# ТЕЛЕКОММУНИКАЦИИ И СВЯЗЬ

**НАУЧНЫЙ РЕЦЕНЗИРУЕМЫЙ ЖУРНАЛ**
№ 2 (11) 2026 г.
Выходит 6 раз в год

Журнал заререгистрирован 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.





**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. Селезенев – *отв. секретарь*, С. С. Игнатов – *верстка*, А. В. Матюшин – *маркетинг и подписка*

Подписано к печати 15.04.2026 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




Подписка на журнал осуществляется в 2026 году через редакцию журнала

# ИССЛЕДОВАНИЕ ПОМЕХОУСТОЙЧИВОСТИ СИСТЕМ MIMO ПРИ ИСПОЛЬЗОВАНИИ МЕТОДА ОБНУЛЕНИЯ

***Савищенко Н. В.[1], Пелин А. А.[2]***

**DOI:10.21681/3034-4050-2026-2-2-17**

***Ключевые слова:*** *беспроводные системы связи, теория информации, цифровая обработка сигналов, каналы с замираниями, многоантенные системы, предварительное кодирование, метод обнуления, специальные интегральные функции.*

***Аннотация***

***Целью статьи*** *является анализ эффективности метода обнуления при приеме сигналов в системах MIMO (Multiple Input Multiple Output) и получение точных аналитических выражений для вероятности ошибки с использованием теории потенциальной помехоустойчивости и теории специальных функций.*

***Методы исследования:*** *используется комплексный подход, сочетающий строгие аналитические расчеты и имитационное моделирование в среде MATLAB для оценки эффективности пространственной фильтрации сигналов методом обнуления в системах MIMO.*

*1. Расчет вероятности битовой ошибки BER (Bit Error Rate) для детектора обнуления производится на основе анализа статистических свойств обратной корреляционной матрицы канала. Вывод выражений для помехоустойчивости выполнен с использованием аппарата специальных интегральных функций (функция Гаусса, Т-функция Оуэна) в соответствии с методикой, изложенной в монографии «Специальные интегральные функции, применяемые в теории связи» [1]. Методика позволяет получить строгие теоретические оценки производительности.*

*2. Имитационное моделирование: для верификации полученных аналитических выражений и исследования поведения системы в условиях реальной сигнально-помеховой обстановки разработана имитационная модель канала MIMO с рэлеевскими замираниями в среде MATLAB.*

***Результаты исследования:*** *полученные аналитические и экспериментальные данные раскрывают специфику работы метода обнуления в системах MIMO. В частности, установлено, что метод обнуления (ZF – Zero Forcing) позволяет полностью устранить межсимвольную интерференцию (межканальные помехи) за счет инверсии матрицы канала. Однако моделирование выявило ключевой недостаток метода – эффект усиления шума (noise enhancement), который проявляется при плохой обусловленности канальной матрицы. Сравнительный анализ показал, что в области низких отношений сигнал/шум метод обнуления уступает алгоритму MMSE (Minimum Mean Square Error, минимальная среднеквадратичная ошибка) по энергетической эффективности, но демонстрирует высокую эффективность и линейный рост пропускной способности при высоких значениях SNR (Signal-to-Noise Ratio). Подтверждена высокая сходимость результатов расчета по предлагаемой аналитической методике (через спецфункции) с результатами Монте-Карло моделирования.*

***Научная новизна работы:*** *заключается в адаптации математического аппарата специальных интегральных функций для точного расчета помехоустойчивости при использовании метода обнуления с учетом статистических характеристик. В отличие от традиционных оценок, базирующихся на асимптотических приближениях, предложенный подход позволяет получить строгие количественные оценки вероятности ошибки приема многопозиционных сигналов линейного детектора в условиях рэлеевских замираний, что повышает достоверность прогнозирования качества связи при проектировании антенных систем.*

## 1. Введение

Эволюция беспроводных телекоммуникаций представляет собой непрерывный процесс, движимый возрастающими требованиями к скорости передачи данных, надежности, помехоустойчивости и пропускной способности. От ранних радиосистем до современных сетей сотовой связи и Wi-Fi (Wireless Fidelity), каждая новая веха в развитии была ответом на растущие потребности потребителей. Изначально беспроводные системы полагались на простейшие конфигурации, которые, несмотря на свою эффективность для базовых задач, столкнулись с фундаментальными ограничениями по мере усложнения информационных потоков и увеличения числа подключенных устройств.

В данном контексте системы с одной антенной на передающей стороне и одной антенной на приёмной стороне SISO (Single Input Single Output) и системы с несколькими антеннами на передающей и приёмных сторонах MIMO занимают центральное место в современной

1 Савищенко Николай Васильевич, доктор технических наук, профессор, профессор кафедры общепрофессиональных дисциплин Военной академии связи им. С. М. Буденного, Санкт-Петербург, Россия. E-mail: snikaspb@mail.ru

2 Пелин Артем Александрович, адъюнкт кафедры общепрофессиональных дисциплин Военной академии связи им. С. М. Буденного, Санкт-Петербург, Россия. E-mail: PelinVUC@yandex.ru

беспроводной связи. Система SISO представляет собой традиционный подход, использующий одну антенну для передачи и одну для приема данных [5]. Вышеуказанная конфигурация, хотя и проста в проектировании и экономична, обладает ограниченными возможностями по использованию пространственных ресурсов. В отличие от неё, система MIMO является серьёзным достижением, которое преодолевает ограничения SISO, используя несколько антенн как на передающей, так и на принимающей стороне для улучшения производительности и пропускной способности беспроводных сетей [5–7].

Фундаментальные математические пределы пропускной способности многоантенных архитектур в условиях многолучевых замираний были впервые строго сформулированы в ставшей классической работе Дж. Фошини (G. J. Foschini) [2]. Развитие данного математического аппарата, подробно изложенное в авторитетных зарубежных монографиях (например, под общей редакцией Э. Бильери и Х. Пора [3]), заложило базис современного пространственного кодирования. Сегодня концепция MIMO трансформировалась в технологии массированных антенных решеток (Massive MIMO) [4], что сделало вопросы поиска низкобюджетных линейных фильтров пространственного разделения потоков (ZF и MMSE) как никогда актуальными для международной инженерной школы.

Переход от системы SISO к системе MIMO является не просто постепенным улучшением, а существенным сдвигом, обусловленным возрастающим спросом на обеспечение скорости передачи. Системы SISO сталкиваются с присущими им ограничениями, в частности, с логарифмическим увеличением пропускной способности с ростом отношения сигнал/шум, (SNR) что означает убывающую отдачу от увеличения мощности или полосы пропускания. Технология MIMO появилась как необходимое решение для преодоления существующих ограничений, поскольку предоставляет возможность использовать пространственное разнесение и передачу. Такая закономерность – выявление фундаментального узкого места в существующей технологии и последующее использование нового физического измерения для его преодоления – является повторяющейся темой в инженерии. Успех технологии MIMO подтверждает стратегию поиска многомерных решений одномерных проблем в телекоммуникации, предполагая, что будущие достижения также могут зависеть от использования других недостаточно используемых физических явлений или вычислительных парадигм [8].

## 2. Основы технологии SISO

Принципы работы и архитектура. Система беспроводной связи, которая использует одну антенну для передачи и одну для приема данных называется SISO [5, 7]. Данная конфигурация является базовой и традиционной в радиотехнике. Архитектура SISO отличается простотой, что приводит к снижению сложности аппаратного обеспечения и экономической эффективности [5, 7].

В системах распределенных антенн (Distributed Antenna System, DAS) технология SISO позволяет развертывать отдельные антенны в различных местах для улучшения покрытия сигнала и пропускной способности в определенной области.

*Математическая модель канала связи SISO*. Математическая модель канала SISO описывает взаимосвязь между передаваемым и принимаемым сигналом.

Входное-выходное соотношение канала SISO может быть представлено следующим образом [9]:

$$y(t) = h\, s_r(t) + n(t),\ r = 0,..., M-1,\ t \in [0,T], \qquad (1)$$

где $y(t)$ – принятый комплексный сигнал (отсчет на стороне приемника); $s_r(t)$ – переданный информационный символ (со средней энергией $E_r$); $h$ – комплексный коэффициент передачи (замирания) скалярного радиоканала. Его амплитуда характеризует затухание, а фаза – сдвиг фазы радиосигнала. Чаще всего модель $h$ описывается как комплексная случайная величина с рэлеевским или райсовским законом распределения; $n(t)$ – аддитивный белый гауссовский шум (АБГШ) в форме комплексной случайной величины $a \in \mathcal{CN}(0,\sigma_n^2)$, где $\sigma_n^2 = N_0/2$ и $N_0$ – односторонняя спектральная плотность мощности шума. Для рэлеевских замираний квадратурные составляющие имеют нулевое математическое ожидание, а для райсовских замираний одна из квадратурных составляющих имеет ненулевое математическое ожидание. Пропускная способность канала Шеннона. Теоретически максимальная скорость передачи данных (пропускная способность) канала SISO определяется теоремой Шеннона-Хартли [5, 9]:

$$\boldsymbol{C} = F\, log_2(1 + \frac{P_c}{N_0 F}), \qquad (2)$$

где $\boldsymbol{C}$ – пропускная способность канала, измеряемая в битах в секунду (бит/с) или, при нормализации по полосе пропускания, в бит/с/Гц; $F$ – полоса пропускания в герцах, диапазон частот, доступный для передачи сигнала (Гц); $P_c$ – средняя мощность сигнала.

Согласно теореме Шеннона-Хартли применительно для SISO-канала, существует принципиальное ограничение: рост пропускной способности при увеличении отношения $P_c / N_0 \gg 1$ подчиняется логарифмическому закону, что накладывает фундаментальные ограничения на эффективность системы. Например, при SNR 10 дБ нормированная пропускная способность $C / F$ составляет приблизительно 3,459 бит/с/Гц, тогда как при SNR 20 дБ (в 10 раз большая мощность) она увеличивается лишь до 6,658 бит/с/Гц. Такое физическое ограничение делает SISO непригодным для удовлетворения требований к высокой скорости передачи данных и большой пропускной способности, что напрямую стимулирует поиск альтернативных подходов к этой проблеме [10]. Практическим следствием этого является то, что достижение даже малого линейного увеличения пропускной способности требует экспоненциального увеличения SNR, а следовательно, и передаваемой мощности, что делает эффективное по мощности масштабирование скорости передачи данных чрезвычайно сложным и дорогостоящим. Указанная неэффективность увеличения пропускной способности напрямую приводит к ограничениям SISO в современных беспроводных сетях, интенсивно использующих данные и объясняет, почему был необходим новый технический подход, такой как MIMO. Еще одна из попыток увеличения характеристик – это переход к многомерным системам, таким, например, как OFDM.

*Типичные применения и ограничения*. Системы SISO идеально подходят для беспроводной связи в небольших помещениях, таких как дома или малые офисы, где развертывание нескольких антенн нецелесообразно. Они обеспечивают надежную связь в замкнутых пространствах и используются для улучшения покрытия Wi-Fi в жилых помещениях.

Однако основное ограничение SISO заключается в его ограниченной способности использовать пространственное разнесение для улучшения пропускной способности данных. Это означает, что системы SISO более подвержены замираниям и помехам, поскольку полагаются на один путь распространения сигнала. Архитектурная простота и экономичность SISO напрямую связаны с его ограничениями в производительности. Фактически это классический инженерный компромисс, при котором снижение сложности достигается за счет отсутствия использования расширенных возможностей, таких как пространственное разнесение. Подобное решение определяет нишу SISO среди всего многообразия технологий беспроводной связи.

*Промежуточные технологии: SIMO (Single Input Multiple Output) и MISO (Multiple Input Single Output)*. Между классической SISO и полномасштабной MIMO-архитектурой лежат две промежуточные технологии: SIMO и MISO. В рамках данных подходов для борьбы с глубокими замираниями многолучевого канала используется эффект пространственного разнесения. Однако на практике достичь полноценного выигрыша на передаче (MISO) позволяет лишь совместное использование пространственных ресурсов с методами временного или частотного разнесения (что реализуется применением ортогональных пространственно-временных STBC

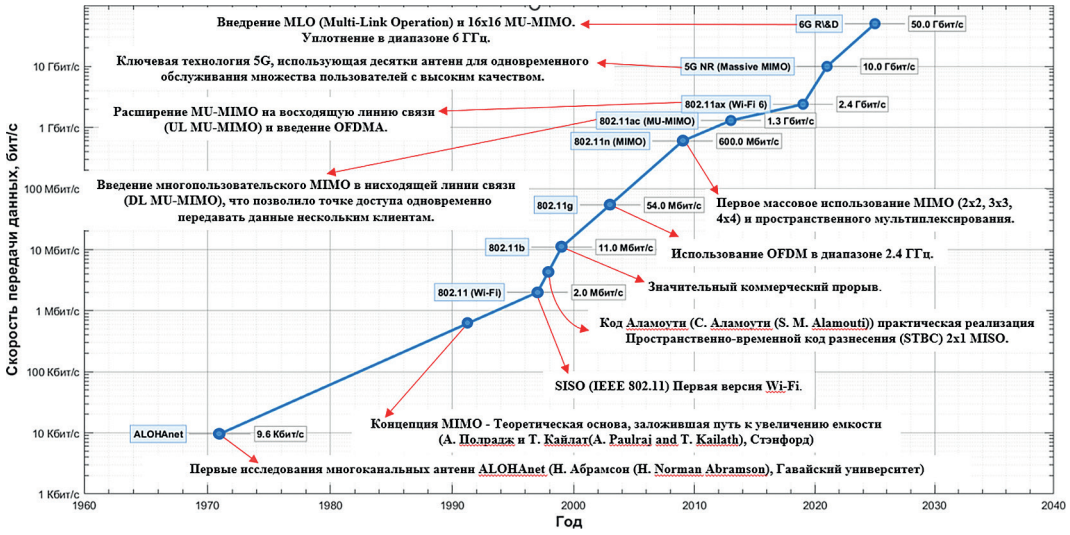



*Рис. 1. Ретроспективный анализ развития стандартов беспроводной связи: влияние внедрения технологий пространственного кодирования и систем MIMO на рост скорости передачи данных*

(Space-Time Block Coding, код Аламоути) [11] или пространственно-частотных блочных кодов. В системах SIMO передатчик использует одну антенну, а приемник – несколько антенн. Прием нескольких копий одного и того же сигнала, прошедших через разные пространственные пути, позволяет приемнику эффективно бороться с замираниями. Это достигается методами пространственного разнесения антенн: Выбор (Selection Combining) приемник постоянно анализирует качество сигнала на каждой из антенн и выбирает для обработки сигнал с наилучшим отношением сигнал/шум. Комбинирование (Combining): Сигналы со всех антенн комбинируются (к примеру, методом максимального отношения) для формирования результирующего сигнала с более высоким SNR. Каждый сигнал умножается на коплексный коэффициент, пропорциональный его амплитуде и синфазно выравнивается. Данная операция приводит к когерентному сложению полезных сигналов и некогерентному сложению шумов.

Системы MISO, напротив, имеют несколько антенн на передающей стороне и одну на приемной. Преимущество достигается за счет разнесения на передаче. Наиболее распространенным методом является пространственно-временное кодирование STC (Space-Time Coding) частный, но самый известный случай – код Аламоути, при котором одни и те же данные передаются с разных антенн, но в разные моменты времени и в определенной кодовой последовательности.

## 3. Основы технологии MIMO. Принципы работы и преимущества

Технология MIMO стала технологическим скачком благодаря тому, что использует несколько антенн на передающей и принимающей сторонах. Это дает двойной выигрыш: повышает скорость передачи (пропускную способность)

*Таблица 1.*

*Классификация технологий MIMO (SISO, SIMO, MISO, MIMO)*

| **Характеристика/ технология** | **SISO (Single-Input Single-Output)** | **SIMO (Single-Input Multiple-Output)** | **MISO (Multiple-Input Single-Output)** | **MIMO (Multiple-Input Multiple-Output)** |
|---|---|---|---|---|
| Количество антенн | 1 передающая антенна ($L_t$), 1 приемная антенна ($L_r$). | 1 передающая антенна ($L_t$), >1 приемных антенн ($L_r$). | >1 передающих антенн ($L_t$), 1 приемная антенна ($L_r$). | >1 передающих антенн ($L_t$), >1 приемных антенн ($L_r$). |
| Принцип работы | Стандартный радиоканал. Один поток данных. | Разнесенный прием (Receive Diversity). Повышение надежности за счет выбора лучшего сигнала из нескольких. | Разнесенная передача (Transmit Diversity). Повышение качества сигнала на приемнике. | Пространственное мультиплексирование или разнесение, формирование луча. |
| Достоинства | Простота и низкая стоимость. | Повышенная надежность и устойчивость к замираниям. | Улучшенное качество и мощность сигнала на приемной стороне. | Более высокая скорость передачи данных, высокая помехоустойчивость и увеличенная пропускная способность сети. |
| Недостатки | Низкая скорость и слабая надежность. Чувствительность к многолучевому распространению. | Не увеличивает максимальную пропускную способность. | Не увеличивает максимальную пропускную способность; сложнее, чем SIMO. | Высокая сложность обработки сигнала и стоимость. |
| Сложность реализации | Минимальная. | Низкая (на стороне приемника). | Средняя (на стороне передатчика). | Высокая (на обеих сторонах). |
| Область применения | Wi-Fi роутеры «старого парка» (802.11b/g), AM/FM радио. | Приемники в мобильных телефонах, базовые станции (на приём). | Средства обеспечения качества обслуживания (QoS) в 4G | Современные стандарты Wi-Fi (802.11n/ac/ax), мобильная связь 4G (LTE) и 5G, 6G |

и улучшает надежность связи [5]. Основной принцип работы MIMO заключается в одновременной передаче и приеме нескольких потоков данных в одном и том же частотном диапазоне за счет использования пространственного разнесения беспроводного канала.

Системы MIMO играют решающую роль в современных беспроводных сетях, обеспечивая более высокую скорость передачи данных, высокую помехоустойчивость и увеличенную пропускную способность сети [7, 12].

*Ключевые методы MIMO: пространственное разнесение, пространственное мультиплексирование, формирование луча*. Три основные методики, используемые в MIMO, часто применяются в совокупности для достижения максимальной пропускной способности и надежности [12].

*Пространственное разнесение (Spatial Diversity)*. Данный метод включает передачу одного и того же потока данных по нескольким независимым каналам, создаваемым пространственно разделенными антеннами (на расстоянии не менее половины длины волны). Он использует независимые замирания в нескольких антенных каналах для повышения помехоустойчивости сигнала [6, 12]. Основное преимущество пространственного разнесения заключается в компенсации эффектов замираний и помех, что приводит к повышению надежности и устойчивости сигнала. Различают разнесение на передаче (несколько передающих, одна принимающая антенна) и разнесение на приеме (одна передающая, несколько принимающих антенн).

*Пространственное мультиплексирование (Spatial Multiplexing)*. Такой подход предполагает одновременную передачу нескольких независимых потоков данных через несколько передающих антенн. Эти потоки разделяются на приемной стороне с помощью пространственной обработки. Главное преимущество пространственного мультиплексирования – значительное увеличение пропускной способности данных и повышение спектральной эффективности без необходимости использования дополнительной полосы пропускания. Однако при использовании указанного метода обычно теряется выигрыш от разнесения, что означает, что он может быть более подвержен замираниям, если не комбинируется с другими методами.

*Формирование луча (Beamforming) [6]*. Формирование луча в MIMO системах включает фокусировку сигнала в определенном направлении для достижения максимально возможного усиления на принимающей стороне. Данный метод требует знания состояния канала CSI (Channel State Information) на передатчике. Существуют три основные техники формирования луча: аналоговая (выполняется с помощью фазированных антенных решеток), цифровая (использует предварительное кодирование с модулированными потоками данных для создания диаграммы направленности) и комбинированная (сочетание аналоговой и цифровой). Преимущество формирования луча заключается в улучшении SNR и снижении помех для других пользователей. MIMO представляет собой не единое решение, а многогранную структуру, предлагающую различные преимущества: повышение помехоустойчивости через разнесение, увеличение пропускной способности через мультиплексирование и снижение влияние помех через формирование луча. Высокая адаптивность является ключевым фактором широкого распространения MIMO в различных беспроводных стандартах, таких как Wi-Fi, 4G (Fourth Generation) и 5G (Fourth Generation).

*Конфигурации и типы MIMO*. Конфигурации MIMO обычно обозначаются как $L_r \times L_t$, где $L_t$ – количество передающих антенн, а $L_r$ – количество принимающих антенн [8]. Распространенные конфигурации включают $2 \times 2$, $4 \times 4$ и $8 \times 8$. Выбор конфигурации зависит от конкретного применения и желаемой производительности, например, для конфигурации $2 \times 2$ с шириной канала 40 МГц скорость передачи составляет до 300 Мбит/с, тогда как при реализации конфигураций $4 \times 4$ или $8 \times 8$ с шириной канала 80 МГц скорости передачи могут достигать от 1,7 Гбит/с до 4,8 Гбит/с. Высшие порядки конфигураций MIMO (например, $64 \times 64$ для Massive MIMO в 5G) могут обеспечить более высокие скорости передачи данных и улучшенную спектральную эффективность, но они также увеличивают сложность систем.

Существует несколько типов MIMO:

*SU-MIMO (Single-User MIMO)*. Система «точка-точка», или однопользовательская канальная, используется для улучшения скорости передачи данных для одного пользователя. Широко применяется в сетях Wi-Fi (IEEE 802.11n, 802.11ac, 802.11ax) и 4G LTE (Long-Term Evolution) [10]. Ресурсы выделяются исключительно одному пользовательскому устройству.

*MU-MIMO (Multi-User MIMO)*. Система «точка-многоточка», сетевая. Используется для одновременного обслуживания нескольких пользователей, что увеличивает общую пропускную способность сети. Широко применяется в сетях 5G [11]. Выделяет нескольких пользователей одному ресурсу времени-частоты.

Влияние конфигураций MIMO на производительность системы можно суммировать в следующей таблице 2:

*Таблица 2.*

*Влияние конфигураций MIMO на производительность системы*

| Конфигурация MIMO | Скорость передачи данных | Спектральная эффективность | Сложность |
|---|---|---|---|
| 2 × 2 | Низкая-Умеренная | Низкая-Умеренная | Низкая |
| 4 × 4 | Умеренная-Высокая | Умеренная-Высокая | Умеренная |
| 8 × 8 | Высокая-Очень Высокая | Высокая-Очень Высокая | Высокая |

## 4. Математическая модель канала связи MIMO

В системах MIMO на передающей и приемной сторонах используются многоэлементные антенны или антенные решетки. Пусть рассматривается канал связи в многоантенной системе связи с $L_t$ передающими и $L_r$ приемными антеннами. Заметим, что пропускная способность в канале связи с замираниями и большим отношением сигнал/шум в $L_{\min}(L_t,L_r)$ раз больше пропускной способности канала без многоэлементных антенн. На передающей стороне формируется комплексный векторный сигнал $s$ размерности $L_t \times 1$, компонентами которого являются сигналы $s_m$, $m = 0,\ldots,L_t - 1$, передаваемые через $(m + 1)$-ю антенну. Матрица канала связи $\mathbf{H} = \mathbf{H}_c + i\mathbf{H}_s$, $i^2 = -1$ является комплексной прямоугольной матрицей размерности $L_r \times L_t$. Компонент матрицы канала $h_{km} = [\mathbf{H}]_{km}$ представляют собой комплексный коэффициент передачи канала связи от $m$-й передающей антенны к $k$-й приемной антенне и являются случайной величиной, имеющей нормальное распределение, $h_{km} \in \mathcal{CN}(a_{km},\sigma^2_{km})$, $k = 0,...,L_r-1, m = 0,...,L_t-1$, т. е. имеют различное математическое ожидание и дисперсию для всех возможных путей от $m$-й передающей к $k$-й приёмной антенне. В частности, при $|h_{km}| \in \mathcal{CN}(0,1)$ имеет рэлеевское распределение и $|h_{km}|^2$ – экспоненциальное (показательное) распределение с единичным математическим ожиданием, $\mathbb{E}[|h_{km}|^2] = 1$. Следовательно, $\mathbb{E}[\|\mathbf{H}\|^2_F] = L_tL_r$, где норма Фробениуса для матрицы $\mathbf{M} = [m_{ij}]^{r,t}_{i,j=1}$ размерностью $r \times t$ определяется как $\|\mathbf{M}\|^2_F = \sum_{i=1}^{r}\sum_{j=1}^{t}|m_{ij}|^2$. $\|\mathbf{M}\|^2_F = \mathrm{tr}(\mathbf{MM}^H) = \mathrm{tr}(\mathbf{M}^H\mathbf{M})$, где tr $\mathbf{X}$ – след матрицы $\mathbf{X}$. Будем полагать, что энергия сигнала в каждой приемной антенне равна суммарной энергии сигналов, излучаемых всеми $L_t$ передающими антеннами.

Математическая модель канала связи с аддитивным белым гауссовским шумом (AWGN, Additive White Gaussian Noise) имеет вид [9]:

$$\mathbf{y} = \mathbf{Hs} + \mathbf{n}, \quad (3)$$

где $\mathbf{y} \in \mathbb{C}^{L_r\times 1}$ – комплексный вектор принимаемого сигнала размером $L_r \times 1$; $\mathbf{H} \in \mathbb{C}^{L_r\times L_t}$ – матрица канала связи, компоненты которой, в общем случае, являются случайными процессами или случайными величинами; $\mathbf{s}$ – передаваемый сигнал, $\mathbf{s} \in \mathbb{C}^{L_t\times 1}$, где $E_s$ – средняя энергия сигнала, используемая одной передающей антенной; $\mathbf{n} \in \mathbb{C}^{L_r\times 1}$ – комплексный вектор аддитивного белого гауссовского шума размером $L_r \times 1$ с нулевым математическим ожиданием и ковариационной матрицей $\mathbf{R}_n = \mathbb{E}[\mathbf{nn}^H] = N_0\mathbf{E}_{L_r} = 2\sigma^2_n\mathbf{E}_{L_r}$, где $N_0$ – односторонняя спектральная плотность мощности шума и $\mathbf{E}_{L_r}$ – единичная матрица размером $L_r \times L_r$, т. е. $\mathbf{n} \in \mathcal{CN}(0,\sigma^2_n\mathbf{E}_{L_r})$. Таким образом, предполагается, что дисперсии шума во всех приемных антеннах являются одинаковыми. Данное ограничение не является существенным. Так, если дисперсии различны, то можно, например, рассматривать максимальную дисперсию. Нетрудно убедиться, что ковариационная матрица для сигнала определяется как $\mathbf{R}_{ss} = \mathbb{E}[\mathbf{ss}^H] = E_s\mathbf{E}_{L_t}$ и, соответственно, $\mathbb{E}[\mathbf{s}^H\mathbf{s}] = E_sL_t$. Таким образом, (3) определяет векторный гауссовский канал.

Заметим, что если $\mathbf{X} = [\mathbf{X}_1,\ldots,\mathbf{X}_n]$ случайная матрица размером $m \times n$, полученная из $n$ случайных независимых векторов размерами $m \times 1$ с ковариационной матрицей $\mathbf{R}$:$\mathbf{X} = [\mathbf{X}_1,\ldots,\mathbf{X}_n]$, где $\mathrm{cov}(\mathbf{X}_k) = \mathbf{R}$, $k = 1,\ldots,n$, то тогда ковариационная матрица имеет размерность $mn \times nm$ $\mathrm{cov}[\mathrm{vec}(\mathbf{X})] = \mathbf{E}_n \otimes \mathbf{R}$, где $\mathbf{A} \otimes \mathbf{B}$ – произведение Кронекера матриц $\mathbf{A}$ и $\mathbf{B}$. Если квадратная матрица $X$ размерностью $n \times n$ имеет ранг $r$, а случайная матрица $\mathbf{H}$ размерностью $p \times n$ элементы которой нормальные случайные величины с невырожденной ковариационной матрицей, то тогда с вероятностью 1 справедливо соотношение $\mathrm{rang}(\mathbf{HXH}^T) = \min(r,p)$ [5].

Разложение по сингулярным значениям SVD (Singular Value Decomposition) и собственные каналы. Матрица канала ($\mathbf{H}$) может быть разложена с использованием сингулярного разложения (SVD) [8]:

$$\mathbf{H} = \mathbf{U}\mathbf{\Sigma}V^{\mathbf{H}}, \quad (4)$$

где $\mathbf{H}$ – унитарные матрица $L_t \times L_r$, описывает взаимодействие между $L_t$ передающими и $L_r$-

приемными антеннами. Унитарная матрица удовлетворяет условию $\mathbf{U}^H\ \mathbf{U} = I$, где $\mathbf{U}^H$ – эрмитово-сопряженная матрица (транспонированная и комплексно-сопряженная). Данная матрица представляет вращение или отражение в пространстве принимающих антенн; $\mathbf{\Sigma}$ – диагональная матрица, сингулярных значений $L_t \times L_r$. На главной диагонали матрицы расположены сингулярные значения $\sigma_i$, которые являются неотрицательными действительными числами и обычно упорядочены по убыванию. Сингулярные значения представляют собой «усиления амплитуды» независимых параллельных каналов, которые могут быть сформированы с помощью SVD.

Вне главной диагонали все элементы равны нулю $\mathbf{\Sigma} = [\mathrm{diag}(\sigma_1,...,\sigma_{L_r})|0_{L_r,L_t-L_r}]$, $L_t \geq L_r$. Матрица $\mathbf{V}^H$ – эрмитово-сопряженная (транспонированная и комплексно-сопряженная) унитарная матрица размером $L_t \times L_r$. Определяет оптимальное преобразование сигнала на передающей стороне (предкодирование) для направления независимых потоков данных в ортогональные каналы.

Сингулярное разложение доказывает, что MIMO-канал эквивалентен набору $L_{\min}$ параллельных, независимых SISO-каналов, где $L_{\min} = \min(L_r,L_t)$, каждый из которых имеет коэффициент усиления, равный соответствующему сингулярному числу $\sigma_i$. По сути, SVD позволяет разделить MIMO канал на несколько ортогональных, независимых подканалов. Это ключевая концепция для достижения высоких скоростей передачи данных в MIMO системах, поскольку позволяет оптимально распределить мощность по подканалам (к примеру, с использованием «водоналивного» (water-filling algorithm) [5, 8] алгоритма и передавать по ним независимые потоки данных.

Пропускная способность канала MIMO. Пропускная способность MIMO-канала является суммой пропускных способностей независимых пространственных каналов, когда предполагается, что передатчик знает полную информацию о состоянии канала:

$$C = F\sum_i log_2(1 + \frac{P_i\lambda_i^2}{N_0}), \qquad (5)$$

где $C$ – общая пропускная способность MIMO канала в бит/с; $F$ – полоса частот; $r$ – ранг матрицы канала (число независимых пространственных каналов, $r \leq min(L_t,L_r)$. Это так же соответствует количеству ненулевых сингулярных значений (количество независимых параллельных подканалов), которые могут быть сформированы с помощью SVD; $P_i$ – мощность, распределенная по $i$-му пространственному каналу; $\lambda_i^2$ – $i$-е собственное число матрицы $\mathbf{HH}^H$ [6, 10].

В том случае, когда передатчик не обладает информацией о состоянии канала, пропускная способность рассчитывается следующим образом:

$$C = \mathbb{E}[F\ log_2(det(\mathbf{E}_{L_r} + \frac{SNR}{L_t}\mathbf{HH}^H)\ )\ ], \qquad (6)$$

где $\mathbb{E}[\cdot]$ – оператор математического ожидания; $SNR$ – отношение сигнал/шум; $L_t$ – количество передающих антенн; $L_r$ – количество приемных антенн; $H$ – матрица канала; $det\ \mathbf{A}$ – определитель матрицы $\mathbf{A}$; $\mathbf{E}_{L_r}$ – единичная матрица размера $L_r \times L_r$.

Важно отметить, что пропускная способность MIMO увеличивается линейно с количеством антенн, в отличие от систем SISO/SIMO/MISO, которые увеличиваются только логарифмически [10]. Вышеуказанное линейное масштабирование является основным преимуществом. Ранг матрицы $\mathbf{H}$ (количество ненулевых сингулярных значений $\sigma_i$ определяет количество пространственных степеней свободы, что указывает на то, сколько независимых потоков данных может быть поддержано [8]).

Фактическая пропускная способность и прирост производительности системы MIMO в значительной степени зависят от характеристик беспроводного канала, в частности от его ранга и сингулярных значений, выявляемых SVD. Это означает, что теоретические «линейные» приросты зависят от наличия среды с активным многолучевым распространением. Например, при прямой видимости LOS (Line Of Site,) канал MIMO обеспечивает прирост мощности, но не прирост степеней свободы, поскольку матрица канала имеет ранг, равный единице. Напротив, многолучевое замирание может быть полезным, если пути имеют значительное угловое разделение, что увеличивает ранг матрицы.

Точное моделирование и своевременная оценка параметров канала связи являются важными условиями для полной реализации потенциала MIMO систем, так как от этих факторов напрямую зависит пропускная способность и помехоустойчивость. Производительность MIMO не является универсальной, она неразрывно связана со средой распространения. Поэтому точная оценка канала и адаптивные стратегии передачи, такие как «водоналивной» алгоритм (water-filling algorithm), имеют решающее значение для оптимизации производительности MIMO в реальных сценариях.

Применение в современных беспроводных стандартах. Технология MIMO широко применяется в различных стандартах беспроводной

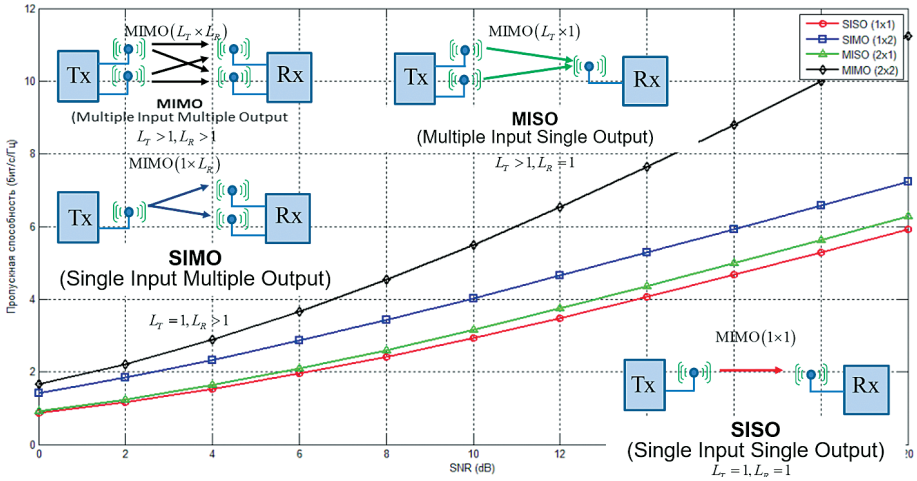



*Рис. 2. Сравнение пропускной способности технологии MIMO (SISO,SIMO,MISO,MIMO)*

связи: Wi-Fi: используется в стандартах IEEE 802.11n, 802.11ac и 802.11ax для повышения скорости передачи данных и пропускной способности сети. 4G (Long-Term Evolution): применяется в сетях LTE для увеличения скорости передачи данных и спектральной эффективности. Технология 5G (New Radio): является ключевой технологией в сетях беспроводной передачи данных, обеспечивая более высокие скорости передачи данных, меньшую задержку и увеличенную пропускную способность сети, включая Massive MIMO. Интеграция MIMO с ортогональным частотным мультиплексированием OFDM (Orthogonal Frequency-Division Multiplexing) приводит к значительному увеличению спектральной эффективности, поскольку выигрыш от пространственного мультиплексирования, предлагаемый MIMO, используется в сочетании с многоканальной модуляцией. Выигрыш от разнесения, достигаемый технологией MIMO, также может повысить стабильность соединения и обеспечить высокое качество обслуживания QoS (Quality Of Service).

## 5. Демодуляция методом обнуления для случайной матрицы канала связи

Известно несколько алгоритмов демодуляции на приемной стороне: Метод обнуления – ZF [15, 16]; Метод демодуляции по критерию минимума среднеквадратической ошибки – MMSE; Метод максимального правдоподобия – ML (Maximum Likelihood), используемый в многоантенных системах на основе архитектуры BLAST (Bell Laboratories Layered Space Time). Первые два неоптимальных метода относятся к линейным приемникам, которые включают в себя линейное преобразование полученного вектора и из-за их возможности снижения сложности часто применяют на практике. В этом случае принятый сигнал уфильтруется линейным фильтром с подавлением мешающих сигналов. Известно, что при $L_r \gg L_t \gg 1$ линейные приемники, используемые в massive MIMO, приближаются к оптимальным приемникам.

Из (3) следует, что ковариационная матрица принимаемого сигнала определяется как

$$\mathbf{R}_{yy} = \mathbb{E}[\mathbf{y}\mathbf{y}^H] = \mathbf{H}\mathbf{R}_{ss}\mathbf{H}^H + \mathbb{E}[\mathbf{n}\mathbf{n}^H] =$$

$$= \mathbf{H}\mathbf{R}_{ss}\mathbf{H}^H + N_0\mathbf{E}_{L_r},$$

где ковариационная матрица передаваемого сигнала $\mathbf{R}_{ss} = E_s\mathbf{E}_{L_t}$, с учетом предположения о равномерном распределении энергии на передающей стороне, т. е. в предположении, что сигналы, излучаемые передающими антеннами, имеют одинаковую энергию $E_s$. Таким образом, $\mathbf{R}_{yy} = \mathbf{H}\mathbf{R}_{ss}\mathbf{H}^H + N_0\mathbf{E}_{L_r}$, $\mathbf{R}_{ss} = E_s\mathbf{E}_{L_t}$, $\mathbf{R}_n = N_0\mathbf{E}_{L_r}$. В общем случае, при использовании линейного приемника используется некоторое линейное преобразование $\mathscr{L}(\mathbf{H})$ зависящее от матрицы канала связи $H$:$\hat{\mathbf{s}} = \mathscr{L}(\mathbf{H})\mathbf{H}\mathbf{s} + \mathscr{L}(\mathbf{H})\mathbf{n}$. В качестве соответствующего линейного преобразования выбирается матрица $A$, такая, что $AH$ представляет собой диагональную матрицу: $\hat{\mathbf{s}} = \mathbf{A}\mathbf{y} = \mathbf{A}(\mathbf{H}\mathbf{s} + \mathbf{n}) = \mathbf{A}\mathbf{H}\mathbf{s} + \mathbf{A}\mathbf{n}$. Суть метода обнуления заключается в умножении обратной матрицы $\mathbf{G}_{ZF}$ на вектор принятых отчетов [16]: $\hat{\mathbf{s}} = \mathbf{G}_{ZF}\mathbf{y} = \mathbf{G}_{ZF}(\mathbf{H}\mathbf{s} + \mathbf{n}) = \mathbf{s} + \mathbf{G}_{ZF}\mathbf{n}$, где $\mathbf{G}_{ZF} = \mathbf{H}^{\dagger} = (\mathbf{H}^H\mathbf{H})^{-1}\mathbf{H}^H$ – псевдообратная матрица канала. Ковариационная матрица шума, влияющего на принятие решения после произвольного линейного преобразования $\mathbf{G}$, имеет следующий вид: $\mathbf{R}_{\mathbf{G},n} = \mathbb{E}[(\mathbf{G}\mathbf{n})(\mathbf{G}\mathbf{n})^H] = \mathbf{G}\mathbf{R}_{\mathbf{n}}\mathbf{G}^H$. Следовательно,

отношение сигнал/шум на выходе $ZF$ приемника в $k$-й ветви определяется как

$$\gamma_{ZF,k} = \left[\frac{\mathbf{R}_{ss}}{\mathbf{R}_{ZF,n}}\right]_{kk} = \left[\frac{E_s \mathbf{E}_{L_t}}{\mathbf{G}_{ZF} N_0 \mathbf{E}_{L_r} \mathbf{G}_{ZF}^H}\right]_{kk} = \frac{\gamma}{[\mathbf{G}_{ZF}\mathbf{G}_{ZF}^H]_{kk}}.$$

Тогда, применяя свойства транспонирования Эрмита, получаем

$$\mathbf{G}_{ZF}\mathbf{G}_{ZF}^H = (\mathbf{H}^H\mathbf{H})^{-1}\mathbf{H}^H[(\mathbf{H}^H\mathbf{H})^{-1}\mathbf{H}^H]^H =$$
$$(\mathbf{H}^H\mathbf{H})^{-1}\mathbf{H}^H(\mathbf{H}^H\mathbf{H})^{-1}\mathbf{H} = (\mathbf{H}^H\mathbf{H})^{-1}.$$

Окончательно получаем, что

$$\gamma_{ZF,k} = \frac{\gamma}{[(\mathbf{H}^H\mathbf{H})^{-1}]_{kk}} = \frac{\gamma}{[\mathbf{W}^{-1}]_{kk}}, \qquad (7)$$

где $\mathbf{W} = \mathbf{H}^H\mathbf{H}$ и $\gamma = E_s / N_0$ – отношение сигнал/шум на приемной антенне.

Таким образом, для метода ZF оценочная версия передаваемого вектора символов получается после умножения в математической модели левой и правой части на псевдообратную матрицу $\mathbf{H}^\dagger$ в виде: $\hat{\mathbf{s}} = \mathbf{s} + \mathbf{H}^\dagger\mathbf{n}$, где используется псевдообратная функция Мура-Пенроуза $\mathbf{H}^\dagger$, которая равна $(\mathbf{H}^H\mathbf{H})^{-1}\mathbf{H}^H$, если столбцы матрицы $\mathbf{H}$ имеют полный ранг (столбцы линейно независимы) и тогда матрица $\mathbf{H}^H\mathbf{H}$ обратима или $\mathbf{H}^H(\mathbf{H}^H\mathbf{H})^{-1}$, если строки матрицы $H$ имеют полный ранг (строки линейнонезависимы) и тогда матрица $\mathbf{H}\mathbf{H}^H$ обратима.

Заметим, что

$$\mathbb{E}[[\mathbf{W}^{-1}]_{kk}] = (L_r - L_t)^{-1}); \ \mathbb{E}\left[\frac{\gamma}{[\mathbf{W}^{-1}]_{kk}}\right] = L_r - L_t + 1,$$
$$k = 1,\ldots,L_t.$$

Нетрудно убедиться, что

$$[\mathbf{W}^{-1}]_{km} = -1^{k+m}\det \mathbf{W}_{mk} / \det\mathbf{W},$$

где $\mathbf{W}_{mk}$ определяет минор элемента $[\mathbf{W}]_{km}$. Следовательно,

$$\gamma_k = \frac{\gamma}{[\mathbf{W}^{-1}]_{kk}} = \frac{\det \mathbf{W}}{\det \mathbf{W}_{kk}}\gamma = \mathbf{W}_{kk}^{sc}\gamma, \ k = 1,\ldots,L_t. \qquad (8)$$

Если $\mathbf{W}$ имеет распределение Уишарта, то функция плотности распределения вероятности и, соответственно, функция распределения для $\gamma_k$, строгим математическим аппаратом, полученным авторами ранее в [17]:

$$f(\gamma_k) = \frac{1}{\Gamma(L_r - L_t + 1)\,\gamma_{0,k}}\left(\frac{\gamma_k}{\gamma_{0,k}}\right)^{L_r - L_t} e^{-\gamma_k / \gamma_{0,k}}, \ k = 1,\ldots,L_t;$$

$$F(\gamma_k) = \frac{1}{\Gamma(L_r - L_t + 1)\gamma_{0,k}}\,\gamma\left(L_r - L_t + 1, \frac{\gamma_k}{\gamma_{0,k}}\right), \ k = 1,\ldots,L_t,$$

где $\gamma_{0,k} = \frac{\gamma}{[\mathbf{R}^{-1}]_{kk}}$, $k = 1,\ldots,L_t$ и $\Gamma(z)$ – гамма-функция, $\gamma(a,z)$ – неполная гамма-функция.

## 6. Военное применение технологии MIMO

В условиях перехода к концепции сетецентрических войн ключевым требованием к системе связи становится обеспечение высокоскоростной передачи мультисервисного траффика (видеоинформация с БПЛА, данные радиолокационной разведки) при сохранении высокой живучести радиолиний. Применение технологии MIMO в военной сфере имеет ряд принципиальных отличий от гражданских сетей (5G/Wi-Fi).

Во-первых, приоритетным свойством систем MIMO специального назначения является не только увеличение пропускной способности (спектральной эффективности), но и повышение помехозащищенности. Многоэлементные антенные системы позволяют реализовать пространственную селекцию сигналов. Алгоритмы пространственной обработки, такие как исследуемый в данной работе метод обнуления ZF, способны формировать «нули» диаграммы направленности в угловых направлениях на источники преднамеренных помех (средства РЭБ противника), обеспечивая функционирование канала связи при отрицательных значениях отношения сигнал/шум.

Во-вторых, эксплуатация средств связи происходит на подвижных объектах вооружения и военной техники (ББМ, танки, КШМ). Габаритные ограничения носителей вынуждают размещать элементы антенной решетки на малом расстоянии друг от друга (менее половины длины волны). Это приводит к возникновению пространственной корреляции каналов, статистические свойства которых описываются распределением Уишарта. Классические алгоритмы приема в таких условиях теряют эффективность, что требует разработки адаптированных методик оценки помехоустойчивости.

В-третьих, технология MIMO критически важна для работы в условиях плотной городской застройки и пересеченной местности (режим NLOS - отсутствие прямой видимости). За счет использования многолучевого распространения радиоволн, которое для традиционных систем связи является деструктивным фактором, системы MIMO обеспечивают устойчивое покрытие и скрытность работы, так как позволяют снизить общую излучаемую мощность при сохранении качества приема за счет выигрыша от разнесения.

Таким образом, внедрение адаптивных алгоритмов MIMO в аппаратуру связи тактического звена является необходимым условием обеспечения информационного превосходства и устойчивости управления войсками в сложной радиоэлектронной обстановке.

*Таблица 3.*

*Изделия БШПД применяющиеся в войсках*

| Наименование оборудования | «Дина» | InfiLINK 2×2 R5000-Mmx | Радиомост Ubiguiti LiteBeam 5AC-Gen2 | Радиомост Ubiguiti LiteBeam M5-23 |
|---|---|---|---|---|
| Внешний вид |  |   |   |  |
| Организация связи | На стоянке «точка-точка», «точка-многоточка» | На стоянке «точка-многоточка», «точка-точка» | На стоянке «точка-точка», «точка-многоточка» | На стоянке «точка-точка», «точка-многоточка» |
| Диапазон частот, МГц | 4900–6000 6050–6400 | 4900–6050 | 5170–5875 | 5170–5875 |
| Мощность ПРД, Вт | 0,2 | 0,5 | 0,3 | 0,3 |
| Усиление антенн, дБ | 23–28 | 28 | 23 | 23 |
| Пропускная способность, Мбит/с | 220–300 | 280 | 450 | 450 |
| Дальность связи, км | 80** | 40** | 10** | 5** |
| Электропитание, В | 220 | 110–240 | 24 | 24 |
| Группа исполнения | 1.10 | класс защиты IP67 (влага, пыль) | IEC-68 (темпер., вибрация) | IEC-68 (темпер., вибрация) |
| Применение | Сам-ное изделие | Сам-ное изделие | Сам-ное изделие | Сам-ное изделие |
| Ор. стоимость | 1,2 млн. р. | 300 т.р | 10–12 т.р. | 7–9 т.р. |
| Производственная мощности | 1000 в год | Нет данных | Нет данных | Нет данных |
| Производитель | АО «Военителеком» | ООО «Инфинет» | Китай | Китай |

## 7. Моделирование каналов в MATLAB

Моделирование в MATLAB представляет собой важный инструмент для подтверждения теоретических моделей и анализа практических компромиссов в производительности систем беспроводной связи. Значительное преимущество моделирования заключается в возможности быстрой оценки производительности и анализа гипотетических сценариев до этапа аппаратной реализации. Таким образом, суть компьютерного моделирования заключается в преобразовании абстрактных математических принципов в чёткие, измеримые результаты. Это укрепляет понимание систем и обеспечивает основу для принятия практических инженерных решений.

Для верификации полученных аналитических выражений и исследования поведения системы в условиях реальной сигнально-помеховой обстановки была разработана имитационная модель канала MIMO в среде MATLAB. Анализ помехоустойчивости линейного демодулятора обнуления ZF проводился в условиях плоских рэлеевских замираний с аддитивным белым гауссовым шумом (АБГШ). Главной задачей моделирования являлось подтверждение способности предложенной математической методики безошибочно прогнозировать вероятность битовой ошибки системы без проведения длительных ресурсоемких стохастических симуляций во всем рабочем диапазоне отношения сигнал/шум.

Традиционные методы оценки помехоустойчивости детектора ZF часто базируются на грубых асимптотических приближениях (например, границах Чернова) и имеют погрешности

в области низких и средних значений $E_s / N_0$. В отличие от них, в предложенном подходе используется точный математический расчет, опирающийся на статистические свойства инвертированной матрицы канала.

Известно, что вероятность ошибки $P_b$ на приемной стороне при когерентном приеме многопозиционных сигналов может быть выражена как алгебраическая сумма интегральных $T$-функций Оуэна [1]. Поскольку в методе обнуления отношение сигнал/шум на символ после обработки имеет $\chi^2$-распределение, определяемое степенью свободы обратной матрицы Уишарта, математическое ожидание (эргодическая вероятность) сводится к вычислению специальных полиномов. Данный математический аппарат позволяет получить строгие количественные оценки BER без использования ресурсоемкого численного интегрирования.

Исходное уравнение для вероятности ошибки выражается суммой $T$-функций Оуэна [1]:

$$P_{e/b}(\gamma_{bc}) = \sum_k a_k T(\sqrt{2g_k\gamma_{bc}}, \eta_k), \qquad (9)$$

где $\gamma_{bc}$ – отношение средних энергий на один бит к спектральной плотности шума; $T(z,a)$ – интегральная функция Оуэна строго определяемая математическим выражением вида:

$$T(z,a) = \frac{1}{2\pi}\int_0^a \frac{e^{-(1+t^2)z^2/2}}{1+t^2}dt, \ |\arg a| < \pi,$$

а коэффициенты $g_k$, $\eta_k$ зависят от параметров применяемой многомерной сигнальной конструкции. Для канала с рэлеевскими замираниями математическое ожидание функции Оуэна сводится к $\mathcal{H}$-функции [1]:

$$\mathbb{E}T\left[\left(\sqrt{2g\gamma_k},\eta\right)\right] = \mathcal{H}_{L_r-L_t+1}\left(0;\sqrt{\frac{g\gamma_{0,k}}{g\gamma_{0,k}+1}},\eta\right), \qquad (10)$$

где $\mathcal{H}_\nu(z;a,b)$ – специальная интегральная функция, при ($\nu \geq 0$, $0 \leq a^2 \leq 1$) задается следующим образом:

$$\mathcal{H}_\nu(z;a,b) = \frac{(1-a^2)^\nu}{2\pi}\int_0^b \frac{1}{(1+x^2)(1+a^2x^2)^\nu} \exp\left(\frac{z^2}{2}\frac{1+x^2}{1+a^2x^2}\right)dx.$$

В частном случае, когда определяется математическое ожидание от функции Гаусса, т.к. $T(z,\infty) = \frac{1}{2}Q(z)$, то:

$$\mathcal{H}_n(0,b,\infty) = \frac{1}{2}\left(\frac{1-b}{2}\right)^n \sum_{k=0}^{n-1}\binom{n+k-1}{k}\left(\frac{1+b}{2}\right)^k. \qquad (11)$$

В данном выражении параметр $b = \sqrt{\gamma/(1+\gamma)}$ обусловлен эквивалентным отношением сигнал/шум, $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ биномиальный коэффициент, а $L_{\text{div}} = L_r - L_t + 1$ строго определяет порядок пространственного разнесения, обеспечиваемый избыточностью приемных антенн. Именно эта формула легла в основу аналитического расчета для сравнительного графического анализа.

