

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

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

### Главный редактор

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

### Председатель Редакционного совета

РУБИС Александр Анатольевич, к.т.н., Москва

### Шеф-редактор

МАКАРЕНКО Григорий Иванович, с.н.с., Москва

### Редакционный совет

ПЫЛИНСКИЙ Максим Валерьевич, д.в.н., профессор, Белоруссия  
РЫЖОВ Геннадий Борисович, д.в.н., профессор, Москва  
СТАРДУБЦЕВ Юрий Иванович, д.в.н., профессор, Санкт-Петербург  
ХАРЧЕНКО Евгений Борисович, к.соц.н., доцент, Москва  
КУЗИН Павел Игоревич, к.т.н., доцент, Санкт-Петербург

### Редакционная коллегия

БУЙНЕВИЧ Михаил Викторович, д.т.н., профессор, Санкт-Петербург  
ГЛУШАНКОВ Евгений Иванович, д.т.н., профессор, Санкт-Петербург  
ИВАНОВ Сергей Александрович, д.т.н., Санкт-Петербург  
КОЗАЧОК Александр Васильевич, д.т.н., доцент, Орел  
КОРОБКА Сергей Владимирович, д.в.н., Москва  
КОСТОГРЫЗОВ Андрей Иванович, д.т.н., профессор, Москва  
МАКАРЕНКО Сергей Иванович, д.т.н., профессор, Санкт-Петербург  
МАРКОВ Алексей Сергеевич, д.т.н., доцент, Москва  
РЫЖКОВ Анатолий Васильевич, д.т.н., профессор, Москва  
САВИЩЕНКО Николай Васильевич, д.т.н., профессор, Санкт-Петербург  
СИВАКОВ Игорь Романович, д.в.н., Москва  
ЦИМБАЛ Владимир Анатольевич, д.т.н., профессор, Серпухов  
ФЕДЮНИН Павел Александрович, д.т.н., профессор, Воронеж  
ФИНЬКО Олег Анатольевич, д.т.н., профессор, Краснодар

### Учредитель и издатель

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

Над номером работали:

Г. И. Макаренко – шеф-редактор, Н. В. Селезнев – отв. секретарь,  
С. С. Игнатов – верстка, А. В. Матюшин – маркетинг и подписка

Подписано к печати 2.02.2026 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

## ВОЕННЫЕ СИСТЕМЫ УПРАВЛЕНИЯ, СВЯЗИ И НАВИГАЦИИ

### ПРИНЦИПЫ ПОВЫШЕНИЯ УСТОЙЧИВОСТИ СЕТИ ОБМЕНА ДАННЫМИ БОЛЬШОЙ ГРУППЫ БПЛА НА ОСНОВЕ КЛАСТЕРИЗАЦИИ ЕЁ СТРУКТУРЫ

Деркач А. Е., Лиманцева Е. В., Чуднов А. М. .... 2

### РАСПРЕДЕЛЕНИЕ НАГРУЗКИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ВОЕННОГО НАЗНАЧЕНИЯ

Алленов Д. С., Курбанов С. Н. .... 8

### ИННОВАЦИОННЫЕ ТЕХНОЛОГИИ В ТЕЛЕКОММУНИКАЦИИ И ИХ ВЛИЯНИЕ НА ВОЕННУЮ СВЯЗЬ

Иванов В. Г., Лукьянчик В. Н., Кузин П. И. .... 16

## СИСТЕМНЫЙ АНАЛИЗ СИСТЕМ ВОЕННОГО НАЗНАЧЕНИЯ

### МОДЕЛЬ ВЛИЯНИЯ МОНИТОРИНГА СЕТЕВОГО ТРАФИКА НА ЭФФЕКТИВНОСТЬ ФУНКЦИОНИРОВАНИЯ СЕТИ ПЕРЕДАЧИ ДАННЫХ

Симонова К. О. .... 33

### ПРИМЕНЕНИЕ ЦИФРОВЫХ ДВОЙНИКОВ В ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ

Яровой Р. В., Карганов В. В., Лукашенко В. И. .... 42

## ИНФОРМАЦИОННЫЕ СИСТЕМЫ

### ОСОБЕННОСТИ ОРГАНИЗАЦИИ СЛУЖЕБНОЙ ТЕЛЕФОННОЙ СВЯЗИ НА ПУНКТАХ УПРАВЛЕНИЯ

Кузина Е. И., Панкин А. А., Потапов И. А., Назаров А. Д. .... 52

### АНАЛИЗ СУЩЕСТВУЮЩИХ ГЕОИНФОРМАЦИОННЫХ СИСТЕМ, ИСПОЛЬЗУЕМЫХ В МЧС РОССИИ И ОЦЕНКА ИХ ФУНКЦИОНАЛЬНЫХ ОГРАНИЧЕНИЙ

Курбанов С. Н., Безвесильная А. А., Григорьян А. А. .... 59

### НЕМАТЕМАТИЧЕСКИЕ МЕТОДЫ В КРИПТОГРАФИИ (ЗАЩИЩЕННАЯ СВЯЗЬ НА ОСНОВЕ ОДНОРАНГОВОЙ MESH-СЕТИ)

Черепнёв М. А. .... 72

## ВОЕННАЯ ЭЛЕКТРОНИКА, АППАРАТУРА КОМПЛЕКСОВ ВОЕННОГО НАЗНАЧЕНИЯ

### КРИТЕРИИ ЭФФЕКТИВНОСТИ ПОЛЕВОЙ СИСТЕМЫ ЭЛЕКТРОСНАБЖЕНИЯ

Асанян А. В., Иванов В. Г., Иванишко А. Н. .... 78

## ТЕХНОЛОГИИ ОБУЧЕНИЯ КУРСАНТОВ ВОЕННЫХ СПЕЦИАЛЬНОСТЕЙ

### ИСПОЛЬЗОВАНИЕ ДОПОЛНЕННОЙ РЕАЛЬНОСТИ В ПРОЦЕССЕ ОБУЧЕНИЯ В ВЫСШИХ УЧЕБНЫХ ЗАВЕДЕНИЯХ

Магера М. А. .... 88

## НАША ИСТОРИЯ

### ПОДВИЖНЫЙ УЗЕЛ СВЯЗИ НАРОДНОГО КОМИССАРИАТА СВЯЗИ СССР: ОПЫТ СТРОИТЕЛЬСТВА ОБЪЕКТА 04, ФОРМИРОВАНИЯ И ПРИМЕНЕНИЯ ПОЕЗДА СВЯЗИ № 1

Шентура В. Н. .... 96

# ПРИНЦИПЫ ПОВЫШЕНИЯ УСТОЙЧИВОСТИ СЕТИ ОБМЕНА ДАННЫМИ БОЛЬШОЙ ГРУППЫ БПЛА НА ОСНОВЕ КЛАСТЕРИЗАЦИИ ЕЁ СТРУКТУРЫ

Деркач А. Е.<sup>1</sup>, Лиманцева Е. В.<sup>2</sup>, Чуднов А. М.<sup>3</sup>

DOI:10.21681/3034-4050-2026-1-2-7

**Ключевые слова:** сеть с коммутацией пакетов, пропускная способность сети, устойчивость сети, управление маршрутизацией пакетов, таблицы маршрутизации пакетов, самоорганизация сетевого обмена.

## Аннотация

**Цель работы:** повышение устойчивости сети обмена данными большой группы беспилотных летательных аппаратов (БПЛА) к дестабилизирующим воздействиям за счет динамической оптимизации ее структуры.

**Методы исследования:** теории сетей массового обслуживания, теория управления, динамическое программирование.

**Результаты исследования:** разработаны принципы анализа и оптимизации структуры системы обмена данными большой группы (роя) БПЛА с кластеризованной структурой маршрутизации пакетов. Показано, что повышение эффективности функционирования сети обмена данными (СОД) может быть обусловлено за счет сокращения трафика, необходимого для сбора данных.

**Научная новизна** результатов состоит в разработке новой модели обмена данными в крупномасштабной СОД, учитывающей в процессе управления маршрутизацией кластеризованную структуру, а также постановке и разработки метода решения задачи оптимизации кластеризованной сетевой структуры.

## Введение

Проблема обеспечения устойчивой работы сетей обмена данными (СОД) в условиях случайных сбоев и целенаправленных дестабилизирующих воздействий является одной из наиболее актуальных в современной телекоммуникационной отрасли [1–21]. Под устойчивостью сети понимается её способность сохранять достаточно эффективное функционирование в определенном классе дестабилизирующих воздействий, под которыми для СОД БПЛА понимаются факторы, приводящие к полному или частичному нарушению работоспособности объектов системы (отказы, уничтожение, случайные и преднамеренные помехи...). При этом в качестве базовых показателей, характеризующих эффективность функционирования системы и определяющих ее работоспособность, как правило, выступают вероятностно-временные характеристики процесса передачи сообщений.

Вопросы разработки методов анализа и оптимизации показателей вероятностно-временных характеристик СОД в условиях различного рода случайных и преднамеренных воздействий изучались в весьма большом числе работ (см., например, [1–10] и библиографию к ним). В [1–9, 11–22] рассматривались задачи, ориентированные на обеспечение связности СОД, в [11–16] для частных примеров результаты основывались на проведении вычислительного эксперимента с использованием статистических оценок. Одно из первых исследований по анализу и оптимизации вероятностно-временных характеристик (ВВХ) прохождения сообщений в сети передачи данных с ограничениями на ресурс приемо-передающих средств было проведено в [4] и в дальнейшем развито в [1] – в индифферентной по отношению к СОД БПЛА среде и в [2] – в условиях преднамеренных (оптимизированных) помех. Вместе с тем в [1, 2], как

<sup>1</sup> Деркач Алексей Евгеньевич, адъюнкт Военной академии связи, г. Санкт-Петербург, Россия. E-mail: alder2000@inbox.ru

<sup>2</sup> Лиманцева Елена Владимировна, адъюнкт Военной академии связи, г. Санкт-Петербург, Россия. E-mail: lena.limantseva@mail.ru

<sup>3</sup> Чуднов Александр Михайлович, доктор технических наук, профессор, профессор Военной академии связи имени Маршала Советского Союза С. М. Буденного, г. Санкт-Петербург, Россия. E-mail: chudnow@yandex.ru

<sup>4</sup> Чуднов А. М. и др. Комплексное управление маршрутизацией пакетов и режимами работы радиосредств в неоднородной сети передачи данных // Радиотехнические и телекоммуникационные системы. 2019. № 1(33). С. 46–56.

и в исходной статье расчеты производились без учета дополнительного трафика, обусловленного потребностью системы управления СОД, в частности, маршрутизацией пакетов. Для сетей с малым числом узлов это не приводит к большим погрешностям расчетных величин, однако для крупномасштабных сетей оперативный сбор данных о состоянии сети и доведение их в конечном счете до исполнительных элементов системы управления погрешности могут оказаться значительными и приводить к несостоятельным выводам. Более того, без должной организации процесса обмена служебной информацией элементов СОД большой группы БПЛА потоки таких данных могут перегрузить сеть и полностью заблокировать ее работу.

Из рассмотренного следует актуальность задачи организации сбора данных о состоянии СОД (в частности, структуре, характеристиках возможных направлений связи, потоках данных в информационных направлениях) и осведомления необходимой информацией объектов подсистемы управления сетью. Это задача решается на основе кластеризации (сегментирования) сетевой структуры, под которой понимается разделение множества узлов сети на фрагменты с выделенными в каждом фрагменте (кластере, сегменте) одним или несколькими центральными элементами [17, 18]. При этом общая задача управления маршрутизацией в СОД декомпозируется на частные:

- задачи управления маршрутизацией в кластерах СОД;
- задачу управления маршрутизацией в межкластерной сети, образованной центральными элементами кластеров.

Заметим, что для крупномасштабных сетей с динамически изменяющейся структурой кластеризация структуры выступает не только как средство повышения эффективности, но и как принципиально необходимое условие обеспечение работоспособности сети связи.

В дальнейшей части работы в формализованном виде дается постановка задачи анализа ВВХ СОД с сегментированной структурой, приводится вариант иерархической кластеризации СОД и методика оценки ее устойчивости, приведены примеры расчета показателей устойчивости с оценкой выигрыша, обеспечиваемого за счет сетевой кластеризации.

### Постановка задачи

Рассмотрим задачу анализа и оптимизации алгоритма маршрутизации в кластеризованной сети. В формализованном виде она задается на наборе исходных данных, аналогичном описанному в [1, 2], но с учетом кластерной структуры.

Исходные данные:

$G = (V, E)$  – граф сети, где  $V$  – множество узлов (объектов СОД),  $E$  – множество возможных связей;

$C = (c_{k,l})$  – матрица пропускных способностей линий связи;

$\Lambda = (\lambda_{i,j})$  – матрица интенсивностей потоков пакетов в информационных направлениях.

$U^*, V^*$  – векторы ресурсов передающих и приемных средств узлов;

$\mathcal{P} = \langle P^k \rangle_{k \in \mathbb{N}_n}$  – набор таблиц маршрутизации пакетов (ТМП), где  $P^k = (p_{i,j}^k)$  – вероятность направления пакета, адресованного  $j$ -узлу на  $l$ -порт.

В кластеризованной сети множество узлов  $V$  разбито на  $K$  кластеров:

$$V = \bigcup_{m=1}^K V_m,$$

где каждый кластер  $V_m$  имеет выделенный центральный узел (хаб)  $h_m$ .

Множества маршрутов:

$M_{(i,j)}$  – множество маршрутов из  $i$  в  $j$ ;

$M_{(k,l)}$  – множество маршрутов, проходящих через линию  $\langle k, l \rangle$ .

$$M\langle i, j; k, l \rangle = M_{(i,j)} \cap M_{(k,l)}.$$

Распределение потоков:

Интенсивность потока на маршруте  $\mu \in M_{(i,j)}$  вычисляется как:

$$s(\mu) = \lambda_{i,j} \prod_{(k,l) \in \mu} p_{i,j}^k.$$

Ограничения на ресурсы:

$$u_k = \sum_l \frac{s(k,l)}{c_{k,l}} \leq u_k^*, \quad v_k = \sum_l \frac{s(l,k)}{c_{l,k}} \leq v_k^*.$$

Целевые показатели:

$F_{T(i,j)}(t)$  — функция распределения вероятностей (ФРВ) времени доставки сообщений в направлении  $\langle i, j \rangle$ .

$F_T(t)$  – ФРВ времени доставки сообщений в сети в целом.

Вероятность своевременной доставки  $Pr\{T \leq T^*\}$ .

**Задача оптимизации:**

Найти набор таблиц маршрутизации пакетов (ТМП)  $\mathcal{P}$ , который максимизирует вероятность своевременной доставки сообщений

при заданных ограничениях на ресурсы в кластерной структуре сети:

$$Pr\{T \leq T^*\} \rightarrow \max_p.$$

### Основные результаты

Методика анализа ВВХ для кластеризованной СОД включает следующие этапы:

#### 1. Вычисление условных потоков по маршрутам.

Для каждого кластера и межкластерных направлений вычисляются интенсивности потоков  $s(\mu)$  по формуле (10) из [1].

#### 2. Учет служебного трафика.

Вводятся дополнительные потоки  $\lambda^{\text{служ}}$ , обусловленные обменом служебной информацией между хабами и узлами кластеров.

#### 3. Расчет нагрузки на средства связи.

По формулам (7) и (8) из [1] вычисляются ресурсы передающих и приемных средств с учетом кластерной структуры.

#### 4. Расчет ВВХ для линий и маршрутов.

Для каждой линии  $(k, l)$  ФРВ времени задержки пакета определяется соотношением

$$F_{T(k,l)}(t) = 1 - e^{-\frac{t}{T(k,l)}}, T(k,l) = \frac{1}{c_{k,l}} \left( \frac{u_k}{1 - u_k} + \frac{v_l}{1 - v_l} \right).$$

Для маршрута  $\mu$  ФРВ времени задержки вычисляется как свертка распределений задержек на участках маршрута.

#### 5. Усреднение по направлениям и сети.

ФРВ времени доставки в направлении  $\langle i, j \rangle$  и в сети в целом вычисляются по формулам (15)–(17) из [1].

#### 6. Оценка вероятности своевременной доставки [1].

Вычисляются вероятности:

$$Pr\{T_{(i,j)} \leq T^*\} = F_{T_{(i,j)}}(T^*), Pr\{T \leq T^*\} = F_T(T^*).$$

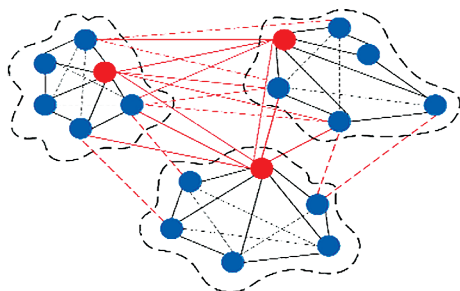


Рис. 1. Пример кластеризованной сетевой структуры (фрагмент)

**Примеры расчета.** Рассмотрена СОД группы БПЛА, состоящая из 96 узлов, разбитых на 16 кластеров, надкластерный фрагмент представлен в виде трех кластеров, содержащих 5, 5 и 6 узлов, соответствующих центральным узлам кластеров. На рисунке 1 приведена структурная схема, иллюстрирующая связность узлов, причем узлы, входящие в общий кластер, обведены пунктирной линией.

В качестве исходных данных приняты оценки компонент:

- наборов матриц потенциальных пропускных способностей  $(i, j)$ -радиолиний  $k$ -кластера  $C^k = (c_{(i,j)}^k)$ ;
- наборов матриц интенсивностей информационных потоков в  $\langle i, j \rangle$ -направлениях  $k$ -кластера  $\Lambda^k = (\lambda_{(i,j)}^k)$  (т. е. матриц тяготения);
- векторов ресурсов  $U^*, V^*$  (из расчета по одному радиопередающему средству и двум приемным на каждом узле);
- ТМП  $\mathcal{P}$ , допускающие рандомизированные и детерминированные алгоритмы маршрутизации [3].

**Результаты расчетов.** Расчеты величины  $Pr\{T_{(i,j)} \leq T^*\}$  проводились для различных параметров состояния сети, характеризующихся показателями  $(c_{(i,j)}^k), (\lambda_{(i,j)}^k)$ . Для иллюстрации выигрыша, обеспечиваемого кластеризацией структуры СОД, результаты расчетов представлены на рисунке 2 зависимостями времени  $T$  доставки пакета сообщения с вероятностью  $P^*$  (т. е.  $Pr\{T \leq T^*\} \leq P^*$  от состояния СОД, характеризующегося отношением  $\lambda/c$  для случаев а) некластеризованная и б) кластеризованная структура при  $P^* = P_1^* = 0,95$  и  $P^* = P_2^* = 0,99$ .

Результаты расчетов по рассмотренному примеру показали, что кластеризация структуры СОД привела к снижению интенсивности

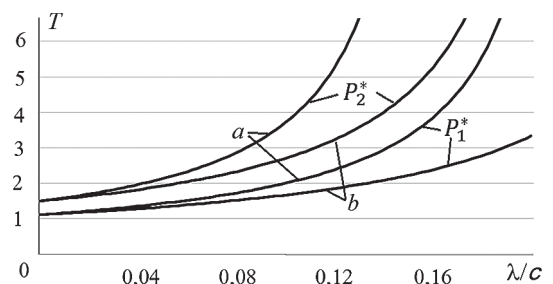


Рис. 2. Зависимость времени задержки пакетов, обеспечиваемого с вероятностью  $P^*$ :  
а) в некластеризованной СОД,  
б) в кластеризованной СОД



потоков служебных данных о состоянии СОД на 15–25 %. При этом коэффициент загрузки СОД служебными данными в кластеризованной сети сократился при периодичности цикла обновления набора ТМП 5с с 50% до 15%, а при периодичности 2с с 80% до 30%.

Из полученных результатов следует, что кластеризация обеспечивает выигрыш, оцениваемый приростом пропускной способности СОД на 15–25 % и соответствующим увеличением устойчивости системы.

### Заключение

Предложенная методика анализа эффективности функционирования СОД БПЛА обеспечивает определение показателей устойчивости сети с кластеризованной структурой

и определяет принципы повышения устойчивости СОД к случайным и преднамеренным дестабилизирующим воздействиям. На рассмотренных примерах получены оценки выигрыша в устойчивости СОД по отношению как отказам объектов системы, так и воздействию помех на радиолинии связи, которые свидетельствуют о целесообразности кластеризации структуры СОД при разработке алгоритмов управления маршрутизацией.

Актуальными задачами следует считать разработку методов оптимальной кластеризации структуры СОД с учетом мобильности БПЛА как носителей средств ретрансляции и коммутации потоков данных, а также с учетом функций по восстановлению сети при ее разрушении.

### Литература

1. Чуднов А. М., Губская О. А., Кичко Я. В. Методика анализа вероятностно-временных характеристик обмена сообщениями в комплексе беспилотных летательных аппаратов // Известия ТулГУ. Технические науки. 2021. Вып. 11. С. 117–124.
2. Чуднов А. М., Положинцев Б. И., Кичко Я. В. Анализ помехозащищенности обмена данными группы беспилотных летательных аппаратов в условиях оптимизированных помех Радиотехника. 2022. Т. 86. № 12. С. 33–46. DOI: <https://doi.org/10.18127/j00338486-202212-03>.
3. Чуднов А. М. Математические основы моделирования, анализа и синтеза систем. – СПб.: ВАС, 2021. – 192 с.
4. Jan Lansky, Saqib Ali, Amir Masoud Rahmani, Mohammad Sadegh Yousefpoor, Efat Yousefpoor, Faheem Khan, Mehdi Hosseinzadeh Reinforcement Learning-Based Routing Protocols in Flying Ad Hoc Networks (FANET): 1 Mathematics 2022, 10, 3017. DOI:10.3390/math10163017.
5. Siddiqi M. A., Vivendi C., Jaroslava K., Anumbe N. Analysis on security-related concerns of unmanned aerial vehicle: Attacks, limitations, and recommendations. Math. Biosci. Eng. 2022, 19, 264/1–2670.
6. Rovira-Sugranes A., Razi A., Afghah F., Chakareski J. A review of AI-enabled routing protocols for UAV networks: Trends, challenges, and future outlook. Ad Hoc Netw. 2022, 130, 102790. DOI:10.48550/arXiv.2104.01283.
7. Rezwan S. Choi W. A survey on applications of reinforcement learning in flying ad hoc networks. Electronics 2021, 10, 449. DOI: 10.3390/electronics10040449.
8. Shrestha R., Bajracharya R., Kim S. 6G enabled unmanned aerial vehicle traffic management: A perspective. IEEE Access 2021, 9, 91119–91136. DOI:10.1109/ACCESS.2021.3092039.
9. Sirajuddin M., Rupa C., Iwendi C., Biamba C. TBSMR: A trust-based secure multipath routing protocol for enhancing the qos of the mobile ad hoc network. Secur. Commun. Netw. 2021, 2021. DOI:10.1155/2021/5521713.
10. Деркач А. Е., Чуднов А. М. Методика структурирования сети обмена данными роя беспилотных летательных аппаратов для обеспечения устойчивого их взаимодействия // В сборнике: Подготовка профессиональных кадров в магистратуре в эпоху цифровой трансформации (ПКМ-2024). Сборник лучших докладов V Всероссийской научно-технической и научно-методической конференции магистрантов и их руководителей. В 2-х томах. Санкт-Петербург, 2025. С. 622–629.
11. Alam M. M., Moh S. Survey on Q-Learning-Based Position-Aware Routing Protocols in Flying Ad Hoc Networks. Electronics 2022, 11, 1099. DOI:10.3390/electronics11071099.
12. Liu T., Sun Y., Wang C., Zhang Y., Qiu Z., Gong W., Lei S., Tong X., Duan X. Unmanned aerial vehicle and artificial intelligence revolutionizing efficient and precision sustainable forest management. J. Clean. Prod. 2021, 311, 127546. DOI: 10.1016/j.jclepro.2021.127546.
13. Khan M. F., Yau K. L. A., Ling M. H., Imran M. A., Chong Y. W. An Intelligent Cluster-Based Routing Scheme in 5G Flying Ad Hoc Networks. Appl. Sci. 2022, 12, 3665. DOI:10.3390/app12073665.

14. Arafat M. Y., Moh S. A. Q-learning-based topology-aware routing protocol for flying ad hoc networks. IEEE Internet Things J. 2021, 9, 1985–2000. DOI: 10.1109/JIOT.2021.3089759.
15. Cui Y., Zhang Q., Feng Z., Wei Z., Shi C., Yang H. Topology-Aware Resilient Routing Protocol for FANETs: An Adaptive Q-Learning Approach. IEEE Internet Things J. 2022. DOI:10.48550/arXiv.2306.17360.
16. Zhang M., Dong C., Feng S., Guan X., Chen H., Wu Q. Adaptive 3D routing protocol for flying ad hoc networks based on prediction-driven Q-learning. China Commun. 2022, 19, 302–317. DOI:10.23919/JCC.2022.05.005.
17. Макаренко С. И. Усовершенствование функций многоуровневой иерархической кластеризации протокола маршрутизации рпнп с целью повышения устойчивости сети связи // I-methods. 2020. Т. 12. № 2. С. 1–21.
18. Guo J., Gao H., Liu Z., Huang F., Zhang J., Li X., Ma J. ICRA: An Intelligent Clustering Routing Approach for UAV Ad Hoc Networks. IEEE Trans. Intell. Transp. Syst. 2022, 1–14. DOI:10.1109/TITS.2022.3145857.
19. Idrissi M., Salami M., Annaz F. A Review of Quadrotor Unmanned Aerial Vehicles: Applications, Architectural Design and Control Algorithms. J. Intell. Robot. Syst. 2022, 104, 1–33. DOI:10.1007/s10846-021-01527-7.
20. Rovira-Sugranes A., Afghah F., Qu J., Razi A. Fully-echoed Q-routing with Simulated Annealing Inference for Flying Adhoc Networks. IEEE Trans. Netw. Sci. Eng. 2021, 8, 2223–2234. DOI:10.48550/arXiv.2103.12870.
21. Da Costa L. A. L., Kunst R., de Freitas E. P. Q-FANET: Improved Q-learning based routing protocol for FANETs. Comput. Netw. 2021, 198, 108379. DOI: 10.1016/J.COMNET.2021.108379.
22. Agrawal J., Kapoor M. A comparative study on geographic-based routing algorithms for flying ad hoc networks. Concurrency and Computation: Practice and Experience. 2021, 33(16). DOI:10.1002/cpe.6253.

## PRINCIPLES OF INCREASING THE STABILITY OF THE DATA EXCHANGE NETWORK OF A LARGE GROUP OF UAVS BASED ON CLUSTERING OF ITS STRUCTURE

*Derkach A. E.<sup>5</sup>, Limantseva E. V.<sup>6</sup>, Chudnov A.M.<sup>7</sup>*

**Keywords:** packet-switched network, network capacity, network resilience, packet routing management, packet routing tables, network exchange self-organization.

### **Abstract**

**The purpose of the work** is to increase the stability of the data exchange network of a large group of unmanned aerial vehicles (UAVs) to destabilizing effects due to the dynamic optimization of its structure.

**Research methods:** queuing network theories, control theory, dynamic programming.

**Results of the study:** the principles of analysis and optimization of the structure of the data exchange system of a large group (swarm) of UAVs with a clustered packet routing structure have been developed. It is shown that the increase in the efficiency of the data exchange network (DPN) can be due to the reduction of traffic required for data collection

**The scientific novelty** of the results lies in the development of a new model of data exchange in a large-scale ODS, which takes into account the clustered structure in the process of routing management, as well as the formulation and development of a method for solving the problem of optimizing the clustered network structure.

### **References**

1. Chudnov A. M., Gubskaja O. A., Kichko Ja. V. Metodika analiza veroyatnostno-vremennykh harakteristik obmena soobshhenijami v komplekse bespilotnykh letatel'nykh apparatov // Izvestija TulGU. Tehnicheskie nauki. 2021. Vyp. 11. S. 117–124.
2. Chudnov A. M., Polozhincev B. I., Kichko Ja. V. Analiz pomehozashchishhennosti obmena dannymi gruppy bespilotnykh letatel'nykh apparatov v usloviyah optimizirovannykh pomeh Radiotekhnika. 2022. T. 86. № 12. S. 33–46. DOI: <https://doi.org/10.18127/j00338486-202212-03>.

<sup>5</sup> Alexey E. Derkach, Adjunct of the Military Academy of Communications, St. Petersburg, Russia. E-mail: alder2000@inbox.ru

<sup>6</sup> Elena V. Limantseva, Adjunct of the Military Academy of Communications, St. Petersburg, Russia. E-mail: lena.limantseva@mail.ru

<sup>7</sup> Alexander M. Chudnov, Dr.Sc. of Technical Sciences, Professor, Professor of the Military Academy of Communications named after Marshal of the Soviet Union S. M. Budyonny, St. Petersburg, Russia. E mail: chudnow@yandex.ru

3. Chudnov A. M. *Matematicheskie osnovy modelirovaniya, analiza i sinteza sistem.* – SPb.: VAS, 2021. – 192 s.
4. Jan Lansky, Saqib Ali, Amir Masoud Rahmani, Mohammad Sadegh Yousefpoor, Efat Yousefpoor, Faheem Khan, Mehdi Hosseinzadeh *Reinforcement Learning-Based Routing Protocols in Flying Ad Hoc Networks (FANET): 1 Mathematics* 2022, 10, 3017. DOI:10.3390/math10163017.
5. Siddiqi M. A., Vivendi C., Jaroslava K., Anumbe N. Analysis on security-related concerns of unmanned aerial vehicle: Attacks, limitations, and recommendations. *Math. Biosci. Eng.* 2022, 19, 264/1–2670.
6. Rovira-Sugranes A. Razi A. Afghah F. Chakareski J. A review of AI-enabled routing protocols for UAV networks: Trends, challenges, and future outlook. *Ad Hoc Netw.* 2022, 130, 102790. DOI:10.48550/arXiv.2104.01283.
7. Rezwan S., Choi W. A survey on applications of reinforcement learning in flying ad hoc networks. *Electronics* 2021, 10, 449. DOI:10.3390/electronics10040449.
8. Shrestha R., Bajracharya R., Kim S. 6G enabled unmanned aerial vehicle traffic management: A perspective. *IEEE Access* 2021, 9, 91119–91136. DOI:10.1109/ACCESS.2021.3092039.
9. Sirajuddin M., Rupa C., Iwendi C., Biamba C. TBSMR: A trust-based secure multipath routing protocol for enhancing the qos of the mobile ad hoc network. *Secur. Commun. Netw.* 2021, 2021. DOI:10.1155/2021/5521713.
10. Derkach A. E., Chudnov A. M. Metodika strukturirovaniya seti obmena dannymi roza bespilotnykh letatel'nykh apparatov dlja obespecheniya ustojchivogo ih vzaimodejstviya // V sbornike: Podgotovka professional'nykh kadrov v magistrature v jepohu cifrovoj transformacii (PKM-2024). Sbornik luchshih dokladov V Vserossijskoj nauchno-tehnicheskoy i nauchno-metodicheskoy konferencii magistrantov i ih rukovoditelej. V 2-h tomah. Sankt-Peterburg, 2025. S. 622–629.
11. Alam M. M., Moh S. Survey on Q-Learning-Based Position-Aware Routing Protocols in Flying Ad Hoc Networks. *Electronics* 2022, 11, 1099. DOI:10.3390/electronics11071099.
12. Liu T., Sun Y., Wang C., Zhang Y., Qiu Z., Gong W., Lei S., Tong X., Duan X. Unmanned aerial vehicle and artificial intelligence revolutionizing efficient and precision sustainable forest management. *J. Clean. Prod.* 2021, 311, 127546. DOI:10.1016/j.jclepro.2021.127546.
13. Khan M. F., Yau K. L. A., Ling M. H., Imran M. A., Chong Y. W. An Intelligent Cluster-Based Routing Scheme in 5G Flying Ad Hoc Networks. *Appl. Sci.* 2022, 12, 3665. DOI:10.3390/app12073665.
14. Arafat M. Y., Moh S. A. Q-learning-based topology-aware routing protocol for flying ad hoc networks. *IEEE Internet Things J.* 2021, 9, 1985–2000. DOI:10.1109/JIOT.2021.3089759.
15. Cui Y., Zhang Q., Feng Z., Wei Z., Shi C., Yang H. Topology-Aware Resilient Routing Protocol for FANETs: An Adaptive Q-Learning Approach. *IEEE Internet Things J.* 2022. DOI:10.48550/arXiv.2306.17360.
16. Zhang M., Dong C., Feng S., Guan X., Chen H., Wu Q. Adaptive 3D routing protocol for flying ad hoc networks based on prediction-driven Q-learning. *China Commun.* 2022, 19, 302–317. DOI:10.23919/JCC.2022.05.005.
17. Makarenko S. I. Uovershenstvovanie funkciy mnogourovnevoj ierarhicheskoy klasterizacii protokola marshrutizacii pnni s cel'ju povysheniya ustojchivosti seti svyazi // I-methods. 2020. T. 12. № 2. S. 1–21.
18. Guo J., Gao H., Liu Z., Huang F., Zhang J., Li X., Ma J. ICRA: An Intelligent Clustering Routing Approach for UAV Ad Hoc Networks. *IEEE Trans. Intell. Transp. Syst.* 2022, 1–14. DOI:10.1109/TITS.2022.3145857.
19. Idrissi M., Salami M., Annaz F. A Review of Quadrotor Unmanned Aerial Vehicles: Applications, Architectural Design and Control Algorithms. *J. Intell. Robot. Syst.* 2022, 104, 1–33. DOI:10.1007/s10846-021-01527-7.
20. Rovira-Sugranes A., Afghah F., Qu J., Razi A. Fully-echoed Q-routing with Simulated Annealing Inference for Flying Adhoc Networks. *IEEE Trans. Netw. Sci. Eng.* 2021, 8, 2223–2234. DOI:10.48550/arXiv.2103.12870.
21. Da Costa L. A. L., Kunst R., de Freitas E. P. Q-FANET: Improved Q-learning based routing protocol for FANETs. *Comput. Netw.* 2021, 198, 108379. DOI: 10.1016/J.COMNET.2021.108379.
22. Agrawal J., Kapoor M. A comparative study on geographic-based routing algorithms for flying ad hoc networks. *Concurrency and Computation: Practice and Experience.* 2021, 33(16). DOI:10.1002/cpe.6253.



