparing approaches have been created, and scientifically based proposals for the digital transformation of communication networks in the interests of ensuring secure information exchange have been presented.

Scientific novelty: scientifically based definition of a single special-purpose digital platform; new ways of using virtualization technologies for domestic networks (NFV, SD-WAN and software-defined networks (SDN); recommendations to military authorities on the content of the stages of building a unified special-purpose digital platform, as well as the timing of the creation of a unified special-purpose digital platform; new approaches to ensuring security for domestic communication networks based on built-in network mechanisms using elements of artificial intelligence and minimizing human participation in management processes.

References

1. Bahnasse A., Ezzahraa Louhab F., Khiat A., Badri A., Talea M., Pandey B.: Springer. – 2020. – Pp. 1107–1131. – URL: <https://link.springer.com/article/10.1007/s11277-020-07411-1>.
2. Lukashev A., Lauta O., Chadnov A. V ozhidanii rossijskoj kvantovoj revolyucii v voennoj sfere // Voennaya mysl'. – 2024. – No. 4. – Pp. 140–147.
3. Dr. Mosks M., Dr. Piani M. – Quantum Threat Timeline report 2022 // Global Risk Institute, Toronto, Canada, December 2022. – Pp. 1–67.
4. Ajzekson U., Ilon Mask. – M.: AST, 2023. – 720 p. – ATP 6–02.54.



ПРИМЕНЕНИЕ РЕКУРРЕНТНЫХ НЕЙРОННЫХ СЕТЕЙ ДЛЯ ВЫЯВЛЕНИЯ СКРЫТЫХ АНОМАЛИЙ В ЖУРНАЛАХ СОБЫТИЙ АВТОМАТИЗИРОВАННЫХ СИСТЕМ ВОЕННОГО НАЗНАЧЕНИЯ

Саенко И. Б.¹, Цыпнятов В. Б.², Сажина А. В.³

DOI:10.21681/3034-4050-2026-5-59-66

Ключевые слова: журналы событий, логи, машинное обучение, скрытые аномальные последовательности, автоматизированная система военного назначения.

Аннотация

Цель: разработка и экспериментальное обоснование метода обнаружения скрытых аномальных последовательностей действий пользователей в журналах событий автоматизированной системы военного назначения (АСВН), основанного на использовании рекуррентных нейронных сетей с механизмом долговременной краткосрочной памяти (LSTM).

Методы: для классификации последовательностей событий применена архитектура LSTM-сети. Поскольку размеченные наборы данных для обучения в большинстве случаев отсутствуют, был разработан алгоритм генерации синтетического датасета, имитирующий поведение пользователей с разными функциональными профилями. Для достижения максимальной эффективности обнаружения скрытых аномалий проведен поиск оптимальной конфигурации гиперпараметров нейронной сети.

Результат: экспериментально подтверждено, что предложенная LSTM-модель позволяет эффективно детектировать скрытые аномальные последовательности пользовательских действий, каждое отдельное действие в которых выглядит легитимным. Определена архитектура, при которой достигается максимальное значение обобщенного показателя эффективности обнаружения аномалий. Показана практическая применимость подхода.

Научная новизна: дана математическая формализация понятия «скрытой аномальной последовательности», позволяющая определить условия, когда упорядоченный набор легитимных действий классифицируется как вредоносный. Предложен метод генерации синтетического датасета логов, воспроизводящего сложные паттерны. Экспериментально обосновано, что настройка гиперпараметров LSTM-модели влияет на способность выявлять распределенные во времени многошаговые аномалии.

Введение

Современные условия функционирования автоматизированных систем военного назначения (АСВН) характеризуются постоянным усложнением решаемых задач и ростом требований к оперативности и достоверности управления [1]. АСВН представляют собой совокупность технических и программных средств, интегрированных в единое информационное пространство, предназначенную для автоматизации процессов сбора, обработки и доведения информации до органов управления. Основное предназначение таких систем заключается в обеспечении командования достоверными и своевременными данными о состоянии своих войск и сил противника, что напрямую влияет на сокращение цикла управления и повышение точности принимаемых решений в условиях динамично меняющейся обстановки. В условиях проведения специальной военной операции, защита

АСВН от деструктивных воздействий выходит на первый план.

Проблема защиты информации в АСВН обусловлена, с одной стороны тем, что активно внедряются новые сетевые технологии, а с другой – реализуется концепция «информационной войны», где АСВН рассматриваются как одна из главных целей для воздействия. Обеспечение требуемого уровня защищенности становится возможным только благодаря постоянному анализу угроз безопасности и комплексному применению различных средств защиты. Однако большую сложность представляет поведенческий аспект. Злоумышленники, все чаще используют различные методы маскировки вредоносной активности, выдавая их под легитимные действия пользователя. Это делает традиционные средства контроля и сигнатурные методы анализа неэффективными.

В АСВН, как и в любых других корпоративных информационных системах, пользовательская

¹ Саенко Игорь Борисович, доктор технических наук, профессор, профессор кафедры Военной академии связи, Санкт-Петербург, Россия. E-mail: ibsaen@mail.ru

² Цыпнятов Валерий Борисович, кандидат технических наук, доцент, начальник кафедры Военной академии связи, Санкт-Петербург, Россия. E-mail: zvb097@mail.ru

³ Сажина Александра Владимировна, адъюнкт Военной академии связи, Санкт-Петербург, Россия. E-mail: sashasazhina@yandex.ru

активность фиксируется в журналах событий (логах), объемы которых постоянно растут. Ручной анализ таких данных практически невозможен, а классические системы обнаружения вторжений, построенные на жестко заданных правилах и сигнатурах, которые не способны распознать новые, ранее неизвестные сценарии атак. Особенно если каждое отдельное действие пользователя не нарушает политику безопасности. Такие целенаправленные атаки формируют, так называемые, скрытые аномальные последовательности, в которых вредоносный паттерн выявляется только при совокупности действия [2].

За последние годы в области обнаружения аномалий в пользовательской активности достигнут значительный прогресс. Классические подходы, основанные на статистических моделях, деревьях решений или методах кластеризации, демонстрируют хорошие результаты при выявлении изолированных отклонений. Анализ современных исследований показывает, что рекуррентные нейронные сети, в частности архитектуры с механизмом долговременной краткосрочной памяти (англ. *LongShort-TermMemory*, *LSTM*), которые рассматривают последовательный характер событий, демонстрируют существенное превосходство над традиционными методами. Тем не менее, существует недостаток, заключающийся в отсутствии обоснованных методов использования LSTM именно для задачи выявления скрытых аномальных последовательностей, при условии отсутствия размеченных реальных данных об инсайдерских угрозах [3].

В данной работе предлагается подход к обнаружению скрытых аномальных последовательностей действий пользователей на основе архитектуры LSTM. В рамках этого подхода предложен и реализован метод генерации специализированного синтетического обучающего набора данных. Этот метод показывает скрытые аномальные последовательности действий пользователя с различными профилями, обеспечивая высокую реалистичность и репрезентативность. В сформированный набор данных были целенаправленно внедрены сценарии, имитирующие действия злоумышленника, пытающегося скрыть свою активность за легитимными операциями. Это позволило создать основу для обучения и валидации модели [4].

В работе описывается процесс обучения архитектуры LSTM-модели на сгенерированном датасете [5]. Особое внимание уделено процедуре подбора и варьирования гиперпараметров. Экспериментальная оценка показала, что конфигурация сети существенно влияет на ее способность находить скрытые аномальные последовательности. Экспериментальным путем были

определены оптимальные настройки гиперпараметров, при которых достигается максимальное значение показателя эффективности (*F-меры*). Данный показатель показывает баланс между полнотой и точностью обнаружения. Значимость представленного исследования заключается в разработке метода генерации синтетического датасета и экспериментальном доказательстве высокой эффективности применения LSTM-сетей для выявления сложных аномальных последовательностей [6, 7].

Анализ релевантных работ

Обеспечение информационной безопасности АСВН связано с постоянным анализом журналов событий (логов). В условиях стремительного развития информационных технологий традиционные сигнатурные методы и системы обнаружения вторжений показывают низкую эффективность против сложных инсайдерских угроз с использованием скомпрометированных легитимных учетных записей. Как показывают современные исследования, такие атаки по своей природе являются многошаговыми [8]. В подобных сценариях каждое отдельное действие (например, чтение конфигурационного файла, вход в систему в рабочее время или выполнение штатной сетевой команды) в изоляции не нарушает правил безопасности и выглядит легитимным. Однако их совокупность, с учетом порядка выполнения, частоты и временных интервалов между событиями, образует паттерн, говорящий о злонамеренной активности [9, 10].

Первое значимое направление исследований заключалось в применении классических методов машинного обучения для анализа логов.

К ним относятся скрытые марковские модели, метод главных компонент, одноклассовый метод опорных векторов и алгоритмы на основе изолирующего леса [11, 12]. Несмотря на их эффективность при выявлении ярко выраженных, изолированных отклонений, недостатком этих подходов остается неспособность учитывать долгосрочные временные зависимости. Как показано в работах [13, 14], классические методы анализируют события либо разрозненно, либо в рамках короткого скользящего окна, что уменьшает их эффективность против сложных многошаговых сценариев, разбросанных во времени. У них нет механизма, связанного с запоминанием контекста предшествующих событий. Это чаще всего приводит к высокому уровню ложных срабатываний при попытке оценить последовательность действий пользователя в целом [15].

Это ограничение обусловило переход ко второму направлению: применению методов глубокого

обучения для анализа последовательных данных. Архитектуры глубокого обучения демонстрируют существенное превосходство в задачах выявления сложных нелинейных и долгосрочных зависимостей в потоках логов. В отличие от традиционных методов, нейронные сети способны автоматически извлекать последовательные признаки из сырых данных журналов, выявляя скрытые закономерности.

Перспективным инструментом в рамках этого направления является использование рекуррентных нейронных сетей, в частности, архитектур LSTM. Архитектура LSTM, обладает ячейками состояния и способна избирательно запоминать и передавать временной контекст действий пользователя. Исследования в работах [16, 17] подтверждают, что модели на основе LSTM способны выявлять скрытые паттерны инсайдерских угроз, которые остаются полностью незаметными для методов, оценивающих данные отдельно.

Однако при практическом применении LSTM-моделей к реальным пользовательским логам возникает проблема, связанная с настройкой параметров самой модели. Качество применения LSTM-сети зависит от точного выбора ее гиперпараметров. К ключевым параметрам относятся: количество слоев LSTM, размерность скрытого состояния, длина входной последовательности и коэффициент регуляризации. Как отмечается в современных работах, неоптимальная конфигурация этих гиперпараметров может привести к существенному снижению качества обнаружения. Слишком маленькая длина последовательности не позволит выявить многошаговую атаку, а слишком большая (также как и избыточное количество слоев) приведет к необходимости переобучения сети.

Данная работа включает реализацию архитектуры LSTM для выявления скрытых аномальных последовательностей действий и проведение экспериментального исследования по варьированию ключевых гиперпараметров для достижения максимального показателя обнаружения.

Формализация задачи

Для строгого описания процесса выявления угроз в журналах событий информационной системы необходимо формализовать понятия действия, последовательности действий и скрытой аномальной последовательности, а также определить математический аппарат для оценки качества их обнаружения.

Пусть $A = \{a_1, a_2, \dots, a_m\}$ – конечное множество всех возможных дискретных действий, регистрируемых в информационной системе.

Множество всех возможных действий A естественным образом разбивается на два непересекающихся подмножества: множество заведомо нормальных действий A_{norm} и множество заведомо аномальных (вредоносных) действий A_{anom} . Формально это записывается как:

$$A_{norm} \cap A_{anom} = \emptyset, A_{norm} \cup A_{anom} = A. \quad (1)$$

Активность пользователя за некоторый фиксированный интервал времени представляет собой упорядоченную во времени последовательность действий S длины T . Математически последовательность S определяется как упорядоченный набор элементов из множества A :

$$S = \langle s_1, s_2, \dots, s_T \rangle, \text{ где } s_t \in A, t = \{1, 2, 3, \dots, T\}. \quad (2)$$

В рамках общей последовательности S нас интересует выявление специфических паттернов. Пусть C – это непрерывная подпоследовательность действий длины L ($L \leq T$), извлеченная из S . Формально цепочка C определяется как:

$$C = \langle s_j, s_{j+1}, \dots, s_{j+L-1} \rangle, 1 \leq j \leq (T - L + 1). \quad (3)$$

Обозначим через Ω_L множество всех возможных цепочек длины L , которые можно составить из множества A (то есть $\Omega_L \subset A_L$). Внутри этого множества выделим подмножество $\Omega_{anom}^L \subset \Omega_L$, содержащее цепочки, представляющие собой известные шаблоны вредоносного поведения. Цепочка C классифицируется как скрытая аномальная последовательность (рис. 1). Формально это записывается как:

$$(\forall s \in C: s \in A_{norm}) \wedge (C \in \Omega_{anom}^L). \quad (4)$$

В результате модель идентифицирует данную совокупность как скрытую аномальную последовательность, свидетельствующую о потенциально вредоносной активности. Это служит основанием для формирования предупреждения службы безопасности.

Для количественной оценки эффективности алгоритма используется стандартный набор метрик, основанный на матрице ошибок. Матрица ошибок формируется путем сопоставления предсказанных алгоритмом меток с истинными метками цепочек и включает четыре базовые величины: истинно положительные срабатывания (TP), когда скрытая аномальная цепочка обнаружена верно. Истинно отрицательные срабатывания (TN), когда нормальная цепочка классифицирована правильно. Ложные срабатывания (FP), когда нормальная цепочка ошибочно признана аномальной. Пропущенные аномалии (FN), когда реальная скрытая аномальная цепочка не была выявлена.

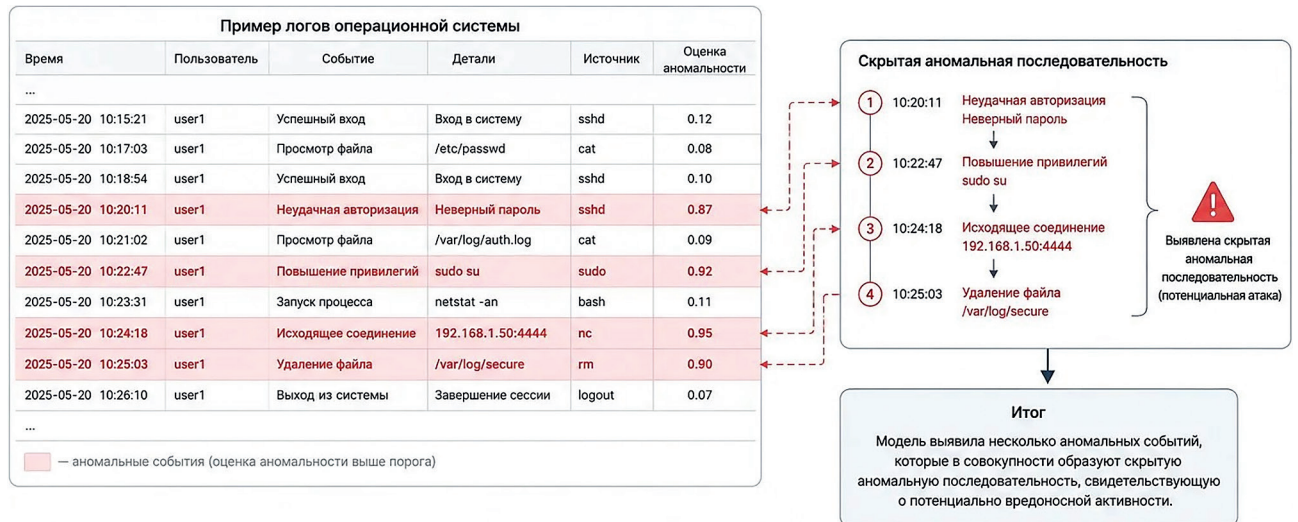


Рис. 1. Скрытая аномальная последовательность

На основе этих величин рассчитываются основные показатели качества классификации. Точность определяет долю цепочек, классифицированных как аномальные, которые действительно являются таковыми, и вычисляется по формуле:

$$Precision = TP / (TP + FP). \quad (5)$$

Полнота (отражает долю реально аномальных цепочек, успешно выявленных алгоритмом:

$$Recall = TP / (TP + FN). \quad (6)$$

Для получения общей оценки используется F -мера, представляющая собой гармоническое среднее точности и полноты:

$$F_1 = 2 \cdot RP / (P + R). \quad (7)$$

В качестве основной целевой метрики для оценки качества обнаружения выбирается F -мера (F_1). Она отражает способность алгоритма выявлять скрытые цепочки действий, максимизируя полноту их обнаружения при допустимом уровне ложных срабатываний.

Генерация набора данных и реализация рекуррентной нейронной сети

Поскольку открытые наборы данных с размеченными скрытыми инсайдерскими атаками отсутствуют, в рамках исследования был разработан и реализован алгоритм генерации специализированного синтетического датасета. Математическая формализация пользовательского поведения задается кортежем $\Pi_u = \langle E_u, P_u, T_u, V_u, R_u \rangle$, где E_u представляет собой множество типов событий, характерных для пользователя; P_u – матрицу вероятностей переходов между событиями; T_u – множество распределений временных

интервалов; V_u – множество параметров вариативности; а R_u – множество ресурсных ограничений. Для обеспечения репрезентативности модель поведения была разделена на несколько функциональных профилей, охватывающих весь спектр субъектов сети. Для каждого профиля на основе экспертного анализа сформированы базовые параметры кортежа Π_u .

Базовой единицей анализа выступает событие – одно действие пользователя, зафиксированное в логе. Признаковое пространство каждого события включает временную метку, должность пользователя, тип действия, объект взаимодействия, длительность действия, результат выполнения, код ошибки, идентификатор сессии и количество ошибок в сессии. Процесс генерации и векторизации данных включает несколько последовательных этапов. Сначала рассматривается множество пользователей, и на основе их профилей генерируется поток событий аудита путем случайного блуждания по графу переходов, заданному матрицей P_u , с учетом распределений временных интервалов T_u и ограничений R_u . Затем выбирается шаг дискретизации $\Delta t > 0$, и временная ось разбивается на равные интервалы $t_k = k\Delta t$, где $k = 0, 1, 2, \dots$. На каждом интервале $[t_k, t_k + \Delta t]$ подсчитываются характеристики активности пользователя, и формально вводится отображение F , ставящее в соответствие набору событий за k -й интервал вектор признаков $x_k(t_k) = [x_{k,1}(t_k), x_{k,2}(t_k), \dots, x_{k,D}(t_k)]^T$, где D – размерность признакового пространства. После векторизации получается обучающая выборка в виде размеченного временного ряда для каждого пользователя, а итоговый датасет формируется как объединение выборок всех пользователей.

Итоговый синтетический датасет был сформирован и разделен на три непересекающихся подмножества: обучающую выборку (70 %), валидационную выборку (15 %) и тестовую выборку (15 %), объективную оценку качества модели.

Для решения задачи классификации последовательностей была реализована архитектура рекуррентной нейронной сети с механизмом долговременной краткосрочной памяти. Входной слой сети принимает матрицу признаков размерности $T \times D$, где T – длина последовательности, а D – размерность признакового пространства. За входным слоем следуют скрытые LSTM-слои, извлекающие долгосрочные временные зависимости и характеризующиеся размерностью скрытого состояния U . Для предотвращения переобучения применяется механизм регуляризации Dropout. Итоговое скрытое состояние подается на выходной слой, вычисляющий вероятность принадлежности последовательности к классу скрытых аномалий.

Ключевым этапом исследования являлось подбор гиперпараметров сети для достижения максимальной F -меры. Пространство поиска включало количество LSTM-слоев L , размерность скрытого состояния U , коэффициент Dropout и длину входной последовательности T . Нахождение оптимальной конфигурации осуществлялось методом случайного поиска на валидационной выборке. Для каждой комбинации гиперпараметров модель обучалась до отсутствия улучшения функции потерь на валидационной выборке. Конфигурация гиперпараметров, обеспечившая наивысшее значение F_1 -меры на этапе валидации, фиксировалась как оптимальная. Финальная оценка достоверности модели проводилась исключительно на тестовой выборке. Это гарантирует объективно судить о способности LSTM-сети выявлять скрытые аномальные последовательности на ранее неизвестных данных.

Экспериментальные исследования и анализ результатов

Целью экспериментальных исследований являлась оценка эффективности предложенной LSTM-сети для выявления скрытых аномальных последовательностей действий пользователей, а также определение оптимальной конфигурации гиперпараметров модели.

Первая часть экспериментов была направлена на анализ влияния ключевых гиперпараметров (количества скрытых слоев, размерности скрытого состояния и коэффициента регуляризации) архитектуры LSTM на значение F_1 -меры. Каждая комбинация гиперпараметров модели обучалась на обучающей выборке, а тестировалась на независимой тестовой выборке последовательностей. Результаты экспериментов представлены на рисунке 2.

Наилучший результат F -меры (0,95) был достигнут при конфигурации: Dropout = 0,5, один скрытый слой, 128 нейронов. Данная конфигурация обеспечивает оптимальный баланс между способностью модели выявлять скрытые аномальные последовательности и предотвращением переобучения. Высокое значение коэффициента Dropout, эффективно регулирует конечный показатель. Он отключает половину нейронов в процессе обучения, что особенно важно при работе с нелинейными данными, характерными для задач обнаружения аномалий.

При сравнении архитектур с одним и двумя скрытыми слоями установлено, что увеличение глубины сети не приводит к существенному улучшению качества обнаружения. Анализ влияния количества нейронов показывает, что при увеличении размерности скрытого состояния с 32 до 128 нейронов приводит к росту F -меры в среднем на 15 %. Это свидетельствует о том, что для эффективного выявления сложных временных паттернов требуется достаточная емкость скрытого состояния LSTM-ячейки.

Эффективность конфигураций LSTM по метрике F_1 -мера

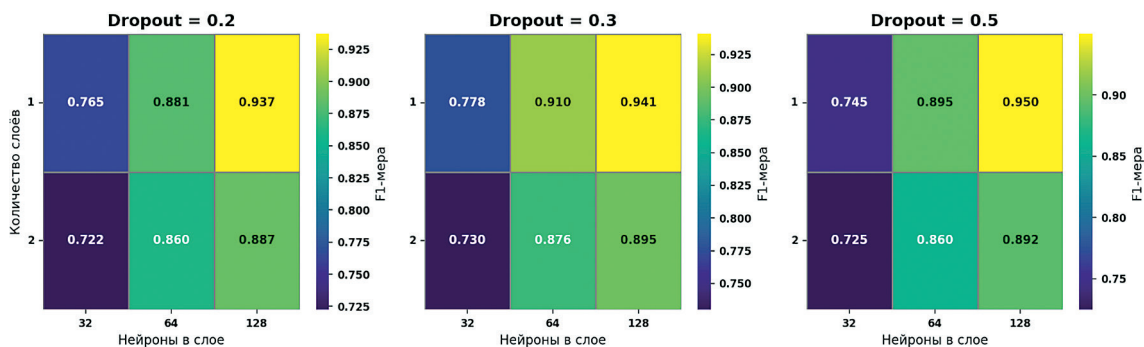


Рис. 2. Эффективность конфигураций LSTM по метрике F -меры

Вторая часть экспериментов была посвящена оценке вычислительной эффективности различных конфигураций LSTM-сети и анализу зависимости времени обучения от параметров архитектуры. На рисунке 3 представлена зависимость времени обучения модели от настройки конфигурации LSTM-модели.

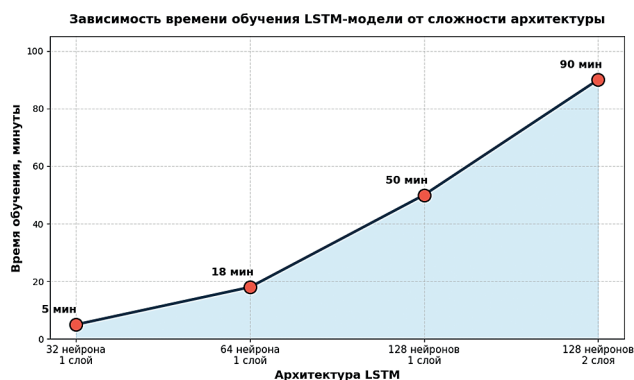


Рис. 3. График зависимости времени обучения от настройки конфигурации LSTM-модели

Анализ полученных результатов показывает, что время обучения зависит от архитектур различной сложности. Легкая конфигурация (32 нейрона, один слой) демонстрирует наилучшую вычислительную эффективность. Время обучения для такой конфигурации составило 5 минут. Для средней конфигурации (64 нейрона, один слой) время обучения составило 18 минут обучения. Тяжелая конфигурация (128 нейронов, один слой), обеспечивающая наилучшее качество обнаружения, требует уже около 50 минут обучения, что является приемлемым только для систем с ежедневным или еженедельным циклом обновления модели. При конфигурации в 128 нейронов и в два слоя время обучения достигает 90 минут. Таким образом, анализ вычислительной эффективности подтверждает обоснованность выбора оптимальной конфигурации, включающей 128 нейронов, один слой и Dropout = 0,5. Она обеспечивает наивысшее качество обнаружения при умеренных временных затратах на обучение.