Полученные графические зависимости раскрывают специфику работы метода обнуления в многоантенных системах и полностью доказывают корректность заявленной методики. В первую очередь стоит отметить полное визуальное наложение экспериментальных данных Монте-Карло (точечные маркеры), усредненных по репрезентативной выборке независимых матриц рэлеевского канала, на аналитические кривые (сплошные линии), полученные через вычисление функции $\mathcal{H}_n$. Такое совпадение,

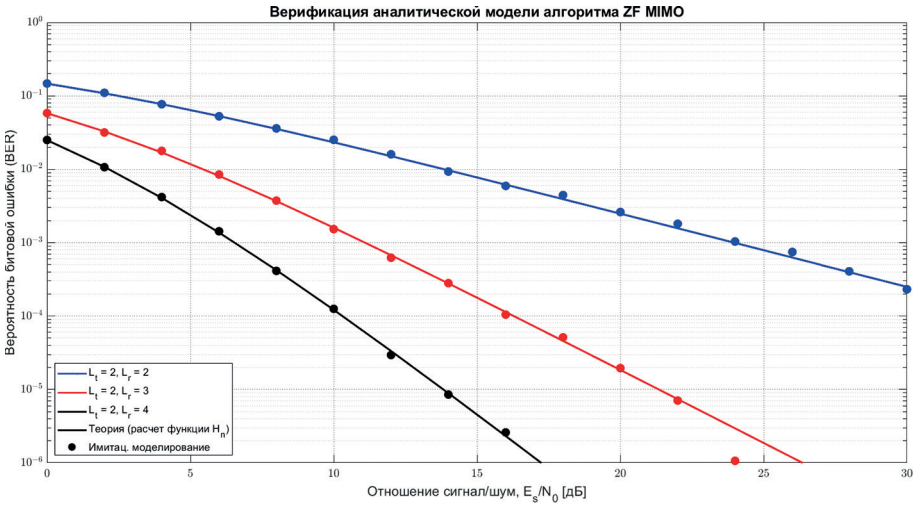



*Рис. 3. Верификация аналитической модели алгоритма ZF MIMO при приеме сигналов с двоичной фазовой манипуляцией (BPSK): сопоставление теоретических расчетов при использовании $H_p(z;a,b)$ функции (сплошные линии) с результатами имитационного Монте-Карло моделирования (маркеры)*

наблюдаемое во всем исследуемом диапазоне $E_s / N_0$ , включая область глубоких замираний (при BER > $10^{-4}$), наглядно верифицирует математическую точность применения аппарата специальных функций. Расчет через указанную конечную сумму дает возможность избегать аппроксимаций для вероятности ошибки.

Кроме того, рисунок прямо подтверждает зависимость устойчивости детектора обнуления от конфигурации приемных антенн (условия эффективности). В базовой конфигурации без избыточного приема ($L_t$ = 2, $L_r$ = 2) параметр пространственного разнесения минимален $L_{\text{div}}$ = 1. Из-за высокой чувствительности инвертированной квадратной матрицы к глубоким замираниям (и возникающему эффекту усиления шума), кривая ошибки снижается линейно, требуя завышенных энергетических затрат. Однако интеграция конфигураций с избыточным приемом $L_r > L_t$ коренным образом меняет динамику системы. Увеличение числа приемных элементов (кривая $L_r$ = 3, разнесение $L_{\text{div}}$ = 2, и $L_r$ = 4, разнесение $L_{\text{div}}$ = 3) позволяет кратно улучшить наклон «водопадных» характеристик. За счет достигнутого порядка разнесения метод обнуления становится оптимальным выбором для высокоскоростной передачи: он позволяет линейно снизить вероятность ошибки без усложнения аппаратной реализации детектора.

Одним из наиболее серьезных фундаментальных ограничений использования линейного метода обнуления в конфигурациях MIMO является физическая уязвимость матричного инвертирования в случае корреляции потоков или пространственных замираний канала (при отсутствии избыточного приема). В условиях сложной помехи квадратная матрица канала часто бывает плохо обусловлена (вырождена). Прямое обращение вырожденных матриц провоцирует математический эффект сингулярности, результатом которого на практике становится критическое многократное увеличение (amplification) мощности дисперсии аддитивного шума, полностью искажающего декодируемый сигнал на выходе приемника. Для устранения данного недостатка и выравнивания помехоустойчивости применяют модификацию детектора обнуления на основе критерия минимума среднеквадратической ошибки (MMSE, Minimum Mean Square Error). Анализируя теоретическую природу усиления шума, необходимо рассмотреть весовые матрицы фильтров демодуляции: Линейное преобразование детектора ZF для вектора оценок сигналов определяется весовой матрицей: $\mathbf{G}_{ZF} = (\mathbf{H}^H\mathbf{H})^{-1}\mathbf{H}^H$. Очевидно, что в вырожденных ситуациях $\det(\mathbf{H}^H\mathbf{H}) \approx 0$ собственные значения инверсной ковариационной матрицы экспоненциально возрастают, усиливая тем самым тепловой аддитивный шум системы $n$ при перемножении: $\hat{\mathbf{s}}_{ZF} = \mathbf{s} + \mathbf{G}_{ZF}\mathbf{n}$. Во избежание данного деструктивного эффекта детектор MMSE включает в матрицу расчета диагональную нагрузку (регуляризатор):

$$\mathbf{G}_{MMSE} = (\mathbf{H}^H\mathbf{H} + (N_0 / E_s)\mathbf{E})^{-1}\mathbf{H}^H, \qquad (12)$$

где $\mathbf{E}$ – единичная матрица соответствующего размера. Введенное слагаемое $N_0 / E_s$, эквивалентное значению обратного отношения сигнал/шум (уравнение получено с учетом равенства $(\mathbf{AB})^{-1} = \mathbf{B}^{-1}\mathbf{A}^{-1}$, сдвигает спектр собственных значений и гарантирует жесткое ограничение роста коэффициентов матрицы $\mathbf{G}_{MMSE}$. С точки зрения энергетических процессов, фильтр MMSE представляет собой компромисс между

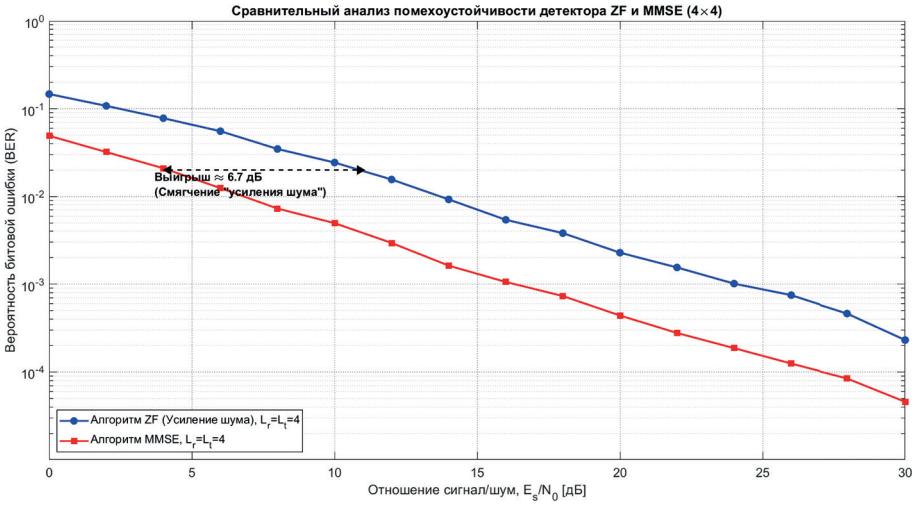



*Рис. 4. Сравнительный анализ помехоустойчивости линейных детекторов ZF и MMSE в условиях симметричного канала связи без избыточного пространственного приема (система 4×4, модуляция BPSK). Эффект компенсации усиления шума*

полным подавлением многоантенной интерференции потоков и ограничением уровня аддитивного шума, тем самым решая главную проблему ZF. В области предельно высоких отношений сигнал/шум $N_0 / E_s \to 0$ оба алгоритма совпадают и метод MMSE переходит в стандартное уравнение ZF, что и наблюдается асимптотически:

$$\mathbf{G}_{MMSE} \mid N_0 \to 0 = (\mathbf{H}^H\mathbf{H})^{-1}\mathbf{H}^H = \mathbf{G}_{ZF}.$$

Проведенное на рисунке 4 сравнительное имитационное моделирование наглядно раскрывает практический вес математической стабилизации детектора MMSE. Экспериментальные зависимости подтвердили доминирующую роль проблемы «усиления шума» в методе ZF в сложных симметричных каналах ($L_t = L_r = 4$). Видно, что при малых отношениях сигнал/шум (зона до 15 дБ), попытка ZF осуществить идеальное обнуление межканальной интерференции любой ценой приводит к недопустимой мощности теплового шума на выходе – алгоритм крайне медленно уходит из области глубоких ошибок (ниже $P_b = 10^{-2}$). При тех же самых параметрах канальной матрицы $\mathbf{H}$ фильтрация по алгоритму MMSE, учитывающая отношение $N_0 / E_s$, формирует оптимальные весовые векторы-строки, защищая детектор. Это визуализируется устойчивым энергетическим выигрышем. Из графика на рисунке 4 установлено, что для достижения пороговой достоверности качества связи $P_b = 10^{-2}$ в многолучевом канале детектору ZF требуется мощность более $X_{ZF}$ дБ, тогда как для приемника MMSE достаточно мощности $X_{MMSE}$ дБ. Зафиксирован энергетический выигрыш от 3 до 5 дБ по спектру низких отношений сигнал/шум (точная дельта зависит от флуктуации канала и видна по курсорам на рисунке 4). Тем не менее, как и предсказывалось формулами, в асимптотическом случае, когда мощности передатчика достаточно (при $E_s / N_0 > 20$ дБ), коэффициент смещения дисперсии теряет свое влияние: обе кривые уверенно смыкаются и продолжают линейный параллельный ход вниз, формируя идентичный наклон характеристик порядка $d$.

Полученный количественный результат достоверно подтверждает выводы исследования: хотя математический алгоритм ZF проще в технической реализации (отсутствует необходимость точной аппаратной оценки текущей дисперсии теплового шума), его применение для слабо обусловленных симметричных решеток вызывает высокие потери энергетического бюджета, поэтому в реальных стандартах передачи его чаще развертывают совместно с алгоритмом избыточного приема конфигурации $L_r \gg L_t$.

Минимизация частоты ошибок, достижимая линейными фильтрами детектирования, неразрывно связана с максимальной скоростью надежной передачи данных в рассматриваемых средах связи. Для подтверждения целесообразности и оптимальности выбора приемника ZF для высокоскоростных магистралей, необходимо исследовать его предельную спектральную эффективность (эргодическую пропускную способность, С, [бит/с/Гц]) в функции отношения сигнал/шум. Поскольку обнуляющий детектор изолирует пространственные подканалы за счет формирования эквивалентных неинтерферирующих параллельных потоков, информационная емкость напрямую зависит от статистической изменчивости (замираний) каждого выделенного виртуального субканала.

Аналитический базис формирования пропускной способности при использовании приемника ZF опирается на выведенное математическое ожидание диагональных элементов обращенной матрицы ковариаций $\mathbf{W} = \mathbf{H}^H\mathbf{H}$. Мгновенное значение отношения сигнал/шум в $k$-ом параллельном потоке задается полученными ранее выражениями (7) и (8). С позиций статистической радиотехники строго доказано, что знаменатель этой функции (минор обратной вырожденной матрицы **W**) имеет маргинальное хи-квадрат распределение со степенью свободы $2(L_r - L_t + 1)$, что напрямую контролирует параметр дисперсии помехоустойчивости $\sigma_k^2$. Из теории информации эргодическая пропускная способность канала Шеннона с эквализацией по методу ZF вычисляется как математическое ожидание логарифмической емкости:

$$\mathbb{E}[C_{ZF}] = \mathbb{E}_{\mathbf{H}}\left[\sum_{k=1}^{L_t} \log_2(1 + \lambda_k)\right]. \qquad (13)$$

Таким образом, степень избыточного приема $L_r > L_t$ выступает ключевым инструментом: увеличивая степени свободы функции распределения замираний Уишарта, мы предотвращаем глубокие флуктуации переменной $[\mathbf{W}^{-1}]_{kk}$, кардинально приближая среднюю пропускную способность субканалов алгоритма обнуления к ее теоретическому асимптотическому пределу гауссовского канала связи.

Представленные на рисунке 5 результаты безоговорочно иллюстрируют математическую оптимальность метода обнуления для конфигураций массивного радиодоступа при условии средних и высоких значений ОСШ. Главный доказываемый критерий эффективности раскрыт через сопоставление кривых спектральной эффективности. Конфигурации 2 × 2 (синяя сплошная линия) и 4 × 4 (красная сплошная линия), не обладающие избыточностью приема $L_r = L_t$, теряют существенный резерв энергетической емкости. Для обеспечения пропускной способности $C$ = 10 бит/с/Гц в системе 2 × 2 требуется более 15 дБ соотношения сигнал/шум. Однако

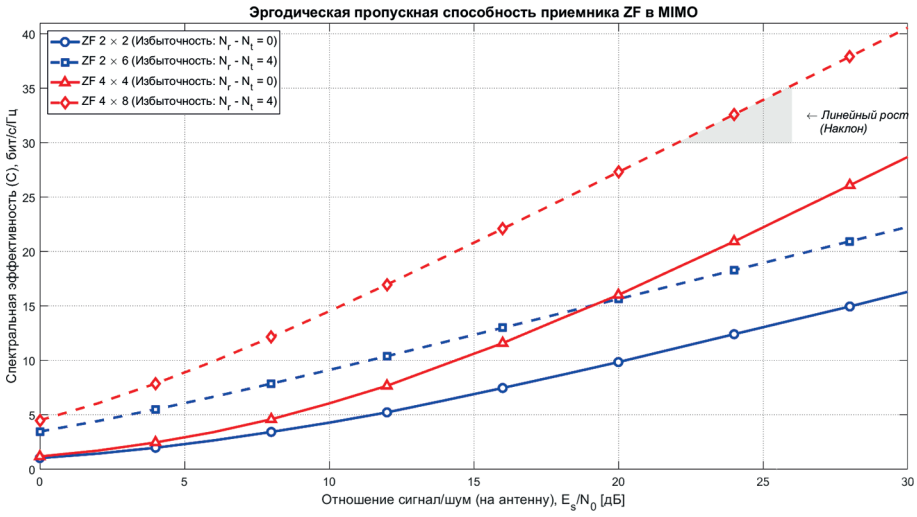



*Рис. 5. Динамика эргодической пропускной способности и влияние пространственного избыточного приема при линейном мультиплексировании ZF в рэлеевском канале*

стоит применить конфигурацию с антенным избыточным приемом (пунктирные кривые 2 × 6 и 4 × 8), где количество $L_r > L_t$, как ситуация коренным образом преображается. Полученный порядок разнесения полностью нивелирует провалы канала (замирания), обеспечивая строгий энергетический выигрыш ≈5…7 дБ по спектральной шкале влево, и устраняя потери «усиления шума». Более того, график надежно фиксирует второй аспект теоретических положений – при переходе рубежа SNR ≥ 15 дБ характеристика $C(E_s / N_0)$ приобретает форму чистых прямых линейно-восходящих зависимостей независимо от параметров замирания. Система начинает прирастать с постоянной скоростью $L_t \log_2 (1 + SNR)$, а значит пропускная способность при применении базового низкобюджетного алгебраического инвертирования ZF масштабируется строго линейно. Следовательно, изложенная методология доказывает целесообразность использования алгоритмов обнуления с избыточным приемным вектором ($L_r \geq 2L_t$), поскольку они обеспечивают пропускную способность, эквивалентную дорогим стохастическим и ML-фильтрам при радикально меньшей аппаратной вычислительной сложности для модемного чипа.

## 8. Заключение

Ключевые выводы и сравнительный анализ. В ходе данного исследования был проведен углубленный анализ эффективности пространственной фильтрации сигналов в системах MIMO с использованием метода обнуления ZF. Вместо общего сравнения технологий, работа сосредоточена на оценке характеристик конкретного линейного алгоритма детектирования, что позволило получить следующие значимые результаты:

*$L_r$ Будущие направления развития*. Развитие MIMO продолжается, и будущие направления исследований включают дальнейшее масштабирование числа антенн в концепциях, таких как Massive MIMO, уже интегрированной в 5G, и Cell-Free Massive MIMO [18], которая обещает еще более равномерное покрытие и пропускную способность за счет распределения большого количества антенн по всей территории обслуживания.

Интеграция искусственного интеллекта и машинного обучения AI (Artificial Intelligence), ML (Machine Learning) играет все более важную роль в оптимизации систем MIMO. Данные технологии могут быть использованы для более точной оценки канала, адаптивного формирования луча, интеллектуального распределения ресурсов и даже для оценки пропускной способности канала, что позволяет системам динамически адаптироваться к изменяющимся условиям среды и потребностям пользователей.

Кроме того, исследования в области миллиметрового (mmWave) и терагерцового (THz) диапазонов частот, где доступна огромная полоса пропускания, тесно связаны с развитием MIMO. В этих диапазонах MIMO, особенно методы формирования луча, имеют решающее значение для преодоления высоких потерь на трассе распространения сигнала. В целом, MIMO остается фундаментальной технологией, которая будет продолжать формировать будущие поколения беспроводной связи, обеспечивая постоянно растущие требования к скорости, надежности и пропускной способности.

## Литература

1. Савищенко Н. В. Специальные интегральные функции, применяемые в теории связи: Монография. – СПб.: ВАС, 2012. 560 с.
2. Foschini G. J., Gans M. J. On limits of wireless communications in a fading environment when using multiple antennas // Wireless Personal Communications, 1998, Vol. 6, no. 3. pp. 311–335.
3. Biglieri E., Calderbank R., Constantinides A., Goldsmith A., Paulraj A., Poor H. V. MIMO Wireless Communications. – Cambridge University Press, 2007. 334 p.
4. Larsson E. G., Edfors O., Tufvesson F., Marzetta T. L. Massive MIMO for next generation wireless systems // IEEE Communications Magazine, 2014, Vol. 52, no. 2. pp. 186–195.
5. Голдсмит А. (2005). Беспроводные телекоммуникации. Перевод Бирюкова Н. Л., Триски Н. Р. – Москва: Техносфера, 2011. 992 с.
6. Tse, D., Viswanath, P. Fundamentals of Wireless Communication. Cambridge University Press, 2005. 378 p.
7. Слюсарь В. И. Системы MIMO: принципы построения и обработка сигналов. // Электроника: Наука, Технология, Бизнес, 2005. № 8. С. 58–65.
8. Paulraj A., Nabar R., Gore D. Introduction to Space-Time Wireless Communications. Cambridge University Press, 2008, pp. 34–38.
9. Бураченко Д. Л., Савищенко Н. В. Геометрические модели сигнально-кодовых конструкций: Учеб. пособие. Изд. 2-е. – СПб.: ВАС, 2020. 390 с.
10. Бакулин М. Г., Варукина Л. А., Крейнделин В. Б. Технология MIMO: принципы и алгоритмы. – М.: Горячая линия – Телеком, 2014. 248 с.
11. Jankiraman M. Space-time codes and MIMO systems. USA, MA: Artech House, 2004. 327 p.
12. Tsoulos G. V. MIMO System Technology for Wireless Communications. CRC Press, 2006, pp. 66–69.
13. Петров В. П., Якушев И. Ю. Современные технологии в системе MIMO // Вестник СибГУТИ. 2019. № 2. С. 14–25.
14. Chen X., Soh P. J., Sharawi M. S. MIMO Antenna Systems for 5G and Beyond. Wiley-IEEE Press, 2024, pp. 15–18, 43–45.
15. Gershman A. B., Sidiropoulos N. D. Space-time processing for MIMO communications. John Wiley Sons, Ltd, 2005. 369 p.
16. Gore D., Heath R. W., Paulraj A. On performance of the zero forcing receiver in presence of transmit correlation. Proc. IEEE Int. Symp. Inf. Theory, Lausanne, Switzerland, 2002, pp. 159–165.
17. Савищенко Н. В., Пелин А. А. Распределение Уишарта для анализа помехоустойчивости приема многоантенных систем беспроводной связи // Актуальные проблемы прикладной математики, информатики и механики: материалы Междунар. научной конференции, Воронеж, 12–15 ноября 2025 г. – Воронеж: Издательский дом ВГУ, 2025. – С. 832–838.
18. Montiouis W., Imoize A. L. Massive MIMO for future wireless communication systems: technology and applications. Wiley, 2025, pp. 61–63.


# PERFORMANCE ANALYSIS OF MIMO SYSTEMS USING THE ZERO-FORCING METHOD

***Savischenko N. V.[3], Pelin A. A.[4]***

***Keywords:*** *wireless communication systems, information theory, digital signal processing, fading channels, multi-antenna systems, precoding, zero-forcing method, special integral functions.*

***Abstract***

***Objective:*** *the objective of this paper is to analyze the efficiency of the zero-forcing (ZF) method for signal reception in MIMO (Multiple Input Multiple Output) systems and to obtain exact analytical expressions for the error probability using the theory of potential noise immunity and the theory of special functions.*

***Methods:*** *the study utilizes a comprehensive approach combining rigorous analytical calculations and simulation modeling in the MATLAB environment to evaluate the performance of spatial signal filtering using the zero-forcing method in MIMO systems.*

*1. The calculation of the bit error rate (BER) for the ZF detector is performed based on the analysis of the statistical properties of the inverse channel correlation matrix. The derivation of expressions for noise immunity is carried out using the mathematical apparatus of special integral functions (Gaussian function, Owen's T-function) in accordance with the methodology presented in the monograph «Special integral functions applied in communication theory» [1]. This methodology allows obtaining rigorous theoretical performance bounds.*

3 Nikolay V. Savischenko, Dr.Sc. of Technical Sciences, Professor, Professor of the Department of General Professional Disciplines of the Military Academy of Communications named after S. M. Budenny, St. Petersburg, Russia. E-mail: snikaspb@mail.ru

4 Artem A. Pelin, Adjunct of the Department of General Professional Disciplines, S. M. Budyonny Military Academy of Communications, St. Petersburg, Russia. E-mail: PelinVUC@yandex.ru

*2. Simulation modeling: to verify the obtained analytical expressions and study the system's behavior under real signal-to-noise and interference conditions, a simulation model of a MIMO channel with Rayleigh fading was developed in the MATLAB environment.*

***Results:*** *the analytical and experimental data obtained reveal the specifics of the zero-forcing method operation in MIMO systems. In particular, it is established that the ZF method allows completely eliminating intersymbol (inter-channel) interference via channel matrix inversion. However, modeling revealed a key drawback of the method – the noise enhancement effect, which manifests itself under ill-conditioned channel matrices. A comparative analysis showed that in the low signal-to-noise ratio region, the ZF method is inferior to the MMSE (Minimum Mean Square Error) algorithm in terms of power efficiency but demonstrates high efficiency and a linear growth of capacity at high SNR values. A close agreement between the calculation results based on the proposed analytical methodology (via special functions) and the Monte Carlo simulation results is confirmed.*

***Scientific novelty:*** *the scientific novelty of the paper lies in the adaptation of the mathematical apparatus of special integral functions for the exact calculation of noise immunity using the zero-forcing method, taking statistical characteristics into account. In contrast to traditional estimates based on asymptotic approximations, the proposed approach allows for obtaining rigorous quantitative estimates of the error probability for M-ary signal reception by a linear detector under Rayleigh fading conditions, which significantly increases the reliability of communication quality prediction during the design of antenna systems.*

## References


1. Savischenko N. V. Special'ny'e integral'ny'e funkcii, primenyaemy'e v teorii svyazi: Monografiya. – SPb.: VAS, 2012. 560 s.
2. Foschini G. J., Gans M. J. On limits of wireless communications in a fading environment when using multiple antennas // Wireless Personal Communications, 1998, Vol. 6, no. 3. pp. 311–335.
3. Biglieri E., Calderbank R., Constantinides A., Goldsmith A., Paulraj A., Poor H. V. MIMO Wireless Communications. – Cambridge University Press, 2007. 334 p.
4. Larsson E. G., Edfors O., Tufvesson F., Marzetta T. L. Massive MIMO for next generation wireless systems // IEEE Communications Magazine, 2014, Vol. 52, no. 2. pp. 186–195.
5. Goldsmit A. (2005). Besprovodny'e telekommunikacii. Perevod Biryukova N. L., Triski N. R. – Moskva: Texnosfera, 2011. 992 s.
6. Tse, D., Viswanath, P. Fundamentals of Wireless Communication. Cambridge University Press, 2005. 378 p.
7. Slyusar' V. I. Sistemy' MIMO: principy' postroeniya i obrabotka signalov. // E'lektronika: Nauka, Texnologiya, Biznes, 2005. № 8. S. 58–65.
8. Paulraj A., Nabar R., Gore D. Introduction to Space-Time Wireless Communications. Cambridge University Press, 2008, pp. 34–38.
9. Burachenko D. L., Savishhenko N. V. Geometricheskie modeli signal'no-kodovy'x konstrukcij: Ucheb. posobie. Izd. 2-e. – SPb.: VAS, 2020. 390 s.
10. Bakulin M. G., Varukina L. A., Krejndelin V. B. Texnologiya MIMO: principy' i algoritmy'. - M.: Goryachaya liniya – Telekom, 2014. 248 s.
11. Jankiraman M. Space-time codes and MIMO systems. USA, MA: Artech House, 2004. 327 p.
12. Tsoulos G. V. MIMO System Technology for Wireless Communications. CRC Press, 2006, pp. 66–69.
13. Petrov V. P., Yakushev I. Yu. Sovremenny'e texnologii v sisteme MIMO // Vestnik SibGUTI. 2019. № 2. S. 14–25.
14. Chen X., Soh P. J., Sharawi M. S. MIMO Antenna Systems for 5G and Beyond. Wiley-IEEE Press, 2024, pp. 15–18, 43–45.
15. Gershman A. B., Sidiropoulos N. D. Space-time processing for MIMO communications. John Wiley Sons, Ltd, 2005. 369 p.
16. Gore D., Heath R. W., Paulraj A. On performance of the zero forcing receiver in presence of transmit correlation. Proc. IEEE Int. Symp. Inf. Theory, Lausanne, Switzerland, 2002, pp. 159–165.
17. Savischenko N. V., Pelin A. A. Raspredelenie Uisharta dlya analiza pomexoustojchivosti priema mnogoantenny'x sistem besprovodnoj svyazi // Aktual'ny'e problemy' prikladnoj matematiki, informatiki i mexaniki: materialy' Mezh-dunar. nauchnoj konferencii, Voronezh, 12–15 noyabrya 2025 g. – Voronezh: Izdatel'skij dom VGU, 2025. – S. 832–838.
18. Montiouis W., Imoize A. L. Massive MIMO for future wireless communication systems: technology and applications. Wiley, 2025, pp. 61–63.

# РЕШЕНИЕ ПРОБЛЕМЫ СЕМАНТИЧЕСКОЙ ИНТЕРОПЕРАБЕЛЬНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ ТАКТИЧЕСКОГО ЗВЕНА

***Михайлов В. П.[1], Зацепин В. А.[2]***

**DOI:10.21681/3034-4050-2026-2-18-24**

***Ключевые слова:*** *сетецентрическое управление, онтологический инжиниринг, категориальный аппарат, дескрипционная логика, цикл НОРД (наблюдение, ориентация, решение, действие), графы знаний, метаданные, сопряжение гетерогенных сред, машинное понимание.*

***Аннотация***

***Цель работы:*** *повышения уровня семантической интероперабельности гетерогенных информационных систем тактического звена в условиях ведения многодоменных операций за счет разработки теоретико-математических моделей и алгоритмического обеспечения.*

***Метод исследования:*** *применен междисциплинарный подход, включающий методы системного анализа, теория категорий для формализации структур данных, логика Хорна для описания правил преобразования информации, а также теорию Демпстера-Шефера и байесовские сети для слияния данных в условиях неопределенности.*

***Результаты исследования:*** *предложена алгебраическая модель объектно-ориентированной архитектуры взаимодействия военных ИС; сформулирован категориальный критерий семантической эквивалентности трансляции данных. Выполнен анализ мирового опыта. Разработан и верифицирован комплекс алгоритмов семантического сопряжения и доверительной фильтрации разведданных, внедренный в прототип специального программного обеспечения. Разработан оригинальный алгоритмический базис автоматизированного онтологического маппинга и разрешения семантических конфликтов, базирующийся на адаптивном структурно-семантическом анализе метаданных и применении нейросетевых моделей для интерпретации неформализованных тактических сообщений в условиях динамичного боя. Предложена инновационная архитектура семантического шлюза специального программного обеспечения, реализующая концепцию «семантической шины данных» для бесшовной интеграции разнородных элементов разведывательно-ударных контуров без необходимости модификации их исходного программного обеспечения.*

***Научная новизна*** *исследования заключается в обосновании теоретико-методического подхода к обеспечению семантической интероперабельности гетерогенных систем тактического звена на основе синтеза теории категорий и дескрипционной логики, что позволило формализовать и верифицировать процессы смысловой трансформации данных между разнородными информационными моделями в реальном масштабе времени.*

## Введение

Современная эволюция военного дела характеризуется переходом от классических иерархических структур к децентрализованным сетецентрическим операциям, где критическим фактором успеха становится превосходство в скорости принятия решений и точности огневого поражения. В условиях ведения многодоменных операций (Multi-Domain Operations, MDO – в терминах принятых в армии США), охватывающих сушу, море, воздух, космос и киберпространство, интеграция гетерогенных информационных систем (ИС) командования, разведки и поражения превращается в фундаментальную научно-техническую проблему.

В современной парадигме вооруженной борьбы успех достигается за счет синергии действий в физическом, информационном и когнитивном пространствах. Ключевым технологическим укладом становится создание разведывательно-ударных контуров (РУК), функционирующих в реальном масштабе времени. В тактическом звене управления (батальон – рота – взвод – отдельный военнослужащий/робот) наблюдается взрывной рост количества источников информации: от носимых терминалов бойца (системы типа «Ратник» и перспективные «Сотник») до роев беспилотных воздушных судов (БВС) и автономных наземных платформ [1, 6, 8].

Однако, несмотря на развитие каналов связи, сохраняется фундаментальная проблема – низкий уровень семантической интероперабельности. Различные изделия, разработанные разными предприятиями ОПК в разное время, используют несовместимые форматы данных, протоколы и, что самое важное, разные понятийные аппараты (модели данных). Например, координаты цели, переданные с БВС гражданского типа

1 Михайлов Владимир Павлович, начальник группы Главного управления цифрового и технологического развития МО РФ., г. Москва, Россия. E-mail: mixaylovvp@yandex.ru

2 Зацепин Владимир Александрович, кандидат педагогических наук, преподаватель кафедры Военной академии связи, г. Санкт-Петербург, E-mail: vsepin@yandex.ru

в формате текстового обмена данными JavaScript Object Notation (JSON), не воспринимаются напрямую баллистическим вычислителем самоходной артиллерийской установки (требующей СК-42/ПЗ-90 и бинарный протокол) [1, 7, 8], а также предписаны ГОСТом[3].

Традиционные подходы к сопряжению таких систем, основанные на жестко заданных форматах сообщений, приводят к возникновению изолированных туннельных систем. Они способны устанавливать технический канал связи, но зачастую не способны бесшовно взаимодействовать в динамически меняющейся обстановке из-за семантических разрывов. Решением данной проблемы выступает обеспечение семантической интероперабельности – способности взаимодействующих систем не только обмениваться данными, но и одинаковым образом интерпретировать их смысл, сохраняя логическую целостность информации на всех этапах цикла «сенсор – стрелок» [5, 8].

Теоретической базой для решения этой задачи служат наработки в области интероперабельности объектно-ориентированных систем (ООС). Исследования показывают, что процессы сборки и модификации программных комплексов могут быть формализованы через алгебраические модели и онтологии. Перенос этого опыта в область тактических ИС позволяет рассматривать элементы боевого порядка – от разведывательного БВС до артиллерийской батареи – как автономные компоненты открытой информационной системы, взаимодействие которых регулируется семантическими интерфейсами и правилами логического вывода [2, 5, 8].

## 1. Генезис и методологические основы открытых информационных систем в военном управлении

Развитие концепций открытых информационных систем в военной сфере тесно связано с историей вычислительной техники и методологиями программной инженерии. В тактическом звене сложность проявляется в необходимости интеграции унаследованных систем с перспективными комплексами на базе искусственного интеллекта (ИИ) [1, 3, 6].

Принципы SOLID принятые в армии США (Single Responsibility, Open-Closed, Liskov Substitution, Interface Segregation, Dependency Inversion) находят свое отражение в современных военных архитектурах, базирующихся на модульном подходе (Modular Open Systems Approach, MOSA). Данные принципы позволяют создавать масштабируемые системы, где новый сенсор или огневая платформа могут «включаться в бой» без переработки всей сетевой инфраструктуры. Информационный аспект открытой системы в данном контексте характеризуется способностью к обмену данными с внешней средой на основе унифицированных интерфейсов [2, 5].

Особое значение приобретает инверсия управления (Inversion of Control, IoC) и внедрение зависимостей (Dependency Injection).

В классических автоматизированных системах управления войсками (АСУВ) последовательность вызовов функций жестко задана. В адаптивных тактических ИС, подобных нашему разрабатываемому специальному программному обеспечению тактического звена (СПО ТЗ), инфраструктурный слой сам управляет потоками данных, динамически «внедряя» нужную разведывательную информацию в модули огневого поражения на основе изменения тактической ситуации. Такой подход позволяет реализовать принцип «all sensors to all shooters» (все сенсоры для всех стрелков) [2, 5].

Анализ проблемы интероперабельности в современных АСУВ (автоматизированных системах управления войсками). Согласно модели LCIM (Levels of Conceptual Interoperability Model), принятой в международной практике (в т.ч. в стандартах, анализируемых в работах Thomas G., Schaper K.), выделяют несколько уровней совместимости:

1. Технический: способность передать биты (физический канал).
2. Синтаксический: способность разобрать структуру (форматы: XML, JSON, бинарный).
3. Семантический: способность понять смысл (контекст) данных [5, 8].

В настоящее время в ВС РФ успешно решены задачи технического и, частично, синтаксического уровней. Однако семантический разрыв сохраняется. Существующие подходы, основанные на жесткой стандартизации протоколов обмена (Message Text Formats – MTF), в условиях тактического звена показывают низкую эффективность по следующим причинам:

- высокая динамика изменений: появление новых типов вооружения (например, FPV-дронов) происходит быстрее, чем обновляются стандарты информационного обмена;
- гетерогенность парка техники: в одном бою могут участвовать новейшие танки с цифровой бортовой системой и модернизированные образцы 80-х годов с аналоговыми или проприетарными цифровыми интерфейсами;
- ограниченность каналов связи: передача полных XML-схем с метаданными в тактических радиосетях невозможна из-за низкой пропускной способности [1, 6, 8].

3 ГОСТ Р 70569-2022. Информационные технологии. Сетецентрические информационно-управляющие системы. Интероперабельность.

Таким образом, необходим переход от жесткой стандартизации «точка-точка» к адаптивной архитектуре на основе онтологий и графов знаний, что соответствует передовым тенденциям применения искусственного интеллекта [4, 8].

## 2. Математическая формализация семантической интероперабельности

Для обеспечения доказательности и надежности взаимодействия элементов ИС тактического звена вводится строгий математический аппарат.

Любая тактическая ИС может быть представлена как совокупность множеств автономно функционирующих блоков и связей:

$$S = \{BP,BD,LU,LE\}, \quad (1)$$

где $BP$ – множество блоков прикладных моделей (отдельные цели, подразделения, события), $BD$ – множество спецификаций и стандартов (доменные ограничения), $LU$ – семантические связи (UML-отношения ассоциации, агрегации, композиции), а $LE$ – пространственно-временные связи. В тактическом звене блок $BP$ инкапсулирует состояние боевой единицы. Любая модификация структуры такой системы (например, передача управления беспилотником от одного штаба другому) формализуется через операции CRUD (Create, Read, Update, Delete) над элементами кортежа.

Использование теории категорий позволяет формализовать процессы преобразования данных между разнородными форматами (XML, JSON, и т.д.) и общей онтологической моделью. Семантическая интероперабельность достигается тогда, когда существует морфизм, отображающий категорию моделей данных в категорию общей тактической онтологии $O$. Условие семантической эквивалентности обмена между системой разведки $A$ и системой артиллерии В формулируется через коммутативность диаграммы преобразований:

$$f_{A\to B} = h_{O\to B} \circ g_{A\to O}. \quad (2)$$

Это математически доказывает, что данные, переданные напрямую (через морфизм $f$), абсолютно идентичны по смыслу данным, прошедшим через семантический онтологический посредник (композиция проекции $g$ в онтологию и генерации $h$ из нее). [4, 7, 10]

Данное свойство критически важно для исключения фатальных ошибок интерпретации в условиях дефицита времени. Процесс низкоуровневой семантической трансляции сообщений формализуется с помощью логики предикатов первого порядка, а именно – дизъюнктов Хорна. Дизъюнкт Хорна представляет собой логическую формулу, имеющую не более одного положительного литерала, и имеет вид: [4, 7]

$$A \leftarrow B_1 \wedge B_2 \wedge \ldots \wedge B_n. \quad (3)$$

В контексте нашего СПО ТЗ модификация ИС и трансляция данных выражается через систему правил, которые система автоматически обрабатывает в реальном времени, обеспечивая доказательную трансформацию информационной модели поля боя.

Для решения задачи формализации смысла передаваемой информации предлагается использовать теоретико-множественный подход к описанию онтологии предметной области (2) [2, 4, 8].

Пусть $O$ – онтология предметной области (тактической обстановки), которая может быть представлена кортежем:

$$O = \{C,R,A,I\}, \quad (4)$$

где: $C$ – конечное множество концептов (классов). Примеры: «Бронетехника», «Личный состав», «Укрепление», «Маршрут». $R \subseteq C \times C$ – множество отношений между концептами. Примеры: «атакует», «находится_в», «подчиняется». $A$ – множество атрибутов, описывающих свойства концептов. Примеры: «калибр», «скорость», «принадлежность (свой/чужой)». $I$ – множество экземпляров классов (конкретных объектов на поле боя). В условиях разнородных ИС мы имеем множество локальных онтологий (моделей данных) $O_{1\ldots n}$ соответствующих различным системам (БПЛА, АСУ ПВО, планшет командира).

Задача семантической интероперабельности сводится к нахождению отображения (mapping) $M$:

$$M : O_i \to O_G, \quad (5)$$

где $O_G$ – глобальная (референтная) онтология или единое информационное пространство.

Однако, прямое отображение затруднено из-за семантических конфликтов: конфликты именования: синонимия (в одной системе «БТР», в другой «ArmoredC)arrier») и омонимия; структурные конфликты: различная детализация (в одной системе класс «Танк», в другой – деление на «Т-72Б3» и «Т-90М»), конфликты единиц измерения [4, 8].

Для разрешения этих конфликтов предлагается ввести функцию семантической близости вычисляемую на основе гибридного подхода: лексического анализа и структурного сопоставления графов.

## 3. Онтологическое моделирование и стандарты (jc3iedm)

Центральным компонентом обеспечения семантической совместимости является единая тактическая онтология.

Базовым международным стандартом НАТО разработанным США в этой области выступает JC3IEDM (Joint Consultation, Command and Control Information Exchange Data Model), утвержденный в рамках соглашения STANAG 5525. Модель содержит более 300 классов и свыше 4500 бизнес-правил, описывающих пять фундаментальных сущностей поля боя: Организация (Organization), Материальные средства (Materiel), Особенности местности (Feature), Сооружения (Facility) и Личный состав (Person)[4].

Однако сложность реляционной структуры JC3IEDM и наличие бизнес-правил, описанных на языке OCL (Object Constraint Language), делает прямую реализацию модели громоздкой. В рамках исследования применяется подход семантического отображения, при котором реляционная модель JC3IEDM переводится в формат онтологий OWL-DL (Web Ontology Language – Description Logic). Это позволяет использовать логику подстановок (SWRL-правила) для машинного вывода новых знаний (например, автоматического определения принадлежности объекта на основе паттернов его поведения) прямо на тактическом крае.

## 4. Алгоритмы слияния данных: байесовские сети и теория Демпстера-Шеферас

Семантическая интероперабельность невозможна без разрешения конфликтов в данных (Data Fusion), поступающих от разных сенсоров. Байесовский подход оперирует жесткими вероятностями, что затруднительно в условиях хаоса боя, когда априорные вероятности неизвестны. Для преодоления этого ограничения в нашем прототипе СПО ТЗ применяется теория очевидностей Демпстера-Шефера (Dempster-Shafer theory), которая позволяет оперировать мерой доверия $m$ (mass) к подмножествам гипотез, включая состояние неопределенности. Важным параметром является коэффициент конфликтности $K$. В условиях сильного конфликта классическое правило Демпстера может давать контринтуитивные результаты (например, приписывая высокую вероятность гипотезе, в которой оба сенсора изначально не были уверены). Для решения этой проблемы в алгоритмы СПО интегрированы модифицированные правила пропорционального перераспределения конфликта (например, PCR5 или взвешенное усреднение на основе расстояния Хеллингера). Если конфликт превышает критический порог ($K > 0.8$), система маркирует цель для дополнительной доразведки, предотвращая «дружественный огонь» или пустую трату боеприпасов[5,6].

## 5. Мировой опыт реализации семантической интероперабельности

Верификация предложенных математических моделей опирается на анализ инициатив цифровизации вооруженных сил других государств[7] [9].

Концепция JADC2 и стратегия VAULTIS (США). Стратегия объединенного вседоменного управления и контроля (JADC2) МВ США направлена на создание единого тактического пространства данных (Data Fabric). Ключевым требованием является переход к архитектуре, ориентированной на данные. Согласно доктрине VAULTIS, все данные в боевой сети должны быть: Visible (Видимыми), Accessible (Доступными), Understandable (Понятными), Linked (Связанными), Trustworthy (Достоверными), Interoperable (Интероперабельными) и Secure (Безопасными). Семантическая интероперабельность («Understandable» и «Linked») достигается за счет строгой разметки метаданными и применения открытых протоколов реального времени (например, DDS – Data Distribution Service). Опыт экспериментов показал, что такая интеграция сокращает цикл «сенсор-стрелок» с десятков минут до считанных секунд [9].

Сети НАТО: FMN Spiral 6 и стандарты Link. Инициатива Federated Mission Networking (FMN) обеспечивает оперативную совместимость коалиционных сил. Новейшая 6-я спираль спецификаций (Spiral 6), утвержденная в конце 2025 года, делает упор на тактический уровень. Спираль включает 53 процедурные инструкции и ссылается на более чем 400 стандартов, требуя бесшовного семантического моста между компонентами[7].

Кроме того, активно решается проблема совместимости тактических каналов передачи данных. Современный стандарт Link 22 (заменяющий Link 11 и дополняющий Link 16) использует архитектуру TDMA и обеспечивает загоризонтную связь (BLOS). Сопряжение форматов J-Series сообщений Link 16/22 с IP-сетями требует сложного онтологического отображения, что подтверждает актуальность алгоритмов трансляции [8].

4 JC3IEDM – Joint Consultation, Command and Control Information Exchange Data Model, ver.3.1b. – Brussels: MIP Group, 2012.

5 Dempster A. P. Upper and lower probabilities induced by a multivalued mapping // The annals of mathematical statistics. – 1967. – Vol. 38, No. 2. – P. 325–339.

6 Shafer G. A Mathematical Theory of Evidence. – Princeton University Press, 1976.

7 NATO Federated Mission Networking (FMN) Spiral 6 Specification. – NATO HQ SACT, 2025.

Израильский опыт: система Tzayad и Fire Weaver. Программа цифровизации сухопутных войск ЦАХАЛ «Tzayad» пятого поколения, реализуемая компанией Elbit Systems, является ярким примером внедрения искусственного интеллекта в управление войсками. Система сохраняет подход «human-in-the-loop», где ИИ берет на себя рутину фильтрации больших данных, сужая фокус внимания командира для быстрого принятия решений.

Система Fire Weaver от компании Rafael демонстрирует возможности единого семантического пространства. Она создает GPS-независимый 3D-язык общения на базе гео-пикселей, позволяя любому бойцу видеть на экране прицела ту же цель, что и оператор БПЛА, с точностью до окна здания. Система мгновенно замыкает цикл «сенсор-стрелок», автоматически подбирая оптимальное огневое средство с учетом баллистики и правил безопасности.

## 6. Практическая реализация: архитектура и алгоритмы прототипа СПО

На основе предложенных моделей был разработан программный прототип СПО. Архитектура построена на микросервисном подходе с использованием графовых СУБД для хранения тактической онтологии в реальном времени в соответствии с ГОСТ[8], а также [4, 8].

Реализация алгоритмов распределения данных базируется на агентной модели параллельных вычислений (на базе фреймворка Akka). Каждый элемент системы (БПЛА, цель, орудие) представлен легковесным программным агентом (Supervisor, Scanner, Parser, Builder), которые обмениваются асинхронными сообщениями. Замеры показали, что использование 5 параллельных агентов-строителей (Builder) и 4 агентов-парсеров (Parser) снижает время обработки массива из 1000 тактических сущностей на 50 % (с 1350 мс до ~675 мс) по сравнению с линейными алгоритмами.

В ходе имитационных экспериментов (сценарий «БПЛА – Артиллерийская батарея») достигнуты следующие показатели:

1. Время реакции: сокращение цикла от обнаружения цели до генерации огневой команды с 7–10 минут до менее 2 минут.
2. Точность целеуказания: полное исключение ошибок ручного пересчета координат (человеческого фактора).
3. Достоверность: фильтрация ложных целей на основе модифицированного алгоритма Демпстера-Шефера предотвратила напрасный расход боеприпасов, повысив долю валидированных целей до 98 %.

В рамках исследования разработанная архитектура СПО выступает в роли «Семантического шлюза». Архитектура включает следующие модули:

- Модуль нормализации и синтаксического разбора. Принимает поток данных от сенсоров (NMEA от GPS, MAVLink от дронов, кодограммы тактической сети). Преобразует их в промежуточное представление (RDF-триплеты), не теряя исходной структуры[9].
- Модуль онтологического отображения. Это ядро системы, использующее методы ИИ. Алгоритм работы следующий:
  - *Извлечение метаданных*: Анализ входящего сообщения для определения его типа и источника.
  - *Поиск соответствий*: Использование предварительно обученной нейронной сети (на базе трансформеров, дообученной на военных текстах и уставах), которая преобразует термины источника в векторы и находит ближайшие векторы в эталонной онтологии. *Пример*: Термин uav_alt (высота БПЛА) автоматически сопоставляется с концептом Altitude с атрибутом Unit: Meters. *Логический вывод*: Применение правил (SWRL) для вывода новых знаний. *Пример*: ЕСЛИ объект имеет атрибут type: T-72 и status: hostile, ТО классифицировать как Target_Priority_1.
- Модуль генерации выходных данных. Преобразование унифицированного представления информации в формат, понятный системе-получателю (например, формирование команды целеуказания для АСУ артиллерии в формате протокола обмена).

Реализация этих алгоритмов и использование искусственного интеллекта является ключевой инновацией предлагаемого подхода. Результатом является отказ от статических таблиц перекодировки в пользу динамического анализа. Для этого используется алгоритм вычисления семантической близости на основе графовых метрик. Использование нейросетевых моделей позволяет системе адаптироваться к сленгу или нестандартным сокращениям, часто встречающимся в текстовых чатах тактического звена (например, распознать, что «коробочка» в контексте переговоров означает «БМП» или «Танк») [4, 8].

## 7. Будущие направления: тактическое пространство данных

Дальнейшее развитие систем подобного класса СПО ТЗ лежит в переходе от локальных баз знаний к концепции тактического

8 ГОСТ Р 70569-2022. Информационные технологии. Сетецентрические информационно-управляющие системы. Интероперабельность.

9 NATO STANAG 4586. Standard Interfaces of UAV Control System (UCS) for NATO UAV Interoperability, Ed.2. – Brussels: NATO Standardization Office, 2012.

пространства данных и сетей пространств данных. Это гибридная архитектура, где семантический слой (Semantic Layer) с помощью открытых API «прошивает» данные от датчиков IoT, логистики и разведки, делая их доступными на периферии. Внедрение искусственного интеллекта (перенос нейросетевых моделей непосредственно на процессоры окопных радиостанций и дронов) потребует сверхкомпактных механизмов логического вывода (на базе дизъюнктов Хорна), чтобы устройства могли «договариваться» о целях автономно в условиях подавления связи [9] или NATO Federated Mission Networking (FMN) Spiral 6 Specification. – NATO HQ SACT, 2025.

## Заключение

Обеспечение семантической интероперабельности ИС тактического звена является не просто технической задачей по сопряжению протоколов, а фундаментальным вызовом, определяющим исход многодоменных боевых действий. Перенос методологий разработки и семантической интероперабельности объектно-ориентированных на разработку СПО тактического звена позволяет создать адаптивную архитектуру, способную к самоорганизации [1, 6, 8] и соответствующую ГОСТ Р 70569-2022. «Информационные технологии. Сетецентрические информационно-управляющие системы. Интероперабельность.»

Применение математического аппарата теории категорий, дизъюнктов Хорна и теории очевидностей Демпстера-Шефера гарантирует строгую эквивалентность преобразования данных и надежность фильтрации конфликтующей разведывательной информации. Разработанный прототип СПО и анализ мирового опыта (JADC2, FMN, Tzayad, Fire Weaver) доказывают, что онтологический подход радикально сокращает разведывательно-ударный цикл, снижает когнитивную нагрузку на командиров и обеспечивает решающее информационное превосходство на современном поле боя. В работе предложено решение фундаментальной научно-технической проблемы семантической интероперабельности ИС тактического звена. Разработанная модель на основе онтологий и алгоритмы семантического маппинга, реализованные в прототипе СПО, доказали свою эффективность.

## Литература


1. Анисимов В. Г., Анисимов Е. Г. Проблемы и подходы к обеспечению информационного взаимодействия в автоматизированных системах военного назначения // Военная мысль. – 2021. – № 9. – С. 64–72.
2. Захаров А. С. Модели и алгоритмы семантической интероперабельности элементов объектно-ориентированных систем: дис. канд. техн. наук: 05.13.01. – Нижний Новгород: НГТУ им. Р. Е. Алексеева, 2022. – 155 с.
3. Кузнецов С. В., Мельников А. А. Методы информационного обеспечения сетецентрических систем управления войсками // Сборник трудов ВИА. – 2020. – № 2(79). – С. 10–18.
4. Ломакин, И. В. Применение методов искусственного интеллекта для автоматизации семантического сопряжения данных в тактических сетях // Телекоммуникации и связь. – 2023. – № 3. – С. 15–23.
5. Макаренко, С. И. Интероперабельность информационных систем: монография. – Санкт-Петербург: Наукоемкие технологии, 2021. – 654 с.
6. Макаренко С. И. Робототехнические комплексы военного назначения – современное состояние и перспективы развития. – СПб.: Наукоемкие технологии, 2019.
7. Мирошников, В. В. Семантическая интероперабельность автоматизированных систем управления в условиях сетецентрических войн // Информационно-управляющие системы. – 2018. – № 4. – С. 45–52.
8. Цыгичко, В. Н., Смолян, Г. Л. Проблемы межуровневой интероперабельности в системах управления специального назначения // Информационные технологии и вычислительные системы. – 2022. – № 1. – С. 12–21.
9. Summary of the Joint All-Domain Command and Control (JADC2) Strategy. – Department of Defense, USA, 2022.


# SOLVING THE PROBLEM OF SEMANTIC INTEROPERABILITY OF TACTICAL INFORMATION SYSTEMS

***Mikhailov V. P.[10], Zatsepin V. A.[11]***

***Keywords:*** *network-centric control, ontological engineering, categorical apparatus, description logic, NORD cycle (observation, orientation, decision, action), knowledge graphs, metadata, coupling of heterogeneous media, machine understanding.*

10 Vladimir P. Mikhailov, Head of the Group of the Main Directorate of Digital and Technological Development of the Ministry of Defense of the Russian Federation, Moscow, Russia. E- mail: mixaylovvp@yandex.ru

11 Vladimir A. Zatsepin, Ph.D. of Pedagogical Sciences, Lecturer of the Department of the Military Academy of Communications, St. Petersburg, E-mail: vsepin@yandex.ru

***Abstract***

***The purpose of the work*** *is to increase the level of semantic interoperability of heterogeneous tactical information systems in the conditions of multi-domain operations through the development of theoretical and mathematical models and algorithmic support.*

***Research method:*** *an interdisciplinary approach is applied, including methods of system analysis, category theory for the formalization of data structures, Horn logic for describing the rules for transforming information, as well as the Dempster-Schaefer theory and Bayesian networks for data fusion under uncertainty.*

***Results of the research:*** *an algebraic model of the object-oriented architecture of interaction of military information systems is proposed; a categorical criterion for semantic equivalence of data translation is formulated. An analysis of world experience is carried out. A set of algorithms for semantic conjugation and trusted filtering of intelligence data, implemented in the prototype of special software, has been developed and verified. An original algorithmic basis for automated ontological mapping and semantic conflict resolution based on adaptive structural-semantic analysis of metadata and the use of neural network models for the interpretation of non-formalized tactical messages in dynamic combat is developed. An innovative architecture of the semantic gateway of special software is proposed, which implements the concept of a «semantic data bus» for seamless integration heterogeneous elements of reconnaissance and strike circuits without the need to modify their original software.*

***The scientific novelty*** *of the study lies in the substantiation of the theoretical and methodological approach to ensuring the semantic interoperability of heterogeneous tactical systems based on the synthesis of category theory and description logic, which made it possible to formalize and verify the processes of semantic transformation of data between heterogeneous information models in real time.*

## References

1. Anisimov V. G., Anisimov E. G. Problemy' i podxody' k obespecheniyu informacionnogo vzaimodejstviya v avtomatizirovanny'x sistemax voennogo naznacheniya // Voennaya my'sl'. – 2021. – № 9. – S. 64-72.
2. Zaxarov A. S. Modeli i algoritmy' semanticheskoj interoperabel'nosti e'lementov ob''ektno-orientirovanny'x sistem: dis. kand. texn. nauk: 05.13.01. – Nizhnij Novgorod: NGTU im. R. E. Alekseeva, 2022. – 155 s.
3. Kuzneczov S. V., Mel'nikov A. A. Metody' informacionnogo obespecheniya setecentricheskix sistem upravleniya vojskami // Sbornik trudov VIA. – 2020. – № 2(79). – S. 10–18.
4. Lomakin, I. V. Primenenie metodov iskusstvennogo intellekta dlya avtomatizacii semanticheskogo sopryazheniya danny'x v takticheskix setyax // Telekommunikacii i svyaz'. – 2023. – № 3. – S. 15–23.
5. Makarenko, S. I. Interoperabel'nost' informacionny'x sistem: monografiya. - Sankt-Peterburg: Naukoemkie texnologii, 2021. – 654 s.
6. Makarenko S. I. Robototexnicheskie kompleksy' voennogo naznacheniya – sovremennoe sostoyanie i perspektivy' razvitiya. – SPb.: Naukoemkie texnologii, 2019.
7. Miroshnikov, V. V. Semanticheskaya interoperabel'nost' avtomatizirovanny'x sistem upravleniya v usloviyax setecentricheskix vojn // Informacionno-upravlyayushhie sistemy'. – 2018. – № 4. – S. 45–52.
8. Cygichko, V. N., Smolyan, G. L. Problemy' mezhurovnevoj interoperabel'nosti v sistemax upravleniya special'nogo naznacheniya // Informacionny'e texnologii i vy'chislitel'ny'e sistemy'. – 2022. – № 1. – S. 12–21.
9. Summary of the Joint All-Domain Command and Control (JADC2) Strategy. – Department of Defense, USA, 2022.