# РАСПРЕДЕЛЕНИЕ НАГРУЗКИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ВОЕННОГО НАЗНАЧЕНИЯ

Алленов Д. С.<sup>1</sup>, Курбанов С. Н.<sup>2</sup>

DOI:10.21681/3034-4050-2026-1-8-15

**Ключевые слова:** балансировка нагрузки, алгоритм кругового обслуживания, сеть CDN, методы кластеризации, аппарат не четкой логики, интеллектуальные технологии.

## Аннотация

**Цель:** на основе общих теоретических положений и актуальных релевантных работ рассмотреть вопросы распределения вычислительной нагрузки и статистических данных по серверам пунктов управления.

**Метод исследования:** обзор работ, посвященных вопросам балансировки нагрузки на сервера. Анализ публикаций по вопросам распределения данных и вычислительных задач между серверами.

**Результаты исследования:** обоснована необходимость учитывать при распределении нагрузки такие параметры состояния серверов на пунктах управления (ПУ), как загруженность вычислительных ресурсов, взаимное географическое положение должностного лица (ДЛ) и сервера, а также пропускную способность каналов связи.

**Практическая ценность:** заключается в обосновании целесообразности применения балансировки нагрузки на серверах информационной сети тактического звена управления для качественного и своевременного решения информационно-расчетных задач.

## Введение

В настоящее время в гражданской и военной сферах используются различные подходы к распределению вычислений и хранения данных, включая алгоритмы Round Robin, Least Connections, Weighted Load Balancing, IP Hash и др. Эти методы значительно повышают производительность информационных сетей, но зависимы от разнообразия решаемых задач и географического расположения серверов.

В настоящей статье рассматривается проблема распределения нагрузки между серверами информационной сети тактического звена и обосновываются пути ее решения. Приводятся существующие методы и алгоритмы решения задачи балансировки нагрузки.

## Основная часть

Информационные системы специального назначения эксплуатируются в условиях высокой интенсивности информационного обмена и динамически изменяющихся нагрузок, что предъявляет повышенные требования к устойчивости их функционирования, скорости обработки данных и способности к адаптивному масштабированию вычислительных ресурсов.

В укрупненном виде архитектура информационной системы специального назначения показана на (рис.1), где должностные лица (ДЛ), от командиров подразделений до высшего командования штабов, используя соответствующую техническую основу, а также общие и прикладные сервисы, способны своевременно обмениваться необходимой информацией.

Особенно остро эти требования проявляются в сфере построения и эксплуатации систем управления тактического звена, где время отклика, надежность обработки информации и рациональное использование вычислительных ресурсов, критически важны для выполнения задач в быстроменяющейся обстановке, что и показывает их актуальность в специальной военной операции (СВО) [1].

С увеличением объемов обрабатываемой информации и возрастанием числа пользователей, взаимодействующих с информационной системой, ключевым становится вопрос правильного распределения вычислительной нагрузки между доступными ресурсами.

Рост объемов обрабатываемых данных и количества активных пользователей приводит к неравномерному распределению информационных потоков между элементами систе-

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

<sup>2</sup> Курбанов Сергей Николаевич, преподаватель кафедры информатики и вычислительной техники инженерного факультета Академия гражданской защиты Министерства Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий имени генерал-лейтенанта Д. И. Михайлика, г. Химки, Московская область, Россия. E-mail: s.kurbanov@agz.50.mchs.gov.ru



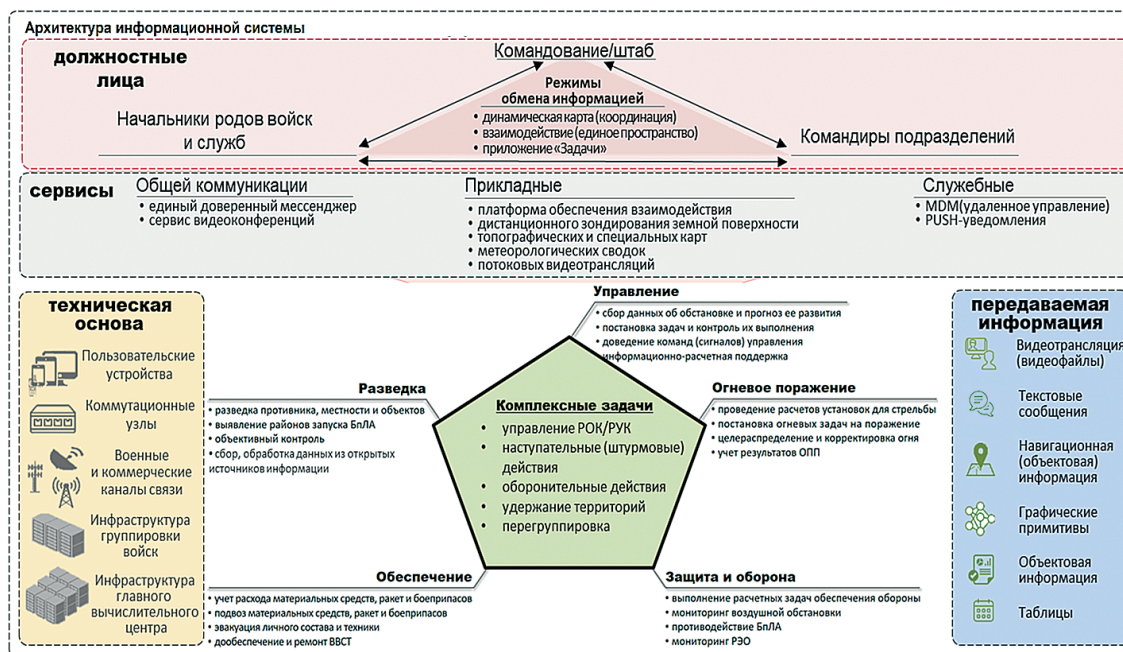


Рис. 1. Архитектура информационной системы специального назначения

мы, что, в свою очередь, негативно сказывается на общей производительности и времени отклика информационной системы.

Использование традиционных архитектур клиент-серверных приложений без внедрения механизмов балансировки нагрузки не позволяет обеспечить необходимый уровень отказоустойчивости и производительности в условиях переменной интенсивности запросов и ограниченности вычислительных ресурсов сетевых узлов.

В распределённых информационных системах под балансировкой нагрузки понимается процесс целенаправленного управления

потоками входящих запросов, при котором осуществляется их перераспределение между несколькими серверными узлами с учётом текущего состояния вычислительных ресурсов. Реализация данного процесса позволяет обеспечить требуемые показатели быстродействия, повысить устойчивость системы к отказам и сократить задержки при обработке запросов пользователей [2].

В настоящее время в различных информационных структурах используются различные методы распределения нагрузки, включая алгоритмы Round Robin, Least Connections, Weighted Load Balancing, IP Hash и др. (рис. 2).

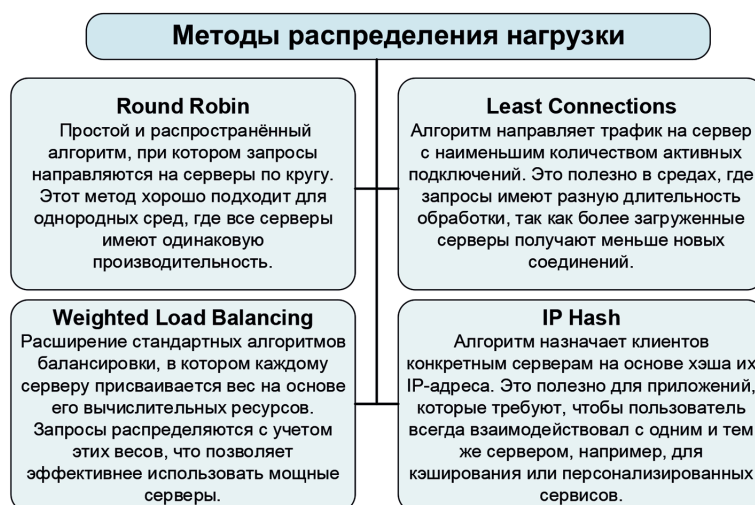


Рис. 2. Методы распределения нагрузки

Каждый из этих методов обладает своими преимуществами и ограничениями, в зависимости от конфигурации вычислительного кластера и специфики решаемых задач.

Особенность информационных систем специального назначения заключается в наличии специфических требований: высокая плотность и изменчивость трафика, необходимость быстрого принятия решений, ограниченность вычислительных ресурсов и каналов связи. При этом эффективность функционирования систем управления во многом зависит от состояния серверного комплекса, их загрузки, географического расположения и пропускной способности каналов связи.

С учетом этого, использование традиционных алгоритмов распределения нагрузки, не учитывающих текущие параметры состояния серверов, приводит к задержкам в обработке запросов и снижению оперативности принятия решений.

В условиях современных вызовов и ограничений становится актуальным использование интеллектуальных методов анализа и управления, таких как кластеризация, нейросетевые подходы и элементы нечёткой логики. Эти методы позволяют адаптировать поведение балансировщика к текущей ситуации в вычислительной системе, обеспечивая более точное и рациональное распределение запросов между серверами.

Кластерный анализ и алгоритмы, такие как К-средних и С-средних, позволяют формировать группы запросов по признакам их принадлежности к определённым вычислительным ресурсам. Нечёткая логика, в свою очередь, расширяет возможности принятия решений в условиях неопределённости параметров состояния [3].

Реализация интеллектуальных подходов к управлению вычислительными ресурсами позволяет повысить оперативность, масштабируемость и эффективность информационных систем специального назначения, что особенно важно в условиях выполнения боевых задач.

Специальные информационные системы в статье рассматриваются на уровне тактического звена управления и охватывают соединения, части и подразделения уровня бригады, батальона, роты и взвода. Система управления (СУ) тактического звена управления предназначена для организации, координации и контроля действий подразделений в ходе

выполнения боевых задач. Она, включает в себя органы управления (ОУ), пункты управления (ПУ) различного уровня, средства управления, средства автоматизации управления и системы связи, а также другие специальные системы [1]. Главная цель СУ – обеспечить принятие своевременных решений, передачу приказов и донесений, а также устойчивую связь между командованием и подчинёнными ПУ.

Система управления строится на основе принципов централизации руководства, непрерывности, оперативности, устойчивости и скрытности [4]. Главная роль принадлежит командирам и штабам, которые принимают решения, доводят приказы и контролируют их выполнение.

Основные угрозы для СУ – радиоэлектронное противодействие, кибератаки и разрушение узлов связи. Для повышения устойчивости СУ создаются резервные ПУ, используются мобильные средства связи, применяются автоматизированные системы защиты и восстановления связи, а также подготавливается личный состав к работе в условиях потери связи.

Использование современных систем автоматизации обеспечивает возможность интеграции различных по своей природе каналов связи. Обмен информацией в СУ организован по функциональным направлениям: оперативное, разведывательное, тыловое, артиллерийское, инженерное, связи и др. Поток информации делится на приказы, распоряжения, донесения, отчёты и запросы. Основные направления обмена: от вышестоящего командования к подчинённым (приказы) и от подчинённых к командованию (донесения, отчёты). Информация передаётся по регламентированным каналам связи и в установленные сроки. Фрагмент структуры обмена данными с перечнем необходимой информации для постановки задач расчетам с рабочего места ПУ подразделением приведен на (рис. 3).

Организация обмена данными в СУ подчинена принципам иерархичности и функциональности. Каждый тип донесений имеет установленную форму и периодичность. Для обеспечения устойчивости применяются резервные каналы связи и дублирование данных. Внедряются меры защиты информации: шифрование, контроль целостности и аутентификация пользователей.



Рис. 3. Структура обмена данными между ПУ и должностными лицами расчетов

Одним из подходов к совершенствованию СУ за счет рационального построения информационной системы, является равномерное (сбалансированное) распределение статистической информации и вычислительной нагрузки между ОУ и ПУ. В настоящее время такие задачи решаются с использованием систем балансировки.

В связи с повышением требований предъявляемых к специализированным информационным системам, таких как скорость, объем передаваемой информации, появляется потребность в разработке нового математического, алгоритмического и программно-аппаратного обеспечения. Для повышения производительности информационных систем разрабатывают новые методы хранения и кэширования больших объемов данных обеспечивающих программное уменьшение объема данных, циркулирующих в телекоммуникационных сетях, и одновременного повышения скорости их доставки [5]. Разработка программ, обеспечивающих производительность информационных систем при работе с обширными массивами данных является актуальной научно-практической задачей. Это особенно важно в контексте опыта, полученного в ходе СВО, что стимулирует поиск и создание прогрессивных подходов к разрешению возникающих задач.

В дополнение к этому, важно установить характеристики работы серверного оборудо-

вания на ПУ, которые оказывают влияние на быстроту передачи информации ДЛ. Также необходимо провести изучение полученных параметров функционирования для последующего оптимального перераспределения запросов клиент-серверных приложений.

Серверы ПУ в современной информатике играют ключевую роль в распределенных вычислительных системах, находя широкое применение в архитектуре клиент-серверных приложений с высокой интенсивностью запросов и в сетях распространения контента (CDN). Сети доставки контента (CDN) представляют собой распределённые вычислительные инфраструктуры, в которых серверные узлы размещаются с учётом географического положения пользователей. Такой подход позволяет минимизировать задержки при передаче данных и снизить нагрузку на магистральные каналы связи за счёт использования ближайших к пользователю серверов. [6].

Состояние вычислительных мощностей и загруженность серверных ресурсов ПУ напрямую влияют на скорость доставки информации и выполнение вычислений. Следовательно, оптимальное распределение нагрузки оказывает непосредственное воздействие на скорость обработки пользовательских запросов. Перераспределение между серверами пользовательской нагрузки поступающей от автоматизированного рабочего места (АРМ) ДЛ, на конкретные серверы осуществляет



балансировщик нагрузки (рис. 4). При этом используются соответствующие программы балансировки [7].

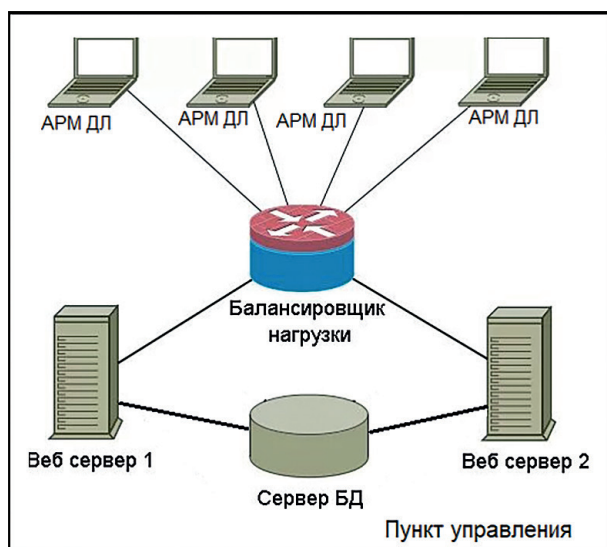


Рис. 4. Балансировка нагрузки на пункте управления

Скорость передачи данных клиент-серверных приложений зависит и от задач решаемых ДЛ (обмен файлами, электронная почта, обмен

картографической информацией и передача данных), использующих приложение, их географического местоположения, что и необходимо учитывать при выполнении анализа текущего состояния параметров состояния клиент-серверного приложения информационной системы специального назначения.

Следовательно, решение проблемы увеличения скорости доставки информации клиент-серверных приложений и информационных систем достигается за счет разработки программного обеспечения (ПО), выполняющего анализ больших объемов данных параметров состояния серверов и данных о АРМ ДЛ, а также ПО, обеспечивающего оптимизацию распределения данных между серверами.

Для этого в настоящее время активно используются сети доставки данных CDN и средства балансировки нагрузки.

Важными аспектами построения CDN являются географические размещения серверов и распределения копий данных на этих серверах, которые обеспечивают оптимизацию доставки данных конечному ДЛ. Порядок распределения запросов ДЛ приведены на рисунке 4.

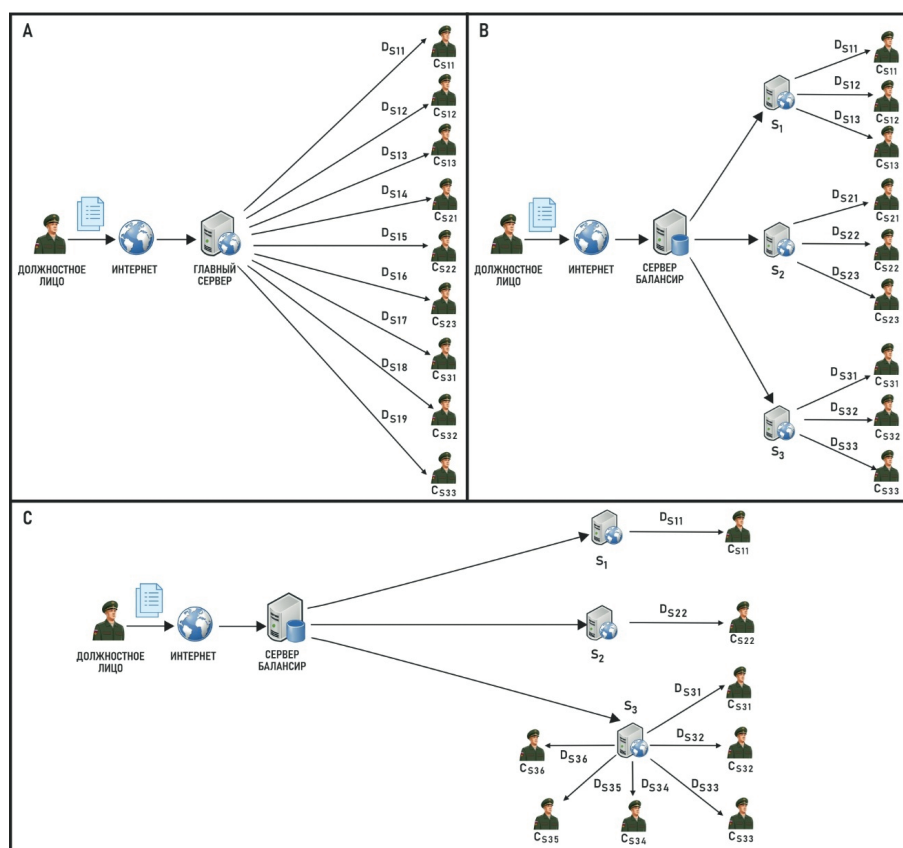


Рис. 4. Порядок распределения запросов должностных лиц



На фрагменте А (рис. 4) показано, когда дублирование данных не производится, а запросы всех ДЛ обрабатываются одним сервером. Вариант распределения запросов ДЛ при размещении копий данных на всех серверах приведен на фрагменте В рисунка 4. Распределение файлов на сервера по первому требованию и последующее удаление копии после интервала времени, за которое данные не были востребованы с данного сервера приведено на фрагмент С (рис. 4).

Размещение копий данных на этих серверах важно, так как рациональное размещение уменьшает как задержку доставки данных для их ДЛ, так и доступную пропускную способность. Таким образом, для распределения данных по серверам стоит учитывать сетевые характеристики (полоса пропускания канала, географическое расстояние от ДЛ до сервера или количество граничных узлов (Hop Count)).

Для распределения вычислительной нагрузки используется сервер-балансир. Такой сервер принимает запросы ДЛ и перераспределяет их на наиболее подходящий сервер для решения вычислительной задачи в данный момент времени. Определение наиболее подходящего сервера происходит на основании заданного алгоритма выбора. В качестве таких алгоритмов выступает алгоритм кругового распределения (Round Robin), взвешенный

алгоритм кругового распределения (Weighted Round Robin), балансировка на основе агента.

Варианты обработки запросов пользователей при отсутствии и при наличии сервера балансировки приведены на рисунке 5). На фрагменте А этого рисунка представлена схема без балансировки нагрузки, при которой все запросы от всех ДЛ адресуются на единственный сервер, производящий вычисления. На фрагменте В представлена схема, при которой запросы ДЛ попадают из внешней сети на сервер-балансир и перенаправляются на наиболее подходящий сервер для вычислений. При этом повышается отказоустойчивость и надежность клиент-серверного приложения.

Решение задачи оптимизации распределения нагрузки предлагается решать методами кластеризации [8]. Кластерный анализ представляет собой процесс группировки объектов выборки в классы. Следовательно, выбор оптимального сервера, необходимо классифицировать через запросы пользователей по серверам, учитывая ранее обозначенные требования. Предлагается выполнять разделение запросов пользователей по узлам вычислительной системы таким образом, чтобы минимизировать загрузку серверов, при этом обеспечивая наилучшую скорость передачи данных конечному пользователю.

Рассмотрим методы кластеризации. Результаты кластеризации могут быть представлены в виде четкого отнесения к кластеру (запрос принадлежит кластеру или нет) или в виде нечеткого отнесения, где запрос пользователя имеет определенную вероятность принадлежности к кластеру. Наиболее распространенные алгоритмы – К-средних и С-средних. Нейронные сети также могут быть использованы для решения задачи распределения вычислительной нагрузки посредством кластерного анализа [9].

Алгоритм К-средних итеративно пересчитывает центры масс кластеров, перераспределяя запросы в соответствии с близостью к новым центрам. Цель – распределить запросы по кластерам (серверам) так, чтобы каждый запрос был отнесен к одному серверу. Алгоритм С-средних позволяет пользователю принадлежать к разным серверам с разной степенью принадлежности.

Однако кластерный анализ может привести к ситуации, когда запросы трудно разделить по серверам из-за схожести параметров

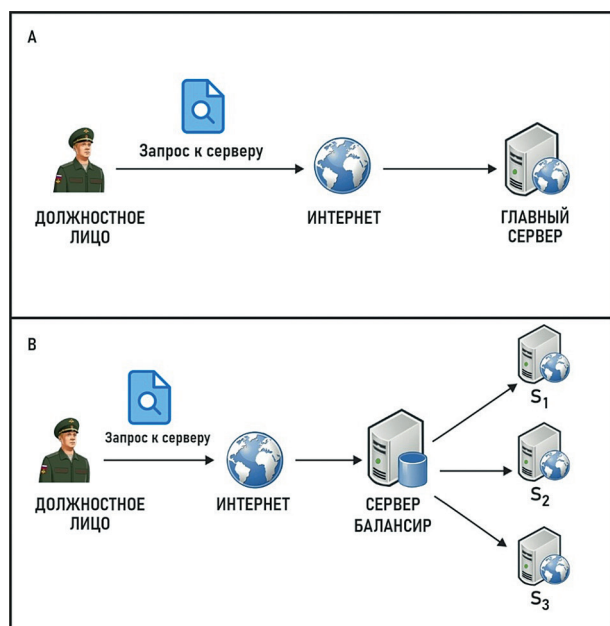


Рис. 5. Обработка запросов пользователей при отсутствии и при наличии сервера балансировки

состояния серверов. В условиях близких значений параметров состояния серверов целесообразным является применение аппарата нечёткой логики, позволяющего учитывать степень принадлежности пользовательского запроса к каждому серверному узлу. Такой подход повышает гибкость принятия решений и устойчивость алгоритма балансировки нагрузки в условиях неопределённости входных данных. [10].

### Выводы

Географический разброс и частые перемещения пунктов управления в тактическом звене управления приводят к временным задержкам при обработке запросов от должностных лиц, особенно когда серверы неравномерно загружены, что в свою очередь, снижает оперативность выполнения, а иногда и срыву

поставленных задач в быстро меняющейся обстановке.

Большинство существующих информационных систем используют круговое распределение нагрузки, не учитывая при этом, состояния серверного оборудования.

Алгоритмы балансировки нагрузки серверов позволяют учитывать их взаимное расположение, загруженность и пропускную способность каналов связи.

Применение алгоритмов балансировки нагрузки серверов в тактическом звене управления позволит повысить быстродействие, устойчивость и производительность высоконагруженных клиент-серверных приложений информационных систем, что в свою очередь, приведет к решению должностными лицами поставленных задач в установленные сроки с требуемым качеством.

### Литература

1. Иванов В. Г. Теория и практика построения и обеспечения функционирования системы связи специального назначения с учётом технологического развития и опытов вооружённых конфликтов: монография / В. Г. Иванов. – М.: Красная Звезда, 2025. – 303 с.
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. Осипова Ю. А., Лавров Д. Н. Применение кластерного анализа методом k-средних для классификации текстов научной направленности / Математические структуры и моделирование 2017. № 3(43). С. 108–121.
4. Иванов В. Г. Основы построения и оценки эффективности функционирования системы связи специального назначения в международном вооружённом конфликте на основе многосферной и конвергентной структуры ее элементов: Монография. – СПб.: ПОЛИТЕХ, 2023. – 298 с.
5. AlKhatib, A. A. Load Balancing Techniques in Software-Defined Cloud Computing: an overview / A. A. AlKhatib, T. Sawalha, S. AlZu'bi. – DOI: 10.1109/SDS49854.2020.9143874 // The Seventh International Conference on Software Defined Systems (Paris, France, 20-23 April 2020). – IEEE, 2020. – P. 240–244.
6. Курушин М. А. Что такое CDN: принципы работы Content Delivery Network URL: <https://timeweb.cloud/blog/cto-takoe-cdn-principy-raboty-content-delivery-network> (дата обращения: 6.01.2025).
7. 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.
8. 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.
9. 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.
10. Абрамов А. В. Интеллектуальный алгоритм балансировки нагрузки в распределённых системах на основе нечёткой логики / А. В. Абрамов, Д. А. Сидоров // Вестник компьютерных и информационных технологий. – 2021. – № 7. – С. 11–19..

# LOAD DISTRIBUTION IN MILITARY INFORMATION SYSTEMS

Allenov D. S.<sup>3</sup>, Kurbanov S. N.<sup>4</sup>

**Keywords:** load balancing, round-robin algorithm, CDN, clustering methods, fuzzy logic apparatus, intelligent technologies.

## Abstract

**The purpose of the work:** on the basis of general theoretical provisions and relevant works, to consider the distribution of the computational load and statistical data on the servers of control points.

**Research method:** review of works devoted to the issues of load balancing on servers. Analysis of publications on the distribution of data and computing tasks between servers.

**Results of the study:** the need to take into account such parameters of the state of servers at control centers (CPs) as the load of computing resources, the mutual geographical location of the official (DL) and the server, as well as the bandwidth of communication channels is substantiated.

**Practical value:** consists in substantiating the expediency of using load balancing on the servers of the information network of the tactical control link for high-quality and timely solution of information and calculation problems..

## References

1. Ivanov V. G. Teoriya i praktika postroeniya i obespecheniya funkcionirovaniya sistemy` svyazi special`no-go naznacheniya s uchytom texnologicheskogo razvitiya i opy`tov vooruzhenny`x konfliktov: monografiya / V. G. Ivanov. – M.: Krasnaya Zvezda, 2025. – 303 s.
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. Osipova Yu. A., Lavrov D. N. Primenenie klasternogo analiza metodom k-srednix dlya klassifikacii tekstov nauchnoj napravlenosti / Matematicheskie struktury` i modelirovanie 2017. № 3(43). S. 108–121.
4. Ivanov V. G. Osnovy` postroeniya i ocenki e`ffektivnosti funkcionirovaniya sistemy` svyazi special`no-go naznacheniya v mezhdunarodnom vooruzhennom konflikte na osnove mnogosfernoj i konvergentnoj struktury` ee e`lementov: Monografiya. – SPb.: POLITEX, 2023. – 298 s.
5. AlKhatib, A. A. Load Balancing Techniques in Software-Defined Cloud Computing: an overview / A. A. AlKhatib, T. Sawalha, S. AlZubi. – DOI: 10.1109/SDS49854.2020.9143874 // The Seventh International Conference on Software Defined Systems (Paris, France, 20-23 April 2020). - IEEE, 2020. – P. 240–244.
6. Kurushin M. A. Chto takoe CDN: principy` raboty` Content Delivery Network URL: <https://timeweb.cloud/blog/chto-takoe-cdn-principy-raboty-content-delivery-network> (data obrashheniya: 6.01.2025).
7. 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.
8. Ermakov D. S. Optimizaciya raspredeleniya nagruzki v oblachny`x vy`chislitel`ny`x sistemax na osnove metodov klasterizacii / D. S. Ermakov, A. L. Kuznecov // Informacionny`e tehnologii. – 2021. – № 4. – S. 215–222.
9. Kuznecov A. L. Intellektual`noe raspredelenie vy`chislitel`noj nagruzki v oblachny`x sistemax na osnove nejronny`x setej i klasternogo analiza / A. L. Kuznecov, D. S. Ermakov // Informacionny`e tehnologii. – 2022. – № 6. – S. 321–328.
10. Abramov A. V. Intellektual`ny`j algoritm balansirovki nagruzki v raspredelyonny`x sistemax na osnove nechotykoj logiki / A. V. Abramov, D. A. Sidorov // Vestnik komp`yuterny`x i informacionny`x tehnologij. – 2021. – № 7. – S. 11–19..

3 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

4 Sergey N. Kurbanov, Lecturer of the Department of Informatics and Computer Engineering, Faculty of Engineering, Academy of Civil Protection of the Ministry of the Russian Federation for Civil Defense, Emergencies and Elimination of Consequences of Natural Disasters named after Lieutenant General D. I. Mikhailik, Khimki, Moscow Region, Russia. E-mail: s.kurbanov@agz.50.mchs.gov.ru

# ИННОВАЦИОННЫЕ ТЕХНОЛОГИИ В ТЕЛЕКОММУНИКАЦИИ И ИХ ВЛИЯНИЕ НА ВОЕННУЮ СВЯЗЬ

Иванов В. Г.<sup>1</sup>, Лукьянчик В. Н.<sup>2</sup>, Кузин П. И.<sup>3</sup>

DOI:10.21681/3034-4050-2026-1-16-32

**Ключевые слова:** информационные технологии, стандарты 5G и 6G, облачные вычисления, интернет вещей (IoT), спутниковая связь, квантовые технологии.