Заключение

В статье предложен и экспериментально обоснован метод выявления скрытых аномальных последовательностей действий пользователей в журналах событий информационной системы на основе применения рекуррентных нейронных сетей с механизмом долговременной краткосрочной памяти. Проведено сравнение различных конфигураций архитектуры LSTM, включающих варьирование количества скрытых слоев, размерности скрытого состояния и коэффициента регуляризации Dropout. Сделан вывод о том, что математическая формализация скрытых аномальных последовательностей с методами глубокого обучения обеспечивает значительное повышение качества обнаружения угроз при сохранении допустимого уровня вычислительных затрат.

Основные результаты исследования заключаются в следующем:

- 1) разработана математическая формализация понятия скрытой аномальной последовательности на основе теории множеств, которая позволяет определить условия, при которых каждое отдельное действие является легитимным, однако их упорядоченная совокупность классифицируется как вредоносная;
- 2) предложен метод генерации синтетического датасета логов с функциональными профилями пользователей с внедрением скрытых аномальных последовательностей;
- 3) показана практическая применимость предложенного подхода и сделан вывод о том, что модель может быть обучена на стандартном ноутбуке в течение одного рабочего дня. Это позволяет проводить регулярное переобучение модели без необходимости использования специализированных вычислительных машин.

Направления дальнейших исследований включают расширение признаков пространства за счет контекстной информации о сессиях пользователей и ресурсах системы, а также валидацию метода на реальных логах корпоративных информационных систем.

Литература

1. Бушуев С. Н., Авраменко В. С., Козленко А. В. Оценка защищенности информации от несанкционированного доступа в условиях стохастической неопределенности угроз // Вопросы радиоэлектроники. 2013. – Т. 3. – № 1. – С. 82–95. EDN: OJYHPJ.
2. Козленко А. В., Авраменко В. С., Саенко И. Б., Кий А. В. Метод оценки уровня защиты информации от НСД в компьютерных сетях на основе графа защищенности // Труды СПИИРАН. – 2012. – № 2 (21). – С. 41–55. – EDN: PCCYEH.
3. Nguyen H. D., Tran K. P., Thomassey S., Hamad M. Forecasting and Anomaly Detection approaches using LSTM and LSTM Autoencoder techniques with the applications in supply chain management // International Journal of Information Management. – 2021. – Vol. 57. – Pp. 102282. DOI: 10.1016/j.ijinfomgt.2020.102282.

4. Котенко И. В., Ичетовкин Е. А. Методика защиты систем обнаружения вторжений от состязательных атак на основе шумоподавляющих автокодировщиков // Правовая информатика. – 2025. – Т. 12. – № 1. – С. 17–25. – DOI: 10.24412/1994-1404-2025-1-110-120.
5. Козлова Н. Ш., Довгаль В. А. Анализ применения искусственного интеллекта и машинного обучения в кибербезопасности // Вестник Адыгейского государственного университета. Серия: Естественно-математические и технические науки. – 2023. – № 3 (326). – С. 65–72. – DOI: 10.53598/2410-3225-2023-3-326-65-72.
6. Букин А. В., Самонов А. В., Тихонов Э. И. Обнаружение инцидентов информационной безопасности на основе технологии нейронных сетей // Вопросы кибербезопасности. – 2022. – № 5. – С. 61–73. – DOI: 10.21681/2311-3456-2022-5-61-73.
7. Зуев В. Н. Обнаружение аномалий сетевого трафика методом глубокого обучения // Программные продукты и системы. – 2021. – № 1. – С. 91–97. – DOI: 10.15827/0236-235X.133.091-097.
8. Aziz A., Munir K. Anomaly Detection in Logs Using Deep Learning // IEEE Access. – 2024. – Vol. 12. – Pp. 176129–176145. – DOI: 10.1109/ACCESS.2024.3506332.
9. Gonzales O., Yang K., Huang S. Contextual Sequence-Based User Behavior Anomaly Detection // IEEE Access. – 2025. – Vol. 13. – Pp. 35539–35554. – DOI: 10.1109/ACCESS.2025.3543500.
10. Саенко И. Б., Котенко И. В., Аль-Барри М. Х. Применение искусственных нейронных сетей для выявления аномального поведения пользователей центров обработки данных // Вопросы кибербезопасности. – 2022. – № 2 (48). – С. 87–97. – DOI: 10.21681/2311-3456-2022-2-87-97.
11. Карцхия А. А., Макаренко Г. И. Актуальные тренды в развитии искусственного интеллекта // Правовая информатика. – 2025. – № 3. – С. 219–231. – DOI: 10.24412/1994-1404-2025-3-00-24.
12. Ветров И. А., Подтопелный В. В. Особенности использования марковских процессов принятия решений при моделировании атак на системы искусственного интеллекта // Вестник Самарского университета. Естественно-научная серия. – 2024. – Т. 30. – № 4. – С. 147–160. – DOI: 10.18287/2541-7525-2024-30-5-147-160.
13. Kiriachek V. A., Salpagarov S. I. Predictive diagnostics of computer systems logs using natural language processing techniques // Discrete and Continuous Models and Applied Computational Science. – 2025. – Vol. 33. – No. 2. – Pp. 172–183. – DOI: 10.22363/2658-4670-2025-33-2-172-183.
14. Lapina M. A., Podruchny N. V., Rusanov M. A., Babenko M. G. Research of machine learning methods for detecting network attacks // Proceedings of the Institute for System Programming of the RAS. – 2025. – Vol. 37. – No. 4-2. – Pp. 147–174. – DOI: 10.15514/ISPRAS-2025-37(4)-24.
15. Macas M., Wu C., Fuertes W. A survey on deep learning for cybersecurity: Progress, challenges, and opportunities // Computer Networks. – 2022. – Vol. 212. – P. 109032. – DOI: 10.1016/j.comnet.2022.109032.
16. Пашшоев Б., Петрусевиц Д. А. Анализ нейросетевых моделей для прогнозирования временных рядов // Russian Technological Journal. – 2024. – Т. 12. – № 4. – С. 106–116. – DOI: 10.32362/2500-316X-2024-12-4-106-116.
17. Чуб В. С. Использование рекуррентных нейронных сетей для анализа временных рядов и выявления тенденций в данных // Образовательные ресурсы и технологии. – 2024. – №2 (47). – С. 91–102. – DOI: 10.21777/2500-2112-2024-2-91-102.

APPLICATION OF RECURRENT NEURAL NETWORKS TO DETECT HIDDEN ANOMALIES IN EVENT LOGS OF AUTOMATED MILITARY SYSTEMS

Sayenko I. B.⁴, Tsypnyatov V. B.⁵, Sazhina A. V.⁶

Keywords: event logs, logs, machine learning, hidden anomalous sequences, automated military system.

Abstract

Objective: development and experimental substantiation of a method for detecting hidden anomalous sequences of user actions in the event logs of an automated military system (ASV), based on the use of recurrent neural networks with a long-term memory (LSTM) mechanism.

Methods: The LSTM network architecture was used to classify event sequences. Since there are no labeled training datasets in most cases, an algorithm for generating a synthetic dataset was developed to simulate the behavior of users with different functional profiles.

Result: it has been experimentally confirmed that the proposed LSTM model allows us to effectively detect hidden anomalous sequences of user actions, each individual action in which looks legitimate.

Scientific novelty: the author provides mathematical formalization of the concept of «hidden anomalous sequence», which makes it possible to determine the conditions when an ordered set of legitimate actions is classified as malicious.

4 Igor B. Sayenko, Dr.Sc. of Technical Sciences, Professor, Professor of the Department of the Military Academy of Communications, St. Petersburg, Russia. E-mail: ibsaen@mail.ru

5 Valery B. Tsypnyatov, Ph.D. of Technical Sciences, Associate Professor, Head of the Department of the Military Academy of Communications, St. Petersburg, Russia. E-mail: zvb097@mail.ru

6 Alexandra V. Sazhina, Adjunct of the Military Academy of Communications, St. Petersburg, Russia. E-mail: sashasazhina@yandex.ru

A method for generating a synthetic log dataset that reproduces complex patterns is proposed. It is experimentally substantiated that the adjustment of the hyperparameters of the LSTM model affects the ability to detect multistep anomalies distributed in time.

References

1. Bushuev S. N., Avramenko V. S., Kozlenko A. V. Ocenka zashchishchennosti informacii ot nesankcionirovannogo dostupa v usloviyah stohasticheskoy neopredelennosti ugroz // Voprosy radioelektroniki. – 2013. – V. 3. – No. 1. – Pp. 82–95. – EDN: OJYHPJ.
2. Kozlenko A. V., Avramenko V. S., Saenko I. B., Kij A. V. Metod ocenki urovnya zashchity informacii ot NSD v komp'yuternyh setyah na osnove grafa zashchishchennosti // Trudy SPIIRAN. – 2012. – No. 2 (21). – Pp. 41–55. – EDN: PCCYEH.
3. Nguyen H. D., Tran K. P., Thomassey S., Hamad M. Forecasting and Anomaly Detection approaches using LSTM and LSTM Autoencoder techniques with the applications in supply chain management // International Journal of Information Management. – 2021. – Vol. 57. – Pp. 102282. – DOI: 10.1016/j.ijinfomgt.2020.102282.
4. Kotenko I. V., Ichetovkin E. A. Metodika zashchity sistem obnaruzheniya vtorzhenij ot sostyazatel'nyh atak na osnove shumopodavlyayushchih avtokodirovshchikov // Pravovaya informatika. – 2025. – V. 12. – No. 1. – Pp. 17–25. – DOI: 10.24412/1994-1404-2025-1-110-120. EDN: JAJRNO.
5. Kozlova N. Sh., Dovgal' V. A. Analiz primeneniya iskusstvennogo intellekta i mashinnogo obucheniya v kiberbezopasnosti // Vestnik Adygejskogo gosudarstvennogo universiteta. Seriya: Estestvenno-matematicheskie i tehniccheskie nauki. – 2023. – No. 3 (326). – Pp. 65–72. – DOI: 10.53598/2410-3225-2023-3-326-65-72.
6. Bukin A. V., Samonov A. V., Tihonov Eh. I. Obnaruzhenie incidentov informacionnoj bezopasnosti na osnove tehnologii nejronnyh setej // Voprosy kiberbezopasnosti. – 2022. – No. 5. – Pp. 61–73. – DOI: 10.21681/2311-3456-2022-5-61-73.
7. Zuev V. N. Obnaruzhenie anomalij setevogo trafika metodom glubokogo obucheniya // Programmnye produkty i sistemy. – 2021. – No. 1. – Pp. 91–97. – DOI: 10.15827/0236-235X.133.091-097.
8. Aziz A., Munir K. Anomaly Detection in Logs Using Deep Learning // IEEE Access. – 2024. – Vol. 12. – Pp. 176129–176145. – DOI: 10.1109/ACCESS.2024.3506332
9. Gonzales O., Yang K., Huang S. Contextual Sequence-Based User Behavior Anomaly Detection // IEEE Access. – 2025. – Vol. 13. – Pp. 35539–35554. – DOI: 10.1109/ACCESS.2025.3543500.
10. Saenko I. B., Kotenko I. V., Al-Barri M. H. Primenenie iskusstvennyh nejronnyh setej dlya vyyavleniya anomal'nogo povedeniya pol'zovatelej centrov obrabotki dannyh // Voprosy kiberbezopasnosti. – 2022. – No. 2 (48). – Pp. 87–97. – DOI: 10.21681/2311-3456-2022-2-87-97
11. Karchiya A. A., Makarenko G. I. Aktual'nye trendy v razvitii iskusstvennogo intellekta // Pravovaya informatika. – 2025. – No. 3. – Pp. 219–231. – DOI: 10.24412/1994-1404-2025-3-00-24.
12. Vetrov I. A., Podtopel'nyj V. V. Osobennosti ispol'zovaniya markovskih processov prinyatiya reshenij pri modelirovanii atak na sistemy iskusstvennogo intellekta // Vestnik Samarskogo universiteta. Estestvennonauchnayaseriya. – 2024. – V. 30. – No. 4. – Pp. 147–160. – DOI:10.18287/2541-7525-2024-30-5-147-160. – EDN: SLIVCV.
13. Kiriachek V. A., Salpagarov S. I. Predictive diagnostics of computer systems logs using natural language processing techniques // Discrete and Continuous Models and Applied Computational Science. – 2025. – Vol. 33. – No. 2. – Pp. 172–183. – DOI: 10.22363/2658-4670-2025-33-2-172-183.
14. Lapina M. A., Podruchny N. V., Rusanov M. A., Babenko M. G. Research of machine learning methods for detecting network attacks // Proceedings of the Institute for System Programming of the RAS. – 2025. – Vol. 37. – No. 4-2. – Pp. 147–174. – DOI: 10.15514/ISPRAS-2025-37(4)-24.
15. Macas M., Wu C., Fuertes W. A survey on deep learning for cybersecurity: Progress, challenges, and opportunities // Computer Networks. – 2022. – Vol. 212. – P. 109032. – DOI: 10.1016/j.comnet.2022.109032.
16. Pashshoev B., Petrushevich D. A. Analiz nejrosetevykh modelej dlyaprognozirovaniya vremennyh ryadov // Russian Technological Journal. – 2024. – V. 12. – No. 4. – Pp. 106–116. – DOI: 10.32362/2500-316X-2024-12-4-106-116.
17. Chub V. S. Ispol'zovanie rekurrentnyh nejronnyh setej dlya analiza vremennyh ryadov i vyyavleniya tendencij v dannyh // Obrazovatel'nye resursy i tehnologii. – 2024. – No. 2 (47). – Pp. 91–102. – DOI: 10.21777/2500-2112-2024-2-91-102.



СПОСОБЫ ОРГАНИЗАЦИИ ФУНКЦИОНИРОВАНИЯ СИСТЕМЫ ВИДЕОТРАНСЛЯЦИИ В УСЛОВИЯХ СОВРЕМЕННЫХ ВОЕННЫХ ДЕЙСТВИЙ

Лебедев П. В.¹, Живодерников А. Ю.²

DOI:10.21681/3034-4050-2026-5-67-76

Ключевые слова: конфиденциальный сегмент сети, нейросетевое сжатие, информационная безопасность, пропускная способность каналов связи, ситуационная осведомленность, периферийные вычисления, компьютерное зрение, сегментация сетей, мультиплексирование, радиоэлектронная борьба, беспилотные летательные аппараты, автоматизированное целеуказание.

Аннотация

Цель работы состоит в фундаментальном анализе, систематизации и разработке концептуальных подходов к организации функционирования систем видеотрансляции и видеонаблюдения, а также в обосновании путей интеграции систем искусственного интеллекта в контур управления войсками в реальном масштабе времени в условиях высокоинтенсивного конфликта.

Метод исследования включает системный анализ архитектур сетей передачи данных, структурно-функциональное моделирование компонентов систем видеотрансляции, сравнительную оценку программных комплексов агрегации видеопотоков, а также исследование методов адаптивного сжатия, мультиплексирования и бортовой нейросетевой обработки видеоинформации в условиях дефицита пропускной способности и воздействия средств радиоэлектронной борьбы.

Результаты исследования: обобщен опыт группировки войск «Запад» по интеграции более 100 стационарных комплексов и сотен тактических беспилотных летательных аппаратов в единое информационное пространство. Выявлены критические зависимости качества управления от пропускной способности каналов связи. Доказана эффективность применения отечественных программных решений («Астра-С», «TrueConf») с различными алгоритмами кодирования. Проведен эксперимент с кодеком NeuroVideoCodec в радиосетях «Азарт», подтвердивший возможность передачи разборчивого видео по каналам низкого качества.

Обоснована необходимость перехода от физической маскировки серверов к распределенному выделению ресурса пропускной способности и внедрению бортовых систем компьютерного зрения на разведывательных беспилотных летательных аппаратах для снижения нагрузки на каналы связи и автоматизации целеуказания.

Научная новизна заключается в разработке комплексного концептуального подхода к организации видеотрансляции, сочетающего строгую сегментацию сетей передачи данных, адаптивное мультиплексирование потоков, применение нейросетевых алгоритмов сжатия для преодоления последствий воздействия средств радиоэлектронной борьбы противника, а также в формализации принципов интеграции систем искусственного интеллекта на периферийных узлах (борту БПЛА) для реализации концепции «интеллектуального края» (intelligentedge) в тактическом звене.

Введение и постановка задачи

Опыт военных действий в ходе проведения специальной военной операции (СВО) фундаментально трансформировал парадигму организации связи и автоматизированных систем управления (АСУ). Видеонаблюдение и видеотрансляция эволюционировали из вспомогательной функции инженерной и тактической разведки в одну из базовых, критически важных услуг, предоставляемых должностным лицам для непрерывного контроля за тактической обстановкой, верификации данных разведки и управления боем в реальном масштабе времени.

Постановка задачи исследования обусловлена необходимостью синтеза разрозненного

опыта применения видеоинформационных систем в войсках, глубокого анализа архитектурных решений сетей передачи данных (СПД) и выработки унифицированных, научно обоснованных способов организации функционирования систем видеотрансляции [1].

Современный общевойсковой бой характеризуется высочайшей динамикой, тотальным применением беспилотных летательных аппаратов (БПЛА) всех классов, а также жестким и непрерывным противодействием средств радиоэлектронной борьбы (РЭБ) противника. В этих условиях традиционные подходы к построению замкнутых, централизованных систем видеонаблюдения оказываются нежизнеспособными. Требуется гибкая, масштабируемая, живучая

¹ Лебедев Павел Владимирович, кандидат технических наук, доцент кафедр Военной академии связи, г. Санкт-Петербург, Россия. E-mail: spirit-angel@yandex.ru

² Живодерников Александр Юрьевич, кандидат технических наук, старший преподаватель кафедры Военной академии связи, г. Санкт-Петербург, Россия. E-mail: sabir.81@mail.ru

и защищенная инфраструктура, способная агрегировать видеопотоки с тысяч источников (стационарных камер, тепловизоров, тактических и оперативно-тактических БПЛА) и доставлять их на пункты управления (ПУ) различного уровня с минимальными задержками, динамически адаптируясь к деградирующим условиям среды распространения радиосигнала.

Основные понятия и состав системы военной видеотрансляции

В военно-техническом контексте «военная видеотрансляция» определяется не просто как процесс передачи видеосигнала, а как непрерывный, надежный и защищенный поток мультимедийных данных, формирующий единое информационно-управляющее поле тактического и оперативного звена. В отличие от гражданских аналогов, военная видеотрансляция жестко лимитирована требованиями информационной безопасности, пропускной способности защищенных каналов связи и необходимостью функционирования в условиях активного огневого и радиоэлектронного противодействия.

Структурно-функциональный состав системы видеотрансляции в интересах управления войсками подразделяется на четыре взаимосвязанных уровня (подсистемы):

1. Подсистема источников формирования видеопотока (периферийный уровень). Включает в себя стационарные комплексы видеонаблюдения («Сапсан», «Муром», «Горизонт»), тепловизионные камеры, а также бортовые полезные нагрузки БПЛА всех классов (от FPV-дронов до аппаратов оперативно-тактического назначения). На этом уровне все чаще начинают внедряться модули первичной предобработки данных.
2. Транспортная подсистема (канальный уровень). Обеспечивает доставку видеопакетов от источников до узлов агрегации. Включает себя проводные линии связи, радиорелейные линии, спутниковые каналы, а также широкополосные радиосети (например, «Азарт-ШПС»).
3. Подсистема агрегации, коммутации и хранения (серверный уровень). Серверные комплексы, осуществляющие прием, декодирование, маршрутизацию, мультиплексирование и архивирование видеопотоков. Обеспечивает разделение потоков по уровням секретности (открытый и конфиденциальный сегменты СПД).
4. Подсистема отображения, анализа и принятия решений (уровень пунктов управления). Аппаратно-программные комплексы на рабочих местах операторов и командиров, включая

видеостены, специализированное ПО для вывода множественных потоков, средства интеграции видео с тактическими планшетами и системами управления огнем.

Принципиальные подходы в организации видеотрансляции

Анализ опыта группировки войск «Запад» (ГВ «Запад») и других объединений позволяет сформулировать четыре принципиальных подхода к организации функционирования систем видеотрансляции в современных условиях:

Первый подход: строгая сегментация по уровню защищенности информации. Маршрутизация видеопотоков жестко привязывается к архитектуре СПД Министерства обороны РФ. Для БПЛА оперативно-тактического назначения (Форпост, Иноходец) и критически важных стационарных узлов вывод изображения обеспечивается исключительно в конфиденциальном сегменте сети передачи данных (КС СПД) с использованием аппаратуры защиты информации (АЗИ), таких как АПКШ «Континент» и межсетевых экранов (МЭ) «Дионис». Для тактического звена (Mavic, Орлан, Зала) и линейных камер допускается использование открытого сегмента (ОС СПД) с интеграцией в транспортные сети группировок войск.

Второй подход: эшелонирование по классам БПЛА и задачам. Серверное оборудование условно делится на две функциональные группы: серверы для агрегации данных со стационарных комплексов (обеспечивающие постоянный мониторинг за обстановкой на местности) и серверы для вывода изображения с БПЛА (обеспечивающие динамическую тактическую разведку). Такое разделение позволяет оптимизировать нагрузку на магистральные каналы и применять различные алгоритмы кодирования для статичных и динамичных сцен.

Третий подход: адаптивность к деградации каналов связи. В условиях применения противником средств РЭБ пропускная способность каналов может падать на порядки. Принципиальным подходом становится использование программного обеспечения с адаптивным битрейтом (например, «TrueConf», способное передавать поток 640x480 при 300-500 кбит/с) и внедрение специализированных кодеков (NeuroVideoCodec), сохраняющих разборчивость изображения на границе Шеннона.

Четвертый подход: физическое и логическое рассредоточение (живучесть). Развернутые элементы системы видеонаблюдения являются приоритетными целями для высокоточного оружия и FPV-дронов противника. Помимо инженерной маскировки, принципиальным подходом

становится логическое разделение: физические камеры и простые узлы ввода устанавливаются на передовых позициях, а мощные вычислительные серверы и пункты анализа выносятся в глубокий тыл [2]. Доступ к видео осуществляется удаленно через выделенный ресурс пропускной способности, что минимизирует риски потери управления при поражении передовых узлов.

Аппаратные средства и серверная инфраструктура

В Объединенной группировке войск применяется более 1100 комплексов видеонаблюдения. Основные технико-эксплуатационные данные некоторых из них представлены в таблице 1.

Так, например, по состоянию на текущий период, в ГВ «Запад» из 177 комплектов видеонаблюдения к транспортной сети подключены 157. Вывод изображения с камер обеспечивается серверами «Интеллект-Х» и «Астра-С» общей

емкостью 4158 каналов. Вывод изображения с БПЛА тактического звена осуществляется через стационарный сервер «TrueConf» (емкость 2607 учетных записей). В среднем серверами видеотрансляции обрабатывается до 29 Тбайт трафика ежемесячно.

Сравнительный анализ программного обеспечения

Анализ использования программного обеспечения по выводу видеоизображения от БПЛА показал, что на сегодняшний день наиболее хорошо себя зарекомендовали «TrueConf» (рис. 1) и «Астра-С» [6]. При этом ПО «Линия» и «Глаз/Гроза» используются в основном подразделениями разведки, артиллерии и подразделениями БПЛА, а для взаимодействия с пунктами организации видеотрансляции в качестве мессенджера для переписки текстовыми сообщениями используется сервер PostLink.

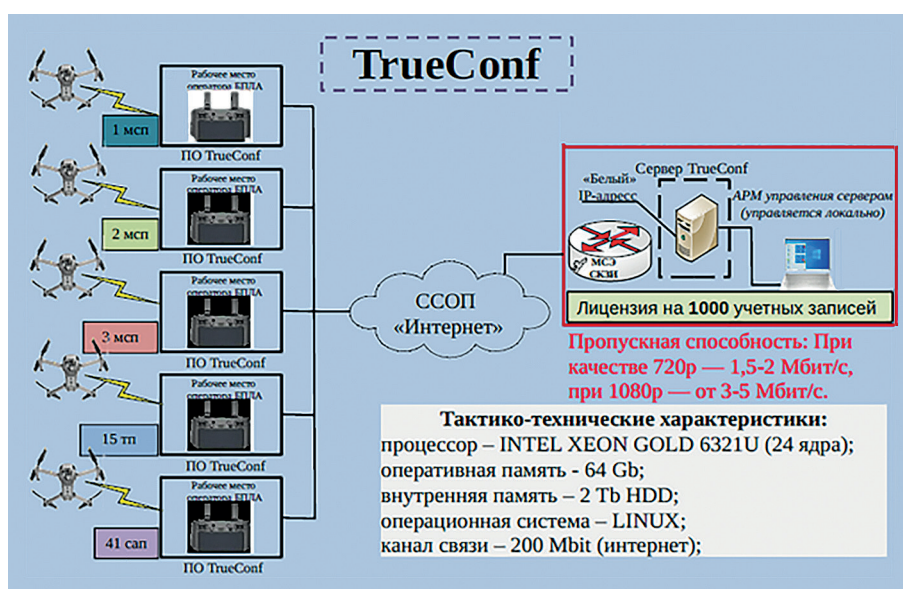


Рис. 1. Система видеотрансляции «TrueConf»

Технико-эксплуатационные данные комплексов видеотрансляции

Таблица 1

Показатель	Сапсан	Сапсан-С	МК ВТр	Starview	Hikvision
Дальность обнаружения целей видеокамерой:					
человек	до 6,8 км	до 6 км	до 3 км	до 3 км	до 3 км
автомобиль	до 19 км	до 9 км	до 5 км	до 5 км	до 5 км
Дальность обнаружения целей тепловизором:					
человек	до 4 км	до 4 км	нет	до 3 км	нет
автомобиль	до 10 км	до 10 км		до 5 км	
Масса, кг	45	11	2	9	10
Стоимость, руб	7 млн	6,5 млн	9,4 млн	2,3 млн	1 млн

Положительные стороны ПО «TrueConf»:

- наличие собственного сервера и дежурной смены, осуществляющей мониторинг его работы и решение проблем пользователей после их авторизации;
- высокое качество трансляции с БПЛА и комплексов видеонаблюдения;
- наличие голосового чата;
- возможность объединить подразделения в единое информационное пространство;
- возможность настройки кластера с серверами других группировок;
- пользователи самостоятельно могут менять пароли для входа в свои учетные записи;
- изображение адаптируется под пропускную способность оконечного оборудования, тем самым при разрешении 640x480 поток передается при 300–500 кбит/с пропускной способности [7], что отсутствует в других программных решениях, предоставляемых для трансляций в группировках, типа «Глаз/Гроза», «Астра-С».