# МЕТОДЫ ОБРАБОТКИ ДАННЫХ ДЛЯ РЕШЕНИЯ ЗАДАЧИ БАЛАНСИРОВКИ НАГРУЗКИ ИНФОРМАЦИОННЫХ СИСТЕМ ВОЕННОГО НАЗНАЧЕНИЯ

***Алленов Д. С.[1], Лукьянчик В. Н.[2], Безвесильная А. А..[3]***

**DOI:10.21681/3034-4050-2026-2-25-35**

***Ключевые слова:*** *информационные ресурсы, вычислительные запросы, критерии выбора сервера, параметры информационно-вычислительной системы (ИВС), интегральные показатели различимости серверов.*

***Аннотация***

***Цель:*** *эффективное распределение информационно-вычислительной нагрузки (ИВН) по серверам пунктов управления (ПУ).*

***Метод исследования:*** *математическое описание, экспериментальное исследование, кластерный анализ параметров состояния серверов.*

***Результаты исследования:*** *разработан математический аппарат распределения ИВН на ПУ, создана кластерно-ориентированная модель для выбора сервера, определен набор параметров для эффективного решения задач распределения вычислительной и статической нагрузок с использованием порядково-инвариантной паттерн-кластеризации.*

***Научная новизна:*** *заключается в обосновании целесообразности применения балансировки нагрузки с использованием кластерно-ориентированной модели для выбора сервера в ИВС на ПУ тактического звена для качественного и своевременного решения информационно-расчетных задач.*

## Введение

Современные информационно-вычислительные системы военного назначения являются сложными многоуровневыми территориально распределёнными организационно-техническими комплексами, предназначенными для обеспечения ведения боевых действий.

Ключевым структурным элементом их функционирования выступают пункты управления, реализующие процессы сбора, обработки, хранения и передачи информации. Показатели надёжности, отказоустойчивости и оперативности реагирования данных систем в решающей степени определяются техническим состоянием серверного оборудования, на базе которого развернуты критически важные службы, базы данных, а также прикладное и специализированное программное обеспечение.

В условиях современных вооружённых конфликтов и информационного противоборства существенно возрастает нагрузка на каналы связи и вычислительные ресурсы. Это обусловливает необходимость обеспечения способности ИВС военного назначения к динамической реконфигурации и адаптивному перераспределению вычислительных и сетевых ресурсов. Реализация механизмов распределения нагрузки способствует повышению эффективности функционирования систем за счёт сокращения временных задержек, повышения устойчивости передачи данных и обеспечения адаптации к изменяющимся параметрам каналов связи и внешним воздействиям [7, 8].

## Основная часть

Одним из ключевых механизмов повышения оперативности и надёжности функционирования ИВС является рациональное распределение нагрузки между узлами серверного комплекса. При этом традиционные методы балансировки нагрузки, ориентированные преимущественно на показатели загрузки процессора, не обеспечивают комплексного учёта специфики военной информационной инфраструктуры [1].

Предлагается рассматривать задачу управления нагрузкой как совокупность двух взаимосвязанных подзадач:

- размещение статических информационных ресурсов;
- распределение динамических вычислительных запросов.

Схема информационного обмена между ПУ с балансировкой нагрузки приведена на рисунке 1.

1 Алленов Денис Сергеевич, соискатель. Военная академия связи им. Маршала Советского Союза С. М. Буденного. Санкт-Петербург, Россия. E-mail: allenovdenis@yandex.ru

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

3 Безвесильная Анжела Александровна, кандидат педагогических наук, доцент, заведующая кафедрой информатики и вычислительной техники инженерного факультета Академии гражданской защиты МЧС России имени генерал-лейтенанта Д. И. Михайлика. Химки, Россия. E-mail: a.bezvesilnaia@agz.50.mchs.gov.ru


*Рис. 1. Схема информационного обмена между пунктами управления с балансировкой нагрузки*

Такое разделение позволяет снизить вычислительную сложность и обеспечить адаптивность системы к изменению оперативной обстановки.

Задача распределения статических данных заключается в рациональном размещении и поиске информационных ресурсов пунктов управления, включающих текстовые материалы, графические данные, видеопотоки, получаемые от беспилотных летательных аппаратов, а также иные виды информации, с целью обеспечения их долговременного хранения и регламентированного предоставления по запросам должностных лиц системы управления.

Задача обработки вычислительных запросов формулируется как распределение поступающих запросов между узлами доступа серверного комплекса и обеспечение выполнения операций поиска, чтения, модификации и удаления данных, динамически изменяющихся во времени в процессе функционирования информационной системы.

Наиболее существенными характеристиками вычислительных ресурсов в условиях функционирования автоматизированных систем военного назначения являются стоимостные показатели эксплуатации, параметры сетевой инфраструктуры и вычислительный потенциал аппаратно-программных средств, оказывающие непосредственное влияние на процессы распределения и обработки информационных массивов, формируемых должностными лицами ПУ.

В контексте обеспечения устойчивого функционирования ПУ различного уровня (тактического, оперативного и стратегического звена) особое значение приобретают:

- **стоимостные характеристики** – показатели ресурсных затрат на развертывание, модернизацию и поддержание в готовности вычислительных комплексов в условиях ограниченного военно-экономического обеспечения;
- **сетевые параметры** – пропускная способность каналов связи, задержки передачи данных, помехоустойчивость, защищённость от несанкционированного доступа и кибервоздействия противника;
- **вычислительные характеристики** – производительность процессорных модулей, объём оперативной и долговременной памяти, отказоустойчивость серверных узлов и возможность масштабирования в условиях динамически изменяющейся оперативной обстановки. [2, 3]

Совокупность указанных параметров определяет эффективность распределения информационных потоков и вычислительной нагрузки между элементами распределённой информационно-вычислительной среды, обеспечивающей поддержку принятия управленческих решений должностными лицами органов военного управления в условиях ведения современных форм и способов вооружённой борьбы.

Для математического описания указанных параметров введем следующие параметры:

- $D_s$ – расстояние от должностного лица до сервера ПУ (км) определяется выражением

$$D_s = R \times \Delta\sigma, \quad (1)$$

где $R$ – радиус Земли (км); $\Delta\sigma$ – вычисляется по формуле сферической тригонометрии.

- $U_{cpu}$ – загрузка центрального процессора:

$$U_{cpu} = \frac{1}{k}\sum_{p=0}^{k}\left(1 - \frac{t_{k-p}^{idle}}{t_{k-p}^{usage}}\right), \quad (2)$$

где $k$ = 60 количество исследований в интервале времени, $p$ – номер исследования, $t^{idle}$ – время остановки главного процессора, $t^{usage}$ – время выполнения процессов, $U_{cpu} \in [0;1]$.

- $U_{ram}$ – загрузка оперативной памяти:

$$U_{ram} = \frac{u_{ram}^{used}}{u_{ram}^{total}}, \quad (3)$$

где $u_{ram}^{used}$ – объем использованной оперативной памяти (Кбайт), $u_{ram}^{total}$ – общий общем оперативной памяти (Кбайт), $U_{ram} \in [0;1]$.

- $B_{ch}$ – пропускная способность канала передачи данных военной системы связи (Кбит/с):

$$B_{ch} = \frac{l}{t}, \quad (4)$$

где $l$ – объем передаваемых данных (Кбит), $t$ – время передачи (с).

- $C_{sdr}$ – стоимость затрат на пусконаладку и закупку оборудования, (ден. ед.).

Параметры, характеризующие сетевые и вычислительные характеристики, относятся к категории изменяющихся величин, поскольку их значения зависят от сложившейся обстановки, интенсивности информационного обмена должностных лиц ПУ.

Стоимостной показатель эксплуатации вычислительного ресурса рассматривается как переменный параметр, потому что его значение определяется регионом дислокации, логистическими особенностями театра военных действий и тарифной политикой поставщика аппаратно-программных средств и, как правило, не изменяется в пределах рассматриваемого временного интервала планирования.

Учитывая, что параметры состояния серверных комплексов (в частности, $D_s$, $B_{ch}$, $C_{sdr}$) имеют различные диапазоны изменения и размерности, для обеспечения корректности их совместного использования в интегральной целевой функции оптимизации требуется приведение указанных величин к единому безразмерному интервалу [0;1]. Нормирование параметров осуществляется путём деления текущего значения каждого показателя на его максимальное значение в массиве исходных данных по выражению:

$$\hat{x}\frac{li}{j} = \frac{x_j^{li}}{x_j^{max}}, \quad (5)$$

где $x_j^{li}$ – текущее значение показателя, $x_j^{max}$ – максимальное значение показателя состояния совокупности всех серверных узлов.

В статье задача балансировки нагрузки рассматриваться по двум направлениям:

- адаптивное перераспределение вычислительных запросов должностных лиц (обработки вычислительных запросов);
- рациональное размещение и доставка статических информационных ресурсов (распределения статических данных).

Каждое из указанных направлений требует использования собственной системы показателей состояния серверного комплекса.

В первом случае будем учитывать $D_s$, $U_{ram}$, $U_{cpu}$, во втором случае $D_s$, $B_{ch}$, $C_{sdr}$.

Совокупность серверов пунктов управления обозначим $S = (S_1, S_2, S_3)$.

Приведем в соответствие введенные выше обозначения параметров состояния серверного комплекса характеристикам серверов.

Для вычислительной нагрузки для каждого $l$ -го запроса относительно $i$-го сервера введём вектор состояния:

$$x^{li} = \left(\hat{x}\frac{li}{1}, x\frac{li}{2}, x\frac{li}{3}\right) = (D_s^{li}, U_{ram}^{li}, U_{cpu}^{li}). \quad (6)$$

При рассмотрении задачи распределения статических данных (РСД) вектор параметров состояния примет вид:

$$x^{li} = \left(\hat{x}\frac{li}{1}, x\frac{li}{2}, x\frac{li}{3}\right) = (D_s^{li}, B_{ch}^{li}, C_{sdr}^{li}). \quad (7)$$

Для задачи распределения вычислительной нагрузки (РВН) требуется отправлять запросы должностных лиц пунктов управления на выбранные сервера так, чтобы временные затраты на выполнение задач были минимальны.

Тогда критерий выбора сервера (с учетом параметров его состояния) для решения задачи РВН примет вид:

$$\sum_{l=1}^{q}\sum_{i=1}^{n}\alpha^{li}F(D_s^{li}, U_{cpu}^{li}, U_{ram}^{li}) = \sum_{l=1}^{q}\sum_{i=1}^{n}\alpha^{li}t^{li} \to \min, \quad (8)$$

где $\alpha^{li}$ – признак отправки $l$-го запроса, на $i$-й сервер комплекса; $\alpha^{li}$ = 1, если запрос отправлен; $\alpha^{li}$ = 0, если не отправлен; $F(D_s^{li}, U_{cpu}^{li}, U_{ram}^{li})$ – функция, характеризующая временные затраты.

В задаче распределения статических данных требуется распределить запросы должностных лиц на загрузку данных так, чтобы минимизировать стоимостные и временные затраты на обработку данных.

Тогда критерий выбора сервера для решения задачи РСД примет вид:

$$\sum_{l=1}^{q}\sum_{i=1}^{n}\alpha^{li}F(D_b^{li}, C_{sdr}^{li}) = \sum_{l=1}^{q}\sum_{i=1}^{n}\alpha^{li}(t^{li} + c^{li}) \to \min, \quad (9)$$

где $\alpha^{li}$ – признак отправки $l$-го запроса, $F(D_b, C_{sdr})$ – функция, характеризующая временные затраты.

Ограничения диапазонов параметров:

$$\begin{cases} D_s^{min} \le D_s \le D_s^{max}; \\ U_{ram}^{min} \le U_{ram} \le U_{ram}^{max}; \\ U_{cpu}^{min} \le U_{cpu} \le U_{ram}^{min}; \\ C_{sdr}^{min} \le C_{sdr} \le C_{sdr}^{max}; \\ B_{ch}^{min} \le B_{ch} \le B_{ch}^{max}. \end{cases} \quad (10)$$

Для упрощения процедуры выбора сервера используется агрегированный показатель:

$$X_{sum}^{li} = \sum_{j=1}^{m} \lambda_j x_j^{li},\ l = 1 \ldots q,\ i = 1 \ldots n; \quad (11)$$

$$\sum_{j=1}^{m} \lambda_j = 1,\ \lambda j \in [0,1],$$

где $\lambda j \in [0,1]$ — весовой коэффициент, значение которого характеризует важность параметра (при этом каждый сервер характеризуется не набором из трёх показателей, а лишь одним параметром).

В отличие от традиционного векторного сравнения, переход к скалярному критерию позволяет: снизить вычислительную сложность, реализовать алгоритм в режиме реального времени, динамически изменять веса при изменении боевой обстановки.

## Экспериментальные данные

Для оценки поведения системы балансировки нагрузки был сформирован тестовый набор данных, включающий 50 запросов к каждому из трёх серверов тактического звена ($S_1$, $S_2$, $S_3$). Схема сбора экспериментальных данных для решения задачи распределения нагрузки информационных систем военного назначения показана на рисунке 2.

Передача выполнялась посредством http-запросов на соответствующие uri-адреса, используя специальное программное обеспечение.

В результате для задачи распределения вычислительной нагрузки получено 150 записей параметров состояния (по 50 для каждого сервера), аналогичный объём данных сформирован для задачи распределения статической нагрузки.

Все параметры предварительно нормированы в диапазоне [0;1].

Исходные данные для задачи распределения вычислительной нагрузки приведены в таблице 1.

Построенное распределение загрузки CPU сервера $S_1$ показывает слабую дисперсию значений в диапазоне 0,50–0,60, что свидетельствует о стабильном вычислительном профиле при выполнении тестовых запросов (рис. 3).

Распределение загрузки оперативной памяти сервера $S_2$ характеризуется более широкой вариацией (0,20–0,63), что указывает на повышенную чувствительность данного ресурса к интенсивности поступающих запросов.

Полученные распределения позволяют сделать вывод о квазистационарном характере

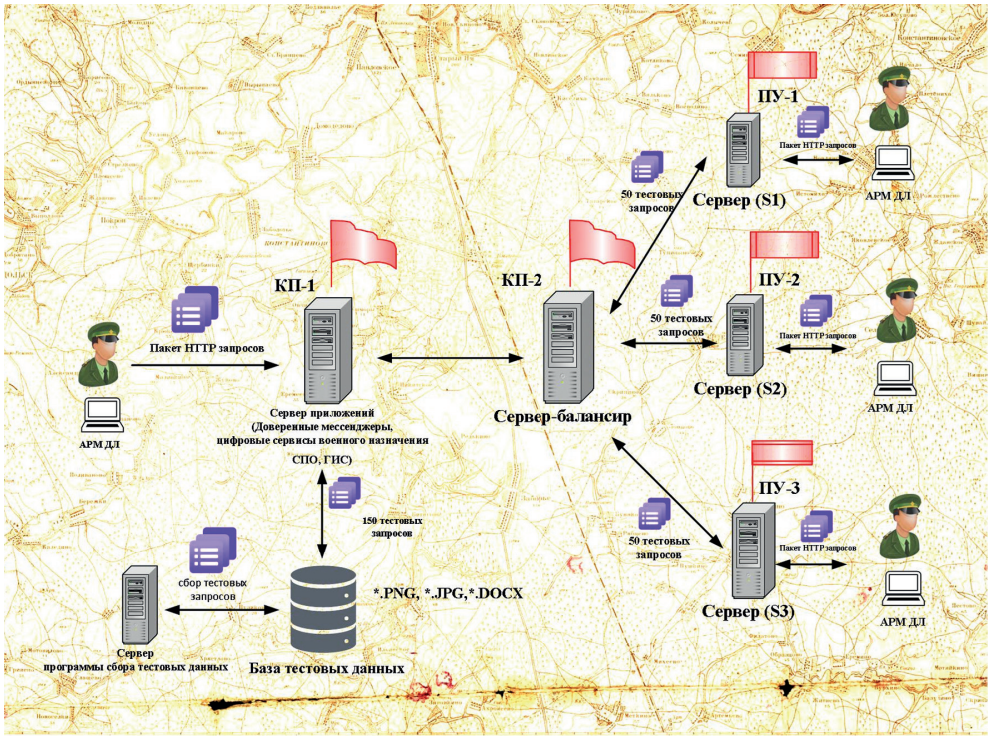



*Рис. 2. Схема сбора экспериментальных данных для решения задачи распределения нагрузки информационных систем военного назначения*

*Таблица 1.*

*Исходные данные для задачи распределения вычислительной нагрузки*

| Номер запроса | Расстояние от должностного лица до сервера пункта управления, $D_s^{li}$ | | | Загруженность оперативной памяти, $U_{ram}^{li}$ | | | Загруженность центрального процессора, $U_{cpu}^{li}$ | | |
|---|---|---|---|---|---|---|---|---|---|
| | $S_1$ | $S_2$ | $S_3$ | $S_1$ | $S_2$ | $S_3$ | $S_1$ | $S_2$ | $S_3$ |
| 1 | 0,66 | 0,7 | 0,71 | 0,41 | 0,53 | 0,72 | 0,59 | 0,49 | 0,55 |
| 2 | 0,7 | 0,7 | 0,81 | 0,65 | 0,35 | 0,67 | 0,6 | 0,51 | 0,53 |
| … | … | … | … | … | … | … | … | … | … |
| 50 | 0,5 | 0,8 | 0,83 | 0,64 | 0,27 | 0,69 | 0,53 | 0,53 | 0,57 |

*Таблица 2.*

*Исходные данные для задачи распределения статической нагрузки*

| Номер запроса | Расстояние от пользователя до сервера, $D_s^{li}$ | | | Пропускная способность канала передачи данных, $B_{ch}^{li}$ | | | Стоимость затрат, $C_{sdr}^{li}$ | | |
|---|---|---|---|---|---|---|---|---|---|
| | $S_1$ | $S_2$ | $S_3$ | $S_1$ | $S_2$ | $S_3$ | $S_1$ | $S_2$ | $S_3$ |
| 1 | 0,16 | 0,29 | 0,55 | 0,5 | 0,57 | 0,6 | 0,26 | 0,49 | 0,82 |
| 2 | 0,18 | 0,54 | 0,58 | 0,58 | 0,62 | 0,59 | 0,34 | 0,53 | 0,81 |
| … | … | … | … | … | … | … | … | … | … |
| 50 | 0,28 | 0,3 | 0,65 | 0,52 | 0,59 | 0,58 | 0,2 | 0,56 | 0,81 |

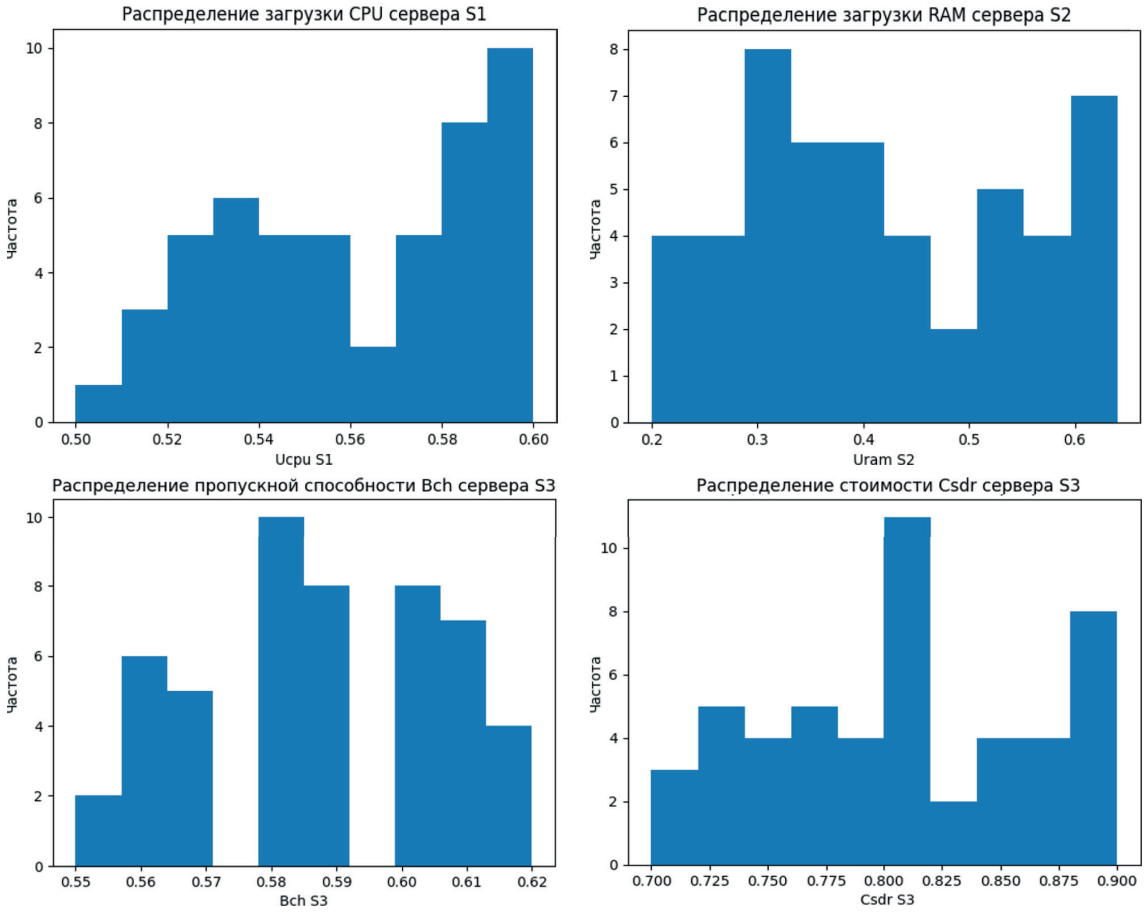



*Рис. 3. Распределение загрузки*

загрузки процессоров, более динамическом изменении загрузки оперативной памяти, отсутствии аномальных выбросов.

Анализ параметров статической нагрузки показывает, что распределение пропускной способности канала сервера $S_3$ демонстрирует концентрацию значений в узком диапазоне 0,55–0,62, что указывает на устойчивость сетевой подсистемы. Распределение стоимости хранения и доставки ($C_{sdr}$) для $S_3$ имеет выраженную асимметрию и охватывает диапазон 0,70–0,90. Это подтверждает доминирующее влияние ценового фактора при выборе данного сервера для размещения статических данных.

Проведённое статистическое исследование распределений параметров позволило установить:

- наличие различной степени вариативности вычислительных и сетевых параметров;
- более высокий уровень детерминированности пропускной способности по сравнению с памятью;
- существенное влияние стоимостного параметра на принятие решения в задаче статического распределения.

Полученные результаты могут быть использованы при формировании весовых коэффициентов в многокритериальной модели оптимизации балансировки нагрузки серверного комплекса.

## Метод структурного анализа паттернов состояния серверного комплекса

Метод структурного анализа паттернов состояния серверного комплекса занимает ключевое место в исследовании, поскольку изолированный анализ отдельных показателей не позволяет выявить причинно-следственные связи между элементами системы. Структурный анализ паттернов обеспечивает выявление устойчивых конфигураций параметров, характеризующих нормальные, предаварийные и критические режимы функционирования. Выявленные структурные паттерны служат основой для построения моделей прогнозирования, что особенно важно в условиях ограниченного времени принятия решений.

С целью обоснования критериев выбора вычислительного узла пункта управления разработана процедура идентификации паттернов состояния серверного комплекса, основанная на порядково-фиксированной кластеризации параметров функционирования.

Пусть для каждого $i$-го сервера формируется усреднённый вектор состояния:

$$\bar{X}^i = (\bar{x}_1^i, \bar{x}_2^i, \ldots, \bar{x}_m^i),\ i = 1,\ldots,n, \qquad (12)$$

где компоненты $\bar{x}_m^i$ представляют собой математические ожидания параметров, рассчитанные по выборке объёма $q = 50$.

Среднее значение для каждого $j$-го параметра определяется выражением:

$$\bar{x}_j^i = \frac{1}{q} \times \sum_{l=1}^{q} \hat{x}_j^{li},\ j = \overline{1,m}. \qquad (13)$$

Предполагается, что нормированные параметры состояния $\bar{x}_j^i \in [0,1]$ формируют уникальную порядковую структуру для каждого сервера.

Для выделения этой структуры вводится отображение

$$\Phi: R^m \rightarrow \{0,1,2\}^{m-l},$$

реализующее попарное сравнение соседних компонент:

$$r_j^i = \begin{cases} 1, \text{ если } \bar{x}_j^i < \bar{x}_{j+1}^i; \\ 0, \text{ если } \bar{x}_j^i = \bar{x}_{j+1}^i; \\ 2, \text{ если } \bar{x}_j^i > \bar{x}_{j+1}^i, \end{cases}$$

характеризует топологическую конфигурацию параметров состояния.

С целью снижения вычислительной сложности процедура сравнения кодов заменяется их позиционным представлением:

$$z^i = \sum_{j=1}^{m-l} 10^{j-1} r_{m-j}^i. \qquad (15)$$

Тем самым задача сопоставления паттернов редуцируется к сравнению целочисленных величин.

Оценка структурной близости серверов выполняется с использованием расстояния Хемминга:

$$d(r_j^i, r_j^h) = \sum_{j=1}^{m-l} |r_j^i - r_j^h|,\ i \neq h. \qquad (16)$$

Серверы относятся к одному кластеру при условии, если $d(r_j^i, r_j^h) = 0$,

В отличие от порядково-инвариантных методов, данная процедура сохраняет фиксированную последовательность параметров, что обеспечивает детерминированность кластерной структуры и однозначность интерпретации результатов.

## Решения задачи распределения вычислительной нагрузки

Вычислим средние значения параметров $D_s^i$, $U_{ram}^i$, $U_{cpu}^i$ для каждого $i$-го сервера на основании исходных данных, приведенных в таблице 1, и представим результаты в таблице 3.

Выполним обработку исходных данных, приведенных в таблице 3, для задачи распределения вычислительной нагрузки, чтобы оценить возможность разбиения серверного комплекса на группы серверов, различимых между собой по параметрам.

*Таблица 3.*

*Параметры состояния серверов пунктов управления для задачи распределения вычислительной нагрузки*

| Обозначение сервера | Средние значения параметров состояния серверов $Si$, $i$ = (1,2,3) | | |
|---|---|---|---|
| | Расстояние от должностного лица до сервера, $D_s^i$ | Загруженность оперативной памяти, $U_{ram}^i$ | Загруженность центрального процессора, $U_{cpu}^i$ |
| $S_1$ | 0,462 | 0,528 | 0,549 |
| $S_2$ | 0,791 | 0,248 | 0,546 |
| $S_3$ | 0,606 | 0,795 | 0,553 |

Так как эксперимент проводится для комплекса из трех серверов разных пунктов управления, то выявим, разделим ли комплекс на три группы.

В соответствии с (11) вектор данных для каждого сервера содержит средние значения параметров состояния:

$$\bar{X}^1 = (\bar{x}_1^1, \bar{x}_2^1, \bar{x}_3^1) = (0{,}462;\ 0{,}528;\ 0{,}549);$$

$$\bar{X}^2 = (\bar{x}_1^2, \bar{x}_2^2, \bar{x}_3^2) = (0{,}791;\ 0{,}248;\ 0{,}546);$$

$$\bar{X}^3 = (\bar{x}_1^3, \bar{x}_2^3, \bar{x}_2^3) = (0{,}606;\ 0{,}795;\ 0{,}553). \qquad (17)$$

Формирование порядково-инвариантных паттернов (позиционных кодов).

В условиях эксплуатации серверного комплекса пункта управления абсолютные значения параметров подвержены флуктуациям (канальная обстановка, профиль задач, пики обращений), поэтому для устойчивого различения объектов целесообразно использовать порядково-инвариантное описание – т.е. не сами значения, а структуру отношений «больше/меньше».

Для каждого сервера выполняется попарное сравнение соседних компонент, приведенных в выражениях (17), и вычислим позиционные коды паттернов (табл. 4).

*Таблица 4.*

*Результаты вычисления позиционных кодов паттернов*

| Сервера | Сравнения | Кодовая последовательность |
|---|---|---|
| $S_1$ | 0,462 < 0,528 < 0,549 | $r^1$ = (1,1) → 11 |
| $S_2$ | 0,791 > 0,248 < 0,546 | $r^2$ = (2,1) → 21 |
| $S_3$ | 0,606 < 0,795 > 0,553 | $r^3$ = (1,2) → 12 |

Таким образом, получены три различные порядковые «сигнатуры» состояния, отражающие разный режим функционирования узлов серверного комплекса пункта управления:

$S_1$ – монотонный рост по всем компонентам;
$S_2$ – «провал» по $U_{ram}$ при высокой удалённости;
$S_3$ – пик по $U_{ram}$ при сравнительно меньших $D_s$ и $U_{cpu}$.

Для кластерного разделения применим расстояние Хемминга между кодовыми последовательностями одинаковой длины (в данном случае длина 2):

$$d(r^1,r^2) = |r^1 - r^2| = |22 - 21| \neq 0;$$
$$d(r^1,r^3) = |r^1 - r^3| = |22 - 12| \neq 0;$$
$$d(r^2,r^3) = |r^2 - r^3| = |21 - 12| \neq 0. \qquad (18)$$

Полученные результаты подтверждают выдвинутую гипотезу: серверы пунктов управления разделимы по выбранному набору параметров состояния ($D_s$, $U_{cpu}$, $U_{ram}$) при применении порядково-инвариантной паттерн-кластеризации.

В условиях рассматриваемого эксперимента (комплекс из трёх серверов пунктов управления) каждый сервер имеет уникальный порядковый паттерн, что приводит к разбиению на три различных кластера.

Практически это означает, что выбранные параметры состояния обеспечивают:

- устойчивое распознавание режимов работы узлов серверного комплекса пунктов управления;
- формирование правил маршрутизации вычислительных запросов должностных лиц на основе типового паттерна, а не мгновенных «шумных» значений;
- повышение живучести и адаптивности распределения нагрузки при изменении обстановки (рост обращений, деградация канала, смена профиля задач).

Таким образом, набор ($D_s$, $U_{cpu}$, $U_{ram}$) является пригодным и достаточным для задачи распределения вычислительной нагрузки в серверном комплексе пунктов управления, а применение порядково-инвариантной паттерн-кластеризации обеспечивает корректное кластерное разделение серверов по состоянию.

## Решение задачи распределения статических данных

В отличие от задачи распределения вычислительных запросов, при размещении статических данных (картографической информации, графических материалов, архивов телеметрии,

*Таблица 5.*

*Параметры серверов пунктов управления для задачи распределения данных*

| Обозначение сервера | Средние значения параметров состояния серверов $Si$, $i$ = (1,2,3) | | |
|---|---|---|---|
| | Расстояние от пользователя до сервера, $D_s^i$ | Доступная пропускная способность канала передачи данных, $B_{ch}^i$ | Стоимость затрат на хранение, доставку и репликацию данных, $C_{sdr}^i$ |
| $S_1$ | 0,286 | 0,5848 | 0,374 |
| $S_2$ | 0,5466 | 0,7526 | 0,376 |
| $S_3$ | 0,787 | 0,2672 | 0,461 |

регламентирующих документов и др.) необходимо учитывать кроме сетевой удалённости, следующие два параметра:

- доступную пропускную способность канала связи $B_{ch}^i$;
- совокупные затраты на хранение, доставку и репликацию данных $C_{sdr}^i$;

Вектор состояния $i$-го сервера формализуется в виде:

$$\bar{X}^i = (\bar{x}_1^i, \bar{x}_2^i, \bar{x}_3^i) = (D_s^i; B_{ch}^i; C_{sdr}^i). \quad (19)$$

В таблице 5 приведены средние значения по результатам обработки 50 экспериментальных запросов получены средние значения параметров.

Таким образом, для задачи распределения данных сервера описываются следующими векторами параметров:

$$\bar{X}^1 = (\bar{x}_1^1, \bar{x}_2^1, \bar{x}_3^3) = (0{,}286; 0{,}584; 0{,}374);$$
$$\bar{X}^2 = (\bar{x}_1^2, \bar{x}_2^2, \bar{x}_3^3) = (0{,}546; 0{,}752; 0{,}376);$$
$$\bar{X}^3 = (\bar{x}_1^3, \bar{x}_2^3, \bar{x}_3^3) = (0{,}787; 0{,}267; 0{,}461). \quad (20)$$

Выполним парные сравнения параметров состояния в соответствии с выражением (13) и сформируем кодовые последовательности по выражению (14) алгоритма порядково-фиксированной паттерн-кластеризации, результаты приведены в таблице 6.

*Таблица 6.*

*Попарное сравнение смежных компонент вектора состояния*

| Сервера | Сравнения | Кодовая последовательность |
|---|---|---|
| $S_1$ | 0,286 < 0,585 > 0,374 | $r^1$ = (1,2) → 12 |
| $S_2$ | 0,547 < 0,753 > 0,376 | $r^2$ = (2,1) → 12 |
| $S_3$ | 0,787 > 0,267 < 0,461 | $r^3$ = (1,2) → 21 |

Из сказанного вы следует, что серверы $S_1$ и $S_2$ имеют совпадающие позиционные коды. В фиксированной постановке задачи они относятся к одному кластеру. Сервер $S_3$ отделим.

Это позволяет выдвинуть гипотезу о структурной близости $S_1$ и $S_2$.

По результатам, приведенным в таблице 6, при порядково-инвариантной кластеризации структуры изменения параметров состояния серверов $S_1$ и $S_2$ различаются, то есть эти объекты отделимы. Это отличается от результатов паттерн-фиксированной кластеризации, когда было получено, что сервера $S_1$ и $S_2$ относятся к одному кластеру (их позиционные коды совпадают (см. табл. 6).

Выдвинутая гипотеза дополнительно проверялась с помощью кластерного анализа данных, и полученные результаты подтвердили, что сервера $S_1$ и $S_2$ трудно отличимы.

Для усиления дискриминационной способности признакового пространства вводится интегральный показатель сетевой эффективности:

$$D_b^i = D_s^i \cdot B_{ch}^i. \quad (21)$$

Новый вектор состояния:

$$X_b^* = (D_b^i, C_{sdr}^i). \quad (22)$$

Данный показатель отражает совокупное влияние удалённости и пропускной способности, что особенно актуально в условиях:

- деградации каналов связи;
- радиоэлектронного противодействия;
- перегрузки сетевой инфраструктуры.

Использование параметра $D_b$ повышает различимость серверов и снижает вероятность ошибочной кластеризации.

На рисунке 4 показаны кусочно-линейные функции параметров серверов для параметров $D_b$, $C_{sdr}$.

В фиксированной постановке серверы $S_1$ и $S_2$ структурно близки. В инвариантной постановке различимость усиливается. Введение параметра $D_b$ повышает устойчивость алгоритма. Разработанная модель позволяет реализовать адаптивный механизм размещения статических данных в условиях динамически изменяющейся оперативной обстановки.

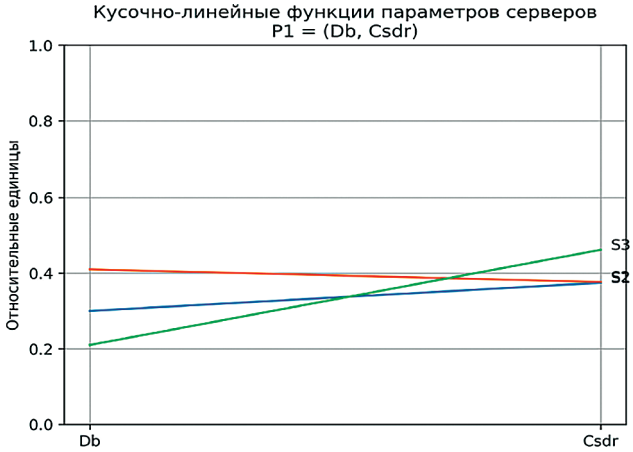



*Рис. 4. Кусочно-линейные функции параметров серверов, соответствующие паттерну P1 = ($D_b$, $C_{sdr}$)*

## Кластерно-ориентированная модель выбора сервера пункта управления.

**Формализация параметров состояния серверного комплекса**

В условиях функционирования автоматизированных систем управления военного назначения распределение нагрузки должно осуществляться с учетом совокупности сетевых, вычислительных и стоимостных характеристик серверных узлов.

С учетом параметрического описания, приведенного в исходном материале, вектор состояния сервера формируется следующим образом:

$$J_0 = \sum_{l=1}^{q}\sum_{i=1}^{n}\|\tilde{X}^1 - C_i\|^2 \to \min, \quad (23)$$

$$x^l = (D_s^l, D_{ram}^l, U_{cpu}^l, B_{ch}^l, C_{sdr}^l). \quad (24)$$

**Нормирование параметров**

Поскольку параметры имеют различную размерность и диапазоны изменения, выполняется их нормализация:

$$\tilde{x}_k^l = \frac{x_k^l}{\max(x_k)}, \quad (25)$$

где $\max(x_k)$ – максимальное значение $k$-го показателя среди всех серверов.

После нормирования формируется безразмерный вектор состояния:

$$\tilde{X}^l = (\tilde{D}_s^l, \tilde{U}_{cpu}^l, \tilde{U}_{ram}^l, \tilde{B}_{ch}^l, \tilde{C}_{sdr}^l). \quad (26)$$

**Формальная модель кластерного выбора сервера**

Задача распределения запросов формализуется как минимизация функционала внутрикластерной дисперсии:

$$J = \sum_{i=1}^{n}\sum_{\tilde{X}^l \in S_i}\|\tilde{X}^l - \mu_i\|^2 \to \min, \quad (27)$$

где центроид кластера:

$$\mu_i = \left(\frac{1}{|S_i|}\right) \times \sum_{\tilde{X}^l \in S_i}\tilde{X}^l. \quad (28)$$

Метрика расстояния:

$$\rho(\tilde{X}^l, \mu_i) = \sqrt{\left(\sum_{k=1}^{m}(\tilde{x}_k^l - \mu_{ik})^2\right)}. \quad (29)$$

Таким образом, сервер выбирается по критерию минимального расстояния:

$$F(\tilde{X}^l) = \operatorname{argmin}_i \rho(\tilde{X}^l, \mu_i). \quad (30)$$

**Учет неопределенности: нечеткая кластеризация**

В условиях динамического изменения параметров состояния серверов используется функционал нечеткой кластеризации: где $m > 1$ – параметр нечеткости.

Центры кластеров:

$$C_i = \frac{\left(\sum_{l=1}^{q}\mu_{li}^m \tilde{X}^l\right)}{\sum_{l=1}^{q}\mu_{li}^m}. \quad (31)$$

Степень принадлежности:

$$\mu_{li} = \left(\sum_{k=1}^{n}\left(\frac{\|\tilde{X}^l - C_i\|}{\|\tilde{X}^l - C_k\|}\right)^{\frac{2}{m-1}}\right)^{-1}. \quad (32)$$

Данный механизм обеспечивает адаптивность распределения при вариациях – загрузки CPU, загрузки памяти, сетевых характеристик, изменения стоимостных ограничений.

## Интегральные показатели различимости серверов

Для повышения дискриминационной способности вводятся интегральные критерии:

**Мультипликативный показатель:**

$$D_b = \tilde{D}_s \times \tilde{B}_{ch}, \quad (33)$$

отражающий совместное влияние удаленности и пропускной способности канала.

Аддитивный критерий вычислительной нагрузки:

$$K_{add} = \alpha_1\tilde{U}_{cpu} + \alpha_2\tilde{U}_{ram} + \alpha_3\tilde{D}_s. \quad (34)$$

Экспериментально установлено, что:

- для распределения статических данных предпочтителен мультипликативный критерий;
- для распределения вычислительной нагрузки – аддитивный критерий.

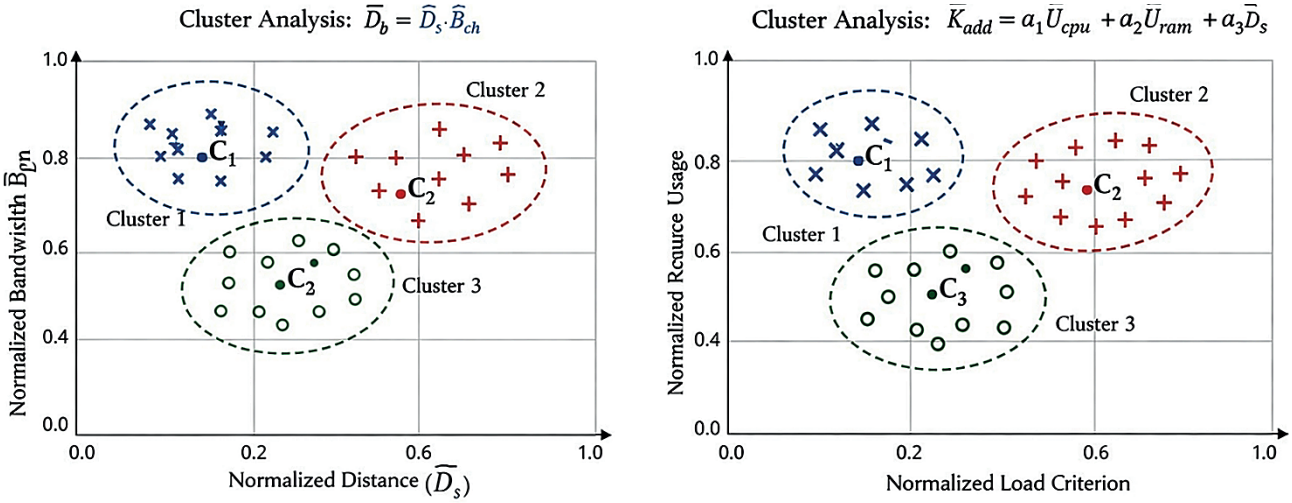
Представим результаты кластеризации данных тестовой выборки для задачи распределения данных с выбранными параметрами.

Результаты кластеризации тестовой выборки (табл. 2) показаны на рисунке 5.

**Кластеризация по мультипликативному критерию**

На рисунке 5а представлено распределение запросов в координатах:

- по оси абсцисс – нормированное расстояние до сервера $\tilde{D}_s$;
- по оси ординат – нормированная пропускная способность канала $\tilde{B}_{ch}$.




а) Мультипликативный критерий $\overline{D}_b = \overline{D}_s \cdot \overline{B}_{ch}$ б) Аддитивный критерий $\overline{K}_{add} = a_1\overline{U}_{cpu} + a_2\overline{U}_{ram} + a_3\overline{D}_s$

*Рис. 5. Результаты кластеризации данных тестовой выборки для задачи распределения данных*

Точки разделены на три кластера, соответствующие трём серверам серверного комплекса:

**Кластер 1** ($S_1$) – минимальное расстояние и высокая пропускная способность канала;

**Кластер 2** ($S_2$) – среднее расстояние и средняя пропускная способность;

**Кластер 3** ($S_3$) – увеличенное расстояние и пониженная пропускная способность.

Центры кластеров $C_1$, $C_2$, $C_3$ отмечены отдельными маркерами.

Наблюдается достаточно четкая пространственная разделимость групп, однако в приграничных областях сохраняется частичное перекрытие, что может приводить к неопределенности при выборе сервера в условиях близких значений сетевых параметров.

Интерпретационно данный критерий эффективен при решении задачи размещения статических данных, где ключевую роль играют параметры транспортной доступности.

**Кластеризация по аддитивному критерию** (рис. 5б).

По оси абсцисс откладывается интегральный нормированный критерий, отражающий совокупное влияние загрузки процессора, памяти и сетевой удаленности, а по оси ординат – нормированная величина вычислительной нагрузки.

В отличие от мультипликативной модели, аддитивный критерий демонстрирует:

- более равномерное распределение центроидов;
- уменьшение областей перекрытия кластеров;
- увеличение межкластерного расстояния.

Кластеры становятся топологически более компактными, что свидетельствует о повышении дискриминационной способности модели при распределении вычислительной нагрузки.

Данный результат подтверждает целесообразность использования аддитивного критерия при обработке динамических вычислительных запросов.

Сравнительный анализ (рис. 5а) и (рис. 5б) показывает, что:

- мультипликативный критерий усиливает влияние сетевых характеристик;
- аддитивный критерий обеспечивает более устойчивое разделение по вычислительным параметрам;
- межкластерная различимость возрастает при использовании интегральных нормированных показателей;
- выбор типа критерия должен определяться характером решаемой задачи (статические данные или вычислительная нагрузка) [4,5,6,7].

## Выводы

Разработанный метод обработки и кластерного анализа параметров состояния серверов обеспечивает структурно обоснованное разделение узлов серверного комплекса и формирует математически корректную основу для адаптивной балансировки нагрузки в условиях динамически изменяющейся оперативной обстановки. Полученные результаты подтверждают достаточность выбранного набора параметров и эффективность применения порядково-инвариантной паттерн-кластеризации при решении задач распределения вычислительной и статической нагрузки в информационных системах военного назначения.

## Литература

1. Алленов Д. С., Курбанов С. Н. Распределение нагрузки в информационных системах военного назначения // Телекоммуникации и связь. 2026. № 1(10). С. 8–15.
2. Агеев А. А. Методы балансировки нагрузки в распределённых информационно-вычислительных системах / А. А. Агеев, И. С. Пахомов // Известия высших учебных заведений. Приборостроение. – 2020. – Т. 63, № 6. С. 537–543.
3. Денисов, О. В. Распределение данных в информационной системе с помощью сервера-балансира / О. В. Денисов, Е. О. Викулов // Прикладная математика и фундаментальная информатика. – 2019. – Т. 6, № 4. – С. 46–57.
4. Кузнецов А. Л. Интеллектуальное распределение вычислительной нагрузки в облачных системах на основе нейронных сетей и кластерного анализа / А. Л. Кузнецов, Д. С. Ермаков // Информационные технологии. – 2022. – № 6. С. 321–328.
5. Ермаков Д. С. Оптимизация распределения нагрузки в облачных вычислительных системах на основе методов кластеризации / Д. С. Ермаков, А. Л. Кузнецов // Информационные технологии. – 2021. – № 4. – С. 215–222.
6. Мячин, А. Л. Анализ паттернов: порядково-инвариантная паттерн-кластеризация / А. Л. Мячин // Управление большими системами: сб. тр. – 2016. Вып. 61. – С. 41–59.
7. 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.
8. Челахов Д. М., Manuel A. C., Кузин П. И., Иванов В. Г. Единое информационное пространство как техническая основа системы управления подразделениями / Известия Высшей военной школы Генерального штаба Вооруженных сил Республики Ангола. 2025. № 1. С. 43–47.


# METHODS OF DATA PROCESSING FOR SOLVING THE PROBLEM OF LOAD BALANCING OF MILITARY INFORMATION SYSTEMS

***Allenov D. S.[4], Lukyanchik V. N.[5], Bezvesilnaya A. A.[6]***

***Keywords:*** *information resources, computational queries, server selection criteria, parameters of the information and computing system (IVS), integral indicators of server distinctiveness.*

***Abstract***

***Goal:*** *effective distribution of the information and computing load (ICN) to the servers of the control points (CP).*

***Research method:*** *mathematical description, experimental research, cluster analysis of server state parameters.*

***Results of the study:*** *a mathematical apparatus for the distribution of IVN to CP has been developed, a cluster-oriented model for server selection has been created, a set of parameters has been determined for effective solution of problems of distribution of computational and static loads using ordinal-invariant pattern clustering.*

***Scientific novelty:*** *consists in the substantiation of the expediency of using load balancing using a cluster-oriented model for the selection of a server in the IVS at the tactical control center for high-quality and timely solution of information and calculation problems.*


## References

1. Allenov D. S., Kurbanov S. N. Raspredelenie nagruzki v informacionny'x sistemax voennogo naznacheniya // Telekommunikacii i svyaz'. 2026. № 1(10). S. 8–15.
2. Ageev A. A. Metody' balansirovki nagruzki v raspredelyonny'x informacionno-vy'chislitel'ny'x sistemax / A. A. Ageev, I. S. Paxomov // Izvestiya vy'sshix uchebny'x zavedenij. Priborostroenie. – 2020. – T. 63, № 6. S. 537–543.
3. Denisov, O. V. Raspredelenie danny'x v informacionnoj sisteme s pomoshh'yu servera-balansira / O. V. Denisov, E. O. Vikulov // Prikladnaya matematika i fundamental'naya informatika. – 2019. – T. 6, № 4. – S. 46–57.
4. Kuzneczov A. L. Intellektual'noe raspredelenie vy'chislitel'noj nagruzki v oblachny'x sistemax na osnove nejronny'x setej i klasternogo analiza / A. L. Kuzneczov, D. S. Ermakov // Informacionny'e texnologii. – 2022. – № 6. S. 321–328.
5. Ermakov D. S. Optimizaciya raspredeleniya nagruzki v oblachny'x vy'chislitel'ny'x sistemax na osnove metodov klasterizacii / D. S. Ermakov, A. L. Kuzneczov // Informacionny'e texnologii. – 2021. – № 4. – S. 215–222.
6. Myachin, A. L. Analiz patternov: poryadkovo-invariantnaya pattern- klasterizaciya / A. L. Myachin // Upravlenie bol'shimi sistemami: sb. tr. – 2016. Vy'p. 61. – S. 41–59.
7. Ivanov V. G. Osnovy' postroeniya i ocenki e'ffektivnosti funkcionirovaniya sistemy' svyazi special'nogo naznacheniya v mezhdunarodnom vooruzhennom konflikte na osnove mnogosfernoj i konvergentnoj struktury' ee e'lementov: Monografiya. – SPb.: POLITEX, 2023. – 298 s.
8. Chelaxov D. M., Manuel A. C., Kuzin P. I., Ivanov V. G. Edinoe informacionnoe prostranstvo kak texnicheskaya osnova sistemy' upravleniya podrazdeleniyami / Izvestiya Vy'sshej voennoj shkoly' General'nogo shtaba Vooruzhenny'x sil Respubliki Angola. 2025. № 1. S. 43-47.