## Аннотация

**Цель работы:** выполнить анализ инновационных технологий в телекоммуникации, определить наиболее востребованные и оценить их влияние на военную связь.

**Метод исследования:** методологическую основу исследования составила общая теория систем с использованием методов системного анализа и выборочного метода на основе соответствия параметров удовлетворяющих военной связи и системам военного управления.

**Результаты исследования:** рассмотрены и выбраны десять инфотелекоммуникационных технологий, которые по мнению авторов окажут существенное влияние на систему военной связи. К ним относится: мобильная связь 5G/6G, в которой осуществляется существенная трансформация и переход на новые форматы; облачные вычисления которые обеспечат развитие не только военной связи; технологии Интернет вещей обеспечивающие взаимодействия физических объектов между собой и/или с внешней средой, с применением специализированного оборудования, программного обеспечения; спутниковая связь на низкой околоземной орбите обеспечивающая предоставление широкополосного доступа в интернет, развития IoT-систем и услуг сотовой связи с применением технологии Direct-to-Device (D2D) «сети с прямым подключением устройств»; квантовые технологии реализующие новые методы инфотелекоммуникации и вычислений; технологии беспроводной связи Wi-Fi 7/Wi-Fi 8. обещающие увеличение максимальной скорости передачи данных в 13 раз выше скорости у Wi-Fi 5 и почти в пять раз – у Wi-Fi 6. Wi-Fi 7; Сети с искусственным интеллектом; технологии скоростного доступа FTTx широкополосной телекоммуникационной сети передачи данных, использующей в своей архитектуре волоконно-оптический кабель в качестве последней мили для обеспечения всей или части абонентской линии; программно-определяемые сети меняющие традиционный подход к управлению сетями, делая их более гибкими, управляемыми и адаптируемыми к требованиям потребителей услуг связи; системы когнитивного радио.

**Практическая полезность** заключается в обзоре и определении инновационных технологий в телекоммуникациях, которые окажут существенное влияние на развитие военной связи, системы управления войсками и оружием на перспективу до 2040 года.

## Введение

Опыт применения войск и оружия, а также организации управления и связи в ходе вооруженных конфликтов, особенно специальной военной операции (СВО) показывает, что помимо военных технологий успешно используются технологии «двойного» назначения. Следовательно, постоянно необходимо рассматривать современные и перспективные инфокоммуникационные технологий которые могут найти применение в военной связи уже сегодня или на ближайшую перспективу.

Термин «информационные технологии» (ИТ) чаще всего встречается в контексте инноваций, перспективных исследований и разработок, улучшения качества данных и их защиты, киберугроз, представления новых технологических реалий современного мира. Сегодня СУ ВН функционирует в условиях технической гетерогенности разнотипного телекоммуникационного оборудования и одновременного использования различных технологий передачи информации.

Развитие телекоммуникационной сферы обуславливается постоянно растущими

1 Иванов Василий Геннадьевич, доктор военных наук, доцент, профессор кафедры информатики и вычислительной техники инженерного факультета Академия гражданской защиты Министерства Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий имени генерал-лейтенанта Д. И. Михайлика. г. Химки, Россия. E-mail: wasj2006@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. г. Санкт-Петербург, Россия. E-mail: v-lukyanichik@bk.ru

3 Кузин Павел Игоревич, кандидат технических наук, доцент кафедры информационных систем и технологий Санкт-Петербургского государственного лесотехнического университета им. С. М. Кирова., г. Санкт-Петербург, Россия. E-mail: kuzik78@mail.ru



требованиями пользователей к доступу информации, при этом в качестве пользователей уже сегодня стали электронно-вычислительные машины в том числе с искусственным интеллектом. Проведенный анализ инновационных технологий в телекоммуникации позволил сформировать, рейтинг наиболее популярных инновационных технологий которые окажут существенное влияние на развитие систем военной связи (рис. 1).

### Основная часть

**Мобильная связь 5G/6G.** Продолжается трансформация отрасли сотовой связи на фоне внедрения 5G. Ожидаются новые развертывания на развивающихся рынках и расширение охвата в развитых странах. Начинает набирать обороты технология 5G Advanced, или 5.5G: это промежуточный этап между стандартами 5G и 6G. Внедрение 5G Advanced поможет повысить пропускную способность каналов связи, сократить время задержки, увеличить надежность и эффективность работы IoT. Другим направлением является развитие 5G

RedCap, или Reduced Capability. Эта версия 5G снижает требования к устройствам, одновременно предлагая расширенные возможности по сравнению с 4G, включая повышенную скорость передачи данных и уменьшенные задержки. Сети RedCap предоставляют базовые функции подключения, адаптированные для менее мощного и требовательного IoT-оборудования. Используя 5G RedCap, предприятия смогут эффективнее управлять техникой благодаря упрощению сетевой инфраструктуры, использовать расширенные возможности видеомониторинга, получать информацию с сенсоров и интегрировать персональные устройства в автоматизированную систему управления предприятием. С появлением 6G человечество делает следующий шаг в эволюции сетей мобильной связи. 6G – это стандарт мобильной связи шестого поколения, который находится в стадии завершения разработки (рис. 2). Ожидается, что сети 6G смогут передавать данные в сотни раз быстрее, чем 5G, с потенциальной скоростью до одного терабита в секунду.



Рис. 1. Рейтинг наиболее популярных инновационных технологий в телекоммуникации

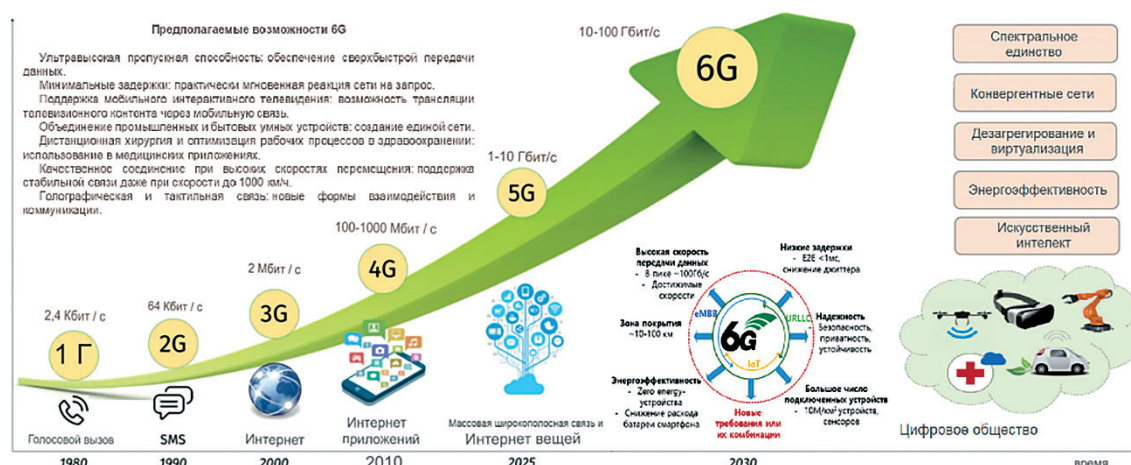


Рис. 2. Развитие сетей мобильной связи

Одним из ключевых отличий будет использование терагерцевого диапазона, что позволит значительно расширить зоны покрытия, включая возможность связи под водой, на больших высотах и даже в космосе.

Если посмотреть на всю картину и области применения, то системы связи 6G должны поддерживать переход различных сфер индустрии на цифровой формат. Как результат, спектр требований от компаний и их количественные значения существенно возрастут (рис. 3).

Для передачи данных стоит ожидать требования на пиковые значения скоростей до нескольких Гб/с. Поддержка зоны покрытия в несколько сот километров для спутниковой связи. Существенно возрастет энергоэффективность при применении мобильных средств (смартфонов, планшетов).

Термин **Облачные вычисления** (Cloud Computing) стал использоваться на рынке ИТ с 2008 года. Идеология заключается в переносе организации вычислений, обработки



Рис. 3. Ключевые особенности 6G



Рис. 4. Облачные и периферийные вычисления

и хранения данных с персональных компьютеров в Интернет.

Потребители облачных вычислений могут значительно уменьшить расходы на инфраструктуру информационных технологий (в краткосрочном и среднесрочном планах) и гибко реагировать на изменения вычислительных потребностей, используя свойства эластичных вычислений (англ. elastic computing) облачных услуг (рис. 4).

К настоящему времени можно выделить несколько основных технологий (моделей) этого направления:

- инфраструктура как услуга (Infrastructure as a Service, IaaS);
- платформа как услуга (Platform as a Service, PaaS);
- данные как услуга (Data as a Service, DaaS);
- программное обеспечение как услуга (Software as a Service, SaaS);
- рабочее место как услуга (Workplace as a Service, WaaS);
- все как услуга (All as a Service, AaaS).

Помимо различных способов предоставления сервисов различают несколько вариантов развертывания облачных систем: публичное, частное и гибридное облака (Public Cloud/Private Cloud/Hybrid Cloud).

Основными характеристиками облачных вычислений являются:

**Масштабируемость**, как способность информационных систем выдерживать растущие нагрузки и обрабатывать большие объемы данных. Масштабируемое приложение позволяет выдерживать большую нагрузку за счет

увеличения количества одновременно запущенных экземпляров. Как правило, для одновременного запуска множества экземпляров используется типовое оборудование.

**Эластичность** позволяет быстро нарастить мощность инфраструктуры, она связана с масштабируемостью приложений, так как решает задачу моментального изменения количества вычислительных ресурсов, выделяемых для работы информационной системы.

**Мультиотенантность** – это один из способов снижения расходов за счёт максимального использования общих ресурсов для обслуживания различных групп пользователей, разных организаций, разных категорий потребителей и т.п.

**Самообслуживание**. Быстрый вывод нового продукта или услуги в современных условиях сопровождается развертыванием или модификацией информационных систем. Самообслуживание позволяет потребителям запросить и получить требуемые ресурсы за считанные минуты.

Концепция **Интернет вещей** (англ. *internet of things*, IoT) представляет собой систему удаленного взаимодействия физических объектов между собой и/или с внешней средой, которая реализуется при помощи специализированного оборудования, программного обеспечения. Происходит такой обмен данными в режиме реального времени и без непосредственного участия человека [1].

Архитектура Интернет вещей представляет собой сложную экосистему, от маленького датчика до корпоративного облака, где данные



собираются, обрабатываются и превращаются в реальные действия.

Структура Интернета вещей описывается тремя уровнями:

Уровень восприятия (Perception Layer). Физические устройства, которые собирают данные (видео, звук, температуру, влажность и т.п.) из окружающей среды с помощью датчиков и обрабатывают их с помощью контроллеров. В некоторых случаях возможна мгновенная реакция на поступающую информацию: включение/выключение освещения, поворот камеры, перемещение, воспроизведение аудио и т.п.

Уровень сети (Network Layer). Собранная информация передается системам обработки данных с помощью технологий проводной и беспроводной связи: Ethernet, Wi-Fi, 5G, NB-IoT, ZigBee, LoRaWAN, Bluetooth и т.п.

Уровень приложений (Application Layer). Переданная информация обрабатывается прикладными инструментами – приложениями на удаленных серверах. Для этих целей обычно используют инфраструктуру облачных провайдеров.

Базовыми технологическими элементами Интернет вещей являются:

1. Устройства. К ним относятся самые разные «вещи» – от маленьких микрофонов до крупных машин. Вещи отличаются формами, они различны и по технологической сложности. Все зависит от задачи, которую они выполняют в рамках IoT. Почти любой

объект можно сделать подобным функциональным устройством, если добавить ряд нужных для этого элементов.

2. Программное обеспечение (ПО) является агрегаторным элементом «оживляющим» устройства и среду. Благодаря ему устройства называются умными. ПО собирает сведения, связывается с облаком, интегрирует устройства и анализирует данные в реальном времени. Также оно обеспечивает взаимодействие с системой IoT. ПО работает через специальные протоколы, которые задействованы в средах IoT.
3. Обеспечения подключения умных устройств и обеспечения взаимодействия между ними осуществляется по средствам различных коммуникаций. Выбор подходящих коммуникаций – один из важных моментов при создании каждой системы. От коммуникаций зависят способы отправки и получения сведений из облака, способы связи с другими устройствами.
4. Платформа – это место, которое собирает и обрабатывает сведения, а после в удобной форме передает их. В качестве платформы можно выбрать облако или локальный сервер. Это зависит от требований проекта и иных факторов: архитектуры, набора технологий, инструментов, которые выполняют определенные функции и взаимодействуют с другими компонентами.
5. Безопасность. Обеспечение защиты информации циркулирующей в системе Интернет



Рис. 5. Области применения интернет вещей



вещей и контроль за вводом ложной обеспечивается программными средствами устройств, платформ и средствами коммуникаций. Учитывая масштаб и сложность интернета вещей, устройства интернета вещей, как правило, подвержены кибератакам и утечкам данных. Производители серьезно относятся к этой проблеме и работают над обеспечением безопасности пользователей.

IoT находит практическое применение не только в создании умного дома, но и в торговле, здравоохранении, энергетике, организации работы транспортных магистралей, в промышленном производстве (IIoT – Industrial Internet of Things), в логистике (рис. 5). Своевременная информация о состоянии какой-либо системы помогает повысить её эффективность и безопасность.

Интернет вещей охватывает основные отрасли глобальной инфраструктуры:

- Жилищная сфера (умным домом). Поддержка комфортных условий внутри жилых помещений с помощью оборудования для анализа и изменения состояния внутренней среды.
- Промышленность. Обслуживание производственной среды и оптимизация процессов создания конечного продукта.
- Энергетика. Распределение энергии, учет ресурсов и контроль состояния электросетевой инфраструктуры.

- Сельское хозяйство. Оптимизация ресурсов для повышения урожайности и качества сельскохозяйственных изделий.
- Логистика. Обеспечение прозрачности цепочек поставок, контроль условий перевозок, а также отслеживание транспорта и грузов в режиме реального времени.
- Здравоохранение. Непрерывный мониторинг и дистанционная диагностика пациентов для улучшения качества лечения и ухода.

Баланс положительных и отрицательных сторон – не исключительное свойство Интернета вещей. Это касается любой технологии, отрасли или продукта. С одной стороны, IoT-решения открывают широкие возможности для автоматизации процессов и оптимизации ресурсов. С другой стороны, они требуют учета рисков в области безопасности, конфиденциальности и стандартизации.

Тем не менее, при грамотном проектировании и продуманной архитектуре IoT-системы могут существенно повлиять на развитие элементов систем военной связи.

**Спутниковая связь** – один из видов космической радиосвязи, основанный на использовании в качестве ретрансляторов искусственных спутников Земли, как правило специализированных спутников связи [2, 3]. Спутниковая связь осуществляется между земными станциями, которые могут быть как стационарными, так и подвижными.



Рис. 6. Перспективная тенденция по созданию низкоорбитальных систем связи со смартфонами D2D

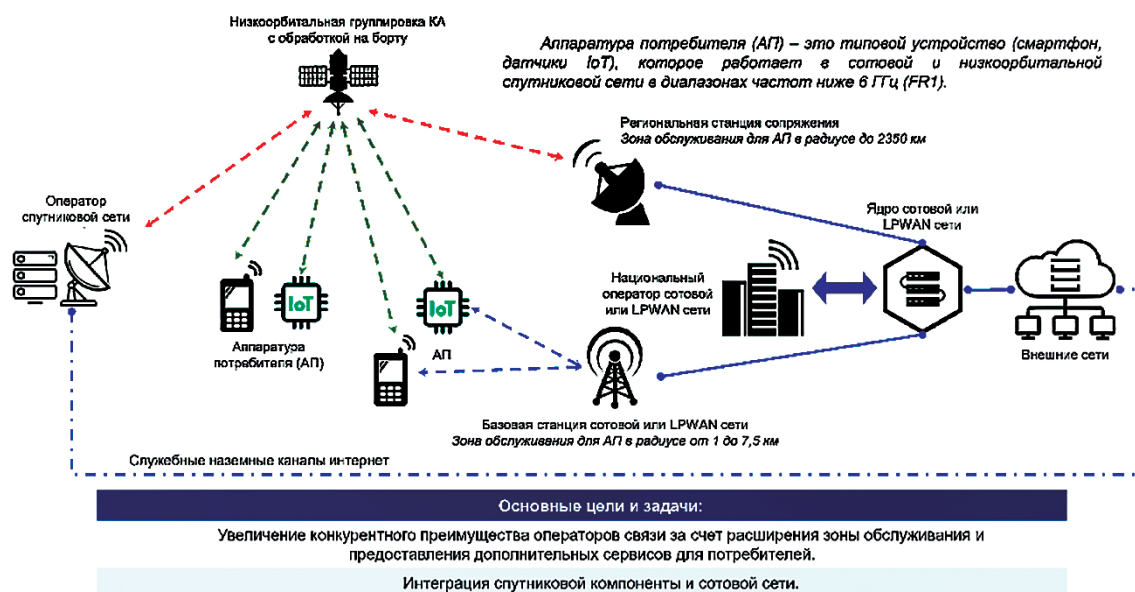


Рис. 7. Архитектура бесшовной низкоорбитальной сети D2D

В настоящее время в связи со стремительным развитием сети спутниковой связи на низкой околоземной орбите (LEO) Starlink (США), которая по сути осуществила революцию по организации спутниковой связи и обеспечению высокоскоростной связи пользователей в любой точки мира, технологически ведущие страны мира стали уделять особое внимание развитию данных систем, в том числе и в России (см. рис. 6).

Группировки LEO могут разворачиваться для предоставления широкополосного доступа в интернет или развития IoT-систем. Кроме того, спутники LEO могут обеспечивать транзитные каналы для услуг сотовой связи с применением технологии Direct-to-Device (D2D) «сети с прямым подключением устройств» (рис. 7). Следует отметить, что в понятие D2D входят системы, предусматривающие прямую связь спутника как со смартфоном (например, AST Mobile, Lynk Global, SpaceX) в сотовых сетях, так и с устройствами IoT (Lacuna, «Марафон IoT» и др.) для работы в сетях LPWAN.

Причем в смартфоне обеспечена возможность работы в сети на основе технологии Интернета вещей NB-IoT.

Основными перспективными технологиями спутникового IoT можно считать LoRa/LoRaWAN и NB-IoT.

Анализ аналитических материалов [4,5]. показывает, что низкоорбитальные системы D2D, в том числе с целевой функцией IoT, – это новый тренд в спутниковой связи. Их реализация создаст новый сегмент спутниковой связи

за счет организации бесшовных глобальных сетей.

Следует особо отметить, что системы D2D – это не системы спутникового широкополосного доступа. Скорости каналов «вниз» при работе со смартфоном не превышают десятка мегабит в секунду, а «вверх» в разы меньше. В ряде случаев, например для сервисов IoT, эквивалентные скорости каналов требуются не более десятков кбит/с. Однако в спутниковых системах IoT достигается новое качество, недоступное для наземных сетей, – предоставление различных сервисов, требующих приближения передачи информации к реальному времени.

**Квантовые технологии** определяют развитие отрасли науки, связанной с реализацией принципиально новых методов инфотелекоммуникации и вычислений (квантовые вычисления, квантовые устройства, квантовые коммуникации) (рис. 8).

Представление квантовой сети заключается в улучшении имеющихся телекоммуникационных технологий за счёт квантовых коммуникаций между любыми двумя точками. Для достижения этой цели создается сетевой стек с учётом принципиально новых свойств квантовой запутанности.

Квантовые сети – это распределенные системы квантовых устройств, использующие фундаментальные явления квантовой механики, такие как суперпозиция, запутанности и квантовые измерения, для достижения возможностей, выходящих за рамки классических

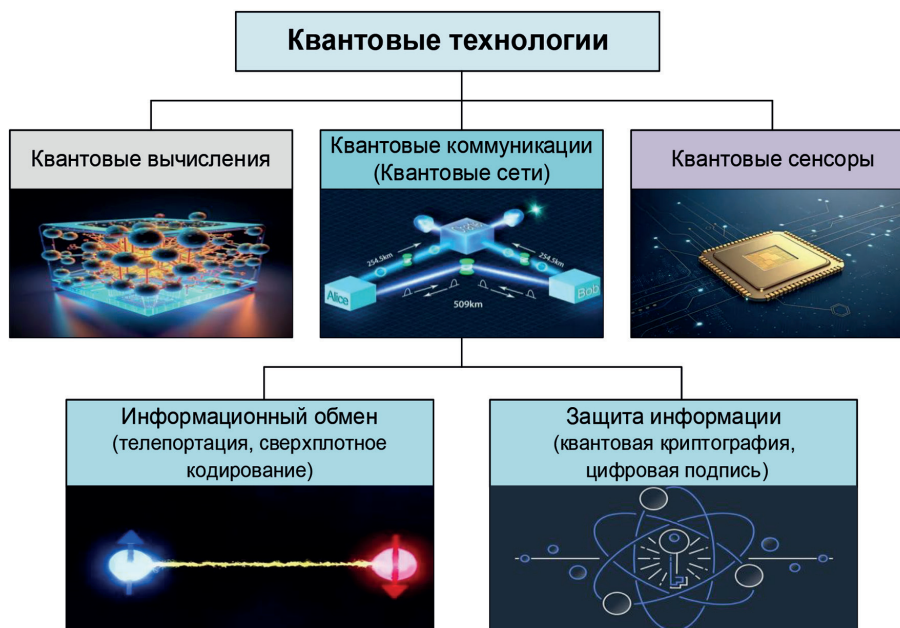


Рис. 8. Квантовые технологии

(не квантовых) сетей. В зависимости от стадии развития квантовой сети такие устройства могут варьироваться от простых фотонных устройств, способных одновременно подготавливать и измерять единственный квантовый бит (кубит – qubit), до крупномасштабных квантовых компьютеров [6]. Квантовые сети предназначены не для замены классических сетей, а скорее для формирования гибридных сетей, поддерживающих новые возможности, которые без этого не реализовать. Наиболее известное применение квантовой связи – квантовое распространение ключей (QKD, Quantum Key Distribution), может создавать и распространять пару симметричных ключей шифрования так, что безопасность всего процесса опирается на законы физики. Небольшие сети с QKD уже развёрнуты на небольшие (около 100 км).

Парадигма квантовых сетей предлагает ещё ряд приложений в дополнение к квантовой криптографии, таких как распределённые квантовые вычисления, защищённые квантовые вычисления в облаке, измерительные сети с квантовым улучшением высокоточные телескопы с длинной базой. Эти приложения гораздо требовательней, чем QKD, и сети, способные их поддерживать, пока находятся в зачаточном состоянии. Лишь недавно была реализована полностью квантовая сеть с множеством узлов, способная передавать, принимать и обрабатывать распределённую квантовую информацию [7].

Квантовые технологии, основанные на ее необычных свойствах, в ближайшем будущем повлияют на основы и дальнейшее развитие систем связи, а сама теория квантовой информации кардинально изменит современные взгляды научного сообщества на основу системы информационной безопасности, что является весьма важным для военных сетей и системы связи ВС РФ. Очевидно, что практическая реализация квантовой системы связи ВС РФ представляет собой сложную научно-технологическую проблему, для решения которой потребуются проведение продолжительных междисциплинарных исследований.

#### Новые поколения беспроводной связи Wi-Fi 7/Wi-Fi 8.

2025-й год является годом глобального внедрения Wi-Fi 7 (стандарта IEEE 802.11be). Разработчики обещают увеличение максимальной скорости передачи данных до 46 Гбит/с, это в 13 раз выше скорости у Wi-Fi 5 и почти в пять раз – у Wi-Fi 6. Wi-Fi 7 часто отводят роль катализатора цифровой трансформации, фундаментально меняющего то, как люди и бизнес взаимодействуют в беспроводном пространстве, см. рис. 9, а также<sup>4</sup>.

Основными особенностями Wi-Fi 7 являются:

Одновременная работа в нескольких диапазонах на основе применения технологии Multi-Link Operation (MLO). Устройства

<sup>4</sup> Информационный портал о Wi-Fi: [Электронный ресурс]. URL: <http://wificonnect.ru> (дата обращения: 04.01.2026)

Wi-Fi 7/8 удваивает доступную полосу пропускания по сравнению с Wi-Fi 6, предлагая три сверхшироких канала с частотой 320 МГц в выделенном диапазоне 2,4; 5; 6 ГГц.

Количество доступных каналов на полосу пропускания	40МГц	80МГц	160МГц	320МГц	max скорость	Спектр	
Wi-Fi 8 (bn)	42	24	12	6	100Гб/с	6ГГц 5ГГц 2.4ГГц	
Wi-Fi 7 (be)	36	17	8	3	40Гб/с		
Wi-Fi 6 (11ax)	11	3	1		9.6Гб/с		
Wi-Fi 5 (11ac)					6Гб/с		
Wi-Fi 4 (11n)	7				600Мб/с		

#### Высокое канальное уплотнение

В сочетании с новой пропускной способностью канала 320 МГц 4К QAM обеспечивает пользователям скорость в 2.4 раза большую, чем в Wi-Fi 6

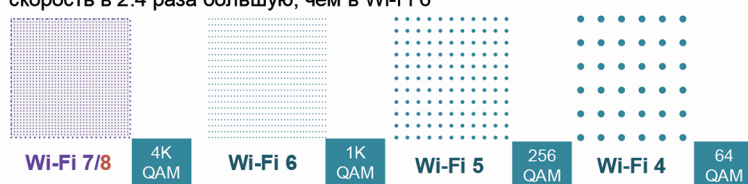


Рис. 9. Сравнительные характеристики Wi-Fi

на предыдущих стандартах могли переключаться между диапазонами (например, между 2,4, 5 и 6 ГГц), но работали только в одном из них. Wi-Fi 7 позволяет использовать сразу три диапазона одновременно. Это делает соединение стабильнее и быстрее – особенно в условиях, когда один из каналов перегружен. Технология позволяет системе динамически выбирать оптимальный путь для каждого пакета данных, учитывая текущую загруженность каналов, качество сигнала и приоритет трафика.

**Новая ширина канала.** Wi-Fi 7 поддерживает ширину канала до 320 МГц в диапазоне 6 ГГц – в два раза шире, чем у Wi-Fi 6. Через такой канал может проходить больше данных за единицу времени, как следствие, возрастает производительность.

**Плотная упаковка данных.** Wi-Fi 7 использует более эффективную модуляцию сигнала – 4096-QAM. Каждый пакет передаёт больше информации – 12 бит вместо 10, как это реализовано в Wi-Fi 6. Это увеличивает скорость передачи, особенно на коротких расстояниях, где сигнал стабилен. Но чем более зашумлён эфир, тем менее эффективно работает технология.

**Эффективное использование спектра.** В Wi-Fi 6 был реализован механизм OFDMA –

он делит канал на множество подканалов (Resource Units– RU), чтобы обслуживать сразу несколько клиентов. Но в случае помех эффективность падала – приходилось использовать менее загруженные, но меньшие по объёму подканалы. Wi-Fi 7 решает эту проблему с помощью технологии Multi Resource Units (MRU). Она позволяет комбинировать сразу несколько отдельных подканалов. Это увеличивает гибкость в распределении ресурсов и позволяет поддерживать высокую скорость даже в условиях загруженного эфира.

Поддержка MU-MIMO 16×16. Wi-Fi 7 расширяет возможности технологии MU-MIMO в сравнении с Wi-Fi 6, который предлагает MU-MIMO 8×8. Технология позволяет более эффективно использовать доступную пропускную способность, распределяя её между множеством клиентов без существенной деградации производительности для каждого отдельного устройства.

**Поддержка большего количества устройств.** Wi-Fi 7 оптимизирован для работы в условиях высокой плотности устройств. Он позволяет подключать и обслуживать гораздо больше устройств одновременно без потери производительности. Это особенно актуально для умных домов и городов, где количество IoT-устройств постоянно растёт.



**Wi-Fi 8** (IEEE 802.11bn Ultra High Reliability), чей релиз состоялся 2025 года, обещает революционизировать мир беспроводных технологий, предлагая беспрецедентную теоретическую максимальную скорость в 100 Гбит/с.

Ключевой аспект нового стандарта Wi-Fi 8 не пиковая пропускная способность, а эффективная пропускная способность, а также повышение стабильности работы, сокращение задержек и обеспечение более плавной работы в среде с большим количеством подключённых устройств.

Направление развития Wi-Fi 8 определяют две основные тенденции.

Во-первых, это растущая экосистема персональных устройств, таких как очки дополненной реальности и медицинские мониторы нового поколения, которым требуется бесперебойное соединение с другими устройствами поблизости с минимальной задержкой.

Во-вторых, растёт популярность систем на базе искусственного интеллекта, которые зависят от быстрого и надёжного доступа к периферийным или облачным вычислительным ресурсам.

В совокупности эти тенденции выводят локальные сети, в том числе Wi-Fi-роутер или даже мобильный 5G-роутер, на территорию, для которой они изначально не предназначались. Wi-Fi 8 позиционируется как базовый уровень подключения, который будет лежать в основе этих всё более динамичных систем, чувствительных к задержкам.

В отличие от обычного удлинителя Wi-Fi, который просто расширяет зону покрытия сигнала, новый стандарт переосмысливает принципы совместной работы точек доступа, роуминга устройств и сохранения качества сигнала на границах зон покрытия.

В Wi-Fi 8 осуществляется усовершенствование технологии MU-MIMO и OFDMA, для эффективности сетей в густонаселённых районах, что может стать ключевым фактором в развитии инфраструктуры будущего, способной поддерживать растущие потребности в высокоскоростной и надёжной беспроводной связи.

Ещё дальше в будущее заглядывает разрабатываемый стандарт IEEE 802.11bf или Wi-Fi Sensing. Его особенность — использование не только связи, но и локации, обнаружение объектов и людей при помощи измерения характеристик Wi-Fi сигналов.

Потенциальные применения Wi-Fi Sensing:

- автоматическое управление освещением, климатом, мультимедиа в зависимости от присутствия и перемещения людей в помещениях;
- охранные системы, обнаруживающие проникновение в здание;
- отслеживание жизненных показателей, дыхания, пульса с целью медицинской диагностики;
- помощь людям с ограниченными возможностями в ориентировании и управлении устройствами без контактных датчиков;
- аналитика поведения покупателей в магазинах, посетителей в музеях, пассажиров в аэропортах.

Wi-Fi Sensing предлагает широкий спектр возможностей для зондирования с использованием Wi-Fi, охватывая частотные диапазоны от 1 ГГц до 7,125 ГГц для основных сервисных интерфейсов, а также частоты выше 45 ГГц для специализированных применений.

Особенно примечательна технология на частоте 60 ГГц, которая обещает обеспечить высокоточное отслеживание и разрешение, открывая новые горизонты для таких приложений, как распознавание жестов в играх и усовершенствованный удаленный мониторинг состояния здоровья, что демонстрирует потенциал стандарта для революционных изменений в различных сферах применения Wi-Fi.

Стандарт IEEE 802.11bf планируется утвердить в 2025 году. А первые устройства и приложения, использующие Wi-Fi Sensing, могут появиться к 2030 году.

Wi-Fi остается одной из самых динамично развивающихся и востребованных ИТ-технологий, следовательно она должна на постоянной основе рассматриваться на применимость в сетях военной связи.

### Сети с искусственным интеллектом

Современная телекоммуникационная отрасль переживает масштабную цифровую трансформацию в связи с ростом количества устройств, подключенных к сети, с учетом активного развития интернета вещей (IoT) и стремительного увеличения объема передаваемых данных, требуют новых подходов к управлению сетевой инфраструктурой. Решение данных задач может эффективно осуществляться с использованием искусственного интеллекта, при этом предлагается

использовать четыре основных технологии (рис. 10):

- 1. Машинное обучение (ML, Machine Learning) [8].
- 2. Глубокое обучение (DL, Deep Learning) [9].
- 3. Обработка естественного языка (NLP, Natural Language Processing) [10].
- 4. AIOps (Artificial Intelligence for IT Operations).