Проработаны различные способы вывода видеотрансляции с БПЛА на пункты управления, в том числе:

- для смартфона с подключением по кабелю к пульту управления БПЛА;
- для пульта управления со своей операционной системой;
- для пульта управления со своей операционной системой с выводом через модуль видеозахвата;
- для пульта управления с VR-очками.

Кроме того, разработан способ вывода дополнительного изображения с пульта управления БПЛА на отдельный источник для передачи видеосигнала со схемой распайки штатного кабеля.

На пункте управления данные с БПЛА выводятся на видеостену, причем реализованы варианты вывода одновременно с большого числа источников, по принципу единой среды обмена видеоданных (рис. 2).

Отрицательные стороны ПО «TrueConf»:

- отсутствие двухфакторной аутентификации;
- отсутствие общей выкладки трансляций всех подразделений и фильтра для нужд пунктов управления;
- невозможность мониторинга сессий абонентов и выявления подозрительной активности.

Положительные стороны ПО «Астра-С» (рис. 3):

- высокое качество трансляций с БПЛА и комплексов видеонаблюдения;
- сервер с пропускной способностью 10 Гбит/с, позволяющий организовывать вывод более чем с 250 источников одновременно и обеспечивающий просмотр трансляций более 1000 пользователям;
- дежурная смена, работающая в круглосуточном режиме и осуществляющая мониторинг работы ПО, решение проблем пользователей (после их авторизации) и возможностью связи по АТС-Р;
- реализация панели администратора с возможностью мониторинга сессий абонентов, позволяющей определять провайдера, локацию,

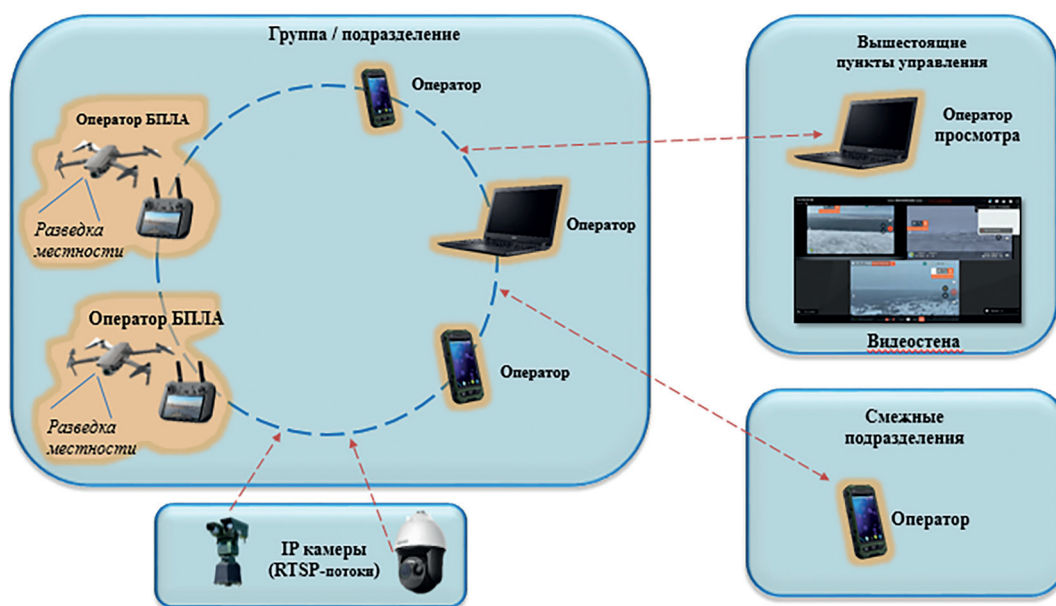


Рис. 2. Организация вывода изображения с БПЛА с использованием сервера «TrueConf»

- IP-адрес устройства, выявлять подозрительную активность;
- иерархия подразделений и возможность получения доступа к трансляциям взаимодействующих подразделений;
- удобный клиент-сервис с поддержкой всех актуальных прошивок, применяемых на пультах БПЛА;
- настраиваемая выкладка трансляций всех подразделений с фильтром в интересах должностных лиц ПУ;
- наличие двухфакторной аутентификации[4].

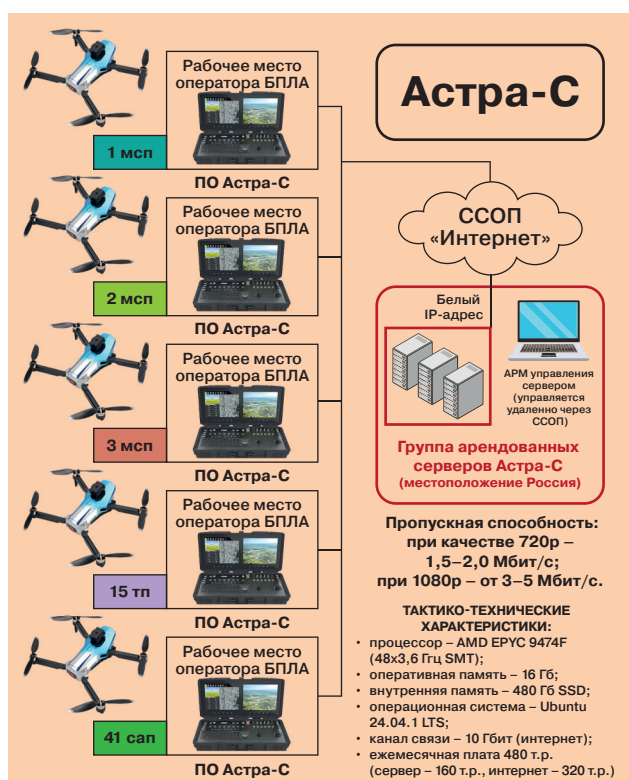


Рис. 3. Система видеотрансляции Астра-С

Хорошее качество трансляции при использовании ПО «Астра-С» достигается тем, что в нем практически не применяется сжатие видеопотока, что в свою очередь приводит к значительному увеличению используемого трафика.

Отрицательные стороны ПО «Астра-С»:

- отсутствие голосового чата (находится в стадии тестирования);
- отсутствие собственного сервера с пропускной способностью не ниже 10 Гбит/с (подключены к центральному серверу «Астра-С»).

Анализ трафика в ГВ «Запад» (около 300 одновременных трансляций) показал, что каждая трансляция в «Астра-С» занимает около 4 Мбит/с ресурса пропускной способности. Общий трафик трансляций составляет 1,23 Гбит/с.

Загрузка сервера достигает 7,2 Гбит/с. В то же время, в ПО «TrueConf» из 2607 выданных учетных записей в режиме онлайн одновременно находится около 1100 пользователей, что обусловлено сменным графиком и адаптивным битрейтом.

Способы и маршруты доставки видеопотоков на пункты управления

Организация бесперебойной доставки видеoinформации от источников формирования (передовых позиций) до пунктов управления (ПУ) различного уровня является сложной телекоммуникационной задачей. Успешность ее решения зависит от выбранной сетевой топологии, методов съема сигнала на передовом крае и алгоритмов распределения полосы пропускания. В Объединенной группировке войск (сил) маршрутизация видеопотоков формализована и осуществляется по двум принципиально различным сценариям, в зависимости от класса беспилотных систем и уровня конфиденциальности передаваемой информации.

Первый способ: маршрутизация в конфиденциальном сегменте СПД (КС СПД).

Применяется для комплексов и БПЛА оперативно-тактического назначения (например, «Форпост», «Иноходец»), передающих критически важную разведывательную информацию.

Алгоритм доставки данных имеет следующий вид:

1. Наземная станция управления (НСУ) БПЛА подключается к транспортной сети через специализированные МЭ «Дионис» или комплексы связи, имеющие в своем составе данные МЭ.
2. Видеопоток шифруется с использованием аппаратуры криптографической защиты информации (АПКШ «Континент») [3].
3. Трафик передается по выделенным защищенным каналам в конфиденциальный сегмент сети передачи данных Минобороны России (КС СПД).
4. На стороне приема видеопоток декодируется и агрегируется на серверах, таких как «Сапфир» (производства «Протей-СТ») или высокопроизводительных узлах «Астра-С».

Достоинства: высокий уровень защищенности от несанкционированного доступа и перехвата.

Недостатки: высокие требования к аппаратуре защиты, задержки (латентность), вносимые алгоритмами шифрования, и жесткая привязка к стационарной инфраструктуре КС СПД. Примером критичности задержек является привязка через спутниковый ретранслятор (рис. 4).

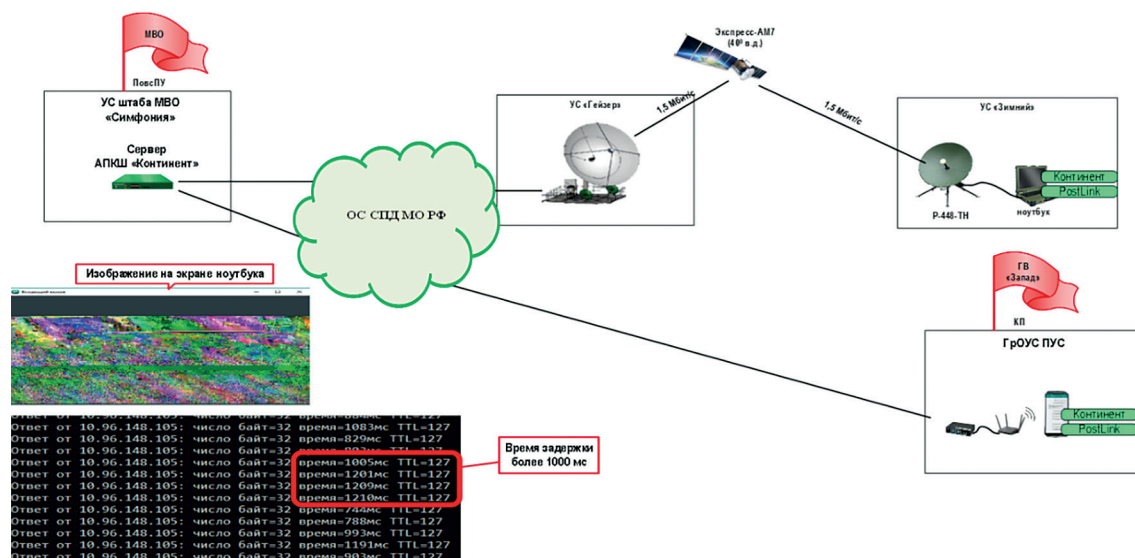


Рис. 4. Способ подключения сервера видеотрансляции к транспортной сети

Второй способ: маршрутизация в ОС СПД [4] применяется для массового сегмента тактических БПЛА (Mavic, Орлан, Зала, FPV-дроны) и стационарных камер видеонаблюдения линейных подразделений.

Алгоритм доставки данных:

1. Видеосигнал с пультов управления или IP-камер поступает в ОС СПД.
2. Осуществляется интеграция в транспортные сети группировок войск с использованием стандартных протоколов маршрутизации.
3. Агрегация, коммутация и распределение потоков абонентами осуществляется на серверных мощностях с использованием ПО «TrueConf», «Интеллект-Х», «АххонNext» или «Астра-С».

Достоинства: высокая скорость развертывания, возможность масштабирования, адаптация к мобильным узлам связи.

Недостатки: необходимость дополнительного контроля за утечкой информации, высокая нагрузка на магистральные каналы ОС СПД из-за отсутствия агрессивного сжатия (в случае с «Астра-С»).

Критическим узлом, часто становящимся «бутылочным горлышком» системы, является процедура съема видео с пульта управления БПЛА и передачи его в транспортную сеть. Анализ практики в ГВ «Запад» выявил четыре основных способа решения этой задачи:

1. Программный мост (ScreenCasting). Трансляция экрана пульта управления или смартфона по локальной сети. Недостаток: высокая нестабильность, задержки, «зависания» при перегреве мобильных устройств.

2. Аппаратный модуль видеозахвата. Использование HDMI/USB-грабберов, подключаемых к видеовыходу пульта. Недостаток: требует наличия штатного видеовыхода на пульте, что есть не у всех моделей тактических БПЛА.

3. Съем через VR-очки (для FPV). Вывод видеопотока с экрана FPV-очков оператора через разветвители или встроенные видеовыходы очков.

4. Аппаратное вмешательство в штатную кабельную трассу (наиболее перспективный способ). Разработан и внедрен способ вывода дополнительного изображения непосредственно с пульта управления БПЛА на отдельный IP-кодировщик [5]. Данный метод предполагает использование индивидуальной схемы распайки штатного соединительного кабеля пульта и камеры. Это позволяет перехватить «сырой» видеопоток до его обработки операционной системой пульта, минуя программные задержки. Данный способ многократно повысил стабильность трансляции на ПУ, исключив сбои, связанные с перегрузкой ОС пульта управления.

Доставленный на ПУ видеопоток должен быть интегрирован в единую картину поля боя. Для этого на рабочих местах должностных лиц и в ситуационных центрах организуются видеостены.

Реализован принцип единой среды обмена видеоданными, позволяющий выводить на видеостену одновременно до нескольких десятков потоков с различных источников (тепловизоры, оптико-электронные средства БПЛА, стационарные камеры) с возможностью динамического изменения сетки отображения. Взаимодействие

между операторами БПЛА, разведчиками и артиллеристами дублируется через защищенный текстовый мессенджер (сервер PostLink), что снижает голосовую нагрузку на каналы связи.

Для повышения живучести системы применяется метод удаленного агрегирования. Вместо того, чтобы размещать дорогостоящие серверы обработки видео в непосредственной близости от переднего края обороны (где они уязвимы для артиллерии и FPV-дронов противника), при планировании связи резервируется ресурс пропускной способности магистральных каналов для удаленного «вытягивания» видеопотоков на серверы, развернутые на удалении. Физические камеры и простые узлы ввода остаются на передовых позициях, а интеллектуальная обработка и хранение осуществляются в защищенных укрытиях.

Опыт противника в организации видеотрансляции

Анализ системы видеотрансляции ВСУ показывает их опору на коммерческие облачные и IT-решения. Совместная трансляция с камер осуществляется через стриминговый сервис Ukr.Stream (GlobalStreamingServices) [8]. Функционирование системы видеотрансляции осуществляется следующим образом: дежурный ситуационного центра через мессенджер Signal отправляет оператору камеры специальную ссылку. Оператор вводит ее как адрес RTMP (Real-TimeMessagingProtocol). Для демонстрации изображения на ПУ используют приложения GoogleMeet, Ochi, TeamViewer или Discord, транслируя экран планшета или телефона.

Такой подход позволяет ВСУ быстро масштабировать сеть и не зависеть от военной инфраструктуры, однако делает их каналы управления уязвимыми для кибератак, перехвата трафика и блокировки со стороны провайдеров. Российская группировка войск, напротив, опирается на суверенные, сегментированные и защищенные транспортные сети МО РФ, что обеспечивает устойчивость управления в условиях радиоэлектронного и огневого противодействия.

Перспективные направления развития систем видеотрансляции

Основные направления развития систем видеотрансляции делятся на две глобальные группы: внедрение искусственного интеллекта (ИИ) и обеспечение работы в условиях ограниченной пропускной способности.

1. Обеспечение работы в условиях ограниченной пропускной способности.

В направлении экономии пропускной способности компанией «Протей-СТ» развивается серверная программа «Видеопортал», позволяющая мультиплексировать несколько видеопотоков в один [9]. Также применяется продукт VideoGrace, позволяющий работать на тонких каналах, образованных посредством технологии ADSL.

Особую актуальность в условиях массового применения противником средств РЭБ приобретают исследования в области нейросетевого сжатия [10]. На базе Военной академии связи совместно со специалистами в 16 ЦНИИ был проведен эксперимент с применением кодера видеосжатия NeuroVideoCodec, разработанным СПбГУТИ им. проф. М. А. Бонч-Бруевича. Кодер обеспечивает передачу видеопотока по каналам связи низкого качества, образованным радиостанцией Р-187-П1 («Азарт») в режиме «Азарт-ШПС». Результаты показали, что при передаче через радиовставку в условиях помех восстановленное изображение имеет удовлетворительную степень разборчивости, достаточную для идентификации типов бронетехники и живой силы.

2. Интеграция систем искусственного интеллекта в разведывательные БПЛА.

Противник, обладая каналами связи с высокой пропускной способностью (в т. ч. за счет терминалов StarLink), идет по пути развития ИИ. Примером является мобильный разведывательный комплекс Palantir [11], интегрированный в систему управления ВСУ «Кропива». Российская Федерация также активно развивает данное направление, делая ставку на концепцию «интеллектуального края» (IntelligentEdge) [12].

Суть концепции заключается в переносе вычислительных мощностей и алгоритмов машинного зрения с облачных серверов пунктов управления непосредственно на борт разведывательных БПЛА (периферийные вычисления).

Это реализуется по следующим направлениям:

1. Автоматическое распознавание и классификация целей (ATR). Внедрение бортовых нейросетевых модулей (на базе отечественных процессоров, таких как «МодулТех» или специализированных FPGA-решений) позволяет БПЛА в автономном режиме сканировать местность, обнаруживать объекты, классифицировать их (отличать свою технику от техники противника, выявлять замаскированные огневые точки) и генерировать не «тяжелый» видеопоток, а легковесные телеметрические пакеты с координатами, курсом и типом цели. Видеопоток передается только в моменты

подтверждения цели или по запросу оператора, что снижает нагрузку на каналы связи на 80–90 %.

2. Интеллектуальная стабилизация и синтез изображения. Алгоритмы ИИ применяются для аппаратной компенсации дрожания камеры, удаления атмосферных помех (дым, туман, пыль) и синтеза сверхразрешения (super-resolution) [13]. Нейросети способны «достраивать» потерянные пиксели видеопотока, деградировавшего в результате воздействия средств РЭБ, обеспечивая оператору на ПУ картинку, субъективно превосходящую по качеству исходный сигнал.
3. Автоматизация доведения информации до огневых средств. Интеграция бортового ИИ БПЛА непосредственно с контурами АСУ тактического звена (аналоги систем типа «Стрелец» или «Кропива»). При обнаружении цели нейросеть автоматически формирует целеуказание, рассчитывает упреждение и передает его на огневые средства (артиллерию, РСЗО, ударные БПЛА) в обход визуального анализа оператором. Это сокращает цикл «разведка-огонь» с десятков минут до секунд.
4. Роевой интеллект и корреляция данных (SwarmIntelligence). При групповом применении разведывательных БПЛА алгоритмы ИИ позволяют объединять видеопотоки с нескольких аппаратов в единое панорамное или 3D-пространство. Нейросеть автоматически сшивает изображения с разных ракурсов, устраняет слепые зоны и обеспечивает непрерывное сопровождение движущейся техники или личного состава противника, даже если они временно перекрываются рельефом местности или зданиями с точки зрения одного конкретного БПЛА.
5. Предиктивная аналитика и выявление аномалий. ИИ способен анализировать видеопоток не только на предмет наличия техники, но и на выявление тактических аномалий: замаскированных линий связи, свежих следов гусеничной техники, признаков оборудования новых огневых позиций или минных полей. Система автоматически выделяет оператору на ПУ подозрительные участки местности, повышая эффективность инженерной разведки.

Таким образом, переход от парадигмы «передачи видео для просмотра человеком» к парадигме «передачи интеллектуально обработанных данных и целевых меток» является безальтернативным путем развития систем видеотрансляции в условиях тотального

доминирования средств РЭБ и дефицита радиочастотного ресурса.

Результаты и выводы

1. Проведен комплексный анализ опыта организации видеотрансляции в ГВ «Запад» и в Объединенной группировке войск. Систематизированы подходы к сегментации сетей передачи данных для тактических и оперативно-тактических БПЛА. Выполнен сравнительный анализ серверного и программного обеспечения («TrueConf», «Астра-С»), выявлены их тактико-технические ограничения и преимущества. Сформулированы принципиальные подходы к построению живучих систем видеотрансляции.
2. Доказано, что применение адаптивных алгоритмов сжатия (до 300 кбит/с) и нейросетевых кодеков (NeuroVideoCodec) позволяет поддерживать непрерывный контроль обстановки в условиях воздействия РЭБ и деградации каналов связи. Мультиплексирование потоков снижает нагрузку на магистральные каналы СПД на 30–40 %. Обоснована высокая эффективность переноса алгоритмов компьютерного зрения на борт БПЛА для радикального снижения требований к пропускной способности каналов связи и автоматизации цикла целеуказания.
3. Внедрение описанных способов организации видеотрансляции, включая аппаратный вывод сигнала через модули видеозахвата, использование видеостен на ПУ и экспериментальное подтверждение работы нейросетевых кодеков в радиосетях, подтвердило свою достоверность и эффективность в ходе проведения СВО.
4. Результаты относятся к области информационного обеспечения, защиты информации и построения телекоммуникационных систем в АСУ.
5. Для сокращения потерь в технических средствах и в целях введения противника в заблуждение, помимо мероприятий маскировки, должностным лицам по связи при планировании необходимо внедрять практику резервирования ресурса пропускной способности для удаленного подключения систем видеонаблюдения к серверам ПУ.
6. В части перспективного развития необходимо форсировать работы по оснащению разведывательных БПЛА отечественными бортовыми вычислителями с алгоритмами машинного зрения для реализации концепции «интеллектуального края».

Литература

1. Сидоров В. Н. Архитектура защищенных сетей передачи данных для систем управления беспилотными летательными аппаратами // Вопросы радиоэлектроники. – 2022. – Т. 12. – № 3. – С. 112–120.
2. Николаев П. С. Тактика применения стационарных и мобильных комплексов видеонаблюдения в общевойсковом бою // Военная мысль. – 2023. – № 8. – С. 56–64.
3. Федоров И. В. Обеспечение информационной безопасности систем видеотрансляции в открытом сегменте СПД // Защита информации. Конфидент. – 2023. – № 3. – С. 44–50.
4. Васильев Г. Р. Сравнительный анализ программных комплексов агрегации видеоданных для нужд Министерства обороны РФ // Специальная техника. – 2023. – № 5. – С. 15–22.
5. Орлов М. Д. Эргономика рабочих мест операторов БПЛА на распределенных пунктах управления // Системы управления, связи и безопасности. – 2022. – № 2. – С. 34–41.
6. Иванов С. В., Петров А. К. Методы адаптивного сжатия видеопотоков в тактических сетях передачи данных военного назначения // Вестник связи. – 2021. – № 4. – С. 45–52.
7. Смирнов А. Л. Мультиплексирование видеопотоков в каналах ограниченной пропускной способности // Труды Академии связи. – 2022. – № 14. – С. 201–210.
8. Григорьев С. А. Применение терминалов спутниковой связи и коммерческих стриминговых сервисов в современных локальных конфликтах // Зарубежное военное обозрение. – 2023. – № 11. – С. 45–51.
9. Кузнецов А. А. Применение нейросетевых алгоритмов для обработки и передачи видеоинформации в условиях радиоэлектронного подавления // Информационные технологии и вычислительные системы. – 2023. – № 1. – С. 78–89.
10. Соколов А. В., Лебедев А. В. Бортовые системы компьютерного зрения для беспилотных летательных аппаратов тактического звена // Вестник Конструкторского бюро приборостроения. – 2023. – № 6. – С. 88–95.
11. Михайлов Д. С. Интеграция алгоритмов машинного обучения в контуры управления огнем артиллерийских подразделений // Военно-технический журнал. – 2024. – № 2. – С. 34–42.
12. Петров И. И. Концепция периферийных вычислений (EdgeComputing) в тактическом звене управления // Информатизация и защита информации. – 2023. – № 2. – С. 33–40.
13. Lovtsov D. A., Gavrilov D. A. Automated special purpose optical electronic system's functional diagnosis // Proceedings of International Seminar on Electron Devices Design and Production, SED-2019. Prague, Czech Republic: IEEE, 2019. – Pp. 70–73.

METHODS OF ORGANIZING THE FUNCTIONING OF A VIDEO STREAMING SYSTEM IN MODERN COMBAT CONDITIONS

Lebedev P. V.³, Zhivodernikov A. Yu.⁴

Keywords: video transmission, confidential network segment, neural network compression, information security, bandwidth of communication channels, situational awareness, peripheral computing, computer vision, network segmentation, multiplexing, electronic warfare, unmanned aerial vehicles, automated targeting.

Abstract

Purpose of work: the purpose of the work is to fundamentally analyze, systematize, and develop conceptual approaches to organizing the functioning of video streaming and surveillance systems, as well as to substantiate the ways of integrating artificial intelligence systems into the troop control loop in real-time during high-intensity conflicts.