4 Denis S. Allenov, applicant. Military Academy of Communications named after Marshal of the Soviet Union S. M. Budyonny. St. Petersburg, Russia. E-mail: allenovdenis@yandex.ru

5 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

6 Angela A. Bezvesilnaya, Ph.D. of Pedagogical Sciences, Associate Professor, Head of the Department of Informatics and Computer Engineering of the Faculty of Engineering of the Academy of Civil Protection of the Ministry of Emergency Situations of Russia named after Lieutenant General D. I. Mikhaylik. Khimki, Russia. E-mail: a.bezvesilnaia@agz.50.mchs.gov.ru

# ИССЛЕДОВАНИЕ ВЛИЯНИЯ МНОГОСЛОЙНЫХ ДИССИПАТИВНЫХ СРЕД НА ЭФФЕКТИВНОСТЬ АНТЕНН ДЕКАМЕТРОВОГО ДИАПАЗОНА

***Бородулин Р. Ю.[1], Исмаил М. М.[2], Юртаев А. С.[3], Боробов А. А.[4]***

**DOI:10.21681/3034-4050-2026-2-36-42**

***Ключевые слова:*** *коротковолновые антенны, защищенные антенны, параметрический синтез, коэффициент защитного действия, подземные антенны, диссипативные среды, метод конечных разностей во временной области.*

***Аннотация***

***Цель работы:*** *анализ влияния изменений электрических свойств грунта (проводимости и диэлектрической проницаемости) на форму диаграммы направленности и эффективность излучения заглубленных антенн в декаметровом диапазоне радиоволн с учетом сезонных изменений почвы.*

***Метод исследования:*** *в качестве численных методов определения электрических характеристик элементов – метод конечных разностей во временной области.*

***Результаты исследования:*** *разработана математическая модель, основанная на методе конечных разностей во временной области (FDTD), для моделирования распространения электромагнитных волн в слоистых диссипативных средах. Представленная модель демонстрирует высокую чувствительность к коэффициенту электрической проводимости почвы. Доказано, что эффективность излучения можно улучшить за счет управления частотой и геометрией антенны.*

***Практическая ценность:*** *полученные результаты обеспечивают прочную основу для проектирования защищенных систем связи в сложных условиях, таких как неоднородные почвы пустыни.*

***Вклад соавторов:*** *Бородулин Р. Ю. – постановка задачи исследования, выбор численного метода электродинамики; Исмаил М. М. – разработка математической модели электродинамического воздействия различных слоев грунта на заглубленную антенну; Боробов А. А. – разработка методологии исследования, построение вычислительного алгоритма модели; Юртаев А. С. – сравнительная оценка влияния состава почвы и глубины погружения вибратора на эффективность излучения.*

## Введение

Системы связи декаметрового диапазона (3–30 МГц) находят все более широкое применение в военной и гражданской сферах благодаря их способности обеспечивать связь на большие расстояния без необходимости построения сложной инфраструктуры. Использование таких систем в боевых условиях затруднено из-за высокой уязвимости антенн перед воздействием противника.

В стационарных системах эта проблема решается применением подземных антенн. Заглубление антенны приводит к значительному изменению ее излучающих свойств из-за взаимодействия с диссипативной средой, где электрическая проводимость $\sigma$ и относительная диэлектрическая проницаемость $\varepsilon_r$ изменяются в зависимости от состояния и состава почвы [1].

Разработчики защищенных стационарных антенных систем сталкиваются с противоречием между необходимостью обеспечения работы в широком диапазоне частот, высокого коэффициента коэффициента полезного действия (КПД) с одной стороны, и ограничениями на геометрические параметры антенн, с другой. Данное противоречие может быть разрешено на этапе проектирования антенных систем, путем разработки точных математических моделей и использования продвинутых алгоритмов оптимизации [2].

## Постановка задачи

На территории Сирийской Арабской Республики грунты характеризуются значительным разнообразием и слоистой неоднородностью, что затрудняет точное прогнозирование характеристик проектируемых подземных антенных систем.

Таким образом, возникает необходимость в создании точной математической модели, способной адекватно описывать электродинамическое воздействие различных слоев грунта

1 Бородулин Роман Юрьевич, доктор технических наук, доцент, профессор кафедры Военной академии связи, г. Санкт-Петербург, Россия. E-mail: borodulroman@yandex.ru

2 Исмаил Мохамад Малик, адъюнкт Военной академии связи, г. Санкт-Петербург, Россия. E-mail: mohammad.esmaael.2024@gmail.com

3 Юртаев Антон Сергеевич, адъюнкт Военной академии связи, г. Санкт-Петербург, Россия. E-mail: ant8720@yandex.ru

4 Боробов Антон Андреевич, кандидат технических наук, старший преподаватель кафедры Военной академии связи, г. Санкт-Петербург, Россия. E-mail: antonborobov@yandex.ru

на заглубленную антенну. Это требует введения понятия комплексной эффективной диэлектрической проницаемости, учитывающей диэлектрические и проводящие свойства каждого слоя, а также учет межслоевых взаимодействий. Данный подход позволяет снизить вычислительную сложность, сохраняя при этом точность описания волнового распространения в слоистых средах.

## Математические основы модели

Математическая модель, соответствующая диссипативным средам (таким как почва), может быть представлена следующим уравнением распространения:

$$\nabla^2 E - j\omega\mu(\sigma + j\omega\varepsilon)E = \nabla^2 E - \gamma^2 E = 0,$$

где $E$ – напряженность электрического поля (В/м); $\omega$ – угловая частота (рад/с); $\mu$ – магнитная проницаемость среды (Гн/м); $\sigma$ – удельная электрическая проводимость среды (См/м); $\varepsilon$ – диэлектрическая проницаемость среды (Ф/м); $\gamma$ – комплексная постоянная распространения.

Первый член $\nabla^2 E$ характеризует распространение волны в вакууме.

$$\gamma = \sqrt{j\omega\mu(\sigma + j\omega\varepsilon)} = \alpha + j\beta a,$$

где $\alpha$ – коэффициент затухания (Нп/м); $\beta$ – коэффициент фазы (рад/м).

Действительная часть $\alpha$: коэффициент затухания, отражающий потери энергии в среде за счет электропроводности.

$$\alpha = \omega\sqrt{\frac{\mu\varepsilon}{2}\left[\sqrt{\left[1 + \left(\frac{\sigma}{\omega\varepsilon}\right)^2 - 1\right]}\right]}.$$

Мнимая часть ($\beta$): коэффициент фазы, определяющий фазовую скорость и длину волны в среде.

Для моделирования электромагнитного взаимодействия между антенной и многослойной грунтовой средой использовался метод конечных разностей во временной области (Finite-Difference Time-Domain, FDTD). Данный метод основан на решении уравнений Максвелла в дифференциальной форме с использованием алгоритма Йи на смещенной пространственной сетке [3].

Работа модели может быть представлена обобщенным алгоритмом (рис. 1).

***Определение размера ячейки***. Для определения размера ячейки $\Delta$ применялся стандартный критерий, согласно которому для обеспечения точности результатов количество ячеек на длину волны должно быть не менее 10–20. Для повышения эффективности вычислений использовалась неравномерная сетка: в областях вблизи антенны и фидерных линий: $\Delta = \lambda/30$ для точного описания резких изменений полей; в удаленных областях и грунтовых слоях: $\Delta = \lambda/15$ с учетом того, что длина волны в диссипативной среде короче, чем в воздухе ($\lambda$среды = $\lambda_0/\varepsilon r$).

Определение временного шага. Временной шаг $\Delta t$ выбирался в соответствии с условием Куранта–Фридрихса–Леви (CFL) для обеспечения устойчивости численного решения:

$$\Delta t \le \frac{1}{c\sqrt{\frac{1}{(\Delta x)^2} + \frac{1}{(\Delta y)^2} + \frac{1}{(\Delta z)^2}}},$$

где: $c$ – скорость света.

В расчете был использован коэффициент запаса 0,9, т.е. $\Delta t = 0{,}9 \times \Delta t_{max}$. Общее количество временных шагов выбиралось достаточным для затухания полей до нуля внутри расчетной области (обычно $N$ = 10000 шагов).

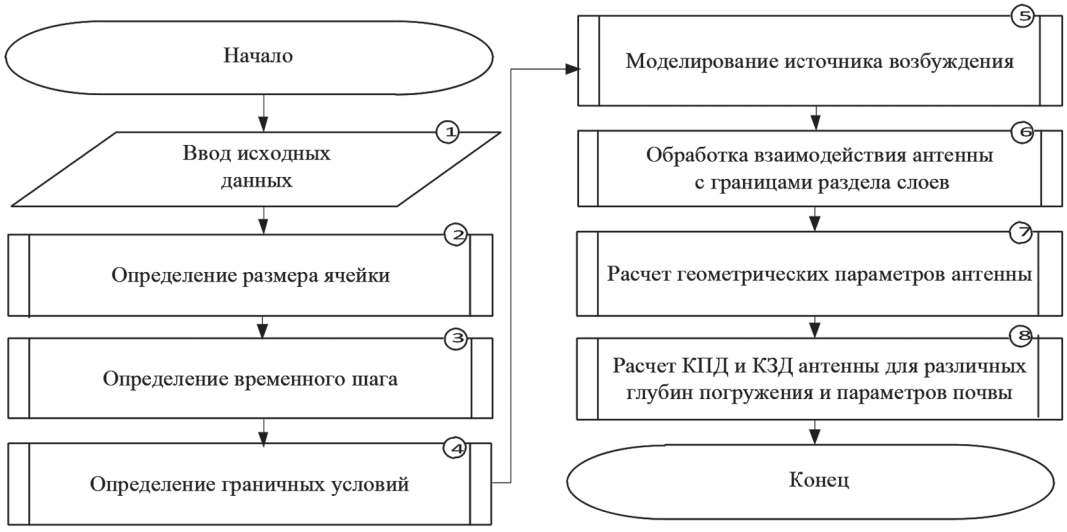



*Рис. 1. Алгоритм работы модели*

***Определение граничных условий***. Для моделирования открытого пространства и предотвращения нежелательных отражений от границ расчетной области применялись поглощающие граничные условия типа «идеально согласованные слои» (Perfectly Matched Layers, PML) которые моделируют бесконечную область с экспоненциальным затуханием амплитуды падающей волны . Эта техника не имеет никакого отношения к физическим процессам, происходящим в макроскопической электродинамике, поскольку основана на искусственно введенной пространственной дисперсии падающих плоских волн, моделируемой на границах расчетной области. Тип PML: Использовалась техника сверточных PML (Convolutional PML, CPML), реализованная во всех шести направлениях ($\pm x,\pm y,\pm z$). CPML обладает высокой эффективностью поглощения поверхностных и наклонных волн по сравнению с традиционными типами [4]. Толщина PML: На каждой границе использовалось 10 слоев (ячеек) PML с постепенным увеличением проводимости согласно полиномиальной функции степени $m = 4$:

$$\sigma(\rho) = \sigma_{max}\left(\frac{\rho}{\delta}\right)^m,$$

где $\rho$ – расстояние от начала PML, $\delta$ – полная толщина PML, а $\sigma_{max}$ рассчитывалась для достижения теоретического коэффициента отражения $R_0 = 10^{-5}$.

***Моделирование источника возбуждения***. Моделирование источника питания антенны выполнялось двумя способами для сравнения:

1. Сосредоточенный источник напряжения (Lumped Voltage Source): идеальный источник напряжения с внутренним сопротивлением $Z_0 = 50\Omega$ помещался в зазор питания между плечами дипольной антенны. Этот метод отличается простотой и быстротой моделирования.
2. Распределенный порт (Distributed Port): Для более точного исследования влияния структуры питания на результаты использовалась модель распределенного порта, охватывающая всю область зазора питания.

В качестве формы волны возбуждения применялся модулированный гауссов импульс, что позволяет охватить требуемый частотный диапазон (3–30 МГц) за одно моделирование [5]:

$$V(t) = sin(2\pi f_0(t - t_0))\ e^{-\left(\frac{t-t_0}{r}\right)^2}.$$

Обработка пересечения антенны с границами различных слоев. Границы раздела между различными слоями грунта (воздух/сухой грунт/влажный грунт) представляют особую сложность при моделировании. Обработка выполнялась следующим образом:

1. Определение электрических характеристик каждой ячейки: значения $\varepsilon$, $\sigma$, $\mu$ присваивались каждой ячейке сетки на основе ее геометрического положения относительно различных слоев. На границах использовалось усреднение значений для избежания резких разрывов.
2. Моделирование тонкопроволочной антенны (Thin-Wire Modeling): Поскольку диаметр антенны ($a$ = 2 мм) значительно меньше размера ячейки ($\Delta$), применялась модифицированная модель тонкого провода (Thin-Wire Model). Эта модель включает коррекцию уравнений поля вокруг провода для учета экспоненциального поведения ближнего поля путем корректировки значений диэлектрической и магнитной проницаемостей в ячейках, окружающих провод, в соответствии с фактическим радиусом провода [6].

***Расчет геометрических параметров антенны***. Целью проектирования антенны является получение определенной диаграммы направленности. Как правило, требуемая форма диаграммы направленности диктуется конкретной задачей – например, обеспечением скрытой связи или управлением беспилотными летательными аппаратами на передовых рубежах, где из-за непрерывных обстрелов и хаотичных разрушений развертывание стационарной сети связи крайне затруднительно. В таких условиях ставка делается на недорогие системы связи, способные обеспечивать непрерывность работы с минимальными затратами. Эту задачу как раз и решают антенны рассматриваемого типа. Геометрические параметры антенны определяют её диаграмму направленности на конкретной частоте [7].

$$I_n(z) = I_{0n} \cdot \frac{sin[k(I_n - |z|)]}{sin(kI_n)},$$

где: $I_{0n}$ – ток питания $n$-го вибратора; $I_n$ – длина $n$-го вибратора; $k$ – волновое число ($k = 2\pi/\lambda$).

В рамках данного исследования было найдено компромиссное решение, обеспечивающее наилучшее согласование таких параметров, как длина антенны, рабочая частота, характеристики слоёв грунта, глубина заглубления, тип металла и необходимое защитное покрытие для предотвращения окисления, которое напрямую влияет на эффективность работы этих антенн (рис. 2).

Дискретизация излучателя и окружающего пространства при использовании метода КРВО создает необходимость определения взаимной импедансной связи между элементами антенны и достижения их достижения их согласования

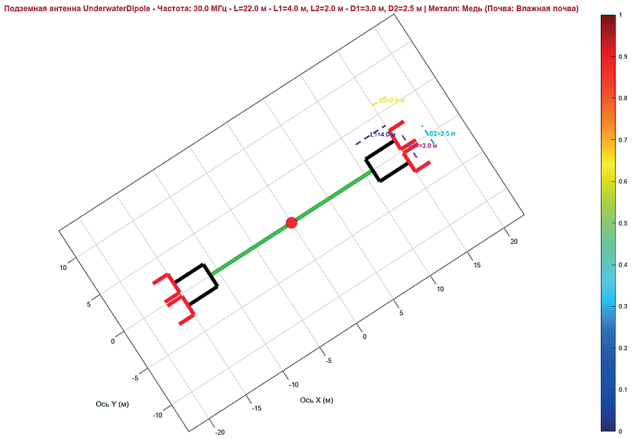



*Рис. 2. Конструкция исследуемой антенны*

по размерам и сопротивлению, взаимное сопротивление двух элементов может быть описано выражением [8]:

$$Z_{mn} = \frac{1}{I_m I_n}\int E_m J_n dV,$$

где $E_m$ – электрическое поле, создаваемое $m$-м вибратором; $J_n$ – плотность тока на $n$-м вибраторе.

Коэффициент отражения, расчитывается по формуле:

$$\Gamma = \frac{Z - Z_0}{Z + Z_0},$$

где $Z$ – входное сопротивление антенны; $Z_0$ – сопротивление источника.

Важность влияния диссипативной среды обусловлена широкой вариативностью её свойств. Помимо поглощения излучения в почве, следует учитывать и действия противника по размещению отражателей , влияющих на эффективность работы антенн, над поверхностью земли. Однако, в данной работе влияние материалов, которые могут быть размещены над поверхностью грунта выведены в ограничения.

Таким образом, при оценке влияние диссипативной среды на распространение радиоволны будем учитывать только коэффициент затухания в почве [9]:

$$\alpha = \omega\sqrt{\frac{\mu\varepsilon}{2}\left[\sqrt{\left[1 + \left(\frac{\sigma}{\omega\varepsilon}\right)^2 - 1\right]}\right]}.$$

В проводящей среде (почве, воде) электромагнитная волна экспоненциально затухает из-за потерь на джоулево тепло. Глубина проникновения $\delta$ обратно пропорциональна коэффициенту затухания $\alpha$

$$\delta = \frac{1}{\alpha} = \sqrt{\frac{2}{\omega\mu\sigma}}.$$

Расчет эффективности излучения антенны для различных глубин погружения и параметров почвы. Оценка эффективности излучения в различных средах произведена по результатам расчетов коэффициента полезного действия (КПД) и коэффициента защитного действия (КЗД) антенны [10]:

$$\eta = \frac{P_{rad}}{P_{rad} + P_{LOSS}},$$

$$\text{КЗД} = \frac{P_{max}(protected)}{P_{max}(unprotected)}.$$

***Результаты моделирования***

На основе вышеизложенного проведено моделирование работы антенны в различных средах в зависимости от глубины погружения в грунт:

а) первый случай: близко к поверхности (воздух) в первом слое – влажный грунт, во втором слое – сухой грунт (рис. 3):

б) второй случай: первый слой – сухой грунт, второй слой – влажный грунт (рис. 4):

Результаты расчетов сведены в таблицу 1.

Влажный грунт дает наименьший процент эффективности излучения – около 45 %. Это объясняется тем, что относительно высокая проводимость (σ = 0,02 см/м) увеличивает потери энергии и снижает эффективность. В то же время в сухом грунте уровень кпд достигает 68 %,

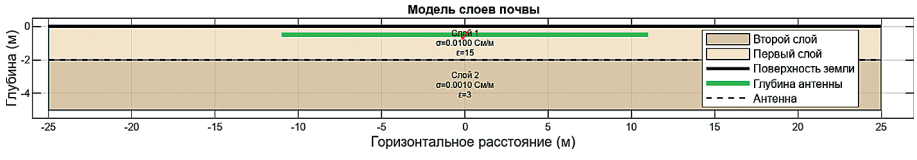



*Рис. 3. Положение антенны для первого случая*

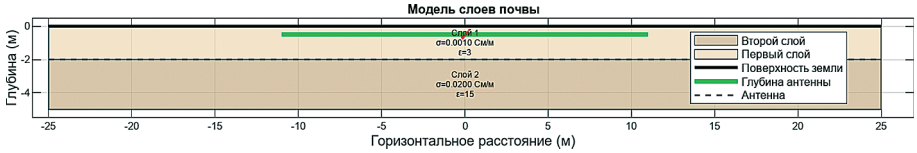



*Рис. 4. Положение антенны для второго случая*

*Таблица 1.*

*Сравнение характеристик антенны в различных средах*

| Эффективность излучения | α (dB/m) | $\varepsilon_r$ | σ (см/м) | Среда распространения волн |
|---|---|---|---|---|
| %98 | 0 | 1 | 0 | Воздух |
| %45 | 2,1 | 15 | 0,02 | Влажная почва |
| %68 | 0,8 | 3 | 0,001 | Сухая почва |

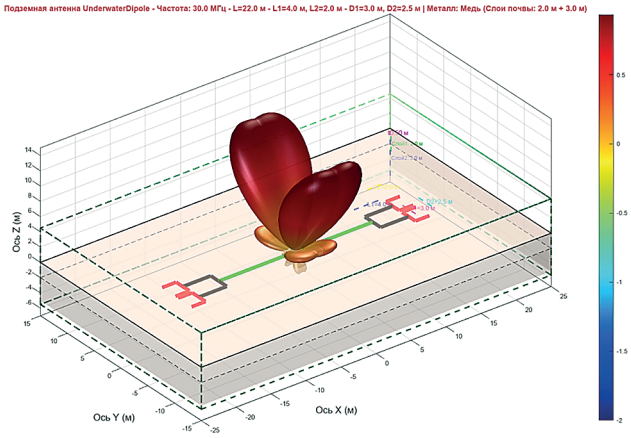



*Рис. 5. Диаграмма направленности для первого случая*

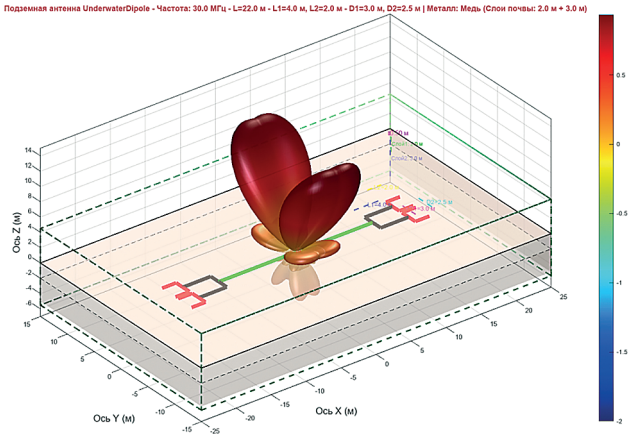



*Рис. 6. Диаграмма направленности для второго случая*

так как низкая проводимость почвы (около 0,001 см/м) уменьшает потери и улучшает эффективность.

Снижение эффективности излучения подтверждается сравнением диаграммы направленности антенны для двух рассматриваемых случаев (рис. 5, 6).

Зависимость коэффициента усиления антенны от частоты носит более выраженный экспоненциальный характер для влажной почвы (рис. 7), что подтверждает непротиворечивость представленной выше модели.

Таким образом, представленная модель демонстрирует высокую чувствительность к коэффициенту электрической проводимости почвы. Доказано, что эффективность излучения можно улучшить за счет управления частотой и геометрией антенны.

На основе вышесказанного можно сделать вывод, что результаты моделирования, представленные в работе, не противоречат известным научным данным, что подтверждает их достоверность

## Заключение

В ходе проведенного исследования, разработана модель многовибраторной антенны, погруженной в среду с потерями, где взаимодействие между вибратором и окружающим пространством моделируется с использованием метода

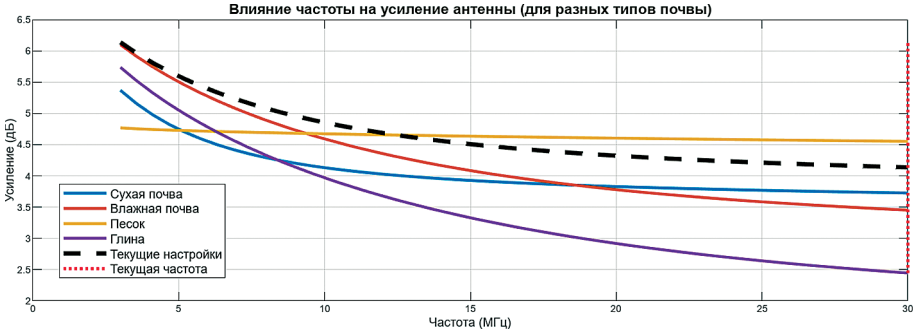



*Рис. 7. Зависимость коэффициента усиления антенны от частоты*

КРВО. Модель основана на предположении, что среда является квази-бесконечной и поглощающей энергию, что позволяет точнее моделировать работу антенны под землей.

Модель предоставляет математическую основу для проектирования высокоэффективных защищенных антенн.

## Литература


1. Бородулин Р. Ю. Методы увеличения эффективности антенн, погруженных в диссипативные среды // Известия высших учебных заведений России. Радиоэлектроника. Вып. 2. СПб.: СПбГЭТУ «ЛЭТИ», 2017. С. 39–45.
2. Баланис К. А. Теория антенн: анализ и проектирование (4-е изд.). Уайли, 2016.
3. Тафлав, А., Хагнесс, С. К. Вычислительная электродинамика: Метод конечных разностей во временной области (3-е изд.). Artech House, 2005.
4. Артемов М. Л. Направления совершенствования характеристик перспективных антенных систем / М. Л. Артемов, О. В. Афанасьев, М. П. Сличенко // Радиотехника. 2023. Т. 87, № 5. С. 184–198.
5. Бородулин Р. Ю. Конструктивный синтез малогабаритных электрических антенн. Санкт-Петербург: Военная академия связи, 2020.
6. Кинг Р. У. П., и Смит, Г. С. Антенны в материи: основы, теория и приложения. Издательство Массачусетского технологического института, 1981.
7. Уэйт Дж. Р. Электромагнитные волны в стратифицированных средах. IEEE Press, 1996.
8. Смит Г. С. «Сравнение антенн с электрическим приводом для использования в геофизической разведке». Труды IEEE по наукам о земле и дистанционному зондированию, GE 22(6), 1984. С. 543–549.
9. Бородулин Р. Ю. Анализ эффективности синфазной системы погруженных вибраторов // Телекоммуникации. 2017. № 9. С. 28–35.
10. Бородулин Р. Ю. Применение концептуальных моделей численных методов электродинамики для анализа характеристик вибраторов в бесконечных диссипативных средах // Информатика. Телекоммуникации. Управление. Научно-технические ведомости СПбГПУ. Вып. 4(236). СПб.: СПбГПУ, 2016. С. 29–42.


# INVESTIGATION OF THE EFFECT OF MULTILAYER DISSIPATIVE MEDIA ON THE EFFICIENCY OF ANTENNAS OF THE DECAMETER RANGE

***Borodulin R. Yu.[5], Ismail M. M.[6], Yurtaev A. S.[7], Borobov A. A.[8]***

***Keywords:*** *short-wave antennas, protected antennas, parametric synthesis, coefficient of protective action, underground antennas, dissipative media, finite difference method in the time domain.*

***Abstract***

***Objective:*** *analysis of the effect of changes in the electrical properties of the soil (conductivity and permittivity) on the shape of the radiation pattern and the radiation efficiency of buried antennas in the decameter range of radio waves, taking into account seasonal changes in the soil.*

***Research method:*** *the method of finite differences in the time domain is used as numerical methods for determining the electrical characteristics of elements.*

***Practical value:*** *the results obtained provide a solid basis for the design of secure communication systems in difficult conditions, such as heterogeneous desert soils.*

***Contribution of co-authors:*** *Borodulin R. Yu. – formulation of the research problem, choice of the numerical method of electrodynamics; Ismail M. M. – development of a mathematical model of the electrodynamic effect of various soil layers on the buried antenna; Borobov A. A. – development of the research methodology, construction of a computational algorithm of the model; Yurtaev A. S. – comparative assessment of the effect of soil composition and immersion depth of the vibrator on the efficiency of radiation.*

## References


1. Borodulin R. Yu. Metody' uvelicheniya e'ffektivnosti antenn, pogruzhenny'x v dissipativny'e sredy' // Izvestiya vy'sshix uchebny'x zavedenij Rossii. Radioe'lektronika. Vy'p. 2. SPb.: SPbGE'TU «LE'TI», 2017. S. 39–45.
2. Balanis K. A. Teoriya antenn: analiz i proektirovanie (4-e izd.). Uajli, 2016.



5 Roman Yu. Borodulin, Dr.Sc. of Technical Sciences, Associate Professor, Professor of the Department of the Military Academy of Communications, St. Petersburg, Russia. E-mail: borodulroman@yandex.ru

6 Ismail Mohamad Malik, Adjunct of the Military Academy of Communications, St. Petersburg, Russia. E-mail: mohammad.esmaael.2024@gmail.com

7 Anton S. Yurtaev, Adjunct of the Military Academy of Communications, St. Petersburg, Russia. E-mail: ant8720@yandex.ru

8 Anton A. Borobov, Ph.D. of Technical Sciences, Senior Lecturer of the Department of the Military Academy of Communications, St. Petersburg, Russia. E-mail: antonborobov@yandex.ru

3. Taflav, A., Xagness, S. K. Vy'chislitel'naya e'lektrodinamika: Metod konechny'x raznostej vo vremennoj oblasti (3-e izd.). Artech House, 2005.
4. Artemov M. L. Napravleniya sovershenstvovaniya xarakteristik perspektivny'x antenny'x sistem / M. L. Artemov, O. V. Afanas'ev, M. P. Slichenko // Radiotexnika. 2023. T. 87, № 5. S. 184–198.
5. Borodulin, R. Yu. Konstruktivny'j sintez malogabaritny'x e'lektricheskix antenn. Sankt-Peterburg: Voennaya akademiya svyazi, 2020.
6. King R. U. P., i Smit, G. S. Antenny' v materii: osnovy', teoriya i prilozheniya. Izdatel'stvo Massachusetskogo texnologicheskogo instituta, 1981.
7. Ue'jt Dzh. R. E'lektromagnitny'e volny' v stratificirovanny'x sredax. IEEE Press, 1996.
8. Smit G. S. Sravnenie antenn s e'lektricheskim privodom dlya ispol'zovaniya v geofizicheskoj razvedke. Trudy' IEEE po naukam o zemle i distancionnomu zondirovaniyu, GE–22(6), 1984. S. 543–549.
9. Borodulin R. Yu. Analiz e'ffektivnosti sinfaznoj sistemy' pogruzhenny'x vibratorov // Telekommunikacii. 2017. № 9. S. 28–35.
10. Borodulin R. Yu. Primenenie konceptual'ny'x modelej chislenny'x metodov e'lektrodinamiki dlya analiza xarakteristik vibratorov v beskonechny'x dissipativny'x sredax // Informatika. Telekommunikacii. Upravlenie. Nauchno-texnicheskie vedomosti SPbGPU. Vy'p. 4 (236). SPb.: SPbGPU, 2016. S. 29–42.

# ЗАДАЧА ГЕНЕРАЦИИ КОДА ПРЕДМЕТНО-ОРИЕНТИРОВАННЫХ ЯЗЫКОВ С ИСПОЛЬЗОВАНИЕМ БОЛЬШИХ ЯЗЫКОВЫХ МОДЕЛЕЙ (НА ПРИМЕРЕ POLKIT)

***Назимов А. М.***[1]

**DOI:10.21681/3034-4050-2026-2-43-49**

***Ключевые слова:*** *большие языковые модели, Polkit, Text2DSL, структурированный контекст, валидация программ.*

***Цель исследования:*** *формализация задачи автоматической генерации кода предметно-ориентированных языков (DSL) по описанию на естественном языке (Text2DSL) как самостоятельного класса задач и эмпирическая оценка роли структурированного контекста при генерации DSL-кода большой языковой моделью.*

***Методы исследования:*** *эксперимент с двумя условиями (базовый режим и режим с контекстом) на датасете PolkitBench (4 204 верифицированные пары «запрос на естественном языке – правило Polkit»), трёхуровневая AST-валидация через парсер esprima, метрики синтаксической и семантической корректности.*

***Результаты исследования:*** *включение структурированного контекста (BNF-грамматика, API-спецификация, словарь допустимых идентификаторов) повышает синтаксическую корректность с 80,5 % до 99,4 % (+23,4 %), семантическую корректность – с 60,4 % до 95,9 % (+58,7 %). Для класса задач Text2DSL включение формальной спецификации целевого языка в контекст запроса является необходимым и достаточным условием качественной генерации без дообучения модели.*

***Научная новизна:*** *формализация задачи Text2DSL как отдельного класса задач генерации кода; датасет PolkitBench (4 204 верифицированные пары, трёхуровневая AST-валидация); эмпирическое обоснование критической роли структурированного контекста для качественной генерации DSL-кода.*

## Введение

Управление политиками безопасности в современных программных системах реализуется посредством специализированных предметно-ориентированных языков (Domain-Specific Languages, DSL). К числу таких языков относятся Polkit – система авторизации привилегированных операций в Linux, SELinux policy language для мандатного управления доступом, OPA Rego для описания политик в облачной инфраструктуре, а также Terraform HCL для декларативного описания инфраструктуры.

Практическая разработка правил на указанных языках требует от администратора одновременного владения синтаксисом DSL, знанием допустимых идентификаторов API и пониманием семантики целевой системы. Ошибка в правиле может приводить как к отказу в обслуживании легитимных пользователей, так и к критическим нарушениям политики безопасности, включая несанкционированную эскалацию привилегий.

Существенный прогресс больших языковых моделей (БЯМ) в задачах генерации программного кода [1–6], а также в смежных задачах семантического преобразования текста в формальные представления (например, Text-to-SQL) [3, 12], создаёт предпосылки для автоматизации разработки DSL-правил на основе естественно-языковых описаний.

Однако между генерацией кода общего назначения и генерацией программ на DSL существует принципиальное различие. В большинстве практических случаев DSL характеризуется:

1) компактной и строго определённой формальной грамматикой;
2) конечным словарём допустимых идентификаторов;
3) детерминированной семантикой операторов, задаваемой спецификацией системы.

Указанные свойства позволяют формализовать задачу генерации DSL-кода как задачу отображения естественно-языкового описания в программу, удовлетворяющую строгим синтаксическим и семантическим ограничениям. В настоящей работе данная постановка обозначается термином Text2DSL.

Основные вклады настоящей работы заключаются в следующем:

1. Формализована задача Text2DSL как самостоятельный класс задач генерации кода с формальными требованиями синтаксической и семантической корректности.
2. Предложен и описан датасет PolkitBench, содержащий 4 204 верифицированные пары «естественно-языковой запрос – правило Polkit», прошедшие многоуровневую AST-валидацию.

1 Назимов Александр Михайлович, сотрудник Академии Федеральной службы охраны Российской Федерации. Орел, Российская Федерация. E-mail: s-nazim@list.ru

3. Экспериментально показано, что включение структурированного контекста (BNF-грамматика, API-спецификация и словарь допустимых идентификаторов) является критическим фактором качества генерации DSL-кода при использовании предварительно обученных языковых моделей без дополнительного дообучения.

## Постановка задачи Text2DSL

Пусть $Q$ – множество запросов на естественном языке, $G$ – формальная грамматика целевого DSL, $V$ – фиксированный словарь допустимых идентификаторов (API-имена, константы, перечисления). Задача Text2DSL определяется как построение отображения $f: Q \to P_g$, где $P_g$ – множество программ, допустимых грамматикой $G$, такого что для произвольного запроса $q \in Q$ порождённая программа $p = f(q)$ удовлетворяет двум условиям:

1. Синтаксическая корректность: $\mathrm{parse}(p,G) = \mathrm{OK}$, т. е. программа $p$ допускает разбор в абстрактное синтаксическое дерево (AST) согласно грамматике $G$.
2. Семантическая корректность: $\mathrm{ids}(p) \subseteq V$, т.е. все идентификаторы, используемые в $p$, принадлежат словарю $V$.

Таким образом, задача Text2DSL может рассматриваться как частный случай семантического парсинга с жёсткими формальными ограничениями на пространство допустимых программ.

Задача Text2DSL отличается от общей задачи генерации программного кода по следующим причинам:

1. Фиксированная грамматика. Целевой DSL описывается компактной BNF-грамматикой с конечным числом продукций. Для Polkit грамматика содержит около 10 правил, тогда как грамматика языков общего назначения (например Python) включает сотни продукций.
2. Конечный словарь идентификаторов. Множество допустимых идентификаторов заранее известно и ограничено. В случае Polkit $|V| \approx 65$ (категории Systemd, login1, PackageKit, NetworkManager и др.).
3. Детерминированная семантика. Каждый элемент API имеет строго определённую интерпретацию. Например, значение polkit.Result.AUTH_SELF однозначно соответствует требованию аутентификации текущего пользователя и не допускает альтернативных интерпретаций.

## Применение больших языковых моделей для задачи Text2DSL

Современные подходы к генерации кода с использованием БЯМ можно классифицировать следующим образом:

1. Zero-shot generation (генерация без примеров) – модель получает только текстовое описание задачи без примеров или дополнительной информации о целевом языке. Такой подход продемонстрирован на моделях GPT-3, Codex и StarCoder [2].
2. Few-shot prompting (генерация с несколькими примерами) – во входной запрос включается несколько примеров пар «вход – выход» [3, 12]. Подход эффективен для задач с регулярной структурой, однако ограничен размером контекстного окна.
3. Fine-tuning (дообучение) – адаптация модели на целевом корпусе, включая методы LoRA и QLoRA [9, 10]. Требует наличия размеченного набора данных и вычислительных ресурсов.
4. Context injection (включение контекста) – добавление во входной запрос специализированной информации: документации API, грамматики, справочников допустимых значений. Не требует дообучения модели.
5. Retrieval-Augmented Generation (генерация с извлечением информации) – извлечение релевантных фрагментов из базы знаний на этапе применения модели [3, 11].

В отсутствие явной спецификации DSL модель демонстрирует несколько характерных типов ошибок:

- псевдокод вместо DSL – модель порождает текст на естественном языке или декларативные конструкции вместо валидного JavaScript;
- генерация несуществующих элементов API – генерируются несуществующие методы и свойства (response.allow(), polkit.grant(), action.verb и т. д.);
- генерация несуществующих идентификаторов – значения `action.id` незначительно отличаются от реальных: `filesystem-disk-mount` вместо `filesystem-mount`.

Причина: обучающий корпус содержит гетерогенную информацию о множестве API, поэтому модель «восстанавливает» идентификаторы по статистическим закономерностям, не имея полной и непротиворечивой спецификации целевого DSL.

Гипотеза настоящего исследования состоит в том, что для класса задач Text2DSL включение во входной запрос структурированного контекста, содержащего:

- BNF-грамматику целевого DSL ($G$);
- API-спецификацию (допустимые свойства, методы, возвращаемые значения);
- словарь идентификаторов ($V$), является необходимым и достаточным условием для существенного повышения качества генерации без дообучения модели. Контекст выполняет функцию эпистемического ограничения: он задаёт замкнутое пространство допустимых конструкций и запрещает модели использовать знания из обучающего корпуса, не соответствующие спецификации.

С эпистемологической точки зрения данное ограничение можно интерпретировать как введение априорного знания о структуре целевого языка. Большая языковая модель в процессе генерации кода опирается на статистические закономерности обучающего корпуса, которые отражают совокупный опыт программирования на различных языках и использования многочисленных API. В отсутствие явной спецификации модель формирует гипотезы о структуре программы на основе вероятностных ассоциаций, что приводит к появлению синтаксически похожих, но фактически некорректных конструкций.

Включение формальной грамматики и спецификации API в контекст запроса выполняет функцию эпистемического ограничения пространства допустимых гипотез. Модель оказывается ограниченной набором допустимых конструкций, определённых спецификацией DSL, что переводит процесс генерации из режима статистической аппроксимации знаний в режим контекстно-ограниченного вывода. В результате пространство возможных программ существенно сужается, что приводит к росту синтаксической и семантической корректности генерируемого кода.

## Датасет PolkitBench

Целевым языком набора данных является Polkit – подмножество JavaScript (интерпретатор SpiderMonkey), используемое для описания правил авторизации привилегированных операций в Linux. API Polkit включает:

- action.id – строковый идентификатор действия (например, org.freedesktop.login1.reboot);
- subject.user – имя пользователя, запрашивающего авторизацию;
- subject.local, subject.active – булевы признаки локальности и активности сессии;
- subject.isInGroup(name) – метод проверки принадлежности к группе;
- polkit.Result.* – перечисление исходов: YES, NO, AUTH_SELF, AUTH_ADMIN.

Набор данных PolkitBench формируется в три этапа:

1. Шаблонная генерация – 50 шаблонов на русском и английском языках, параметризованных значениями групп, пользователей и действий, дают 5 000 уникальных запросов.
2. Генерация эталонных правил – для каждого запроса БЯМ Grok-4.1-fast (temperature= 0,0) генерирует правило Polkit, используя BNF-грамматику, API-спецификацию и механизм вызова функций.
3. AST – верификация (парсер esprima, 3 уровня): синтаксис → структура (polkit.addRule, параметры, возврат polkit.Result.*) → семантика (валидность свойств action/subject).

   Итого 4 204 валидных пары (84,1 % от 5 000).

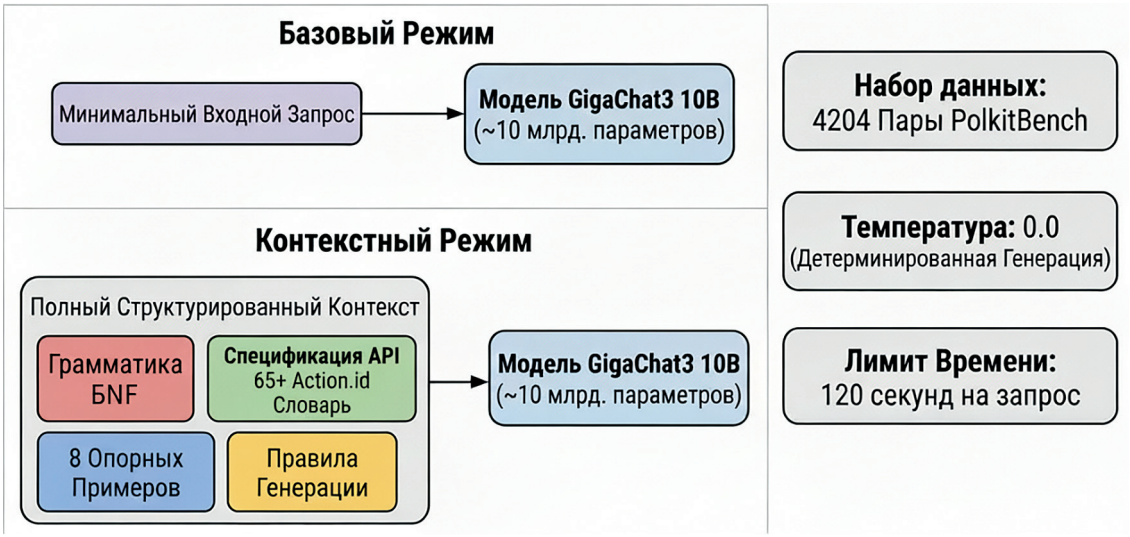



*Рис. 1. Архитектура экспериментальной установки: сравнение базового и контекстного режимов генерации правил Polkit*

## Экспериментальные исследования

Для проверки гипотезы о критической роли структурированного контекста был проведён сравнительный эксперимент в двух режимах генерации: базовом (baseline) и режиме с контекстом (context-enhanced). Схема экспериментальной установки представлена на рисунке 1.

Во всех экспериментах на вход модели подавались текстовые запросы из датасета PolkitBench, представляющие собой описания правил авторизации на естественном языке. Для каждого из 4 204 запросов модель генерировала правило Polkit, которое затем сравнивалось с эталонным правилом из датасета и проходило автоматическую проверку корректности.

Базовый режим (baseline) – модель получает только минимальную инструкцию и текст запроса на естественном языке без дополнительной информации о синтаксисе или API целевого DSL.

Инструкция имеет следующий вид:

*Ты генератор polkit правил для Linux. ФОРМАТ: Верни ТОЛЬКО код polkit правила в блоке ```javascript ... ```*

Режим с контекстом (context-enhanced) – модель получает тот же запрос из датасета PolkitBench, однако дополнительно во входной контекст включается формализованная спецификация целевого DSL.

Контекст содержит:

- BNF-грамматику языка правил Polkit;
- API-спецификацию (допустимые свойства и методы);
- словарь допустимых идентификаторов action.id;
- восемь эталонных примеров корректных правил;
- правила генерации.

Модель получает следующую инструкцию:

*Ты генератор polkit правил. Используй ТОЛЬКО информацию из контекста ниже. НЕ используй свои знания о polkit.*

В эксперименте использовались все 4 204 верифицированные пары из датасета PolkitBench. Каждая пара включает текстовый запрос на естественном языке, описывающий требуемую политику авторизации, и соответствующее эталонное правило Polkit.

На этапе эксперимента в качестве входных данных модели использовались только текстовые запросы из датасета, тогда как эталонные правила применялись исключительно для последующей проверки корректности генерации. Для каждого запроса модель генерировала одно правило Polkit, после чего полученный код автоматически проверялся на синтаксическую и семантическую корректность посредством трёхуровневой AST -валидации.

Генерация выполнялась моделью GigaChat 3 10B при значении параметра temperature = 0,0, что обеспечивает детерминированный режим вывода и исключает стохастические вариации между запусками. Для каждого запроса устанавливалось ограничение времени генерации, равное 120 секундам.

Параметры эксперимента:

- модель: GigaChat 3 10B;
- набор данных: все 4 204 пары из PolkitBench;
- temperature: 0,0 (детерминированная генерация);
- ограничение по времени: 120 секунд на запрос.

Между условиями варьировалась только одна независимая переменная – наличие или отсутствие структурированного контекста во входном запросе.

В базовом режиме 19,5 % сгенерированных программ содержат синтаксические ошибки JavaScript. Для выявления причин возникновения этих ошибок был проведён качественный анализ некорректно сгенерированных правил Polkit. Анализ показал, что большинство ошибок связано с отсутствием у модели явного представления о синтаксисе и API целевого DSL, вследствие чего модель воспроизводит конструкции, статистически похожие на правила управления доступом, но не соответствующие реальной спецификации языка Polkit. По результатам анализа ошибки можно разделить на три основных подкласса.

1. Генерация псевдокода – модель порождает декларативные конструкции (allow {user = root;}) вместо императивного JavaScript.
2. Неверная структура – отсутствует обязательный вызов polkit.addRule() или некорректный формат callback-функции.

*Таблица 1.*

*Сравнение условий Baseline и Context – enhanced (N = 4204)*

| Метрика | Базовый режим | С контекстом | Δ, % |
|---|---|---|---|
| Синтаксическая корректность | 80,5 % (3386) | 99,4 % (4178) | +23,4 % |
| Семантическая корректность | 60,4 % (2540) | 95,9 % (4031) | +58,7 % |

3. Некорректные возвращаемые значения – вместо polkit.Result.YES модель генерирует polkit.Result.Denied, response.allow() и иные несуществующие конструкции.

Включение структурированного контекста практически полностью устраняет синтаксические ошибки: синтаксическая корректность достигает 99,4 %. Остаточные 0,6 % ошибок обусловлены превышением ограничения по времени и граничными случаями с вложенными условиями.

## Обсуждение полученных результатов

Полученные результаты подтверждают гипотезу о критической роли структурированного контекста для задачи Text2DSL. Прирост семантической корректности на 58,7 % демонстрирует, что без явного задания спецификации модель не располагает достаточными сведениями о целевом DSL и подменяет его синтаксис конструкциями из обучающего корпуса (декларативный псевдокод, конструкции SELinux, собственные построения). Существенный рост точности воспроизведения строковых идентификаторов свидетельствует, что словарь $V$ в контексте переключает модель от генерации произвольных идентификаторов к выбору из заранее определённого перечня допустимых значений.

К ограничениям подхода относятся следующие:

1. Необходимость формальной спецификации. Метод включения контекста работает только при наличии BNF-грамматики и словаря $V$. Для DSL без формальной документации построение контекста представляет нетривиальную задачу.
2. Масштабируемость словаря. В эксперименте $|V| \approx 65$. При $|V| > 10^3$ (например, для SELinux type enforcement) контекст может превысить допустимый размер контекстного окна модели. В таких случаях необходим гибридный подход (RAG + context injection).
3. Одна модель. Эксперимент проведён на единственной модели (~10B параметров). Для обобщения результатов необходимо исследование на моделях различного масштаба.
4. Остаточные галлюцинации. Даже при наличии контекста модель генерирует 1 413 невалидных action.id, что указывает на необходимость дополнительных механизмов (постобработка, grammar–constrained decoding [7, 11]).

## Выводы

В настоящей работе формализована задача Text2DSL – автоматической генерации кода предметно-ориентированных языков по описанию на естественном языке – как самостоятельный класс задач генерации кода. Определены формальные требования синтаксической и семантической корректности, предложена система метрик (синтаксическая и семантическая корректность).

Представлен набор данных PolkitBench, содержащий 4 204 верифицированные пары «запрос – правило Polkit», прошедших трёхуровневую AST-валидацию.

Проведённый эксперимент показал, что включение структурированного контекста (BNF-грамматика, API-спецификация, словарь идентификаторов) во входной запрос БЯМ повышает синтаксическую корректность генерации с 80,5 % до 99,4 % (+23,4 %), семантическую корректность – с 60,4 % до 95,9 % (+58,7 %). Результаты демонстрируют, что для задач Text2DSL включение формальной спецификации целевого языка является ключевым фактором качества генерации, позволяющим достичь высоких показателей без дообучения модели.

В дальнейшем планируется: дообучение модели на PolkitBench (LoRA/QLoRA) для снижения числа ошибок; применение декодирования с грамматическими ограничениями для гарантии синтаксически корректного кода.

## Литература


1. Rozière B., Gehring J., Gloeckle F., et al. Code Llama: Open Foundation Models for Code // arXiv. – 2023. – DOI: 10.48550/arXiv.2308.12950.
2. Li R., Allal L. B., Zi Y., et al. StarCoder: May the Source Be with You! // Transactions on Machine Learning Research. – 2023. – DOI: 10.48550/arXiv.2305.06161.
3. Zan D., Chen B., Zhang F., Lu D., Wu B., Guan B., Wang Y., Lou J.-G. Large Language Models Meet NL2Code: A Survey // Proceedings of the 61st Annual Meeting of the Association for Computational Linguistics (ACL). – 2023. – P. 7443–7464. – DOI: 10.18653/v1/2023.acl-long.411.
4. Austin J., Odena A., Nye M., et al. Program Synthesis with Large Language Models // arXiv. – 2021. – DOI: 10.48550/arXiv.2108.07732.
5. Wang Y., Wang W., Joty S. CodeT5: Identifier-Aware Unified Pre-trained Encoder-Decoder Models for Code Understanding and Generation // Proceedings of the Conference on Empirical Methods in Natural Language Processing (EMNLP). – 2021. – DOI: 10.18653/v1/2021.emnlp-main.685.
6. Guo D., Ren S., Lu S., et al. GraphCodeBERT: Pre-training Code Representations with Data Flow // International Conference on Learning Representations (ICLR). – 2021. – DOI: 10.48550/arXiv.2009.08366.

7. Scholak T., Schucher N., Bahdanau D. PICARD: Parsing Incrementally for Constrained Auto-Regressive Decoding from Language Models // Proceedings of the Conference on Empirical Methods in Natural Language Processing (EMNLP). – 2021. – DOI: 10.18653/v1/2021.emnlp-main.779.
8. Hu E. J., Shen Y., Wallis P., et al. LoRA: Low-Rank Adaptation of Large Language Models // International Conference on Learning Representations (ICLR). – 2022. – DOI: 10.48550/arXiv.2106.09685.
9. Dettmers T., Pagnoni A., Holtzman A., Zettlemoyer L. QLoRA: Efficient Finetuning of Quantized Large Language Models // Advances in Neural Information Processing Systems (NeurIPS). – 2023. – DOI: 10.48550/arXiv.2305.14314.
10. Chen X., Lin Y., Schürmann C. Neural Code Generation with Grammar Constraints // International Conference on Learning Representations (ICLR). – 2021. – DOI: 10.48550/arXiv.2010.00904.
11. Zhong R., Yin P., Yu T., et al. Semantic Parsing for Code Generation: A Survey // Findings of the Association for Computational Linguistics (ACL Findings). – 2022. – DOI: 10.18653/v1/2022.findings-acl.2.
12. Yin P., Neubig G. StructCoder: Structure-Aware Code Generation with Language Models // Proceedings of the Annual Meeting of the Association for Computational Linguistics (ACL). – 2022. – DOI: 10.18653/v1/2022.acl-long.39.
13. Barke S., James M., Polikarpova N. Grounded Copilot: How Programmers Interact with Code-Generating Models // Proceedings of the International Conference on Software Engineering (ICSE). – 2023. – DOI: 10.1109/ICSE48619.2023.00015.
14. Pourreza M., Rafiei D. DIN-SQL: Decomposed In-Context Learning of Text-to-SQL with Self-Correction // Advances in Neural Information Processing Systems (NeurIPS). – 2023. – DOI: 10.48550/arXiv.2304.11015.

# THE PROBLEM OF CODE GENERATING DOMAIN-SPECIFIC LANGUAGES USING LARGE LANGUAGE MODELS (USING POLKIT AS AN EXAMPLE)

***Nazimov A. M.*[2]**

***Keywords:*** *large language models, Polkit, Text2DSL, structured context, program validation.*

***Abstract***

***Purpose of the study:*** *to formalize the task of automatic generation of domain-specific language (DSL) code from natural language descriptions – referred to as Text2DSL – as an independent class of code generation problems, and to empirically evaluate the role of structured context in DSL code generation by a large language model.*

***Methods of research:*** *the study is based on an experimental evaluation conducted under two conditions (baseline mode and context-enhanced mode) using the PolkitBench dataset, which contains 4,204 verified pairs of natural language requests and corresponding Polkit rules. A three-level AST validation procedure based on the esprima parser was employed, along with quantitative metrics of syntactic and semantic correctness.*

***Results:*** *the inclusion of structured context (BNF grammar, API specification, and a dictionary of valid identifiers) increases syntactic correctness from 80.5 % to 99.4 % (+23.4 %) and semantic correctness from 60.4 % to 95.9 % (+58.7 %). The results demonstrate that for the class of Text2DSL tasks, incorporating the formal specification of the target language into the prompt context constitutes a necessary and sufficient condition for achieving high-quality DSL code generation without additional model fine-tuning.*

***Scientific novelty:*** *the study formalizes the Text2DSL problem as a distinct class of code generation tasks; introduces the PolkitBench dataset consisting of 4,204 verified pairs validated through a three-level AST analysis; and provides empirical evidence of the critical role of structured context in enabling accurate DSL code generation by large language models.*

## References

1. Rozière B., Gehring J., Gloeckle F., et al. Code Llama: Open Foundation Models for Code // arXiv. – 2023. – DOI: 10.48550/arXiv.2308.12950.
2. Li R., Allal L. B., Zi Y., et al. StarCoder: May the Source Be with You! // Transactions on Machine Learning Research. – 2023. – DOI: 10.48550/arXiv.2305.06161.
3. Zan D., Chen B., Zhang F., Lu D., Wu B., Guan B., Wang Y., Lou J.-G. Large Language Models Meet NL2Code: A Survey // Proceedings of the 61st Annual Meeting of the Association for Computational Linguistics (ACL). – 2023. – P. 7443–7464. – DOI: 10.18653/v1/2023.acl-long.411.
4. Austin J., Odena A., Nye M., et al. Program Synthesis with Large Language Models // arXiv. – 2021. – DOI: 10.48550/arXiv.2108.07732.
5. Wang Y., Wang W., Joty S. CodeT5: Identifier-Aware Unified Pre-trained Encoder-Decoder Models for Code Understanding and Generation // Proceedings of the Conference on Empirical Methods in Natural Language Processing (EMNLP). – 2021. – DOI: 10.18653/v1/2021.emnlp-main.685.