Несмотря на схожесть решаемых задач, данные технологии имеют различия, которые могут дополнять, так и выполнять задачи обо-собленно друг от друга. Отличия технологий заключаются в:

- Извлечении признаков. В машинном обучении это требует ручного вмешательства, в то время как глубокое обучение способно

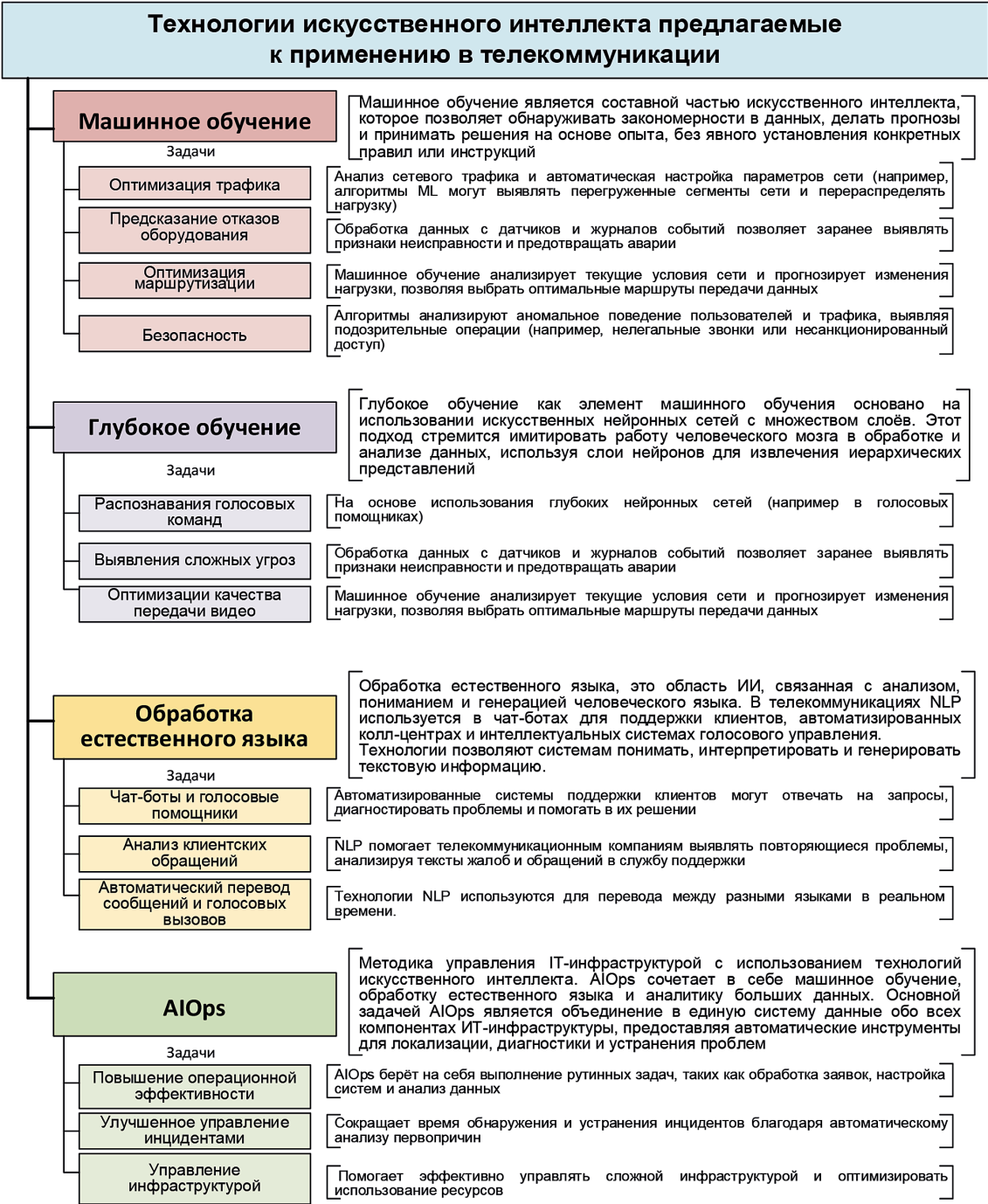


Рис. 10. Технологии искусственного интеллекта, предлагаемые к применению в телекоммуникации

автоматически извлекать признаки на разных уровнях абстракции, что позволяет моделям обучаться более сложным представлениям.

- **Объёме данных.** Машинное обучение может быть эффективным с небольшими объёмами данных, в то время как глубокое обучение чаще требует больших объёмов данных для эффективного обучения из-за большого числа параметров.
- **Вычислительных ресурсах.** Машинное обучение может быть реализовано на менее мощных вычислительных структурах, в то время как глубокое обучение обычно требует мощных вычислительных ресурсов, таких как графические процессоры (Graphics Processing Unit – GPU) или тензорные процессоры (Tensor Processing Unit – TPU).

Следовательно, ML позволяет системам обучаться на данных и делать прогнозы без явного программирования. Машинное обучение использует алгоритмы для поиска закономерностей в данных. В телекоммуникациях ML в основном применяется для предсказания нагрузки на сеть, выявления аномалий и автоматизации управления трафиком. Глубокое обучение, в свою очередь, является более сложным видом машинного обучения, основанный на многослойных нейронных сетях. Оно особенно полезно для работы с большими объёмами данных и сложными зависимостями. В телекоммуникациях DL применяется для предсказания отказов оборудования, распознавания голоса в интеллектуальных ассистентах и анализа сетевого трафика. NLP отвечает за работу с текстом и голосом

AIOps сочетает ML, DL и анализ больших данных для мониторинга, предсказания сбоев, обнаружения аномалий и управления инцидентами в телекоммуникационных сетях. Оно помогает операторам быстрее реагировать на проблемы, минимизируя время простоя и повышая стабильность сети.

Таким образом, ML и DL – это методы обучения ИИ, NLP отвечает за работу с текстом и голосом, а AIOps объединяет ИИ-алгоритмы для автоматизации управления ИТ-инфраструктурой.

Положительные аспекты применения искусственного интеллекта:

- повышение эффективности обработки данных за счет автоматизации рутинных операций;

- существенное снижение затрат на обслуживание сетевой инфраструктуры;
- повышение устойчивости сетей за счет раннего выявления неполадок;
- адаптивность и масштабируемость сетей в условиях роста нагрузки;
- снижение времени реакции на инциденты.
- отрицательные стороны применения:
  - высокая стоимость разработки и внедрения ИИ-решений;
  - зависимость от качества обучающих данных и возможность ошибок модели;
  - потеря прозрачности в принятии решений (проблема «чёрного ящика»);
  - угрозы безопасности и возможные уязвимости ИИ-систем.

ИИ уже сегодня играет ключевую роль в повышении эффективности телекоммуникационных сетей. Отечественные и зарубежные примеры демонстрируют широкий потенциал технологий ИИ в обеспечении устойчивости, предсказуемости и масштабируемости сетевой инфраструктуры.

Несмотря на успешное применение искусственного интеллекта отдельными «гражданскими» компаниями, внедрение ИИ в систему военной связи, потребует изменение нормативно-правовой базы, оснащение мощными вычислительными ресурсами и развитие профессиональных компетенции у специалистов.

### Технологии скоростного доступа FTTx

Название технологии произошло от англ. *fiber to the x* – оптическое волокно до точки X. Это общий термин для любой широкополосной телекоммуникационной сети передачи данных, использующей в своей архитектуре волоконно-оптический кабель в качестве последней мили для обеспечения всей или части абонентской линии [11]. Термин является собирательным для нескольких конфигураций развёртывания оптоволокна – начиная от FTTN (до узла) и заканчивая FTTD (до рабочего стола). Технология FTTx разработана для передачи данных через оптические кабели (рис. 11). При этом, FTTx означает использование оптического волокна для передачи данных к конечной точке в процессе предоставления услуг. Кроме этого, возможен вариант, при котором оптика прокладывается непосредственно до абонентского устройства.

В технологию семейства FTTx включены различные виды архитектур:

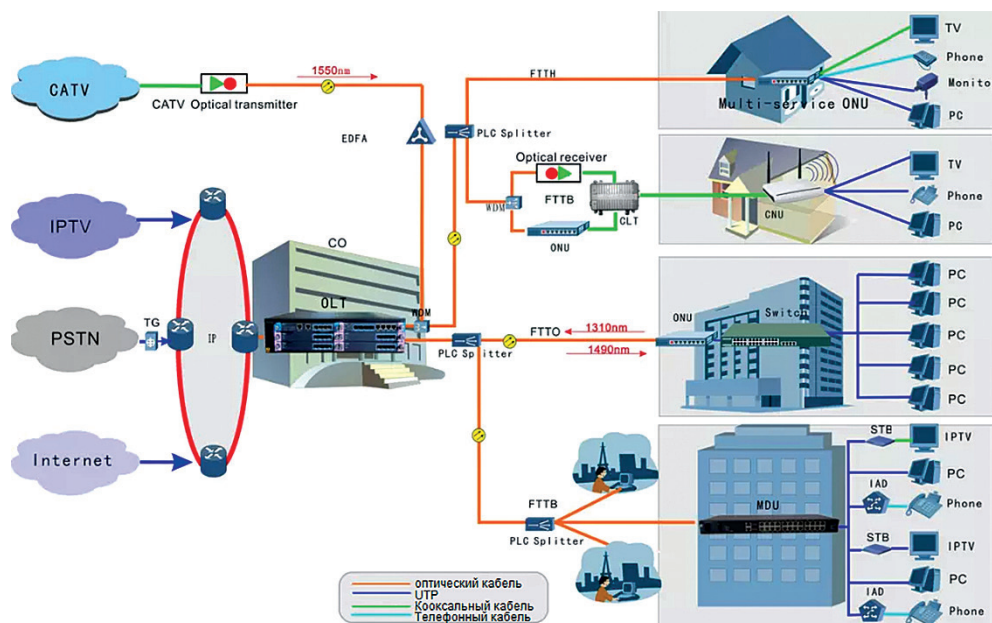


Рис. 11. Технологии скоростного доступа FTTx

- FTTN (*Fiber to the Node*) – волокно до сетевого узла;
- FTTC (*Fiber to the Curb*) – волокно до микрорайона, квартала или группы домов;
- FTTB (*Fiber to the Building*) – волокно до здания;
- FTTH (*Fiber to the Home*) – волокно до жилища.

Основная задача данной технологии – доставлять пакеты разнообразных услуг и сервисов. В качестве примера можно назвать популярный набор, получивший название тройной услуги (Triple Play) – доступ к сети Интернет, телефония, телевизионное вещание и доставка видео. Стремительно растущая потребность во всех трех видах услуг позволяет уже сейчас говорить о неизменности тенденции, в соответствии с которой объемы строительства FTTx будут расти на протяжении многих лет.

## Программно-определяемая сеть SDN

Программно-определяемые сети (SDN, от англ. *Software-Defined Networking*) — инновационный подход к построению и управлению сетевой инфраструктурой. SDN радикально меняет традиционный подход к управлению сетями, делая их более гибкими, управляемыми и адаптируемыми к требованиям потребителей услуг связи.

Программно-определяемая сеть обеспечивает управление сетевой инфраструктурой

с помощью программных решений, отделённых от физического уровня. В традиционных сетях управление и передача данных связаны в единый процесс, что усложняет настройку и масштабирование сети. SDN меняет эту парадигму, позволяя централизованно управлять сетью с помощью программного контроллера, который отделён от непосредственно передающего оборудования.

SDN разделяет управление и передачу данных, делая архитектуру сети более гибкой и управляемой. Основные компоненты SDN:

Контроллер SDN, который отвечает за управление всей сетью. Контроллер обрабатывает запросы приложений и управляет сетевой инфраструктурой в реальном времени.

Инфраструктурный уровень. Состоит из физических или виртуальных коммутаторов и маршрутизаторов, которые непосредственно выполняют передачу данных.

Уровень приложений. Здесь находятся приложения и сервисы, которые обращаются к контроллеру для выполнения сетевых операций, таких как управление пропускной способностью или распределение нагрузки.

SDN используется в различных отраслях и сценариях, где необходимы гибкость, масштабируемость и управление сетевой нагрузкой:

Центры обработки данных, где помогает управлять сетью и трафиком, снижая затраты на оборудование и эксплуатацию. SDN активно используется для управления



распределёнными ресурсами, увеличения пропускной способности и контроля нагрузки.

Корпоративные сети. Компании, которым требуется безопасный и масштабируемый доступ, используют SDN для гибкого управления сетью. SDN позволяет централизованно управлять сетью и контролировать доступ к критически важным данным.

Поставщики облачных услуг. SDN позволяет облачным провайдерам, гибко управлять ресурсами для обеспечения бесперебойного доступа к данным.

Телекоммуникационные сети и 5G. Для обеспечения высокой пропускной способности и низкой задержки SDN помогает управлять телекоммуникационными сетями, обеспечивая надёжное и безопасное соединение в сетях 5G.

Применение SDN также способствует усилению безопасности, так как контроллер может динамически применять политики безопасности.

Развитие SDN связано с рядом современных технологий, таких как IoT, 5G, и искусственный интеллект. С ростом интернет-вещей и развитием 5G возникает необходимость в гибких и масштабируемых сетях, способных выдерживать растущий объем данных.

SDN играет важную роль в построении «умных сетей» (smart networks), где искусственный интеллект используется для анализа данных о трафике и принятия решений. Применение машинного обучения позволяет прогнозировать нагрузку и автоматизировать настройку сети.

Программно-определяемые сети (SDN) представляют собой революционное решение для управления современными сетями. Благодаря SDN обеспечивается гибкость, снижают затраты и повышают уровень безопасности. В будущем SDN будет играть важную роль в таких областях, как 5G и IoT, способствуя внедрению инноваций и улучшению производительности.

### Системы когнитивного радио

Системы когнитивного радио (СКР) [12] в настоящее время активно развиваются и востребованы мировыми производителями систем связи и телекоммуникаций. Согласно рекомендациям МСЭ-Р М.2330-0 «Когнитивные системы радиосвязи в наземной подвижной службе» радиоустройства с программно-определяемыми свойствами

и характеристиками (SDR, Software Defined Radio) признаны передовой технологией для реализации СКР<sup>5</sup>. SDR способны осуществлять радиомониторинг спектра, автономно и динамически изменять собственные параметры работы и могут адаптироваться к новым технологиям, тем самым реализовывая необходимые для разработки СКР функции: мониторинг, адаптация, реконфигурация.

Международный союз электросвязи использует следующее определение термина СКР: «Система когнитивного радио – радиосистема, использующая технологию, позволяющую этой системе получать знания о своей среде эксплуатации и географической среде, об установившихся правилах и о своем внутреннем состоянии; динамически и автономно корректировать свои эксплуатационные параметры и протоколы, согласно полученным знаниям, для достижения заранее поставленных целей; и учиться на основе полученных результатов». Следовательно, СКР обладает двумя отличительными возможностями: реконфигурирование или самоконфигурирование и интеллектуальная адаптация. Реконфигурация СКР это процесс, при котором радиоустройство программным образом изменяет свои эксплуатационные параметры и протоколы для наиболее эффективной и надежной передачи и приема информации, даже при отсутствии запроса от пользователя устройства. Под интеллектуальной адаптацией подразумевается способность устройства адаптироваться через какую-либо форму обучения, не являясь заранее запрограммированным для этого. Из этого следует, что для работы СКР необходимы как минимум следующие возможности:

- Реконфигурируемость. Способность устройства быстро изменять форму сигнала и другие рабочие параметры, например стандарт связи, для взаимодействия с другими системами или улучшения качества связи.
- Мониторинг. Способность постоянного наблюдения и измерения явлений и процессов, происходящих в окружающей среде. Мониторинг необходим радиоустройству для изменения собственных параметров работы на основании статистики занятости спектра.
- Адаптируемость и обучаемость. Способность анализировать влияние явлений

5 Рекомендация МСЭ-Р М.2330-0 Когнитивные системы радиосвязи в наземной подвижной службе. 11/2014.

и процессов, распознавать закономерности и подстраивать параметры работы устройства для новых условий эксплуатации в результате машинного обучения.

Соответствующие возможности становятся доступными с помощью использования интерфейсов программных приложений управления в рамках концепции реконфигурируемых радиосистем. Под реконфигурируемой радиосистемой понимаются радиоустройства с программно-определяемыми свойствами и характеристиками (SDR). SDR – это радиопередатчик/радиоприемник или их совокупность, использующие программную технологию, позволяющую устанавливать или изменять рабочие радиочастотные параметры такие как диапазон частот, тип модуляции, кодирование с исправлением ошибок, сжатие или выходную мощность [13]. SDR позволяют предоставлять различные виды услуг для пользователей, так как способны изменять стандарты связи в любое время, поскольку последние реализуются на программном уровне.

В качестве основных характеристик SDR выделяют:

- программное управление одним или несколькими приемопередающими радио модулями;
- радиочастотные компоненты с большим динамическим диапазоном;
- высокоскоростной тракт аналогово-цифрового и цифро-аналогового преобразования с большим динамическим диапазоном;
- процессор управления, обладающий достаточной вычислительной мощностью;
- специализированный цифровой тракт для фильтрации сигналов.

На практике SDR представляет собой радиоустройство, в котором основные функции радиоустройства (аналогово-цифровое и цифро-аналоговое преобразование, фильтрация и т.д.) реализуются программными модулями

работающими на базе встроенных вычислительных устройств. С использованием SDR существует возможность выбирать различные системы связи для получения требуемой услуги, так как есть возможность работать с различными стандартами связи. Для предоставления пользователю требуемой услуги связи SDR в автоматическом или полуматематическом режиме выбирает требуемый частотный диапазон, стандарт радиосвязи, а также программное приложение. Основную концепцию реализации SDR можно применять как для построения абонентских устройств, так и базовых станций. SDR позволяет проводить радиомониторинг спектра, отслеживать и обрабатывать передачу информации на физическом и канальном уровнях нескольких систем радиосвязи одновременно, тем самым позволяя реализовать необходимые для СКР функции (мониторинг, адаптация, реконфигурация). Также SDR могут адаптироваться к новым технологиям, так как обладают гибкими программными настройками, что невозможно для существующих радиосистем из-за их аппаратной ограниченности. В качестве SDR может рассматриваться абонентский терминал с программным управлением на основе загружаемой операционной системы (смартфон) или аналогичное устройство.

В настоящее время SDR используются для реализации простых радиомоделей, в частности GSM, WiFi, WiMax. Со временем SDR станет основной частью системы когнитивного радио.

### Заключение

Применение перспективных технологий в интересах военной связи будет способствовать более продуктивному и безопасному информационному взаимодействию органов управления. Обеспечивая высокую управляемость войск органами управления независимо от территориального рассредоточения, выполняемых задач и оперативной обстановки.

### 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. Анпилогов В., Пехтерев С., Шишлов А. Анализ терминалов, планируемых для применения в системах Starlink и OneWeb // Технологии и средства связи. 2022. № S1. С. 30–36.
3. Урличич Ю. М. Анализ низкоорбитальных спутниковых систем широкополосного доступа на примере развития Starlink // Электросвязь. 2024. № 7. С. 14–19.

4. Анпилогов В. Р., Нгуен Д. А. Анализ совместимости спутниковых сетей IoT с устройствами SRD и LPWAN в диапазонах частот 868/915 МГц // Электросвязь. 2020. № 1. С. 37–43.
5. Анпилогов В. Р., Гриценко А.В. Спутниковый IoT – новые системы и новый рынок // CONNECT. № 5–6, 2023. С. 76–80.
6. Колесников П. О., Голубничий А. А. К вопросу о квантовых компьютерах их развитии и современном состоянии // Научно-образовательный журнал для студентов и преподавателей «StudNet» №1/2022. С 754–762.
7. Кузнецов В. М. Квантовая механика. – М.: БИНОМ. Лаборатория знаний, 2015. 291 с.
8. Принс С. Машинное обучение. От основ до продвинутых моделей / С. Принс; – БОМБОРА, 2025. – 610 с.
9. Гудфеллоу Я. Глубокое обучение / Я. Гудфеллоу, И. Бенджио, А. Курвилль; – ДМК Пресс, 2017. – 654 с.
10. Хобсон Л. Обработка естественного языка в действии / Л. Хобсон, Х. Ханнес, Х. Коул; – Питер, 2021. – 576 с.
11. Иванов В. Г. Теория и практика построения и обеспечения функционирования системы связи специального назначения с учётом технологического развития и опытов вооружённых конфликтов: Монография. – М.: Красная Звезда, 2025. – 303 с.
12. Волков, Л. Н. Системы цифровой радиосвязи: базовые методы и характеристики / Л. Н. Волков, М. С. Немировский, Ю. С. Шинаков. – Москва.: Эко-Трендз, 2005. – 392 с.
13. Проскуряков, В. Когнитивные радиосистемы в сетях тактического назначения / В. Проскуряков // Электронные компоненты. – 2014. – № 3. – С. 36–38.

## INNOVATIVE TECHNOLOGIES IN TELECOMMUNICATIONS AND THEIR IMPACT ON MILITARY COMMUNICATIONS

*Ivanov V. G.<sup>6</sup>, Lukyanchik V. N.<sup>7</sup>, Kuzin P. I.<sup>8</sup>*

**Keywords:** *information technology, 5G and 6G standards, cloud computing, Internet of Things (IoT), satellite communications, quantum technologies.*

### **Abstract**

**The purpose of the work:** *to analyze innovative technologies in telecommunications, to identify the most popular ones and to assess their impact on military communications.*

**Research method:** *the methodological basis of the research is the general theory of systems using the methods of system analysis and the sampling method based on the correspondence of parameters that satisfy military communication and military command and control systems.*

**Results of the study:** *ten information and telecommunication technologies are considered and selected, which, in the authors' opinion, will have a significant impact on the military communication system. These include: 5G/6G mobile communications, in which a significant transformation and transition to new formats are being carried out; cloud computing, which will ensure the development of not only military communications; Internet of Things technologies, which ensure the interaction of physical objects with each other and/or with the external environment, with the use of specialized equipment, software; satellite communications in low Earth orbit, providing broadband Internet access, the development of IoT systems and cellular communication services using Direct-to-Device (D2D) technology; quantum technologies that implement new methods of infotelecommunications and computing; Wi-Fi 7/Wi-Fi 8 wireless technologies, promising a maximum data transfer speed of 13 times faster for Wi-Fi 5 and almost five times faster for Wi-Fi 6. Wi-Fi 7; Networks with artificial intelligence; FTTx high-speed access technologies of a broadband telecommunications data transmission network, which uses fiber optic cable as the last mile in its architecture to provide all or part of the subscriber line; Software-defined networks are changing the traditional approach to network management, making them more flexible, manageable and adaptable to the requirements of communication consumers; cognitive radio systems.*

6 Vasily G. Ivanov, Dr.S. of Military Sciences, Associate Professor, Professor of the Department of Informatics and Computer Engineering, Faculty of Engineering, Academy of Civil Protection of the Ministry of the Russian Federation for Civil Defense, Emergencies and Elimination of Consequences of Natural Disasters named after Lieutenant General D. I. Mikhailik. Khimki, Moscow Region. Russia. E-mail: wasj2006@yandex.ru

7 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

8 Pavel I. Kuzin, Ph.D. of Technical Sciences, Associate Professor of the Department of Information Systems and Technologies, S.M. Kirov St. Petersburg State Forestry University, St. Petersburg, Russia. E-mail: kuzik78@mail.ru

***Practical usefulness** lies in the review and identification of innovative technologies in telecommunications that will have a significant impact on the development of military communications, the command-and-control system for troops and weapons in the future until 2040.*

### References

1. 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. – SPb.: POLITEH, 2023. – 298 s.
2. Anpilogov V., Pehterev S., Shishlov A. Analiz terminalov, planiruemyh dlja primenenija v sistemah Starlink i OneWeb // Tehnologii i sredstva svjazi. 2022. № S1. S. 30–36.
3. Urlichich Ju. M. Analiz nizkoorbital'nyh sputnikovyh sistem shirokopolosnogo dostupa na primere razvitija Starlink // Jelektrosvjaz'. 2024. № 7. S. 14–19.
4. Anpilogov V. R., Nguen D. A. Analiz sovместимости sputnikovyh setej IoT s ustrojstvami SRD i LPWAN v diapazonah chastot 868/915 MGc // Jelektrosvjaz'. 2020. № 1. S. 37–43.
5. Anpilogov V. R., Gricenko A. V. Sputnikovyj IoT – novye sistemy i novyj rynek // CONNECT № 5–6, 2023. S. 76–80.
6. Kolesnikov P. O., Golubnichij A. A. K voprosu o kvantovyh komp'juterah ih razvitii i sovremennom sostojanii // Nauchno-obrazovatel'nyj zhurnal dlja studentov i prepodavatelej «StudNet» №1/2022. S. 754–762.
7. Kuznecov V. M. Kvantovaja mehanika. – M.: BINOM. Laboratorija znanij, 2015. 291 s.
8. Prins S. Mashinnoe obuchenie. Ot osnov do prodvinutyh modelej / S. Prins; – BOMBORA, 2025. – 610 s.
9. Gudfellou Ja. Glubokoe obuchenie / Ja. Gudfellou, I. Bendzhio, A. Kurvill'; – DMK Press, 2017. – 654 c.
10. Hobson L. Obrabotka estestvennogo jazyka v dejstvii / L. Hobson, H. Hannes, H. Koul: – Piter, 2021. – 576 s.
11. Ivanov V. G. Teorija i praktika postroenija i obespechenija funkcionirovanija sistemy svjazi special'nogo naznachenija s uchjotom tehnologicheskogo razvitija i opytov vooruzhennyh konfliktov: Monografija. – M.: Krasnaja Zvezda, 2025. – 303 s.
12. Volkov, L. N. Sistemy cifrovoj radiosvjazi: bazovye metody i harakteristiki / L. N. Volkov, M. S. Nemirovskij, Ju. S. Shinakov. – Moskva. Jeko-Trendz, 2005. – 392 s.
13. Proskurjakov, V. Kognitivnye radiosistemy v setjah takticheskogo naznachenija / V. Proskurjakov // Jelektronnye komponenty. – 2014. – № 3. – S. 36–38.





# МОДЕЛЬ ВЛИЯНИЯ МОНИТОРИНГА СЕТЕВОГО ТРАФИКА НА ЭФФЕКТИВНОСТЬ ФУНКЦИОНИРОВАНИЯ СЕТИ ПЕРЕДАЧИ ДАННЫХ

Симонова К. О.<sup>1</sup>

DOI:10.21681/3034-4050-2026-1-33-41

**Ключевые слова:** мультисервисные сети, качество обслуживания, системы массового обслуживания, самоподобный трафик, оптимизация.

## Аннотация

**Целью исследования** является разработка и анализ математической модели, описывающей влияние мониторинга параметров сетевого трафика и показателей качества обслуживания на эффективность функционирования мультисервисной сети передачи данных при использовании различных сетевых механизмов.

**Метод исследования:** в работе применяются аналитическое и имитационное моделирование процессов передачи данных в сетевых устройствах, статистический анализ параметров трафика, а также методы оптимизации распределения потоков и ресурсов с ограничениями на управляемые параметры. Для идентификации характеристик трафика использованы критерии согласия Пирсона и Колмогорова, а также параметр Херста как мера самоподобия.

**Результаты исследования:** разработана математическая модель функционирования сети передачи данных с учетом служебного трафика мониторинга, аппроксимированы зависимости средней задержки от нагрузки и параметра Херста, получены аналитические выражения, позволяющие оценивать эффективность функционирования сети при различных сетевых механизмах распределения потоков. Показано, что ошибки мониторинга в пределах диапазона параметра Херста  $H = 0,5 - 0,75$  незначительно влияют на оптимальное распределение потоков, но существенно изменяют абсолютные значения задержек, что важно при реализации механизмов предотвращения перегрузок.

**Научная новизна:** заключается в разработке комплексной модели, объединяющей процессы мониторинга, анализа трафика и оптимизации сетевых механизмов, а также в предложении новых аппроксимационных зависимостей, связывающих параметры самоподобного трафика с показателями качества обслуживания. Это позволяет аналитически оценивать влияние точности мониторинга на эффективность функционирования мультисервисной сети передачи данных.

## Введение

В современных условиях цифровизации всех сфер деятельности наблюдается стремительный рост объемов передаваемой информации и усложнение структуры сетей передачи данных. Современные телекоммуникационные системы объединяют разнородные сервисы – от голосовой и видеoinформации до потоков данных, критичных к задержкам, таких как управление беспилотными и роботизированными платформами. В результате сети передачи данных превращаются в мультисервисные системы (СПД), которым необходимо обеспечивать надежную и устойчивую работу при резком изменении характера и интенсивности трафика.

Одним из ключевых показателей эффективности функционирования сетей является качество обслуживания (Quality of Service, QoS), которое отражает совокупность характеристик, определяющих возможность предоставления пользователям требуемого уровня сервиса. Для поддержания заданного QoS в условиях динамично изменяющихся параметров сети используются различные сетевые механизмы – распределение потоков данных по маршрутам, балансировка нагрузки, управление очередями, приоритизация и механизмы предотвращения перегрузок. Эти механизмы функционируют в тесной связи с системой мониторинга, которая обеспечивает сбор, обработку и анализ информации о параметрах трафика и состоянии сети.

<sup>1</sup> Симонова Карина Олеговна, адъюнкт кафедры «Сети связи и системы коммутации» Военная академия связи им. С. М. Буденного, г. Санкт-Петербург, Россия. E-mail: desire\_8912@bk.ru

Мониторинг сетевого трафика в современных СПД выполняет не только функцию наблюдения, но и становится активным элементом контура управления. Результаты мониторинга позволяют в реальном времени корректировать параметры сетевых механизмов, распределять ресурсы, изменять маршрутизацию и адаптировать систему к изменяющимся условиям функционирования. Таким образом, мониторинг формирует основу для интеллектуального управления сетями нового поколения, основанного на принципах адаптивности, прогнозирования и самооптимизации. [1]

Однако при всех преимуществах таких подходов остается нерешенной важная проблема – влияние точности мониторинга функционирования сети. Ошибки в измерении параметров трафика, особенно в условиях высокой вариабельности мультимедийных потоков, могут приводить к некорректной настройке сетевых механизмов, ошибочному распределению потоков данных и, как следствие, к ухудшению качества обслуживания. Наиболее чувствительными к погрешностям мониторинга оказываются параметры, описывающие статистическую природу трафика – его интенсивность, распределение межпакетных интервалов и степень самоподобия, характеризующую параметром Херста ( $H$ ).

Современные исследования показывают, что мультимедийный трафик обладает выраженным свойством самоподобия: его колебания сохраняются на различных временных масштабах, что делает его существенно отличным от традиционных потоков, описываемых экспоненциальными или пуассоновскими распределениями [2–5]. Для адекватного описания поведения таких потоков применяются распределения Парето, Вейбулла и логнормальное распределение, которые позволяют учитывать тяжелые хвосты и фрактальную структуру трафика. При этом классические методы анализа сетевой производительности, основанные на простых марковских предположениях, не способны корректно оценивать поведение самоподобных процессов.

В рамках данного исследования предлагается комплексная модель влияния мониторинга сетевого трафика и качества обслуживания на эффективность функционирования сети передачи данных при использовании различных сетевых механизмов. Модель сочетает элементы теории массового обслуживания, методов статистического анализа и оптимизации.

Она описывает взаимосвязь между параметрами мониторинга (интенсивностью, функцией распределения, параметром Херста), управляемыми характеристиками сетевых механизмов и результирующими показателями QoS – в первую очередь средней задержкой, вариацией задержки и вероятностью потери пакетов.