Research method: the research method includes a systems analysis of data transmission network architectures, structural-functional modeling of video streaming system components, a comparative assessment of software complexes for video stream aggregation, and an investigation of adaptive compression, multiplexing, and onboard neural network processing methods for video information under conditions of bandwidth deficit and electronic warfare impact.

Results of the study: the experience of the Grouping of Forces «West» in integrating over 100 stationary complexes and hundreds of tactical UAVs into a single information space is generalized. Critical dependencies of command quality on the bandwidth of communication channels are identified. The effectiveness of using domestic software solutions («Astra-S», «TrueConf») with various encoding algorithms is proven. An experiment with the Neuro Video Codec in «Azart» radio networks was conducted, confirming the possibility of transmitting intelligible video over low-quality channels. The necessity of transitioning from physical server masking to distributed bandwidth allocation and the implementation of onboard computer vision systems on reconnaissance UAVs to reduce the load on communication channels and automate target designation is substantiated.

Scientific novelty: the scientific novelty lies in the development of a comprehensive conceptual approach to organizing video streaming, combining strict segmentation of data transmission networks, adaptive stream multiplexing,

³ Pavel V. Lebedev, Ph.D. of Technical Sciences, Associate Professor of the Department of Communication Networks and Switching Systems at the Military Academy of Communications named after Marshal of the Soviet Union S. M. Budyonny, St. Petersburg, Russia. E-mail: spirit-angel@yandex.ru

⁴ Alexander Yu. Zhivodernikov, Ph.D. of Technical Sciences, Senior Lecturer of the Department of Communication Networks and Switching Systems at the Military Academy of Communications named after Marshal of the Soviet Union S. M. Budyonny, St. Petersburg, Russia. E-mail: sabir.81@mail.ru

the use of neural network compression algorithms to overcome the consequences of enemy electronic warfare, as well as in the formalization of principles for integrating artificial intelligence systems at peripheral nodes (onboard UAVs) to implement the «intelligent edge» concept in the tactical link.

References

1. Sidorov V. N. Arhitektura zashchishchennykh setej peredachi dannykh dlya sistem upravleniya bespilotnymi letatel'nyimi apparatami // *Voprosy radioelektroniki*. – 2022. – V. 12. – No. 3. – Pp. 112–120.
2. Nikolaev P. S. Taktika primeneniya stacionarnykh i mobil'nykh kompleksov videonablyudeniya v obshchevojskovom boyu // *Voennaya mysl'*. – 2023. – No. 8. – Pp. 56–64.
3. Fedorov I. V. Obespechenie informacionnoj bezopasnosti sistem videotranslyacii v otkrytom segmente SPD // *Zashchita informacii. Konfident.* – 2023. – No. 3. – Pp. 44–50.
4. Vasil'ev G. R. Sravnitel'nyj analiz programmnykh kompleksov agregacii videodannykh dlya nuzhd Ministerstva oborony RF // *Special'naya tekhnika*. – 2023. – No. 5. – Pp. 15–22.
5. Orlov M. D. Ehrgonomika rabochih mest operatorov BpLA na raspredelennykh punktakh upravleniya // *Sistemy upravleniya, svyazi i bezopasnosti*. – 2022. – No. 2. – Pp. 34–41.
6. Ivanov S. V., Petrov A. K. Metody adaptivnogo szhatiya videopotokov v takticheskikh setyah peredachi dannykh voennogo naznacheniya // *Vestnik svyazi*. – 2021. – No. 4. – Pp. 45–52.
7. Smirnov A. L. Mul'tipleksirovanie videopotokov v kanalah ogranichennoj propusknokh sposobnostei // *Trudy Akademii svyazi*. – 2022. – No. 14. – Pp. 201–210.
8. Grigor'ev S. A. Primenenie terminalov sputnikovoy svyazi i kommercheskikh strimingovykh servisov v sovremennykh lokal'nykh konfliktakh // *Zarubezhnoe voennoe obozrenie*. – 2023. – No. 11. – Pp. 45–51.
9. Kuznecov A. A. Primenenie nejrosetevykh algoritmov dlya obrabotki i peredachi videoinformacii v usloviyakh radioelektronnogo podavleniya // *Informacionnye tekhnologii i vychislitel'nye sistemy*. – 2023. – No. 1. – Pp. 78–89.
10. Sokolov A. V., Lebedev A. V. Bortovye sistemy komp'yuternogo zreniya dlya bespilotnykh letatel'nykh apparatov takticheskogo zvena // *Vestnik Konstruktorskogo byuro priborostroeniya*. – 2023. – No. 6. – Pp. 88–95.
11. Mihajlov D. S. Integraciya algoritmov mashinnogo obucheniya v kontury upravleniya ognem artillerijskikh podrazdelenij // *Voенно-tekhnicheskij zhurnal*. – 2024. – No. 2. – Pp. 34–42.
12. Petrov I. I. Konceptiya periferijnykh vychislenij (EdgeComputing) v takticheskom zvене upravleniya // *Informatizaciya i zashchita informacii*. – 2023. – No. 2. – Pp. 33–40.
13. Lovtsov D. A., Gavrilov D. A. Automated special purpose optical electronic system's functional diagnosis // *Proceedings of International Seminar on Electron Devices Design and Production, SED-2019. Prague, Czech Republic: IEEE, 2019.* – Pp. 70–73.



МОДЕЛИРОВАНИЕ ЗАДАЧИ МАРШРУТИЗАЦИИ В СЕТИ ПЕРЕДАЧИ ДАННЫХ ПО ПОКАЗАТЕЛЮ ВЕРОЯТНОСТИ СВОЕВРЕМЕННОЙ ДОСТАВКИ СООБЩЕНИЙ

Курашев З. В.¹

DOI:10.21681/3034-4050-2026-5-77-82

Ключевые слова: маршрутизация, алгоритм оптимизации, показатель эффективности, вероятность своевременной доставки пакетов.

Аннотация

Цель исследования заключается в анализе и разработке модели маршрутизации в сетях передачи данных, основанной на максимизации вероятности своевременной доставки сообщений, отличающейся от известных учетом времени задержки не только на линиях связи, но и в узлах коммутации.

Методы исследования: в работе использованы методы теории графов, теории вероятностей, математического моделирования. Сеть передачи данных представляется в виде ориентированного графа, в котором узлы соответствуют маршрутизаторам или коммутаторам, а ребра – каналам (линиям) связи. Для описания времени передачи по каналам используются случайные величины и вероятностные распределения задержек. В качестве критерия оптимизации применяется вероятность доставки сообщения в пределах предельно допустимого времени.

Результаты: в результате исследования сформирована математическая модель маршрутизации, в которой выбор пути осуществляется по критерию максимальной вероятности своевременной доставки сообщения. Получены аналитические соотношения для вычисления вероятности выполнения временного ограничения с учетом случайного характера задержек на узлах коммутации и каналах связи. Разработан алгоритм оптимизации маршрута, позволяющий выбирать путь, обеспечивающий наилучшее значение вероятностного критерия.

Практическая ценность: полученные результаты могут быть использованы при разработке адаптивных алгоритмов маршрутизации для сетей, в которых критически важна доставка сообщений в пределах установленного времени.

Введение

В современных сетях передачи данных, особенно в системах связи, функционирующих в условиях реального времени, важна не только доставка сообщения, но и его поступление в пределах предельно допустимого времени. Классические алгоритмы маршрутизации, как правило, ориентированы на минимизацию числа скачков, средней задержки или стоимости передачи, однако такие подходы не всегда обеспечивают высокую вероятность своевременной доставки сообщений в условиях случайных задержек, перегрузок и потерь пакетов. В связи с этим возрастает необходимость разработки и исследования моделей маршрутизации, основанных на вероятностной оценке выполнения временных ограничений, что позволяет повысить эффективность функционирования сетей в условиях неопределенности.

Современные сети передачи данных используются в различных прикладных областях, включая телекоммуникационные сети, беспроводные сенсорные сети, системы реального времени. В таких условиях особое значение приобретает

не только сам факт доставки сообщения, но и соблюдение требований по времени его передачи. Для многих приложений сообщение, поступившее с опозданием, теряет свою практическую ценность, даже если в конечном итоге было успешно доставлено.

Классические алгоритмы маршрутизации в основном ориентированы на такие критерии, как минимальное число переходов [1], минимальная средняя задержка [2], минимальная стоимость передачи [3] или максимальная надежность канала [4–5]. Однако в условиях случайного характера сетевых задержек, потерь пакетов, перегрузки узлов и изменяющихся параметров каналов связи такие подходы не всегда позволяют обеспечить высокую вероятность своевременной доставки сообщений [6–10]. В результате возникает необходимость применения новых методов маршрутизации, учитывающих вероятностную природу процессов передачи данных в сети.

Одним из перспективных направлений является моделирование маршрутизации на основе вероятности своевременной доставки

¹ Курашев Заур Валерьевич, кандидат технических наук, начальник научно-исследовательской лаборатории ФГБУ «16 Центральный научно-исследовательский испытательный институт» Минобороны России, Московская область, г. Мытищи. E-mail: ZKing07198@xmail.ru

сообщений. В этом случае маршрут оценивается не только по усредненным характеристикам, но и по вероятности того, что сообщение будет доставлено в пределах предельно допустимого времени. Такой подход особенно актуален для сетей, функционирующих в условиях неопределенности и предъявляющих повышенные требования к качеству обслуживания.

В современных сетях передачи данных классический выбор маршрута по критерию минимального среднего времени задержки уже не всегда обеспечивает требуемое качество обслуживания. Для систем реального времени существенно не просто уменьшить среднюю задержку, а максимизировать вероятность того, что сообщение будет доставлено за время не превышающее допустимое. Именно поэтому в моделях маршрутизации все чаще используется вероятностный критерий своевременной доставки:

$$P\{T_3 \leq T_{\text{доп}}\}, \quad (1)$$

где T_3 – время задержки информационного пакета, а $T_{\text{доп}}$ – допустимое предельное время задержки.

Такой подход заключается в том, что маршрут оценивается не по одному усредненному показателю, а по распределению задержек на каждом канале и по их совокупному влиянию на итоговую вероятность доставки в срок. Это важно, поскольку маршрут с меньшей средней задержкой может иметь большую дисперсию и, следовательно, чаще нарушать временные ограничения, чем более «стабильный» путь с немного большим средним временем передачи.

При вероятностном моделировании сеть обычно представляют ориентированным графом $G = (V, E)$, где вершины соответствуют узлам коммутации (маршрутизации), а ребра – каналам (линиям) связи. Каждому ребру сопоставляются случайные параметры: задержка передачи, вероятность потери пакета, доступная пропускная способность и иногда стоимость использования канала. Тогда задача маршрутизации формулируется как поиск маршрута μ , максимизирующего вероятность выполнения ограничения

$$\max_{\mu \in M(s,d)} P\{T_3 \leq T_{\text{доп}}\}, \quad (2)$$

где $M(s,d)$ – множество путей между источником s и получателем d .

Для каждой дуги $e = (i,j) \in E$ задаются следующие параметры: X_{ij} – случайная величина задержки на канале; q_{ij} – вероятность успешной передачи за одну попытку; $p_{ij} = 1 - q_{ij}$ – вероятность потери; c_{ij} – стоимость использования канала; b_{ij} – доступная пропускная способность.

Для пары узлов «источник – получатель» (s,d) требуется выбрать маршрут $\mu \in M_{sd}$, обеспечивающий максимальную вероятность своевременной доставки сообщения при заданном $T_{\text{доп}}$.

Если маршрут μ состоит из n последовательно проходящих каналов, то задержка определяется суммой случайных задержек на отдельных участках:

$$T_3 = \sum_{k=1}^n X_k, \quad (3)$$

где X_k – случайная величина задержки на узле коммутации.

Если задержки на участках считаются независимыми случайными величинами, то время задержки информационного пакета на маршруте определяется как сумма задержек на его узлах и ребрах. В этом случае вероятность своевременной доставки может быть получена через свертку распределений или через аппроксимации. В более общих моделях учитывают не только задержку, но и вероятность успешной передачи на каждом канале, что позволяет оценивать уже не просто временную, а совместную надежно-временно-временную характеристику маршрута.

При предположении независимости задержек в узлах коммутации и каналах связи получаем распределение суммы случайных величин. Для односкачковой задержки принимается экспоненциальное распределение, а для суммы неодинаковых экспоненциальных величин используется гиперэкспоненциальное или нормальное (гауссовское) распределение.

Если

$$X_k \sim \text{Exp}(\lambda_k), \quad (4)$$

то

$$E[X_k] = \frac{1}{\lambda_k}, \quad \text{Var}(X_k) = \frac{1}{\lambda_k^2}. \quad (5)$$

Тогда для маршрута:

$$E[T_\mu] = \sum_{k=1}^n \frac{1}{\lambda_k}; \quad (6)$$

$$\text{Var}(T_\mu) = \sum_{k=1}^n \frac{1}{\lambda_k^2}. \quad (7)$$

Эти выражения удобны для сравнения маршрутов не только по среднему времени, но и по устойчивости задержки. Именно различие по дисперсии объясняет, почему маршрут с меньшим средним временем может проигрывать по вероятности своевременной доставки.

Вероятность выполнения предельно допустимого времени доставки сообщения от источника до получателя для маршрута μ определяется как:

$$P_d(T_d) = P\{T_3 \leq D\} = F_{T_3}(T_{\text{доп}}), \quad (8)$$

где $F_{T_3}(T_{\text{доп}})$ – функция распределения сквозной задержки.

Для гиперэкспоненциального случая:

$$P_d(T_d) = F_{T_3}(T_{\text{доп}}) = 1 - \sum_{i=1}^n e^{-\lambda_i T_d} \prod_{\substack{j=1 \\ j \neq i}}^n \frac{\lambda_j}{\lambda_j - \lambda_i}. \quad (9)$$

Учитывая, что время доставки сообщения соответствует максимальному времени доставки пакета из состава пакетов этого сообщения, то можно записать соотношение $P\{t_c \leq \tau\} = P^l\{t_n \leq \tau\}$ где l – длина сообщения (выраженная в числе пакетов). Отсюда следует, что в рамках рассматриваемых допущений требования к времени доставки сообщения можно преобразовать к времени доставки пакета [33]. С учётом этого в качестве показателя принимается вероятность своевременной доставки информационных пакетов. Распределение (9) дает возможность вычислять вероятность доставки пакета до момента предельно допустимого времени доставки сообщения от источника до получателя и использовать ее как целевую метрику при выборе маршрута.

Алгоритм оптимизации

Шаг 1. Ввод исходных данных

Задаются: топология сети $G = (V, E)$; источник s и приемник d ; распределения задержек на узлах коммутации и каналах (линиях) связи; ограничения по стоимости, числу переходов или пропускной способности.

Шаг 2. Формирование множества допустимых маршрутов

Строится множество:

$$M_{sd} = \{\mu_1, \mu_2, \dots, \mu_m\}.$$

На практике все возможные маршруты обычно не перебираются полностью, потому что число путей быстро растет. Поэтому используют либо ограничение на длину маршрута, либо поиск только k лучших, либо динамическое программирование. Работы по этой теме прямо рассматривают локальные и итерационные алгоритмы, которые избегают полного перебора и постепенно улучшают таблицы маршрутизации.

Шаг 3. Вычисление задержки для каждого маршрута

Для каждого маршрута μ строится распределение задержки по формуле (9).

Если предполагается, что на каждом ребре задержка экспоненциальна, формула (4) то для маршрута получаем:

$$E[T_\mu] = \sum_{e \in \mu} \frac{1}{\lambda_e}, \quad \text{Var}(T_\mu) = \sum_{e \in \mu} \frac{1}{\lambda_e^2}.$$

Шаг 4. Вычисление вероятности своевременной доставки

Для каждого маршрута вычисляется

$$P_d(T_d) = P\{T_3 \leq T_d\} = F_{T_3}(T_d),$$

если задержки гиперэкспоненциальны, вероятность можно записать как (9). Если аналитическое вычисление затруднено, используется имитационная оценка:

$$\hat{P}_d(T_d) = \frac{N_\mu^{\text{ontime}}}{N},$$

где N – общее число прогонов, а N_μ^{ontime} – число успешных доставок информационных пакетов по маршрутам μ .

С точки зрения имитационного моделирования исследование алгоритмов маршрутизации обычно включает построение сетевой топологии, задание вероятностных законов для задержек и потерь, генерацию потоков сообщений и сравнение алгоритмов по нескольким метрикам: вероятности своевременной доставки, средней задержке, доле потерянных пакетов, нагрузке на сеть и устойчивости при росте трафика.

Шаг 5. Проверка ограничений

Для каждого маршрута проверяются ограничения:

$$C_\mu = \sum_{e \in \mu} c_e \leq C_{\max},$$

$$|\mu| \leq H_{\max},$$

$$P_d(T_d) \geq P_{\min}.$$

Если маршрут не удовлетворяет ограничениям, он исключается из рассмотрения.

Шаг 6. Выбор оптимального маршрута

Среди допустимых маршрутов выбирается маршрут с максимальным значением целевой функции:

$$\mu^* = \arg \max_{\mu \in M_{sd}} F(\mu).$$

Результат – это маршрут, который дает наибольшую вероятность своевременной доставки сообщения.

Алгоритм оптимизации маршрутизации на основе вероятности своевременной доставки сообщений состоит в последовательной оценке всех допустимых маршрутов между узлами источника и назначения, вычислении для каждого маршрута распределения задержки, определении вероятности выполнения ограничения и последующем выборе маршрута, максимизирующего целевую функцию.

Для сравнения возьмем иллюстративный расчетный пример.

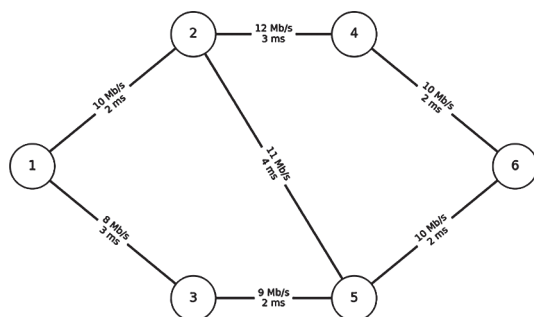


Рис. 1. Пример сети передачи данных для задачи маршрутизации

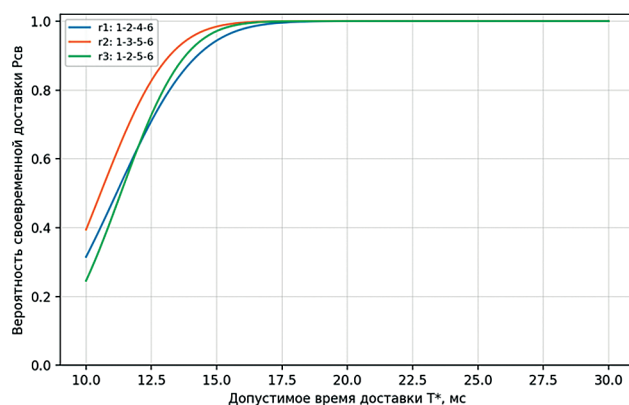


Рис. 2. Зависимость вероятности своевременной доставки от допустимого порога времени

Рассмотрим сеть из 6 узлов и 3 альтернативных маршрутов от узла 1 к узлу 6.

Для каждого канала заданы задержка распространения и интенсивность обслуживания. Порог своевременной доставки принят 18 мс.

Маршрут	Состав маршрута	Параметры участков
r1	1–2–4–6	(2 мс; 0.90), (3 мс; 1.10), (2 мс; 1.00)
r2	1–3–5–6	(3 мс; 1.20), (2 мс; 0.95), (2 мс; 1.05)
r3	1–2–5–6	(2 мс; 0.90), (4 мс; 1.15), (2 мс; 1.05)

На примере для каждого участка указаны пары задержки в миллисекундах и интенсивности обслуживания в пак/мс.

Заключение

Проведённый анализ показывает, что классические алгоритмы маршрутизации эффективны при решении задач связности и базовой оптимизации, однако не всегда адекватны для обслуживания потоков с жёсткими временными ограничениями. При переходе от критерия кратчайшего пути к критерию вероятности своевременной доставки возникает новая, более прикладная постановка задачи. Она позволяет учитывать случайный характер задержек, потерь и перегрузок на маршрутах прохождения информационных пакетов.

Преимущество вероятностного подхода состоит в том, что он лучше отражает реальную природу сети как случайной среды. Вместо жесткого предположения о фиксированных задержках он позволяет оценивать риск нарушения временных требований и выбирать маршрут с учетом компромисса между стоимостью, надежностью и временной устойчивостью. Это особенно важно для управления на сетях, где ценность сообщения резко падает после истечения допустимого времени доставки.

Таким образом, моделирование маршрутизации на основе вероятности своевременной доставки сообщений представляет собой развитие классических методов QoS-маршрутизации. В таких моделях ключевым объектом оптимизации становится не просто путь с минимальной задержкой, а путь с максимальной вероятностью удовлетворения временных ограничений. Дальнейшее развитие этой области связано с применением стохастических моделей для адаптивного выбора маршрутов в условиях изменяющейся нагрузки и нестабильных каналов связи.

Литература

- Guoqing Tian, Yanmei Jia, Suzhi Cao, Xiaohua Wang, Hongen Zhong An Improved Minimum Hop Count Routing for LEO Mega-Constellations // ICNCC '23: Proceedings of the 2023 12th International Conference on Networks, Communication and Computing. – 2024. – Pp.22–31.
- Fu X., Modiano E. A Learning Approach to Minimum Delay Routing in Stochastic Queueing Networks // IEEE INFOCOM 2023 – IEEE Conference on Computer Communications. – DOI: 10.1109/INFOCOM53939.2023.10229039.
- Swaminathan A., Chaba M., Sharma D. K., Ghosh U. GraphNET: Graph Neural Networks for Routing Optimization in Software Defined Networks // Computer Communications. – 2021. – Vol. 178. – Pp. 169–182. – DOI: 10.1016/j.comcom.2021.07.025.
- Liang Q., Liu X., Zhang Y. et al. A Dynamic Source Routing Protocol Based on Path Reliability and Monitoring Repair Mechanism // – 2021. – DOI:10.1371/journal.pone.0251548.
- Lyu J. et al. Reliable Route Selection for Wireless Sensor Networks. – 2021. – URL: <https://doi.org/10.3390/s21217254>.
- Чуднов А. М., Кирик Д. И., Курашев З. В. Оптимизация распределения информационных потоков в информационной системе по показателю вероятности своевременной доставки сообщений // Радиотехнические и телекоммуникационные системы. – 2017. – № 2. – С. 41–49. – EDN: ZCSAYZ.

7. Чуднов А. М., Курашев З. В. Принципы формирования маршрутных таблиц на основе оптимизации распределения потоков в сети передачи данных // Научные технологии в космических исследованиях Земли. – 2017. – Т.9. – № 6. – С. 46–51. – EDN: YPPYSR.
8. Чуднов А. М., Путилин А. Н., Попов А. И. Комплексное управление маршрутизацией пакетов и режимами работы радиосредств в неоднородной сети передачи данных // Радиотехнические и телекоммуникационные системы. – 2019. – № 1. – С. 46–56. – EDN: SFUSML.
9. Дымарский Я. С., Крутикова Н. П., Яновский Г. Г. Управление сетями связи: принципы, протоколы, прикладные задачи. М.: Связь и бизнес. – 2003. – 384 с. – ISBN 5-93533-014-8.
10. Чуднов А. М. Методика анализа вероятностно-временных характеристик обмена сообщениями в комплексе беспилотных летательных аппаратов / А. М. Чуднов, О. А. Губская, Я. В. Кичко // Известия Тульского государственного университета. Технические науки. – 2021. – № 11. – С. 117–124. – DOI: 10.24412/2071-6168-2021-11-117-124.

MODELING OF THE ROUTING PROBLEM IN THE DATA TRANSMISSION NETWORK BY THE PROBABILITY OF TIMELY DELIVERY OF MESSAGES

Kurashev Z. V.²

Keywords: routing, optimization algorithm, efficiency indicator, probability of timely delivery of packets.

Abstract

The purpose of the study is to analyze and develop a routing model in data transmission networks based on maximizing the probability of timely delivery of messages, which differs from the known ones by considering the delay time not only on communication lines, but also in switching nodes.

Research methods: the author uses the methods of graph theory, probability theory, and mathematical modeling. The data transmission network is represented as a directed graph in which nodes correspond to routers or switches, and edges correspond to communication channels (lines). Random variables and probabilistic delays distributions are used to describe the transmission time through channels.

Results: as a result of the study, a mathematical routing model was formed, in which the path is selected according to the criterion of the maximum probability of timely delivery of the message. Analytical ratios were obtained to calculate the probability of meeting the time limit, considering the random nature of delays at switching nodes and communication channels. An algorithm for route optimization was developed, which allows you to choose the path that provides the best value of the probabilistic criterion.

Practical value: the results obtained can be used in the development of adaptive routing algorithms for networks in which the delivery of messages within the set time is critical.