2 Alexandr M. Nazimov, Academy of the Federal Security Service of the Russian Federation. Orel, Russian Federation. E-mail: s-nazim@list.ru

6. Guo D., Ren S., Lu S., et al. GraphCodeBERT: Pre-training Code Representations with Data Flow // International Conference on Learning Representations (ICLR). – 2021. – DOI: 10.48550/arXiv.2009.08366.
7. Scholak T., Schucher N., Bahdanau D. PICARD: Parsing Incrementally for Constrained Auto-Regressive Decoding from Language Models // Proceedings of the Conference on Empirical Methods in Natural Language Processing (EMNLP). – 2021. – DOI: 10.18653/v1/2021.emnlp-main.779.
8. Hu E. J., Shen Y., Wallis P., et al. LoRA: Low-Rank Adaptation of Large Language Models // International Conference on Learning Representations (ICLR). – 2022. – DOI: 10.48550/arXiv.2106.09685.
9. Dettmers T., Pagnoni A., Holtzman A., Zettlemoyer L. QLoRA: Efficient Finetuning of Quantized Large Language Models // Advances in Neural Information Processing Systems (NeurIPS). – 2023. – DOI: 10.48550/arXiv.2305.14314.
10. Chen X., Lin Y., Schürmann C. Neural Code Generation with Grammar Constraints // International Conference on Learning Representations (ICLR). – 2021. – DOI: 10.48550/arXiv.2010.00904.
11. Zhong R., Yin P., Yu T., et al. Semantic Parsing for Code Generation: A Survey // Findings of the Association for Computational Linguistics (ACL Findings). – 2022. – DOI: 10.18653/v1/2022.findings-acl.2.
12. Yin P., Neubig G. StructCoder: Structure-Aware Code Generation with Language Models // Proceedings of the Annual Meeting of the Association for Computational Linguistics (ACL). – 2022. – DOI: 10.18653/v1/2022.acl-long.39.
13. Barke S., James M., Polikarpova N. Grounded Copilot: How Programmers Interact with Code-Generating Models // Proceedings of the International Conference on Software Engineering (ICSE). – 2023. – DOI: 10.1109/ICSE48619.2023.00015.
14. Pourreza M., Rafiei D. DIN-SQL: Decomposed In-Context Learning of Text-to-SQL with Self-Correction // Advances in Neural Information Processing Systems (NeurIPS). – 2023. – DOI: 10.48550/arXiv.2304.11015.

# СТРУКТУРНЫЙ ПОДХОД К СТАТИЧЕСКОМУ АНАЛИЗУ ФАЙЛОВ ФОРМАТА ELF ДЛЯ ОБНАРУЖЕНИЯ ВРЕДОНОСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

***Матовых С. С.***[1]

**DOI:10.21681/3034-4050-2026-2-50-57**

***Ключевые слова:*** *структурная модель, машинное обучение, классификация вредоносного программного обеспечения, файлы формата ELF, операционная система Linux, статический анализ исполняемых файлов.*

***Аннотация***

***Цель исследования:*** *разработать и экспериментально проверить интерпретируемую структурную модель статического анализа ELF-файлов для выявления вредоносного программного обеспечения без выполнения кода.*

***Метод исследования:*** *применены методы статического анализа структуры ELF-файлов и формализация признаков в виде бинарного вектора индикаторов. Классификация выполнена методами машинного обучения с перекрёстной проверкой и сравнением нескольких алгоритмов на едином признаковом пространстве.*

***Результат исследования:*** *сформировано пространство из 63 бинарных структурных индикаторов, охватывающих подсистемы управления памятью, процессов, сетевого взаимодействия, файловых операций, привилегий, механизмов противодействия анализу и упаковки. Проведён сравнительный эксперимент на сбалансированной выборке ELF-файлов, включающей легитимные и вредоносные файлы. Показано, что ансамблевые методы обеспечивают наилучший баланс метрик качества, для модели Random Forest получены следующие результаты Accuracy 0,874, F1-мера 0,860, что подтверждает практическую применимость предложенной модели в задачах раннего статического выявления угроз.*

***Научная новизна:*** *предложена интерпретируемая подсистемная организация индикаторов, повышающая объяснимость решения и пригодность модели для мультиархитектурных сценариев анализа ELF-объектов.*

## Введение

Обнаружение вредоносного программного обеспечения (ВПО) в исполняемых файлах формата ELF (Executable and Linkable Format) является критически важной задачей для защиты серверов, встраиваемых систем и IoT-устройств на базе Linux. Актуальность усиливается эволюцией угроз в сторону малозаметных и устойчивых к анализу образцов, например, OrBit использует перехват потока выполнения через механизмы разделяемых библиотек и ориентирован на долговременное скрытное присутствие в системе [1].

Классические сигнатурные средства обнаружения в таких условиях сталкиваются с принципиальными ограничениями. Во-первых, развитие полиморфных и метаморфных техник порождает большое число вариантов одного и того же семейства, что снижает точность обнаружения на основе сигнатур и увеличивает длительность обновления баз [2]. Во-вторых, упаковка и обфускация искажают наблюдаемые статические признаки и могут существенно ухудшать качество обнаружения ВПО, что требует учитывать фактор упаковки как отдельный источник ошибок классификации [3].

В этих условиях закономерно смещение фокуса к развитию методов анализа ELF-файлов по извлечению информативных признаков из структуры и метаданных без выполнения кода с последующей классификацией методами машинного обучения. Такой подход позволяет опираться не на один совпадающий признак, а на совокупность устойчивых структурных характеристик и их комбинаций, что делает обнаружение более пригодным для выявления ранее неизвестных вариантов при заданных ограничениях по времени анализа [4].

Подходы на основе машинного обучения уже продемонстрировали высокую эффективность при статическом обнаружении ВПО в файлах формата Portable Executable (PE-файлы). Появление открытого датасета EMBER сделало возможным воспроизводимое сравнение моделей и показало, что даже относительно простые алгоритмы на инженерных признаках могут достигать высоких показателей качества на задачах детектирования [5]. Обобщающие обзоры по обнаружению ВПО также выделяют устойчивую тенденцию к развитию различных методов анализа, опирающийся на признаки структуры файла, способные выявлять скрытые

1 Матовых Сергей Сергеевич, сотрудник Федерального государственного казённого военного образовательного учреждения высшего образования «Академия Федеральной службы охраны Российской Федерации». Орёл, Россия. E-mail: coolt88@gmail.com

закономерности и обеспечивать высокую обобщающую способность по сравнению с чисто сигнатурными механизмами, особенно в условиях роста вариативности образцов [6]. Параллельно развивается линия, в которой модели обучаются непосредственно на сыром байтовом представлении исполняемого файла, что расширяет класс используемых закономерностей и подтверждает потенциал нейросетевых подходов [7].

Однако основная масса работ исторически сосредоточена на формате PE, тогда как ELF-файлы до недавнего времени изучались заметно меньше. В последние годы ситуация меняется и появляются исследования, предлагающие извлекать признаки из ELF-структуры и статически аппроксимировать поведенческие маркеры с последующей классификацией, в том числе применительно к мультиархитектурным выборкам [8–9]. При этом сохраняется методический разрыв, где остаётся открытым вопрос переносимости и масштабируемости тех принципов статического моделирования, которые хорошо зарекомендовали себя на анализ ELF-файлов с учётом отличий в компоновке, секциях, таблицах и механизмах динамической линковки.

В настоящей работе в качестве методической основы такого переноса используется ранее разработанная и экспериментально обоснованная структурная модель PE-файлов, содержащих вредоносный код, в которой объект анализа трактуется как система взаимосвязанных компонент, отображаемая в интерпретируемое пространство признаков [10]. Цель исследования состоит в разработке и экспериментальной проверке структурной модели ELF-файлов для выявления ВПО, где под моделью понимается совокупность статических индикаторов, извлекаемых из внутренней структуры и содержимого ELF-контейнера без выполнения кода, с последующей классификацией методами машинного обучения. Предлагается набор из 63 бинарных индикаторов, охватывающих признаки, связанные с потенциально вредоносными паттернами (операции с памятью и процессами, сеть, файловая система, привилегии, закрепление, противодействие анализу и упаковка). Приоритет интерпретируемости заложен в конструкцию модели и каждый индикатор имеет однозначный семантический смысл, что согласуется с общей линией развития объяснимого машинного обучения [11]. Далее приводится описание набора признаков и алгоритма классификации, результаты экспериментов на наборе ELF-файлов и выводы о переносимости подходов статического анализа.

## Модель и методология

Набор индикаторов M01–M63 задаёт бинарный профиль файла $X \in \{0,1\}^{63}$, где каждый признак фиксирует наличие наблюдаемого артефакта в контейнере ELF. Важно подчеркнуть: речь идёт не о «поведении» в динамическом смысле, а о структурно наблюдаемых следах, которые можно извлечь без исполнения кода. Источниками таких следов выступают формальные элементы ELF, такие как Program Header Table (PHT) и права сегментов PT_LOAD, Section Header Table (SHT), динамический раздел PT_DYNAMIC/.dynamic, таблицы .dynsym/.dynstr и релокации PLT/GOT, а также строковые константы и статистические профили секций/сегментов.

*Таблица 1.*

*Распределение индикаторов по подсистемам ELF-контейнера*

| Подсистема | Индикаторы | Что именно фиксируется в контейнере |
|---|---|---|
| MEM | M01–M10 | Аномалии прав/разметки исполняемых областей и следы динамической работы с памятью (RWX, mmap/mprotect, dlopen/dlsym и др.) |
| PROC | M11–M18, M61 | Контур исполнения: порождение процессов, демонизация, запуск команд/внешних программ (exec*, fork/clone, system и др.) |
| NET | M19–M30, M62 | Сетевой слой: достаточный набор для C2/обмена данными (socket/connect/send/recv, DNS, event-loop, TLS) |
| FS | M31–M42, M63 | Файловые операции: развёртывание на диск, подмена/зачистка, манипуляции метаданными, низкоуровневые ioctl и др. |
| PRIV | M43–M46 | Манипуляции привилегиями и capabilities (setuid/setgid/capset и аналоги) |
| PERS | M47–M48 | Закрепление и обращения к чувствительным точкам ОС (/etc/passwd, cron и др.) |
| ANTI | M49–M56 | Противодействие анализу: ptrace/TracerPid, /proc/*/status, VM/sandbox-строки, LD_PRELOAD и др. |
| PACK | M57–M60 | Упаковка/обфускация: высокая энтропия PT_LOAD, stripped-профиль, UPX-подобные секции и маркеры |

Чтобы признаки не превращались в набор разрозненных флагов, индикаторы M01–M63 заранее организованы в подсистемы. Это принципиально важно для интерпретации решений классификатора и диагностического анализа ошибок. Распределение индикаторов по подсистемам приведено в таблице 1.

Подсистема Mem отражает признаки, связанные с организацией исполняемых областей и управлением памятью. Здесь есть два структурных слоя. Первый сегментный слой по PHT проверяется наличие загружаемых сегментов PT_Load с правами записи и исполнения одновременно. Для прикладного ПО это обычно нетипичная конфигурация контейнера, вместе с тем во вредоносных цепочках подобная разметка встречается существенно чаще, поэтому она включается как риск-маркер. Второй слой механистический по .dynamic, .dynsym/.dynstr и по PLT-релокациям фиксируются обращения к механизмам mmap/mprotect, а также к dlopen/dlsym. Эти маркеры не являются доказательством вредоносности сами по себе, но в совокупности с признаками упаковки и антианализа дают хорошо интерпретируемый сигнал: файл способен динамически формировать исполняемую память или подгружать код во время работы [12].

Proc-индикаторы описывают контур исполнения, такой как порождение процессов и запуск внешних программ/команд. Статически это наблюдается через импортируемые символы и релокации, через .dynsym/.dynstr и Plt/Got. Отдельно полезны составные шаблоны, вроде комбинации fork/vfork/clone с execve или system. Такой паттерн не обнаруживает ВПО, но фиксирует характерную для загрузчиков и дропперов схему отделения процесса и передачи управления полезной нагрузке именно как структурно наблюдаемый факт наличия соответствующих механизмов.

Net-группа формируется по наличию импортов функций сетевого стека (socket, connect, send, recv и др.) и их комбинаций. Составной шаблон удобно трактовать как признак того, что исследуемый файл содержит минимально достаточный набор механизмов для исходящего соединения и обмена данными. В контуре IoT-вредоноса подобная функциональность действительно является типовой частью жизненного цикла (управление, участие в ботнете, доставочные сценарии), что хорошо показано на крупных исследованиях IoT-ботнетов и на работах по кросс-архитектурному threat hunting [13]. При этом в статье корректно оговаривать доменную специфику для легитимных сетевых утилит и сервисов такие импорты ожидаемы, поэтому диагностическая сила Net повышается именно при совместном присутствии Proc/FS/Anti/Pack.

FS-индикаторы фиксируют операции создания/изменения файлов, удаления, переименования и смены прав. Структурно они извлекаются так же, как Proc/Net через динамические символы и релокации. Наиболее информативны здесь не одиночные функции, а цепочки, описывающие типовые сценарии доставки и активации создать/открыть, записать, сделать исполняемым. Именно такой подход к статическим признакам хорошо ложится на практику анализа ВПО формата ELF.

Признаки Priv/Pers (привилегии/закрепление) намеренно сделаны интерпретируемыми по импорту функций изменения Uid/Gid (setuid, setgid, setresuid) фиксируется потенциальная возможность манипулировать привилегиями, а по строковым маркерам обращение к типовым точкам закрепления (например, crontab, /etc/passwd). Такие признаки лучше всего работают как контекстные в отдельности они могут встречаться в системном ПО, но в композиции с сетевыми и файловыми цепочками дают содержательную картину возможного сценария вредоносной активности.

Anti-группа включает как маркеры (например, импорт ptrace), так и строковые признаки окружения (TracerPid, упоминания гипервизоров). Важно, что подобные проверки встречаются не только у ВПО, однако современные исследования показывают, что анти-отладочные признаки и обнаружение исследовательского окружения устойчивый класс приёмов, особенно в Linux, где злоумышленники ориентируются на затруднение статического и инструментального анализа [14]. Поэтому Anti-признаки логично включаются как отдельная подсистема и учитываются совместно с Pack/Mem/Net.

Pack-индикаторы опираются на две вещи, статистику содержимого и правильность компоновки. Энтропия секций/сегментов – классическая эвристика для выявления сжатия и шифрования, но в литературе подчёркивается, что упаковка бывает многослойной и не всегда сводится к высокой энтропии, поэтому правильная постановка использовать энтропию как вероятностный сигнал и усиливать его структурными маркерами (strip-профиль, характерные секции/паттерны) [15]. Для практики важно, что Pack-индикаторы не «решают задачу за модель», а повышают устойчивость детектора к обфускации.

Каждый из описанных индикаторов представляет булев признак (присутствует или отсутствует).

Таким образом, профиль из 63 признаков для каждого файла фиксирует набор обнаруженных подозрительных индикаторов. Важным преимуществом такого подхода является архитектурная независимость, где многие признаки (импорты функций, строки, энтропия и т.д.) не зависят от конкретной аппаратной архитектуры CPU, что особенно ценно для анализа IoT-файлов, распространяющегося на множестве платформ. В отличие от низкоуровневых признаков (opcode, n-grams и т.д.), структурные индикаторы легко интерпретируются экспертами и непосредственно указывают на известные вредоносные техники. Практическая реализация извлечения признаков базируется на существующих инструментах статического анализа ELF (библиотеки LIEF, утилиты readELF/objdump). Это позволяет автоматизировать получение всех 63 индикаторов из каждого файла перед классификацией. Группировка индикаторов по подсистемам облегчает последующую интерпретацию решения классификатора и согласуется с линией исследований в задачах классификации ВПО формата ELF.

## Экспериментальная часть

Для оценки предложенной структурной модели сформирован датасет ELF-файлов двух классов. Ввиду ограниченности публично доступных и воспроизводимо размеченных выборок ВПО файлов формата ELF для экспериментов подготовлен собственный набор объёмом порядка 3000 объектов, где 1500 легитимных ELF-файлов из стандартных дистрибутивов Linux (служебные утилиты и библиотеки) и около 1500 вредоносных ELF-файлов взятых с ресурса vx-underground.org, собранных из исследовательской коллекции Malvare Bazaar декабря 2025 года содержащего различные семейства ВПО. Выборка сбалансирована по классам, что облегчает интерпретацию метрик качества и матрицы ошибок.

Для каждого файла автоматически извлекался полный набор из 63 бинарных индикаторов M01–M63 с использованием разработанного парсера, формируя вектор признаков $X \in \{0,1\}^{63}$. Далее были обучены и сопоставлены несколько алгоритмов классификации на одном и том же признаковом пространстве XGBoost, LightGBM, Random Forest, Gradient Boosting, SVM с RBF-ядром, логистическая регрессия, Decision Tree, Naive Bayes и kNN. Датасет разделялся на обучающую и тестовую части в соотношении 80/20, подбор гиперпараметров выполнялся на обучающей части с применением перекрёстной проверки (k-fold cross-validation). По результатам сравнительного эксперимента таблица № 2 в качестве основной модели для последующего анализа выбран Random Forest – как алгоритм, обеспечивший наилучшие значения F1-меры и Accuracy в рассматриваемом наборе моделей.

Для выбранного классификатора Random Forest дополнительно рассмотрена матрица ошибок на тестовой выборке рисунок 1. Модель правильно классифицировала 523 из 598 файлов Accuracy 0,874. При этом из 301 легитимного файла 9 были ошибочно помечены как вредоносные (FP), тогда как 292 распознаны верно (TN). Одновременно из 297 вредоносных образцов детектировано 231 (TP), а 66 были ошибочно отнесены к классу легитимных (FN).

Полученные результаты подчёркивают практическую направленность детектора Precision 0,963 указывает на низкую долю ложных срабатываний, что критично для эксплуатационного применения, тогда как Recall 0,777 фиксирует, что часть ВПО всё ещё остаётся невыявленной с текущим набором статических индикаторов. Значимая часть пропусков в данном исследовании относится к различным вариантам

*Таблица 2.*

*Сравнение алгоритмов классификации на ELF-признаках*

| Model | Accuracy | Precision | Recall | F1 |
|---|---|---|---|---|
| XGBoost | 0,873 | 0,963 | 0,774 | 0,858 |
| LightGBM | 0,872 | 0,964 | 0,772 | 0,857 |
| Random Forest | 0,874 | 0,963 | 0,777 | 0,860 |
| Gradient Boosting | 0,866 | 0,955 | 0,767 | 0,850 |
| Logistic Regression | 0,860 | 0,941 | 0,766 | 0,844 |
| SVM | 0,861 | 0,972 | 0,758 | 0,851 |
| Decision Tree | 0,861 | 0,950 | 0,760 | 0,844 |
| Naive Bayes | 0,787 | 0,826 | 0,805 | 0,798 |
| KNN | 0,812 | 0,957 | 0,650 | 0,774 |

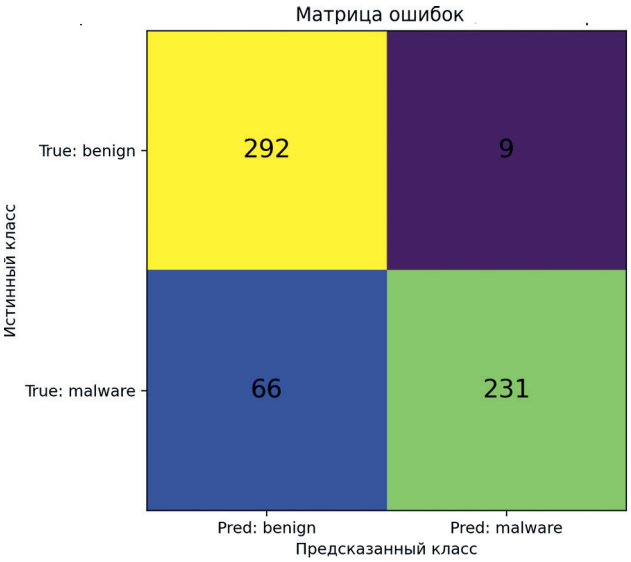



*Рис. 1. Матрица ошибок для классификатора Random Forest*

семейства Linux.Mirai и его производным, что отражает высокую вариативность данного ВПО. Различия сборок, архитектур и приёмов маскировки приводят к ослаблению или неуверенности в части структурных маркеров, на которых основано признаковое описание. Такая картина согласуется с общими выводами о том, что упаковка и обфускация способны снижать эффективность статического детектирования и требуют либо расширения статического признакового описания, либо введения дополнительных этапов анализа.

Для корректной интерпретации таких результатов классификатора необходимо перейти от сводных метрик к анализу механизма принятия решения какие именно структурные индикаторы оказываются наиболее значимыми

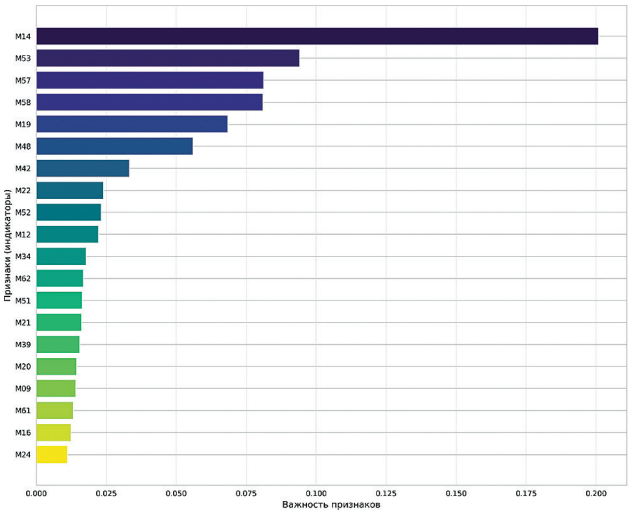



*Рис. 2. Важность признаков модели Random Forest*

для различения классов. В связи с этим далее приводится распределение важности признаков в модели Random Forest на рисунке 2 показана диаграмма важности, позволяющая визуально оценить вклад.

График важности признаков показывает, что вклад распределён неравномерно небольшая группа индикаторов формирует основную часть дискриминирующего сигнала, тогда как остальные признаки выполняют уточняющую функцию. Для точного представления состава ведущих индикаторов приведём десять признаков с наибольшими значениями важности в таблице 3.

*Таблица 3.*
*Наиболее значимые индикаторы по важности*

| Индикатор | Подсистема | Важность |
|---|---|---|
| M14 (system) | PROC | 0,201 |
| M53 (CPUID present) | ANTI | 0,094 |
| M57 (High entropy PT_LOAD) | PACK | 0,081 |
| M58 (Stripped + entropy) | PACK | 0,081 |
| M19 (socket) | NET | 0,068 |
| M48 (cron persistence) | PERS | 0,056 |
| M42 (ioctl) | FS | 0,033 |
| M22 (recv/recvfrom) | NET | 0,024 |
| M52 (LD_PRELOAD/ LD_LIBRARY_PATH) | ANTI | 0,023 |
| M12 (fork/vfork) | PROC | 0,022 |

Анализ результатов важности признаков позволяет перейти от формального ранжирования к содержательной интерпретации вклада индикаторов.

Наибольший вклад в различение классов формирует индикатор M14 (system) подсистемы PROC. Его значимость объясняется тем, что наличие механизма выполнения команд оболочки характерно для сценариев удалённого управления, запуска вспомогательных компонентов и активации полезной нагрузки. В рассматриваемой выборке данный признак выступает наиболее сильным разделяющим фактором.

Значимый вклад вносят признаки подсистемы PACK – M57 и M58. Они отражают повышенную энтропию загружаемых сегментов и сочетание энтропии с отсутствием таблицы символов. Это указывает на статистико-структурные признаки упаковки или обфускации. Таким образом, модель учитывает не только функциональные возможности файла, но и особенности его компоновки.

Индикаторы подсистемы ANTI (M53 и M52) также входят в число наиболее значимых. Их вклад связан с фиксацией признаков противодействия анализу и проверки окружения выполнения. Наличие подобных маркеров усиливает различение классов, особенно в сочетании с процессными и упаковочными признаками.

Сетевые индикаторы M19 (socket) и M22 (recv/recvfrom) формируют дополнительный вклад, отражая наличие коммуникационного контура. Однако сами по себе сетевые импорты встречаются и в легитимном программном обеспечении, поэтому их диагностическая сила проявляется преимущественно в комбинации с индикаторами PROC, PACK и ANTI.

Признак закрепления M48 (cron persistence) и файловый индикатор M42 (ioctl) вносят меньший, но статистически значимый вклад, уточняя решение классификатора в случаях, когда вредоносный сценарий включает элементы закрепления или низкоуровневые операции.

Таким образом, анализ важности признаков показывает, что основное качество классификации обеспечивается индикаторами подсистем PROC, PACK и ANTI, тогда как признаки подсистем NET, PERS и FS выполняют усиливающую и уточняющую функцию. Следовательно, модель различает классы не по отдельному эвристическому маркеру, а по совокупности структурных признаков, отражающих механизмы выполнения команд, маскировки, противодействия анализу и сетевого взаимодействия. Именно согласованность этих подсистем формирует устойчивый дискриминирующий профиль вредоносных ELF-объектов в рамках рассматриваемого датасета.

## Обсуждение и выводы

Показано, что для задачи обнаружения вредоносного программного обеспечения, распространяемого в виде ELF-файлов, может быть построена компактная интерпретируемая модель статического анализа, опирающаяся не на единичный высокоинформативный маркер, а на согласованную совокупность структурных сигналов контейнера ELF и связанных с ним метаданных. Предложенный набор из 63 бинарных индикаторов формирует воспроизводимое признаковое представление ELF-объекта, достаточное для обучения классификаторов без выполнения кода и допускающее содержательное объяснение решения как на уровне отдельных признаков, так и на уровне подсистем признакового пространства.

Экспериментальная проверка на сформированном датасете объёмом порядка 3000 ELF-файлов показала, что на данном признаковом пространстве наилучший баланс метрик обеспечивают ансамблевые методы. Среди протестированных алгоритмов наилучшие значения качества продемонстрировал Random Forest (*Accuracy* = 0,874; *Precision* = 0,963; *Recall* = 0,777; *F1* = 0,860), что соответствует режиму высокой точности положительных решений при наличии пропусков части вредоносных объектов. Прикладная мотивация данного режима состоит в приоритете минимизации ложных срабатываний, поскольку ошибочная блокировка легитимных файлов в типовых сценариях применения является более критичной, чем пропуск части вредоносных объектов.

Анализ ошибок указывает, что основное ограничение подхода связано не с выбором конкретного классификатора, а с неполнотой текущего признакового покрытия для отдельных групп ELF-ВПО. В частности, среди пропущенных образцов присутствуют модификации семейства Linux.Mirai и близкие варианты, для которых вариативность сборок, различия целевых архитектур и приёмы маскировки приводят к ослаблению выраженности используемых статических маркеров. Следовательно, набор из 63 индикаторов достаточен для надёжного выделения значимой доли угроз при минимизации ложноположительных результатов, однако недостаточен для достижения полноты обнаружения, близкой к 1, на широком спектре современных ELF-семейств.

Дальнейшее развитие подхода целесообразно связывать с расширением структурного признакового пространства в тех подсистемах, где проявляются пропуски, а также с расширением и стратификацией датасета по семействам и архитектурам. В прикладном плане предложенная модель уже в текущем виде может рассматриваться как быстрый статический компонент раннего выявления ELF-ВПО с последующим направлением неоднозначных объектов на углублённые процедуры проверки.

## Литература

1. Louis D. Advanced analysis of a Linux-dedicated malware (OrBit) [Электронный ресурс]. – URL:www.stormshield.com/news/orbit-analysis-of-a-linux-dedicated-malware. – (дата обращения: 30.01.2026).
2. Sharma A., Sahay S. Evolution and Detection of Polymorphic and Metamorphic Malware: A Survey. – 2014. – https://doi.org/10.5120/15544-4098.

3. Daniel G., et al.: Assessing the Impact of Packing on Machine Learning Based Malware Detection Systems. – 2024. – https://doi.org/10.1016/j.cose.2025.104495.
4. Ramamoorthy J., et al. A Novel Static Analysis Approach Using System Calls for IoT Malware Detection // Electronics. – 2024. – Vol. 13, No. 15. – Article 2906. https://doi.org/10.3390/electronics13152906.
5. Anderson H. S., Roth P. EMBER: An Open Dataset for Training Static PE Malware Machine Learning Models // arXiv. – 2018. – https://doi.org/10.48550/arXiv.1804.04637.
6. Ucci D., Aniello L., Baldoni R. Survey of Machine Learning Techniques for Malware Analysis // Computers & Security. – 2019. – Vol. 81. – P. 123–147. https://doi.org/10.1016/j.cose.2018.11.001.
7. Maniriho, P.; Mahmood, A.N.; Chowdhury, M.J.M. A Survey of Recent Advances in Deep Learning Models for Detecting Malware in Desktop and Mobile Platforms. // ACM Comput. Surv. – 2024. – Vol. 56, Issue 6. – Article No. 145 P. 1–41. https://doi.org/10.1145/3638240.
8. Tien C.-W., Chen S.-W., Ban T., Kuo S.-Y. Machine Learning Framework to Analyze IoT Malware Using ELF and Opcode Features // Digital Threats: Research and Practice. – 2020. – Vol. 1, No. 1. – Art. 5. – DOI: 10.1145/3378448.
9. Souza C. H. M. et al. On the Use of Machine Learning for Modern IoT ELF Malware Detection // IEEE.LA-CCI. – 2025 – DOI:10.1109/LA-CCI66231. 2025.11270436.
10. Козачок А. В., Матовых С. С. Структурная модель файлов формата Portable Executable, содержащих вредоносный код // Проблемы информационной безопасности. Компьютерные системы. 2025. № 2. С. 41–59. DOI:10.48612/jisp/pdu2-fvxz-g5d3.
11. Arrieta A. B. et al. Explainable Artificial Intelligence (XAI): Concepts, Taxonomies, Opportunities and Challenges toward Responsible AI // Information Fusion. – 2020. – Vol. 58. – P. 82–115. – DOI: 10.1016/j.inffus.2019.12.012.
12. Ravi A., Chaturvedi V. Static Malware Analysis using ELF features for Linux based IoT devices // Proceedings of the 35th International Conference on VLSI Design & 21st International Conference on Embedded Systems (VLSID). – IEEE, 2022. – P. 114–119. – DOI: 10.1109/VLSID2022.2022.00033.
13. Antonakakis M., April T., Bailey M., Bernhard M., Bursztein E., Cochran J., Durumeric Z., Halderman J. A., Invernizzi L., Kallitsis M., Kumar D., Lever C., Ma Z., Mason J., Menscher D., Seaman C., Sullivan N., Thomas K., Zhou Y. Understanding the Mirai Botnet // Proceedings of the 26th USENIX Security Symposium. – 2017. – P. 1093–1110.
14. Park Y. et al. A practical approach for finding anti-debugging routines in the Arm-Linux using hardware tracing // Scientific Reports. 2024. – Article number: 14728 – DOI:10.1038/s41598-024-65374-w.
15. Lyda R., Hamrock J. Using Entropy Analysis to Find Encrypted and Packed Malware // IEEE Security & Privacy. – 2007. – Vol. 5, No. 2. – P. 40–45. – DOI: 10.1109/MSP.2007.48.

# A STRUCTURAL APPROACH TO STATIC ANALYSIS OF ELF FILES FOR MALWARE DETECTION

***Matovykh S. S.***[2]

***Keywords:*** *structural model, machine learning, malware classification, ELF files, Linux operating system, static executable analysis.*

***Abstract***

***Purpose of work:*** *the objective of this study is to develop and experimentally validate an interpretable structural model for the static analysis of ELF files aimed at detecting malicious software without code execution.*

***Research method:*** *the proposed approach is based on static analysis of ELF file structures and formalization of features in the form of a binary indicator vector. Classification is performed using machine learning techniques with cross-validation and comparative evaluation of multiple algorithms within a unified feature space.*

***Results of the study:*** *a feature space consisting of 63 binary structural indicators has been constructed. The indicators cover subsystems related to memory management, process control, network interaction, file system operations, privilege manipulation, anti-analysis mechanisms, and packing characteristics. A comparative experiment was conducted on a balanced dataset of ELF files containing both benign and malicious samples. The results demonstrate that ensemble methods provide the best trade-off between performance metrics. For the Random Forest model, the following values were obtained: Accuracy = 0.874 and F1-score = 0.860, confirming the practical applicability of the proposed model for early-stage static threat detection.*

***Scientific novelty:*** *the study introduces an interpretable subsystem-based organization of structural indicators that enhances model explainability and ensures applicability in multi-architecture ELF analysis scenarios.*

## References

1. Louis D. Advanced analysis of a Linux-dedicated malware (OrBit) [E`lektronny`j resurs]. – URL:www.stormshield.com/news/orbit-analysis-of-a-linux-dedicated-malware. – (data obrashheniya: 30.01.2026).
2. Sharma A., Sahay S. Evolution and Detection of Polymorphic and Metamorphic Malware: A Survey. – 2014. – https://doi.org/10.5120/15544-4098.

2 Sergey S. Matovykh, employee of the Russian Federation Security Guard Service Federal Academy. Orel, Russia. E-mail: coolt88@gmail.com

3. Daniel G., et al.: Assessing the Impact of Packing on Machine Learning Based Malware Detection Systems .– 2024. – https://doi.org/10.1016/j.cose.2025.104495.
4. Ramamoorthy J., et al. A Novel Static Analysis Approach Using System Calls for IoT Malware Detection // Electronics. – 2024. – Vol. 13, No. 15. – Article 2906. https://doi.org/10.3390/electronics13152906.
5. Anderson H. S., Roth P. EMBER: An Open Dataset for Training Static PE Malware Machine Learning Models // arXiv. – 2018. – https://doi.org/10.48550/arXiv.1804.04637.
6. Ucci D., Aniello L., Baldoni R. Survey of Machine Learning Techniques for Malware Analysis // Computers & Security. – 2019. – Vol. 81. – P. 123–147. https://doi.org/10.1016/j.cose.2018.11.001.
7. Maniriho, P.; Mahmood, A.N.; Chowdhury, M.J.M. A Survey of Recent Advances in Deep Learning Models for Detecting Malware in Desktop and Mobile Platforms. // ACM Comput. Surv. – 2024. – Vol. 56, Issue 6. – Article No. 145 P. 1–41. https://doi.org/10.1145/3638240.
8. Tien C.-W., Chen S.-W., Ban T., Kuo S.-Y. Machine Learning Framework to Analyze IoT Malware Using ELF and Opcode Features // Digital Threats: Research and Practice. – 2020. – Vol. 1, No. 1. – Art. 5. – DOI: 10.1145/3378448.
9. Souza C. H. M. et al. On the Use of Machine Learning for Modern IoT ELF Malware Detection // IEEE.LA-CCI. – 2025 – DOI:10.1109/LA-CCI66231. 2025.11270436.
10. Kozachok A. V., Matovy'x S. S. Strukturnaya model` fajlov formata Portable Executable, soderzhashhix vredonosny'j kod // Problemy' informacionnoj bezopasnosti. Komp'yuterny'e sistemy'. 2025. № 2. S. 41–59. DOI:10.48612/jisp/pdu2-fvxz-g5d3.
11. Arrieta A. B. et al. Explainable Artificial Intelligence (XAI): Concepts, Taxonomies, Opportunities and Challenges toward Responsible AI // Information Fusion. – 2020. – Vol. 58. – P. 82–115. – DOI: 10.1016/j.inffus.2019.12.012.
12. Ravi A., Chaturvedi V. Static Malware Analysis using ELF features for Linux based IoT devices // Proceedings of the 35th International Conference on VLSI Design & 21st International Conference on Embedded Systems (VLSID). – IEEE, 2022. – P. 114–119. – DOI: 10.1109/VLSID2022.2022.00033.
13. Antonakakis M., April T., Bailey M., Bernhard M., Bursztein E., Cochran J., Durumeric Z., Halderman J. A., Invernizzi L., Kallitsis M., Kumar D., Lever C., Ma Z., Mason J., Menscher D., Seaman C., Sullivan N., Thomas K., Zhou Y. Understanding the Mirai Botnet // Proceedings of the 26th USENIX Security Symposium. – 2017. – P. 1093–1110.
14. Park Y. et al. A practical approach for finding anti-debugging routines in the Arm-Linux using hardware tracing // Scientific Reports. 2024. – Article number: 14728 – DOI:10.1038/s41598-024-65374-w.
15. Lyda R., Hamrock J. Using Entropy Analysis to Find Encrypted and Packed Malware // IEEE Security & Privacy. – 2007. – Vol. 5, No. 2. – P. 40–45. – DOI: 10.1109/MSP.2007.48.

# СРАВНИТЕЛЬНЫЙ АНАЛИЗ СОВРЕМЕННЫХ МЕТОДОВ ОБНАРУЖЕНИЯ АНОМАЛИЙ В КОНТЕЙНЕРНЫХ СРЕДАХ НА ОСНОВЕ СИСТЕМНЫХ ВЫЗОВОВ

***Вьюгов С. Г.***[1]

**DOI:10.21681/3034-4050-2026-2-58-69**

***Ключевые слова:*** *обнаружение вторжений, аномальное обнаружение, системные вызовы, HIDS, анализ поведения программ, кибербезопасность, машинное обучение, графовые модели.*

***Цель исследования:*** *систематизация и сравнительный анализ современных методов обнаружения атак в контейнерных средах на основе системных вызовов с выявлением их сильных сторон, ограничений и областей применимости.*

***Методы исследования:*** *исследование основано на комплексном анализе существующих подходов к обнаружению атак в контейнерных средах, их систематизации и классификации по ключевым характеристикам: полноте используемой информации о системных вызовах, необходимости предварительного обучения и спектру обнаруживаемых угроз. Сравнительная оценка методов проведена на основе количественных метрик с использованием публичного набора данных LID-DS и результатов экспериментов на реальных микросервисных приложениях.*

***Результаты исследования:*** *выполнена систематизация современных подходов к обнаружению аномалий в контейнерных средах по критериям полноты анализируемых данных, спектра обнаруживаемых угроз и операционных требований. Количественное сравнение на наборе LID-DS показало, что нейросетевой метод на основе двухэтапного автоэнкодера с механизмом внимания превосходит графовый метод, так как оказался единственным, обнаружившим все рассмотренные сценарии, включая CVE-2014-0160 и CVE-2020-13942. Выявлено, что PROCATCH при F1-score 0,999 для исполнительных атак принципиально не обнаруживает неисполняемые атаки (SQL-инъекции, утечки данных через уязвимости протоколов, эксплуатацию уязвимостей веб-приложений), а CHIDS не способен выявить аномалии, проявляющиеся исключительно в параметрах системных вызовов. На основе полученных результатов сформулированы практические рекомендации по выбору метода обнаружения атак в зависимости от требований к безопасности системы.*

***Научная новизна:*** *заключается в систематизации и сравнительном анализе методов обнаружения вторжений в контейнерных средах по критериям полноты используемой информации, спектра обнаруживаемых угроз и операционных требований. Выявлении компромисса между простотой методов без обучения и полнотой обнаружения нейросетевых методов. Предложена классификация методов по типу анализируемых данных и уровню абстракции.*

## Введение

Технология контейнеризации стала неотъемлемой частью современного мира, обеспечивая масштабируемость, переносимость и лёгкую виртуализацию приложений, особенно в облачных средах. Согласно данным опроса *Cloud Native Computing Foundation* (*CNCF*) [1], более 92 % респондентов используют контейнеры в производственных средах, что свидетельствует о массовом переходе организаций на контейнерные архитектуры. Инструменты оркестрации, такие как *Kubernetes* [2], позволяют эффективно управлять развёртыванием и масштабированием контейнерных приложений, предоставляя предприятиям возможность оперативно адаптировать и масштабировать свою инфраструктуру к изменяющимся нагрузкам. Вместе с широким распространением контейнеров возросло и количество угроз информационной безопасности. По данным того же опроса *CNCF*, 32 % организаций называют безопасность главной проблемой при работе с контейнерами. Контейнерные приложения представляют собой мишень для кибератак, которые могут привести к отказу в обслуживании критически важных сервисов, утечке данных и значительному финансовому ущербу.

Традиционные подходы к обеспечению безопасности контейнеров: сканирование образов и управление уязвимостями – являются элементами защиты конвейера *CI*/*CD*, однако они неспособны противодействовать угрозам, возникающим непосредственно во время выполнения. К таким угрозам относятся эксплуатация уязвимостей нулевого дня (*Heartbleed CVE-2014-0160*), атаки с повышением привилегий (*DirtyCOW*, *Dirty Pipe*), а также более сложные комплексные атаки (*Scarleteel*, *LABRAT*). Для противодействия

1 Вьюгов Станислав Георгиевич, сотрудник Академии Федеральной службы охраны Российской Федерации. Орел, Орел. E-mail: stas.viugov@yandex.ru

подобным угрозам необходимы системы обнаружения вторжений (*IDS*), способные выявлять аномальное поведение в реальном времени.

Существующие подходы к обнаружению вторжений в контейнерных средах разделяются на три класса. Первый – сигнатурные (*rule-based*) системы, такие как *Falco* и *Tracee*, основанные на предопределённых правилах обнаружения. Они эффективны против известных угроз, однако требуют значительных экспертных усилий для создания правил и не обнаруживают ранее неизвестные атаки. Второй – системы без обучения (*training-free*), использующие стабильность атрибутов исполняемых файлов для обнаружения отклонений. Третий – нейросетевые системы на основе анализа системных вызовов, обучаемые на трассировках нормального поведения. В отечественной литературе данная проблематика активно развивается: Котенко и Мельник предложили подход к обнаружению аномалий в контейнерных системах на основе частотного анализа дизассемблированных инструкций и гибридной нейронной сети *AE-LSTM*. В последующей работе ими же выполнена классификация методов обнаружения атак и аномалий на основе анализа аномалий и профилирования, интегрированный подход на основе чёрных и белых списков представлен в [3]. Каждый из подходов обладает существенными ограничениями, что определяет необходимость их систематического сравнительного анализа.

## Системные вызовы как источник данных для обнаружения атак

Системные вызовы представляют собой программный интерфейс взаимодействия пользовательских процессов с ядром операционной системы *Linux*. Каждая операция, выполняемая внутри контейнера: работа с файловой системой, сетевое взаимодействие, управление процессами, межпроцессное взаимодействие – реализуется через один или несколько системных вызовов. Это делает системные вызовы наиболее информативным источником данных о поведении программного обеспечения на уровне системы. Каждый системный вызов характеризуется набором атрибутов:

- имя вызова (*syscall name*), определяющий тип системной операции;
- имя процесса (*process name*), идентифицирующий инициатора вызова;
- идентификатор потока (*thread ID*), позволяющий разделять действия различных потоков исполнения;
- возвращаемое значение (*return value*), указывающий на успешность выполнения;
- параметры (*arguments*), содержащий конкретные аргументы операции.

Авторский коллектив Forrest и др., предложивший модель *N-Gram* для описания поведения программного обеспечения через последовательности системных вызовов, исследования обнаружения аномалий на хосте последовательно расширяли объём используемой информации от простых имён вызовов через параметры к полной информации [4]. Сбор системных вызовов в контейнерных средах осуществлялся инструментами, которые взаимодействуют с ядром операционной системы Linux. Современные решения, такие как Falco, используют технологию *eBPF* (*Extended Berkeley Packet Filter*) для перехвата системных вызовов непосредственно в ядре с минимальными накладными расходами, что обеспечивает точность мониторинга без значительного влияния на производительность контролируемых контейнеров [5].

Анализ текущего состояния исследований в области обнаружения вторжений в контейнерных средах позволяет выделить ключевое противоречие: методы без обучения, избавляющие от операционных затрат на обучение и переобучение модели, принципиально ограничены в спектре обнаруживаемых угроз, в то время как нейросетевые методы, обеспечивающие более полный охват атак, требуют периодического переобучения при модификации контейнерного приложения.

Цель исследования – систематизация и сравнительный анализ современных методов обнаружения атак в контейнерных средах на основе системных вызовов с выявлением их сильных сторон, ограничений, слепых зон и областей применимости. Для достижения поставленной цели решаются следующие задачи:

1. Систематизировать существующие подходы к обнаружению аномалий в контейнерных средах на основе системных вызовов и предложить классификацию по типу анализируемых данных, спектру обнаруживаемых атак и операционным характеристикам.
2. Провести критический анализ четырёх современных методов (*CHIDS*, нейросетевой, *PROCATCH*, *AE-LSTM*) с количественным определением слепых зон каждого.
3. Формализовать модель обнаружения аномалий на основе полной информации о системных вызовах для определения базовой архитектуры нейросетевого подхода.
4. Выполнить сравнительный анализ рассмотренных подходов по критериям полноты обнаружения, точности, устойчивости к обходу,

операционных затрат и применимости к различным типам контейнерных сред.

### Графовый метод контекстуализации системных вызовов

Работа El Khairi и соавторов [6], представленная на семинаре *CCSW'22* (*ACM*), предлагает систему обнаружения вторжений на уровне хоста (*HIDS*), основанную на мониторинге разнородных свойств системных вызовов с учётом их контекста. Авторы формулируют ключевую гипотезу: аномалии могут быть точно обнаружены, когда свойства системных вызовов рассматриваются совместно в рамках их относительного контекста, а не изолированно.

Предложенный метод использует граф системных вызовов процесса (*Process Syscall Sequence Graph*, $PSSG$) – взвешенный направленный граф $G = (N,E,W)$, в котором множество узлов $N$ содержит комбинации имён системных вызовов и их значений возврата, множество ребер $E$ отражает направление выполнения от исходных узлов к узлам назначения, а функция весов $W$ определяет значимость узлов на основе обратной частоты обращений. Для каждого узла $i$ вес вычисляется по формуле:

$$W_i = 1 - \sum_{j \in \text{neighbour}(i)} f_{ji}, \quad (1)$$

где $\text{neighbour}(i)$ – множество входящих соседей узла $i$, а $f_{ji}$ – частота переходов от узла $j$ к узлу $i$.

Метод анализирует три категории признаков: характеристики потока выполнения, характеристики файловых данных и характеристики частоты [7].

Подход был оценён на двух наборах данных из 20 сценариев атак (11 700 нормальных и 1 980 атакующих трассировок системных вызовов). Результаты показали эффективность обнаружения различных аномалий при разумных затратах времени. Однако выявлены существенные ограничения: в сценариях *CVE-2014-0160* (*Heartbleed*) и *CVE-2020-13942* (*Apache Struts*) метод не обнаружил аномалии (*recall* = 0, *F1-score* = 0) [8]. Это связано с двумя причинами: во-первых, модель использует только имена системных вызовов и значения возврата для построения *PSSG*, игнорируя имена процессов, идентификаторы потоков и параметры; во-вторых, для обнаружения аномалий используется относительно простая модель, не способная улавливать тонкие аномалии, проявляющиеся исключительно в параметрах системных вызовов (например, аномальный объём данных, передаваемых через сетевые вызовы при эксплуатации *Heartbleed*) [9].

Анализ результатов позволяет выделить три класса ограничений данного метода:

1. Система на основе *CHIDS* строит граф $PSSG$ исключительно по именам вызовов и знакам возвращаемых значений. Атаки, при которых последовательность и состав вызовов идентичны нормальному поведению, а аномалия проявляется только в параметрах (объём данных, адреса, аргументы), остаются полностью необнаруженными.
2. Пороговый классификатор *CHIDS* оперирует суммарными характеристиками графа и неспособен моделировать нелинейные зависимости между компонентами вектора признаков. Это приводит к пропуску атак со сложными, но статистически неяркими паттернами.
3. В отличие от четырёхкомпонентного вектора нейросетевого метода, *CHIDS* не содержит аналога компонента вектора характеристик системных ресурсов, что исключает обнаружение аномалий в объёмах передаваемых данных.

### Нейросетевой метод на основе полной информации о системных вызовах

Работа Guo [10], представленная на конференции *DSAI 2024* (*ACM*), развивает графовый подход путём целенаправленного расширения набора анализируемых признаков. Автор впервые объединяет полный набор информации о системных вызовах – имена процессов, идентификаторы потоков, имена вызовов, возвращаемые значения и параметры в единую модель обнаружения вторжений. Архитектура системы включает три основных компонента, каждый из которых формализован математически. Модуль кодирования исходных данных преобразует последовательности системных вызовов в вектор аномалий $A$, состоящий из четырёх подвекторов:

$$A = [EFAV,UFV,FF,SRF], \quad (2)$$

где $EFAV$ – вектор аномалий потока выполнения (*Execution Flow Anomaly Vector*), $UFV$ – вектор непросмотренных файлов (*Unseen File Vector*), $FF$ – вектор характеристик частоты (*Frequency Features*), $SRF$ – вектор характеристик системных ресурсов (*System Resource Features*).

Вектор аномалий потока выполнения $EFAV$ вычисляется на основе модифицированного графа $PSSG$, расширенного информацией об именах процессов, идентификаторах потоков и возвращаемых значениях. При обнаружении аномального ребра (ребра, отсутствующего в эталонном графе) $EFAV$ рассчитывается как:

$$EFAV = \sum_{i=1}^{M}(W_{sn_i} + w_{dn_i}), \quad (3)$$

где $M$ – количество аномальных рёбер, $W_{sn}$ – вес узла-источника, $W_{dn}$ – вес узла назначения.

Вектор непросмотренных файлов $UFV$ формируется при обнаружении обращений к файловым путям, не наблюдавшимся на этапе обучения. В отличие от предшествующей работы [4], использовавшей четыре системных вызова для мониторинга файловых операций, данный подход задействует тринадцать вызовов, обеспечивая более полный охват:

$$UFV = N \times \sum_{i=1}^{N} W_i, \quad (4)$$

где $N$ – количество аномальных узлов, а $W_i$ – вес аномального узла, определённый из $PSSG$.

Модель обнаружения вторжений на основе двухэтапного автоэнкодера реализует двухфазную архитектуру с механизмом внимания. На первом этапе входной вектор признаков $x$ подвергается реконструкции, на втором этапе ошибка реконструкции первого этапа объединяется с входом и обрабатывается модулем многоголового внимания (рис. 1). Функция потерь определяется как:

$$L = \frac{1}{n} \times MSE(x, O_1) + (1 - \frac{1}{n}) \times MSE(x, O_2), \quad (5)$$

где $n$ – номер эпохи обучения, $MSE$ – функция средней квадратичной ошибки, $O_1$ – выход первого этапа, $O_2$ – выход второго этапа.

На ранних эпохах обучения (малые $n$) доминирует первый этап, обеспечивающий базовую

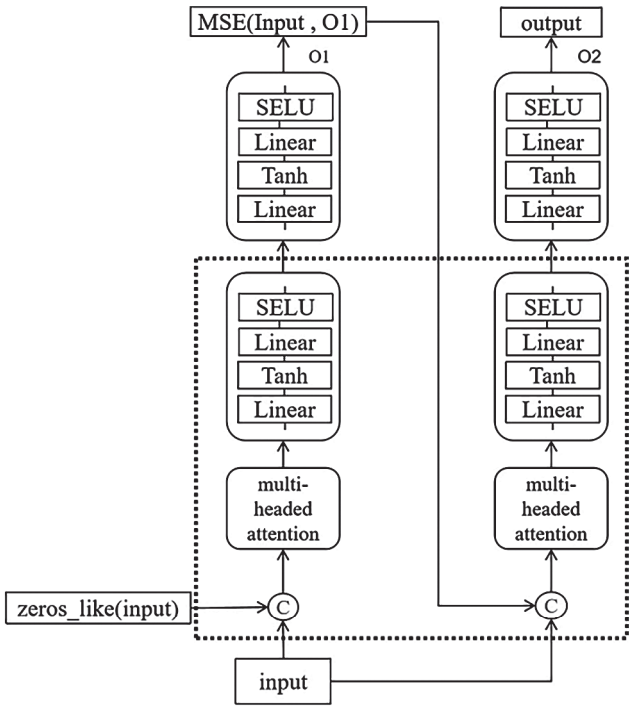



*Рис. 1. Архитектура двухэтапного автоэнкодера*

реконструкцию, по мере обучения (большие $n$) увеличивается вклад второго этапа с механизмом внимания, позволяющего выделять наиболее информативные паттерны аномалий.