Результаты работы имеют практическое значение для проектирования систем связи, обеспечивающих устойчивое функционирование при высокой изменчивости трафика и воздействии внешних факторов. Реализация разработанной модели позволяет не только повысить точность оценки состояния сети, но и оптимизировать работу сетевых механизмов, минимизировать задержки передачи и увеличить общую пропускную способность без необходимости значительного увеличения аппаратных ресурсов.

Таким образом, разработка модели влияния мониторинга сетевого трафика и качества обслуживания на эффективность функционирования сети передачи данных является актуальным направлением исследований, направлением исследований, направленным на создание адаптивных и интеллектуальных систем связи, способных к самоорганизации и устойчивому функционированию в условиях неопределенности.

### Математическая модель функционирования сети

Разработка модели влияния мониторинга сетевого трафика и качества обслуживания на эффективность функционирования сети передачи данных предполагает формализацию взаимосвязей между наблюдаемыми параметрами трафика, характеристиками сетевых механизмов и результирующими показателями QoS. В отличие от традиционных подходов, в которых данные мониторинга используются лишь для регистрации состояния сети, в предлагаемой концепции они становятся активным элементом системы управления, непосредственно влияющим на перераспределение потоков данных и ресурсов.

В основе построения модели лежит идея представления сети передачи данных как мультиагентной системы, состоящей из совокупности взаимосвязанных элементов (узлов, каналов, маршрутов), каждый из которых может адаптировать свои параметры в зависимости от текущего состояния трафика. Такая система функционирует под воздействием

множества факторов, включая внутренние процессы (нагрузку, очереди, производительность узлов) и внешние воздействия (помехи, ошибки мониторинга, изменение маршрутов).

Для формального описания функционирования СПД в работе используется аппарат теории массового обслуживания (СМО), что позволяет учитывать вероятностный характер процессов поступления, обработки и передачи данных. При этом ключевым отличием модели является учёт самоподобных свойств трафика, которые проявляются в виде фрактальных зависимостей и тяжёлых хвостов распределений межпакетных интервалов [6, 7]. Такие свойства невозможно корректно описать с использованием классических пуассоновских моделей, что требует введения обобщённых функций распределения, например, распределений Вейбулла, Парето или логнормального распределения.

Для учёта влияния мониторинга вводится дополнительный параметр – точность измерений, определяющая степень отклонения наблюдаемых данных от истинных характеристик трафика. Ошибки мониторинга проявляются в виде искажений интенсивности потоков, неточности оценки параметра Хёрста, а также неверной идентификации типа распределения межпакетных интервалов. Эти искажения влекут за собой изменения в расчётах нагрузки на каналы, величины задержки, вероятности потерь и других метрик QoS.

Таким образом, разработка математической модели должна учитывать следующие ключевые положения:

1. Нагрузка на сеть определяется не только характеристиками трафика, но и точностью мониторинга.
2. Показатели качества обслуживания зависят от реальных и измеренных параметров потоков.
3. Оптимальные управляемые параметры сетевых механизмов (например, доли распределения трафика по маршрутам) изменяются при учёте ошибок мониторинга.

Для описания этих взаимосвязей необходимо ввести систему уравнений, связывающих интенсивности потоков данных, пропускные способности каналов, управляемые параметры механизмов распределения и результаты мониторинга. Введём обозначение (1):

$$S_{\text{СПД}}(A, B, \Lambda, Z, Q), \quad (1)$$

где:  $A$  – множество узлов,  $B$  – множество ребер,  $\Lambda$  – интенсивность потоков данных,  $Z$  – управляемые параметры,  $Q$  – показатели качества обслуживания.

Нагрузка на каждый маршрут определяется соотношением (2):

$$\rho_l = \lambda_l / \mu_l, \mu_l = g_l / V, g_l = \min_{r \in R_l} g_{rl}, \quad (2)$$

где:  $\rho_l$  – интенсивность потока данных,  $\mu_l$  – интенсивность обслуживания,  $g_{rl}$  – пропускные способности ребер.

Для оценки общей эффективности функционирования сети целесообразно использовать интегральный показатель качества обслуживания, отражающий совокупное влияние всех маршрутов и механизмов распределения (3):

$$Q(q) = \sum_{k=1}^K \beta_k \cdot T_k, T_k = \sum_{m \in M_k} \alpha_{km} \cdot \tau_m, \quad (3)$$

где:  $T_k$  – усредненная задержка для  $k$ -го типа трафика,  $\beta_k$  – весовой коэффициент его приоритета,  $\alpha_{km}$  – доля потока, проходящая через маршрут  $m$ ,  $\tau_m$  – среднее время задержки на данном маршруте.

Средняя задержка, в свою очередь, выражается зависимостью (4):

$$\tau_l = (q_l(\rho_l) + 1) / \mu_l. \quad (4)$$

Эти выражения формируют основу математической модели функционирования СПД, в которой мониторинг выступает в роли механизма, обеспечивающего адаптацию управляемых параметров сети на основе текущих наблюдений. В дальнейшем данная модель будет расширена с учётом аппроксимационных зависимостей показателей QoS от параметра Хёрста и ошибок мониторинга, что позволит аналитически оценить влияние точности измерений на эффективность функционирования сети.

### Модель мониторинга параметров трафика и качества обслуживания

Одним из ключевых факторов, влияющих на точность работы сетевых механизмов управления, является качество мониторинга параметров сетевого трафика. Мониторинг выполняет не только информационную, но и управляющую функцию, обеспечивая обратную связь между текущим состоянием сети и системой принятия решений. В предлагаемой модели процесс мониторинга рассматривается как элемент, непосредственно участвующий в управлении потоками данных и влияющий на показатели качества обслуживания (QoS).

Для корректного выбора механизмов распределения трафика требуется информация о статистических характеристиках потока, включая интенсивность поступления пакетов, распределение межпакетных интервалов и коэффициент самоподобия. Эти характеристики формируются на основании данных мониторинга и определяют входные параметры математической модели функционирования сети.

### 1. Контролируемые параметры сетевого трафика

Мониторинг должен обеспечивать измерение и оценку следующих параметров:

- интенсивность потока ( $\lambda$ ) — среднее количество пакетов, поступающих в сеть за единицу времени;
- распределение межпакетных интервалов ( $p(t)$ ) — функция плотности вероятности, определяющая характер поступления пакетов;
- параметр Хёрста ( $H$ ) — мера самоподобия, отражающая фрактальную структуру трафика.

Эти параметры определяются по данным выборок, получаемых в процессе наблюдения, и подвержены ошибкам, обусловленным как ограниченным временем измерений, так и случайными внешними воздействиями. Таким образом, реальные значения параметров  $\hat{\lambda}$ ,  $\hat{H}$ ,  $\hat{p}(t)$ , полученные мониторингом, могут отличаться от истинных, что влечёт за собой искажения в расчётах нагрузки и показателей QoS.

### 2. Идентификация распределений и статистический анализ

Для оценки соответствия наблюдаемых выборок теоретическим моделям распределений межпакетных интервалов используются критерии согласия Пирсона ( $\chi^2$ ) и Колмогорова. Эти критерии позволяют определить степень близости эмпирической функции распределения  $F_n(x)$  к теоретической функции  $F(x)$ , что даёт возможность идентифицировать тип трафика и применить соответствующую аналитическую модель.

В рамках исследования рассматривались четыре наиболее распространённых типа распределений, описывающих поведение трафика в мультисервисных сетях:

- экспоненциальное распределение, характерное для потоков с равномерным поступлением пакетов;

- распределение Вейбулла, применяемое для описания слабо самоподобных потоков;
- распределение Парето, отражающее высокую степень самоподобия и наличие «тяжёлых хвостов»;
- логнормальное распределение, описывающее сложные нелинейные процессы в мультимедийном трафике.

Результаты вычислительных экспериментов показали, что при параметре  $H = 0,75$  критерий  $\chi^2$  является более чувствительным к различиям распределений, чем критерий Колмогорова. Это позволяет точнее определять модель трафика и выбирать соответствующую аппроксимацию для расчёта задержек и загрузки сети.

### 3. Аппроксимационные зависимости показателей QoS

На основании результатов анализа были получены аппроксимационные зависимости, связывающие параметры трафика с показателями QoS. Среднее относительное время ожидания (задержка) выражается как:

$$q_a = \frac{c(H) \cdot (\rho - \rho_0)^{a(H)}}{(1 - \rho)^{b(H)}}, \quad (5)$$

где  $\rho$  — относительная нагрузка, а параметры  $a(H)$ ,  $b(H)$  и  $c(H)$  зависят от коэффициента самоподобия:

$$\begin{aligned} a(H) &= d_a + e_a H, \\ b(H) &= \frac{d_b + e_b H}{1 - H}, \\ c(H) &= \frac{d_c + e_c H}{1 - H}. \end{aligned} \quad (6)$$

Эти зависимости позволяют описать характер изменения задержек при изменении нагрузки и учитывать влияние фрактальных свойств трафика. При увеличении параметра Хёрста наблюдается рост дисперсии межпакетных интервалов, что приводит к увеличению средней задержки и снижению устойчивости системы при высокой нагрузке.

Таким образом, предложенная аппроксимационная модель обеспечивает аналитическую взаимосвязь между измеряемыми параметрами мониторинга и показателями качества обслуживания. Это даёт возможность проводить прогнозирование поведения сети при различных сценариях нагрузки без необходимости проведения длительных имитационных экспериментов.



#### 4. Мониторинг QoS и адаптивное управление

На основании полученных зависимостей можно реализовать динамическую систему адаптивного управления. В этой системе результаты мониторинга (измеренные значения  $\hat{\lambda}$ ,  $\hat{H}$ ,  $\hat{p}(t)$ ) используются для вычисления прогнозных значений QoS-показателей – задержки ( $\tau$ ), вероятности потерь ( $P_{loss}$ ) и пропускной способности ( $C_{eff}$ ). Если наблюдаемые значения QoS отклоняются от допустимых, выполняется перераспределение потоков данных и ресурсов с помощью механизмов балансировки нагрузок.

Таким образом, модель мониторинга параметров трафика и качества обслуживания выполняет две функции:

1. Диагностическую – обеспечивает анализ текущего состояния сети и выявление отклонений от нормативных значений QoS;
2. Прогностическую – позволяет заранее оценивать последствия изменений параметров трафика и корректировать стратегию управления.

Данная модель мониторинга создаёт основу для последующего построения оптимизационной модели распределения потоков и ресурсов, в которой данные мониторинга используются как входные переменные. Это позволяет рассматривать мониторинг не как вспомогательный процесс, а как активный элемент контура управления, определяющий эффективность функционирования сети передачи данных в целом.

#### Оптимизация распределения потоков и ресурсов в условиях неточного мониторинга

Разработанные модели мониторинга параметров трафика и качества обслуживания позволяют использовать полученные данные для оптимизации распределения потоков данных и ресурсов сети. Цель оптимизации состоит в минимизации средней задержки передачи данных при заданных ограничениях на доступные ресурсы и уровне допустимых ошибок мониторинга. [6, 7]

В мультисервисных сетях передача данных осуществляется по нескольким маршрутам, которые могут иметь различную пропускную способность, задержку и надёжность. Для каждого маршрута определяются интенсивность потока  $\lambda_i$ , доля выделенных ресурсов  $\gamma_i$ , а также относительная нагрузка  $\rho_i = \lambda_i / \mu_i$ , где  $\mu_i$  – интенсивность обслуживания. Оптимальное

распределение трафика должно учитывать как реальные характеристики сети, так и измеренные значения параметров, полученные в процессе мониторинга.

#### 1. Постановка задачи оптимизации

Функционирование сети описывается интегральным показателем эффективности – средней задержкой передачи данных, выражаемой как:

$$T_0 = \frac{1}{\mu} \sum_{i=1}^n \frac{\alpha_i}{\gamma_i} (q(\rho_i) + 1), \quad (7)$$

где  $\alpha_i$  – доля потока данных, направляемого по  $i$ -му маршруту,  $\gamma_i$  – доля выделенных ресурсов, а  $q(\rho_i)$  – функция относительного времени ожидания, аппроксимированная в предыдущем разделе.

Задача оптимизации формулируется как поиск такого вектора управляемых параметров:

$$Z^* = \{\alpha_i, \gamma_i\}, \quad (8)$$

при котором достигается минимум интегрального показателя:

$$T_0(Z^*) = \min_Z T_0(Z), \quad (9)$$

при соблюдении ограничений на ресурсы и условия балансировки потоков:

$$\sum_{i=1}^n \alpha_i = 1, \sum_{i=1}^n \gamma_i = 1, \alpha_i, \gamma_i \geq 0. \quad (10)$$

Задача относится к классу нелинейных задач оптимизации с ограничениями, так как функция  $q(\rho_i)$  имеет нелинейную зависимость от нагрузки и параметра Хёрста. Для её решения могут применяться как аналитические методы (метод Лагранжа), так и численные методы (градиентные и итерационные алгоритмы).

#### 2. Влияние ошибок мониторинга на процесс оптимизации

В реальных условиях параметры  $\lambda_i$ ,  $\mu_i$ ,  $H$  определяются не точно, а с некоторой погрешностью, обусловленной ограниченной точностью мониторинга. Пусть измеренные значения параметров обозначены как  $\hat{\lambda}_i$ ,  $\hat{H}$ . Тогда реальная функция времени ожидания принимает вид:

$$\hat{q}_a = \frac{c(\hat{H}) \cdot (\hat{\rho} - \hat{\rho}_0(\hat{H}))^{a(\hat{H})}}{(1 - \hat{\rho})^{b(\hat{H})}}, \quad (11)$$

где параметры  $\hat{a}$ ,  $\hat{b}$ ,  $\hat{c}$  определяются по аппроксимационным формулам, аналогичным (2)–(4), но с ошибочными значениями  $\hat{H} = H + \Delta H$ .

Анализ показывает, что ошибки в параметре Хёрста ( $\Delta H = \pm 0,05 \dots 0,1$ ) и в интенсивности трафика ( $\Delta \lambda = \pm 5\%$ ) не оказывают значительного влияния на форму оптимального распределения потоков ( $\alpha_i^*$ ), однако приводят к смещению абсолютных значений задержки ( $T_0$ ) на величину до 20–30 %. Это означает, что оптимальные доли маршрутов остаются устойчивыми, но абсолютное качество обслуживания может ухудшиться из-за роста очередей и изменения пропускной способности при перегрузках.

Для учёта ошибок мониторинга в модели вводится корректирующий множитель точности:

$$K_m = 1 - \frac{\sigma_m}{\sigma_0}, \quad (12)$$

где  $\sigma_m$  — среднеквадратическое отклонение измеряемых параметров от истинных значений, а  $\sigma_0$  — нормативная точность мониторинга. При  $K_m < 0,9$  система должна переходить в режим стабилизации — перераспределяя ресурсы в сторону более надёжных маршрутов, не требующих высокой точности оценки трафика.

### 3. Механизм адаптивного перераспределения потоков

В условиях динамического изменения параметров трафика и возможных ошибок мониторинга применяется итерационная процедура перераспределения потоков. Она реализуется следующим образом:

1. На основании текущих данных мониторинга вычисляются значения интенсивностей  $\hat{\lambda}_i$ , нагрузок  $\hat{\rho}_i$  и параметра  $\hat{H}$ .
2. Производится расчёт оптимальных долей потоков  $\alpha_i^{(k)}$  и ресурсов  $\gamma_i^{(k)}$  по формуле (8).
3. Выполняется проверка критерия устойчивости:

$$|T_0^{(k)} - T_0^{(k-1)}| < \varepsilon, \quad (13)$$

где  $\varepsilon$  — допустимая погрешность.

### 4. Оценка эффективности функционирования сети

Для количественной оценки эффективности сети при различных уровнях точности мониторинга введён интегральный критерий эффективности:

$$E = \frac{Q_{ref}}{Q_{real}} \cdot K_m, \quad (14)$$

где  $Q_{ref}$  — эталонное значение показателя качества обслуживания (например, при идеальном

мониторинге),  $Q_{real}$  — значение при текущем уровне точности измерений.

Если  $E \geq 0,9$ , сеть функционирует в оптимальном режиме; если  $E < 0,7$ , требуется корректировка параметров или усиление мониторинга.

Моделирование показало, что при снижении точности мониторинга на 10 % интегральная эффективность уменьшается не более чем на 5 %, однако при погрешности свыше 25 % эффективность снижается на 20–25 %. Это подтверждает, что для устойчивой работы сетевых механизмов требуется поддержание точности мониторинга не ниже 75–80 % от номинального уровня.

Таким образом, предложенная модель оптимизации распределения потоков и ресурсов в условиях неточного мониторинга обеспечивает комплексный учёт параметров трафика, характеристик сети и ошибок измерений. Она позволяет формировать устойчивые управленческие решения, направленные на поддержание требуемого качества обслуживания при ограниченных ресурсах и неполной информации о состоянии сети.

В дальнейшем данная модель может служить основой для построения интеллектуальных систем управления мультисервисными сетями, способных к самоадаптации и прогнозируемому контролю качества обслуживания в реальном времени.

### Результаты исследования и выводы

Проведённые исследования позволили разработать и обосновать математическую модель, описывающую влияние мониторинга параметров сетевого трафика и качества обслуживания на эффективность функционирования мультисервисной сети передачи данных при использовании различных сетевых механизмов. Модель объединяет в себе процессы измерения и анализа параметров трафика, прогнозирования показателей QoS и оптимизации распределения потоков данных и ресурсов.

Рассмотренная в работе концепция исходит из предположения, что мониторинг должен рассматриваться не как пассивная подсистема наблюдения, а как активный элемент контура управления, определяющий эффективность функционирования сети в целом. Именно точность мониторинга параметров трафика, таких как интенсивность потока, распределение межпакетных интервалов и параметр Хёрста, оказывает определяющее

влияние на корректность принимаемых решений в механизмах распределения нагрузки и предотвращения перегрузок.

Результаты аналитического и имитационного моделирования показали, что при изменении точности мониторинга в пределах 10–15 % отклонение интегральных показателей эффективности функционирования сети не превышает 5 %. При этом распределение потоков данных по маршрутам остаётся практически неизменным, что свидетельствует о высокой устойчивости оптимизационного решения к незначительным ошибкам мониторинга. [4, 6, 7]

Однако при увеличении погрешности измерений параметров трафика до 25–30 % наблюдается значительное ухудшение показателей качества обслуживания – средняя задержка возрастает на 20–25 %, а вероятность потери пакетов увеличивается более чем в 1,5 раза. Особенно чувствительными оказываются сети с высокой степенью самоподобия трафика (параметр Хёрста  $H > 0.7$ ), для которых флуктуации нагрузки носят квазипостоянный характер, и ошибки мониторинга приводят к накоплению ошибок при прогнозировании QoS.

На основе предложенной модели получены следующие количественные и качественные результаты:

- разработаны аналитические зависимости, связывающие параметры трафика и точность мониторинга с показателями QoS (задержкой, пропускной способностью и вероятностью потерь);
- установлено, что параметр Хёрста оказывает существенное влияние на динамику нагрузки и должен учитываться при проектировании алгоритмов адаптивного управления;
- показано, что оптимизация распределения потоков данных по маршрутам возможна в режиме реального времени при использовании аппроксимационных зависимостей, построенных на основе данных мониторинга;
- доказано, что ошибки мониторинга до 10–15 % не влияют на структуру оптимального распределения потоков, однако снижают абсолютные показатели эффективности сети на 5–8 %;

- определено, что при уровне ошибок выше 25 % эффективность функционирования сети снижается не менее чем на 20 %, что требует внедрения механизмов компенсации и самокоррекции мониторинга.

Предложенная модель обеспечивает аналитическую оценку влияния мониторинга на показатели эффективности работы сети и может использоваться для обоснования требований к точности измерений параметров трафика. На её основе возможно формирование интеллектуальной системы адаптивного управления, способной в реальном времени корректировать параметры сетевых механизмов с учётом изменений нагрузки и погрешностей мониторинга.

Практическая значимость полученных результатов заключается в том, что предложенные зависимости и алгоритмы могут быть использованы при проектировании и эксплуатации мультисервисных сетей связи специального назначения, в том числе в системах управления беспилотными аппаратами, военных сетях передачи данных и критически важных инфраструктурах, где надёжность и своевременность обмена информацией имеют первостепенное значение.

В перспективе данная модель может быть расширена для учёта дополнительных факторов – вероятностных потерь пакетов при помехах, влияния протоколов транспортного уровня, стохастических свойств внешних воздействий, а также для интеграции с технологиями искусственного интеллекта, применяемыми в интеллектуальных системах мониторинга и адаптивного управления.

Таким образом, разработанная модель влияния мониторинга сетевого трафика и качества обслуживания на эффективность функционирования сети передачи данных позволяет не только повысить точность оценки параметров функционирования сети, но и обеспечить повышение устойчивости и производительности за счёт оптимизации использования доступных ресурсов. Она является основой для построения новых систем управления мультисервисными сетями, ориентированных на принципы самонастройки, самоорганизации и предиктивного контроля в условиях неопределённости.

## Литература

1. Белов Д. В., Сафронов Е. И. Методы мониторинга и анализа сетевого трафика в мультисервисных системах связи. // Телекоммуникации. – 2021. – № 6. – С. 14–21.
2. Одоевский С. М., Симонова К. О., Зизевский В. А. Анализ влияния точности мониторинга параметров сетевого трафика на качество его обслуживания // Техника средств связи. – 2024. – № 4(168). – С. 8–19.
3. Иванов А. А., Сидоров П. Н., Аналитические модели очередей в мультисервисных сетях передачи данных // Информационные технологии и телекоммуникации. – 2021. – Т. 9, № 4. – С. 45–54.
4. Кузьмин Д. В., Орлов С. Е. Моделирование задержек и перегрузок в сетях передачи данных при высокой нагрузке // Вестник связи. – 2022. – № 6. – С. 32–40.
5. Одоевский С. М., Симонова К. О., Зизевский В. А. Оценка степени влияния точности мониторинга сетевого трафика на качество его обслуживания в сетях связи военного назначения методами имитационного моделирования // Третья всероссийская научно-практическая конференция по имитационному моделированию и его применению в военной сфере «Имитационное моделирование систем военного назначения, действий войск и процессов их обеспечения» («ИМСВН-2024»). Труды конференции. – Санкт-Петербург: ВА МТО; Москва: РИОР, 2024. – 380 с. – ISBN 978-5-369-02166-8. С. 275–285.
6. Бердюгин А. В., Ковалев С. Н. Аналитическая модель влияния мониторинга на эффективность сетей передачи данных. // Научный вестник ВАС. – 2023. – № 2. – С. 40–48.
7. Одоевский С. М., Зизевский В. А., Рафальская М. И. Аппроксимация статистических характеристик процесса обслуживания мультимедийного трафика на основе логнормального распределения // Радиолокация, навигация, связь. Сборник трудов XXX Международной научно-технической конференции. В 5-ти томах. Воронеж, 2024. С. 96–105.

## NETWORK TRAFFIC MONITORING IMPACT MODEL AND EFFICIENCY ON THE NETWORK DATA TRANSFERS

Simonova K. O.<sup>2</sup>

**Keywords:** multiservice networks, quality of service, queuing systems, self-similar traffic, optimization.

### Abstract

**The purpose of the study** is to develop and analyze a mathematical model that describes the impact of monitoring network traffic parameters and quality of service indicators on the efficiency of the multiservice data transmission network using various network mechanisms.

**Research method:** analytical and simulation modeling of data transmission processes in network devices, statistical analysis of traffic parameters, as well as methods for optimizing the distribution of flows and resources with restrictions on control parameters are used in the work. To identify the characteristics of traffic, the criteria of agreement of Pearson and Kolmogorov, as well as the Hirst parameter as a measure of self-similarity, are used.

**Results of the study:** a mathematical model of the functioning of the data transmission network taking into account the service traffic of the monitoring was developed, the dependencies of the average delay on the load and the Hurst parameter were approximated, analytical expressions were obtained that allow assessing the efficiency of the network functioning under various network mechanisms of flow distribution. It is shown that monitoring errors within the range of the Hurst parameter  $H = 0.5 - 0.75$  insignificantly affect the optimal distribution of flows, but significantly change the absolute values of delays, which is important when implementing overload prevention mechanisms.

**Scientific novelty** consists in the development of a comprehensive model that combines the processes of monitoring, traffic analysis and optimization of network mechanisms, as well as in the proposal of new approximation dependencies that link the parameters of self-similar traffic with the indicators of service quality. This allows us to analytically assess the impact of monitoring accuracy on the efficiency of the multiservice data transmission network.

<sup>2</sup> Karina O. Simonova, Adjunct of the Department of Communication Networks and Switching Systems, S. M. Budenny Military Academy of Communications, St. Petersburg, Russia.  
E-mail: desire\_8912@bk.ru



## References

1. Belov D. V., Safronov E. I. Metody' monitoringa i analiza setevogo trafika v mul'tiservisny'x sistemax svyazi. // Telekommunikacii. – 2021. – № 6. – S. 14–21.
2. Odoevskij S. M., Simonova K. O., Zizevskij V. A. Analiz vliyaniya tochnosti monitoringa parametrov setevogo trafika na kachestvo ego obsluzhivaniya // Texnika sredstv svyazi. – 2024. – №4 (168). – S. 8–19.
3. Ivanov A. A., Sidorov P. N., Analiticheskie modeli ocheredej v mul'tiservisny'x setyax peredachi danny'x // Informacionny'e tekhnologii i telekommunikacii. – 2021. – T. 9, № 4. S. 45–54.
4. Kuz'min D. V., Orlov S. E. Modelirovanie zaderzhek i peregruzok v setyax peredachi danny'x pri vy'sokoj nagruzke // Vestnik svyazi. – 2022. - № 6. – S. 32–40.
5. Odoevskij S. M., Simonova K. O., Zizevskij V. A. Ocenka stepeni vliyaniya tochnosti monitoringa setevogo trafika na kachestvo ego obsluzhivaniya v setyax svyazi voennogo naznacheniya metodami imitacionnogo modelirovaniya // Tret'ya vserossiyskaya nauchno-prakticheskaya konferenciya po imitacionnomu modelirovaniyu i ego primeneniyu v voennoj sfere «Imitacionnoe modelirovanie sistem voennogo naznacheniya, dejstvij vojsk i processov ix obespecheniya» («IMSVN-2024»). Trudy' knferencii. – Sankt-Peterburg: VA MTO; Moskva: RIOR, 2024. – 380 s. – ISBN 978-5-369-02166-8. C. 275-285.
6. Berdyugin A. V., Kovalev S. N. Analiticheskaya model' vliyaniya monitoringa na e'ffektivnost' setej peredachi danny'x. // Nauchny'j vestnik VAS. – 2023. – № 2. – S. 40–48.
7. Odoevskij S.M., Zizevskij V.A., Rafal'skaya M.I. Approksimaciya statisticheskix xarakteristik processa obsluzhivaniya mul'timedijnogo trafika na osnove lognormal'nogo raspredeleniya // Radiolokaciya, navigaciya, svyaz'. Sbornik trudov XXX Mezhdunarodnoj nauchno-texnicheskoj konferencii. V 5-ti tomah. Voronezh, 2024. S. 96–105.



# ПРИМЕНЕНИЕ ЦИФРОВЫХ ДВОЙНИКОВ В ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ

Яровой Р. В.<sup>1</sup>, Карганов В. В.<sup>2</sup>, Лукашенко В. И.<sup>3</sup>

DOI:10.21681/3034-4050-2026-1-42-51

**Ключевые слова:** цифровой двойник, телекоммуникационная сеть, обнаружение аномалий, синтетические данные, машинное обучение, телеметрия, предиктивное обслуживание, искусственный интеллект.

## Аннотация

**Цель работы:** анализ возможности применения технологии цифровых двойников для обнаружения аномалий в телекоммуникационных сети с применением технологий искусственного интеллекта и обучением на синтетических данных.

**Метод исследования:** основан на применении математического моделирования, который предполагает созидание цифрового двойника телекоммуникационной сети посредством применения синтетически сгенерированных данных, которые имитируют поведение сети, а для обнаружения аномалий используется машинное обучение – обучение LSTM-автоэнкодера, с последующей оценкой качества обнаружения аномалий на основе метрик (precision, recall и F1-score).

**Результаты исследования:** включают разработку модели цифрового двойника телекоммуникационной сети, а также генерацию датасета на основе синтетических данных. В ходе исследования продемонстрировано, что может быть создан цифровой двойник телекоммуникационной сети, синтетически сгенерированы данные для обучения модели машинного обучения, при помощи которой могут быть обнаружены различные аномалии. В дальнейшем модель машинного обучения может быть использована в реальных телекоммуникационных сетях связи для обнаружения разного рода аномалий.

**Научная новизна:** заключается в разработке методики генерации синтетических данных с аномалиями, которые адаптированы под телекоммуникационные сети, а также в использовании цифрового двойника как инструмента для тестирования алгоритмов машинного обучения для обнаружения аномалий.

## Введение

Телекоммуникационные сети, которые используются в настоящее время для обмена информацией, охватывают все большее количество территорий, трансформируются и модифицируются с течением времени. Они предоставляют возможность огромному числу пользователей обмениваться разного рода информацией (звук, изображения, видео), являются основой для функционирования от мобильных сетей связи до интернета вещей, от автономного транспортного сообщения до услуг телеприсутствия в сфере здравоохранения. С учетом всеобъемлющего использования в подавляющем числе сфер жизни необходимость автоматизации наблюдения за различными параметрами сети, а также управления ими и адаптации становится

важным элементом для предоставления качественных услуг связи.

С учетом того, что традиционные методы обнаружения аномалий [1], с ростом объема трафика в телекоммуникационных сетях, становятся менее эффективными, необходим качественно новый переход от традиционных методов к более модернизированным. Более важным является вопрос обнаружения разного рода аномалий, таких как DDoS-атаки, перегрузка каналов, технические сбои, которые впоследствии могут привести к ухудшению качества предоставляемых услуг связи или к временному выходу из строя оборудования.

С учетом вышеизложенного одним из возможных решений, которое может повысить устойчивость и безотказность системы, является технология цифрового двойника.

<sup>1</sup> Яровой Роберт Владимирович, научный сотрудник научно-исследовательского центра Военной академии связи, г. Санкт-Петербург, Россия. E-mail: Nadzar@yandex.ru

<sup>2</sup> Карганов Виталий Вячеславович, кандидат технических наук, доцент, старший научный сотрудник научно-исследовательского центра Военной академии связи, г. Санкт-Петербург, Россия. E-mail: vitalik210277@mail.ru

<sup>3</sup> Лукашенко Василий Ильич, младший научный сотрудник научно-исследовательского центра Военной академии связи, г. Санкт-Петербург, Россия. E-mail: lukasenokvasilij@gmail.com

## 1. Теоретические основы цифровых двойников в телекоммуникациях

### 1.1. Понятие и определение цифрового двойника

Впервые концепция цифрового двойника, как виртуальной копии физического объекта, была предложена в 2002 году Майклом Гривсом. Цифровой двойник может быть использован для исследования влияния различных воздействий на моделируемый объект, не подвергая риску реальный объект. На данный момент концепция активно развивается и стандартизируется в различных сферах [2].

Согласно стандарту, BS ISO/IEC 30173, цифровой двойник – это «виртуальное представление физического объекта или системы, которое используется для понимания, прогнозирования и оптимизации характеристик и поведения физического объекта».

В телекоммуникационных системах цифровой двойник представляет из себя виртуальную модель сети, которая соединена с физической сетью и получает актуальные данные при помощи телеметрии и позволяет следующее [3]:

- моделировать поведение сети при различном влиянии на сеть;
- прогнозировать сбои и оптимизировать ресурсы сети;
- тестировать алгоритмы управления без ущерба для физической сети;
- автоматизировать процессы мониторинга сети.

### 1.2. Архитектура цифрового двойника телекоммуникационной сети

Архитектура цифрового двойника телекоммуникационной сети в большинстве случаев состоит из следующих частей [4]:

1. Физический уровень, который содержит реальные компоненты сети:

- базовые станции;
- устройства пользователей;
- ядро сети;
- различное сетевое оборудование: коммутаторы, маршрутизаторы, серверы.