References

1. Guoqing Tian, Yanmei Jia, Suzhi Cao, Xiaohua Wang, Hongen Zhong An Improved Minimum Hop Count Routing for LEO Mega-Constellations // ICNCC '23: Proceedings of the 2023 12th International Conference on Networks, Communication and Computing. – 2024. – Pp. 22–31.
2. Fu X., Modiano E. A Learning Approach to Minimum Delay Routing in Stochastic Queueing Networks // IEEE INFOCOM 2023 – IEEE Conference on Computer Communications. – DOI: 10.1109/INFOCOM53939.2023.10229039.
3. Swaminathan A., Chaba M., Sharma D. K., Ghosh U. GraphNET: Graph Neural Networks for Routing Optimization in Software Defined Networks // Computer Communications. – 2021. – Vol. 178. – Pp. 169–182. – DOI: 10.1016/j.comcom.2021.07.025.
4. Liang Q., Liu X., Zhang Y. et al. A Dynamic Source Routing Protocol Based on Path Reliability and Monitoring Repair Mechanism // – 2021. – DOI:10.1371/journal.pone.0251548.
5. Lyu J. et al. Reliable Route Selection for Wireless Sensor Networks. 2021. – URL: <https://doi.org/10.3390/s21217254>.
6. Chudnov A. M., Kirik D. I., Kurashev Z. V. Optimizaciya raspredeleniya informacionnyh potokov v informacionnoj sisteme po pokazatelyu veroyatnosti svoevremennoj dostavki soobshchenij // Radiotekhnicheskie i telekommunikacionnye sistemy. – 2017. – No. 2. – Pp. 41–49. – EDN: ZCSAYZ.
7. Chudnov A. M., Kurashev Z. V. Principy formirovaniya marshrutnyh tablic na osnove optimizacii raspredeleniya potokov v seti peredachi dannyh // Naukoemkie tehnologii v kosmicheskikh issledovaniyah Zemli. – 2017. – V. 9. – No. 6. – Pp. 46–51. – EDN: YPPYSR.
8. Chudnov A. M., Putilin A. N., Popov A. I. Kompleksnoe upravlenie marshrutizaciej paketov i rezhimami raboty radiosredstv v neodnorodnoj seti peredachi dannyh // Radiotekhnicheskie i telekommunikacionnye sistemy. – 2019. – No. 1. – Pp. 46–56. – EDN: SFUSML.

² Zaur V. Kurashev, Ph.D. of Technical Sciences, Head of the Research Laboratory of the 16th Central Research and Testing Institute of the Ministry of Defense of the Russian Federation. Moscow Region, Mytishchi, Russia. E-mail: Zking07198@gmail.ru

9. Dymarskij Ya. S., Krutikova N. P., Yanovskij G. G. Upravlenie setyami svyazi: principy, protokoly, prikladnye zadachi. M.: Svyaz' i biznes. – 2003. – 384 p. – ISBN 5-93533-014-8.
10. Chudnov A. M. Metodika analiza veroyatnostno-vremennyh harakteristik obmena soobshcheniyami v komplekse bespilotnyh letatel'nyh apparatov / A. M. Chudnov, O. A. Gubskaya, Ya. V. Kichko // Izvestiya Tul'skogo gosudarstvennogo universiteta. Tehnicheskie nauki. – 2021. – No. 11. – Pp. 117–124. – DOI: 10.24412/2071-6168-2021-11-117-124.



ПАРАМЕТРИЧЕСКИЙ СИНТЕЗ МНОГОВИБРАТОРНОЙ ПОДЗЕМНОЙ АНТЕННЫ, ФУНКЦИОНИРУЮЩЕЙ В ДИССИПАТИВНЫХ СЛОИСТЫХ СРЕДАХ

Леонюк А. С.¹, Юртаев А. С.², Исмаил М. М.³

DOI:10.21681/3034-4050-2026-5-83-90

Ключевые слова: численное моделирование, гибридный алгоритм, глобальная оптимизация, электродинамическое ядро, геофизические параметры, защитная конструкция, частотный диапазон, алгоритм роя частиц, эффективность излучения, дифракционные искажения.

Аннотация

Цель: разработка комплексной модели многовибраторной подземной антенны, функционирующей в диссипативных слоистых средах, с учётом реальных геофизических параметров, и создание алгоритма автоматического расчёта габаритов защитных конструкций.

Метод: использован гибридный алгоритм параметрической оптимизации, интегрирующий электродинамическое ядро, реализованное методом конечных разностей во временной области (FDTD), с методом роя частиц (PSO). Расчёты выполнены для частотного диапазона 4–30 МГц с учётом двухслойной модели подстилающего объёма (песок/щебень), параметры которой обоснованы геофизическими данными для района Хомсской впадины.

Результаты: получены оптимальные геометрические параметры антенны, обеспечивающие на частоте 15 МГц коэффициент усиления 4,4 дБи и активное сопротивление 47,2 Ом, что даёт энергетический выигрыш 3,2 дБ по сравнению с эталонным полуволновым диполем. Разработан и верифицирован алгоритм автоматического расчёта размеров пластикового бокса и котлована, основанный на длине волны и оптимизированных размерах антенны.

Научная новизна: впервые предложена комплексная модель, связывающая геофизические данные реального региона с численным электродинамическим моделированием и глобальной оптимизацией; впервые реализован автоматический расчёт защитных конструкций на основе анализа дифракционных искажений в ближней зоне.

Введение

Интерес к антеннам, размещённым на некоторой глубине в диссипативной среде (среде с потерями), сохраняется на протяжении десятилетий. Данные антенны известны достаточно длительное время, их исследованию были посвящены обширные работы отечественных и зарубежных специалистов. Однако эффективность таких антенн остаётся довольно низкой по сравнению с антеннами, расположенными в воздушном пространстве, из-за влияния среды с потерями на их характеристики.

С появлением современных численных методов электродинамики, развитием алгоритмов и программ, основанных на них, встал вопрос о возможности расчёта подземных антенн (ПА) данными методами, хорошо зарекомендовавшими себя при расчётах антенн в свободном пространстве. Численные методы позволяют моделировать излучатели произвольной формы. Нами были найдены решения ряда задач по возможности моделирования ПА методом

конечных элементов (МКЭ) [1] и методом конечных разностей во временной области (FDTD) [2] с использованием искусственно вводимых поглощающих слоёв (PML) [3]. Реализованная возможность применения современных численных методов для расчёта ПА позволила начать работу по исследованию путей увеличения их эффективности без проведения трудоёмких и дорогих экспериментов [4].

В отличие от известных работ, в данной статье особое внимание уделено не только анализу одиночных вибраторов, но и разработке комплексной модели многовибраторной антенны с учётом реальной слоистой структуры подстилающего объёма (на примере района Хомсской впадины) [11]. Кроме того, впервые предложен алгоритм автоматического расчёта габаритов пластикового защитного бокса и котлована, основанный на длине волны и оптимизированных размерах антенны, что позволяет перейти от теоретических исследований к инженерной реализации.

¹ Леонюк Антон Сергеевич, доцент кафедры Военной академии связи им. С. М. Буденного, Санкт-Петербург, Россия. E-mail: leonuck@yandex.ru

² Юртаев Антон Сергеевич, адъюнкт кафедры Военной академии связи им. С. М. Буденного, Санкт-Петербург, Россия. E-mail: ant8720@yandex.ru

³ Исмаил Мохаммад, адъюнкт кафедры Военной академии связи им. С. М. Буденного, Санкт-Петербург, Россия. E-mail: mohammad.esmaael.2024@gmail.com

1. Геометрическая и физическая модель антенны и окружающей среды

Для увеличения эффективности ПА, закладываемых в грунт с различными электрическими параметрами, целесообразно использовать многовибраторные структуры. В качестве базовой конфигурации выбран горизонтальный симметричный вибратор, дополненный первичными и вторичными ответвлениями. Такая топология позволяет увеличить эффективную длину антенны и перераспределить поверхностные токи, что критически важно для повышения излучательной способности в среде с потерями.

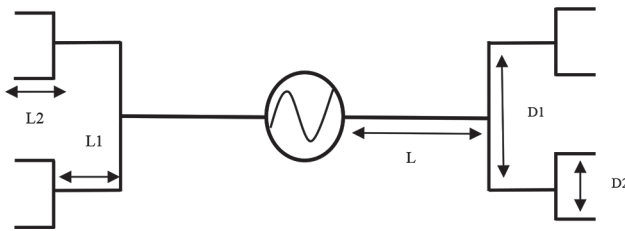


Рис. 1. Схема многовибраторной антенны с обозначениями L , L_1 , L_2 , D_1 , D_2

Независимыми переменными проектирования являются девять параметров:

- L – длина основного диполя (м);
- N_1 , L_1 , D_1 – количество, длина (м) и шаг (м) первичных ответвлений;
- N_2 , L_2 , D_2 – количество, длина (м) и шаг (м) вторичных ответвлений;
- индексы материала (медь, алюминий, серебро, золото, сталь) и покрытия (без покрытия, серебряное, золотое, оловянное).

Параметры слоёв обоснованы результатами численного моделирования и геофизических измерений. В ходе анализа физико-географических условий района Хомсской впадины (Сирия) установлено, что подстилающий объём характеризуется ярко выраженной слоистостью. Для целей электродинамического моделирования принята двухслойная модель (рис. 2):

- Верхний слой (песок): толщина 0,5 м, относительная диэлектрическая проницаемость $\epsilon_{r1} = 4$, удельная проводимость $\sigma_1 = 10^{-4}$ См/м.
- Нижний слой (щебень/гравий): полубесконечный, $\epsilon_{r1} = 5$, $\sigma_2 = 5 \times 10^{-4}$ См/м.

Обоснование выбора модели

Следует отметить, что реальный геологический разрез Хомсской впадины характеризуется значительным разнообразием: помимо песков и гравия, встречаются прослои глин, суглинков, известняков и базальтов. Однако для инженерных расчётов радиотехнических систем общепринятой практикой является использование упрощённых моделей, отражающих усреднённые электрические свойства верхней части разреза. Выбранная двухслойная модель (песок/гравий) является репрезентативной для данного региона, поскольку именно эти породы составляют основную мощность аллювиальных отложений, а их электрические параметры ($\epsilon_r = 4-5$, $\sigma_r = 10^{-4} - 5 \times 10^{-4}$ См/м.) являются наиболее характерными для сухих и полусухих районов Восточного Средиземноморья. Данный подход согласуется с методикой, принятой в работах, где также используются усреднённые модели для расчёта характеристик подземных антенн.

Антенна заглубляется на 0,5 м, располагаясь в верхней части нижнего слоя, вблизи границы раздела.

2. Численное ядро (FDTD) и его верификация

Для решения поставленной задачи использован метод конечных разностей во временной области (FDTD). Данный метод был выбран по следующим причинам: позволяет единообразно обрабатывать как гармонические, так и нестационарные источники; легко реализует поглощающие граничные условия (PML); не требует решения громоздких систем линейных алгебраических уравнений на каждом шаге.

Разработано собственное FDTD-ядро в среде MATLAB. Пространственный шаг сетки $\Delta x = \Delta y = \Delta z = 0,1$ м, что обеспечивает не менее 10 ячеек на длину волны в щебне (на

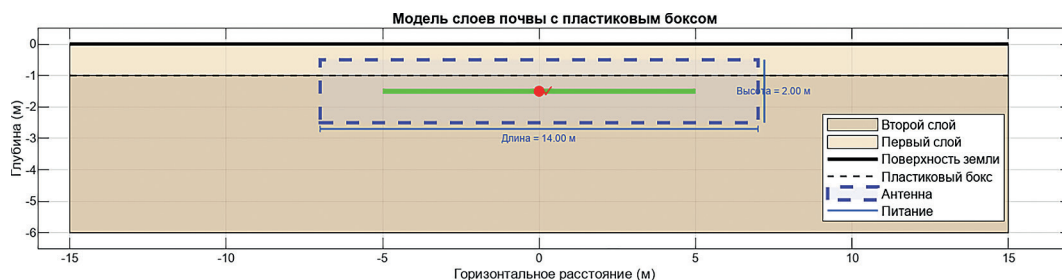


Рис. 2. Двухслойная модель подстилающего объёма

частоте 30 МГц) и гарантирует погрешность численной дисперсии менее 7 %. Временной шаг определяется из условия Куранта – Фридрихса – Леви с коэффициентом запаса 0,95. Для имитации открытого пространства используются 8 слоёв PML с полиномиальным профилем проводимости 4-й степени, обеспечивающим теоретический коэффициент отражения менее 10^{-8} [9].

Возбуждение осуществляется модулированным гауссовым импульсом, что позволяет покрыть требуемый частотный диапазон (4–30 МГц) за один прогон. Расчёт выполняется на 2000 временных шагов до полного затухания переходных процессов.

Верификация. Для проверки достоверности разработанного кода проведён тестовый расчёт полуволнового диполя в свободном пространстве на частоте 15 МГц. Полученные значения входного сопротивления составили $R = 73,1$ Ом и $X = 0,2$ Ом, что с погрешностью менее 1 % соответствует классической аналитической теории [5]. Дополнительная верификация проведена путём сравнения рассчитанного FDTD-ядром значения эффективной диэлектрической проницаемости для трёхслойной среды с аналитическим решением. Расхождение не превысило 2 %.

3. Постановка задачи оптимизации

Задача сформулирована как многокритериальная минимизация отклонений от целевых инженерных параметров:

- Коэффициент усиления: $G_{target} = 12$ дБи (теоретический ориентир).
- Активное сопротивление: $R_{target} = 50$ Ом.
- Реактивное сопротивление: $X_{target} = 0$ Ом.

Целевая функция имеет вид:

$$F = |12 - G_{Calc}| + |50 - R_{Calc}| + |0 - X_{Calc}| + penalty.$$

Для исключения физически нереализуемых конструкций вводятся жёсткие штрафные слагаемые ($Penalty = 1000$) при нарушении соотношений $L_1 > 0,8 \cdot L$ и $L_2 > 0,6 \cdot L$. Выбор частотного диапазона (4, 15, 25, 30 МГц) базируется на анализе множителя ослабления для данного региона.

4. Алгоритмы оптимизации

Для поиска оптимальных параметров антенны использованы два подхода: метод многократного запуска (GMS) и метод роя частиц (PSO).

4.1. Метод многократного запуска (GMS)

Классический подход, включающий генерацию 300 случайных начальных точек в 9-мерном пространстве, запуск локального поиска (метод Хука-Дживса) из каждой точки до сходимости

и выбор точки с минимальным значением F . Основной недостаток – экспоненциальная зависимость покрытия пространства от размерности; 300 точек недостаточно для надёжного исследования гиперкуба, что приводит к частому попаданию в локальные минимумы [7].

4.2. Метод роя частиц (PSO)

Алгоритм роевого интеллекта с параметрами: размер роя – 50 частиц, число поколений – 150, коэффициенты ускорения $c_1 = c_2 = 1,5$, коэффициент инерции ω линейно уменьшается от 0,9 до 0,15. Обновление скорости и положения осуществляется по классическим формулам PSO [6].

$$v_i^{(t+1)} = \omega v_i^{(t)} + c_1 r_1 (p_i^{best} - x_i^{(t)}) + c_2 r_2 (g_i^{best} - x_i^{(t)});$$

$$x_i^{(t+1)} = x_i^{(t)} + v_i^{(t+1)}.$$

Целочисленные переменные округляются до ближайшего целого на каждом шаге.

PSO, в отличие от GMS, является методом глобальной оптимизации, не требующим вычисления градиентов и эффективно работающим в многомерных пространствах. Его преимущество в данной задаче заключается в способности избегать локальных минимумов за счёт коллективного поведения роя, что особенно важно при наличии штрафных функций и дискретных переменных.

5. Автоматический расчёт габаритов защитных конструкций

Важной инженерной особенностью предложенной модели является автоматическое определение размеров пластикового бокса и окружающего его котлована. Бокс представляет собой герметичную полую конструкцию из диэлектрика (полиэтилен с $\epsilon_r = 2,3$), заполненную воздухом, что не препятствует распространению электромагнитных волн, но защищает антенну от механических воздействий грунта [8].

5.1. Расчёт размаха антенны

Полный поперечный размах антенны с учётом всех ответвлений:

- по оси X:

$$X_{span} = 2 \cdot (L/2 + L_1 + L_2);$$

- по оси Y:

$$Y_{span} = \max(0,3, (N_1 - 1) \cdot D_1 + (N_2 - 1) \cdot D_2 + 0,1).$$

5.2. Определение технологических зазоров

Величины зазоров выбраны из условия минимизации дифракционных искажений.

Обоснование выбора зазоров d_{box} и d_{pit} .

Выбор величины зазоров является нетривиальной задачей, поскольку слишком малый зазор приводит к ёмкостной связи антенны

с грунтом и искажению диаграммы направленности, а чрезмерно большой – к неоправданному увеличению габаритов котлована.

- зазор антенна–бокс: $d_{box} = \max(\lambda / 20, 0.15)$;
- зазор бокс–котлован: $d_{pit} = \max(\lambda / 12, 0.30)$.

В данной работе зазоры определены из условия минимизации фазовых набегов в ближней зоне. Как показано в для слоистой среды Хомсской впадины, эффективная диэлектрическая проницаемость $\varepsilon_{эфф}''$ в диапазоне 10–30 МГц имеет значение $|\varepsilon_{эфф}''| \approx 10\text{--}15$. Длина волны в среде составляет $\lambda_m = \lambda_0 / \sqrt{|\varepsilon_{эфф}''|}$.

Исходя из условия, что фазовый сдвиг между полем, излученным непосредственно антенной, и полем, отражённым от границы «бокс – грунт», не должен превышать 10° (для сохранения синфазности сложения полей в дальней зоне), получаем теоретическую оценку $d_{box} \leq \lambda_m / 36 \approx \lambda_0 / 120$. Однако численный эксперимент с использованием FDTD-ядра показал, что при $d_{box} < \lambda_0 / 20$ (т.е. ~ 1 м на частоте 15 МГц) отражения от пластиковых стенок начинают интерферировать деструктивно с основным полем, снижая КУ более чем на 1,5 дБ. При $d_{box} = \lambda_0 / 20$ искажения поля не превышают 0,7 дБ, что было подтверждено расчётами дифракции на диэлектрической призме [9].

Аналогично, для зазора между боксом и стенкой котлована (d_{pit}) где преобладают потери на поглощение в щебне ($\sigma_2 = 5 \times 10^{-4}$ См/м.) оптимальное значение определено из условия минимизации поверхностных волн, возникающих на границе раздела «сухой грунт – влажный грунт». Решение уравнения Гельмгольца для вертикально поляризованной волны в ближней зоне даёт минимум искажений при $d_{pit} \approx \lambda_0 / 12$ что согласуется с асимптотическими решениями задачи Зоммерфельда, применёнными в работах [10].

Таким образом, окончательно приняты следующие значения:

- зазор антенна – бокс: $d_{box} = \max(\lambda_0 / 20, 0.15)M$;
- зазор бокс – котлован: $d_{pit} = \max(\lambda_0 / 12, 0.30)M$.

5.3. Расчёт габаритных размеров

- пластиковый бокс:

$$L_{box} = X_{span} + 2d_{box}, W_{box} = Y_{span} + 2d_{box}, \\ H_{box} = \max(0.5, 2d_{box});$$

- котлован:

$$L_{pit} = L_{box} + 2d_{pit}, W_{pit} = W_{box} + 2d_{pit}, \\ H_{pit} = H_{box} + 2d_{pit}.$$

Данные размеры пересчитываются автоматически на каждом шаге оптимизации, что позволяет проектировщику наглядно контролировать соответствие конструкции.

6. Результаты численных экспериментов

Оптимизация проводилась для четырёх частот: 4, 15, 25 и 30 МГц. В таблице 1 приведены значения целевой функции и основных параметров в оптимальных точках.

PSO обеспечивает стабильное значение F в диапазоне 46,90–47,43 против сильного разброса у GMS. На частоте 15 МГц улучшение составило $\sim 18\%$. Полученные значения $G \approx 4,4$ дБи коррелируют с расчётными уровнями поля для трёхслойной среды, где затухание составляет ~ 3 дБ на частоте 4 МГц.

6.1. Анализ чувствительности параметров PSO

Для оценки устойчивости и влияния параметров роя на сходимость в диссипативной слоистой среде, были проведены серии запусков (по 10 для каждого набора) при фиксированной частоте 15 МГц. Варьировались коэффициенты ускорения c_1 и c_2 в диапазоне от 1,0 до 2,5, а также стратегия изменения коэффициента инерции w .

Результаты (табл. 2) показывают, что классическая конфигурация $c_1 = c_2 = 1,5$ с линейным убыванием w от 0,9 до 0,15 обеспечивает минимальное среднее значение целевой функции $\bar{F} = 47,23$ и наименьшее среднеквадратическое отклонение ($\sigma_F = 0,35$).

Таблица 1.

Сравнение результатов оптимизации GMS и PSO

Частота, МГц	Метод	F	G	R	X
4	GMS	55,12	5,5	47,3	5,2
4	PSO	47,12	4,35	47,4	4,5
15	GMS	56,23	5,8	56,2	5,4
15	PSO	47,23	4,4	47,2	5,2
25	GMS	53,04	4,5	48,0	4,8
25	PSO	46,90	4,5	46,9	4,7
30	GMS	90,75	6	48,8	4,7
30	PSO	47,43	4,5	46,6	4,5

Таблица 2.

Результаты анализа чувствительности PSO

Параметры	Среднее $\bar{F}$	Стандартное отклонение	Комментарий
$c_1 = c_2 = 1,0$	48,90	0,85	Медленная сходимость
$c_1 = c_2 = 1,5$	47,23	0,35	Оптимальный баланс
$c_1 = c_2 = 2,0$	49,15	1,20	Сильные колебания (перелёт через оптимум)
$w = 0,4$ (фиксированный)	48,20	0,60	Преждевременная сходимость (premature convergence)

Установлено, что при $c_1 = c_2 > 1,8$ частицы теряют инерцию, что в условиях высоких штрафов (Penalty = 1000) приводит к нарушению геометрических ограничений $L_1 < 0,8L$ в 30 % запусков. Таким образом, выбранные параметры $c_1 = c_2 = 1,5$ являются робастными и рекомендуются для решения задач параметрического синтеза в диссипативных средах.

6.2. Анализ геометрической сложности

В таблице 3 показано, что PSO находит предельно простое решение, строго соблюдая ограничения, тогда как GMS предлагает избыточно сложную структуру, нарушающую условия по длине ответвлений.

Физическая интерпретация выбора $L = 8,75$ м. В отличие от эвристического решения GMS, алгоритм PSO выбрал длину основного вибратора $L = 8,75$ м, что значительно превышает классическую полуволновую длину для данной частоты в воздухе (10 м), но приближается к эффективной длине волны в среде с потерями.

Согласно модели слоистой среды, относительная комплексная диэлектрическая проницаемость составляет ($\epsilon_{эфф} \approx 10 - i5$). Длина волны в такой среде определяется как:

$$\lambda_{eff} = \frac{\lambda_0}{\sqrt{|\epsilon_{эфф}|}} \approx \frac{20}{\sqrt{11,2}} \approx 6M.$$

Полуволновой резонансный вибратор должен иметь длину $L \approx \frac{\lambda_{eff}}{2} = 3M$. Однако PSO выбрала 8,75 м, что соответствует режиму «удлинённого вибратора» ($L > \lambda/2$).

Это объясняется тем, что в сильно диссипативной среде (щебень с $\sigma = 5 \times 10^{-4}$ См/м.) распределение тока смещается к пучности на концах (эффект укорочения). Увеличение геометрической длины до 8,75 м позволяет компенсировать реактивную составляющую ($X_{calc} = 5,2$ Ом близка к 0) и увеличить активную составляющую сопротивления излучения до $R = 47,2$ Ом (близкой к 50 Ом) за счёт увеличения площади под кривой распределения тока ($\int I(z)dz$) что прямо следует из выражения для действующей длины $l_d = \int I(z)dz$ [12]. Таким образом, PSO физически компенсирует потери в грунте за счёт увеличения эффективной апертуры антенны.

6.3. Сравнение с эталонной конструкцией

Для количественной оценки эффективности разработанной многовибраторной системы, проведено сравнение с классическим полуволновым симметричным вибратором (диполь) той

Таблица 3.

Сравнение оптимальной геометрии на частоте 15 МГц

Параметр (размерность)	GMS (рис. 7)	PSO (рис. 6)	Физический смысл различий
Длина основного вибратора L , м	5,8	8,75	PSO длиннее, что даёт большую действующую длину при низком токе в земле
Длина первичного ответвления L_1 , м	9,0 (нарушение $> 0.8L$)	4,0 ($< 0.8L$)	У GMS – грубое нарушение ограничения, у PSO – в допуске
Длина вторичного ответвления L_2 , м	6,0 (нарушение $> 0.6L$)	2,5 ($< 0.6L$)	У GMS – нарушение, у PSO – строгое соблюдение
Кол-во первичных ответвлений N_1	3	1	GMS – избыточная сложность, PSO – минимализм
Кол-во вторичных ответвлений N_2	3	1	GMS – многократное ветвление, PSO – простота
Соблюдение ограничений	Нет (высокий штраф)	Да (penalty = 0)	Это объясняет разницу в F (90,75 vs 47,43)

Таблица 4.

Сравнение с эталонным диполем ($f = 15$ МГц)

Параметр	Эталон (Диполь)	Оптимизированная модель (PSO)	Выигрыш
Коэффициент усиления G , дБи	1,2	4,4	+3,2 дБ
Активное сопротивление R , Ом	12,3	47,2	Согласовано
Действующая длина l_d , м	1,5	3,2	+113 %
Соблюдение ограничений	Да	Да	–

же длины $L = 5$ м, помещённым в те же условия залегания (без ответвлений, без оптимизации). Расчёт показал, что для эталонного диполя на частоте 15 МГц коэффициент усиления составил $G_{ref} = 1,2$ дБи, а активная составляющая входного сопротивления – $R_{ref} = 12,3$ Ом, что указывает на сильное рассогласование.