Модуль динамического порога адаптивно изменяет порог обнаружения в зависимости от предшествующих результатов оценки:

$$\text{threshold} = \frac{1}{1 + e^{-\alpha(result - outlast)}} \times$$
$$\times \{-\beta \cdot (1 - \text{result} + \text{outlast}) \times \frac{1}{e} + \frac{1}{1 - e^{-0,2}}\} \times$$
$$\times (1 - e^{-w}), \quad (6)$$

где $\alpha$ управляет скоростью снижения порога, $\beta$ – скоростью повышения, $\omega$ – скоростью начального повышения.

Экспериментально определены оптимальные значения: $\alpha = 1$, $\beta = 0,3$, $\omega = 50$. Когда в предыдущий момент обнаружена аномалия, порог быстро снижается, повышая чувствительность к последующим аномальным событиям в рамках продолжающейся атаки [11]. При нормальном поведении порог медленно возрастает, снижая число ложных срабатываний. Эксперименты по сравнению вышеизложенных методов проведены на публичном наборе данных LID-DS по 13 сценариям. Результаты представлены в таблице 1.

Результаты демонстрируют значительное улучшение: средний *F1-score* увеличился с 0,813 до 0,977 (+20,2 %), средний *recall* – с 0,795 до 0,968 (+21,8 %), среднее число ложных срабатываний снизилось с 3,23 до 2,84 (–12,1 %).

Принципиально важно, что метод успешно обнаружил все 13 сценариев атак, включая *CVE-2014-0160* (*Heartbleed*) и *CVE-2020-13942*, которые оставались полностью невидимыми для графового метода *CHIDS*. Это стало возможным благодаря учёту характеристик системных ресурсов – аномальных объёмов данных в параметрах сетевых вызовов при эксплуатации *Heartbleed* и более точному извлечению признаков потока выполнения [12].

## Система обнаружения атак без обучения

Система *PROCATCH*, представленная El Khairi и соавторами [6,7], предлагает принципиально иную парадигму обнаружения вторжений, основанную на мониторинге стабильности атрибутов выполнения контейнерных микросервисов без какого-либо предварительного обучения. Ключевое наблюдение авторов: контейнерные микросервисы, следуя модели единой ответственности (*single-concern model*), выполняют единственную рабочую нагрузку на протяжении всего жизненного цикла, что обеспечивает стабильность

*Таблица 1*

*Сравнительные результаты CHIDS и нейросетевого метода на наборе LID-DS*

| Сценарий | Precision (CHIDS) | Recall (CHIDS) | FP (CHIDS) | F1 (CHIDS) | Precision (NEURO) | Recall (NEURO) | FP (NEURO) | F1 (NEURO) |
|---|---|---|---|---|---|---|---|---|
| EPS_CWE-434 | 1,000 | 1,000 | 0 | 1,000 | 0,980 | 1,000 | 6 | 0,992 |
| CVE-2020-9484 | 0,991 | 1,000 | 2 | 0,996 | 1,000 | 1,000 | 0 | 1,000 |
| PHP_CWE-434 | 1,000 | 1,000 | 0 | 1,000 | 0,992 | 1,000 | 1 | 0,996 |
| CVE-2020-23839 | 0,960 | 1,000 | 17 | 0,979 | 0,968 | 1,000 | 16 | 0,984 |
| CVE-2019-5418 | 1,000 | 0,867 | 0 | 0,928 | 1,000 | 1,000 | 0 | 1,000 |
| **CVE-2014-0160** | **0,000** | **0,000** | **1** | **0,000** | **0,967** | **1,000** | **11** | **0,984** |
| Bruteforce_CWE-307 | 0,956 | 0,949 | 19 | 0,953 | 1,000 | 0,978 | 0 | 0,989 |
| CVE-2017-7529 | 1,000 | 0,916 | 0 | 0,956 | 1,000 | 1,000 | 0 | 1,000 |
| CWE-89-SQL-injection | 1,000 | 1,000 | 0 | 1,000 | 1,000 | 1,000 | 0 | 1,000 |
| CVE-2018-3760 | 1,000 | 1,000 | 0 | 1,000 | 1,000 | 1,000 | 0 | 1,000 |
| CVE-2012-2122 | 1,000 | 1,000 | 0 | 1,000 | 1,000 | 1,000 | 0 | 1,000 |
| **CVE-2020-13942** | **0,000** | **0,000** | **0** | **0,000** | **1,000** | **0,992** | **0** | **0,996** |
| Juice Shop | 0,986 | 0,611 | 3 | 0,755 | 0,988 | 0,620 | 3 | 0,761 |
| **Среднее** | **0,838** | **0,795** | **3,23** | **0,813** | **0,992** | **0,968** | **2,84** | **0,977** |

их атрибутов выполнения. Предварительное исследование на четырёх микросервисных приложениях (*BOOKINFO*, *SOCK-SHOP*, *MU-SHOP*, *MARTIAN BANK*) подтвердило, что атрибуты исполняемых файлов – имя (*exe*), путь (*exe_path*), индексный дескриптор (*exe_inode*) и текущий рабочий каталог (*cwd*) – сохраняют полную стабильность при нормальной работе. Единственным неустойчивым атрибутом является имя процесса (*proc*), подверженное изменениям из-за создания и переименования потоков в средах управляемого выполнения (*JVM*, *V8*, *HikariPool*).

Система функционирует в два этапа. На первом этапе после достижения подом состояния *PodReady* система идентифицирует контейнер, разрешает его контрольную группу (*cgroup*) через «*/proc/<PID>/cgroup*», перечисляет все *PID* в данной группе и для каждого процесса извлекает атрибуты выполнения (*exe*, *exe_path*, *exe_inode*, *cwd*) через файловую систему «*/proc*». На втором этапе система непрерывно отслеживает отклонения от базовой линии с использованием *Falco – eBPF*-инструмента [13].

*PROCATCH* демонстрирует выдающиеся показатели: средняя *precision* = 99,77 %, средний *recall* = 100,00 %. Время обнаружения атак составляет от 700 до 900 мс для большинства сценариев. Однако исследование устойчивости к обходу выявило существенные ограничения. При попытке злоумышленника использовать технику выполнения в контексте существующих интерпретаторов (*in-line execution*) результаты обнаружения на различных стадиях атаки распределяются следующим образом: разведка – 0 %, подготовка среды – 0 %, подготовка полезной нагрузки – 66,72 %, выполнение – 100,00 %. Таким образом, *PROCATCH* полностью не эффективен на стадиях разведки и подготовки среды. На стадии подготовки полезной нагрузки обнаружение достигается только в тех микросервисах, которые не содержат встроенных интерпретаторов (*Python*, *Node.js*), что составляет 66,72 % случаев. Для микросервисов на *Python* и *Node.js* подготовка полезной нагрузки через встроенные библиотеки (*urllib.urlretrieve, os.chmod*) остаётся полностью необнаруженной.

Кроме того, *PROCATCH* принципиально не обнаруживает неисполнительные атаки: *SQL*-инъекции, утечки данных через уязвимости типа Heartbleed, обход каталогов (*directory traversal*) и уязвимости веб-приложений (*CVE-2020-13942*). Эти типы атак не порождают новых исполняемых файлов и не изменяют атрибуты выполнения, поэтому остаются за пределами возможностей любого метода, основанного исключительно на мониторинге атрибутов *executables*.

### Метод на основе гистограмм дизассемблированных инструкций (AE-LSTM)

Работа Котенко и Мельника [3, 4], предлагает принципиально отличный подход к обнаружению аномалий в контейнерных системах, основанный

на частотном анализе дизассемблированных машинных инструкций бинарных файлов выполняемых процессов.

В отличие от методов, анализирующих системные вызовы или атрибуты выполнения, данный подход оперирует на уровне содержимого исполняемых файлов. Сбор данных осуществляется с помощью *Falco Security* (*eBPF*) для получения путей к бинарным файлам, после чего утилитой *objdump* извлекаются дизассемблированные инструкции. На этапе нормализации формируются гистограммы процессов фиксированного размера путём подсчёта количества каждой инструкции и вычисления её относительной частоты:

$$h_i = \frac{count(instr_i)}{\sum_{j=1}^{K} count(instr_j)}, \quad (7)$$

где $count(instr_i)$ – количество вхождений $i$-й инструкции, $K$ – общее число уникальных инструкций в словаре.

Для обнаружения аномалий применяется гибридная неконтролируемая модель нейронной сети *AE-LSTM* (*Autoencoder – Long Short-Term Memory*). *AE*-компонент сжимает входные данные в представление размерности *ROWS* × *LINES/2*, а *LSTM*-компонент обрабатывает последовательности гистограмм, учитывая временные зависимости между процессами. Обнаружение аномалий выполняется путём вычисления ошибки реконструкции: если *MSE* входного вектора после реконструкции превышает порог $threshold = = \mu_{MSE} + \sigma_{MSE}$, то последовательность классифицируется как аномальная.

Экспериментальная оценка проведена на испытательном стенде, включающем два *Docker*-контейнера (*ssh/rdp*-сервер и почтовый сервер *Postfix*), с тремя группами наборов данных: нормальная активность (группа A), аномальная (группа B) и вредоносная (группа C). Каждый набор содержит не менее 700 тысяч записей последовательностей гистограмм.

Авторы отмечают следующие особенности подхода:

- высокую точность обнаружения аномальных последовательностей процессов;
- низкий уровень ложных срабатываний;
- эффективное выявление атак, связанных с перехватом выполнения программного кода и манипулированием адресами функций в бинарных файлах.

Однако метод имеет принципиальное ограничение: неспособность анализировать программы на интерпретируемых языках и языках с байт-кодом, поскольку дизассемблирование применимо только к нативным бинарным файлам формата ELF.

В последующей работе [5] авторами выполнена систематическая классификация методов обнаружения атак и аномалий в контейнерных системах на основе анализа аномалий и профилирования, включая анализ подходов на основе глубокого обучения (*LSTM*, *AE*, *CNN*, *SOM* + *MLP*), с выявлением их особенностей, преимуществ и недостатков.

## Систематизация рассмотренных подходов

На основании проведённого анализа сформирована классификация рассмотренных методов по ключевым характеристикам (табл. 2 и табл. 3).

## Формализация нейросетевого подхода к обнаружению аномалий

На основании проведённого анализа опишем в формализованном виде модель обнаружения аномалий, предложенную в работе Guo [10] и основанную на нейросетевом анализе полной информации о системных вызовах.

Пусть $S = \{s_1, s_2, \ldots, s_n\}$ – последовательность системных вызовов, собранных в течение периода $\tau(\tau = 1$ с). Каждый системный вызов $S_k$ характеризуется кортежем:

$$s_k = (name_k, proc_k, tid_k, ret_k, arg\ s_k), \quad (8)$$

где $name_k$ – имя системного вызова, $proc_k$ – имя процесса-инициатора, $tid_k$ – идентификатор потока, $ret_k$ – возвращаемое значение, $arg\ s_k$ – вектор параметров.

**Этап 1. Построение графа системных вызовов процесса (PSSG)**

Для каждого процесса $p \in P$, наблюдаемого в период $\tau$, строится взвешенный направленный граф:

$$G_p = (N_p, E_p, W_p). \quad (9)$$

Множество узлов $N_p$ формируется из пар $(name, ret\_sign)$, где $ret\_sign \in \{success, failure\}$ определяется знаком возвращаемого значения. Множество ребер $E_p$ содержит направленные ребра между последовательно вызванными парами системных вызовов в рамках одного потока $tid$. Весовая функция $W_p$ для узла $i$ определяется формулой (1).

**Этап 2. Извлечение вектора признаков**

Вектор аномалий $A \in R^d$ для периода $\tau$ формируется как конкатенация четырех подвекторов:

$$A = EFAV \oplus UFV \oplus FF \oplus SRF. \quad (10)$$

Компонент $EFAV$ кодирует аномалии потока выполнения. При фиксированном эталоне графа $G_p^{ref}$, построенном на этапе обучения, для каждого ребра $(u,v) \in E_p$ текущего периода

*Таблица 2*

*Классификация методов по типу анализируемых данных*

| Метод | Тип данных | Источник данных | Предобработка |
|---|---|---|---|
| CHIDS | Имена системных вызовов и возвращаемые значения | eBPF | Построение PSSG |
| Нейросетевой | Полная информация о системных вызовах | eBPF | Построение расширенно PSSG и извлечение 4-компонентного вектора |
| PROCATCH | Атрибуты выполнения | /proc, eBPF | Построение базовой линии атрибутов |
| AE-LSTM | Гистограммы дизассемблированных инструкций | objdump | Нормализация частот инструкций |

*Таблица 3*

*Матрица обнаруживаемых типов атак*

| Тип атаки | Пример | CHIDS | Нейро-сетевой | PROCATCH | AE-LSTM |
|---|---|---|---|---|---|
| Исполнительные (exec-based) | Kinsing, TeamTNT, Mirai | Да | Да | Да | Да |
| Утечки данных (data exfiltration) | Heartbleed (CVE-2014-0160) | Нет | Да | Нет | Нет |
| Инъекции | SQL-injection (CWE-89) | Да | Да | Нет | Нет |
| Удалённое выполнение кода | Apache Struts CVE-2020-13942 | Нет | Да | Частично | Нет |
| Повышение привилегий | DirtyCOW, Dirty Pipe | Частично | Да | Да | Да |
| Криптоджекинг | Kinsing, скрытый майнинг | Да | Да | Да | Да |
| Разведка (reconnaissance) | Сканирование сети, перечисление | – | Частично | Нет | – |
| In-line execution (через интерпретаторы) | Python reverse shell | – | Да | 66,72 % | Нет |
| Перехват выполнения бинарного кода | Подмена адресов функций в ELF | – | Частично | Частично | Да |

проверяется его принадлежность множеству $G_p^{ref}$. Если ребро отсутствует в эталоне, оно классифицируется как аномальное и его вклад определяется суммой весов инцидентов узлов.

Компонент $UFV$ аккумулирует информацию об обращениях к файловым путям, не наблюдавшимся при обучении, с использованием расширенного набора из 13 файловых системных вызовов: *open*, *openat*, *creat*, *rename*, *renameat*, *unlink*, *unlinkat*, *mkdir*, *mkdirat*, *rmdir*, *chmod*, *chown*, *link* [14].

Компонент $FF$ отражает общую частоту системных вызовов за $\tau$, без разделения по процессам, поскольку аномалии в частоте отдельных процессов отражаются в общей последовательности.

Компонент $SRF$ кодирует аномалии в объемах данных, передаваемых через системные вызовы с параметрами размера (*send*, *sendto*, *recv*, *recfrom*, *read*, *write*). Данный компонент критически важен для обнаружения атак, при которых уязвимость проявляется исключительно в аномально большом объеме данных, возвращаемых через сетевые вызовы.

**Этап 3. Двухэтапный автоэнкодер с механизмом внимания**

Модель $f: R^d \rightarrow R^d$ обучается минимизировать ошибку реконструкции на данных нормального поведения. На первом этапе кодер $E_1$ и декодер $D_1$ формируют выход $O_1$:

$$O_1 = D_1(E_1(A)). \quad (11)$$

Ошибка реконструкции первого этапа $\varepsilon_1 = A - O_1$ конкатенируется с входом и обрабатывается модулем внимания $MHA$ и вторым декодером $D_2$:

$$O_2 = D_2(MHA(A \oplus \varepsilon_1)). \quad (12)$$

Общая функция потерь определяется формулой (5), где балансировка между этапами контролируется номером эпохи $n$. При тестировании аномальность определяется сравнением

$MSE(A,O_2)$ с адаптивным порогом, вычисляемым по формуле (6).

**Этап 4. Принятие решения**

Для каждого периода вычисляется оценка аномальности:

$$score(\tau) = MSE(A_\tau, O_{2,\tau}). \quad (13)$$

Период классифицируется как аномальный, если $score > threshold(\tau)$, где $treshhold$ адаптивно вычисляется по формуле (6). Агрегация результатов по периодам внутри образа позволяет классифицировать образец как нормальный или атакующий.

## Ключевые отличия от существующих решений

Модель, предложенная Guo, отличается от графового метода *CHIDS* по следующим параметрам:

1. **Полнота представления.** *CHIDS* использует для построения *PSSG* исключительно имена системных вызовов, игнорируя имена процессов, идентификаторы потоков и параметры. Предлагаемая модель расширяет узлы *PSSG* комбинациями (*name*, *ret_sign*) в контексте конкретного потока *tid* конкретного процесса *proc*, что обеспечивает более точное отображение потока выполнения.
2. **Мощность модели.** *CHIDS* применяет пороговый классификатор на основе совокупности извлечённых признаков. Предлагаемая двухэтапная архитектура автоэнкодера с механизмом многоголового внимания обладает существенно большей моделирующей способностью, позволяя улавливать тонкие аномалии в нелинейных зависимостях между компонентами вектора признаков.
3. **Охват файловых операций.** Расширение набора контролируемых файловых системных вызовов с 4 до 13 повышает полноту обнаружения атак, связанных с несанкционированным доступом к файловой системе.
4. **Учет системных ресурсов.** Введение компонента *SRF* позволяет обнаруживать атаки, проявляющиеся исключительно в аномальных объёмах передаваемых данных, что принципиально недоступно для *CHIDS*. Именно этот компонент обеспечил обнаружение *CVE-2014-0160*, при котором уязвимый сервер возвращает до 64 КБ содержимого оперативной памяти через обычный *TLS* запрос.

Отличие от системы без обучения *PROCATCH* носит фундаментальный характер: *PROCATCH* отслеживает дискретное множество атрибутов выполнения (*exe*, *exe_path*, *exe_inode*, *cwd*), тогда как предлагаемая модель анализирует непрерывный многомерный вектор признаков, извлечённый из полной информации о системных вызовах. Это даёт возможность обнаруживать атаки, не порождающие новые исполняемые файлы: *SQL*-инъекции, утечки данных, эксплуатацию уязвимостей приложений, аномальное использование сетевых ресурсов.

## Анализ проблемы переобучения

Нейросетевые модели обнаружения вторжений на основе системных вызовов требуют обучения на данных нормального поведения и периодического переобучения при изменении профиля контейнерного приложения. Как отмечается в работе [16], базовые профили деградируют в динамических микросервисных средах, что требует частого переобучения – операционно затратного процесса. Причины необходимости переобучения можно классифицировать по трём категориям. Обновление версии микросервиса приводит к изменению набора выполняемых системных вызовов, структуры потоков исполнения и обращений к файловой системе. Изменение конфигурации (параметры запуска, переменные окружения, подключаемые библиотеки) может модифицировать паттерны взаимодействия с ядром. Изменение характера нагрузки (количество одновременных запросов, типы операций) влияет на частотные характеристики и объёмы передаваемых данных [15].

Интеграция в конвейер *CI/CD*. В современных микросервисных архитектурах развёртывание новых версий приложений осуществляется через автоматизированные конвейеры непрерывной интеграции и доставки. Переобучение модели обнаружения вторжений может быть встроено в этот конвейер как автоматический этап, выполняемый после успешного прохождения функциональных тестов. Формально конвейер расширяется следующим образом:

$$Pipeline_{extended} = Build \rightarrow Test \rightarrow Train_{IDS} \rightarrow \rightarrow Deploy \rightarrow Monitor. \quad (14)$$

На этапе $Train_{IDS}$ модель обучается на трассировках системных вызовов, собранных в ходе функционального тестирования. Поскольку тестовая среда воспроизводит типичные сценарии использования микросервиса, собранные данные достоверно представляют нормальное поведение новой версии. Модуль извлечения признаков на основе *PSSG* существенно снижает размерность данных. Из миллионов системных вызовов за один образец формируется вектор размерности $d$, порядок которой определяется числом уникальных процессов, системных вызовов и файловых путей. Экспериментальные

данные [16] показывают, что обучение на наборе *LID-DS* завершается за приемлемое для промышленного использования время.

Контейнерные микросервисы, спроектированные в соответствии с принципом единой ответственности, демонстрируют высокую стабильность поведения между версиями. Как подтверждено в исследовании [16], атрибуты выполнения сохраняют полную стабильность в пределах жизненного цикла микросервиса. Это означает, что переобучение требуется не непрерывно, а дискретно – при каждом обновлении версии. Перспективным направлением снижения операционных затрат является переход от полного переобучения к инкрементному обновлению модели. Формально:

$$\theta_{new} = \theta_{\{old\}} - \eta \nabla_{\theta} L(D_{new}; \theta_{old}), \quad (15)$$

где $\theta$ – параметры модели, $\eta$ – скорость обучения (существенно меньшая, чем при полном обучении), $D_{new}$ – набор данных нового нормального поведения. Такой подход сокращает время переобучения в десятки раз по сравнению с обучением с нуля.

Для корректной оценки перспективности нейросетевого подхода необходимо сопоставить операционные затраты на переобучение ($C_{train}$) с ожидаемыми потерями от пропущенных атак ($C_{miss}$):

$$C_{retrain} \ll C_{miss} = P_{attack} \times P_{miss} \times D_{impact}, \quad (16)$$

где $P_{attack}$ – вероятность атаки за цикл обновления, $P_{miss}$ – вероятность пропуска атаки методом без обучения, $D_{impact}$ – ожидаемый ущерб от инцидента.

По данным исследований [17, 18], публичные контейнерные микросервисы подвергаются атакам с высокой частотой. При этом $P_{miss}$ для *PROCATCH* составляет не менее 33,28 % для атак через встроенные интерпретаторы и 100 % для неисполнительных атак. В противоположность этому, стоимость $C_{retrain}$ ограничивается вычислительными ресурсами на обучение модели и интеграцией в существующий *CI/CD*-конвейер. Таким образом, даже при консервативных оценках выполняется неравенство $C_{retrain} \ll C_{miss}$, что экономически обосновывает выбор нейросетевого подхода с периодическим переобучением [19].

## Сравнительный анализ подходов

Для систематизации результатов проведённого анализа представим сравнение рассмотренных подходов по ключевым критериям.

Анализ таблицы 4 показывает, что нейросетевой метод на основе полной информации о системных вызовах является единственным подходом, обеспечивающим обнаружение всех рассмотренных классов атак. *PROCATCH*, несмотря на более высокий *F1-score* в пределах своей области применения (исполнительные атаки), обладает фундаментальной слепой зоной, составляющей значительную часть реального ландшафта угроз [20]. Метод *AE-LSTM* дополняет систему обнаружения на ином уровне абстракции – анализ содержимого бинарных файлов позволяет выявлять атаки, при которых злоумышленники перехватывают выполнение программного кода и манипулируют адресами функций, однако

*Таблица 4*

*Сравнительный анализ подходов к обнаружению атак*

| Критерий | CHIDS | Нейросетевой | PROCATCH | AE-LSTM |
|---|---|---|---|---|
| Метод обнаружения | Графовый + порог | Автоэнкодер с вниманием | Сравнение атрибутов | AE-LSTM + гистограммы |
| Тип анализируемых данных | Имена системных вызовов и возвращаемые значения | Полная информация о системных вызовах | Атрибуты выполнения | Дизассемблир. инструкции |
| Необходимость обучения | Да | Да | Нет | Да |
| Средний F1-score | 0,813 | 0,977 | 0,999 | Высокий |
| Обнаружение атак без исполнения | Частично | Да | Нет | Нет |
| Устойчивость к обходу | – | Частично | 0 % | – |
| Анализ Python/Java | Да | Да | Частично | Нет |
| Число сценариев с recall = 0 | 2 из 13 | 0 из 13 | 0 из 10 | – |
| Набор данных | LID-DS | LID-DS | Реальные атаки | Собственный стенд |

он неприменим к интерпретируемым средам и не обнаруживает атаки, не порождающие аномалий на уровне машинных инструкций.

## Выводы

В ходе исследования получены следующие результаты:

1. Проведён систематический сравнительный анализ четырёх современных подходов к обнаружению вторжений в контейнерных средах. Предложена классификация методов по типу анализируемых данных. Выявлены ключевые ограничения каждого метода.
2. Систематизирована и представлена в формализованном виде модель обнаружения аномалий, включающая: расширенный граф *PSSG*, четырёхкомпонентный вектор признаков, двухэтапный автоэнкодер с механизмом внимания и адаптивный динамический порог. Описаны формулы весовых функций, векторов аномалий, функции потерь и динамического порога.
3. На экспериментальных данных набора *LID-DS* продемонстрировано значительное превосходство нейросетевого подхода: средний *F1-score* увеличился с 0,813 (*CHIDS*) до 0,977 (рост на 20,2 %), средний *recall* – с 0,795 до 0,968 (рост на 21,8 %), число обнаруженных сценариев – с 11 до 13 из 13 (полный охват). Среднее число ложных срабатываний снизилось с 3,23 до 2,84 (снижение на 12,1 %).
4. Проведен анализ проблемы переобучения и обоснован выбор в пользу систем с переобучением.

## Литература


1. CNCF Survey 2020. – 2020. – URL: https://www.cncf.io/wp-content/uploads/2020/11/CNCF_Survey_Report_2020.pdf (дата обращения: 15.02.2026).
2. Aqasizade, H. Kubernetes in Action: Exploring the Performance of Kubernetes Distributions in the Cloud / H. Aqasizade, E. Ataie, M. Bastam // Software – Practice and Experience. – 2025. – Vol. 55, No. 10. – P. 1711–1725. – DOI 10.1002/spe.70000. – EDN DRFXVH.
3. Котенко, И. В. Обнаружение аномалий в контейнерных системах: применение частотного анализа и гибридной нейронной сети / И. В. Котенко, М. В. Мельник // Программные продукты и системы. – 2025. – № 3. – С. 426–437. – DOI 10.15827/0236-235X.151.426-437. – EDN GMQDSA.
4. Котенко, И. В. Обнаружение атак и аномалий в контейнерных системах: подходы на основе анализа аномалий и профилирования / И. В. Котенко, М. В. Мельник // Искусственный интеллект и принятие решений. – 2025. – № 2. – С. 3–18. – DOI 10.14357/20718594250201. – EDN DZEPTN.
5. Kotenko I., Melnik M., Abramenko G. Anomaly detection in container systems: using normal process histograms and an autoencoder // 2024 IEEE 25th International Conference of Young Professionals in Electron Devices and Materials (EDM 2024). IEEE. 2024. P.1930–1934. DOI: 10.1109/EDM61683.2024.10615118.
6. Khairi, Asbat & Peter, Andreas & Continella, Andrea. (2025). PROCATCH: Detecting Execution-Based Anomalies in Single-Instance Microservices. 1–9. 10.1109/CNS66487.2025.11194959.
7. El Khairi A., Caselli M., Knierim C., Peter A., Continella A. Contextualizing System Calls in Containers for Anomaly-Based Intrusion Detection // Proceedings of the 2022 Cloud Computing Security Workshop (CCSW '22). – ACM, 2022. – P. 9–21.
8. Jain V., Singh B., Khenwar M., Sharm M. Static vulnerability analysis of docker images // IOP Conference Series: Materials Science and Engineering. IOP Publishing. 2021. V. 1131. No 1. P. 012018. EDN: KUZGXN.
9. Nakata R., Otsuka A. Evaluation of vulnerability reproducibility in container-based Cyber Range // arXiv preprint arXiv:2010.16024. 2020.
10. Guo P. Intrusion Detection Based on Complete System Call Information // 2024 International Conference on Digital Society and Artificial Intelligence (DSAI 2024). – ACM, 2024. – 5 p.
11. Ahmed M. E., Kim H., Camtepe S., Nepal S. Peeler: Profiling kernel-level events to detect ransomware // Computer Security-ESORICS 22: 26th European Symposium on Research in Computer Security. Springer International Publishing. 2021. P. 240–260.
12. Tien C. W., Huang T. Y., Tien C. W., Huang T. C., Kuo S. Y. KubAnomaly: Anomaly detection for the Docker orchestration platform with neural network approaches // Engineering reports. 2019. V. 1. No 5. P. e12080.
13. Gantikow H., Zohner T., Reich C. Container anomaly detection using neural networks analyzing system calls // 2020 28th Euromicro International Conference on Parallel, Distributed and Network-Based Processing (PDP). IEEE. 2020. P. 408–412.
14. Kosinska J., Tobiasz M. Detection of Cluster Anomalies With ML Techniques // IEEE Access. 2022. V. 10. P. 110742–110753. EDN: VQHQOQ.
15. Wang Y., Wang Q., Qin X., Chen X., Xin B., Yang R. DockerWatch: a two-phase hybrid detection of malware using various static features in container cloud // Soft Computing. 2023. V. 27. No 2. P. 1015–1031. EDN: ISIKGC.
16. Chan K. Y., Abu-Salih B., Qaddoura R., Ala'M A. Z., Palade V., Pham D. S., Javier D. S., Muhammad K. Deep neural networks in the cloud: Review, applications, challenges and research directions // Neurocomputing. 2023. P. 126327.

17. Grimmer M., Röhling M. M., Kreusel D., Ganz S. A Modern and Sophisticated Host Based Intrusion Detection Data Set // IT-Sicherheit als Voraussetzung für eine erfolgreiche Digitalisierung. – 2019. – P. 135–145.
18. Castanhel G. R., Heinrich T., Ceschin F., Maziero C. Taking a peek: An evaluation of anomaly detection using system calls for containers // 2021 IEEE Symposium on Computers and Communications (ISCC). IEEE. 2021. P. 1–6.
19. Karn R. R., Kudva P., Huang H., Suneja S., Elfadel I. M. Cryptomining detection in container clouds using system calls and explainable machine learning // IEEE transactions on parallel and distributed systems. 2020. V. 32. No 3. P. 674–691.
20. Abubakar A. I., Chiroma H., Muaz S. A., Ila L. B. A review of the advances in cyber security benchmark datasets for evaluating data-driven based intrusion detection systems // Procedia Computer Science. 2015. V. 62. P. 221–227.

# ICOMPARATIVE ANALYSIS OF CURRENT METHODS FOR DETECTING ANOMALIES IN CONTAINER ENVIRONMENTS BASED ON SYSTEM CALLS

***Vyugov S. G.*[2]**

***Keywords:*** *intrusion detection, anomaly detection, system calls, HIDS, program behavior analysis, cybersecurity, machine learning, graph-based models.*

***Abstract***

***Purpose of the study:*** *to systematize and conduct a comparative analysis of modern attack detection methods in containerized environments based on system calls, identifying their strengths, limitations, and areas of applicability.*

***Methods of research:*** *the study is based on a comprehensive analysis of existing approaches to attack detection in containerized environments, including their systematization and classification according to key characteristics: completeness of system call information utilized, requirement for prior training, and the spectrum of detectable threats. A comparative evaluation was performed using quantitative metrics on the public LID-DS dataset, as well as experimental results obtained from real microservice-based applications.*

***Results:*** *a systematic classification of modern detection approaches in containerized environments was performed based on the completeness of analyzed data, the range of detectable threats, and operational requirements. Quantitative comparison on the LID-DS dataset demonstrated that the neural network-based two-stage autoencoder method with an attention mechanism outperforms the graph-based method, as it was the only approach that successfully detected all considered attack scenarios, including CVE-2014-0160 and CVE-2020-13942. It was found that PROCATCH, despite achieving an F1-score of 0.999 for executable attacks, fundamentally fails to detect non-executable attacks (such as SQL injections, data exfiltration via protocol vulnerabilities, and exploitation of web application vulnerabilities). CHIDS was shown to be incapable of detecting anomalies manifested exclusively in system call parameters. Based on the obtained results, practical recommendations were formulated for selecting an attack detection method depending on system security requirements.*

***Scientific novelty:*** *the novelty of this research lies in the systematization and comparative analysis of intrusion detection methods in containerized environments according to the completeness of utilized information, the spectrum of detectable threats, and operational requirements. A trade-off between the simplicity of training-free methods and the detection completeness of neural network–based approaches is identified. A classification of methods based on the type of analyzed data and the level of abstraction is proposed.*

## References

1. CNCF Survey 2020. – 2020. – URL: https://www.cncf.io/wp-content/uploads/2020/11/CNCF_Survey_Report_2020.pdf (data obrashheniya: 15.02.2026).
2. Aqasizade, H. Kubernetes in Action: Exploring the Performance of Kubernetes Distributions in the Cloud / H. Aqasizade, E. Ataie, M. Bastam // Software - Practice and Experience. – 2025. – Vol. 55, No. 10. – P. 1711–1725. – DOI 10.1002/spe.70000. – EDN DRFXVH.
3. Kotenko, I. V. Obnaruzhenie anomalij v kontejnerny'x sistemax: primenenie chastotnogo analiza i gibridnoj nejronnoj seti / I. V. Kotenko, M. V. Mel'nik // Programmny'e produkty' i sistemy'. – 2025. – № 3. – S. 426–437. – DOI 10.15827/0236-235X.151.426-437. – EDN GMQDSA.
4. Kotenko, I. V. Obnaruzhenie atak i anomalij v kontejnerny'x sistemax: podxody' na osnove analiza anomalij i profilirovaniya / I. V. Kotenko, M. V. Mel'nik // Iskusstvenny'j intellekt i prinyatie reshenij. – 2025. – № 2. – S. 3–18. – DOI 10.14357/20718594250201. – EDN DZEPTN.
5. Kotenko I., Melnik M., Abramenko G. Anomaly detection in container systems: using normal process histograms and an autoencoder // 2024 IEEE 25th International Conference of Young Professionals in Electron Devices and Materials (EDM 2024). IEEE. 2024. P.1930-1934. DOI: 10.1109/EDM61683.2024. 10615118.

2 Stanislav G. Vyugov, Academy of the Federal Security Service of the Russian Federation. Orel, Russia. E-mail: stas.viugov@yandex.ru

6. Khairi, Asbat & Peter, Andreas & Continella, Andrea. (2025). PROCATCH: Detecting Execution-Based Anomalies in Single-Instance Microservices. 1–9. 10.1109/CNS66487.2025.11194959.
7. El Khairi A., Caselli M., Knierim C., Peter A., Continella A. Contextualizing System Calls in Containers for Anomaly-Based Intrusion Detection // Proceedings of the 2022 Cloud Computing Security Workshop (CCSW 22). – ACM, 2022. – P. 9–21.
8. Jain V., Singh B., Khenwar M., Sharm M. Static vulnerability analysis of docker images // IOP Conference Series: Materials Science and Engineering. IOP Publishing. 2021. V. 1131. No 1. P. 012018. EDN: KUZGXN.
9. Nakata R., Otsuka A. Evaluation of vulnerability reproducibility in container-based Cyber Range // arXiv preprint arXiv:2010.16024. 2020.
10. Guo P. Intrusion Detection Based on Complete System Call Information // 2024 International Conference on Digital Society and Artificial Intelligence (DSAI 2024). – ACM, 2024. – 5 p.
11. Ahmed M. E., Kim H., Camtepe S., Nepal S. Peeler: Profiling kernel-level events to detect ransomware // Computer Security-ESORICS 22: 26th European Symposium on Research in Computer Security. Springer International Publishing. 2021. P. 240–260.
12. Tien C. W., Huang T. Y., Tien C. W., Huang T. C., Kuo S. Y. KubAnomaly: Anomaly detection for the Docker orchestration platform with neural network approaches // Engineering reports. 2019. V. 1. No 5. P. e12080.
13. Gantikow H., Zohner T., Reich C. Container anomaly detection using neural networks analyzing system calls // 2020 28th Euromicro International Conference on Parallel, Distributed and Network-Based Processing (PDP). IEEE. 2020. P. 408–412.
14. Kosinska J., Tobiasz M. Detection of Cluster Anomalies With ML Techniques // IEEE Access. 2022. V. 10. R. 110742–110753. EDN: VQHQOQ.
15. Wang Y., Wang Q., Qin X., Chen X., Xin B., Yang R. DockerWatch: a two-phase hybrid detection of malware using various static features in container cloud // Soft Computing. 2023. V. 27. No 2. P. 1015–1031. EDN: ISIKGC.
16. Chan K. Y., Abu-Salih B., Qaddoura R., AlaM A. Z., Palade V., Pham D. S., Javier D. S., Muhammad K. Deep neural networks in the cloud: Review, applications, challenges and research directions // Neurocomputing. 2023. P. 126327.
17. Grimmer M., Röhling M. M., Kreusel D., Ganz S. A Modern and Sophisticated Host Based Intrusion Detection Data Set // IT-Sicherheit als Voraussetzung für eine erfolgreiche Digitalisierung. – 2019. – P. 135–145.
18. Castanhel G. R., Heinrich T., Ceschin F., Maziero C. Taking a peek: An evaluation of anomaly detection using system calls for containers // 2021 IEEE Symposium on Computers and Communications (ISCC). IEEE. 2021. P. 1–6.
19. Karn R. R., Kudva P., Huang H., Suneja S., Elfadel I. M. Cryptomining detection in container clouds using system calls and explainable machine learning // IEEE transactions on parallel and distributed systems. 2020. V. 32. No 3. P. 674–691.
20. Abubakar A. I., Chiroma H., Muaz S. A., Ila L. B. A review of the advances in cyber security benchmark datasets for evaluating data-driven based intrusion detection systems // Procedia Computer Science. 2015. V. 62. P. 221–227.

# ПРИМЕНЕНИЯ КОММУНИКАЦИОННОГО УСТРОЙСТВА «МЕТАФОРА» В ЦЕЛЯХ ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ СИСТЕМЫ СВЯЗИ ТАКТИЧЕСКОГО ЗВЕНА УПРАВЛЕНИЯ

***Асанин А. В.[1], Иванов В. Г.[2], Лукьянчик В. Н.[3]***

**DOI:10.21681/3034-4050-2026-2-70-80**

***Ключевые слова:*** *радиосвязь, радиостанция, эффективность системы, ретрансляция.*

***Аннотация***

***Цель работы:*** *выработка практических предложений для обеспечения эффективности радиосвязи в системе связи тактического звена управления на основе применения тактического коммуникационного устройства связи с функциями защиты информации и межсетевой ретрансляции «Метафора».*

***Метод исследования:*** *методологическую основу исследования составила общая теория систем, теория военной связи, теория открытых систем с использованием методов системного анализа. Достоверность результатов обеспечивается практической реализаций приложенных в статье способов организации радиосвязи с применением тактического коммуникационного устройства связи с функциями защиты информации и межсетевой ретрансляции «Метафора» в ходе специальной военной операции.*

***Результаты исследования:*** *выбраны и обоснованы наиболее востребованные способы организации связи обеспечивающие развитие новых способов построения сетей радиосвязи и организации связи как в подразделениях при выполнении боевых задач, так и на пунктах управления. Представлены предложения по дальнейшему развитию тактического коммуникационного устройства связи с функциями защиты информации и межсетевой ретрансляции «Метафора», с учетом опыта организации связи в ходе специальной военной операции.*

***Практическая ценность:*** *заключается в разработке обоснованных способов организации радиосвязи в тактическом звене управления с учетом требований по обеспечению управления и технологического развития телекоммуникационных средств.[4][5][6]*

## Введение

В настоящее время для обеспечения радиосвязи применяется большое количество радиостанций различной номенклатуры, стандартов и типов, что вызывает сложности при организации радиосвязи в подразделениях различных звеньев управления, на снабжении которых находятся данные средства радиосвязи, следовательно основной сложностью является организация и обеспечение радиосвязи взаимодействия между подразделениями [1].

При этом технологические возможности дополнительного оборудования [2,3], для радиосредств (коммутаторы, ретрансляторы, концентраторы, преобразователи сигналов и др.) обеспечивают существенное повышение эффективности применения радиосредств и построение сетей радиосвязи, взаимодействие с сетями передачи данных и телефонными сетям связи.

Одним из направлений совершенствования способов организации и обеспечения радиосвязи по опыту специальной военной операции, является разработка и применение коммуникационных устройств, которые позволяют обеспечить сопряжение разнотипных средств радиосвязи, а также сопряжение радиостанций с сетями связи различного назначения (телефонные, передачи данных, сети «Интернет») с обеспечением ретрансляции сообщений между разнотипными оконечными устройствами.

Из всего ряда вышеприведенных разработок в данной области заслуживает внимание тактическое коммуникационное устройство связи с функциями защиты информации и межсетевой ретрансляции «Метафора» (ТКУ «Метафора», рис. 1) которая прошла успешную апробацию в ходе специальной военной операции и нашла применение как нештатное но высоко

1 Асанин Антон Викторович, кандидат технических наук, доцент, декан 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, Московской обл., Россия. E-mail: a.asanin@agz.50.mchs.gov.ru

2 Иванов Василий Геннадьевич, доктор военных наук, советник Российской академии ракетных и артиллерийских войск, профессор кафедры информатики и вычислительной техники 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, Московской обл., Россия. E-mail: wasj2006@yandex.ru

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

4 Тактический PTT коммутатор D4OPS. URL: https://npo-dvina.ru/2020/11/30/takticheskij-ptt-kommutator-d4ops/ (дата обращения: 6.01.2026).

5 Нагрудный коммутатор ODIN-2 с соединителем для р/ст Motorola URL: https://www.kbpriboi.ru/catalog/kommutacionnye-ustrojstva/nagrudnyy-kommutator-odin-ii/?ysclid=mkjodmpouk83717495 (дата обращения: 12.01.2026).

6 Тактическое коммуникационное устройство связи с функциями защиты информации и межсетевой ретрансляции «Метафора» URL: https://metapho.ru/ (дата обращения: 10.01.2026).

**Основные возможности ТКУ**

- сопряжение ТКУ с различными радиостанциями;
- передача речи через различные абонентские устройства;
- последовательная передача речи в различные радиосети;
- одновременная передача речи в различные радиосети;
- межсетевая ретрансляция, ретрансляция речи из одной радиосети в другую;
- последовательная защищенная передача речи в различные радиосети;
- одновременная защищенная передача речи в различные радиосети;
- межсетевая защищенная ретрансляция;
- последовательная передача речи в смешанном режиме;
- одновременная передача речи в смешанном режиме;
- ретрансляция речи в смешанном режиме;
- последовательная передача речи в радиосеть и через IP-сеть;
- одновременная передача речи в радиосеть и через IP-сеть;
- ретрансляция речи через IP-сеть;
- последовательная защищенная передача речи в радиосеть и через IP-сеть;
- одновременная защищенная передача речи в радиосеть и через IP-сеть;
- ретрансляция защищенной речи через IP-сеть;
- голосовая связь в IP-сети;
- защищенная передача сообщений нескольким корреспондентам (в группе);
- защищенная передача сообщений между двумя корреспондентами;
- одновременная защищенная передача сообщений в различные радиосети;
- защищенная ретрансляция сообщений из одной радиосети в другую.

а) носимый

б) стационарный (возимый)

Внешний вид тактического коммуникационного устройства

*Рис. 1. Основные тактико-технические характеристики ТКУ «Метафора»*

**Способы организации радиосвязи с применением ТКУ «Метафора»**

| | | |
|---|---|---|
| 1 | Работа в радиосетях развернутых с применением двух типов радиостанций | *Попеременная голосовая связь с двумя отдельными разнотипными радиосетями* |
| 2 | Автоматическая ретрансляция из одной радиосети в другую | *1. Объединение двух разнотипных радиосетей в единую радиосеть;*<br>*2. Ретрансляция речи из одной радиосети в другую и обратно.* |
| 3 | Ретрансляция из одной радиосети в другую через транспортную сеть связи | *1. Объединение двух радиосетей в единую радиосеть через транспортную сеть;*<br>*2. Ретрансляция речи из одной радиосети в другую и обратно через транспортную сеть.*<br>*3. Доступ в транспортную сеть осуществляется через точку доступа (WI-FI мосты, БШПД, маршрутизаторы MikroTik и. др)*<br>*4. Доверенный узел настроен на одной из ТКУ* |
| 4 | Ретрансляция из одной радиосети в другую через сеть Интернет (сеть сотовой связи) | *1. Объединение двух радиосетей в единую радиосеть через сеть Интернет;*<br>*2. Ретрансляция речи из одной радиосети в другую и обратно через сеть Интернет.*<br>*3. Подключение к Internet осуществляется через сети 4G или оборудование проводных провайдеров* |
| 5 | Работа с тремя радиосетями через транспортную сеть (IP) | *1. Раздельная голосовая связь с тремя радиосетями через транспортную сеть.*<br>*2. Применение в качестве оконечного устройства командирского планшета (смартфона)* |
| 6 | Ретрансляция из одной радиосети в другую через сеть Интернет (сеть сотовой связи) | *1. Объединение двух радиосетей в единую радиосеть через сеть Интернет;*<br>*2. Ретрансляция речи из одной радиосети в другую и обратно через сеть Интернет.*<br>*3. Подключение к Internet осуществляется через сети 4G или оборудование проводных провайдеров* |
| 7 | Обеспечение связи в режиме «Аудиокомнаты» с двумя радиосетями | *1. Один звонок на ТКУ из «Аудиокомнаты»;*<br>*2. Ретрансляция речи из радиосетей в «Аудиокомнату».* |
| 8 | Групповая работа IP телефонов с радиосетями | *1. До 5 звонков на Метафору, 5 добавочных номеров (10,11,20,21,30);*<br>*2. Одновременная ретрансляция SIP звонков в радиосети и обратно;*<br>*3. Ретрансляция SIP звонка по ключу через транспортную сеть (IP). До восьми радиосетей.* |

*Рис. 2. Способы организации радиосвязи с применением ТКУ «Метафора»*


*Рис. 3. Размещение ТКУ для обеспечения сопряжения двух радиосетей, развернутых на разнотипных радиостанциях.*

эффективное средство обеспечения связи во многих подразделениях группировок войск [4].

На основе реализованных тактико-технических характеристик ТКУ, разработаны новые способы организации и обеспечения радиосвязи, которые позволяют обеспечить взаимодействие и совместную работу радиосетей построенных на различных радиосредствах, но и их интеграцию в транспортную сеть (сеть «Интернет»), с обеспечением защищенной голосовой связи (рис. 2).

Рассмотрим подробно каждый из способов организации радиосвязи с применением ТКУ.

### 1. Работа в радиосетях развернутых с применениемдвух типов радиостанций

Для обеспечения управления должностным лицам пунктов управления, как правило, тактического звена управления (*мср*, *мсб*, *мсп*) развертываются радиосети соответствующих должностных лиц. В некоторых случаях, подчиненные подразделения могут быть оснащены различными типами средств радиосвязи (Р-187П1 «Азарт», Kirisun, Motorola, Hytera, Callta, AnyTone, Аргут, TYT, Комбат, Терек, PriZma и т.д.) и различного диапазона (КВ, УКВ) в этом случае у командира должны иметься все типы радиосредств которые имеются у подчинённых и с применением которых они обеспечивают управление подразделениями. При этом взаимодействие между соседними подразделениями, на имеющихся разнотипных радиосредствах, в большинстве случаев будет невозможно, вследствие отсутствия встречной работы радиостанций по различным причинам (не совпадение частотного диапазона, различные типы радиостанций, различные алгоритмы шифрования и т. д.).

Для решения вышеизложенной проблемы взаимодействия и сопряжения разнотипных радиосетей предлагается использовать ТКУ «Мета-


*Рис. 4. Вариант размещения ТКУ на вышке для ретрансляции и сопряжения радиосетей*

фора» которое размещается на экипировке командира одного из подразделений с подключенными к ней радиостанциями (например «Kirisun» и «Азарт»). При таком способе использования командир может вызывать поочередно 1 и 2 радиосеть, в которых находятся разные подразделения, а также работать сразу в двух радиосетях (рис. 3).

ТКУ «Метафора» применяемая командиром, позволяет подразделениям использующих различные типы радиостанций обмениваться информацией между собой.

## 2. Автоматическая ретрансляция из одной радиосети в другую

В целях обеспечения автоматической ретрансляции голоса из одной радиосети в другую предлагается размещать ТКУ «Метафора» с радиостанциями на вышке (дереве, высотном здании и т.д) (рис. 4). При данном способе обеспечивается существенное увеличение дальности связи без применения дорогостоящих ретрансляторов радиосвязи.

*Рис. 5. Вариант состава и размещения мобильного комплекса ретрансляции с ТКУ*

Для создания автономной группы ретрансляторов предлагается в подразделениях создавать мобильный комплекс ретрансляций связи (рис. 5).

В составе (ТКУ «Метафора», радиостанций используемых в подразделении, выносных антенн и источника электропитания).

## 3. Ретрансляция из одной радиосети в другую черезтранспортную сеть связи

Данный способ обеспечения радиосвязи между должностными лицами может применяться в различных условиях тактической обстановки и обстановки по связи (при действии подразделений друг от друга и от пункта управления старшего начальника, на удалении, при котором обеспечение радиосвязи невозможно; сложные физико-географические условия, блокирующие прохождение радиосигнала и т.д.). При этом в качестве сети связи, через которую осуществляется ретрансляция сообщений между различными радиосетями, с применением ТКУ «Метафора», может использоваться транспортная сеть связи группировки войск (рис. 6) развертываемая на различных штатных и не штатных средствах связи (проводными, оптоволоконными, средствами беспроводного широкополосного доступа, радиорелейными, средствами спутниковой связи).

Для увеличения числа взаимоувязанных радиосетей развёрнутых на различных радиостанциях к ТКУ «Метафора» подключаются одновременно две независимые радиосети, но работа обеспечивается только по парно (рис. 7).

Данный способ нашел наибольшее применение, так как работает на пунктах управления звена полк (бригада, дивизия) где имеются квалифицированные специалисты связи, способные

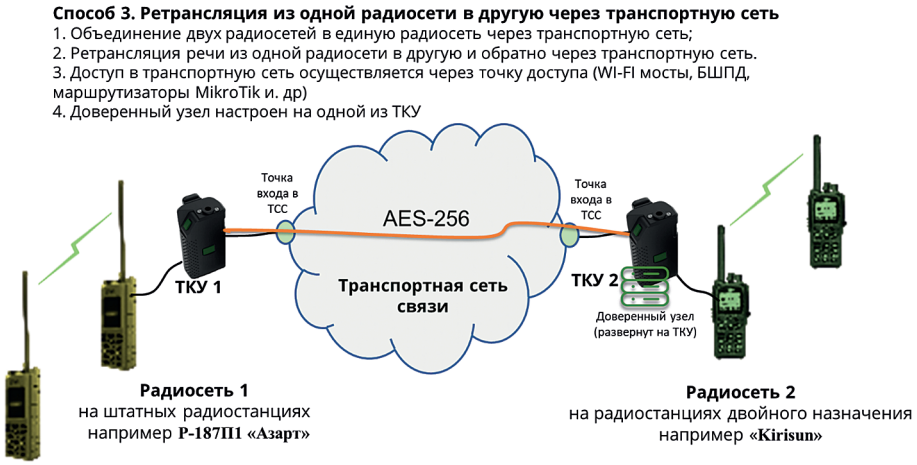



*Рис. 6. Ретрансляция сообщений между различными радиосетями, с применением ТКУ, используя транспортную сеть связи группировки войск*


*Рис. 7. Вариант подключения для обеспечение одновременной по парной работы в радиосетях через транспортную сеть связи*

осуществить распайку необходимых кабелей, настройку ТКУ «Метафора» и обладающие компетенциями по настройке сетевого оборудования, работающего по протоколу «Ethernet» и способные подключать изделия к транспортной сети связи.

Также при организации связи данным способом обеспечивается шифрование с помощью ТКУ «Метафора», в котором имеются реализован алгоритм шифрования AES-256, настройка и смена ключей в ТКУ осуществляется с использованием смартфона (планшета) или ПЭВМ.

## 4. Ретрансляция из одной радиосети в другую, через сеть Интернет (сеть сотовой связи)

В районах хорошо подготовленных в отношении связи, где имеется доступ к сети «Интернет» через официального провайдера, а также имеется устойчивое покрытие сетью сотовой связи, можно осуществить объединение радиосетей находящихся на значительном удалении с применением ТКУ «Метафора» (рис. 8).

Для этого предлагается использовать встроенный Wi-Fi модуль в ТКУ обеспечивающий подключения к беспроводному роутеру провайдера или с применением UTP кабеля. Работа через сеть сотовой связи ТКУ «Метафора» осуществляется путем подключения к нему модема сотовой связи или через сотовый телефон работающий в качестве модема.

При необходимости обеспечивается шифрования AES-256.

## 5. Работа с тремя радиосетями через транспортную сеть (IP)

Для работы с пункта управления размещенного на значительном удалении от мест развертывания радиосетей, с применением ТКУ «Метафора» через транспортную сеть связи обеспечивается работа в трех радиосетях, развёрнутых на разнотипных радиостанциях. Радиосети подключаются к транспортной сети с применением ТКУ «Метафора» (рис. 9).