2. Цифровой уровень (модель), который содержит виртуальное представление физических объектов:

- модели базовых станций, каналов связи, пользователей;

- алгоритмы расчета качества сигнала, пропускной способности, задержки;
- модели поведения пользователей (к примеру активность и мобильность).

3. Аналитический уровень, который содержит обработку данных и система принятия решений:

- сбор и хранение телеметрии;
- анализ в реальном времени;
- управление сетью (настройка параметров телекоммуникационной сети для предоставления услуг связи должного уровня).

### 1.3. Ключевые метрики телекоммуникационных сетей

Для создания цифрового двойника в целях предиктивной защиты от различных аномалий в телекоммуникационной сети необходимо подобрать набор соответствующих параметров [5, 6]:

1. Active UE: отражает число устройств, находящихся в зоне покрытия сети и ведущие обмен данными в настоящий момент времени. Данный параметр влияет на нагрузку телекоммуникационной сети, на число потребляемых ресурсов, а также на качество обслуживания.

2. DL Traffic: обозначает объем данных, передаваемых от сети к устройствам (пользователям сети). Данный параметр особо важен для планирования пропускной способности сети и распределения нагрузки между передающим оборудованием.

3. RSRP (Received Signal Reference Power, измеряется в дБм): данный параметр обозначает мощность сигнала, принимаемого устройством от базовой станции и принадлежит к перечню ключевых показателей качества радиоканала.

4. Active Sessions: данный параметр обозначает количество активных сессий в сети. Данный параметр близок по значению к Active UE, но может отличаться от него в определенных случаях (к примеру, когда пользователь в данный момент времени одновременно ведет разговор и пользуется интернетом).

### 1.4. LSTM-автоэнкодеры, как инструмент обнаружения аномалий

Для детектирования аномалий в телекоммуникационных сетях анализируют временные ряды с высокой размерностью и сложными зависимостями. В качестве инструмента для решения данной задачи могут быть использованы методы машинного обучения, которые

способны обучиться нормальным паттернам и определять отклонения от них для выявления аномалий в сети [7].

Можно выделить следующие достоинства автоэнкодеров:

- возможно обучение без учителя (не требуются размеченные данные для всех типов аномалий);
- способность обрабатывать многомерные данные (могут одновременно учитывать UE, трафик, RSRP и сессии в процессе мониторинга);
- обладают высокой эффективностью при грамотном обучении и настройке.

LSTM выбран исходя из следующих причин:

- работа с последовательностями, т.е. обладает способностью учета временных зависимостей (например, рост трафика за последний период времени);
- устойчивость к шуму (благодаря внутренним механизмам (забывание, вход, выход));
- предрасположенность к работе с длинными последовательностями (важно для телекоммуникационных сетей, в моментах аномалии могут проявляться в течении времени).

### 1.5. Методология обнаружения аномалий на основе ошибки восстановления

Основная идея метода – сначала обучить автоэнкодер на нормальных данных, для того чтобы он мог точно восстанавливать их. После обучения на нормальных данных, провести обучения на тестовых данных (включая аномалии), где вычисляется ошибка восстановления (MSE) [8], а если ошибка превышает порог – считается, что произошла аномалия.

Пусть  $X \in \mathbb{R}^{T \times D}$  – входная последовательность длиной  $T$  с  $D$  признаками.

Автоэнкодер предсказывает  $\hat{X} = f_{\theta}(X)$ .

Ошибка восстановления может быть определена по следующей формуле:

$$MSE = \frac{1}{T \times D} \sum_{t=1}^T \sum_{d=1}^D (X_{t,d} - \hat{X}_{t,d})^2, \quad (1)$$

где  $X$  – исходная последовательность,  $\hat{X}$  – восстановленная последовательность,  $T$  – длина последовательности,  $D$  – число признаков.

Порог  $\tau$  определяется как  $q$ -й перцентиль ошибки на нормальных данных по следующей формуле:

$$\tau = percentile(MSE_{normal}, q). \quad (2)$$

Аномалия в телекоммуникационной сети обнаруживается, если  $MSE > \tau$ .

## 2. Практическая реализация цифрового двойника телекоммуникационной сети

### 2.1. Генерация синтетических телеметрических данных

В целях создания цифрового двойника была разработана процедура генерации синтетических данных, которые имитируют работу телекоммуникационной сети в течение суток (24 часов) с шагом 10 секунд. Общее количество временных меток равно 8640, что соответствует 24 часам  $\times$  60 минут  $\times$  6 (интервалов в минуту).

Основой для создания нормальной нагрузки сети стал суточный профиль, который характерен для городских сетей, определяется по следующей формуле:

$$load\_profile(t) = 0,3 + 0,7 \cdot \left[ \exp\left(-\frac{(h(t)-8)^2}{8}\right) + \exp\left(-\frac{(h(t)-20)^2}{10}\right) \right], \quad (3)$$

где  $h(t) = [t/360] \bmod 24$  – текущий час суток,  $t$  – номер временного интервала.

На основе данного профиля были сгенерированы четыре ключевые метрики, которые представлены в таблице 1.

Таблица 1.

Ключевые метрики

№ п/п	Метрика	Диапазон
1	Active UE	10–300
2	DL Traffic Mbps	0–150
3	RSRP dBm	(–120) – (–70)
4	Active Sessions	5–400

Здесь  $\varepsilon$  – случайный шум, имитирующий флуктуации реальной сети.

Физический смысл метрик:

- Active UE – означает число активных пользовательских устройств, которое напрямую связано с нагрузкой;
- DL Traffic – означает объем передаваемых данных и важен для планирования ресурсов телекоммуникационной сети;
- RSRP – означает уровень сигнала и определяет качество связи;
- Active Sessions – означает число активных сессий и коррелирует с UE, но может отличаться от UE из-за мульти-сессий на устройствах пользователей.



## 2.2. Внедрение аномалий

В целях проверки эффективности и работоспособности цифрового двойника в синтетические данные были искусственно внедрены аномалии, характерные для реальных телекоммуникационных сетей [9–12]. Первая аномалия – технический сбой – в данном случае моделируется ситуация при которой происходит намеренное ухудшение качества радиоканала вследствие отказа оборудования или внешних помех. Данная аномалия была смоделирована в интервале с 12:00 до 12:10, когда уровень сигнала (показатель RSRP) искусственно понижался до диапазона от  $-115$  до  $-105$  дБм, что соответствует критично низкому качеству связи. В тоже время, когда было смоделировано снижение качества связи, в процессе мониторинга наблюдалось снижение загрузочного объема трафика на 70 %, что можно обусловить ухудшением качества соединения с активными пользователями, число которых также демонстрировало некоторое снижение. Вышеописанная ситуация отражает обычный сценарий сбоя в сети, при котором падение качества сигнала приводит к ухудшению сервиса и, следовательно, к потере пользователей. Вторая аномалия – DDoS-даный тип атаки имитирует злонамеренную нагрузку на сеть, при которой объем передаваемых данных стремительно возрастает, но при этом не уваливается число активных устройств пользователей [13, 14]. Аномалия с имитацией DDoS-атаки была смоделирована во временной период с 18:30 до 18:45, когда DL Traffic искусственно доводился

до уровня 120–200 Мбит/с, что значительно превышает нормальные значения для данного времени суток, при этом количество активных пользователей в сети оставалось неизменным. Состояние системы в данный момент времени с подобными параметрами соответствует стандартным признакам DDoS-атаки, т.к. рост трафика не сопровождается ростом пользовательской активности, что соответственно указывает на искусственное увеличение нагрузки на систему. Соответственно две вышеописанные аномалии были отмечены метками – «FAILURE» для технического сбоя и «DDoS» для атаки – что позволит в дальнейшем использовать их для оценки качества разработанной модели для обнаружения аномалий в сети.

## 2.3. Визуализация синтетических данных

На рисунке 1 представлены графики трех ключевых метрик за 24 часа: DL Traffic, RSRP и Active UE. Красные полупрозрачные области выделяют зоны аномалий:

Результаты анализа рисунка 1 позволили сделать следующие выводы:

- в зоне технического сбоя (с 12:00 до 12:10) наблюдается резкое падение показателей RSRP и DL Traffic, что соответственно сочетается с понижением количества пользователей;
- во временном промежутке с DDoS-атакой (18:30–18:45) наблюдается резкое повышение объема трафика без роста количества активных пользователей, что является маркером намеренного искусственного повышения нагрузки;



Рис. 1. Визуализация синтетических телеметрических данных телекоммуникационной сети с внедренными аномалиями

- нормальные параметры в телекоммуникационной сети в соответствии с суточным профилем с увеличением нагрузки в 8:00 и 20:00 соответствуют человеческой активности.

#### 2.4. Подготовка данных для обучения модели

В целях качественного обучения модели автоэнкодера были подготовлены данные следующим образом:

- выбраны признаки, на основе которых формируется результат (Active\_UE, DL\_Traffic\_Mbps, RSRP\_dBm, Active\_Sessions);
- проведена нормализация признаков: использован MinMaxScaler для масштабирования всех признаков в диапазоне от 0 до 1 включительно;
- формирование временных интервалов, где для работы с LSTM использованы последовательности длиной 60 шагов (10 минут).

#### 2.5. Архитектура и обучение LSTM-автоэнкодера

Для обнаружения аномалий была выбрана архитектура LSTM-автоэнкодера, которая хорошо работает с временными рядами и способна учиться нормальным паттернам, выявляя отклонения.

Модель создана с использованием библиотеки TensorFlow [15] и построена на следующей архитектуре из четырех блоков:

- Encoder: LSTM слой с 32 нейронами – предназначен для сжатия входной последовательности в скрытый массив данных;
- RepeatVector: создает копию скрытого массива данных для каждого временного интервала;
- Decoder: LSTM с 32 нейронами – восстанавливает исходную последовательность;
- TimeDistributed Dense: выходной слой, предназначенный для предсказания значения

определенных признаков на каждом временном интервале.

На основе синтетически сгенерированных данных [16] модель была обучена на нормальных данных (8431 последовательностей) в течение 15 эпох с размером батча равным 32 и размером валидационной выборки равным 10 % (от датасета), что в свою очередь соответствует рисунку 2.

На графике (рис. 2) можно обнаружить, что функция потерь на тренировочной и валидационной выборке имеет тенденцию стабильного снижения, следовательно, модель имеет хорошую сходимость. После 15 эпох функция потерь достигает значения ~0.005, что в свою очередь свидетельствует о том, что модель научилась восстанавливать нормальные паттерны.

#### 2.6. Обнаружение аномалий на полном датасете

После обучения модель была применена к полному датасету (включая аномалии). Для каждой последовательности вычислялась ошибка восстановления (MSE) согласно формуле 1. Порог для определения аномалии был установлен как 95-й перцентиль ошибки на нормальных данных на основе формулы 2. В данном случае аномалия обнаруживается, если  $MSE > \tau$ .

#### 2.7. Оценка качества обнаружения аномалий

Для оценки эффективности модели были рассчитаны стандартные метрики Precision, Recall, F1 [17] согласно формулам 4, 5, 6 соответственно:

$$\text{Precision} = \frac{TP}{TP + FP}; \quad (4)$$

$$\text{Recall} = \frac{TP}{TP + FN} \quad TP/(TP+FN); \quad (5)$$

$$F1 = 2 \times \frac{\text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}} \quad (6)$$

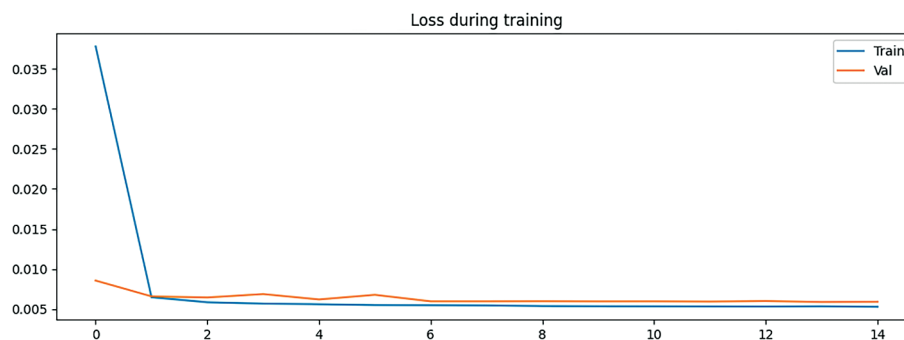


Рис. 2. График потерь

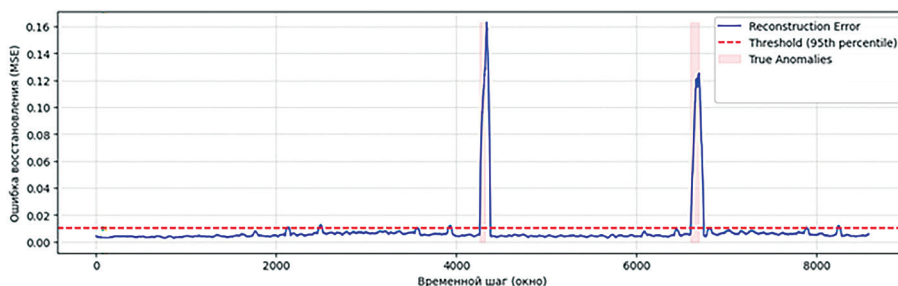


Рис. 3. Обнаружение аномалий с помощью цифрового двойника

где  $TP$  — истинно положительные,  $FP$  — ложно положительные,  $FN$  — ложно отрицательные.

В итоге были получены следующие результаты:

- Precision 89,2 % — означает, что из всех обнаруженных аномалий, 89,2 % действительно являются аномалиями;
- Recall 94,1% — означает, что модель обнаружила 94,1 % всех реальных аномалий;
- F1-score 91,6% — означает, что модель эффективно определяет истинные случаи, с низкой вероятностью ошибки.

## 2.8. Визуализация результатов обнаружения аномалий

На рисунке 3 представлена динамика ошибки восстановления для всех временных диапазонов, которая получена в результате работы LSTM-автоэнкодера. На основе визуального анализа графика можно сделать вывод о способности модели обнаруживать отклонения от нормального поведения сети на основе анализа различных временных последовательностей на основе ряда параметров.

На основе анализа графика (рис. 3) можно сделать следующие выводы:

1. На подавляющей части временного диапазона ошибка восстановления имеет низкое значение и не превышает 0,01, что также свидетельствует о том, что модель была качественно обучена на нормальных данных и способна восстанавливать нормальные паттерны телеметрии.

2. На временном шаге ~4200 можно наблюдать резкий скачок ошибки восстановления, который в пике достигает ~0,16, что в более чем 10 раз больше порога, который равен ~0,012, при этом данный скачок совпадает с розовой областью, которая обозначает аномалию и соответствует временному диапазону технического сбоя, который симулирован во временном диапазоне с 12:00 до 12:10.

3. Следующий рост ошибки  $MSE = \sim 0,13$  восстановления наблюдается на временном шаге ~6700, который соответствует временному диапазону симулирования DDoS-атаки с 18:30 до 18:45. Пик роста ошибки восстановления совпадает с областью аномалии и также значительно превышает пороговое значение.

4. Для баланса между чувствительностью и количеством ложных срабатываний был выбран порог на уровне 95-го перцентиля, следствием чего модель адекватно реагирует на небольшие естественные всплески активности, а при значительных всплесках правильно детектирует аномалии.

5. Возможность вывода актуального состояния телекоммуникационной сети в визуальном формате (в качестве примера можно привести график, который отображен на рисунке 3) предоставляет оператору сети возможность своевременно реагировать на возникающие аномалии с учетом возможности записи времени начала и идентификации типа атаки.

Объединяя вышеизложенное можно сделать вывод, что предложенный подход на основе LSTM-автоэнкодера, обученного на синтетических данных, обладает возможностью надежно детектировать как технические сбои, так и DDoS-атаки, путем анализа временных паттернов телеметрии.

## 2.9. Выводы по практической реализации

В итоге цифровой двойник позволил:

- генерировать правдоподобные синтетические данные с подконтрольными аномалиями;
- смоделировать и обучить LSTM-автоэнкодер для обнаружения аномалий;
- достигнуть показателей качества по метрике  $F1\text{-score} = 0,916$ , что является показателем качества модели;
- графически отобразить работу модели на примере двух типов аномалий (технического сбоя и DDoS-атаки).

Выше представленные результаты подтверждают возможность применения цифровых двойников в целях обучения, тестирования и внедрения алгоритмов обнаружения аномалий в телекоммуникационных сетях.

### 3. Анализ результатов и обсуждение

#### 3.1. Интерпретация метрик качества

Ссылаясь на раздел 2.7., модель продемонстрировала следующие показатели качества:

- Precision: 0,892;
- Recall: 0,941;
- F1-score: 0,916.

Основываясь на показателях перечисленных метрик, модель обладает высокой эффективностью модели в задаче обнаружения аномалий. Рассмотрим каждый показатель подробнее.

Precision (точность) = 0,892. Точность отражает количество истинно аномальных событий среди тех, которые модель классифицировала как аномалии. Значение 89,2 % означает, что на каждые 100 обнаруженных аномалий 89 действительно истинные, а 11 – соответственно ложные срабатывания. Достигнутый уровень считается приемлемым для систем мониторинга, в которых лишние оповещения не влияют на работу сети и не выводят ее из строя.

Recall (полнота) = 0,941 – данная метрика отражает способность модели обнаруживать все реальные аномалии. Значение 94,1 % соответствует тому, что модель успешно обнаруживает 94 из 100 реальных аномалий, что действительно важно в телекоммуникационных сетях, где какое-либо пропущенное негативное влияние может отрицательно сказаться на работоспособности сети или полностью вывести ее из строя.

F1-score = 0,916. F1-мера, отражающая гармоническое среднее между точностью и полнотой и отражает баланс между данными характеристиками. Значение 0,916 подтверждает тот факт, что был достигнут консенсус между точностью и полнотой, т.е. модель имеет небольшое число ложных срабатываний и в тоже время правильно выявляет большинство аномалий.

Исходя из удовлетворительных значений перечисленных метрик можно сделать вывод, что модель может быть использована в системах мониторинга телекоммуникационных сетей.

#### 3.2. Анализ причин ложных срабатываний и пропусков

С учетом достаточно высоких показателей метрик, модель все же допускает ошибки. На графике (рис. 3) присутствуют участки, на которых ошибка восстановления превышает заданный порог, но не детектируется как истинная аномалия (розовая область). Данные случаи могут трактоваться следующими факторами:

##### 1. Переходные процессы и шум.

В начале и в конце временного диапазона могут наблюдаться небольшие скачки, которые могут быть связаны с процессами запуска, остановки и шумом в данных. Примером является промежуток от 2000 до 2500 шага, где наблюдается небольшой рост ошибки восстановления, которая превышает порог и не совпадает с истинными аномалиями. Данный случай может быть вызван случайными процессами, которые модель интерпретирует как отклонение от нормального состояния.

##### 2. Пороговое значение.

С учетом того, что порог установлен на уровне 95 перцентиля, для определенного перечня аномалий, которые могут происходить в телекоммуникационных сетях, он (порог) может быть завышен, что приведет к тому, что аномалия не будет своевременно обнаружена. В обучающих данных также могут присутствовать выбросы, которые в итоге «приподнимают» порог вверх, что способствует пропуску незначительных аномалий. Для решения данного случая может быть использован динамический порог, который основан на статических методах (например,  $\text{mean} + 3\sigma$ ).

##### 3. Ограничения модели.

При использовании LSTM-автоэнкодера, который обучен на нормальных данных, автоэнкодер будет пытаться восстановить их, при этом, если аномалия будет иметь форму, которая близка к нормальному паттерну (в качестве примера можно привести медленный рост числа активных пользователей), модель может не обнаружить аномалию. Решением данного случая может быть использование добавочных признаков (скорость изменения RSRP) а также задействование ансамблевых методов.

#### 3.3. Влияние параметров на качество модели

На успех детектирования аномалий влияет следующий перечень параметров:



### 1. Длина временного окна.

Грамотный выбор временного диапазона (60 шагов равные по длительности 10 минутам) позволяет модели учитывать краткосрочные зависимости без излишней нагрузки на вычислительные ресурсы оборудования, но для обнаружения аномалий, которые по длительности меньше временного диапазона окна, необходим подбор соответствующей длины временного окна.

### 2. Количество нейронов в LSTM.

Каждый LSTM-слой в архитектуре модели использует 32 нейрона, что обеспечивает необходимую емкость для корректного обучения, если увеличить число нейронов до 64 или до 128 при грамотном обучении позволит повысить точность модели (но увеличивается время обучения и риск переобучения).

### 3. Количество эпох.

В данной исследовании модель обучалась в течении 15 эпох, чего достаточно для ее сходимости. Дальнейшее увеличение числа функция потерь продолжит снижаться, но незначительно, что указывает на достижение плато (рис. 2), т.е. дальнейшее обучение модели без изменения архитектуры и увеличения датасета не позволит увеличить качество модели.

## Заключение

В рамках проведенного анализа было выявлено, что подход с применением цифрового двойника и LSTM-автоэнкодера обладает требуемыми качествами для обнаружения аномалий. Разработанная модель показывает

высокие показатели по ряду метрик и с высокой вероятностью обнаруживает технические сбои и DDoS-атаки. При этом каждое «свое решение» модель основывает не только на основе текущего момента времени, но также на основе предыдущих параметров, что делает ее более подходящим вариантом для телекоммуникационных сетей, чем традиционные методы.

Однако, учитывая ранее изложенные результаты исследований в рамках данной статьи, модель имеет незначительные ограничения, которые связаны с чувствительностью к различным шумам, конечному набору признаков и заданному уровню порога. В целях повышения качества модели рекомендуется:

- применять более сложные архитектуры (к примеру, CNN-LSTM и Transformer);
- использовать при оценке качества модели дополнительные метрики (SINR, Latency, Handover Count);
- расширять количество параметров, на основе которых производится многомерный анализ, до перечня параметров в реальной сети.

Перечисленные выше рекомендации позволят создать эффективный инструмент для автоматизированного мониторинга телекоммуникационных сетей, который будет своевременно реагировать на разного рода угрозы и предотвращать их прежде чем они нанесут деструктивное воздействие, которое снизит качество предоставляемых услуг связи или выведет оборудование из строя.

## Литература

1. Попов А. А. Методы обнаружения аномалий в сетевом трафике // В сборнике: Наука, инновации, образование: актуальные вопросы XXI века. Сборник статей XIV Международной научно-практической конференции. Пенза, 2025. С. 30–33.
2. Шпак П. С., Сычева Е. Г., Меринская Е. Е. Концепция цифровых двойников как современная тенденция цифровой экономики // Вестник Омского университета. Серия: Экономика. 2020. Т. 18. № 1. С. 57–68.
3. Канаев А. К., Степанова А. Р. Цифровые двойники в телекоммуникациях // Научно-техническая конференция Санкт-Петербургского НТО РЭС им. А. С. Попова, посвященная Дню радио. 2024. № 1(79). С. 228–230.
4. Афонин И. Г., Кучерявый Е. А., Осипов Д. В., Морозов А. В. Алгоритмы ML для построения цифровых двойников в 5G // Вестник связи. 2024. № 12. С. 29–30.
5. Талибаева А. И., Рамазанов М. Б., Сайкен Д. Р., Хисамутдинов Р. М. Исследование технологических параметров телекоммуникационных сетей связи: методы оценки производительности беспроводных сетей // В сборнике: Global Challenges – Scientific Solutions II. proceedings. Antwerp, 2020. С. 225–227.
6. Новиковский К. В. Анализ параметров и модели качества в современных телекоммуникационных системах // Вестник Воронежского института высоких технологий. 2025. № 2(53).

7. Адамовский Е. Р., Богуш Р. П., Чертков В. М. Исследование эффективности LSTM нейронных сетей для прогнозирования занятости канальных ресурсов на основе данных карты радиосреды когнитивной системы связи // В сборнике: Информатика: проблемы, методы, технологии. Материалы XXIV Международной научно-практической конференции им. Э. К. Алгазиева. Воронеж, 2024. С. 148–153.
8. Кукурхоев А. М. Функция потерь MSE и MAE // В сборнике: Наука, образование, инновации: актуальные вопросы и современные аспекты. сборник статей XV Международной научно-практической конференции в 2 частях. Пенза, 2022. С. 85–86.
9. Амосов О. С., Амосова С. Г., Иванов Ю. С., Жиганов В. С. В. Использование глубоких нейронных сетей для распознавания аномалий сетевого трафика в информационно-телекоммуникационных системах предприятий // В сборнике: Управление развитием крупномасштабных систем MLSD'2019. Материалы двенадцатой международной конференции Научное электронное издание. Под общей ред. С. Н. Васильева, А. Д. Цвиркуна. 2019. С. 968–971.
10. Протасова М. А. Нейросетевой классификатор аномалий телекоммуникационной сети // В сборнике: Нейроинформатика–2015. XVII Всероссийская научно-техническая конференция с международным участием: сборник научных трудов. Ответственный редактор А. Г. Трофимов. 2015. С. 138–148.
11. Живодерников А. Ю., Ковайкин Ю. В., Лебедев П. В. Анализ источников сетевых аномалий в системах управления телекоммуникационными сетями // В сборнике: Проблемы технического обеспечения войск в современных условиях. Труды IV межвузовской научно-практической конференции. 2019. С. 298–301.
12. Акыев Г. А. Современные методы и алгоритмы мониторинга телекоммуникационных сетей // Инновационная наука. 2025. № 2-2. С. 37–39.
13. Яровой Р. В., Рябов Г. А., Карганов В. В. Кибербезопасность в мире инфотелекоммуникаций: вызовы и стратегии защиты // В сборнике: Инновационная деятельность в Вооруженных Силах Российской Федерации. Труды всеармейской научно-практической конференции. Санкт-Петербург, 2023. С. 373–377.
14. Зеленский М. Д. DDoS-атаки: типы атак, устранение DDoS-атак // В сборнике: Студенческая наука для развития информационного общества. сборник материалов IV Всероссийской научно-технической конференции: в 2-х томах. 2016. С. 241–243.
15. Эдель Г. Е. Глубокое обучение с использованием библиотеки TensorFlow // Электронные средства и системы управления. Материалы докладов Международной научно-практической конференции. 2020. № 1-2. С. 162–164.
16. Чайкин Г. А. Создание синтетических данных пользовательской активности на основе вопросно-ответных текстовых данных // Процессы управления и устойчивость. 2025. Т. 12. № 1. С. 417–421.
17. Никкель К. Е., Сосунов А. А. Классификация данных: метрики оценки качества моделей и алгоритмы // В сборнике: Цифровизация: новые тренды и опыт внедрения. Сборник статей Международной научно-практической конференции. Уфа, 2024. С. 39–44.

## APPLICATION OF DIGITAL TWINS IN TELECOMMUNICATIONS SYSTEMS

Yarovoy R. V.<sup>4</sup>, Karganov V. V.<sup>5</sup>, Lukashenok V. I.<sup>6</sup>

**Keywords:** digital twin, telecommunications network, anomaly detection, synthetic data, machine learning, telemetry, predictive maintenance, artificial intelligence.

### Abstract

**The aim of the work** is to analyze the possibility of using digital twin technology to detect anomalies in telecommunication networks using artificial intelligence technologies and training on synthetic data.

**Research method:** is based on the use of mathematical modeling, which involves the creation of a digital twin of a telecommunications network through the use of synthetically generated data that simulate the behavior of the network, and machine learning is used to detect anomalies – training of an LSTM autoencoder, with subsequent assessment of the quality of anomaly detection based on metrics (precision, recall and F1-score).

4 Robert V. Yarovoy, Researcher, Research Center, Military Academy of Communications, St. Petersburg, Russia. E-mail: Nadzar@yandex.ru

5 Vitaly V. Karganov, Ph.D. of Technical Sciences, Associate Professor, Senior Researcher of the Research Center of the Military Academy of Communications, St. Petersburg, Russia. E-mail: vitalik210277@mail.ru

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

**Results of the study:** include the development of a digital twin model of a telecommunications network, as well as the generation of a dataset based on synthetic data. In the course of the study, it was demonstrated that a digital twin of a telecommunications network can be created, data can be synthetically generated to train a machine learning model, with the help of which various anomalies can be detected. telecommunication networks to detect various kinds of anomalies.

**Scientific novelty:** lies in the development of a methodology for generating synthetic data with anomalies that are adapted to telecommunication networks, as well as in the use of a digital twin as a tool for testing machine learning algorithms to detect anomalies.

### References

1. Popov A. A. Metody obnaruzhenija anomalij v setevom trafike // V sbornike: Nauka, innovacii, obrazovanie: aktual'nye voprosy XXI veka. Sbornik statej XIV Mezhdunarodnoj nauchno-prakticheskoy konferencii. Penza, 2025. S. 30–33.
2. Shpak P. S., Sycheva E. G., Merinskaja E. E. Konceptija cifrovych dvojn timer kak sovremennaja tendencija cifrovoy jekonomiki // Vestnik Omskogo universiteta. Serija: Jekonomika. 2020. T. 18. № 1. S. 57–68.
3. Kanaev A. K., Stepanova A. R. Cifrovye dvojn timer v telekommunikacijah // Nauchno-tehnicheskaja konferencija Sankt-Peterburgskogo NTO RJeS im. A.S. Popova, posvjashhennaja Dnju radio. 2024. № 1(79). S. 228–230.
4. Afonin I. G., Kucherjavj E. A., Osipov D. V., Morozov A. V. Algoritmy ML dlja postroenija cifrovych dvojn timer v 5G // Vestnik svjazi. 2024. № 12. S. 29–30.
5. Talibaeva A. I., Ramazanov M. B., Sajken D. R., Hisamutdinov R. M. Issledovanie tehnologicheskix parametrov telekommunikacionnyx setej svjazi: metody ocenki proizvoditel'nosti besprovodnyx setej // V sbornike: Global Challenges – Scientific Solutions II. proceedings. Antwerp, 2020. S. 225–227.
6. Novikovskij K. V. Analiz parametrov i modeli kachestva v sovremennyx telekommunikacionnyx sistemah // Vestnik Voronezhskogo instituta vysokix tehnologij. 2025. № 2(53).
7. Adamovskij E. R., Bogush R. P., Chertkov V. M. Issledovanie jeffektivnosti LSTM nejronnyx setej dlja prognozirovanija zanjatosti kanal'nyx resursov na osnove dannyx karty radiosredy kognitivnoj sistemy svjazi // V sbornike: INFORMATIKA: PROBLEMY, METODY, TEHNOLOGII. Materialy XXIV Mezhdunarodnoj nauchno-prakticheskoy konferencii im. Je.K. Algazinova. Voronezh, 2024. S. 148–153.
8. Kukurhoev A. M. Funkcija poter' MSE i MAE // V sbornike: Nauka, obrazovanie, innovacii: aktual'nye voprosy i sovremennye aspekty. sbornik statej XV Mezhdunarodnoj nauchno-prakticheskoy konferencii v 2 chastjah. Penza, 2022. S. 85–86.
9. Amosov O. S., Amosova S. G., Ivanov Ju. S., Zhiganov V. S. V. Ispol'zovanie glubokix nejronnyx setej dlja raspoznavanija anomalij setevogo trafika v informacionno-telekommunikacionnyx sistemah predpriyatij // V knige: Upravlenie razvitiem krupnomasshtabnyx sistem MLSD'2019. Materialy dvenadcatoj mezhdunarodnoj konferencii Nauchnoe jelektronnoe izdanie. Pod obshhej red. S. N. Vasil'eva, A. D. Cvirguna. 2019. S. 968–971.
10. Protasova M. A. Nejrosetevoj klassifikator anomalij telekommunikacionnoj seti // V sbornike: Nejroinformatika–2015. XVII Vserossijskaja nauchno-tehnicheskaja konferencija s mezhdunarodnym uchastiem: sbornik nauchnyx trudov. Otvetstvennyj redaktor A. G. Trofimov. 2015. S. 138–148.
11. Zhivodernikov A. Ju., Kovajkin Ju. V., Lebedev P. V. Analiz istochnikov setevyx anomalij v sistemah upravlenija telekommunikacionnymi setjami // V sbornike: Problemy tehnicheskogo obespechenija vojsk v sovremennyx uslovijah. Trudy IV mezhvuzovskoj nauchno-prakticheskoy konferencii. 2019. S. 298–301.
12. Akyev G. A. Sovremennye metody i algoritmy monitoringa telekommunikacionnyx setej // Innovacionnaja nauka. 2025. № 2-2. S. 37–39.
13. Jarovoj R. V., Rjabov G. A., Karganov V. V. Kiberbezopasnost' v mire infotelekkommunikacij: vyzovy i strategii zashhity // V sbornike: Innovacionnaja dejatel'nost' v Vooruzhennyx Silah Rossijskoj Federacii. Trudy vsearmejskoj nauchno- prakticheskoy konferencii. Sankt-Peterburg, 2023. S. 373–377.
14. Zelenskij M. D. DDoS-ataki: tipy atak, ustranenie DDoS-atak // V sbornike: Studencheskaja nauka dlja razvitija informacionnogo obshhestva. sbornik materialov IV Vserossijskoj nauchno-tehnicheskoy konferencii: v 2-h tomah. 2016. S. 241–243.
15. Jedel' G. E. Glubokoe obuchenie s ispol'zovaniem biblioteki TensorFlow // Jelektronnye sredstva i sistemy upravlenija. Materialy dokladov Mezhdunarodnoj nauchno-prakticheskoy konferencii. 2020. № 1-2. S. 162–164.
16. Chajkin G. A. Sozdanie sinteticheskix dannyx pol'zovatel'skoj aktivnosti na osnove voprosno-otvetnyx tekstovyx dannyx // Processy upravlenija i ustojchivost'. 2025. T. 12. № 1. S. 417–421.
17. Nikkel' K. E., Sosunov A. A. Klassifikacija dannyx: metriki ocenki kachestva modelej i algoritmy // V sbornike: Cifrovizacija: novye trendy i opyt vnedrenija. Sbornik statej Mezhdunarodnoj nauchno-prakticheskoy konferencii. Ufa, 2024. S. 39–44.