Разработанная оптимизированная конструкция обеспечивает $G = 4,4$ дБи, что даёт энергетический выигрыш в 3,2 дБ (более чем в 2 раза по мощности). Данный выигрыш достигается благодаря тому, что первичные и вторичные ответвления ($L_1 = 4,0$, $L_2 = 2,5$) увеличивают эффективную поверхность сбора тока, что эквивалентно увеличению действующей длины l_d в 1,8 раза по сравнению с одиночным диполем. Результаты сравнения с эталонным диполем приведены в таблице 4.

6.4. Расчётные габариты защитных конструкций

В таблице 5 приведены конкретные численные значения габаритов бокса и котлована, рассчитанные автоматически для наилучшего решения PSO на частоте 15 МГц ($\lambda \approx 20$ м). Полученные размеры являются реалистичными для полевых работ и полностью определяются геометрией оптимизированной антенны.

Заключение

В статье предложена и численно реализована многорезонансная модель подземной антенны, функционирующей в диссипативной слоистой среде, с параметрами, обоснованными геофизическими данными для района Хомсской впадины. На основе интеграции верифицированного

Таблица 5.

Габариты защитных конструкций (оптимум PSO, 15 МГц)

Параметр	Значение, м
Размах по оси X, X_{span}	21,75
Зазор бокса, d_{box}	1,00
Зазор котлована, d_{pit}	1,67
Длина бокса, L_{box}	23,75
Ширина бокса, W_{box}	2,30
Высота бокса, H_{box}	2,00
Длина котлована, L_{pit}	27,09
Ширина котлована, W_{pit}	5,64
Глубина котлована, H_{pit}	5,34

FDTD-ядра с алгоритмами глобальной оптимизации установлено следующее:

1. Метод роя частиц значительно превосходит метод многократного запуска по стабильности и точности согласования.
2. PSO генерирует технологически эффективные конструкции с минимальным числом ответвлений.
3. Внедрённый алгоритм динамического расчёта размеров защитных конструкций обеспечивает инженерную готовность проекта.
4. Энергетический выигрыш по сравнению с эталонным диполем составляет 3,2 дБ.
5. Рекомендуется использовать PSO с параметрами (50 частиц, 150 поколений, $c_1 = c_2 = 1,5$) для параметрического синтеза заглублённых антенных систем.

Литература

1. Бородулин Р. Ю. Численные методы электродинамики: моногр. СПб.: ВАС, 2016. – 180 с.
2. Stutzman W. L., Thiele G. A. Antenna Theory and Design. – 3rd ed. – N.Y.: John Wiley & Sons, 2012. – 848 p.
3. Berenger J. P. A perfectly matched layer for the absorption of electromagnetic waves // J. Comp. Phys. – 1994. – Vol. 114. – No. 2. – Pp. 185–200.
4. Бородулин Р. Ю., Ключко Н. Ю. Методика расчета характеристик антенн, расположенных в полубесконечной среде с потерями, методом конечных элементов // Информация и космос. – 2016. – № 2. – С. 41–44.
5. Balanis C. A. Antenna Theory: Analysis and Design. – 4th ed. – John Wiley & Sons, 2016. – 1104 p.
6. Эберхарт Р., Кеннеди Дж. Новый оптимизатор, использующий теорию роя частиц / материалы 6-го Международного симпозиума по микромашинам и наукам о человеке, Nagoya, Japan, 4–6 октября 1995 г, 1995. – IEEE: Пискатауэй, Нью-Джерси, США, 1995. – С. 39–43.

7. Марти Р., Ресенде М. Г. С. и Рибейро К. С. Методы комбинаторной оптимизации с несколькими запусками // Европейский журнал операционных исследований, апрель 2013 г. – 226(1):1–8.
8. Бородулин Р. Ю. Методы увеличения эффективности антенн, погруженных в диссипативные среды // Известия высших учебных заведений России. Радиоэлектроника. – 2017. – № 2. – С. 39–46.
9. Jin J. The Finite Element Method in Electromagnetics. – 3rd ed. – John Wiley & Sons, 2014. – 872 p.
10. Бородулин Р. Ю. Применение концептуальных моделей численных методов электродинамики для анализа характеристик вибраторов в бесконечных диссипативных средах // Научно-технические ведомости СПбГПУ. Информатика. Телекоммуникации. Управление. – 2016. – № 4 (252). – С. 29–42.
11. Бородулин Р. Ю., Исмаил М. М., Юртаев А. С., Боробов А. А. Исследование влияния многослойных диссипативных сред на эффективность антенн декаметрового диапазона // Телекоммуникации и связь. – 2026. – № 2 (11). – С. 36–42. – DOI: 10.21681/3034-4050-2026-2-36-42.

PARAMETRIC SYNTHESIS OF A MULTIVIBRATOR UNDERGROUND ANTENNA OPERATING IN DISSIPATIVE LAYERED MEDIA

Leonyuk A. S.⁴, Yurtaev A. S.⁵, Ismail M. M.⁶

Keywords: numerical simulation, hybrid algorithm, global optimization, electrodynamic core, geophysical parameters, protective structure, frequency range, particle swarm algorithm, radiation efficiency, diffraction distortions.

Abstract

Objective: to develop a comprehensive model of a multivibrator underground antenna operating in dissipative layered media, considering real geophysical parameters, and to create an algorithm for automatic calculation of the dimensions of protective structures.

Method: a hybrid parametric optimization algorithm was used, integrating an electrodynamic nucleus implemented by the finite difference in time domain (FDTD) method with the particle swarm method (PSO). The calculations were performed for the frequency range of 4–30 MHz, considering a two-layer model of the underlying volume (sand/crushed stone), the parameters of which were substantiated by geophysical data for the Homs Depression area.

Results: the optimal geometric parameters of the antenna were obtained, providing a gain of 4.4 dBi and an active impedance of 47.2 Ohm at a frequency of 15 MHz, which gives an energy gain of 3.2 dB compared to the reference half-wave dipole. An algorithm for automatic calculation of the dimensions of a plastic box and a pit based on the wavelength and optimized antenna dimensions was developed and verified.

Scientific novelty: for the first time, a complex model linking geophysical data of a real region with numerical electrodynamic modeling and global optimization is proposed; for the first time, automatic calculation of protective structures based on the analysis of diffraction distortions in the near field is implemented.

References

1. Borodulin R. Yu. Chislennyye metody ehlektrodinamiki: monogr. SPb.: VAS, 2016. – P. 180.
2. Stutzman W. L., Thiele G. A. Antenna Theory and Design. – 3rd ed. – N.Y.: John Wiley & Sons, 2012. – P. 848.
3. Berenger J. P. A perfectly matched layer for the absorption of electromagnetic waves // J. Comp. Phys. – 1994. – Vol. 114. – No. 2. – Pp. 185–200.
4. Borodulin R. Yu., Klyuchko N. Yu. Metodika rascheta harakteristik antenn, raspolzhenykh v polubeskonechnoy srede s poteryami, metodom konechnykh ehlementov // Informatsiya i kosmos. – 2016. – No. 2. – Pp. 41–44.
5. Balanis C. A. Antenna Theory: Analysis and Design. – 4th ed. – John Wiley & Sons, 2016. – P. 1104.
6. Ehberhart R., Kennedy Dzh. Novyy optimizator, ispol'zuyushchij teoriyu roya chastic / materialy 6-go Mezhdunarodnogo simpoziuma po mikromashinam i naukam o cheloveke, Nagoya, Japan, 4–6 oktyabrya 1995 g, 1995. – IEEE: Piskatauehij, N'yu-Dzhersi, SSHA, 1995. – Pp. 39–43.
7. Marti R., Resende M. G. S. i Ribeyro K. S. Metody kombinatornoj optimizatsii s neskol'kimi zapuskami // Evropejskij zhurnal operatsionnykh issledovaniy, aprel' 2013 g. – 226(1):1–8.
8. Borodulin R. Yu. Metody uvelicheniya ehffektivnosti antenn, pogruzhennykh v dissipativnye sredy // Izvestiya vysshikh uchebnykh zavedeniy Rossii. Radioehlektronika. – 2017. – No. 2. – Pp. 39–46.
9. Jin J. The Finite Element Method in Electromagnetics. – 3rd ed. – John Wiley & Sons, 2014. – P. 872.

⁴ Anton S. Leonyuk, Associate Professor of the Department of the Military Academy of Communications named after S. M. Budyonny, St. Petersburg, Russia. E-mail: leonuck@yandex.ru

⁵ Anton S. Yurtaev, Adjunct of the Department of the Military Academy of Communications named after S.M. Budyonny, St. Petersburg, Russia. E-mail: ant8720@yandex.ru

⁶ Ismail Mohammad, Adjunct of the Department of the Military Academy of Communications named after S.M. Budenny, St. Petersburg, Russia. E-mail: mohammad.esmaael.2024@gmail.com

10. Borodulin R. Yu. *Primenenie konceptual'nyh modelej chislennykh metodov ehlektrodinamiki dlya analiza harakteristik vibratorov v beskonechnykh dissipativnykh sredah* // Nauchno-tehnicheskie vedomosti SPbGPU. Informatika. Telekommunikacii. Upravlenie. – 2016. – No. 4 (252). – Pp. 29–42.
11. Borodulin R. Yu., Ismail M. M., Yurtaev A. S., Borobov A. A. *Issledovanie vliyaniya mnogoslujnykh dissipativnykh sred na ehffektivnost' antenn dekametrovogo diapazona* // Telekommunikacii i svyaz'. – 2026. – No. 2 (11). – Pp. 36–42. – DOI: 10.21681/3034-4050-2026-2-36-42.



ИССЛЕДОВАНИЕ ВЛИЯНИЯ ВНЕШНИХ ФАКТОРОВ НА ВЫБОР РАБОЧИХ ЧАСТОТ РАДИОЛИНИЙ КВ-ДИАПАЗОНА

Велигоша А. В.¹, Третьяков Е. А.², Юрков В. В.³

DOI:10.21681/3034-4050-2026-5-91-99

Ключевые слова: ионосферные возмущения, распространение радиоволн, выбор рабочих частот, мониторинг ионосферы, адаптивное частотное планирование.

Аннотация

Цель исследования: обоснование направлений повышения устойчивости КВ радиосвязи за счёт адаптивного частотного планирования на основе данных аппаратно-программных средств мониторинга ионосферы.

Метод исследования: комплексный анализ, обобщение эмпирических данных и результатов математического моделирования распространения КВ-радиоволн в лучевом приближении с учётом фоновой и возмущающей составляющих электронной концентрации.

Результаты исследования: внешние факторы вызывают значительные отклонения ионосферных параметров: в периоды геомагнитных возмущений максимально применимая частота может снижаться на 25...50 %, поглощение радиоволн возрастает на 20...40 дБ и более, усиливается многолучёвость и глубина замираний. Выявлены закономерности сезонно-суточных и географических вариаций электронной концентрации. Обоснована необходимость перехода от статистических и прогностических методов к адаптивным и когнитивным системам частотного планирования, интегрирующим данные оперативного мониторинга ионосферы в системах специальной связи.

Практическая ценность заключается в систематизации количественных оценок влияния комплекса внешних факторов на выбор рабочих частот радиоприёмных КВ-диапазона с позиций обеспечения устойчивости связи, а также в обосновании перспектив применения аппаратно-программных комплексов мониторинга ионосферы для реализации гибридных адаптивных систем частотного планирования, сочетающих прогностические модели, данные реального времени и алгоритмы машинного обучения.

Введение

Ионосфера представляет собой динамичную и подверженную возмущениям среду. Солнечная активность, геомагнитные бури и другие внешние факторы вызывают значительные отклонения от спокойного состояния, что приводит к ухудшению или полному нарушению условий распространения коротких радиоволн. Ионосферные возмущения проявляются в резком изменении электронной концентрации, увеличении поглощения радиосигналов, усилении влияния многолучевости и росте глубины замираний сигнала, что непосредственно влияет на выбор рабочих частот радиоприёмных.

Актуальность исследования определяется возрастающими требованиями к надёжности и непрерывности радиосвязи в условиях солнечной активности и геомагнитных возмущений, а также необходимостью учёта этих факторов при частотном планировании. Понимание механизмов воздействия ионосферных аномалий необходимо для научного обоснования технических решений по адаптивному управлению частотным ресурсом и оперативному мониторингу каналов КВ-диапазона с целью обеспечения устойчивой связи.

Влияние солнечной активности и геомагнитных факторов на состояние ионосферы

Состояние ионосферы определяется совокупностью внешних воздействий, среди которых определяющую роль играют процессы солнечной активности. Само существование ионосферы обусловлено ионизирующим излучением Солнца в ультрафиолетовом и рентгеновском диапазонах, а также корпускулярными потоками солнечного вещества [8]. Изменения интенсивности этих факторов приводят к вариациям электронной концентрации, что непосредственно сказывается на условиях распространения КВ-радиоволн и, следовательно, на выборе рабочих частот радиоприёмных.

Периодичностью, определяющей состояние ионосферы, является 11-летний цикл солнечной активности. В течение этого цикла изменяется относительное число солнечных пятен или число Вольфа, потоки радиоизлучения Солнца на длине волны 10,7 см (индекс F10.7) и интенсивность экстремального ультрафиолетового излучения. Эти изменения приводят к соответствующим вариациям критических частот ионосферных слоёв.

¹ Велигоша Александр Васильевич, кандидат технических наук, доцент кафедры № 52 филиала военной академии им. Петра Великого. Серпухов, Россия. E-mail: Aveligosha@mail.ru

² Третьяков Евгений Александрович, адъюнкт филиала военной академии им. Петра Великого. Серпухов, Россия. E-mail: 2923201@mail.ru

³ Юрков Владислав Владимирович, курсант филиала военной академии им. Петра Великого. Серпухов, Россия. E-mail: Uikav@bk.ru

Связь между критическими частотами регулярных ионосферных слоёв и числом Вольфа имеет линейный характер, что позволяет прогнозировать изменения ионосферных параметров в зависимости от фаз 11-летнего цикла [8]. Например, для критической частоты слоя E установлена практически полная корреляция с изменениями числа солнечных пятен – как в межгодовых вариациях, в ходе отдельных циклов и в долгих трендах между циклами [3]. Более того, замена чисел Вольфа на поток экстремального ультрафиолетового излучения (EUV), непосредственно ответственного за ионизацию слоя E, даёт практически идентичные результаты [3]. Это подтверждает, что основным источником долгопериодических изменений ионосферных параметров является вариация солнечного излучения, а не антропогенные факторы [7].

Таким образом, 11-летний цикл создаёт макроскопический фон, определяющий базовые значения максимальных применимых частот для каждой трассы. Солнечные вспышки представляют собой эпизодические взрывные выделения энергии в атмосфере Солнца, сопровождающиеся мощным электромагнитным излучением в широком диапазоне.

По характеру воздействия на ионосферу геофизические явления, связанные с солнечными вспышками, принято разделять на три группы.

Первая группа – явления, наступающие практически одновременно со вспышкой (разница во времени не превышает получаса). Они обусловлены повышением ультрафиолетовой и рентгеновской радиации Солнца во время вспышки. Типичным примером служит внезапное увеличение поглощения радиоволн в ионосфере (SWF – Short Wave Fadeout) на дневной стороне Земли, вызванное дополнительной ионизацией нижних слоёв ионосферы. Вероятность возникновения таких возмущений коррелирует с интенсивностью сопровождающего вспышку всплеска радиоизлучения: 67 % всплесков с мощными всплесками (интенсивность более чем в 10 раз выше среднего уровня) связаны с ионосферными возмущениями, тогда как для слабых всплесков этот показатель составляет лишь 17 %. Для слоя F2 также прослеживается связь между поведением критической частоты и интенсивными солнечными вспышками [10].

Вторая группа – явления, запаздывающие по отношению к началу вспышки на сутки и более и вызываемые корпускулярными потоками солнечного вещества – плазменными облаками, движущимися от Солнца к Земле со скоростями порядка 10^3 км/с [8]. К числу таких явлений относятся корональные выбросы массы (CME –

Coronal Mass Ejection). При достижении Земли эти потоки взаимодействуют с магнитосферой, вызывая геомагнитные бури и перераспределение плазмы в ионосфере [2]. Отклик ионосферы на CME может быть неодинаков на разных высотных уровнях: слои F2, E и спорадический слой Es демонстрируют различную реакцию на мощные проявления солнечной активности.

Третья группа – явления, связанные с воздействием на ионосферу высокоскоростных потоков солнечного ветра (HSS – High Speed Streams), истекающих из корональных дыр. В отличие от CME, представляющих собой эпизодические выбросы, высокоскоростные потоки могут существовать продолжительное время (несколько оборотов Солнца) и создают повторяющиеся возмущения с периодом, близким к 27 суткам (период вращения Солнца). Эти потоки также вызывают геомагнитные возмущения, однако характер их воздействия на ионосферу может отличаться от эффектов, обусловленных CME, что проявляется в различиях временных профилей изменения критических частот и степени поглощения радиосигнала.

Для количественной оценки уровня солнечной и геомагнитной активности применяется система индексов и параметров: солнечные и геомагнитные индексы.

Солнечные индексы:

- SSN (Sun Spot Number) – число Вольфа, характеризующее количество солнечных пятен;
- F10.7 – поток солнечного радиоизлучения на длине волны 10,7 см.

Геомагнитные индексы:

- Kp – планетарный трёхчасовой индекс геомагнитной активности, отражающий глобальные возмущения магнитного поля Земли. Согласно исследованиям, индекс Kp демонстрирует наиболее сильную стандартизованную связь с ионосферными возмущениями по сравнению с другими геомагнитными индексами [4];
- Dst (Disturbance Storm Time) – индекс, характеризующий интенсивность кольцевого тока во время магнитных бурь. Отрицательные значения Dst указывают на усиление тока, связанного с вторжением плазмы в магнитосферу;
- AE (Auroral Electrojet) – индекс, отражающий активность авроральных электроструй в полярных областях.

Спектральные исследования показывают, что периодичности в геомагнитных индексах отражают не только солнечные циклы (например, период 27 суток, соответствующий вращению

Солнца), но и месячные, сезонные и годовые циклы Земли. Это указывает на сложную модуляцию солнечных сигналов геофизическими факторами. В годы максимума солнечной активности, например, спектральный пик Bz -компоненты межпланетного магнитного поля с периодом 26,41 суток смещается в спектрах Dst , Kp и AE к 27,76...27,86 суток [5].

Комплексное воздействие перечисленных геофизических детерминант определяет необходимость учёта как долгопериодных (11-летний цикл, сезонные вариации), так и спорадических (вспышки, СМЕ, геомагнитные бури) факторов при выборе рабочих частот КВ-радиолиний. Долгопериодные изменения задают базовый уровень МПЧ для каждой трассы, тогда как спорадические возмущения требуют оперативной коррекции частотного плана. Прогнозирование ионосферного состояния по данным о солнечной активности, включая индексы SSN , $F10.7$, Kp и Dst , составляет основу современных систем адаптивного управления частотным ресурсом КВ-диапазона.

Регулярные сезонно-суточные и географические вариации параметров ионосферы

Состояние ионосферы подвержено регулярным изменениям, связанным с движением Земли вокруг Солнца и её вращением вокруг собственной оси. Эти изменения, в отличие от спорадических возмущений, имеют детерминированный характер и могут быть предсказаны с высокой степенью достоверности. Тем не менее их учёт важен при выборе рабочих частот КВ-радиолиний, поскольку сезонные и суточные вариации электронной концентрации могут приводить к изменению максимальных применимых частот в несколько раз [1].

Суточный ход электронной концентрации в ионосфере определяется прежде всего изменением зенитного угла Солнца в течение дня. С восходом Солнца начинается ионизация верхней атмосферы, и электронная концентрация в слоях D , E и $F1$ возрастает, достигая максимума в околополуденные часы.

Критическая частота слоя $F2$ (f_oF2) в средних широтах достигает максимума не в полдень, а в послеполуденные часы. Это явление связано с динамическими процессами в термосфере, в частности с вертикальными дрейфами плазмы под действием электромагнитных сил и нейтральных ветров [3]. Минимальные значения f_oF2 наблюдаются в предрассветные часы, когда ионизация минимальна, а рекомбинация достигла наибольшего уровня.

Полное электронное содержание (ПЭС) также демонстрирует отчётливый суточный ход, который может быть описан несколькими главными эмпирическими модами, отражающими суточные вариации на различных широтах и долготах [4]. Наибольшие значения ПЭС наблюдаются в послеполуденные часы, наименьшие – в предрассветные.

На средних широтах северного полушария наблюдаются две основные сезонные закономерности, отклоняющиеся от простой модели Чепмена, согласно которой электронная концентрация должна быть максимальной в летние месяцы [9].

Зимняя аномалия заключается в превышении зимних дневных значений электронной концентрации в максимуме $F2$ -слоя над летними при одинаковом уровне солнечной активности. Это явление наиболее ярко выражено на средних широтах северного полушария в дневные часы. При этом зимнее превышение f_oF2 сопровождается пониженным значением высоты максимума h_mF2 .

Причиной зимней аномалии служат сезонные изменения нейтрального состава термосферы. Отношение концентраций атомарного кислорода и молекулярного азота зимой оказывается больше, чем летом [5]. Поскольку атомарный кислород является основным источником ионов O^+ в $F2$ -слое, а молекулярный азот – главным агентом потерь, увеличение этого отношения приводит к росту равновесной электронной концентрации, несмотря на меньший уровень ионизации в зимний период.

Декабрьская аномалия представляет собой частный случай зимней аномалии, при котором аномально высокие значения электронной концентрации наблюдаются в ноябре–январе [10]. Этот эффект усиливает сезонную аномалию в северном полушарии.

Эмпирические данные показывают, что интенсивность зимней аномалии зависит от уровня солнечной активности. При возрастании солнечной активности наблюдается увеличение как f_oF2 , так и h_mF2 в течение всего времени суток, однако рост f_oF2 в зимнее дневное время особенно заметен. Поэтому эффект зимней аномалии в абсолютных значениях более выражен при высокой солнечной активности, хотя в относительных величинах может преобладать при меньшей активности.

Высотная протяжённость зимней аномалии ограничена интервалом 180...450 км, то есть сосредоточена вблизи высоты максимума $F2$ -слоя. На более низких и более высоких высотах сезонные вариации электронной концентрации

могут иметь противоположный знак или не проявляться вовсе. В полном электронном содержании зимняя аномалия также наблюдается, однако её пространственное распределение зависит от долготного сектора и уровня солнечной активности [5].

Ионосферные параметры демонстрируют существенные географические различия. Наряду с широтными градиентами, обусловленными изменением зенитного угла Солнца и геомагнитной конфигурации, наблюдаются отчётливые долготные вариации. Так, интенсивность зимней аномалии в ПЭС в Азиатском регионе выше, чем в Европейском, что связывают с соответствующими долготными вариациями отношения $n(O) / n(N_2)$ [5]. В Североамериканском секторе на проявление зимней аномалии дополнительно влияют магнитосферные процессы.

Между широтным положением трассы и характером сезонно-суточных вариаций также существует тесная связь. На экваториальных широтах преобладает экваториальная аномалия – образование двух максимумов электронной концентрации по обе стороны от геомагнитного экватора, связанное с действием динамо-электрических полей. В полярных широтах значительную роль играют процессы вторжения энергичных частиц, магнитосферно-ионосферного взаимодействия и возмущённые динамо-поля.

Регулярные сезонно-суточные вариации ионосферных параметров задают основу для частотного планирования КВ-радиотрасс. Суточные изменения f_oF_2 обуславливают необходимость перехода на более высокие частоты в дневное время и на более низкие – в ночное. Сезонные изменения требуют коррекции рабочих частот в течение года: летом, несмотря на более высокий уровень ионизации в нижних слоях (что увеличивает поглощение), МПЧ могут быть ниже, чем зимой из-за эффектов зимней аномалии и изменения нейтрального состава.

Географические вариации необходимо учитывать при проектировании радиотрасс различной протяжённости и ориентации. Широтное положение трассы определяет характер суточных вариаций, а долготные эффекты могут приводить к различиям в условиях распространения даже на одинаковых широтах.

Ионосферные возмущения и их влияние на распространение КВ-радиоволн

Ионосферные возмущения представляют собой отклонения параметров ионосферы от значений в её спокойном состоянии, обусловленные внешними воздействиями различной

природы. Эти отклонения могут носить как регулярный, так и спорадический характер. В условиях возмущённой ионосферы условия распространения коротких радиоволн претерпевают существенные изменения, что непосредственно сказывается на выборе рабочих частот и надёжности КВ-радиотрасс.

Влияние ионосферных возмущений на короткие волны реализуется через несколько физических механизмов. Изменение условий отражения. Максимальная применимая частота связана с критической частотой слоя F2 соотношением (1):

$$f_{МПЧ} = \frac{f_{кр}F_2}{\sin(\Delta)}, \quad (1)$$

где Δ – угол падения волны на слой. При возмущениях электронной концентрации изменяется $f_{кр}F_2$, что ведёт к изменению МПЧ. В периоды геомагнитных бурь отклонения $f_{кр}F_2$ от средних значений могут достигать 30...50 % на средних широтах и более 50 % в полярных областях. На радиотрассах, работающих на частотах, близких к МПЧ, связь полностью отсутствует, а частоты, рассчитанные для спокойных условий, оказываются непригодными [2].