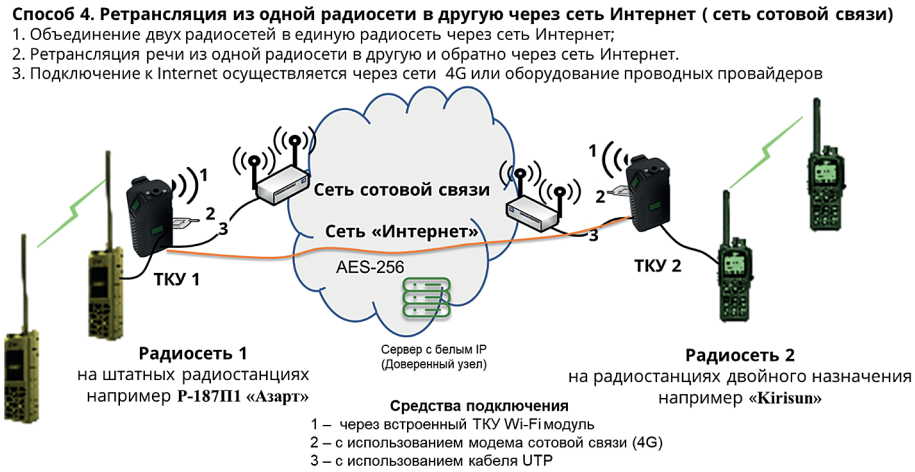



*Рис. 8. Варианты подключения ТКУ «Метафора» для работы в сети «Интернет» и сотовой связи*

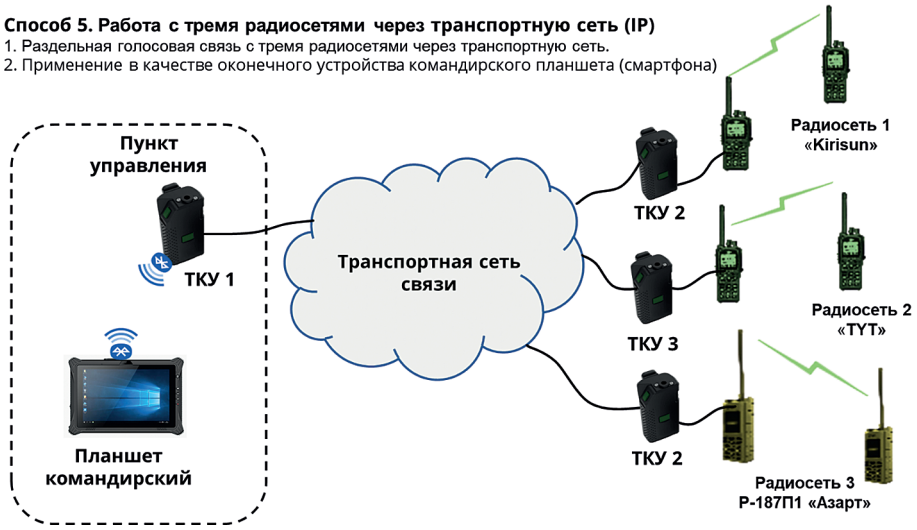



*Рис. 9. Варианты подключения ТКУ «Метафора» для работы в трех радиосетях через транспортную сеть*

На пункте управления в качестве оконечного устройства может быть использован командирский планшет или смартфон.

## 6. Голосовой обмен с IP телефона на две радиосети через транспортную сеть связи

Совмещение радиосвязи с телефонной сетью на базе ТКУ «Метафора» позволяет подключать военные узлы связи к IP-АТС и использовать стандартные VoIP-протоколы (SIP/RTP) рис. 10. Функционально устройство играет роль RoIP-шлюза в котором преобразуются аудиосигналы радиостанции в IP-пакеты и обратно, обеспечивая связь между радиосетью и телефонной/IP-сетью. Это даёт возможность напрямую присоединять полевые радиостанции к военным АТС (в т.ч. АТС-О) или коммерческим IP-АТС, а также к серверам IP-телефонии.

В результате голосовые вызовы могут свободно маршрутизироваться между радиоканалами и АТС-О. Например, абонент через ТКУ способен набрать внутренний номер телефонной сети (DTMF-набором) и установить связь с конкретной радиосетью на ЛБС. ТКУ выступит транзитом, передав звонок в эфир нужной радиосети.

Кроме того, радиосети могут быть включены в голосовые конференции IP-телефонии: одно ТКУ «Метафора» способно объединить в едином сеансе переговоров пользователей различных радиостанций, телефонной сети общего пользования (ТФОП), сотовой связи и диспетчерские пункты.

Тем самым устраняется разрозненность каналов и появляется единое коммуникационное голосовое пространство, позволяющее осуществлять голосовое управления элементами боевого порядка.

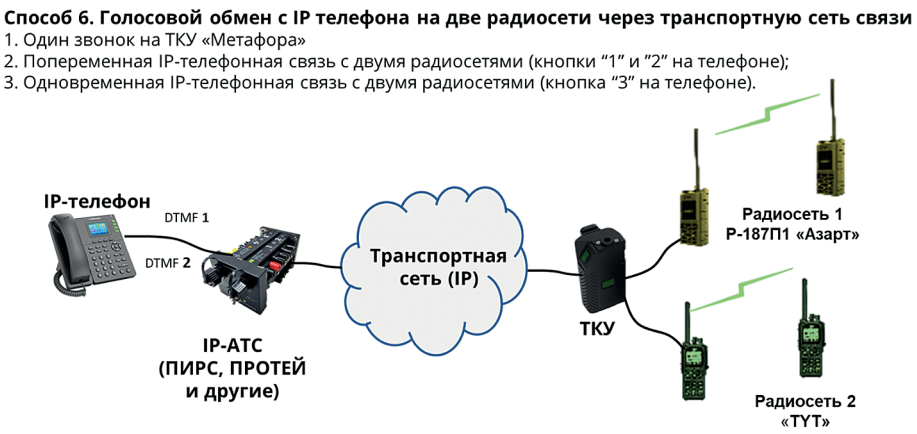



*Рис. 10. Вариант применения ТКУ «Метафора» совместно с IP АТС*


*Рис. 11. Вариант применения ТКУ «Метафора» для обеспечения связи при взаимодействии телефонных и радиосетей*

## 7. Обеспечение связи в режиме «Аудиокомнаты» с двумя радиосетями

В целях организации управления в режиме «реального времени» командиры различных уровней управления работают с подчинёнными командирами в «аудикомнатах», организованных с использованием современных АТС (например АРС ПИРС») и телефонных аппаратов. Для подключения в состав «аудикомнаты» командира находящегося на удалении и работающего в радиосети предлагается променять ТКУ «Метафора» (рис. 11).

Таким образом применение ТКУ обеспечивает создание нового способа взаимодействия телефонных и радиосетей.

## 8. Групповая работа IP телефонов с радиосетями

В целях обеспечения единого голосового пространства в интересах стационарных (находящихся на пункте управления) и мобильных (в элементах боевого порядка) пользователей с применением ТКУ «Метафора» разработан способ обеспечения групповой работы с телефонов развернутых на ПУ в радиосетях развернутых на различных типах радиостанции (рис. 12).

Интеграция сетей позволяет решить проблему их взаимодействия, когда радиосети разных подразделений и телефонные линии штаба – это изолированные контуры и прямой связи между ними нет. ТКУ «Метафора» позволяет устранить несовместимость этих разнородных систем и объединить их в единую сеть через широкополосные каналы и транспортную сеть связи (рис. 12).

Благодаря этому командиры и штабы обеспечиваются устойчивым управлением подразделениями: офицер штаба с IP-телефона или полевого телефона мгновенно выходит на связь с абонентом в радиосети, как если бы это был обычный телефонный звонок. Корреспонденту радиосети не нужно иметь отдельных устройств – вызов поступает на их штатные радиостанции. Аналогично и обратная связь: Корреспонденты по имеющимся у них радиостанциям могут


*Рис. 12. Вариант применения ТКУ «Метафора» для обеспечения групповой работы*

докладывать напрямую на цифровые средства связи (телефон) командования. Это заметно упрощает управление подразделениями и ускоряет передачу команд. Кроме того, облегчается горизонтальное взаимодействие между подразделениями. Если раньше связь в звене «рота – рота» требовала участия узла связи, то теперь различные подразделения могут связываться друг с другом используя IP-сеть как транспортный «мост». Например, две тактические группы на разных участках, каждая со своей радиосетью, через IP-канал и ТКУ «Метафора» объединяются в общий канал переговоров.

В результате повышается координация в бою, все необходимые звенья – от штабов до передовых групп – остаются на голосовой связи между собой, независимо от того, используют они радиостанции, полевые или стационарные IP-телефоны.

Передача голоса через IP-инфраструктуру снижает зависимость от ограниченного радиочастотного ресурса. В полевых условиях диапазоны радиосвязи перегружены и подвержены помехам, поэтому возможность частично перевести трафик в альтернативные сети важная задача. ТКУ «Метафора» поддерживает подключение по нескольким каналам: через USB-модем она выходит в сотовую сеть, есть порт для проводного Ethernet и модуль Wi-Fi для подключения к беспроводной IP-сети. Таким образом, где доступна проводная связь (полевой кабель, оптоволокно) или широкополосный канал, туда можно перенаправить значительную часть переговоров. Голосовые команды от штаба к подчиненным могут идти по IP-сети, освобождая эфир для других задач.

Опыт применения ТКУ позволил выявить следующие наиболее востребованные варианты организации связи.

Вариант № 1 «*Организация связи между подразделениями, использующими разные типы радиостанций*».

Практическое применение варианта в боевых условиях:

- взаимодействие штурмовых групп и артиллерии;
- системы оповещения о ракетной опасности и БПЛА.

Результат:

- обеспечивается тактическое преимущество подразделений за счет оперативного объединения разрозненных радиосетей в единый контур управления;
- повышена оперативность боевого управления – приказы и информация доводятся до всех подразделений без промедления;
- создано единое голосовое пространство без замены штатного оборудования – связь осуществляется между всеми средствами;
- снижена стоимость организации связи за счет замены дорогостоящих ретрансляторов на ТКУ «Метафора».

Вариант № 2 «*Межсетевая ретрансляция голосовых потоков между радиосетями образованных различными радиосредствами через транспортные сети и сеть «Интернет*».

Применение данного варианта определяются условиями, когда различные воинские подразделения (штурмовые группы, артиллерия, службы оповещения, ПВО) могут располагаться на значительном удалении друг от друга, а УКВ-радиостанции не всегда способны обеспечить стабильную голосовую связь. Это усугубляется отсутствием единой транспортной инфраструктуры: у одних частей используется канал через спутниковую систему связи, у других – сети 4G, у третьих – Wi-Fi мосты и локальные решения на базе сети «Ethernet». Данный вариант развертывания системы связи позволяет объединить разнородные радиосети и предоставить возможность оперативного взаимодействия и боевого управления даже на больших дистанциях.

Результат:

- сквозное боевое управление обеспеченное интеграцией разнотипных радиостанций и транспортных сетей в общий контур связи;
- расширение зоны контроля объединение четырех радиосетей (включая сеть «Ethernet») позволило охватить участки фронта большой протяженности;
- быстрое увеличение зоны связи и объедение разрозненных сетей повышает боевую эффективность подразделений за счёт упрощения координации между подразделениями разных видов и родов войск;
- оптимизация затрат (ТКУ «Метафора» выступает альтернативой дорогостоящим ретрансляторам, позволяя использовать существующие каналы связи и радиостанции без существенных затрат).

Рассмотрев данные способы, можно утверждать, что ТКУ «Метафора» – это универсальный коммуникационный шлюз, способный обеспечить взаимодействие между различными сетями связи. Его ключевыми функциями являются:

- объединение разрозненных радиосетей подразделений (например радиосетей на базе Р-187П1 и радиосетей DMR ). Без каких-либо модификаций самих средств связи;
- интеграция с транспортными сетями (возможность передачи речи через Ethernet, Wi-Fi, 4G);

- создание гибридных IP-радиосетей. Преобразование радиосигналов в IP-потоки, подключения к IP-телефонии и аудио конференциям;
- организация единого пространства голосовой связи. Разные подсистемы голосовой связи (радио, IP-телефония, транспортные сети) объединяющиеся в общую сеть.

На основании опыта применения ТКУ «Метафора» в СВО сформулированы основные направления дальнейшего ее развития. Модернизация изделия должна быть направлена не только на расширение номенклатуры поддерживаемых интерфейсов, но и на внедрение элементов искусственного интеллекта (Edge AI), повышение помехозащищенности и интеграцию с системами управления.

## 9. Основные направления совершенствования ТКУ «Метафора»

1. **Развитие аппаратной архитектуры и радиочастотных возможностей.**

*Многомодульная архитектура*. Увеличение числа интерфейсных портов за счет программного объединения нескольких устройств позволит трансформировать устройство из индивидуального шлюза в узловой концентратор. Это обеспечит возможность одному оператору (командиру или связисту) микшировать и маршрутизировать потоки трех-четырех радиосетей одновременно, создавая единый контур управления без необходимости использования громоздких полевых коммутаторов.

*Гибридизация (интеграция SDR)*. Перспективным направлением является встраивание в ТКУ программно-определяемого радиомодуля (SDR). Это позволит устройству выступать не только как шлюз, но и как самостоятельная радиостанция или ретранслятор. Такой подход снизит зависимость от внешних приемопередатчиков: для сопряжения сетей потребуется лишь одна внешняя радиостанция, либо (при работе SDR-модуля) устройство сможет самостоятельно обеспечивать выход в эфир, динамически меняя частоты и типы модуляции.

*Повышение автономности и эргономики*. Для длительных операций необходимо предусмотреть модульную систему питания с возможностью «горячей» замены аккумуляторов повышенной емкости (до 3800 мА·ч). Также, в целях повышения удобства эксплуатации в условиях отсутствия доступа к управляющему смартфону (смарт-устройству), целесообразно оснащение корпуса ТКУ минималистичным индикаторным блоком (OLED или LED-матрица) для отображения статуса каналов, уровня заряда и режима шифрования, а также физическими органами управления для оперативного переключения пресетов маршрутизации.

2. **Внедрение технологий Edge AI и интеллектуальная обработка сигналов.**

*Интеллектуальное шумоподавление*. В условиях интенсивного огневого контакта разборчивость речи критически снижается. Предлагается внедрение легковесных нейросетевых моделей (типа RNNoise или DeepFilterNet), оптимизированных для работы на текущей аппаратной платформе.

*Автоматическое распознавание речи (ASR) и семантический анализ*. Интеграция оффлайн-моделей распознавания речи (например, на базе Vosk) позволит реализовать функцию автоматического мониторинга эфира на наличие ключевых слов («ранен», «контакт», «артналет»). При обнаружении маркера устройство сможет автоматически формировать и отправлять тревожное уведомление командиру. Кроме того, транскрибация голоса в текст позволяет передавать информацию в условиях крайне узких каналов связи, где передача голоса невозможна.

3. **Сетевая интеграция и протоколы повышенной живучести**

*Интеграция с тактическими терминалами*. Реализация передачи данных голосовые каналы аналоговых радиостанций позволит использовать ТКУ как аудио-модем. Преобразуя координаты и метки целеуказания в аудиосигнал (с использованием протоколов OFDM или AFSK), ТКУ «Метафора» позволит интегрировать устаревшие или простейшие аналоговые средства связи в цифровые системы управления боем, обеспечивая отображение местоположения бойцов на карте командира. Тактическая обстановка часто представляется на планшете/ноутбуке. Поэтому интеграция возможностей ТКУ «Метафора» с такими системами как ГЛАЗ/ГРОЗА и ему подобными значительно возможности голосового управления боем.

*Применение Mesh-технологий и LPI-каналов*. Задействование USB-интерфейсов устройства для подключения модулей LoRa создаст резервный, скрытный контур связи. В условиях подавления УКВ-связи средствами РЭБ, ТКУ сможет автоматически перенаправлять телеметрию и текстовые команды через энергоэффективную Mesh-сеть с низкой вероятностью обнаружения.

*Поддержка DTN (Delay Tolerant Networking)*. Для работы в условиях нестабильного соединения («рваный» канал связи, работа через спутник в движении) необходимо внедрение стека протоколов, устойчивых к задержкам (например, IBR-DTN). Реализация принципа Store-and-Forward гарантирует доставку приказов и донесений: при

обрыве связи данные накапливаются во внутренней памяти ТКУ «Метафора» и передаются автоматически при восстановлении канала или появлении в зоне доступа дрона-ретранслятора.

**4. Криптографическая защита.**

Перспективная версия ПО должна поддерживать модульную архитектуру шифрования, позволяющую интегрировать отечественные алгоритмы (ГОСТ).

## Заключение

Реализация предложенных направлений модернизации ТКУ «Метафора» позволит существенно изменить существующие подходы к организации радиосвязи, объединяю элементы радиосетей в единую интеллектуальную коммуникационную среду. В которой будет повышено качество передаваемой информации, обеспечена скрытность управления и интегрированность в единое информационное пространство в части создания единый контура голосового управления.

Высокие тактико-технические характеристики ТКУ «Метафора» позволяют обеспечить взаимодействия не только между подразделениями в группировках войск, но и с подразделениями силовых министерств и ведомств Российской Федерации, а также с подразделениями Организации Договора о коллективной безопасности (ОДКБ) при выполнении совместных задач с учетом того, что достичь однотипного оснащения средствами радиосвязи данных подразделений практически невозможно.

## 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. Султанов Б. В., Дорошкевич В. В. Краткий обзор зарубежных военных тактических систем связи / Инжиниринг и технологии 2019. – Vol. 4(2) – С. 1–5. DOI 10.21685/2587-7704-2019-4-2-2.
3. Акимов А. В., Масалимов А. В., Удалова А. П. Обзор систем связи тактического звена управления вооруженных сил США // Военная мысль. 2023. № 8. С.146–157.
4. 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.


# THE USE OF THE METAPHOR COMMUNICATION DEVICE IN ORDER TO IMPROVE THE EFFECTIVENESS OF THE COMMUNICATION SYSTEM OF THE TACTICAL CONTROL LEVEL

***Asanin A. V.[7], Ivanov V. G.[8], Lukyanchik V. N.[9]***

***Keywords:*** *radio communication, radio station, system efficiency, retransmission.*

***Abstract***

***The purpose of the work*** *is to develop practical proposals for ensuring the effectiveness of radio communication in the communication system of the tactical control level based on the use of a tactical communication device with the functions of information protection and internetwork retransmission «Metaphor».*

***Research method:*** *the methodological 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 organizing radio communication with the use of a tactical communication device with the functions of information protection and internetwork relay «Metaphor» during a special military operation.*

***Results of the study:*** *the most popular methods of communication organization have been selected and substantiated, ensuring the development of new ways of building radio communication networks and organizing communications both in units during combat missions and at command posts. Proposals are presented for the further development*

7 Anton V. Asanin, Ph.D. of Technical Sciences, Associate Professor, Dean of the 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, Moscow Region, Russia. E-mail: asanin-anton@mail.ru

8 Vasily G. Ivanov, Dr.Sc. of Military Sciences, Advisor to the Russian Academy of Missile and Artillery Forces, Professor of the Department of Informatics and Computer Engineering of the Engineering Faculty of the Academy of Civil Defense 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, Moscow Region, Russia. E-mail: wasj2006@yandex.ru

9 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

*of the tactical communication device with the functions of information protection and internetwork relay «Metaphor», taking into account the experience of organizing communications during a special military operation.*

***Practical value:*** *consists in the development of justified methods of organizing radio communication in the tactical control level, taking into account the requirements for ensuring control and technological development of telecommunication facilities.*

## References

1. Ivanov V. G. Osnovy' postroeniya i ocenki e'ffektivnosti funkcionirovaniya sistemy' svyazi special'nogo naznacheniya v mezhdunarodnom vooruzhennom konflikte na osnove mnogosfernoj i konvergentnoj struktury' ee e'lementov: Monografiya. – SPb.: POLITEX, 2023. – 298 s.
2. Sultanov B. V., Doroshkevich V. V. Kratkij obzor zarubezhny'x voenny'x takticheskix sistem svyazi / Inzhiniring i texnologii 2019. – Vol. 4(2) – S. 1–5. DOI 10.21685/2587-7704-2019-4-2-2
3. Akimov A. V., Masalimov A. V., Udalova A.P. Obzor sistem svyazi takticheskogo zvena upravleniya vooruzhenny'x sil SShA // Voennaya my'sl'. 2023. № 8. S.146–157
4. Ivanov V. G. Teoriya i praktika postroeniya i obespecheniya funkcionirovaniya sistemy' svyazi special'nogo naznacheniya s uchyotom texnologicheskogo razvitiya i opy'tov vooruzhenny'x konfliktov: monografiya – M.: Krasnaya Zvezda, 2025. – 304 s.

# ПОВЫШЕНИЕ ЖИВУЧЕСТИ ЭЛЕМЕНТОВ СИСТЕМЫ СВЯЗИ ГРУППИРОВКИ ВОЙСК ПРИ ВЫПОЛНЕНИИ МЕРОПРИЯТИЙ БОЕВОГО ОБЕСПЕЧЕНИЯ ВОЙСК СВЯЗИ

***Падишин С. А.[1], Вольхин С. Д.[2]***

**DOI:10.21681/3034-4050-2026-2-81-88**

***Ключевые слова:*** *эффективность, модель воздействия, разведзащищенность, огневое поражение, система связи, система управление.*

***Аннотация***

***Цель работы:*** *на основе анализа и обобщения исходных данных, используя модель огневого воздействия противника, сформулировать основные направления и выработать мероприятия боевого обеспечения системы и войск связи обеспечивающие необходимую живучесть элементов системы связи (СС) в современном вооруженном противоборстве.*

***Метод исследования*** *основан на разработке комплексных аналитических и имитационных моделей, оценивающих процессы неопределенности и многоаспектности ведения боевых действий.*

***Результаты исследования*** *позволят оценить возможный ущерб элементам системы связи группировки войск (ГрВ) в результате комплексного огневого воздействия разведывательно-ударных комплексов противника, разработать комплекс мероприятий по основным видам боевого обеспечения, выполнение которых позволят повысить живучесть как отдельного элемента, так и системы связи в целом. Используя созданную модель огневого воздействия на элементы системы связи ГрВ в современном вооруженном конфликте предложен инновационный метод синтеза мероприятий боевого обеспечения, обеспечивающих повышение живучести системы связи. Обновленный подход позволяет прогнозировать предполагаемый ущерб элементам системы, нанесенный в условиях динамично меняющейся оперативной обстановки и комплексного огневого воздействия противника.*

***Результаты моделирования*** *определяют научно обоснованные требования к организационно-штатным структурам соединений и частей связи (управления) в целях выполнения мероприятий по живучести. Результаты будут положены в основу предложений по созданию и внедрению в штаты подразделений боевого обеспечения и тактики их применения. Ключевым аспектом методологии стало внедрение алгоритмов математического моделирования, способных воспроизводить совокупность вероятностных событий, разведки (добывания, обработки, анализа разведданных об объекте от различных видов разведки, доразведку) элементов системы связи, принятия решения на их поражение, выбор огневого средства и его применение.*

***Практическая ценность:*** *предложенный подход позволяет прогнозировать предполагаемый ущерб элементам системы, нанесенный в условиях динамично меняющейся оперативной обстановки и комплексного огневого воздействия противника. Это обеспечивает аналитическую основу для оценки живучести элементов системы связи; прогнозирования критических важных элементов; формулирования мероприятий защиты; создание и применение ресурсов обеспечения живучести.*

## Введение

Специальная военная операция (СВО), операции израильских войск против «ХАМАС» и Ирана показывают, что современный международный вооруженный конфликт носит затяжной характер, не одна из сторон не может в короткие сроки одержать победу.

В данных условиях на первый план выходит организация и ведение разведывательно-ударных действий высокоструктурированных систем и комплексов разведки, РЭБ, и применением всего спектра средств огневого поражения. Кроме того, СВО кардинально трансформировала принципы ведения современных боевых действий. Задача «дезорганизация системы управления» вышла на первые роли в структуре общевойсковых операций.

Противник при ведении разведки применяет ее комплексирование, что позволяет компенсировать слабые стороны одного вида разведки сильными сторонами других. Учитывая опыт проведения СВО, противник применяет комплексирование не только видов разведки и доразведки, но и средств поражения, например, беспилотные летательные аппараты (БПЛА) имеют на борту средства радиоэлектронной и оптической разведки, а также средства огневого поражения. Благодаря новым технологиям нынешние возможности по обнаружению целей, корректировке огня и оценке нанесенного урона просто несравнимы с теми, что существовали

1 Падишин Сергей Александрович, кандидат военных наук, доцент, профессор кафедры Военной академии связи, г. Санкт-Петербург, Россия. E-mail: chesstar@mail.ru

2 Вольхин Сергей Дмитриевич, адъюнкт Военной академии связи, г. Санкт-Петербург, Россия. E-mail: volkhin21@mail.ru

еще 10 лет назад, что резко повышает эффективность применения даже неуправляемых боеприпасов, не говоря уж об управляемых средствах.

Приходится констатировать, что на текущем технологическом этапе развития средств технической разведки ведущих зарубежных государств жизненной необходимостью стала разработка разведзащищенных средств и режимов работы оборудования, постоянного проведения мероприятий обеспечения живучести элементов системы и войск связи, создании ложных объектов.

Опыт СВО показал, что требуется разработка более адаптивной, живучей и помехоустойчивой СС, учитывающей специфику современных боевых действий. Живучесть СС становится основным свойством, определяющим эффективное применение СС. Обеспечение живучести СС невозможно без грамотного планирования и выполнения мероприятий боевого обеспечения.

## Постановка задачи

Основным деструктивным воздействием на все элементы СС в ходе проведения операций группировкой войск, направленным на снижение ее устойчивости является комплексное огневое поражение противником – применение различных типов высокоточного оружия (ВТО), беспилотных систем (в частности беспилотных летательных аппаратов (БПЛА)), огневое поражение сил и средств артиллерии, действие диверсионно-разведывательных групп (ДРГ).

Показатели живучести СС должны сочетаться с требованиями по устойчивости, непрерывности, оперативности, мобильности и качества управления [4].

Для решения этих задач требуется научно-методический аппарат, позволяющий осуществлять моделирование огневого воздействия противника на протяжении всего периода боевых действий. В широком смысле вероятность успешного функционирования элементов СС группировки войск в ходе боевых действий и активного воздействия, возможна если элемент системы не обнаружен противником, или обнаружен, но не поражен огневыми средствами с достаточной степенью (выражение 1).

$$P_{\text{функ}_i}(t_{\text{эо}}) = (1 - P_{\text{расп}_i}(t_{\text{эо}})) + P_{\text{расп}_i}(1 - P_{\text{пор}}(t_{\text{эо}})). \quad (1)$$

Количественной мерой живучести элемента системы связи является вероятность его выживания (живучесть), то есть вероятность того, что в случае воздействия по нему соответствующего поражающего фактора он сохранит работоспособность.

Исходя из этого разработанная комплексная модель включает частные математические модели вероятности распознавания элементов системы связи и расчета их живучести.

## Решение задачи

Процесс вскрытия (распознавания) элемента системы разведкой противника во времени можно сформулировать как совокупность случайных событий (добывания, обработки, анализа разведданных об объекте от различных видов разведки, принятия решения на организацию воздействия или доразведку). Для оценки разведзащищенности элементов СС определены наиболее эффективные для противника виды разведки (рис. 3) и безусловная вероятность распознавания, основанная на информативности демаскирующих признаков (формула 2).

$$P_{\text{расп}_i}(\bar{t}) = 1 - (1 - P_{\text{распРР}}(t))(1 - P_{\text{распОР}}(t)) \times \\ \times (1 - P_{\text{распИКР}}(t))(1 - P_{\text{распСР}}(t)). \quad (2)$$

где: $P_{\text{расп}_i}(\bar{t})$ – безусловная вероятность распознавания; $P_{\text{распРР}}$ – вероятность распознавания радиоразведкой; $P_{\text{распИКР}}$ – вероятность распознавания ИКР; $P_{\text{распОР}}$ – вероятность распознавания оптической разведкой; $P_{\text{распСР}}$ – вероятность распознавания войсковой специальной разведкой.

Проведена классификация информативности демаскирующих признаков по видам разведки (табл. 1).

Для каждого из рассмотренных видов разведки сформулированы и обобщены основные мероприятия по снижению информативности ДМП (выражение 3) [7].

$$P_{\text{РЗДМП}} = \sum_{i=1}^{N} K_{\text{ВМ}i}\delta_{ji} \le 1, \quad (3)$$

где: $K_{\text{ВМ}}$ – коэффициент важности мероприятия по снижению информативности ДМП; $\delta_{ji}$ – показатель выполнения мероприятий по снижению ДМП (1 – выполнено, 0 – не выполнено) у $j$-го объекта $i$-го ДМП.

Расчёт условной вероятности распознавания элементов СС можно в общем виде можно описать экспоненциальным законом противодействия с учетом фоновой открытости района разведки (выражение 4).

$$P_{\text{расп}_i}(\bar{t}) = 1 - e^{\frac{(1 - P_{\text{РЗДМП}})}{(1 - P_{\text{распЭл}})} C_{фот}}. \quad (4)$$

После оценки выполненных мероприятий проведены расчёты вероятности распознавания элемента СС.

Вероятность противодействия рассчитывается при условии выполнения максимально возможных мероприятий снижения информативности демаскирующих признаков.

DOI: 10.21681/3034-4050-2026-2-81-88

Таблица 1

| Виды разведки, наиболее эффективные для вскрытия элементов опорной сети связи | Демаскирующие признаки | Мероприятия по снижению демаскирующих признаков (способы повышения разведывательной защищённости) | Эффект | Ресурсопотребление (затраты) | Необходимый для выполнения ресурс, n * t (чел * час) | Необходимый для выполнения ресурс, s (тыс. усл. ед.) | Коэффициент важности мероприятия, Квы | Отметка о выполнении | Вероятность вскрытия за демаскирующий признак, $P_{вскрДИ}$ | Вероятность вскрытия за вид разведки, $P_{вскрВР}$ |
|---|---|---|---|---|---|---|---|---|---|---|
| Радио разведка | Радиоизлучение средств связи | Работа с минимальной мощностью излучающих средств, сокращение расстояний интервалов РРЛ, увеличение количества | средний | среднее | 2 | 500 | 0,2 | 1 | | |
| | | Применение направленных антенн | средний | не требуется | - | - | 0,2 | 1 | | |
| | | Работа на минимально поднятых антеннах (высота подъёма не более 10 м) | средний | не требуется | 2 | 500 | 0,2 | 1 | | |
| | | Созданием ложных УС с имитацией работы радиоэлектронных средств | высокий | max высокое | 1 | 500 | 0,2 | 1 | | |
| | | Изменение диаграмм направленности антенн за счёт увеличения количества интервалов и РТП | средний | высокое | 2 | 500 | 0,2 | 1 | | |
| | | Своевременная смена районов размещения УС | средний | высокое | 4 | - | 0 | 1 | | |
| Итого за вид разведки | | | | | 11 | 2000 | | | 0,01 | 0,01 |
| Видовая оптическая разведка | Высокие массо-габаритные показатели аппаратных и станций (наличие в составе УС аппаратных на АБШ с КУНГ) | Применение переносных (мобильных) средств с меньшими линейными размерами | высокий | среднее | - | 1700 | 0,3 | 1 | | |
| | | Покраска аппаратных и станций в соответствии с ФГУ и временем года | низкий | низкое | 1 | 3,5 | 0,1 | 1 | | |
| | | Применение табельных средств маскировки | низкий | высокое | 1 | - | 0,1 | 0 | | |
| | | Инженерное оборудование района размещения УС (применение укрытий котлованного типа) | средний | высокое | 21,5 | 12 | 0,2 | 0 | | |
| | | ИЛИ (вместо п. 3,4) размещение элементов УС на территориях заводов, складов, предприятий внутри зданий, цехов | высокий | не требуется | - | - | 0,3 | 1 | | |
| | | Созданием ложных УС (антенны, надувные аппаратные под тентом) | высокий | высокое | 2 | 1000 | 0,3 | 1 | | |
| | Итого за разведывательный признак | | | | 25,5 | 2715,5 | | | 0,01 | |
| | Наличие ятенно-мачтовых устройств (АМУ) | Работа на минимально поднятых антеннах (высота подъёма не более 10 м) | низкий | не требуется | 2 | 500 | 0,1 | 1 | | |
| | | Применение АМУ в невоенном исполнении | средний | низкое | - | 1,5 | 0,3 | 1 | | |
| | | Применение радиопрозрачных покрытий для маскировки АМУ, маскировка АМУ под рельеф местности | высокий | среднее | 0,5 | 1 | 0,6 | 1 | | |
| | Итого за разведывательный признак | | | | 2,5 | 502,5 | | | 0,01 | |
| | Перемещение техники | Перемещение УС с учетом маскирующих свойств местности | средний | не требуется | - | - | 0,4 | 1 | | |
| | | Максимальное сокращение времени перемещения УС | низкий | не требуется | - | - | 0,3 | 1 | | |
| | | Максимальное сокращение времени развёртывания УС | низкий | не требуется | - | - | 0,3 | 1 | | |
| | Итого за разведывательный признак | | | | 0 | 0 | | | 0,01 | |
| | Наличие обслуживающего персонала, следов жизнедеятельности | Строгая регламентация действий обслуживающего персонала | низкий | не требуется | - | - | 0,1 | 1 | | |
| | | Проведение мероприятий по легендированию (переодевание личного состава, использование гражданской техники подвоза) | средний | низкое | 0,5 | 3570 | 0,3 | 1 | | |
| | | Дистанционное управление функционированием оборудования | высокий | среднее | 0,5 | 1700 | 0,6 | 1 | | |
| | Итого за разведывательный признак | | | | 1 | 5270 | | | 0,01 | |
| Итого за вид разведки | | | | | 29 | 8488 | | | | 0,03940399 |
| Видовая оптическая разведка в инфракрасном диапазоне | Наличие нагревательных элементов в аппаратуре связи, излучение тепла | Охлаждение нагревающихся элементов аппаратуры связи | средний | низкое | - | 1 | 0,3 | 1 | | |
| | | Применение теплоотражающих экранов | средний | низкое | 1 | 0,5 | 0,4 | 1 | | |
| | | Размещение на ложных УС тепловых ловушек | средний | низкое | 0,5 | 0,5 | 0,3 | 1 | | |
| | Итого за разведывательный признак | | | | 1,5 | 2 | | | 0,01 | |
| | Наличие тепловых контуров источников непрерывного электропитания (применение электроагрегатов) | Применение теплоотражающих экранов | средний | низкое | 0,5 | 0,25 | 0,3 | 1 | | |
| | | Применение промышленного электропитания | высокий | низкое | 0,5 | 40 | 0,4 | 1 | | |
| | | Применение ИБП (солнечных батарей) | средний | низкое | 0,5 | 100 | 0,3 | 1 | | |
| | Итого за разведывательный признак | | | | 1,5 | 140,25 | | | 0,01 | |
| | Наличие обслуживающего персонала | Строгая регламентация действий обслуживающего персонала | низкий | низкое | - | - | 0,1 | 1 | | |
| | | Применение теплоотражающих экранов | средний | среднее | 1 | 0,5 | 0,4 | 1 | | |
| | | Оборудование блиндажей для личного состава экипажей | средний | среднее | 21,5 | 12 | 0,5 | 1 | | |
| | | ИЛИ (вместо п. 2,3) дистанционное управление функционированием оборудования | высокий | среднее | 0,5 | 1700 | 0,9 | 0 | | |
| | Итого за разведывательный признак | | | | 23 | 1712,5 | | | 0,01 | |
| Итого за вид разведки | | | | | 26 | 1854,75 | | | | 0,029701 |
| Радиолокационная разведка | Высокие массо-габаритные показатели аппаратных и станций (наличие в составе УС аппаратных на АБШ с КУНГ) | Применение переносных (мобильных) средств с меньшими линейными размерами | средний | среднее | - | 1700 | 0,3 | 1 | | |
| | | Применение уголковых отражателей, ложных объектов | низкий | среднее | 2 | 15 | 0,2 | 1 | | |
| | | Применение табельных средств маскировки | низкий | низкое | 1 | - | 0,2 | 0 | | |
| | | Инженерное оборудование района размещения УС (применение укрытий котлованного типа) | средний | низкое | 21,5 | 12 | 0,3 | 0 | | |
| | | ИЛИ (вместо п. 3,4) размещение элементов УС на территориях заводов, складов, предприятий внутри зданий, цехов | высокий | низкое | - | - | 0,5 | 1 | | |
| | Итого за разведывательный признак | | | | 24,5 | 1727 | | | 0,01 | |
| | Перемещение техники | Перемещение УС с учетом маскирующих свойств местности | средний | низкое | - | - | 0,4 | 1 | | |
| | | Максимальное сокращение времени перемещения УС | низкий | низкое | - | - | 0,3 | 1 | | |
| | | Максимальное сокращение времени развёртывания УС | низкий | низкое | - | - | 0,3 | 1 | | |
| | Итого за разведывательный признак | | | | 0 | 0 | | | 0,01 | |
| Итого за вид разведки | | | | | 24,5 | 1727 | | | | 0,0199 |
| Войсковая специальная разведка | Высокие массо-габаритные показатели аппаратных и станций | Применение переносных (мобильных) средств с меньшими линейными размерами | низкий | среднее | - | 1700 | 0,2 | 1 | | |
| | | Применение табельных средств маскировки | низкий | высокое | 1 | - | 0,2 | 0 | | |
| | | Инженерное оборудование района размещения УС (применение укрытий котлованного типа) | средний | высокое | 21,5 | 12 | 0,3 | 0 | | |
| | | ИЛИ (вместо п. 2,3) размещение элементов УС на территориях заводов, складов, предприятий внутри зданий, цехов | высокий | высокое | - | - | 0,5 | 1 | | |
| | | Создание ложных УС (антенны, надувные аппаратные под тентом) | средний | высокое | 2 | 1000 | 0,3 | 1 | | |
| | Итого за разведывательный признак | | | | 24,5 | 2712 | | | 0,01 | |
| | Наличие характерного звука от источников непрерывного электропитания (применение электроагрегатов) | Применение промышленного электропитания, ИБП | низкий | низкое | 0,5 | 100 | 0,2 | 1 | | |
| | | Применение нештатных малошумящих АБ (ЭД) | высокий | низкое | - | 20 | 0,5 | 1 | | |
| | | Оборудование заглубленных мест размещения АБ (ЭД), применение шумопоглощающих экранов | средний | низкое | 0,5 | 2 | 0,3 | 1 | | |
| | Итого за разведывательный признак | | | | 1 | 122 | | | 0,01 | |
| | Наличие характерных АМУ | Работа на минимально поднятых антеннах (высота подъёма не более 10 м) | низкий | не требуется | 2 | 500 | 0,1 | 1 | | |
| | | Применение АМУ в невоенном исполнении | средний | низкое | - | 1,5 | 0,3 | 1 | | |
| | | Применение радиопрозрачных покрытий для маскировки АМУ, маскировка АМУ под рельеф местности | высокий | среднее | 0,5 | 1 | 0,6 | 1 | | |
| | Итого за разведывательный признак | | | | 2,5 | 502,5 | | | 0,01 | |
| | Наличие следов жизнедеятельности (мусор, следы костров, тропинки, колеи от машин, вырубка леса, выкопка грунта), обслуживающего персонала | Проведение мероприятий по легендированию (переодевание личного состава, использование гражданской техники подвоза) | средний | низкое | 0,5 | 3570 | 0,3 | 1 | | |
| | | Дистанционное управление функционированием оборудования | высокий | среднее | 0,5 | 1700 | 0,6 | 1 | | |
| | | Строгая регламентация действий обслуживающего персонала | низкий | низкое | - | - | 0,1 | 1 | | |
| | Итого за разведывательный признак | | | | 1 | 5270 | | | 0,01 | |
| Итого за вид разведки | | | | | 29 | 8606,5 | | | | 0,03940399 |
| Итого за все виды разведки | | | | | 119,5 | 22676,25 | | | | |

Условная вероятность (вероятность распознавания в различных условиях) распознавания элемента в динамике операции (рис. 4) при выполнении мероприятий разведзащищенности и без их выполнения.

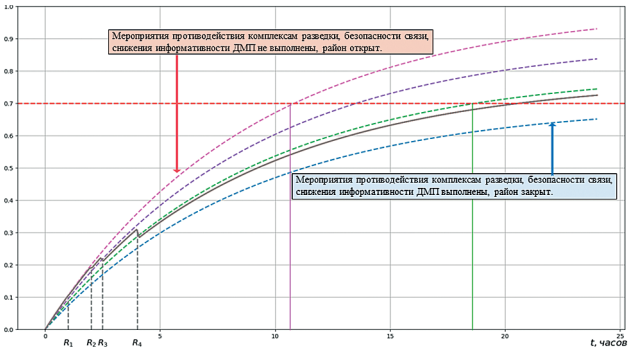



*Рис. 4. Вероятность распознавания элементов сети радиосвязи*

На графике розовым цветом показана вероятность вскрытия элемента СС без выполнения мероприятий по повышению разведзащищенности и полной открытости района разведки средствам разведки, синим цветом – вероятность распознавания элемента при выполнении всего комплекса мероприятий и использовании закрытого района средствам разведки.

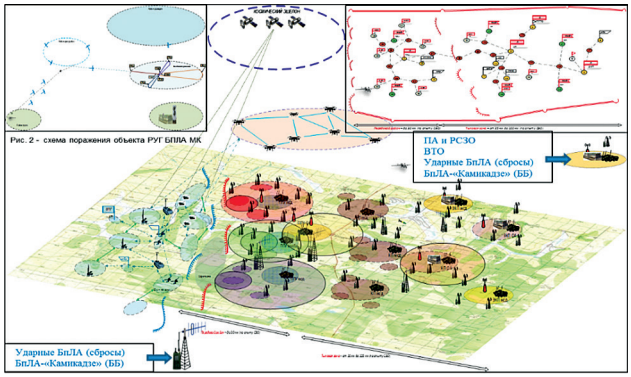



*Рис. 5. Пространственная схема огневого поражения элементов системы связи*

Для оценки живучести элементов СС в операции ГрВ в изменившихся условиях ведения боевых действий и развития средств огневого поражения разработана пространственная схема характера действий противника огневого поражения элементов системы связи.

Проведенный анализ огневого воздействия на элементы СС в зоне ответственности ГрВ показал, что наиболее вероятным вариантом поражения будут [9]:

- артиллерийские системы и РСЗО с применением как обычных, так и высокоточных боеприпасов;
- высокоточное оружие в ракетном исполнении (типа «Himars»);
- ударные БПЛА малого класса;
- БПЛА – «Камикадзе», барражирующие боеприпасы.

Для проведения расчетов вероятности поражения элементов системы связи в реальных условиях (условной вероятности) разработаны структурные графы процессов поражения каждым видом оружия с учетом развития средств поражения и изменившимися условиями применения (рис. 6–9).

В качестве показателя живучести элемента сети радиосвязи от воздействия средств огневого поражения противника целесообразно применить вероятность его защищенности (выражениями 6–8).

$$P_{\text{защ}_i} = 1 - (1 - P^{\text{ф}}_{\text{защ}})(1 - P^{\text{м}}_{\text{защ}})(1 - P^{\text{р}}_{\text{защ}}), \qquad (6)$$

где $P_{\text{защ}}$ – вероятность защищенности элемента сети; $P^{\text{ф}}_{\text{защ}}$ – вероятность физической защищенности; $P^{\text{м}}_{\text{защ}}$ – вероятность маскировки; $P^{\text{р}}_{\text{защ}}$ – вероятность рассосредоточения объектов в пределах элемента сети.

$$P^{\text{ф}}_{\text{защ}} = 1 - (1 - P^{\text{акт}}_{\text{защ}})(1 - P^{\text{пас}}_{\text{защ}}), \qquad (7)$$

где $P^{\text{пас}}_{\text{защ}}$ – уровень пассивной защиты; $P^{\text{акт}}_{\text{защ}}$ – уровень активной защиты.

$$P^{\text{р}}_{\text{защ}} = \frac{\rho_{\text{н}}}{\rho_{\text{об}}}, \qquad (8)$$

где $\rho_{\text{н}}$ – нормативная плотность размещения объектов на элементе; $\rho_{\text{факт}}$ – фактическая плотность размещения объектов на элементе.

Физическая защищенность ($K^{\text{ф}}_{\text{защ}}$) является одной из важнейших характеристик живучести и определяет возможности по активной и пассивной защите от возможного воздействия противника.

Активная защита обеспечивается организацией и осуществлением мероприятий по охране и обороне, а также противовоздушной обороны (ПВО) объекта в районах размещения.

Пассивная защита объектов в районе размещения обеспечивается наличием и состоянием защитных сооружений для личного состава, средств, техники и АМУ, созданием и инженерным оборудованием зон рассредоточения. Элементы СС располагают различными средствами пассивной защиты, а, следовательно, и различными уровнями живучести:

Для определения живучести элемента важно оценивать проводимые мероприятия по рассредоточению элементарных объектов в районе

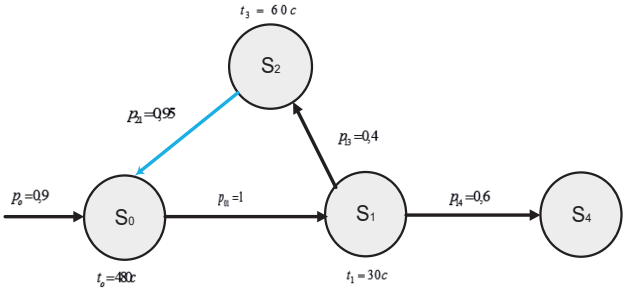



*Рис. 6. Структурный граф процесса поражения элементов сети радиосвязи группами артиллерии*

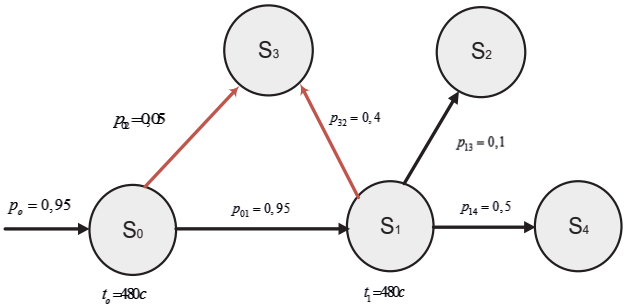



*Рис. 7. Структурный граф процесса поражения элементов сети радиосвязи ВТО*

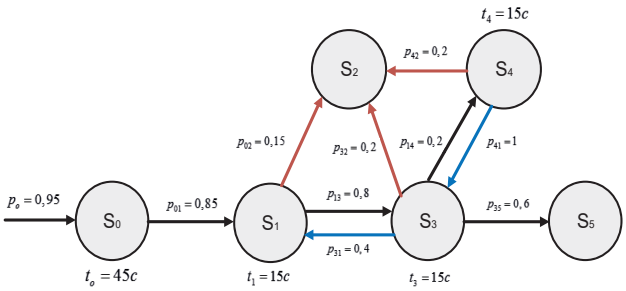



*Рис. 8. Структурный граф процесса элементов сети радиосвязи группой ударных БПЛА МК*

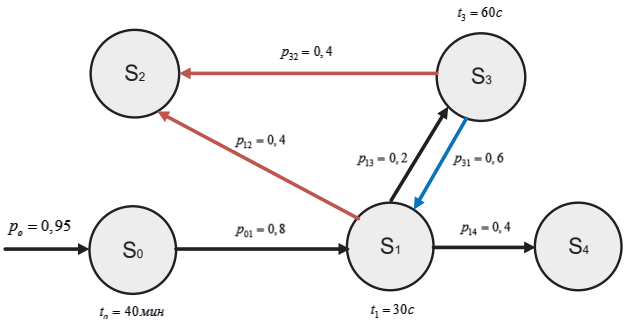



*Рис. 9. Структурный граф процесса поражения элементов сети радиосвязи БПЛА «Камикадзе» (ББ)*

размещения. Очевидно, что чем ниже плотность расположения элементарных объектов, тем выше живучесть элементов СС при одном и том же огневом воздействии противника. Однако существуют определенные пределы минимальных значений плотности расположения элементарных объектов в районе, которые определяются оперативно-тактическими требованиями.

Для комплексного удовлетворения оперативно-тактических требований и требований живучести рассчитываются значения нормативной плотности размещения элементарных объектов элемента СС с учетом физико-географических, климатических, инфраструктурных условий базирования.

Исходя из того, что элементы радиосвязи будут интенсивнее поражаться и деструктивное воздействие в ходе поражения будет сильнее без выполнения мероприятий по обеспечению живучести, и наоборот, то условную вероятность поражения элемента сети целесообразно рассчитывать выражением 9.

$$P_{\text{оп}_i}(\bar{t}) = 1 - e^{-\frac{(1-P_{\text{защ}_i})}{(1-P_{\text{оп}_i})}t}. \qquad (9)$$

Проведенные расчеты показывают, что организацией и комплексным применением мероприятий по обеспечению живучести элементов

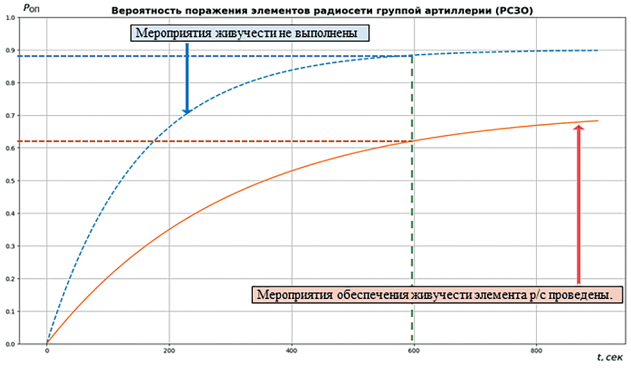



*Рис. 10. График поражения элементов СС группой артиллерии*

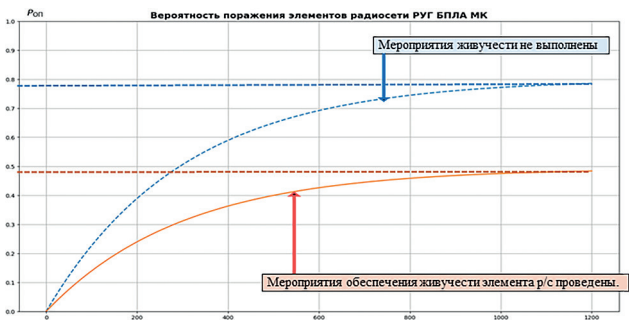



*Рис. 11. График поражения элементов ССРУГ БПЛА МК*

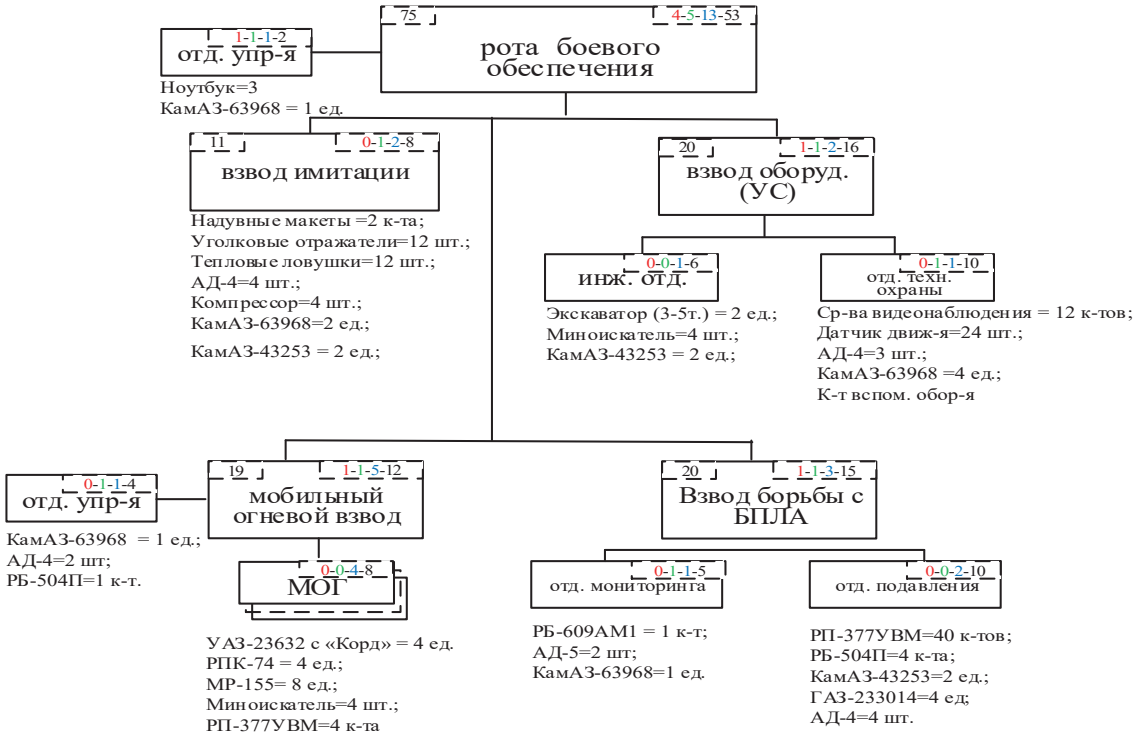



*Рис. 12. Организационно-штатная структура роты боевого обеспечения бс(ПУ)*

системы связи, подразделения связи в состоянии уменьшить вероятность огневого поражения элемента на 15–25 %.