# ОСОБЕННОСТИ ОРГАНИЗАЦИИ СЛУЖЕБНОЙ ТЕЛЕФОННОЙ СВЯЗИ НА ПУНКТАХ УПРАВЛЕНИЯ

Кузина Е. И.<sup>1</sup>, Панкин А. А.<sup>2</sup>, Потапов И. А.<sup>3</sup>, Назаров А. Д.<sup>4</sup>

DOI:10.21681/3034-4050-2026-1-52-58

**Ключевые слова:** аудиоконференцсвязь, системы связи, оперативное управление, время реакции, управляемость.

## Аннотация

**Цель исследования:** разработать предложения по использованию перспективной служебной телефонной аудиоконференцсвязи при ограниченном ресурсе служебных каналов связи.

**Метод исследования:** имитационное моделирование системы связи с ее оценкой по показателям эффективности. Эмпирический анализ на основе опыта трассовых испытаний для военных радиолиний различного назначения.

**Результат:** предложено описание варианта использования гибридной сети служебной телефонной аудиоконференцсвязи системы. На основе сети упрощается принятие коллективных решений, когда необходимо согласовать действия органов управления системой связи разных объединений, соединений и воинских частей.

**Научная новизна** исследования заключается в разработке ключевых требований к системе аудиоконференцсвязи, её классификации и влияния на управляемость системы связи. Рассматриваются аспекты надёжности, защищённости и устойчивости к внешним воздействиям. Проведена оценка показателя управляемости, учитывающая временные задержки на принятие решений, передачу информации и оперативную реакцию командного состава. Выявлены основные факторы, влияющие на скорость и эффективность управления. Рассмотрены пути повышения оперативности и устойчивости системы связи в сложных условиях. Обоснована необходимость совершенствования средств аудиоконференцсвязи для повышения эффективности управления подразделениями. Статья может быть полезной для специалистов и разработчиков алгоритмов функционирования систем радиосвязи в сложной помеховой обстановке.

## Введение

В современных условиях информационной насыщенности и быстрого развития технологий все большие требования предъявляются к системам оперативного управления [1]. Актуальность эффективных способов коммуникации не вызывает сомнений, поскольку даже малейшая задержка в передаче распоряжений (указаний) способна повлиять на итог выполнения поставленной задачи. Это особенно важно при управлении системой связи в ходе проведения различных учений. В таких обстоятельствах особую роль играет аудиоконференцсвязь специального назначения (АКС СН), позволяющая нескольким участникам одновременно обмениваться устной служебной информацией в рамках одного непрерывного

сеанса [2, 3]. Она становится критически значимой для координации действий и оперативного реагирования [4]. Любой нештатный сбой в подобных коммуникационных решениях может привести к невосполнимой потере времени и ресурсов.

Ввиду отсутствия в действующих руководящих документах понятийного аппарата возникает необходимость дать чёткое определение, назначение и классификацию АКС СН. Аудиоконференцсвязь специального назначения – это организационно-техническое объединение сил и средств по обеспечению доступа к телекоммуникационным сервисам, обеспечивающим прием, обработку, передачу и доставку голосовых сообщений между несколькими участниками в режиме реального времени

<sup>1</sup> Кузина Екатерина Ивановна, преподаватель кафедры общепрофессиональных дисциплин Военной академии связи имени Маршала Советского Союза С. М. Буденного, Санкт-Петербург. Россия. E-mail: kuzik78@mail.ru

<sup>2</sup> Панкин Андрей Алексеевич, кандидат технических наук, доцент кафедры общепрофессиональных дисциплин Военной академии связи имени Маршала Советского Союза С. М. Буденного, Санкт-Петербург. Россия. E-mail: vava\_60@mail.ru

<sup>3</sup> Потапов Илья Александрович, кандидат технических наук, доцент кафедры общепрофессиональных дисциплин Военной академии связи имени Маршала Советского Союза С. М. Буденного, Санкт-Петербург. Россия. E-mail: potap\_ia@mail.ru

<sup>4</sup> Назаров Алексей Дмитриевич, адъюнкт кафедры сетей связи и систем коммутации Военной академии связи имени Маршала Советского Союза С. М. Буденного, Санкт-Петербург. Россия. E-mail: salexey07@mail.ru.ru



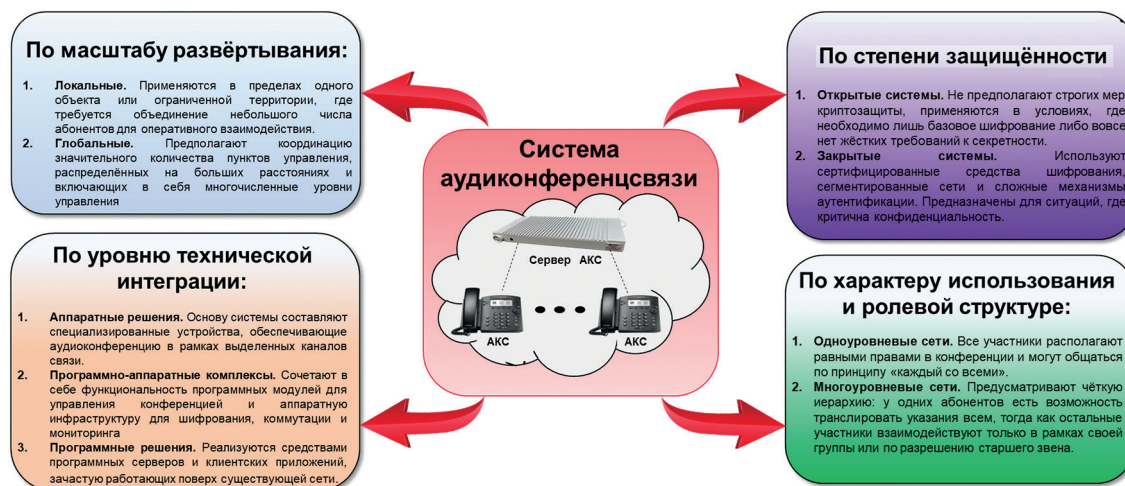


Рис. 1. Классификация аудиоконференцсвязи

с целью организации групповой связи. Классификация АКС может базироваться на нескольких критериях, включая масштабы применения, уровень технической интеграции, степень секретности, а также характеру использования и ролевой структуре (рис. 1).

Независимо от выбранной классификации, требование к АКС остаётся общей, обеспечить одновременную голосовую коммуникацию в режиме реального времени [5]. Важно также подчеркнуть, что подобные системы могут эффективно работать только при условии правильной организационной подготовки и регулярного контроля за техническим состоянием системы АКС [6]. Наличие чёткой структуры классификации упрощает выбор конкретного решения для каждой ситуации. Дополнительно обращают внимание на требования к шифрованию, чтобы исключить возможную утечку служебной информации в ходе переговорного процесса. При создании локальной или глобальной сети АКС СН учитывают предполагаемые сценарии использования, численность абонентов и их иерархию.

### Постановка задачи

В настоящее время АКС СН представляет собой незаменимый инструмент, позволяющий синхронизировать усилия многочисленных участников процесса управления системой связи. Её роль и актуальность особенно велика в ситуациях, требующих мгновенной реакции и безошибочного распространения критической служебной информации [7]. При соблюдении всех требований и грамотном учёте классификационных особенностей

она обеспечивает устойчивое, непрерывное и безопасное взаимодействие. Необходимым ключевым фактором обеспечения бесперебойного управления системой связи является организация надёжной и защищённой служебной связи на узлах связи пунктов управления [8, 9]. От того, какова география развёртывания и как распределяются роли участников, напрямую зависят требования к пропускной способности каналов и вариантам шифрования. Возникает задача предоставления пользователям услуги АКС СН при ограниченном ресурсе служебных каналов связи. Построенная система АКС СН по принципу постоянно действующей, обязана реагировать на все изменения внешних и внутренних воздействий сети. Основные требования к АКС СН сводятся к стабильности и устойчивости канала связи, защищённости передаваемых данных, стойкости против внешних и внутренних воздействий, а также наличия резервных маршрутов передачи данных.

**Решение.** Рассмотрим основные особенности построения предлагаемых сетей АКС СН, исходя из классификации, в которой ключевым признаком будет выступать именно масштаб сетей, локальный или глобальный, а также предопределённость их применения к управляемости системы связи в целом.

**Локальные сети АКС СН.** Локальная сеть АКС СН - это форма защищённой служебной связи, организуемой в пределах узла связи для обеспечения оперативного управления его элементами. Они предназначены для объединения всех постов, включая удалённые опорные узлы связи (или другие элементы),

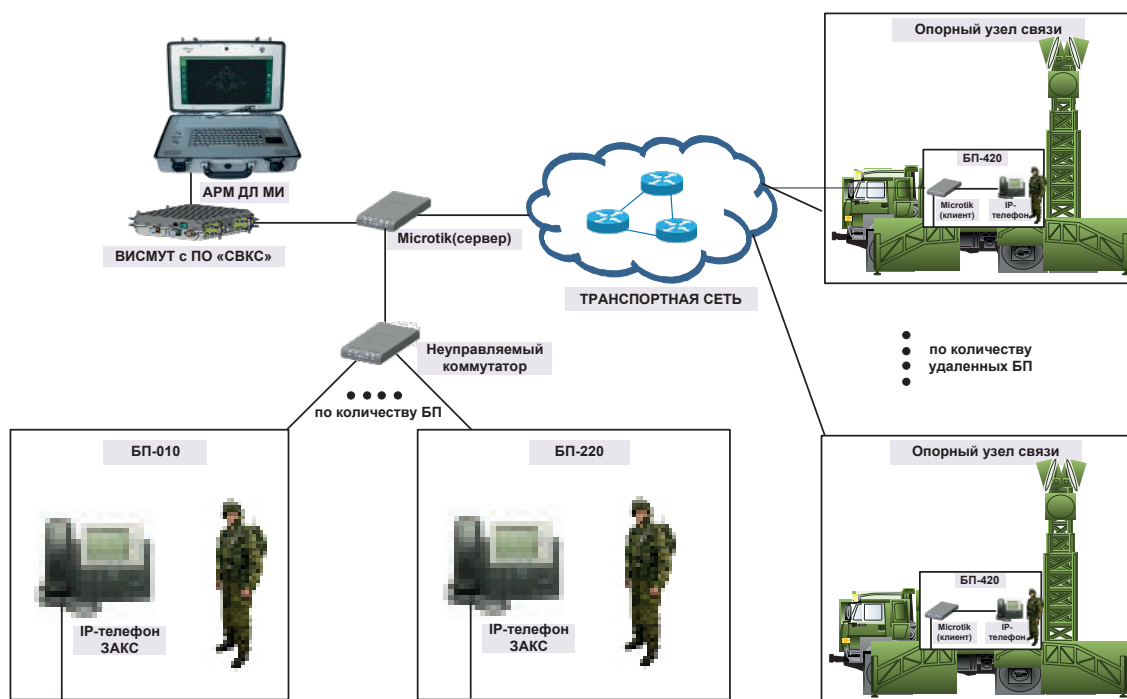


Рис. 2. Типовой пример развертывания локальной аудиоконференцсвязи специального назначения

в единую коммуникационную сеть, позволяя оперативно передавать команды, координировать действия дежурных расчетов и обеспечивать бесперебойное функционирование системы связи (рис. 2).

Чтобы локальная сеть АКС СН выполняла свою функцию максимально эффективно, необходимо учесть ряд рекомендаций при её построении:

- учёт конфигурации узла связи, на этапе проектирования важно определить физические и логические сегменты, которые нужно объединить в одну сеть. Сюда входят как непосредственно посты, так и вспомогательные элементы (центры каналообразования, центры радиосвязи, отдельные узлы для обеспечения связи начальников родов и служб, передовые пункты технического обслуживания и др.), чем точнее отражена структура узла связи, тем проще реализовать схему взаимодействия;
- безопасность передачи данных, несмотря на то, что локальная сеть АКС СН ориентируется на ближайший круг абонентов, сохраняется риск несанкционированного доступа. Важно применять как минимум базовые криптографические решения, шифруя голосовой трафик и используя

защищённые протоколы аутентификации для каждой подключаемой точки;

- удобство масштабирования, задача локальной сети АКС СН может выйти за первоначально задуманные пределы (например, при расширении узла связи или добавлении новых постов). За ранее необходимо заложить возможность подключения дополнительных абонентов или интеграции сети с другими элементами системы связи без радикальной перестройки оборудования.

Таким образом, локальная сеть АКС СН даёт значительные преимущества в координации и скорости принятия решений, обеспечивая высокую степень надёжности и устойчивости при условии правильно спроектированной архитектуры и грамотного использования технических средств АКС. Её применение в пределах одного узла связи помогает оперативно решать тактические задачи и закладывает основу для поддержания устойчивого информационного обмена при дальнейшей интеграции с другими звеньями управления системы связи.

### Глобальная сеть АКС СН

Глобальная сеть АКС СН – это форма защищенной служебной связи, организуемой

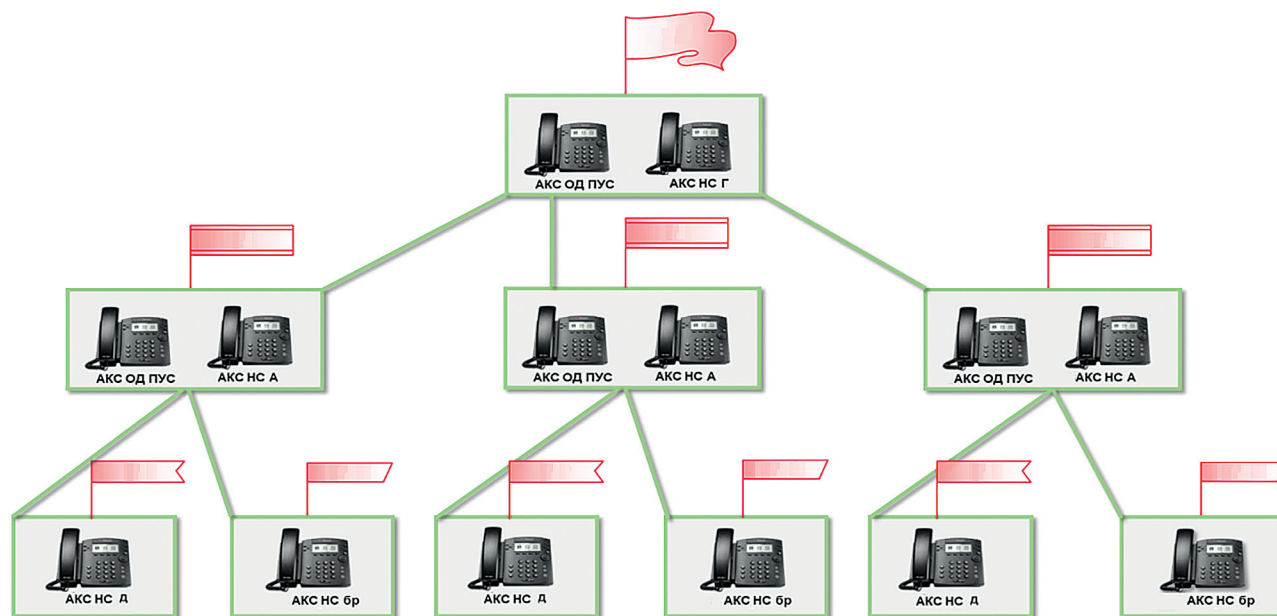


Рис. 3. Типовой пример развертывания глобальной аудиоконференцсвязи специального назначения

для обеспечения централизованного управления пунктами управления связи подчиненных объединений, соединений и подразделений с пункта управления связи (рис. 3). Она предназначена для объединения всех элементов системы управления связи в единую сеть, позволяя оперативно передавать распоряжения, координировать взаимодействие между различными уровнями управления, обеспечивать контроль за работой всех узлов связи и гарантировать бесперебойное функционирование всей системы связи по направлениям.

Организация глобальной сети АКС СН предоставляет ряд неоспоримых преимуществ. Во-первых, она создаёт единую платформу взаимодействия, позволяющую оперативно передавать распоряжения и поддерживать постоянный контакт между различными уровнями управления. Во-вторых, централизованный подход даёт возможность контролировать работоспособность и нагрузку на все узлы связи, своевременно выявлять и устранять неисправности или сбои. В-третьих, подобная система гарантирует непрерывное функционирование всей сети по всем направлениям, обеспечивая мгновенное доведение команд до всех ее элементов.

Необходимо учитывать ряд рекомендаций, при которых глобальная сеть АКС СН действительно оправдывает своё предназначение и будет работать без сбоев:

- централизованный формат управления и гибкая интеграция абонентов, высокий уровень управления и возможность подключать новые подразделения к сети без сложных процедур. Это может быть реализовано через создание «конференц-комнат» или групповых сегментов, где определённые абоненты наделяются правами управления и контроля. Важно выработать понятные регламенты, чтобы все участники системы понимали процедуру подключения и взаимодействия;
- присвоение позывных и организация непрерывного дежурства, в масштабной сети особенно важно быстро и корректно идентифицировать абонентов, исключая путаницу и задержки. Назначение цифровых позывных для каждого участника упрощает взаимодействие, дополнительно требуется обеспечить круглосуточное дежурство операторов, отвечающих за техническую поддержку системы;
- особое внимание обратить к защите каналов связи, поскольку в глобальном формате передаётся стратегически ценная служебная информация, кибербезопасность выходит на первый план. Использование зашифрованных протоколов (криптографических алгоритмов, VPN-технологий), постоянная проверка ключей и сертификация оборудования минимизируют риски

перехвата, искажения или блокировки потока данных.

В условиях, когда управление крупными силами требует слаженного и оперативного взаимодействия десятков и сотен пунктов связи, глобальная сеть АКС СН служит незаменимым инструментом. Она не только ускоряет процесс принятия решений, но и существенно уменьшает вероятность дезорганизации при обострении обстановки. При правильной организации такой связи, включая чёткое соблюдение регламентов, распределение ролей, установку защищённого оборудования и непрерывное круглосуточное дежурство, удаётся добиться высокой эффективности управления системой связи. Именно поэтому глобальные сети АКС СН становятся основополагающим элементом инфраструктуры системы связи пунктов управления, гарантируя надёжный и безопасный канал взаимодействия на всех уровнях управления.

### Влияние АКС СН на управляемость системы связи

Одним из ключевых аспектов применения АКС СН в системе управления является её влияние на оперативность принятия решений и координацию действий. Эффективность функционирования системы связи определяется не только её техническими характеристиками, но и степенью влияния АКС СН на управляемость системы связи в целом. В условиях динамично меняющейся обстановки критически важно учитывать, как взаимодействие между участниками конференц-связи сказывается на скорости передачи информации и принятию решений [10].

Управляемость системы определяется как её способность переходить из одного состояния в другое под воздействием управляющих факторов. Известно множество подходов к оценке управляемости: математические, системно-динамические, структурные, эмпирические, экспертные, комплексные. В прикладных задачах часто используются упрощённые критерии, такие, как время достижения цели. Тогда количественно управляемость системы АКС СН можно выразить через временные затраты  $T_{\text{упр.АКС СН}}$  на её переходы между состояниями [11]:

$$T_{\text{упр.АКС СН}} = T_{\text{пр}} + T_{\text{обр}} + T_{\text{прд}} + T_{\text{р}}, \quad (1)$$

где  $T_{\text{пр}}$  – время принятия решения,  $T_{\text{обр}}$  – время обработки информации,  $T_{\text{прд}}$  – время передачи

управляющего сигнала,  $T_{\text{р}}$  – время оперативной реакции.

Важным аспектом является влияние АКС СН на оперативную реакцию. В условиях коллективного обсуждения и необходимости координации действий нескольких участников может увеличиваться из-за временных затрат на согласование позиций, передачу распоряжений и подтверждение их получения. Таким образом, общая управляемость системы ухудшается при недостаточно регламентированном процессе взаимодействия.

Для решения минимизации этого эффекта и повышения управляемости системы АКС СН необходимо: оптимизировать алгоритмы принятия решений и их автоматизированную поддержку, применять эффективные протоколы передачи команд, исключая избыточные коммуникации, использовать специализированные технические средства, снижающие задержки в передаче и обработке информации.

Управляемость системы связи, построенной на основе АКС СН требует тщательной организации и технической оптимизации для уменьшения и обеспечения своевременного управления, а также подтверждает ее ключевую роль в управлении системой связи. Локальные сети обеспечивают оперативное доведение команд и координацию дежурных расчетов, глобальные обеспечивают централизованное управление несколькими пунктами связи, а наибольшая эффективность достигается при ее гибридной архитектуре, объединяя оба формата в единую систему с общим управлением АКС СН.

### Выводы

Таким образом, накопленный практический опыт применения АКС СН показывает, что возникает необходимость в совершенствовании гибридной структуры сети:

- усиление мер по кибербезопасности, развитие криптографических механизмов и протоколов шифрования, обеспечивающие удобство использования и интеграции новых устройств связи в общую сеть;
- увеличение масштабируемости и отказоустойчивости, создание программно-аппаратных комплексов, автоматически адаптирующихся к изменениям топологии внешней и внутренней сети;



- совершенствование нормативно-методической базы, детализация подходов к развертыванию, эксплуатации и обслуживанию АКС СН на разных уровнях управления;
- подготовка и обучение младших специалистов АКС СН способных эффективно работать с современными средствами связи, устранять проблемы на местах и реагировать на новые требования оперативно-тактической обстановки.

Стремительное развитие АКС СН в современных условиях, не только способствует повышению оперативности и защищенности предоставленных каналов служебной связи,

но и повышает общий уровень управляемости всей системы связи за счет применения гибридной архитектуры сети АКС СН. В дальнейшем комплексный подход к модернизации, включающий технологические, организационные и методические аспекты, станут залогом повышения эффективности управления подразделениями и непрерывного совершенствования всей инфраструктуры связи. На основе гибридной сети АКС СН упрощается принятие коллективных решений, особенно когда необходимо срочно согласовать действия органов управления системой связи разных объединений, соединений и воинских частей.

### Литература

1. Виноградов М. В. Современные методы и средства управления в сетях видеоконференцсвязи / М. В. Виноградов // Вестник связи. – 2007. – № 6. – С. 81–85.
2. Карапузов А. Н., Мякотин А. В., Кузин П. И. Поддержка защищенности в автоматизированных системах управления повседневной деятельности. Известия Высшей военной школы Генерального штаба Вооруженных сил Республики Ангола. 2025. № 1. С. 25–27.
3. Сорокин М. А., Курило А. А., Кузин П. И. Модель процесса анализа служебного трафика при управлении безопасностью информационной сети. Вопросы оборонной техники. Серия 16: Технические средства противодействия терроризму. 2021. № 1-2 (151-152). С. 67–73.
4. Олифер В. Г. Компьютерные сети. Принципы, технологии, протоколы / В. Г. Олифер, Н. А. Олифер – Санкт-Петербург: Питер, 2017. – 992 с.
5. Wischik D. Buffer Size for Core Routers / D. Wischik, N. McKeown // Computer Communication Review. – 2005. – V. 3. – № 35. – P. 75–78.
6. Виноградов В. С. Системы видеоконференцсвязи / В. С. Виноградов, В. В. Метлицкий // СТЭЛ [сайт]. – URL: <http://www.stel.ru/press/article> (дата обращения: 02.03.2022).
7. Кузин П. И., Челахов Д. М., Miguel Domingos P. Предложения по применению беспроводных сенсорных сетей в военной отрасли // Известия Высшей военной школы Генерального штаба Вооруженных сил Республики Ангола. 2025. № 1. С. 34–38.
8. Болюбаш О. О. Алгоритм сбора, обработки и передачи информации о состоянии сети передачи данных / О. О. Болюбаш // Информационные технологии: наука, техника, технология, образование, здоровье. Материалы XI международной НПК. – Москва: НТУ «ХИИ», 2003. – С. 45.
9. Лившиц Б. С. Теория телетрафика / Б. С. Лившиц, А. П. Пшеничников, А. Д. Харкевич – Москва : Связь, 1979. – 224 с.
10. Иванов В. Г., Челахов Д. М., Кузин П. И., Manuel André C. Единое информационное пространство как техническая основа системы управления подразделениями. Известия Высшей военной школы Генерального штаба Вооруженных сил Республики Ангола. 2025. № 1. С. 43–47.
11. Lipatnikov V., Belov A., Kuzin P., Rabin A. Determination of linear spectral frequencies // В сборнике: AIP Conference Proceedings. Melville, New York, United States of America, 2021. С. 30046.

## FEATURES OF THE ORGANIZATION OF BUSINESS TELEPHONE COMMUNICATION AT CONTROL ROOMS

*Kuzina E. I.<sup>5</sup>, Pankin A. A.<sup>6</sup>, Potapov I. A.<sup>7</sup>, Nazarov A. D.<sup>8</sup>*

5 Ekaterina I. Kuzina, Lecturer of the Department of General Professional Disciplines of the Military Academy of Communications named after Marshal of the Soviet Union S. M. Budyonny, St. Petersburg. E-mail: kuzik78@mail.ru

6 Andrey A. Pankin, Ph.D. of Technical Sciences, Associate Professor of the Department of General Professional Disciplines of the Military Academy of Communications named after Marshal of the Soviet Union S. M. Budyonny, St. Petersburg. E-mail: vava\_60@mail.ru

7 Ilya A. Potapov, Ph.D. of Technical Sciences, Associate Professor of the Department of General Professional Disciplines of the Military Academy of Communications named after Marshal of the Soviet Union S. M. Budyonny, St. Petersburg. E-mail: potap\_ia@mail.ru

8 Alexey D. Nazarov, Adjunct of the Department of Communication Networks and Switching Systems of the Military Academy of Communications named after Marshal of the Soviet Union S.M. Budyonny, St. Petersburg. E-mail: salexey07@mail.ru

**Keywords:** audio conferencing, communication systems, operational control, response time, controllability.

#### **Abstract**

**Objective:** to develop proposals for the use of promising business telephone audio conferencing with a limited resource of communication service channels.

**Research method:** simulation modeling of the communication system with its evaluation by performance indicators. Empirical analysis based on the experience of en-route tests for military radio links for various purposes.

**Result:** a description of the use of a hybrid network of the service telephone audio conferencing system is proposed. On the basis of the network, collective decision-making is simplified, when it is necessary to coordinate the actions of the management bodies of the communication system of different associations, formations and military units.

**The scientific novelty** of the research lies in the development of key requirements for the audio-conferencing system, its classification and impact on the controllability of the communication system. The aspects of reliability, security and resistance to external influences are considered. An assessment of the controllability index is carried out, taking into account the time delays for decision-making, information transmission and operational reaction of the command staff. Ways to increase the efficiency and stability of the communication system in difficult conditions are considered. The need to improve audio conferencing tools to improve the efficiency of department management is substantiated. The article may be useful for specialists and developers of algorithms for the functioning of radio communication systems in a complex jamming environment.

#### **References**

1. Vinogradov M. V. Sovremennyye metody i sredstva upravleniya v setjah videokonferentsvjazi / M. V. Vinogradov // Vestnik svjazi. – 2007. – № 6. – С. 81–85.
2. Karapuzov A. N., Mjakotin A. V., Kuzin P. I. Podderzhka zashishhennosti v avtomatizirovannyh sistemah upravleniya povsednevnoj dejatel'nosti. Izvestija Vysshej voennoj shkoly General'nogo shtaba Vooruzhennyh sil Respubliki Angola. 2025. № 1. S. 25–27.
3. Sorokin M. A., Kurilo A. A., Kuzin P. I. Model' processa analiza sluzhebnogo trafika pri upravlenii bezopasnost'ju informacionnoj seti. Voprosy oboronnoj tehniki. Seriya 16: Tehnicheskie sredstva protivodejstviya terrorizmu. 2021. № 1-2 (151-152). S. 67–73.
4. Olifer V. G. Komp'yuternye seti. Principy, tehnologii, protokoly / V. G. Olifer, N. A. Olifer – Sankt-Peterburg: Piter, 2017. – 992 s.
5. Wischik D. Buffer Size for Core Routers / D. Wischik, N. McKeown // Computer Communication Review. – 2005. – V. 3. – № 35. – P. 75–78.
6. Vinogradov V. S. Sistemy videokonferentsvjazi / V. S. Vinogradov, V. V. Metlickij // STJeL [sajt]. – URL: <http://www.stel.ru/press/article> (data obrashhenija: 02.03.2022).
7. Kuzin P. I., Chelahov D. M., Miguel Domingos P. Predlozhenija po primeneniju besprovodnyh sensornyh setej v voennoj otrasli // Izvestija Vysshej voennoj shkoly General'nogo shtaba Vooruzhennyh sil Respubliki Angola. 2025. № 1. S. 34–38.
8. Boljubash O. O. Algoritm sbora, obrabotki i peredachi informacii o sostojanii seti peredachi dannyh / O. O. Boljubash // Informacionnye tehnologii: nauka, tehnika, tehnologija, obrazovanie, zdorov'e. Materialy XI mezhdunarodnoj NPK. – Moskva: NTU «XIII», 2003. S. 45.
9. Livshic B. S. Teorija teletrafika / B. S. Livshic, A. P. Pshenichnikov, A.D. Harkevich – Moskva : Svjaz', 1979. – 224 s.
10. Ivanov V. G., Chelahov D. M., Kuzin P. I., Manuel André C. Edinoe informacionnoe prostranstvo kak tehničeskaja osnova sistemy upravleniya podrazdelenijami. Izvestija Vysshej voennoj shkoly General'nogo shtaba Vooruzhennyh sil Respubliki Angola. 2025. № 1. S. 43–47.
11. Lipatnikov V., Belov A., Kuzin P., Rabin A. Determination of linear spectral frequencies. V sbornike: AIP Conference Proceedings. Melville, New York, United States of America, 2021. S. 30046.