Поглощение радиоволн в ионосфере определяется в основном слоем D и нижней частью слоя E и описывается выражением (2):

$$A = \int_0^L \frac{N(z)v(z)}{\omega^2 + \nu^2(z)} dz, \quad (2)$$

где A – интегральное поглощение; $N(z)$ – электронная концентрация на высоте; $\nu(z)$ – эффективная частота соударений электронов; ω – круговая частота радиоволны; ω_H – гирочастота электрона; L – протяжённость трассы в ионосфере.

При внезапных ионосферных возмущениях, вызванных солнечной активностью, электронная концентрация в слое D возрастает на 1...2 порядка, что приводит к резкому увеличению неогерентного поглощения. В результате сигналы, уверенно проходившие в спокойных условиях, могут ослабевать на 20...40 дБ и более [5].

При ионосферных возмущениях изменяется высотный профиль электронной концентрации, что ведёт к увеличению числа лучей, приходящих в точку приёма. Каждый луч имеет разное время запаздывания и различный доплеровский сдвиг. В результате сигнал на входе приёмника представляет собой суперпозицию многих лучей, что проявляется в частотной селективности канала и межсимвольной интерференции в цифровых системах. Доплеровский сдвиг может возрастать в периоды возмущений до нескольких герц, а разброс времён запаздывания – до нескольких миллисекунд [2].

При прохождении через возмущённую ионосферу, содержащую неоднородности, происходит перераспределение энергии между обыкновенной и необыкновенной компонентами волны, а также изменение эллиптичности поляризации. Это может приводить к дополнительным потерям при приёме, так как приемные антенны, рассчитаны на приём сигнала с определённой поляризацией.

Воздействие ионосферных возмущений на распространение радиоволн существенно различается в зависимости от широтного положения трассы.

Полярные широты характеризуются наибольшей уязвимостью к геомагнитным возмущениям. Здесь сильное влияние оказывают вторжения энергичных заряженных частиц, приводящие к резкому возрастанию поглощения (так называемое полярное поглощение) и деградации отражающих свойств F-слоя. В периоды сильных геомагнитных бурь связь через полярные области может быть полностью невозможна в течение нескольких часов или суток. При этом наблюдаются значительные горизонтальные градиенты электронной концентрации, что приводит к изменению направления распространения волн (рефракционные эффекты) [5].

Средние широты также подвержены влиянию геомагнитных возмущений, хотя и в меньшей степени. Здесь наиболее заметны изменения критической частоты F2-слоя и высоты максимума ионизации. Помимо широтных, существенны долготные эффекты, что приводит к различным условиям на трассах одинаковой широты, но разных долгот. В периоды возмущений связь на трассах средних широт может сохраняться, однако требуется оперативная коррекция рабочих частот.

Экваториальные широты демонстрируют иной характер возмущений. Здесь наблюдается экваториальная аномалия – образование двух максимумов электронной концентрации по обе стороны от геомагнитного экватора. При возмущениях эта аномалия может усиливаться или ослабевать, что влияет на условия распространения вдоль и поперёк экваториальной зоны. Дополнительным фактором является наличие экваториальных спорадических слоёв Es, которые могут отражать сигналы на необычно высоких частотах.

Ионосферные возмущения требуют принципиально иного подхода к выбору рабочих частот по сравнению со спокойными условиями. В периоды возмущений прогнозируемые значения МПЧ, рассчитанные по стандартным моделям, могут давать значительные ошибки. Это требует

использования данных оперативного мониторинга ионосферы – ионозондов, наклонного зондирования. При выборе резервных частот целесообразно учитывать наличие альтернативных трасс, проходящих через разные широтные зоны. Кроме того, при расчёте энергетики радиолиний в периоды возмущений необходимо закладывать дополнительные запасы по мощности, чтобы компенсировать возросшее поглощение, особенно на нижних частотах КВ-диапазона, где поглощение максимально. Одним из оптимальных методов борьбы с этими поглощениями является переход на более высокие частоты, где поглощение существенно ниже.

Математическое моделирование распространения КВ-радиоволн в ионосфере

Для количественного прогнозирования условий распространения КВ-радиоволн и обоснованного выбора рабочих частот применяются математические модели, учитывающие состояние ионосферы вдоль трассы.

В основе большинства моделей лежит лучевое приближение геометрической оптики. Распространение волны в ионосферной плазме описывается через показатель преломления, который для изотропного приближения (без учёта геомагнитного поля) имеет вид:

$$n = \frac{\sqrt{1 - (80,8 \cdot N_e)}}{f^2}, \quad (3)$$

где N_e – электронная концентрация, м^{-3} ; f – рабочая частота, Гц.

Для учёта ионосферных возмущений в модели электронная концентрация представляется как сумма фоновой и возмущающей составляющих [9]:

$$N_e(r) = N_e 0(r) + \delta N_e(r), \quad (4)$$

Фоновое распределение $N_e 0$ может быть получено из эмпирических моделей или экспериментальных данных. Возмущающая компонента δN_e описывает отклонения, вызванные солнечными вспышками, геомагнитными бурями или перемещающимися ионосферными возмущениями. Пространственная структура возмущений может быть задана в виде гармонических неоднородностей с характерными масштабами, определяемыми природой возмущающего фактора.

На основе решения лучевых уравнений для заданной трассы рассчитываются основные параметры КВ-канала: максимальная применимая частота, групповое время запаздывания сигнала, наличие многолучевости и доплеровские искажения.

На рисунке 1 представлен суточный ход МПЧ для трассы средней широты ($45...55^\circ$ с.ш., расстояние 2500 км) в спокойных и возмущённых условиях, рассчитанный с использованием лучевой модели распространения КВ-радиоволн, а также приведены оптимальные рабочие частоты (ОРЧ), составляющие 85 % от МПЧ, которые рекомендуется использовать для обеспечения надёжной коротковолновой связи.

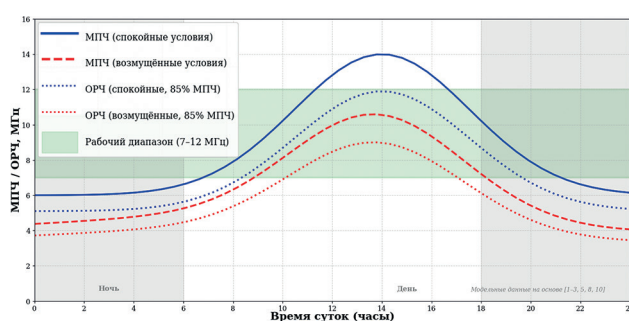


Рис. 1. Суточный ход максимальной применимой частоты для трассы средней широты в спокойных и возмущённых условиях

Из рисунка 1 видно, что в периоды геомагнитных возмущений МПЧ может снижаться на 25...35 %, особенно в утренние часы, что сужает доступный частотный диапазон и требует оперативной коррекции рабочих частот.

Сравнение результатов моделирования с данными наклонного зондирования позволяет верифицировать модель и уточнять прогнозы для конкретных трасс. Практическое применение таких моделей заключается в возможности прогнозирования доступности частотных каналов в условиях возмущённой ионосферы и выработки рекомендаций по адаптивному выбору рабочих частот.

Методы и подходы к выбору рабочих частот радиотрасс КВ-диапазона

Выбор оптимальной рабочей частоты является одной из центральных задач при организации КВ-радиотрасс. От правильности этого выбора зависит не только качество и надёжность связи, но и сама возможность установления канала в конкретных ионосферных условиях [8]. В зависимости от решаемых задач, доступных средств и уровня автоматизации сложились различные подходы к частотному планированию, которые можно классифицировать по степени учёта динамики изменения состояния ионосферы и оперативности принятия решений.

Физические механизмы и математические модели распространения КВ-радиоволн в ионосфере служат основой для решения практической

задачи — обоснованного выбора рабочих частот радиотрасс. Исторически первыми и наиболее распространёнными являются методы, основанные на статистических моделях ионосферы и долговременных прогнозах. Эти подходы используют заранее рассчитанные таблицы и карты, содержащие среднемесячные значения критических частот и максимальных применимых частот для различных трасс и сезонов [11].

В основе таких методов лежат эмпирические модели, которые базируются на многолетних данных ионосферных станций. Для расчёта МПЧ используются статистические распределения f_oF_2 , привязанные к солнечным индексам SSN и F10.7, а также к широтно-долготным координатам трассы.

Простота реализации и отсутствие необходимости в специализированной аппаратуре мониторинга делают статистические методы удобным инструментом для заблаговременного планирования частотных сеток. Они применимы для широкого круга трасс и обеспечивают приемлемую точность в спокойных ионосферных условиях. Однако в периоды геомагнитных возмущений ошибки прогноза МПЧ могут достигать 30...50 % от реальных значений, поскольку статистические модели не учитывают спорадические явления и локальные особенности состояния ионосферы вдоль конкретной трассы. Кроме того, традиционный подход к выбору рабочей частоты в диапазоне 0,8...0,9 от МПЧ, рекомендованный для обеспечения надёжности отражения не ниже 90 % [3], не позволяет в полной мере контролировать многолучевость, что ухудшает частотно-временные характеристики канала.

Дальнейшим развитием статистических подходов стали методы, использующие современные физические и эмпирические модели ионосферы. В отличие от табличных методов, эти модели позволяют рассчитывать пространственно-временное распределение электронной концентрации с учётом текущих значений солнечной активности, геомагнитных индексов и сезонно-суточных вариаций.

Прогностические методы базируются на решении лучевых уравнений для заданной трассы с использованием модели электронной концентрации, которые обеспечивают более высокую точность по сравнению со статистическими, поскольку учитывают динамику ионосферы через модельные расчёты. Они позволяют получать прогнозы с различной временной дискретностью. Вместе с тем точность таких методов ограничена в условиях сильных возмущений, особенно в высоких широтах, где модели могут

давать значительные ошибки при отсутствии актуальных входных данных об ионосферном состоянии.

Наиболее точными и оперативными являются адаптивные методы, использующие данные реального времени о состоянии ионосферы вдоль трассы. Эти подходы базируются на сети средств ионосферного зондирования: вертикального (ВЗ), наклонного (НЗ) и возвратно-наклонного (ВНЗ) зондирования, а также на приёме сигналов от радиомаяков и спутниковых навигационных систем.

Принцип действия адаптивных систем заключается в циклическом зондировании рабочих и резервных частотных каналов, измерении их качества (отношение сигнал/шум, битовая ошибка, уровень помех) и выборе наилучшего канала для связи. В системах с обратной связью информация о качестве канала передаётся от приёмной стороны к передающей, что позволяет динамически корректировать рабочую частоту. Примером реализации адаптивного подхода является метод BAFS (Burst Adaptive Frequency Selection), при котором зондирование каналов осуществляется короткими импульсными сигналами, а выбор частоты происходит на основе измерений в реальном времени без разрыва основного канала связи.

Адаптивные методы обеспечивают высокую точность в реальных ионосферных условиях, включая периоды возмущений, и позволяют автоматизировать процесс выбора частоты. Их применение особенно эффективно в условиях, когда ошибки прогноза становятся недопустимыми. Вместе с тем такие системы требуют развёртывания аппаратуры зондирования, организации каналов обратной связи, что усложняет их реализацию на мобильных и маломощных платформах.

Как показывают исследования, при нормальном уровне диффузности ионосферы значение параметра Райса может изменяться в широких пределах (от 0,2 до 100), что существенно зависит от выбора рабочей частоты относительно МПЧ. При сильной диффузности ионосферы, характерной для возмущённых условий, замирания в диапазоне отношений $f_0 / f_{МПЧ}$ от 1 до 0,4 приближаются к релеевским [12].

Современным направлением в области выбора рабочих частот являются когнитивные подходы, использующие алгоритмы машинного обучения и искусственного интеллекта. Эти методы объединяют принципы адаптивного частотного выбора с возможностью самообучения системы на основе накопленного опыта и анализа широкого спектра факторов [12].

Когнитивные системы КВ-связи способны непрерывно анализировать всю полосу КВ-диапазона, выявлять закономерности распространения сигналов и источников помех, и на основе этого прогнозируют оптимальные частоты для установления связи [4]. Применение нейросетевых алгоритмов, статистического обучения и методов подкрепления позволяет значительно повысить точность прогноза и адаптироваться к изменяющимся условиям быстрее, чем традиционные системы [6].

Экспериментальные данные показывают, что когнитивные системы способны использовать частоты вплоть до 19 МГц там, где традиционные статистические модели предсказывают их непригодность [4]. Это связано с тем, что естественные и техногенные помехи сосредоточены в нижней части КВ-диапазона, и переход на более высокие частоты обеспечивает лучшее качество канала. Потенциально когнитивные подходы обладают наиболее высокой адаптивностью, позволяя учитывать широкий спектр факторов – ионосферных, помеховых и аппаратных – при автоматизированном выборе частоты без участия оператора. Однако на современном этапе развития такие системы требуют значительных вычислительных ресурсов и больших объёмов экспериментальных данных для обучения, а их эффективность напрямую зависит от качества и актуальности исходных данных.

Заключение

Проведённый анализ показывает, что развитие методов выбора рабочих частот эволюционирует от статических статистических таблиц к интеллектуальным когнитивным системам, причём каждый из подходов сохраняет свою область применения. Статистические методы остаются основой для долгосрочного частотного планирования и работы в спокойных ионосферных условиях. Прогностические модели целесообразно использовать для расчётов с учётом текущей фазы солнечного цикла и сезонных вариаций. Адаптивные методы необходимы для обеспечения связи в условиях возмущений, когда ошибки прогноза становятся недопустимыми. Когнитивные системы являются наиболее перспективным направлением, позволяющим автоматизировать выбор частот учитывая ионосферные, помеховые и аппаратные факторы.

Выбор конкретного подхода определяется требованиями к надёжности, наличием аппаратуры мониторинга, допустимыми затратами ресурсов и условиями эксплуатации радиолинии. В перспективе наиболее эффективными будут гибридные системы, сочетающие прогностические модели, данные оперативного

зондирования и алгоритмы машинного обучения для принятия решений в реальном времени.

Таким образом, для обеспечения устойчивой КВ-радиосвязи в условиях изменяющейся внешней среды необходим комплексный подход, сочетающий долгосрочное планирование, оперативную коррекцию частот по данным

мониторинга и применение интеллектуальных алгоритмов прогнозирования. Дальнейшие исследования целесообразно направить на развитие гибридных систем адаптивного частотного планирования, интегрирующих данные глобальных сетей мониторинга ионосферы с методами машинного обучения.

Литература

1. Благовещенский Д. В. Моделирование распространения КВ-радиоволн в высоких широтах / Д. В. Благовещенский, А. В. Благовещенская // Геомагнетизм и аэронавигация. – 2016. – Т. 56. – № 5. – С. 621–630.
2. Дэвис К. Радиоволны в ионосфере: пер. с англ. / К. Дэвис. – М.: Мир, 1973. – 502 с.
3. Иванов Д. В. Эффекты дисперсии в ионосферных радиоканалах. Ч. 2. Виды частотно-временной дисперсии / Д. В. Иванов, В. А. Иванов, М. И. Рябова, В. В. Овчинников // Радиотехника. – 2024. – Т. 88. – № 12. – С. 63–77.
4. Иванов Д. В. Подходы к экспериментальному оцениванию SDR-сенсором вариаций спектральной плотности мощности помех и прогнозированию вариаций их среднего уровня при изменении полосы КВ-радиоканала / Д. В. Иванов, В. А. Иванов, Н. В. Рябова, Р. Р. Бельгибаев // Электромагнитные волны и электронные системы. – 2025. – Т. 30. – № 1. – С. 68–78.
5. Клименко М. В. Высотная протяженность зимней аномалии и её проявление в полном электронном содержании / М. В. Клименко, В. В. Клименко, И. Е. Захаренкова и др. // Химическая физика. – 2019. – Т. 38. – № 10. – С. 83–90.
6. Крюковский А. С. Математическое моделирование амплитудных, угловых и временных характеристик коротких радиоволн при слабонаклонном зондировании ионосферы / А. С. Крюковский, Д. С. Лукин, Е. В. Михалёва, Д. В. Растягаев // Радиотехника и электроника. – 2023. – Т. 68. – № 6. – С. 553–562.
7. Пашинцев В. П. Методика оценки влияния диффузности ионосферы и выбора рабочей частоты на помехоустойчивость коротковолновой связи / В. П. Пашинцев, Д. А. Белоконов, В. А. Цимбал и др. // Журнал радиоэлектроники. – 2024. – № 12.
8. Рыбаков А. И. Моделирование основных характеристик и параметров функциональных блоков и системы в целом при выборе оптимальных частотных каналов связи / А. И. Рыбаков // Экономика и качество систем связи. – 2019. – № 1 (11). – С. 13–18.
9. Семенова Н. А. Моделирование распространения КВ-радиоволн на трассе Кипр – Нижний Новгород при регистрации Z-образных ПИВ / Н. А. Семенова, Ф. И. Выборнов, С. М. Грач // Материалы 22-й Международной конференции «Современные проблемы дистанционного зондирования Земли из космоса». – М.: ИКИ РАН, 2024. – С. 490.
10. Выборнов Ф. И., Шейнер О. А. Отклик ионосферы Земли на явления солнечной активности в феврале – марте 2023 года // Космические исследования. – 2024. – Т. 62. – № 2. – С. 157–167.
11. Брюнелли Б. Е. Физика ионосферы / Б. Е. Брюнелли, А. А. Намгаладзе. – М.: Наука, 1988. – 528 с.
12. Hirvonen E. A. O. AU-Ray Program for Modeling Radio Wave Propagation in the Ionosphere / E. A. O. Hirvonen, K. Kauristie, E. Kallio // Radio Science. – 2025. – Vol. 60. – No. 8. – DOI: 10.1029/2024RS008209.

STUDY OF THE INFLUENCE OF EXTERNAL FACTORS ON THE CHOICE OF OPERATING FREQUENCIES OF HF RADIO LINKS

Veligosha A. V.⁴, Tretyakov E. A.⁵, Yurkov V. V.⁶

Keywords: *ionospheric disturbances, radio wave propagation, selection of operating frequencies, ionospheric monitoring, adaptive frequency planning.*

Abstract

The purpose of the work: *substantiation of directions for improving the stability of HF radio communications through adaptive frequency planning based on data from hardware and software ionosphere monitoring tools.*

⁴ **Aleksandr V. Veligosha**, Ph.D. of Technical Sciences, Associate Professor of Department No. 52 of the Branch of the Peter the Great Military Academy. Serpukhov, Russia. E-mail: Aveligosha@mail.ru

⁵ **Evgeny A. Tretyakov**, adjunct of the branch of the Peter the Great Military Academy. Serpukhov, Russia. E-mail: 2923201@mail.ru

⁶ **Vladislav V. Yurkov**, cadet of the branch of the Peter the Great Military Academy. Serpukhov, Russia. E-mail: Uikav@bk.ru

Research method: comprehensive analysis, generalization of empirical data and results of mathematical modeling of HF radio wave propagation in the ray approximation, taking into account background and disturbing components of electron concentration.

Results of the study: it is shown that external factors cause significant deviations of ionospheric parameters: during periods of geomagnetic disturbances, the MUF can decrease by 25–50 %, radio wave absorption increases by 20–40 dB and more, multipath propagation and fading depth increase. Regularities of seasonal-diurnal and geographical variations of electron concentration have been revealed. The necessity of transitioning from statistical and predictive methods to adaptive and cognitive frequency planning systems integrating operational ionosphere monitoring data is substantiated.

Scientific novelty consists in systematization of quantitative assessments of the influence of a complex of external factors on the selection of operating frequencies of HF radio links from the standpoint of ensuring communication stability, as well as in substantiation of the prospects for the use of hardware and software ionosphere monitoring complexes for the implementation of hybrid adaptive frequency planning systems combining predictive models, real-time data and machine learning algorithms.

References

1. Blagoveshchenskij D. V. Modelirovanie rasprostraneniya KV-radiovoln v vysokih shirotah / D. V. Blagoveshchenskij, A. V. Blagoveshchenskaya // Geomagnetizm i aehronomiya. – 2016. – V. 56. – No. 5. – Pp. 621–630.
2. Dehvis K. Radiovolny v ionosfere: per. s angl. / K. Dehvis. – M.: Mir, 1973. – 502 p.
3. Ivanov D. V. Ehffekty dispersii v ionosfernyh radiokanalakh. Ch. 2. Vidy chastotno-vremennoj dispersii / D. V. Ivanov, V. A. Ivanov, M. I. Ryabova, V. V. Ovchinnikov // Radiotekhnika. – 2024. – V. 88. – No. 12. – Pp. 63–77.
4. Ivanov D. V. Podhody k ehksperimental'nomu ocenivaniyu SDR-sensorom variacij spektral'noj plotnosti moshchnosti pomeh i prognozirovaniyu variacij ih srednego urovnya pri izmenenii polosy KV-radiokanala / D. V. Ivanov, V. A. Ivanov, N. V. Ryabova, R. R. Bel'gibaev // Ehlektronnaya fizika i ehlektronnyye sistemy. – 2025. – V. 30. – No. 1. – Pp. 68–78.
5. Klimenko M. V. Vysotnaya protyazhennost' zimnej anomalii i eyo proyavlenie v polnom ehlektronnom sodержanii / M. V. Klimenko, V. V. Klimenko, I. E. Zaharenkova i dr. // Himicheskaya fizika. – 2019. – V. 38. – No. 10. – Pp. 83–90.
6. Kryukovskij A. S. Matematicheskoe modelirovanie amplitudnyh, uglovyyh i vremennyh harakteristik korotkiy radiovoln pri slabonaklonnom zondirovanii ionosfery / A. S. Kryukovskij, D. S. Lukin, E. V. Mihalyova, D. V. Rastyagaev // Radiotekhnika i ehlektronika. – 2023. – V. 68. – No. 6. – Pp. 553–562.
7. Pashincev V. P. Metodika ocenki vliyaniya diffuznosti ionosfery i vybora rabochej chastoty na pomehoustoichivost' korotkovolnovoy svyazi / V. P. Pashincev, D. A. Belokon', V. A. Cimbal i dr. // Zhurnal radioehlektroniki. – 2024. – No. 12.
8. Rybakov A. I. Modelirovanie osnovnyh harakteristik i parametrov funktsional'nyh blokov i sistemy v celom pri vybore optimal'nyh chastotnyh kanalov svyazi / A. I. Rybakov // Ehkonomika i kachestvo sistem svyazi. – 2019. – No. 1 (11). – Pp. 13–18.
9. Semenova N. A. Modelirovanie rasprostraneniya KV-radiovoln na trasse Kipr – Nizhnij Novgorod pri registratsii Z-obraznyh PIV / N. A. Semenova, F. I. Vybornov, S. M. Grach // Materialy 22-j Mezhdunarodnoj konferentsii «Sovremennyye problemy distantsionnogo zondirovaniya Zemli iz kosmosa». – M.: IKI RAN, 2024. – P. 490.
10. Vybornov F. I., Shejner O. A. Otklik ionosfery Zemli na yavleniya solnechnoj aktivnosti v fevrale – marte 2023 goda // Kosmicheskie issledovaniya. – 2024. – V. 62. – No. 2. – Pp. 157–167.
11. Bryunelli B. E. Fizika ionosfery / B. E. Bryunelli, A. A. Namgaladze. – M.: Nauka, 1988. – 528 p.
12. Hirvonen E. A. O. AU-Ray Program for Modeling Radio Wave Propagation in the Ionosphere / E. A. O. Hirvonen, K. Kauristie, E. Kallio // Radio Science. – 2025. – Vol. 60. – No. 8. – DOI: 10.1029/2024RS008209.



СПОСОБ ОБЕСПЕЧЕНИЯ ВЫБОРА И ОБОСНОВАНИЯ ПЕРСПЕКТИВНЫХ СРЕДСТВ СВЯЗИ ДЛЯ ПОСТРОЕНИЯ АДАПТИВНОЙ СИСТЕМЫ СВЯЗИ ТАКТИЧЕСКОГО ЗВЕНА УПРАВЛЕНИЯ

Слепова В. П.¹

DOI:10.21681/3034-4050-2026-5-100-105

Ключевые слова: адаптивная система связи, выбор перспективных образцов, интегральный показатель, дерево свойств, нормализация, метод анализа иерархий.

Аннотация

Цель работы: разработать способ выбора и обоснования перспективных средств связи для построения адаптивной системы связи тактического звена управления на основе формализованного оценивания свойств образцов техники, определяющих их способность обеспечивать перестроение топологии, изменение режимов функционирования и сохранение управляемости в условиях динамической обстановки.

Метод: системный и функциональный анализ.

Результаты: предложен порядок выбора перспективных средств связи, основанный на иерархической системе показателей адаптивности. Система включает функциональный, конструктивно-технологический, эксплуатационный и организационно-управленческий блоки. Разработана процедура нормализации исходных характеристик, рекурсивного агрегирования частных показателей и формирования интегрального индекса пригодности образца для построения адаптивной системы связи тактического звена управления. Предложен критерий выбора перспективного средства связи с учетом ограничений по минимально допустимым значениям частных и групповых показателей. Выполнена апробация подхода на образцах Р-149МА1 и Р-142НМР.

Научная новизна: выбор перспективных средств связи представлен как формализованная многокритериальная процедура, в которой адаптивность рассматривается не как вспомогательная характеристика, а как самостоятельное системное свойство, определяющее пригодность образца для включения в адаптивную систему связи тактического звена управления.