Опыт СВО показывает, что воинские части и подразделения родов войск и специальных войск оперативных объединений, прежде всего радиоэлектронной борьбы, войск ПВО, инженерных войск (зрбр, исп, об РЭБ общевойскового объединения) в настоящее время не могут обеспечить требуемый уровень живучести элементов СС, как одной из составляющей системы управления, ввиду увеличения количества прямых задач по предназначению и значительного увеличения элементов СС (УС, ОУС, РТП, УСД и т.д.). Перечисленные факторы обусловили необходимость включения в организационную-штатную структуру соединений и воинских частей связи подразделений боевого обеспечения, и в первую очередь подразделений, обеспечивающих маскировку, инженерное оборудование районов развертывания элементов системы связи, защиту от БПЛА.

Для решения задач обеспечения живучести элементов СС объединения предлагается включить в состав 1,2 батальонов связи (бс (ПУ)) бригады управления (бру) общевойсковой (танковой) армии роты боевого обеспечения. К рассмотрению предлагается следующий состав и техническое оснащение (как один из вариантов) роты боевого обеспечения бс (ПУ) бру (рис. 1).

На роту боевого обеспечения возлагается развертывание ложных элементов СС (отдельных аппаратных и станций), мониторинг частотной обстановки в районах развертывания узлов связи, техническое оборудование элементов СС (УС ПУ, ОУС, УСД) в системе охраны и обороны, борьба с БПЛА техническими и огневыми средствами.

Взвод имитации предназначен для развертывания и обеспечения 1-2 ложных УС ППУ или элементов УС КП (ЗКП) общевойскового объединения, а также выполнения мероприятий радиоэлектронной защиты на узлах связи. Комплект надувных макетов должен включать реально применяемые аппаратные, станции, средства связи. Пример содержания комплектов представлен в таблице 2.

*Таблица 2.*

| Аппаратная, стация | Состав комплекта | |
|---|---|---|
| | Вариант 1 | Вариант 2 |
| АПЕ-5 | 1-2 | |
| Р-149МА | | 1 |
| Р-177 | 1 | |
| П-230Т | 2 | 2 |
| П-243 | 1 | 1 |
| П-240-И5(7) | 1 | |
| Р-448ТН | 2 | 2 |
| Р-444НЛ, НМ, ПТН | 4 | 4 |

Взвод оборудования (УС) предназначен для обеспечения охраны УС ПУ техническими средствами, частичного оборудования позиций размещения аппаратных и станций, скрытия проводных (оптико-волоконных) линий связи.

Мобильный огневой взвод предназначен для огневого поражения БПЛА в районах УС ПУ, РТП, УСД, обороны узлов, обеспечения рекогносцировки районов развертывания элементов СС, сопровождения колонн техники связи, групп обслуживания ретрансляторов.

Взвод борьбы с БПЛА предназначен для мониторинга радиоэлектронной обстановки в районе узла связи, защиты аппаратных и станций в ходе маршей (обеспечение и установка на транспортные средств комплексами РБ-377П), радиоэлектронного подавления каналов управления БПЛА противника в районах развертывания элементов СС.

Имеющимися силами и средствами рота боевого обеспечения способна:

- развернуть элементы ложного УС ППУ и КП (ЗКП) армии (2-х положений УС ППУ);
- развернуть систему видеонаблюдения на 2-3 УС ППУ, КП(ЗКП) армии;
- обеспечить мониторинг радиоэлектронной обстановки в районе УС ППУ, КП (ЗКП) армии применением РБ-609АМ1 (Свет-КУ);
- обеспечить до 40 ед. ВВТ средствами обнаружения БПЛА и противодействия каналам управления минно-взрывных устройств на радиоуправлении применением РП-377УВМ;
- подавления каналов управления БПЛА в четырех районах развертывания УС в радиусе 3 км с использованием РБ-504П;
- огневое поражение БПЛА в районах УС ППУ и КП армии.

## Заключение

Разработанная модель огневого воздействия противника позволяет спрогнозировать и оценить потенциальный ущерб, который будет нанесен системе в ходе операции.

В качестве результатов использования модели появляется возможность:

- выявить потенциальный ущерб воздействия противника и определить наиболее опасные средства огневого поражения;
- разработать структуру системы связи в операции, обеспечивающую лучшую эффективность по показателю живучести;
- определить необходимость применения тех, или иных способов активной или пассивной защиты элементов системы связи.

Модель функционирования СС ГрВ, проведенные расчеты и опыт СВО определили необходимость применения новых способов развертывания элементов системы связи, принятия мер обмана противника, тщательного планирования и неукоснительного выполнения мероприятий маскировки, охранения, инженерного оборудования, что предполагает выполнение целого перечня работ, с привлечением личного состава, расходованием материальных средств и ресурсов.

## Литература


1. Киселев А. В., Макаренко С. И. Анализ боевого потенциала сторон в конфликте средств огневого поражения противника и средств войсковой противовоздушной обороны // Системы управления, связи и безопасности. 2022. № 1. С. 8–48.
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 В. Г. Иванов – Спб: ПОЛИТЕХ-ПРЕСС, 2023. – 300 с.
3. Тевс О. П., Пустошкин М. М. Моделирование тактики подразделений связи в условиях современного вооруженного противоборства // Телекоммуникации и связь. 2024. № 3. С. 5–12. DOI: 10.21681/3034-4050-2024-3-5-12.
4. Корепанов В. О., Шумов В. В. Моделирование военных, боевых и специальных действий // Военная мысль. 2023. № 1. – С. 28–41.
5. Тевс О. П., Исаченко В. Г. Особенности и выводы организации и обеспечения связи при проведении специальной военной операции // Итоги науки и техники: научно-технический сборник № 120. Труды академии. – СПб.: ВАС, 2022. С. 64–70.
6. Пустошкин М. М., Степынин Д. В., Филимоненков М. Х., Васильева Т. Г., Ульянов В. В. Направления развития вооруженной борьбы, влияющие на тактику войск связи // Научно-практический междисциплинарный журнал: «Стратегическая стабильность» № 4(109). – 2024. С. 37–40.
7. Пустошкин М. М., Анализ тактики применения соединений (воинских частей, подразделений) связи в условиях современного вооруженного противоборства // Сборник научных трудов III международной научно-практической конференции: Карбышевские чтения «Наше дело правое – победа будет за нами», т. 6 – Тюмень.: ТВВИКУ, 2024. стр. 62–67.
8. Скуридин А. Е. Программа расчета защищенности элементов сети связи специального назначения, их живучести и сравнительной оценки устойчивости функционирования сети связи специального назначения с использованием логико-вероятностного метода. Свидетельство о государственной регистрации программы для ЭВМ № 2025611173 от 16.01.2025 г.

# INCREASING THE SURVIVABILITY OF THE ELEMENTS OF THE COMMUNICATION SYSTEM OF THE GROUPING OF TROOPS DURING THE IMPLEMENTATION OF COMBAT SUPPORT MEASURES FOR THE SIGNAL TROOPS

***Padishin S. A.[1], Volkhin S. D.[2]***

***Keywords:*** *effectiveness, impact model, reconnaissance protection, fire damage, communication system, control system.*

***Abstract***

***The purpose of the work*** *on the basis of the analysis and generalization of the initial data, using the model of the enemy's fire impact, to formulate the main directions and develop measures for the combat support of the system and signal troops that provide the necessary survivability of the elements of the communication system (SS) in modern armed confrontation.*

***The research method*** *is based on the development of complex analytical and simulation models that assess the processes of uncertainty and multifaceted nature of warfare.*

***The results of the study*** *will make it possible to assess the possible damage to the elements of the communication system of the grouping of forces as a result of the integrated fire impact of enemy reconnaissance and strike systems, to develop a set of measures for the main types of combat support, the implementation of which will increase the survivability of both an individual element and the communication system as a whole. Using the created model of fire impact on the elements of the communication system in a modern armed conflict, an innovative method of synthesizing combat support measures that ensure an increase in the survivability of the communication system is proposed. The updated approach makes it possible to predict the expected damage to the elements of the system caused in a dynamically changing operational situation and the complex fire impact of the enemy.*

***The results*** *of the simulation determine the scientifically based requirements for the organizational and staff structures of formations and communication (control) units in order to carry out survivability measures. The results will be used as the basis for proposals for the creation and implementation of combat support units and tactics for their use. The key aspect of the methodology was the introduction of mathematical modeling algorithms capable of reproducing a set of probabilistic events, reconnaissance (acquisition, processing, analysis of intelligence data about an object from various types of reconnaissance, additional reconnaissance) of the elements of the communication system, decision-making to destroy them, the choice of fire weapons and its use.*

***Practical value:*** *the proposed approach makes it possible to predict the expected damage to the elements of the system caused in a dynamically changing operational situation and the complex fire impact of the enemy. This provides an analytical basis for assessing the survivability of the elements of the communication system; predicting critical elements; formulating protection measures; creating and using survivability resources.*

## References

1. Kiselev A. V., Makarenko S. I. Analiz boevogo potenciala storon v konflikte sredstv ognevogo porazhenija protivnika i sredstv vojskovoj protivovozdushnoj oborony // Sistemy upravlenija, svjazi i bezopasnosti. 2022. № 1. S. 8–48.
2. Ivanov V. G. Osnovy postroenija i ocenki jeffektivnosti funkcionirovanija sistemy svjazi special'nogo naznachenija v mezhdunarodnom vooruzhennom konflikte na osnove mnogosfernoj i konvergentnoj struktury ee jelementov // monografija V. G. Ivanov – Spb: POLITEH-PRESS, 2023. 300 s.
3. Tevs O. P., Pustoshkin M. M. Modelirovanie taktiki podrazdelenij svjazi v uslovijah sovremennogo vooruzhennogo protivoborstva // Telekommunikacii i svjaz'. 2024. № 3. S. 5–12. DOI: 10.21681/3034-4050-2024-3-5-12.
4. Korepanov V. O., Shumov V. V. Modelirovanie voennyh, boevyh i special'nyh dejstvij // Voennaja mysl'. 2023. № 1. – S. 28–41.
5. Tevs O. P., Isachenko V. G. Osobennosti i vyvody organizacii i obespechenija svjazi pri provedenii special'noj voennoj operacii // Itogi nauki i tehniki: nauchno-tehnicheskij sbornik № 120. Trudy akademii. – SPb.: VAS, 2022. S. 64–70.
6. Pustoshkin M. M., Stepynin D. V., Filimonenkov M. H., Vasil'eva T. G., Ul'janov V. V. Napravlenija razvitija vooruzhennoj bor'by, vlijajushhie na taktiku vojsk svjazi // Nauchno-prakticheskij mezhdisciplinarnyj zhurnal: «Strategicheskaja stabil'nost'» № 4(109). – 2024. S. 37–40.
7. Pustoshkin M. M., Analiz taktiki primenenija soedinenij (voinskih chastej, podrazdelenij) svjazi v uslovijah sovremennogo vooruzhennogo protivoborstva // Sbornik nauchnyh trudov III mezhdunarodnoj nauchno-prakticheskoj konferencii: Karbyshevskie chtenija «Nashe delo pravoe – pobeda budet za nami», t. 6 – Tjumen'.: TVVIKU, 2024. str. 62–67.
8. Skuridin A. E. Programma rascheta zashhishhennosti jelementov seti svjazi special'nogo naznachenija, ih zhivuchesti i sravnitel'noj ocenki ustojchivosti funkcionirovanija seti svjazi special'nogo naznachenija s ispol'zovaniem logiko-verojatnostnogo metoda. Svidetel'stvo o gosudarstvennoj registracii programmy dlja JeVM № 2025611173 ot 16.01.2025 g.

1 Sergey A. Padishin, Ph.D. of Military Sciences, Associate Professor, Professor of the Department of the Military Academy of Communications, St. Petersburg, Russia. E-mail: chesstar@mail.ru

2 Sergey D. Volkhin, Adjunct of the Military Academy of Communications, St. Petersburg, Russia. E-mail: volkhin21@mail.ru

# ОПТИМИЗАЦИЯ РЕЖИМА СБОРА ИНФОРМАЦИИ С ПОМОЩЬЮ БПЛА НА РАСПРЕДЕЛЕНЫХ НАЗЕМНЫХ СЕТЯХ ИЗМЕРИТЕЛЬНЫХ ДАТЧИКОВ

***Асадов Х. Г.[1], Ахмедов Э. М.[2]***

**DOI:10.21681/3034-4050-2026-2-89-93**

***Ключевые слова:*** *скорость съёма информации, шумы в канале, гауссовский белый шум, вариационная оптимизация, ограничительное условие.*

***Аннотация***

***Целью исследования*** *является оптимизации режима сбора информации с помощью БПЛА с датчиков наземных измерительных сетей и анализ возможности увеличения скорости передачи данных от наземных датчиков к БПЛА.*

***Метод исследования:*** *использован метод безусловной вариационной оптимизации.*

***Результат:*** *сформулирована и решена задача оптимизации сбора данных от кластеризованных наземных датчиков с использованием группы БПЛА. На основе предположения о наличии некоторой зависимости между интенсивностью белого гауссовского шума в канале приема БПЛА и ширины полосы пропускаемых частот этого же канала, а также наложив на указанную зависимость определенного интегральное ограничения, был построен целевой функционал безусловной вариационной оптимизации. В результате применением метода Эйлера для решения оптимизационной задачи показано, что скорость сбора информации может достичь максимума при наличии прямой линейной зависимости между шириной частотный полосы канала приема данных БПЛА и интенсивностью белого гауссовского шума в канале приема.*

***Научная новизна и практическая ценность*** *заключается в выявлении дополнительной возможности для увеличения скорости съёма информации с наземных датчиков с применением БПЛА при наличии некоторого режимного ограничения на функцию взаимосвязи между шириной частотный полосы канала приема данных и интенсивностью гауссовского белого шума в канале приема.*

## Введение

Как отмечается в работе [1] БПЛА предназначены для выполнения широкого класса задач в таких сферах как аэрофоторазведка, военные деле, обнаружение цели, контроль состояния трубных линий и линий электропередачи, георазведка, сельское хозяйство, доставка товаров. Одной из таких сфер применение БПЛА является мониторинг пожарной опасности в лесах [2]. Функционально, во многих применениях БПЛА в целях мониторинга, работа беспилотных устройств сводится к сбору информации с датчиков определенные распределенной сети измерительных преобразователей, распределённых по полю контроля состояния объекта. Как указано в работе [3], согласно прогнозам, к 2030 году количество датчиков во всем мире достигнет сотни миллиардов. Следовательно, сбор и обработка такого большого объема информации требует проведения работ по усовершенствованию систем сбора и предобработки информации.

Согласно [4] применение БПЛА для сбора данных для интернета вещей даст следующие преимущества:

- высокую эффективность, гибкость при сборе информации: БПЛА позволяет существенно уменьшить время сбора информации т.к. траектория полета может быть оптимизирована [5–7];
- малое энергопотребление и возможность обеспечения датчиков энергией без проводов [8, 9];
- широкое поле схвата. При большой высоте полета БПЛА появляется возможность охватить большой участок объекты в котором расположены датчики [10, 11].

Вместе с тем особый порядок расположения датчиков на участке диктуют необходимость выбора специальной траектории полета, а также повышение эффективности сбора информации с наземных датчиков.

Модельное представление сети, в которой группа БПЛА осуществляют сбор и передачу информации в базовую станции приведено на рисунке 1.

Как отмечено в работе [4] в системе используется канал связи типа LoS (линия передачи данных по прямой линии видимости). Вероятность успеха передачи данных по такой линии связи вычисляется по формуле

1 Асадов Хикмет Гамид оглы, доктор технических наук, профессор, Национальное Аэрокосмическое Агентство, г. Баку, Азербайджанская Республика. E-mail: asadzade@rambler.ru

2 Ахмедов Эмиль Мехман оглы, аспирант, Национальное Аэрокосмическое Агентство, г. Баку. Азербайджанская Республика. E-mail: emil.ahmedov21@gmail.com

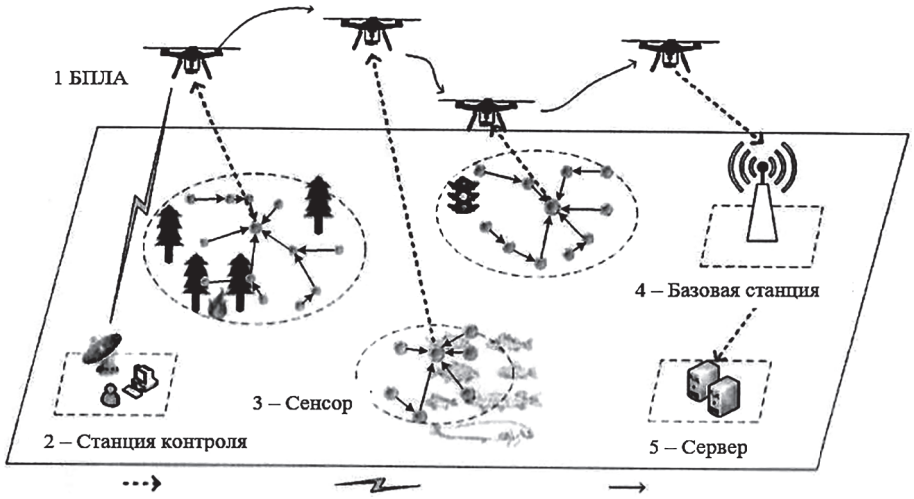



*Рис. 1. Модельное представление сбора информации группой БПЛА с наземных датчиков и передачи информации в базовый центр [4]*

$$P_{LOS}(S_{m,U}) = \frac{1}{1 + a\exp[-b\,(A(S_{m,U}) - a)]}, \quad (1)$$

где $A(S_{m,U})$ – угол между сенсорами $S_m$ и $m$, $m \in M$, $\alpha$ и $b$ – параметры окружающей среды, которые в основном зависят от насыщенности территории зданиями; а также от высоты зданий.

При этом скорость передачи данных от сенсора $S_m$ БПЛА определяется как [12]

$$R(S_{m,U}) = B \cdot \log_2\left(\frac{1 + |h|S_{m,U})|^2 P_m}{N_0}\right), \quad (2)$$

где $B$ – ширина полосы частот канала; $h(S_{m,U})$ – усиление канала между БПЛА и сенсором; $P_m$ – мощность передаваемого сигнала от сенсора к БПЛА; $N_0$ – мощность аддитивного Гаус---сового шума.

Целью настоящей работы является анализ возможности повышения $R$ путем оптимизации режима работы БПЛА.

## Материалы и методы

Допустим, что система сбора и передачи данных показанное на рисунке 1 кластеризована и приведено в вид, показанный на рисунке 2.

Допустим, что в канале связи $i$-го БПЛА существуют белые шумы с интенсивность $N_{0i}$. При этом $i = \overline{1,n}$.

Примем следующую модель $N_{0i}$

$$N_{0i} = N_{0i-1} + \Delta N_0$$

где $\Delta N_0 = \text{const}$

$$N_{0,0} = 0. \quad (3)$$

Отметим, что условие (3) подразумевает наличие упорядоченного множестве

$$N_0 = \{N_{0i}\}. \quad (4)$$

Также примем следующую модель множества $B$:

$$B_j = B_{j-1} + \Delta B, \text{ где } \Delta B = \text{const},$$

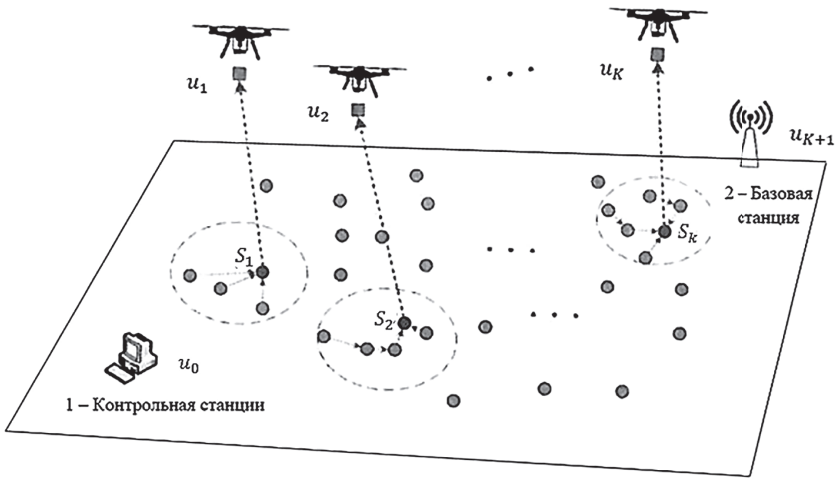



*Рис. 2. Система сбора и передачи данных с кластеризованных сенсоров с помощью БПЛА*

при $B_0 = 0; j = \overline{1,n}$.

Также подразумевается наличие упорядоченного множества

$$B = \{B_j\}. \quad (5)$$

Далее введем на рассмотрение следующий возможную функцию связи

$$N_i = \varphi(B_j). \quad (6)$$

С учетом (2), (5) и (6) составим следующую дискретную сумму

$$R_\Sigma = \sum_{j=1}^{n} B_j \cdot \log_2\left(\frac{1 + |h(S_{m,U})|^2 \cdot P_m}{\varphi(B_j)}\right). \quad (7)$$

Дискретный функционал (7) запишем в условной аналоговой форме.

$$R_\Sigma = \int_0^{B_{\max}} B \cdot \log_2\left[\frac{1 + |h(S_{m,U})|^2 \cdot P_m}{\varphi(B)}\right] dB. \quad (8)$$

Для нахождения оптимального вида функции $\varphi(B)$ наложим к этой функции следующее ограничительное условие

$$\int_0^{B_{\max}} \varphi(B)dB = C;\ C = const. \quad (9)$$

С учетом выражений (8) и (9) составим целевой функционал оптимизации $F$

$$F = \int_0^{B_{\max}} B \cdot \log_2\left[\frac{1 + |h(S_{m,U})|^2 \cdot P_m}{\varphi(B)}\right] dB + \lambda\left[+\int_1^{B_{\max}} \varphi(B)dB - C\right], \quad (10)$$

где $\lambda$ – множитель Лагранжа.

Решение оптимизационной задачи (10) согласно методу Эйлера-Лагранжа удовлетворяет условию

$$\frac{d\left\{B \cdot \log_2\left[\frac{1 + |h(S_{m,U})|^2 \cdot P_m}{\varphi(B)}\right] dB + \lambda \cdot \varphi(B)\right\}}{d\varphi(B)}. \quad (11)$$

Из условия (11) получаем

$$\frac{-B}{d\varphi(B)} + \lambda = 0. \quad (12)$$

Из выражения (12) находим

$$\varphi(B) = \frac{B}{\lambda}. \quad (13)$$

Вычислим множитель Лагранжа. Для этого воспользуемся выражениями (9) и (13) имеем

$$\int_0^{B_{\max}} \frac{B}{\lambda} dB = C. \quad (14)$$

Из выражения (14) находим

$$\lambda = \frac{B_{\max}^2}{2C}. \quad (15)$$

С учетом выражений (13) и (15) получим

$$\varphi(B) = \frac{2BC}{B_{\max}^2}. \quad (16)$$

Покажем, что при решении (13), $R_\Sigma$ достигает максимума, т.е. скорость передачи данных от датчиков к БПЛА достигает максимума. Для этого согласно признаку Лагранжа достаточно вычислить вторую производную подынтегрального выражения в (18) убедиться, что она всегда отрицательная величина.

## Обсуждение

Таким образом, сформулирована и решена задача оптимизации сбора данных от кластеризованных наземных датчиков с использованием группы БПЛА. Сделано предположение о наличии некоторой зависимости интенсивности гауссовского белого шума в канале приема БПЛА от ширины полосы пропускаемых частот этого же канала. При этом на указанную зависимость приложено интегральное ограничение, которого существенно сужает выбор оптимальной зависимости из пространства непрерывных и дважды дифференцируемых функций. Построен целевой функционал оптимизации системы сбора информации. Применение метода безусловной вариационной оптимизации и метода Эйлера для решения оптимизационной задачи позволило получить оптимальный вид искомой функции при которой выбранный целевой функционал достигает максимума.

## Заключение

Рассмотрена задачи оптимизации сбора информации с помощью БПЛА с кластеризованных наземных датчиков. Показано, что скорость сбора информации может достичь максимума при наличии прямой линейной зависимости между шириной частотный полосы канала приема данных БПЛА и интенсивностью белого Гауссово шума в канале приема.

## Литература

1. Ahmed H., Nasir N. Drone patrolling applications, challenges and its future: a review // Vol. XX. 2017.
2. Chen X., Hopkins B., Wang H., Oneill L., Afghah F., Razi A., Fule P. Wildland fire detection and monitoring using a drone-collected RGB/IR image dataset // IEEE Access. Vol. 10. 2022.

3. Ehret and Michael. «The zero marginal cost society: The internet of things, the collaborative commons, and the eclipse of capitalism» // The Journal of Sustainable Mobility, vol. 2, no. 2, pp. 67–70, 2015.
4. Wei Z., Zhu M., Zhang N., Wang L., Zou Y., Meng Z., Feng Z. UAV assisted data collection for internet of things: A survey. Nov 2022.
5. P. Tong, J. Liu, X. Wang, B. Bai, and H. Dai. «Uav-enabled age-optimal data collection in wireless sensor networks» // IEEE International Conference on Communications Workshops (ICC Workshops), pp. 1–6, 2019.
6. J. Zong, C. Shen, J. Cheng, J. Gong, T. -H. Chang, L. Chen, and B. Ai. «Flight time minimization via uavs trajectory design for ground sensor data collection» // 16th International Symposium on Wireless Communication Systems (ISWCS), pp. 255–259, 2019.
7. Z. Wei, X. Liu, C. Han, and Z. Feng. «Neighbor discovery for unmanned aerial vehicle networks // IEEE Access, vol. 6, pp. 68288–68301, 2018.
8. S. Poudel and S. Moh. «Medium access control protocols for unmanned aerial vehicle-aided wireless sensor networks: A survey» // IEEE Access, vol. 7, pp. 65728–65744, 2019.
9. J. Baek, S. I. Han, and Y. Han. «Optimal uav route in wireless charging sensor networks» // IEEE Internet of Things Journal, vol. 7, no. 2, pp. 1327–1335, 2020.
10. C. M. de A. Lima, E. A. da Silva, and P. B. Velloso. «Performance evaluation of 802.11 iot devices for data collection in the forest with drones» // IEEE Global Communications Conference (GLOBECOM), pp. 1–7, 2018.
11. Z. Wei, H. Wu, S. Huang, and Z. Feng. «Scaling laws of 21unmanned aerial vehicle network with mobility pattern information» // IEEE Communications Letters, vol. 21,no. 6, pp. 1389–1392, 2017.
12. C. Zhan and Y. Zeng. «Completion time minimization for multi-uav-enabled data collection» // IEEE Transactions on Wireless Communications, vol. 18, no. 10, pp. 4859–4872, 2019.

# OPTIMIZATION OF THE DATA COLLECTION MODE USING UAVS ON DISTRIBUTED TERRESTRIAL NETWORKS OF MEASURING SENSORS

***Asadov Kh. G.[3], Akhmedov E. M.[4]***

***Keywords:*** *data acquisition rate, channel noise, Gaussian white noise, variational optimization, restrictive condition.*

***Abstract***

***The purpose of the study*** *is to optimize the mode of collecting information using UAVs from sensors of ground measuring networks and to analyze the possibility of increasing the speed of data transfer from ground sensors to UAVs.*

***Research method:*** *the method of unconditional variational optimization is used.*

***Result:*** *the problem of optimizing data collection from clustered ground sensors using a group of UAVs has been formulated and solved. Based on the assumption that there is a certain dependence between the intensity of white Gaussian noise in the UAV receiving channel and the bandwidth of the transmitted frequencies of the same channel, as well as imposing a certain integral constraint on this dependence, the objective functional of unconditional variational optimization was constructed. As a result, the use of the Euler method to solve the optimization problem showed that the speed of information collection can reach a maximum in the presence of a direct linear relationship between the frequency bandwidth of the UAV data reception channel and the intensity of white Gaussian noise in the receiving channel.*

***The scientific novelty and practical value*** *lie in the identification of an additional opportunity to increase the speed of data acquisition from ground sensors using UAVs in the presence of a certain mode limitation on the function of the relationship between the frequency bandwidth of the data receiving channel and the intensity of Gaussian white noise in the receiving channel.*

## References

1. Ahmed H., Nasir N. Drone patrolling applications, challenges and its future: a review // Vol. XX. 2017.
2. Chen X., Hopkins B., Wang H., Oneill L., Afghah F., Razi A., Fule P. Wildland fire detection and monitoring using a drone-collected RGB/IR image dataset // IEEE Access. Vol. 10. 2022.
3. Ehret and Michael. «The zero marginal cost society: The internet of things, the collaborative commons, and the eclipse of capitalism» // The Journal of Sustainable Mobility, vol. 2, no. 2, pp. 67–70, 2015.
4. Wei Z., Zhu M., Zhang N., Wang L., Zou Y., Meng Z., Feng Z. UAV assisted data collection for internet of things: A survey. Nov 2022.
5. P. Tong, J. Liu, X. Wang, B. Bai, and H. Dai. «Uav-enabled age-optimal data collection in wireless sensor networks» // IEEE International Conference on Communications Workshops (ICC Workshops), pp. 1–6, 2019.

3 Asadov Hikmet Hamid oglu, Dr.Sc. of Technical Sciences, Professor, National Aerospace Agency, Baku. Republic of Azerbaijan. E-mail: asadzade@rambler.ru
4 Ahmadov Emil Mehman oglu, postgraduate student, National Aerospace Agency, Baku. Republic of Azerbaijan. E mail: emil.ahmedov21@gmail.com

6. J. Zong, C. Shen, J. Cheng, J. Gong, T. -H. Chang, L. Chen, and B. Ai. «Flight time minimization via uavs trajectory design for ground sensor data collection» // 16th International Symposium on Wireless Communication Systems (ISWCS), pp. 255–259, 2019.
7. Z. Wei, X. Liu, C. Han, and Z. Feng. «Neighbor discovery for unmanned aerial vehicle networks // IEEE Access, vol. 6, pp. 68288–68301, 2018.
8. S. Poudel and S. Moh. «Medium access control protocols for unmanned aerial vehicle-aided wireless sensor networks: A survey» // IEEE Access, vol. 7, pp. 65728–65744, 2019.
9. J. Baek, S. I. Han, and Y. Han. «Optimal uav route in wireless charging sensor networks» // IEEE Internet of Things Journal, vol. 7, no. 2, pp. 1327–1335, 2020.
10. C. M. de A. Lima, E. A. da Silva, and P. B. Velloso. «Performance evaluation of 802.11 iot devices for data collection in the forest with drones» // IEEE Global Communications Conference (GLOBECOM), pp. 1–7, 2018.
11. Z. Wei, H. Wu, S. Huang, and Z. Feng. «Scaling laws of 21unmanned aerial vehicle network with mobility pattern information» // IEEE Communications Letters, vol. 21,no. 6, pp. 1389–1392, 2017.
12. C. Zhan and Y. Zeng. «Completion time minimization for multi-uav-enabled data collection» // IEEE Transactions on Wireless Communications, vol. 18, no. 10, pp. 4859–4872, 2019.

# ПРИМЕНЕНИЕ РОБОТИЗИРОВАННЫХ КОМПЛЕКСОВ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ ПРИ ВЫПОЛНЕНИИ МЕРОПРИЯТИЙ ТЕХНИЧЕСКОГО ОБЕСПЕЧЕНИЯ СВЯЗИ

***Клименко А. Д.[1], Решетов В. В.[2]***

**DOI:10.21681/3034-4050-2026-2-94-99**

***Ключевые слова:*** *техническое обеспечение связи, техническая разведка, роботизированный кабелеукладчик, диагностика повреждений, беспилотные летательные аппараты.*

***Аннотация***

***Цель работы*** *состоит в систематизации направлений применения роботизированных комплексов специального назначения при выполнении мероприятий технического обеспечения связи и технической разведки поврежденной техники на основе анализа боевого опыта их использования в зоне специальной военной операции, а также в выявлении тактико-технических особенностей, определении перспектив развития систем управления и методов автоматической диагностики.*

***Метод исследования*** *базируется на методах системного анализа, классификации и обобщения данных, полученных в ходе специальной военной операции, что позволяет обеспечить достоверность и обоснованность полученных выводов.*

***Результаты исследования:*** *на основе актуального боевого опыта проведена систематизация применения роботизированных комплексов для выполнения задач системы технического обеспечения связи и автоматизированных систем управления (ТОС и АСУ). Разработана классификация роботизированных средств по функциональному назначению, включающая: наземные роботизированные кабелеукладчики на электротяге (обеспечивающие механизированную прокладку защищенных линий связи с заглублением кабеля в грунт и работающие в связке с беспилотными летательными аппаратами для корректировки маршрутов); воздушные роботизированные кабелеукладчики (FPV-дроны, оснащенные бобинами с кабелем для воздушной прокладки линий через минные поля и труднопроходимую местность); многофункциональные транспортно-логистические платформы; ремонтно-диагностические комплексы для технической разведки поврежденной техники связи, а также робототехнические средства и комплексы связи. Выявлены преимущества применения робототехнических средств и комплексов. Систематизирован перечень специализированных задач, решаемых робототехническими комплексами военного назначения в интересах организации и обеспечения связи, решения задач ТОС и АСУ в ходе СВО.*

***Практическая ценность:*** *выявлены ключевые зависимости эффективности технической разведки от методов автоматической классификации, технологии цифровых двойников и точности оценивания состояния. Определено противоречие между растущей автономностью роботизированных средств и требованиями к гарантированному управлению ими в боевых условиях при интенсивном радиоэлектронном подавлении.*

## Введение

Одной из главных особенностей специальной военной операции является то, что поставленные цели достигаются без стратегического развертывания ВС РФ, и войска связи выполняют боевые задачи в составе комплекта войск мирного времени.

Одним из факторов, влияющих на выполнение задач системой ТОС и АСУ, является реализация противником концепции «Армия дронов». Количество применения ударных БПЛА по объектам связи, таким как, опорные узлы связи и комплексы видеонаблюдения существенно возросло. Соответственно, возросла нагрузка на подсистемы снабжения и восстановления.

Современное состояние вооруженного противоборства характеризуется активным развитием и внедрением робототехнических систем и комплексов специального назначения. В условиях специальной военной операции (СВО) особую актуальность приобретают задачи обеспечения устойчивого управления войсками и оперативного восстановления поврежденной техники связи и автоматизированных систем управления (АСУ). Традиционные методы прокладки и обслуживания линий связи, а также технической разведки поврежденной техники связи вблизи линии боевого соприкосновения (ЛБС) связаны с высоким риском для жизни личного состава подразделений связи и ремонтных подразделений, что требует поиска новых технологических решений.

Целью настоящей статьи является систематизация направлений применения роботизированных комплексов при выполнении мероприятий

1 Клименко Андрей Дмитриевич, адъюнкт Военной академии связи, Санкт-Петербург. E-mail: Klimenko andrew@mail.ru

2 Решетов Владимир Владимирович, адъюнкт Военной академии связи, Санкт-Петербург. E-mail: sibnsk1407@mail.ru

технического обеспечения связи на основе анализа боевого опыта их использования в зоне СВО, выявление особенностей применения РТСК, определение перспектив развития систем управления и методов автоматической диагностики.

## Обсуждение

РТК ВН представляют собой дистанционно управляемые или автономные образцы ВВСТ, используемые для полной или частичной замены человека в процессе выполнения боевых и обеспечивающих задач [1].

Типовой образец РТК ВН можно представить в виде совокупности связанных элементов: базовый носитель (корпус или шасси разных конфигураций для применения в различных средах); специализированное навесное (встраиваемое) оборудование в виде набора съемных модулей полезной (целевой) нагрузки; средства обслуживания и обеспечения (для технической эксплуатации РТК ВН и подготовки его к применению) [2].

Состав специализированного оборудования устанавливается, исходя из функционального предназначения робота, и может включать: средства разведки, вооружения, навигационные устройства; специальное технологическое оборудование; средства телекоммуникации; специализированные вычислители с программно-алгоритмическим обеспечением; средства радиоэлектронной борьбы (РЭБ).

Для обеспечения управления и обслуживания в состав комплекса дополнительно включаются:

- диспетчерский (наземный) пункт управления, контроля и обработки информации;
- средства доставки, транспортировки и запуска;
- средства снаряжения, заправки и зарядки.

РТК ВН по среде применения подразделяются на различные типы базирования – наземные РТК (дистанционно-управляемые машины), морские (надводные, подводные и гибридные необитаемые подводные аппараты), воздушные – беспилотные летательные аппараты (БПЛА).

Современные РТК ВН применяются для решения широкого спектра боевых и обеспечивающих задач, основными из которых являются:

- разведка и наблюдение на всех театрах военных действий (поиск, обнаружение и слежение за силами и средствами обеспечения вооружения);
- целеуказание для нанесения ударов высокоточным оружием;
- корректировка огня артиллерии;
- длительное воздушное патрулирование заданных районов;
- оценка результатов нанесения ударов;
- уничтожение важных целей, объектов и живой силы противника с помощью бортового оружия;
- ретрансляция сигналов;
- радиоэлектронная борьба;
- доставка грузов, в том числе боеприпасов, медикаментов и продовольствия;
- нейтрализация взрывных устройств, разминирование местности [3].

Современные РТК представляют собой, как правило, мобильные электромеханические и гидравлические платформы с телеуправлением, имеющие программно-аппаратные средства, позволяющие автоматизировать выполнение некоторых задач без участия оператора [2].

Одним из основных преимуществ использования РТК ВН является возможность выполнения сложных и опасных операций, роботы могут работать в неблагоприятных условиях и в зоне повышенной опасности (под огнем противника, в зоне радиационного, химического и биологического заражения воздуха и местности и пр.), избегая при этом рисков для личного состава.

Ниже представлены примеры реализации РТСК в интересах системы технического обеспечения связи в ходе СВО:

- дистанционное управление БШПД, свозможностью удаленной юстировки антенн размещенных на мачтах операторов сотовой связи;
- использование стационарных и мобильных, дистанционно поднимаемых призматических мачт для подъема радиорелейных станций, камер видеонаблюдения, развертывания мобильных ретрансляторов радиостанций Р-187П1 «Азарт» и радиостанций двойного назначения;
- использование мобильных радиоуправляемых платформ с устройствами крепления оборудования WiMax и ретрансляторов Р-187П1, для обеспечения увеличения зон покрытия транспортной сети связи;
- монтаж рентансляторов тактического звена управления с использованием БПЛА;
- использование FPV-дронов с устройствами для доставки и сбрасывания ретрансляторов радиостанций Р-187П1 «Азарт» на здания, деревья и другие возвышенности, находящиеся в районе ведения активных действий, прокладки полевых кабельных линий;
- применение транспортных радиоуправляемых роботизированных платформ «Линейщик» с устройствами для доставки и прокладки кабельной полевой линии связи П-274М;

*Таблица 1.*

*Классификация РТСК, применяемых в интересах системы ТОСиАСУ*

| Класификационная группировка РТСК | Решаемые задачи |
|---|---|
| Наземные роботизированные кабелеукладчики | Доставка и прокладка полевой кабельной линии связи средней протяженности с использованием колесных и гусеничных робототехнических платформ |
| Воздушные роботизированные кабелеукладчики | Прокладка полевых кабельных линий с использованием FPV-дронов на малые расстояния в короткие сроки |
| Транспортно-логистические платформы | Транспортировка грузов, доставка сменных блоков и катушек с кабелем, снабжение подразделений на передовой с использованием наземных, воздушных и морских РТК |
| Интеллектуальные системы диагностики и ремонта техники связи | Диагностика поврежденной техники связи в полевых условиях с использованием ИИ-ассистента без доступа к интернету (в перспективе – частично автономного РТК) |
| Робототехнические средства и комплексы связи | Дистанционное управление БШПД; увеличение зон покрытия транспортной сети связи; увеличение дальности радиосвязи |

- монтаж камер видеонаблюдения и ретрансляторов тактического звена управления на радиоуправляемую универсальную платформу с колёсным или гусеничным движителем и на буксируемую тележку-прицеп;
- оснащение радиоуправляемых универсальных платформ с колёсным или гусеничным движителем для транспортировки грузов для подразделений в зоне линии боевого соприкосновения.

Массовое (широкое) применение роботов и технологий робототехники изменяет формы и способы ведения боя, операции, тактику действия войск и технический облик перспективных систем вооружения, военной и специальной техники (ВВСТ), повышает эффективность их применения.

На основе анализа боевого применения в зоне СВО и зарубежного опыта предлагается классификация роботизированных комплексов, применяемых для решения задач в интересах системы технического обеспечения связи и автоматизированных систем управления (табл. 1).

В ходе СВО в интересах организации, обеспечения и восстановления связи активно применяются как наземные, так и воздушные РТК для прокладки кабельных линий связи. Наземные роботизированные кабелеукладчики, применяемые в зоне СВО, представляют собой гусеничные или колесные платформы на электротяге, оснащенные плужным оборудованием. При движении платформа роет канаву (глубиной 1-2 штыка лопаты) для кабеля связи, после чего она засыпается с помощью специального устройства. Управление кабелеукладчиком осуществляется оператором при помощи пульта дистанционного управления и системы видеокамер на корпусе РТК. Имеется возможность работы кабелеукладчика совместно с БПЛА для корректировки маршрута прокладки кабеля с учетом особенностей местности и боевой обстановки.

Воздушные РТК находят применение при прокладке полевых кабельных линий связи с использованием FPV-дронов [1], позволяя значительно снизить потери личного состава подразделений связи на переднем крае, прокладывая проводные линии связи в местах, где прокладка кабеля личным составом подразделений связи невозможна или нецелесообразна. Максимальная дальность прокладки легкого кабеля (П-274М) составляет 500 м за время 10 минут при полете квадрокоптера до 20 минут.

Перспективной разработкой является грузовой БПЛА «Слон», прошедший полигонную апробацию и получивший положительное заключение главного управления инновационного развития Минобороны РФ. С максимальной полезной нагрузкой до 120 кг и дальностью полета до 15 км, он предназначен для снабжения подразделений на передней линии фронта, где транспортировка обычными средствами затруднена. Платформа рассматривается как многофункциональная, способная выполнять задачи по перевозке спецоборудования, средств РЭБ, минированию[3].

Важными направлениями развития являются:

- разработка и внедрение интеллектуальных систем диагностики и ремонта техники связи. Примером таких систем является ИИ-ассистент NeoLens, (применяемый ВСУ в ходе СВО) предназначенный для диагностики и ремонта военной техники (Humvee, MaxxPro,

3 В зоне СВО начнут применять дрон-тяжеловес «Слон», дрон-кабелеукладчик «Заноза» – уже там // Российская газета. 07.10.2025. URL: https://rg.ru/2025/10/07/v-zone-svo-budut-primeniat-kvadrokopter-tiazheloves-slon.html (дата обращения: 10.03.2026).

М113) и обладающий способностью работать без доступа к интернету, что критически важно в условиях отсутствия устойчивой связи или риска перехвата данных. Ассистент обеспечивает пошаговую диагностику, позволяет находить неисправности и проводить полевой ремонт на высоком уровне даже операторам, впервые работающим с данным оборудованием. Данный опыт подтверждает перспективность внедрения аналогичных интеллектуальных систем для технической разведки и ремонта техники связи и АСУ в российских вооруженных силах;

- применение технологии «цифровых двойников» для диагностики технического состояния поврежденной техники, сравнения реального состояния с эталонными моделями и прогнозирования отказов;
- разработка и внедрение частично автономных РТК для ведения технической разведки и диагностирования поврежденной техники связи на основе машинного зрения и радиочастотных меток [4].

Успех выполнения задач с применением современных и перспективных РТК ВН напрямую зависит от устойчивого доведения управляющей информации и бесперебойного обмена данными по каналам связи с постоянно меняющимися параметрами в условиях дестабилизирующего воздействия естественного и искусственного характера.

Для обеспечения помехозащищенности беспроводных каналов связи РТК ВН необходимо применение устойчивых к помехам видов модуляции, например, способ доведения управляющей и телеметрической информации в интересах РТК ВН различных типов базирования с использованием линейно-частотно модулируемых сигналов (ЛЧМ-сигналов) и цифровой фильтрации, детально описанный в работе [5], обеспечивающий доведение команд управления и телеметрии до РТК ВН в условиях сложной помеховой обстановки.

## Анализ применения РТК

Анализ боевого применения роботизированных комплексов позволяет систематизировать преимущества их использования для решения задач системы технического обеспечения связи и автоматизированных систем управления

1. Снижение рисков для личного состава подразделений связи и ремонтно-восстановительных групп. Оператор управляет роботизированным комплексом (платформой) из укрытия, не выходя на простреливаемую территорию. Это особенно актуально при работе вблизи ЛБС.
2. Возможность применения РТСК в условиях, когда использование традиционных техники невозможно или нецелесообразно. Например, прокладка роботизированными кабелеукладчиками проводной линии связи (П-274М, ВОЛС) через минные поля, водные преграды, овраги и другие препятствия, где пешая прокладка невозможна или требует длительной инженерной подготовки и разминирования.
3. Постоянно повышающийся уровень автономности современных РТСК и возможность их работы в круглосуточном режиме (при замене элементов питания и организации

*Таблица 2.*

*Проблемные вопросы и направления их решения*

| Проблемный вопрос | Направления решения |
|---|---|
| Ограниченное время автономной работы робототехнических платформ и комплексов | Разработка быстросменных аккумуляторных батарей, создание полевых зарядных станций, совершенствование энергоэффективности |
| Уязвимость каналов управления к средствам РЭБ | Разработка комбинированных систем управления (оптоволокно + радиоканал), внедрение функций автоматического восстановления связи, резервирование каналов [2] |
| Необходимость оперативной диагностики и ремонта в полевых условиях | Разработка и внедрение систем пошаговой диагностики с ИИ-ассистентом для диагностики поврежденной техники связи, работающих офлайн; разработка систем пошаговой диагностики для неподготовленных операторов [4] |
| Недостаток квалифицированных операторов | Разработка программ подготовки специалистов двойной квалификации, создание тренажерных комплексов, внедрение интеллектуальных систем поддержки принятия решений |
| Отсутствие единых стандартов управления и интеграции | Разработка унифицированных протоколов обмена данными и интерфейсов для интеграции разнородных роботизированных средств в единую АСУ |

правильного несения дежурства операторов РТСК), повышая эффективность выполнения мероприятий системы ТОС и АСУ.

4. Интеллектуальная поддержка принятия решений. Внедрение ИИ-ассистентов для диагностики и ремонта поврежденной техники связи позволяет увеличить оперативность и достоверность технического диагностирования.

Проведенный анализ позволяет выявить ряд проблемных вопросов, требующих решения для повышения эффективности применения роботизированных средств и комплексов в интересах выполнения задач системы ТОС и АСУ (табл. 2).

## Заключение

Активное применение робототехнических средств и комплексов оказывает все большее влияние на ход и исход вооруженного противоборства. В настоящее время, а тем более в обозримом будущем сложно представить проведение военных операций любого уровня без использования БПЛА, необитаемых и автоматических образцов вооружения. Применение РТСК для выполнения различных задач обеспечения и ведения боевых действий является достаточно важным направлением для ВС РФ в СВО.

Проведенный анализ их боевого применения в ходе специальной военной операции позволил: предложить классификацию РТСК, применяемых в интересах системы ТОСиАСУ по их функциональному предназначению; систематизировать перечень специализированных задач, решаемых с применением РТСК; выявлить преимущества и проблемные вопросы их применения, а также направления их решения.

Полученные результаты имеют значение для развития теории управления войсками и технического обеспечения связи, совершенствования тактики действий подразделений связи и ремонтных подразделений, обоснования тактико-технических требований к перспективным роботизированным комплексам специального назначения и системам управления ими.

## Литература


1. Макаренко С. И. Робототехнические комплексы военного назначения – текущее состояние и перспективы развития // Системы управления, связи и безопасности. 2016, №2. С 74-75.
2. Сорокин К. Н., Лукьянчик В. Н., Кудрявцев А. О. Применение робототехнических комплексов связи в системах связи специального назначения // Телекоммуникации и связь. 2025. № 6(09). С. 88–100.
3. Раковенко А. А., Кузьмин А. А., Куницын Р. И. Роль группового применения робототехнических комплексов военного назначения в современных вооруженных конфликтах // Арсенал Отечества. 2022, № 3.
4. Семенов С. С., Педан А. В., Смолеха А. В. Применение технологий распознавания образов как инструмент решения задач технической разведки техники связи и автоматизированных систем управления // Системы управления, связи и безопасности. 2015. № 1. С 26–28.
5. Будко Н. П., Будко П. А., Клюшин М. А., Шаталов А. Е. Способ доведения управляющей и телеметрической информации в интересах робототехнических платформ различных типов базирования // Системы управления, связи и безопасности. 2025. № 3. С. 294–322. DOI: 10.24412/2410-9916-2025-3-294-322.


# THE USE OF SPECIAL-PURPOSE ROBOTIC SYSTEMS IN THE IMPLEMENTATION OF TECHNICAL COMMUNICATIONS SUPPORT MEASURES

***Klimenko A. D.[4], Reshetov V. V.[5]***

***Keywords:*** *military robotic systems, communications support, technical reconnaissance, robotic cable laying, fault diagnostics, unmanned aerial vehicles.*

***Abstract***

***Purpose of the work*** *is to systematize the directions of application of robotic complexes for special purposes in the implementation of technical communication support measures and technical reconnaissance of damaged equipment based on the analysis of combat experience of their use in the special military operation zone, as well as to identify tactical and technical features, determine the prospects for the development of control systems and methods of automatic diagnostics.*

4 Klimenko Andrey Dmitrievich, adjunct of the department of Technical support of communication of the Military Academy of Communications named after Marshal of the Soviet Union S. M. Budyonny, St. Petersburg. E-mail: klimenko-andrew@mail.ru

5 Reshetov Vladimir Vladimirovich adjunct of the department of Technical support of communication of the Military Academy of Communications named after Marshal of the Soviet Union S. M. Budyonny, St. Petersburg. E-mail: sibnsk1407@mail.ru

***Research method*** *is based on a comprehensive analysis of open sources of information, including official data from the Ministry of Defense of the Russian Federation, materials from departmental media, expert opinions of specialists in the field of robotics and communications troops, patent documents and scientific publications, as well as a comparative analysis of the tactical and technical characteristics of the samples used. The work uses methods of system analysis, classification and generalization of empirical data obtained during a special military operation, which ensures the reliability and validity of the conclusions obtained.*

***Results of the research:*** *the article, based on current combat experience, systematizes the use of robotic systems for tasks in the technical support system of communications and automated control systems. A classification of robotic equipment by functional purpose has been developed, including: ground-based robotic cable layers; aerial cable layers; multifunctional transport and logistics platforms; repair and diagnostic systems for diagnosing damaged equipment, as well as robotic equipment and communication systems. The advantages of using robotic systems have been identified. A list of specialized tasks solved by military robotic systems for the purposes of organizing communications and solving communication maintenance problems during a special military operation has been systematized.*

***The Scientific novelty*** *of the study lies in the fact that, based on the analysis of the combat use of military robotic systems in the zone of a special military operation, a systematization was carried out for communnications and technical reconnaissance of damaged communication equipment, which had not previously been the subject of a scientific analysis.*

## References

1. Makarenko S.I. Military robotic systems – current state and development prospects // Control, communication, and security systems, 2016. № 2. P. 74–75.
2. Sorokin K. N., Lukyanchik V. N., Kudryavtsev A. O. Application of robotic communication complexes in a special-purpose communication system // Telecommunikacii I svyaz', 2025. № 6. P. 90.
3. Rakovenko A. A., Kuz'min A. A., Kunicin R. I. The role of group use of military-grade aerobic systems in modern armed conflicts. The arsenal of the fatherland, 2022. № 3.
4. The heavy-duty drone «Slon» will be used in the SVO zone, and the cable-laying drone «Zanoza» is already in use there // Rossiyskaya Gazeta, 07.10.2025. URL:https://rg.ru/2025/10/07/v-zone-svo-budut-primeniat-kvadrokopter-tiazheloves-slon.html.
5. Semenov S. S., Pedan A. V., Smoleha A. V. The use of recognition technologies as a tool for solving problems of technical intelligence, communications technology and automated control systems // Control, communication and security systems, 2015. № 1. P 26–28.
6. Budko N. P, Budko P. A., Klyshin M. A., Shatalov A. E. A method for delivering control and telemetry information to robotic platforms of various types of basing // Control, communication and security systems, 2025. № 3. P 294–322. DOI: 10.24412/2410-9916-2025-3-294-322.

**TELECOMMUNICATIONS and COMMUNICATIONS**

**SCIENTIFIC PEER-REVIEWED JOURNAL**
№ 1 (10) 2026
Published 6 times a year

The journal is registered by the Federal Servicefor Supervision of Communications, Information Technology and Mass Communications.
Registration Certificate
PI № FS77-88069 от 16.08.2024



**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 2/02/2026.
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