Введение

Современные условия применения подразделений тактического звена управления характеризуются высокой изменчивостью обстановки, ростом интенсивности информационного обмена, расширением сетевых принципов управления и повышением требований к устойчивости связи. В этих условиях эффективность управления войсками во многом определяется не только наличием работоспособных средств связи, но и способностью системы связи оперативно изменять свою структуру, режимы работы и порядок взаимодействия элементов [1, 2].

Воздействие деструктивных факторов, перегрузка каналов, отказ отдельных технических средств, изменение условий распространения радиоволн и необходимость перераспределения информационных потоков требуют от системы связи тактического звена управления свойства адаптивности. При оценке эксплуатационных свойств техники существенны техническая готовность, выработка ресурса и режимы эксплуатации; их взаимосвязь исследована в работе [3].

В настоящей статье адаптивность рассматривается шире технической готовности: как способность образца обеспечивать перестроение топологии сети и изменение режимов функционирования в меняющихся условиях.

Выбор технических средств по совокупности частных характеристик относится к задачам многокритериального оценивания. В работе [4] предложен метод определения обобщенных показателей эффективности технических средств для выбора предпочтительного варианта в составе организационно-технической системы. В обзоре [5] показана необходимость учитывать ограничения методов многокритериального принятия решений. Поэтому оценивание по разрозненным характеристикам без единой процедуры сопоставления не обеспечивает достаточной обоснованности выбора.

В связи с этим возникает необходимость разработки способа, который позволял бы не только оценивать отдельные свойства средств связи, но и использовать результаты оценки для обоснованного выбора перспективных образцов.

¹ Слепова Валентина Павловна, адъюнкт Военной академии связи им. С. М. Буденного. Санкт-Петербург, Россия. E-mail: slepovavalentina719@gmail.com

Такой способ должен учитывать функциональные возможности, конструктивно-технологические особенности, эксплуатационные свойства и организационно-управленческую пригодность средств связи, а итоговая оценка должна быть представлена в форме единого интегрального показателя. Общие вопросы оценки эффективности вооружения и военной техники рассматриваются в монографии [6].

Цель настоящей статьи состоит в разработке способа обеспечения выбора и обоснования перспективных средств связи для построения адаптивной системы связи тактического звена управления на основе иерархической системы показателей, процедур нормализации и рекурсивного агрегирования частных характеристик.

Модель выбора перспективных средств связи и постановка задачи

Рассмотрим множество сравниваемых образцов средств связи

$$S = \{S_1, S_2, \dots, S_q\}, \quad (1)$$

где S_i – i -й образец средства связи, включаемый в процедуру выбора; q – число рассматриваемых вариантов.

Каждый образец S_i характеризуется совокупностью исходных показателей.

$$X_i = \{x_{ijmn}\}, \quad (2)$$

где индекс i соответствует оцениваемому образцу, индекс j – блоку показателей, индекс m – группе, а индекс n – частному измеряемому показателю.

В качестве основных блоков оценки принимаются:

F – функциональная адаптивность;

K – конструктивно-технологическая адаптивность;

E – эксплуатационная адаптивность;

O – организационно-управленческая адаптивность.

Тогда множество блоков оценки задается выражением

$$J = \{F, K, E, O\}. \quad (3)$$

Функциональная адаптивность отражает способность средства связи обеспечивать изменение режимов функционирования, маршрутизацию, взаимодействие с другими элементами сети и поддержку различных способов организации информационного обмена.

Конструктивно-технологическая адаптивность характеризует модульность, возможность модернизации, совместимость с перспективными

техническими решениями и способность образца к наращиванию функциональных возможностей.

Эксплуатационная адаптивность определяется пригодностью средства связи к применению в различных условиях обстановки, удобством обслуживания, ремонтпригодностью, устойчивостью к эксплуатационным ограничениям и возможностью быстрого восстановления работоспособности.

Организационно-управленческая адаптивность отражает возможность включения образца в существующие и перспективные контуры управления, соответствие требованиям жизненного цикла, совместимость с процедурами планирования, контроля состояния и модернизации. Методический пример планирования и управления процессами жизненного цикла техники на основе сетевой модели представлен в работе [7].

Задача выбора перспективного средства связи заключается в определении такого образца, который обеспечивает наибольшее значение интегрального показателя адаптивности при выполнении заданных ограничений:

$$S^* = \arg \max_{S_i \in S} I_i, \quad (4)$$

при условиях

$$B_{ij} \geq B_j^{\min}, j \in J; \quad (5)$$

$$P_{ijmn} \geq P_{jmn}^{\min}, \quad (6)$$

где I_i – интегральный индекс адаптивности i -го образца; B_{ij} – значение j -го блока для i -го образца; $B_j^{\min}$ – минимально допустимое значение соответствующего блока; P_{ijmn} – нормализованное значение частного показателя; $P_{jmn}^{\min}$ – минимально допустимое значение частного показателя.

В такой постановке выбор средства связи рассматривается не как простое ранжирование по одному техническому параметру, а как многокритериальная процедура, учитывающая соответствие образца требованиям адаптивной системы связи тактического звена управления.

Основные результаты

Для реализации предложенного способа используется четырехуровневая иерархическая модель показателей. Первый уровень образует интегральный индекс адаптивности I_i , который характеризует обобщенную пригодность i -го образца для построения адаптивной системы связи. Второй уровень включает блоки F, K, E, O . Третий уровень представлен группами показателей внутри каждого блока. Четвертый уровень составляют базовые измеряемые показатели, получаемые по результатам испытаний, анализа

технической документации, экспертного оценивания и опыта эксплуатации.

Исходные показатели имеют различную физическую природу и могут измеряться в разных единицах. Поэтому предварительно выполняется их нормализация, необходимая для приведения разнородных показателей к общей шкале [8]. Для i -го образца нормализованное значение частного показателя определяется в общем виде:

$$P_{ijmn} = N_{jmn}(x_{ijmn}), \quad (7)$$

где N – функция нормализации, выбранная с учетом смысла соответствующего показателя.

Если увеличение исходного значения повышает адаптивность, применяется прямая нормализация по минимальному и максимальному значениям (min–max) [8, с. 2–3]:

$$P_{ijmn} = \frac{x_{ijmn} - x_{jmn}^{\min}}{x_{jmn}^{\max} - x_{jmn}^{\min}}. \quad (8)$$

Если увеличение исходного значения ухудшает оценку, используется обратная нормализация:

$$P_{ijmn} = \frac{x_{jmn}^{\max} - x_{ijmn}}{x_{jmn}^{\max} - x_{jmn}^{\min}}. \quad (9)$$

Для показателей, имеющих нормативный или пороговый характер, может применяться пороговая функция:

$$P_{ijmn} = \begin{cases} 1, & x_{ijmn} \geq x_{jmn}^{\text{req}} \\ \frac{x_{ijmn}}{x_{jmn}^{\text{req}}}, & x_{ijmn} < x_{jmn}^{\text{req}} \end{cases}, \quad (10)$$

где требуемое значение показателя задается нормативом или условиями применения.

После нормализации выполняется рекурсивное агрегирование с использованием взвешенной суммы. Пример последовательного применения нормализации min–max и взвешенного среднего с учетом иерархии показателей представлен в [8]. Сначала частные показатели объединяются в групповой показатель:

$$G_{ijm} = \sum_n u_{jmn} P_{ijmn}, \quad (11)$$

где G_{ijm} – значение m -й группы j -го блока для i -го образца; u_{jmn} – весовой коэффициент частного показателя.

Далее групповые показатели агрегируются в значение блока:

$$B_{ij} = \sum_m v_{jm} G_{ijm}, \quad (12)$$

где v_{jm} – весовой коэффициент m -й группы внутри j -го блока.

Итоговый интегральный индекс адаптивности определяется выражением

$$I_i = \sum_{j \in J} w_j B_{ij}, \quad (13)$$

где w_j – весовой коэффициент j -го блока, удовлетворяющий условию

$$\sum_{j \in J} w_j = 1. \quad (14)$$

Весовые коэффициенты u , v и w могут определяться методом анализа иерархий на основе парных сравнений элементов. При использовании экспертных суждений необходимо проверять согласованность матриц парных сравнений; процедура ее повышения рассмотрена в работе [9]. Выбор процедуры определения весов должен соответствовать принятой модели оценки и характеру исходных данных.

Для повышения обоснованности выбора перспективного средства связи предлагается учитывать не только максимальное значение интегрального индекса, но и сбалансированность профиля адаптивности. Для этого может использоваться показатель минимального блока:

$$B_i^{\min} = \min_{j \in J} B_{ij}. \quad (15)$$

Если два образца имеют близкие значения интегрального индекса, предпочтение целесообразно отдавать варианту с более высоким значением минимального блока, поскольку такой образец обладает менее выраженными ограничивающими факторами.

С учетом этого уточненный критерий выбора может быть представлен в виде

$$S^* = \arg \max_{S_i \in S} (\alpha I_i + (1 - \alpha) B_i^{\min}), \quad (16)$$

где α_{Ipha} – коэффициент значимости интегральной оценки, принимающий значения от 0 до 1.

Предложенный способ реализуется в виде последовательности этапов.

На первом этапе определяется цель выбора: оснащение подразделений, модернизация существующей системы связи, формирование требований к перспективному образцу либо сравнительная оценка вариантов технического оснащения.

На втором этапе задаются сценарии применения, определяются ограничения, формируется перечень сравниваемых образцов и устанавливается система показателей.

На третьем этапе выполняется сбор исходных данных, формируется массив исходных характеристик и проводится нормализация по формулам (7)–(10).

На четвертом этапе рассчитываются групповые показатели, значения блоков и интегральный индекс по формулам (11)–(13).

На пятом этапе осуществляется проверка ограничений (5) и (6), после чего выполняется ранжирование образцов по критериям (4) или (16).

На шестом этапе формируются рекомендации по выбору средства связи, выявляются ограничивающие факторы и определяются направления модернизации.

Апробация способа выполнена на двух штатных образцах техники связи: Р-149МА1 и Р-142НМР. По результатам нормализации и рекурсивного агрегирования получены значения интегрального индекса:

$$I_{R-149MA1} = 0,81; \quad (17)$$

$$I_{R-142NMR} = 0,85. \quad (18)$$

Полученные значения показывают, что образец Р-142НМР имеет более высокий интегральный уровень адаптивности. При этом анализ структуры показателей позволяет установить не только итоговое преимущество, но и причины различий между образцами. Для Р-149МА1 одним из ограничивающих факторов выступает функциональная адаптивность, связанная с возможностями перестроения режимов работы и взаимодействия с элементами сети. Для Р-142НМР профиль адаптивности является более сбалансированным, что свидетельствует о более равномерном распределении свойств по функциональному, конструктивно-технологическому, эксплуатационному и организационно-управленческому блокам.

Таким образом, предложенный способ позволяет не только выбрать предпочтительный образец, но и обосновать выбор через структуру показателей. Это особенно важно при формировании требований к перспективным средствам связи, поскольку интегральный индекс показывает общий уровень пригодности, а частные и групповые показатели указывают, какие свойства необходимо развивать в первую очередь.

Практическая значимость способа заключается в возможности его применения на различных этапах жизненного цикла средств связи: при разработке тактико-технических требований,

сравнении существующих образцов, планировании модернизации, оценке результатов опытной эксплуатации и формировании предложений по построению адаптивной системы связи тактического звена управления. В более широком контексте обоснование перспективного облика силовых компонентов военной организации рассматривается в монографии [10]; настоящая работа посвящена частной задаче выбора средств связи.

Заключение

Разработан способ обеспечения выбора и обоснования перспективных средств связи для построения адаптивной системы связи тактического звена управления. В основу способа положена иерархическая модель показателей, позволяющая связать частные измеряемые характеристики средств связи с интегральным индексом адаптивности.

Предложенная процедура включает нормализацию исходных показателей, рекурсивное агрегирование, формирование интегральной оценки, проверку ограничений и выбор перспективного образца по заданному критерию. В отличие от подходов, ориентированных на отдельные технические характеристики, разработанный способ позволяет учитывать функциональные, конструктивно-технологические, эксплуатационные и организационно-управленческие свойства средств связи в единой системе оценивания.

Апробация на образцах Р-149МА1 и Р-142НМР показала возможность количественного сравнения средств связи и выявления ограничивающих факторов адаптивности. Полученные значения 0,81 и 0,85 подтверждают применимость предложенного способа для обоснования выбора перспективного образца и формирования направлений модернизации.

Использование разработанного способа создает научно-методическую основу для перехода от фрагментарной экспертной оценки средств связи к формализованному выбору образцов, обеспечивающих построение адаптивной системы связи тактического звена управления.

Литература

1. Воробьев И. Г., Романов В. М. Развитие форм и способов построения системы связи тактического звена управления // Военная мысль. – 2022. – № 6. – С. 62–71.
2. Тишков В. В., Иванов В. Г., Лукьянчик В. Н. Обоснование облика построения перспективных комплексов и средств связи на основе опыта организации связи при проведении специальной военной операции // Военная мысль. – 2023. – № 9. – С. 59–72.
3. Буравлев А. И., Белорозов М. С. Модели управления технической готовностью ВВСТ при планировании и реализации государственной программы вооружения // Вооружение и военная техника. – 2022. – № 1(59). – С. 12–32.

4. Кожевин Д. Ф., Матвеев А. В., Самигуллин Г. Х., Смирнов А. С. Метод многокритериальной оценки эффективности технических средств в организационно-технических системах // Вестник Санкт-Петербургского университета ГПС МЧС России. – 2023. – № 4. – С. 59–70. – DOI: 10.61260/2218-13X-2023-4-59-70.
5. Чечнев В. Б. Анализ и классификация многокритериальных методов принятия решений // Онтология проектирования. – 2024. – Т. 14. – № 4(54). – С. 607–624. – DOI: 10.18287/2223-9537-2024-14-4-607-624.
6. Буренок В. М. Методы оценки эффективности вооружения и военной техники / под ред. В. М. Буренка. М.: Издательский дом «Граница», 2022. – 264 с.
7. Дубовский В. А., Курбанов А. Х., Плотноков В. А. Сетевая модель планирования и управления процессами жизненного цикла вооружения и военной техники: процедура построения и реализации // Известия РАРАН. – 2020. – № 3 (113). – С. 39–45.
8. Becker W., Caperna G., Del Sorbo M., Norlén H., Papadimitriou E., Saisana M. COINr: An R package for developing composite indicators // Journal of Open Source Software. – 2022. – Vol. 7. – No. 78. – Article 4567. – DOI: 10.21105/joss.04567.
9. Salomon V. A. P., Gomes L. F. A. M. Consistency Improvement in the Analytic Hierarchy Process // Mathematics. – 2024. – Vol. 12. – No. 6. – Article 828. – DOI: 10.3390/math12060828.
10. Буренок В. М. Концепция обоснования перспективного облика силовых компонентов военной организации Российской Федерации. М.: Издательство «Граница», 2018. – 520 с.

METHOD FOR SELECTING AND JUSTIFYING PROMISING COMMUNICATION EQUIPMENT FOR BUILDING AN ADAPTIVE COMMUNICATION SYSTEM AT THE TACTICAL COMMAND LEVEL

Slepova V. P.²

Keywords: adaptive communication system, selection of promising samples, integral indicator, property tree, normalization, method of hierarchy analysis.

Abstract

The purpose of the work is to develop a method for the selection and justification of promising means of communication for the construction of an adaptive communication system of the tactical control link on the basis of a formalized assessment of the properties of equipment samples, which determine their ability to ensure the rebuilding of the topology, changing the modes of operation and maintaining controllability in a dynamic environment.

Method: system and functional analysis.

Results: the procedure for selecting promising means of communication, based on the hierarchical system of indicators of adaptability, is proposed. The system includes functional, constructive-technological, operational, organizational-managerial blocks. A procedure for normalization of initial characteristics, recursive aggregation of partial indicators and formation of an integral index of sample suitability for building an adaptive communication system of tactical control is developed. A criterion for choosing a promising means of communication is proposed, taking into account restrictions on the minimum permissible values of partial and group indicators.

Scientific novelty: the choice of promising means of communication is presented as a formalized multi-criteria procedure, in which adaptability is considered not as an auxiliary characteristic, but as an independent system property that determines the suitability of the sample for inclusion in the adaptive communication system of the tactical control link.

References

1. Vorob'yov I. G., Romanov V. M. Razvitie Form i sposobov postroeniya sistemy svyazi takticheskogo zvena upravleniya // Voennaya mysl'. – 2022. – No. 6. – Pp. 62–71.
2. Tishkov V. V., Ivanov V. G., Luk'yanchik V. N. Obosnovanie oblika postroeniya perspektivnykh kompleksov i sredstv svyazi na osnove opyta organizatsii svyazi pri provedenii special'noj voennoj operatsii // Voennaya mysl'. – 2023. – No. 9. – Pp. 59–72.
3. Buravlev A. I., Belorozov M. S. Modeli upravleniya tehnikeskoy gotovnost'yu VVST pri planirovani i realizatsii gosudarstvennoy programmy vooruzheniya // Vooruzhenie i voennaya tekhnika. – 2022. – No. 1 (59). – Pp. 12–32.
4. Kozhevina D. F., Matveev A. V., Samigullin G. H., Smirnov A. S. Metod mnogokriterial'noy ocenki ehffektivnosti tehnikeskikh sredstv v organizatsionno-tehnicheskikh sistemah // Vestnik Sankt-Peterburgskogo universiteta GPS MCHS Rossii. – 2023. – No. 4. – Pp. 59–70. – DOI: 10.61260/2218-13X-2023-4-59-70.
5. Chechnev V. B. Analiz i klassifikatsiya mnogokriterial'nykh metodov prinyatiya resheniy // Ontologiya proektirovaniya. – 2024. – V. 14. – No. 4 (54). – Pp. 607–624. – DOI: 10.18287/2223-9537-2024-14-4-607-624.
6. Burenok V. M. Metody ocenki ehffektivnosti vooruzheniya i voennoy tekhniki / pod red. V. M. Burenka. M.: Izdatel'skiy dom «Granica», 2022. – 264 p.

² Valentina P. Slepova, adjunct of the Military Academy of Communications named after S. M. Budyonny. St. Petersburg, Russia. E-mail: slepovavalentina719@gmail.com

7. Dubovskij V. A., Kurbanov A. H., Plotnikov V. A. Setevaya model' planirovaniya i upravleniya processami zhiznennogo cikla vooruzheniya i voennoj tehniki: procedura postroeniya i realizacii // Izvestiya RARAN. – 2020. – No. 3(113). – Pp. 39–45.
8. Becker W., Caperna G., Del Sorbo M., Norlén H., Papadimitriou E., Saisana M. COINr: An R package for developing composite indicators // Journal of Open Source Software. – 2022. – Vol. 7. – No. 78. – Article 4567. – DOI: 10.21105/joss.04567
9. Salomon V. A. P., Gomes L. F. A. M. Consistency Improvement in the Analytic Hierarchy Process // Mathematics. – 2024. – Vol. 12. – No. 6. – Article 828. – DOI: 10.3390/math12060828.
10. Burenok V. M. Konceptiya obosnovaniya perspektivnogo oblika silovyh komponentov voennoj organizacii Rossijskoj Federacii. M.: Izdatel'stvo «Granica», 2018. – 520 p.



The journal is registered by the Federal Service for
Supervision of Communications, Information Technology
and Mass Communications.

Registration Certificate
PI № FS77-88069 from 16/08/2024

Editor-in-Chief

Vasily IVANOV, *Dr.Sc., Professor, Moscow*

Assistant Editor-in-Chief

Grigory MAKARENKO, *Senior Research Fellow, Moscow*

Board of Trustees

Alexander RUBIS, *Ph.D., Deputy Head of the Main Directorate
of Communications of the Armed Forces of the Russian Federation
for Armament (Chairman)*

Roman PANKOV, *Ph.D., Head of the Federal State Budgetary
Institution 16 Central Research and Testing Institute*

Evgeny KHARCHENKO, *Ph.D., Ass. Professor (Secretary)*

Editorial Board

Nikolay ACHKASOV, *Dr.Sc., Professor, St. Petersburg*

Anton BYCHKOV, *Dr.Sc., Ass. Professor, St. Petersburg*

Mikhail BUINEVICH, *Dr.Sc., Professor, St. Petersburg*

Evgeny GLUSHANKOV, *Dr.Sc., Professor, St. Petersburg*

Igor GRUDININ, *Dr.Sc., Professor, St. Petersburg*

Sergey IVANOV, *Dr.Sc., Professor, St. Petersburg*

Alexander KOZACHOK, *Dr.Sc., Ass. Professor, Orel*

Andrey KOSTOGRYZOV, *Dr.Sc., Professor, Moscow*

Pavel KUZIN, *Ph.D., Ass. Professor, St. Petersburg*

Sergey MAKARENKO, *Dr.Sc., Professor, St. Petersburg*

Alexey MARKOV, *Dr.Sc., Professor, Moscow*

Evgeny NOVIKOV, *Dr.Sc., Ass. Professor, St. Petersburg*

Andrey PRIVALOV, *Dr.Sc., Professor, St. Petersburg*

Maxim PYLINSKY, *Dr.Sc., Professor, Belarus*

Gennady RYZHOV, *Dr.Sc., Professor, Moscow*

Nikolay SAVISHCHENKO, *Dr.Sc., Professor, St. Petersburg*

Yuriy STARODUBTSEV, *Dr.Sc., Professor, St. Petersburg*

Pavel FEDYUNIN, *Dr.Sc., Professor, Voronezh*

Oleg FINKO, *Dr.Sc., Professor, Krasnodar*

Vladimir TSYMBAL, *Dr.Sc., Professor, Serpukhov*

Mikhail CHERNYSHOV, *Dr.Sc., Professor, St. Petersburg*

Founder and publisher

Federal State Budgetary Institution
«16 Central Research and Testing Institute»
of the Ministry of Defense
of the Russian Federation

Signed to the press on 15/10/2026

The total circulation is 120 copies. The price is free

Postal address: 1st Rupasovsky lane, 1, 141006,
Mytishchi, Moscow region, Russia

E-mail: editor.tis@yandex.ru. Tel.: +7 (985) 939-75-01

The requirements for the manuscripts are posted
on the website: <https://telemil.ru/>

CONTENTS

SYSTEM ANALYSIS OF MILITARY SYSTEMS

EVALUATION OF DYNAMIC DATA IN THE CONTEXT OF MODERN METHODOLOGIES

Lukashenok V. I., Panyayev A. I., Izotov D. Yu 2

DEVELOPMENT OF A METHODOLOGY FOR ANALYZING AND IMPROVING THE STRUCTURAL SECRECY OF DATA TRANSMISSION NETWORKS

Slami Ali Yusuf 12

DIRECTIONS OF DEVELOPMENT AND APPLICATION OF WIRELESS BROADBAND ACCESS IN THE COMMUNI- CATION SYSTEM TACTICAL COMMAND AND CONTROL

Lukyanchik V. N., Kartashev A. V., Vasilyeva T. G 21

INFORMATION CONFRONTATION IN THE MILITARY SPHERE

ANALYSIS OF THE EFFICIENCY OF THE Δ -LAYER OF INDISTINGUISHABILITY OF PHASE-SHIFT KEYED SIGNALS RECEIVED UNDER NONCOHERENT INTENTIONAL INTERFERENCE

Neguritsa A. O 33

PROPOSALS FOR THE CONSTRUCTION OF AN AUTOMATED COMMUNICATION CONTROL SYSTEM FOR THE TACTICAL CONTROL LEVEL

Ivanov V. G., Sorokin A. Yu., Lukyanchik V. N 39

MILITARY CONTROL, COMMUNICATIONS AND NAVIGATION SYSTEMS

DIGITAL TRANSFORMATION – NEW TECHNOLOGIES FOR SPECIAL-PURPOSE COMMUNICATION NETWORKS. Part I

Lukashev A. V 50

APPLICATION OF RECURRENT NEURAL NETWORKS TO DETECT HIDDEN ANOMALIES IN EVENT LOGS OF AUTOMATED MILITARY SYSTEMS

Sayenko I. B., Tsygnyatov V. B., Sazhina A. V 59

METHODS OF ORGANIZING THE FUNCTIONING OF A VIDEO STREAMING SYSTEM IN MODERN COMBAT CONDITIONS

Lebedev P. V., Zhivodernikov A. Yu 67

MODELING OF THE ROUTING PROBLEM IN THE DATA TRANSMISSION NETWORK BY THE PROBABILITY OF TIMELY DELIVERY OF MESSAGES

Kurashev Z. V 77

MILITARY ELECTRONICS OF MILITARY COMPLEXES

PARAMETRIC SYNTHESIS OF A MULTIVIBRATOR UNDERGROUND ANTENNA OPERATING IN DISSIPATIVE LAYERED MEDIA

Leonyuk A. S., Yurtaev A. S., Ismail M. M 83

STUDY OF THE INFLUENCE OF EXTERNAL FACTORS ON THE CHOICE OF OPERATING FREQUENCIES OF HF RADIO LINKS

Veligosh A. V., Tretyakov E. A., Yurkov V. V 91

METHOD FOR SELECTING AND JUSTIFYING PROMISING COMMUNICATION EQUIPMENT FOR BUILDING AN ADAPTIVE COMMUNICATION SYSTEM AT THE TACTICAL COMMAND LEVEL

Slepova V. P 100