# АНАЛИЗ СУЩЕСТВУЮЩИХ ГЕОИНФОРМАЦИОННЫХ СИСТЕМ, ИСПОЛЬЗУЕМЫХ В МЧС РОССИИ И ОЦЕНКА ИХ ФУНКЦИОНАЛЬНЫХ ОГРАНИЧЕНИЙ

Курбанов С. Н.<sup>1</sup>, Безвесильная А. А.<sup>2</sup>, Григорьян А. А.<sup>3</sup>

DOI:10.21681/3034-4050-2026-1-59-71

**Ключевые слова:** чрезвычайные ситуации, пространственный анализ, поддержка принятия решений, оперативное управление, мониторинг опасностей, прогнозирование рисков, спасательные подразделения.

## Аннотация

**Цель:** анализ практики применения геоинформационных систем в деятельности МЧС России при предупреждении и ликвидации чрезвычайных ситуаций, а также выявление функциональных ограничений существующих решений в контексте управления силами и средствами.

**Метод исследования:** использовались методы системного анализа, сравнительного анализа и обобщения практического опыта применения геоинформационных систем в органах управления МЧС России. Дополнительно применялся метод структурно-функционального анализа для оценки роли геоинформационных технологий в системе поддержки принятия решений при чрезвычайных ситуациях.

**Результат:** проанализированы нормативные документы, материалы научных публикаций, а также данные, отражающие использование геоинформационных систем на федеральном, региональном и территориальном уровнях управления. Рассмотрены решения, включая «Атлас опасностей и рисков», систему «Термические точки», QGIS и «Аксиома ГИС», которые позволяют эффективно решать задачи выявления опасных зон, прогнозирования развития неблагоприятных процессов, оценки потенциального ущерба и информационного обеспечения органов управления. Вместе с тем выявлено, что существующие геоинформационные системы ориентированы преимущественно на аналитические и мониторинговые функции и не обеспечивают в полной мере автоматизированного планирования и координации перемещения сил и средств при масштабных чрезвычайных ситуациях. Показано, что отсутствие единой специализированной геоинформационной платформы, интегрирующей логистику, анализ транспортной доступности и управление группировками, снижает эффективность реагирования в условиях динамично меняющейся обстановки. Полученные результаты могут быть использованы при разработке перспективных информационных решений для повышения устойчивости системы управления РСЧС.

**Практическая ценность** работы заключается в комплексном анализе применения геоинформационных систем в деятельности МЧС России с позиций управления силами и средствами и выявления их функциональных ограничений при ликвидации крупномасштабных чрезвычайных ситуаций.

## Введение

Геоинформационные системы занимают ключевое место в современной практике предупреждения и ликвидации чрезвычайных ситуаций. Для МЧС России они становятся одним из базовых инструментов, позволяющих интегрировать данные различной природы, проводить пространственный анализ, визуализировать оперативную обстановку и поддерживать принятие решений. В условиях

чрезвычайных ситуаций, особенно характеризующихся большой протяжённостью зоны поражения и необходимостью быстрого перераспределения сил, возможности ГИС приобретают особое значение. Геоинформационные системы являются незаменимым инструментом для органов управления всех уровней, от муниципального до федерального.

Одной из первостепенных задач ГИС в МЧС России является получение и отображение

1 Курбанов Султан Нариманович, преподаватель кафедры информационных систем и технологий инженерного факультета Академии гражданской защиты МЧС России имени генерал-лейтенанта Д. И. Михайлика», г. Химки, Россия. E-mail: s.kurbanov@agz.50.mchs.gov.ru

2 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», г. Химки, Россия. E-mail: a.bezvesilnaia@agz.50.mchs.gov.ru

3 Григорьян Альмита Артуровна, научный сотрудник научно-исследовательского отдела научно-исследовательского центра Академии гражданской защиты МЧС России имени генерал-лейтенанта Д. И. Михайлика», г. Химки, Россия. E-mail: a.grigoryan@agz.50.mchs.gov.ru

оперативной информации о чрезвычайной ситуации. В едином пространстве отображаются данные о её месте возникновения, масштабах распространения, интенсивности воздействия опасных факторов, количестве затронутых населённых пунктов и состоянии критически важных объектов. Такая визуализация значительно сокращает время, необходимое для первичного анализа обстановки, и обеспечивает единое понимание ситуации всеми участниками межведомственного взаимодействия.

Не менее важной задачей является формирование и оптимизация маршрутов движения сил и средств. При наводнениях, лесных пожарах, авариях на химически опасных объектах или в условиях разрушенной инфраструктуры требуется быстро определить наиболее безопасные и доступные направления для переброски спецтехники, гуманитарных грузов или эвакуации населения.

Задачи прогнозирования являются одной из центральных функций ГИС. Моделирование развития чрезвычайной ситуации – нарастания уровня воды, распространения огня, перемещения облака химического загрязнения или динамики разрушений, это позволяет принимать решения заблаговременно. Пространственно-временные модели дают возможность определить участки, которые могут оказаться под воздействием опасных факторов в ближайшие часы или сутки, оценить необходимое время эвакуации и определить наиболее уязвимые элементы инфраструктуры. Данный подход позволяет перейти от реагирования по факту к упреждающим действиям.

Особый блок задач ГИС связан с оценкой ущерба. После прохождения опасной фазы чрезвычайной ситуации требуется определение площади затоплений, количества разрушенных объектов, повреждений транспортных сетей, сельскохозяйственных угодий и коммунальной инфраструктуры. ГИС позволяют быстро провести пространственный анализ разрушений, сопоставить данные с кадастровой и социально-экономической информацией и сформировать объективную оценку материального ущерба. Это важно как для организации восстановительных мероприятий, так и для подготовки документов, необходимых для выделения федеральной помощи.

Геоинформационные системы обеспечивают возможность комплексного анализа территорий, где сохраняется риск повторного

возникновения чрезвычайных ситуаций. На основе исторических данных, статистики происшествий, динамики климатических изменений и состояния инфраструктуры составляются карты опасностей и рисков, которые позволяют выявить наиболее уязвимые районы. Таким образом, ГИС становятся инструментом стратегического планирования, позволяющим формировать программы модернизации гидротехнических сооружений, укрепления береговых линий, обеспечения пожарной безопасности и повышения устойчивости территорий [8; 9].

В совокупности все эти задачи делают ГИС одним из наиболее значимых инструментов поддержки управленческих решений в деятельности МЧС России. Они обеспечивают высокий уровень информированности, точность прогнозов, обоснованность распределения сил и возможность оперативной адаптации к изменяющейся обстановке. В условиях роста масштабов и сложности современных чрезвычайных ситуаций необходимость дальнейшего развития и интеграции ГИС в деятельность МЧС становится очевидной.

В настоящее время в деятельности МЧС России внедряется широкий спектр геоинформационных систем (ГИС), среди которых наиболее известны такие программно-аналитические комплексы, как «Атлас опасностей и рисков»<sup>4</sup>, системы мониторинга термических аномалий «Термоточки»<sup>5</sup>, а также свободное ГИС-приложение QGIS<sup>6</sup>, используемое территориальными органами, подразделениями управления рисками и образовательными учреждениями. Дополнительно развивается модульная среда «Аксиома ГИС», которую рассматривают как перспективную отечественную платформу для пространственного анализа, отображения оперативной обстановки и моделирования опасных природных процессов (рис. 1).

Несмотря на многообразие систем, используемых на различных уровнях, их функционал во многом сосредоточен вокруг задач мониторинга, картографирования и информационного обеспечения. Такие системы позволяют отображать границы зон чрезвычайных ситуаций, прогнозировать воздействие опасных факторов, анализировать климатические

4 Атлас опасностей и рисков [Электронный ресурс]. – Режим доступа: <https://atlas.mchs.gov.ru/> (дата обращения: 10.12.2025).

5 Термические точки [Электронный ресурс]. – Режим доступа: <https://firenotification.mchs.gov.ru/user/login> (дата обращения: 10.12.2025).

6 QGIS [Электронный ресурс]. – Режим доступа: <https://qgis.org/> (дата обращения: 12.12.2025).



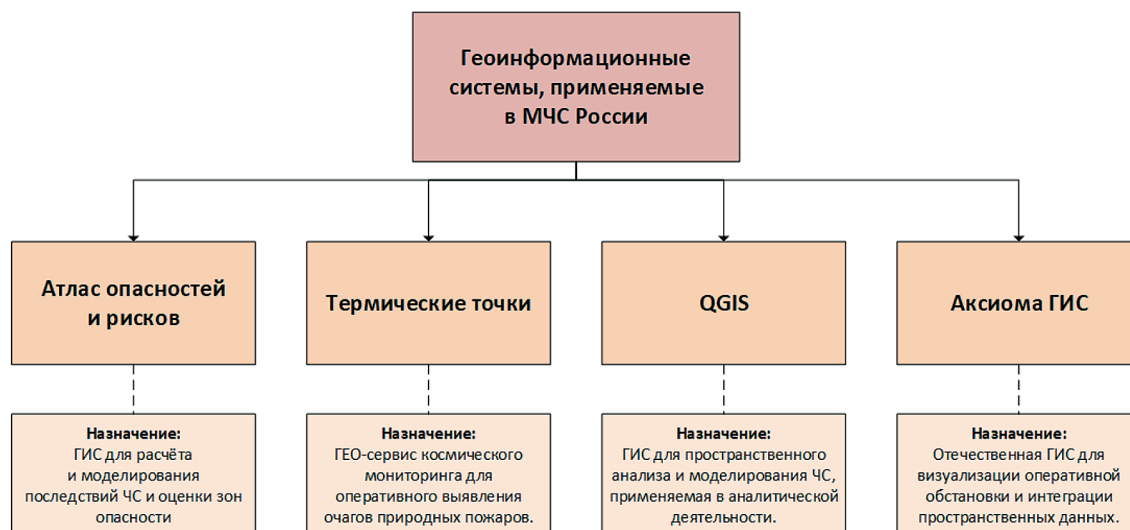


Рис. 1. Геоинформационные системы, применяемые в МЧС России

и гидрологические параметры, оценивать потенциальные риски, формировать тематические карты и проводить аналитическую обработку данных. Однако большинство указанных решений не обладают инструментами оперативного управления значительными группировками сил и средств, поскольку они не предназначены для расчёта логистики, моделирования перемещения техники и формирования оптимальных маршрутов в условиях динамично изменяющейся обстановки.

Отдельного внимания заслуживает опыт города Москвы, где создана и эффективно функционирует Комплексная информационная система мониторинга и управления силами и средствами (КИС УСС) [5]. Эта система интегрирует данные различных ведомств, обеспечивает автоматическую регистрацию сообщений о происшествиях, формирует карточки вызовов, осуществляет автоматизированную высылку подразделений в соответствии с расписанием выездов, отслеживает движение техники на основе данных ГЛОНАСС и позволяет контролировать весь цикл реагирования – от момента поступления сигнала до завершения работ. КИС УСС демонстрирует, что интеграция картографической основы, средств мониторинга, навигации, маршрутизации и информационного обмена между службами способна существенно повысить скорость и качество реагирования в условиях высоко урбанизированной территории.

Однако важно отметить, что, несмотря на высокую технологическую зрелость КИС УСС, её применение ограничено территорией города

Москвы и нормативно ориентировано на задачи локального уровня. Система не предназначена для управления крупными межрегиональными группировками, перемещающимися на сотни километров, не интегрирована в общероссийские процессы оперативного планирования, а её архитектура не рассчитана на координацию действий десятков главных управлений, как это требуется при чрезвычайных ситуациях федерального масштаба.

Проанализируем используемые в МЧС России геоинформационные системы более подробно.

### Атлас опасностей и рисков

Одним из наиболее функциональных и востребованных геоинформационных решений, используемых в МЧС России, является комплекс «Атлас опасностей и рисков» (рис. 2).

Данная система представляет собой специализированную ГИС-платформу, ориентированную на анализ воздействия опасных природных и техногенных процессов, моделирование сценариев развития чрезвычайных ситуаций и оценку возможных последствий для населения и территорий. Атлас используется на федеральном, региональном и муниципальном уровнях как инструмент поддержки принятия решений в области предупреждения и управления рисками.

Ключевым преимуществом Атласа является наличие широкого набора расчётных модулей, позволяющих моделировать широкий спектр сценариев. Система позволяет проводить анализ подъёма уровня воды по цифровым

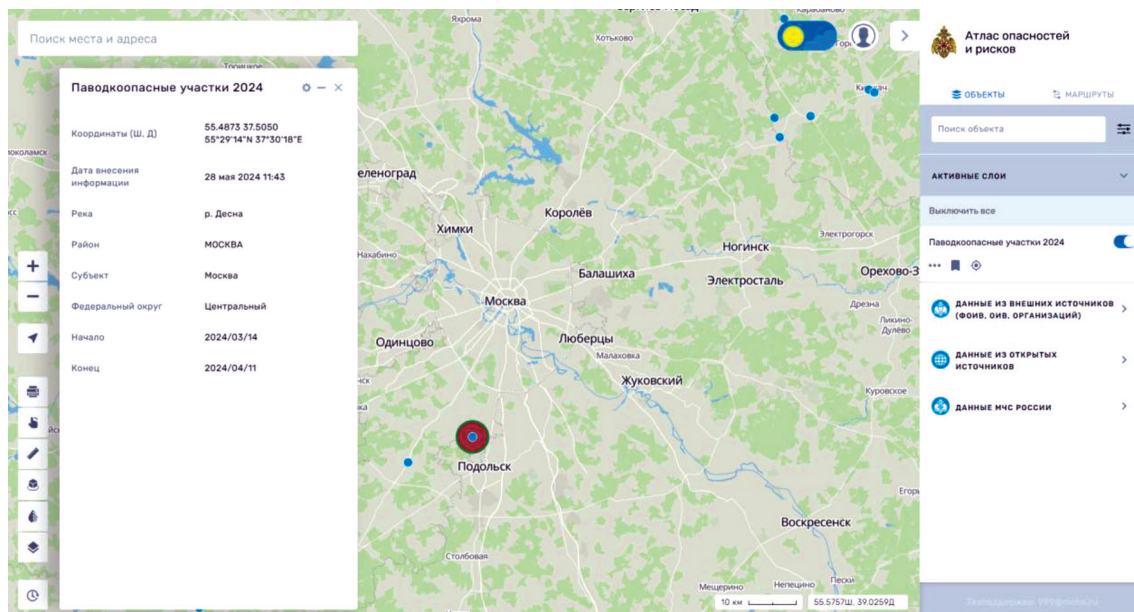


Рис. 2. Интерфейс «Атласа опасностей и рисков»

моделям рельефа, рассматривать развитие низового лесного пожара, моделировать параметры радиационной аварии, оценивать последствия землетрясений различной интенсивности и прогнозировать высоту волны цунами при сейсмических возмущениях. Дополнительно в системе предусмотрены инструменты для расчёта теплотехнических процессов, таких как охлаждение помещений при отключении отопления, что важно для регионов с суровым климатом.

Особое место занимают модули, ориентированные на анализ химически опасных ситуаций.

Атлас позволяет оценивать распространение продуктов аварийного выброса АХОВ, формировать карты зон химического заражения и учитывать параметры рельефа и метеоусловий. В контексте техногенных рисков используются модели обрушения зданий, развития пожаров разного типа – проливов, вспышек, факельного горения, огненного шара, а также расчёты параметров взрывов газопаровых смесей, ёмкостей с горючими сжиженными газами, твёрдых взрывчатых веществ. Таким образом, система обеспечивает многоуровневый анализ воздействия чрезвычайной

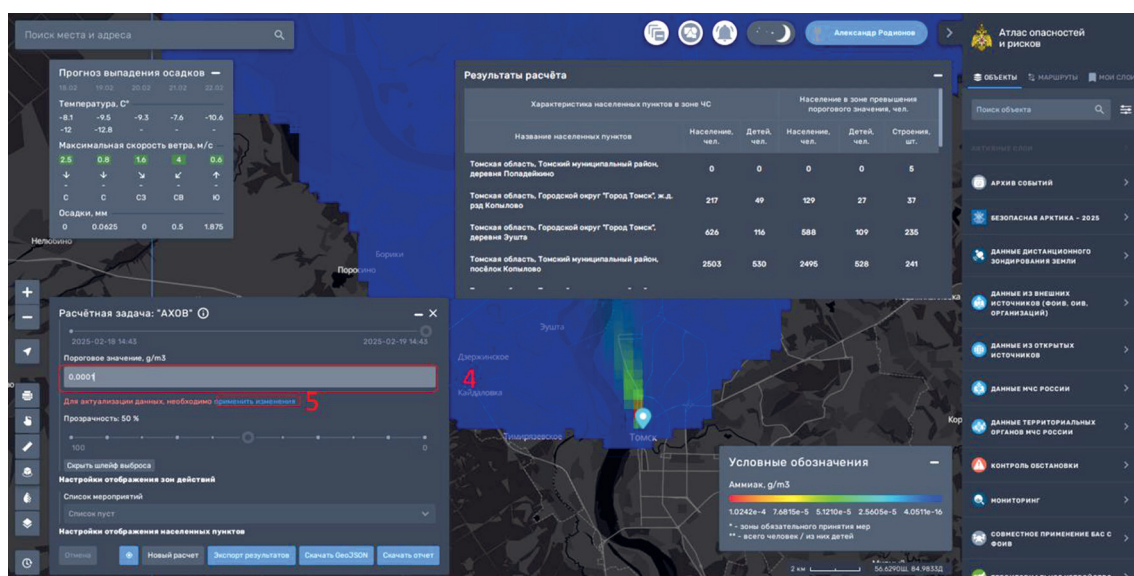


Рис. 3. Модуль расчета распространения продуктов АХОВ в «Атласе опасностей и рисков»

ситуации и позволяет органам управления заранее оценивать масштабы возможных последствий.

В дополнение к моделированию опасностей Атлас включает функции мониторинга отдельных категорий объектов. На его карте отображаются данные о дорожной ситуации – пробках, ДТП, состоянии дорожной сети, а также сведения о железнодорожном движении, включая гражданские, ремонтные и специализированные пожарные поезда. В системе предусмотрены возможности наблюдения за передвижением отдельных единиц техники, подключённых к навигационным датчикам, что обеспечивает актуальную картину пространственного распределения транспортных ресурсов на территории субъекта.

Однако, несмотря на развитый аналитический функционал и наличие отдельных элементов мониторинга, «Атлас опасностей и рисков» остаётся инструментом преимущественно прогнозно-аналитического характера. Его основная задача заключается не в управлении группировками сил и средств, а в моделировании опасных процессов и предоставлении руководителям органов управления научно обоснованной информации о возможных масштабах чрезвычайной ситуации. Система не выполняет функцию маршрутизации, не анализирует пропускную способность транспортных сетей в условиях ЧС и не формирует оптимальные варианты перемещения техники. Она также не предназначена для

автоматизированного распределения ресурсов, координации подразделений или оценки логистики при работе межрегиональных группировок.

Атлас опасностей и рисков представляет собой мощный инструмент моделирования, мониторинга и анализа чрезвычайных ситуаций, но при этом не является системой оперативного управления или логистического планирования.

### Термические точки

Система выявления и обработки термических аномалий «Термические точки» является одним из ключевых инструментов МЧС России в области космического мониторинга природных пожаров и иных тепловых проявлений на местности. Она представляет собой специализированный программно-аппаратный комплекс, основанный на данных дистанционного зондирования Земли, позволяющий в режиме, близком к реальному времени, фиксировать тепловые аномалии и оперативно доводить информацию о них до подразделений РСЧС (рис. 4).

Основой работы системы является интерпретация спутниковых снимков высокой частоты обновления. В результате автоматизированной тематической обработки формируется слой термических точек – участков поверхности Земли, на которых зарегистрировано тепловое излучение, превышающее естественный фон. Термическая точка не обя-

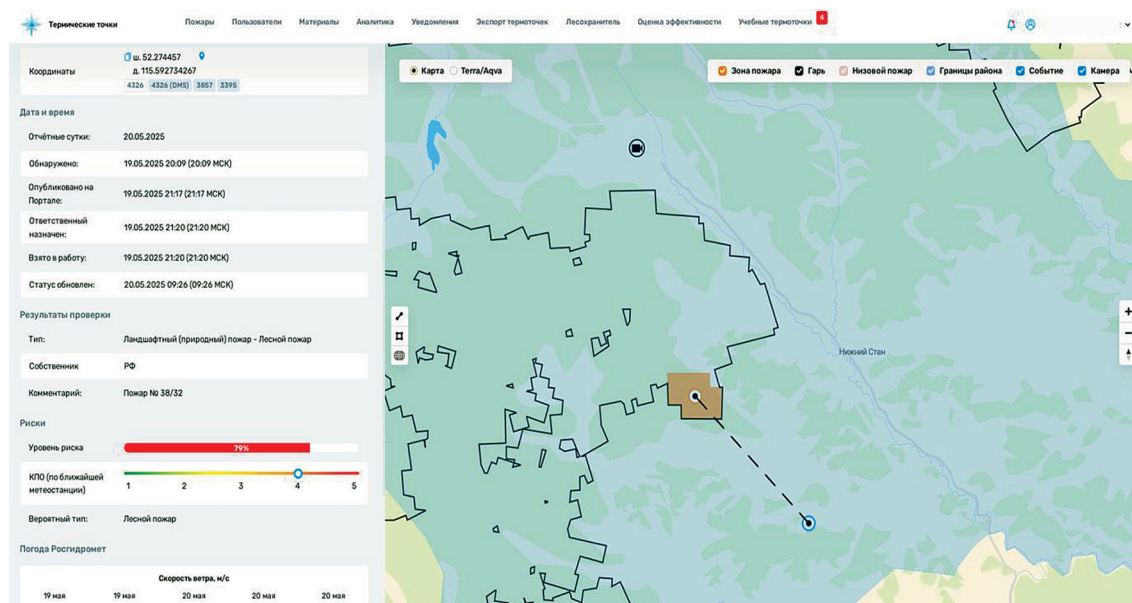


Рис. 4. Интерфейс «Термические точки»



зательно означает лесной пожар: к ней могут относиться горение мусора, пал сухой травы, техногенный нагрев, тепловые выбросы промышленных объектов или признаки развивающегося пожара в природной среде. Такой подход обеспечивает высокую чувствительность мониторинга и позволяет фиксировать возгорания на ранних стадиях.

Отдельного внимания заслуживает архитектура и принципы функционирования системы «Термические точки», которые делают её одним из самых технологических решений МЧС России в сфере дистанционного мониторинга. Система опирается на автоматизированный процесс обработки спутниковых данных, включающий несколько последовательных этапов: первичную радиометрическую коррекцию изображений, тематическую фильтрацию тепловых характеристик и геопривязку выявленных аномалий к цифровой карте местности. Такой подход исключает влияние погодных условий, времени суток и локальных особенностей рельефа, обеспечивая высокую степень достоверности получаемой информации.

Характерной особенностью системы является использование данных сразу нескольких спутниковых платформ с различным пространственным и спектральным разрешением. Это позволяет компенсировать ограничения, присущие отдельным типам сенсоров: спутники с высоким разрешением дополняют

информацию точными координатами очагов, а спутники с большим покрытием обеспечивают широкий охват территории и позволяют обнаруживать возгорания на ранней стадии. Благодаря многим источникам информации возрастает стабильность мониторинга, а вероятность пропуска термической аномалии существенно снижается.

Система также предусматривает многократное обновление данных. Обработка спутниковой информации каждые несколько часов обеспечивает почти непрерывный мониторинг пожароопасной обстановки. Это особенно важно в условиях стремительного распространения низовых и верховых лесных пожаров, когда задержка даже в 1–2 часа может привести к крупномасштабным последствиям. Оперативность обновления данных делает систему востребованной для ежедневной работы ЦУКС, ЕДДС, лесных служб и органов местного самоуправления.

В целях сокращения времени реагирования МЧС России разработало мобильное приложение «Термические точки», доступное должностным лицам всех уровней, от НЦУКС и руководства МЧС до ЕДДС, глав муниципальных образований и сотрудников пожарно-спасательных подразделений (рис. 5).

Приложение синхронизируется с системой космического мониторинга и получает обновления до четырёх раз в сутки, обеспечивая актуальным слоем термических аномалий

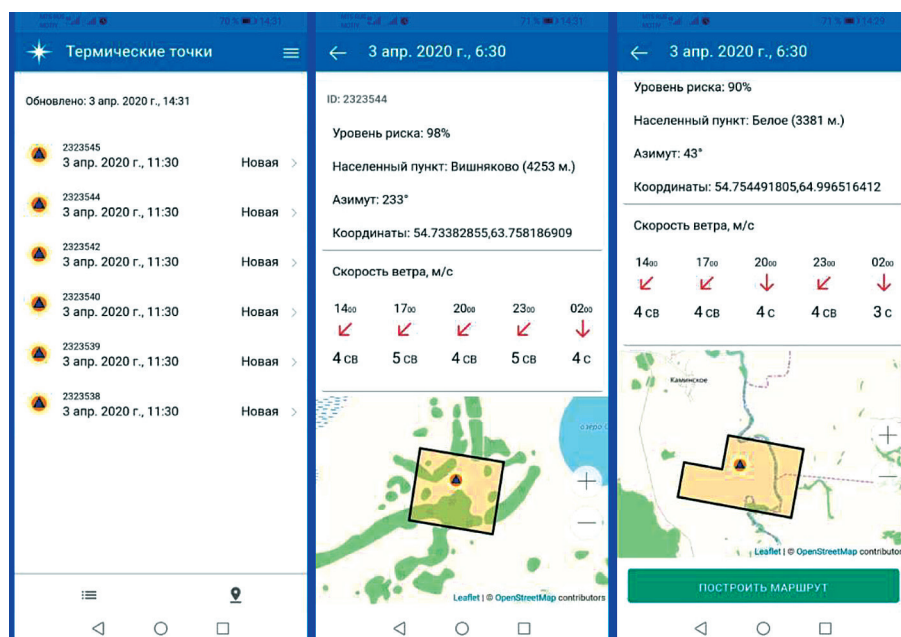


Рис. 5. Интерфейс мобильной версии «Термические точки»



территориальные органы управления. Благодаря этому информация о потенциальных очагах возгорания доводится до подразделений значительно быстрее, чем при использовании традиционных схем уведомления.

Особое значение система имеет в пожароопасный период. По данным региональных ЦУКС, только в Вологодской области посредством космического мониторинга в 2020 году было выявлено более 70 термоточек, а в 2021 году – 32, из которых значительная часть относилась к неконтролируемому горению сухой растительности и мусора. После получения данных о термической точке назначенные должностные лица обязаны провести проверку: выезд оперативных групп позволяет подтвердить характер аномалии и определить необходимость привлечения дополнительных сил.

Система позволяет не только отображать термические точки на карте, но и обеспечивать двустороннее взаимодействие. Пользователи могут самостоятельно направлять сообщения о замеченных возгораниях, прикладывать фото- и видеоматериалы и передавать информацию в ЕДДС, что делает приложение инструментом общественного мониторинга. Приложение поддерживает различные роли пользователей, что обеспечивает разграничение доступа и организацию контролируемой передачи данных через ведомственные сети.

Внедрение системы позволило существенно повысить оперативность и точность реагирования на природные пожары. По результатам внедрения точность определения термических аномалий достигла 92,5 %, а время доведения информации до подразделений сократилось в три раза. Это стало возможно благодаря регулярной, круглосуточной обработке спутниковых снимков и автоматизации процессов уведомления. Непрерывность наблюдений, высокая чувствительность спутниковых сенсоров и оперативная передача данных обеспечивают эффективное раннее обнаружение пожаров, что способствует снижению ущерба и предотвращению перехода огня на населённые пункты и объекты экономики.

Несмотря на высокую эффективность в сфере мониторинга природных пожаров, система «Термические точки» имеет специализированный характер и не предназначена для решения задач оперативного управления группировками сил и средств. Она не

выполняет функций маршрутизации пожарной техники, не осуществляет логистическое моделирование, не учитывает транспортную доступность и не предназначена для координации действий межрегиональных подразделений при крупных чрезвычайных ситуациях. Её функционал ограничивается ранним обнаружением термических аномалий, передачей данных и поддержкой принятия решений по первичному реагированию.

Таким образом, «Термические точки» представляют собой высокотехнологичный инструмент оперативного космического мониторинга, но, как и другие используемые в МЧС специализированные ГИС-решения, не обеспечивают управление силами и средствами в масштабах крупных межрегиональных чрезвычайных ситуаций.

### Quantum Geographic Information System

QGIS (Quantum Geographic Information System) занимает важное место среди инструментов, которые применяются в структурах МЧС России для анализа, мониторинга и прогнозирования опасных природных явлений (рис. 6).

В отличие от специализированных ведомственных комплексов, QGIS представляет собой универсальную платформу с открытым исходным кодом, что делает её доступной, гибкой и легко интегрируемой в существующие рабочие процессы территориальных органов МЧС. Программа используется как в учебных целях, так и при выполнении практических задач, связанных с обработкой пространственных данных, моделированием сценариев развития пожаров, паводков и других ЧС.

Одним из ключевых направлений внедрения QGIS является анализ и прогнозирование природных пожаров. Лесные и ландшафтные пожары остаются одной из наиболее актуальных угроз, оказывающих серьёзное влияние на экосистемы, качество воздуха, экономику регионов и безопасность населения. В условиях роста частоты пожаров, вызванного климатическими изменениями и антропогенным воздействием, использование ГИС-подходов становится не просто желательным, а обязательным для точного прогнозирования и оперативного реагирования.

QGIS позволяет объединять разнородные данные – спутниковые снимки, цифровые модели рельефа, данные о растительности, почвенном покрове, метеорологические показатели,

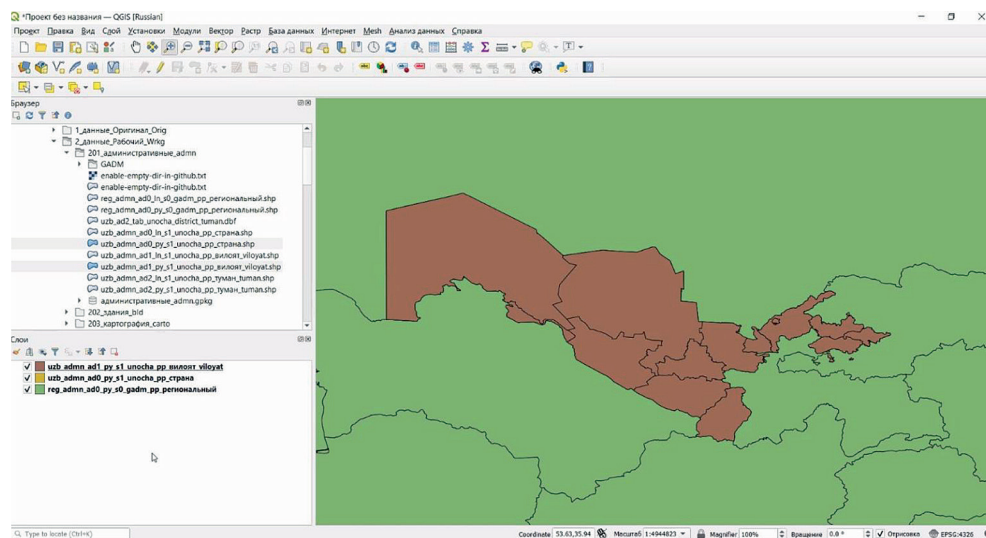


Рис. 6. Интерфейс программы «QGIS»

историческую информацию о прошлых пожарах. Такой интеграционный подход обеспечивает комплексное понимание пожарной опасности на территории и создаёт основу для построения прогнозных моделей.

Использование QGIS в работе МЧС строится на последовательной методологии, включающей несколько этапов. На первом этапе осуществляется сбор исходных данных: геопространственных слоёв рельефа, вегетации, гидрографии, почвенно-климатических характеристик, а также сведений о температуре, влажности, скорости ветра и других параметрах, влияющих на вероятность возгорания. Значимую роль играют исторические данные, отражающие динамику предыдущих пожаров, их причины, масштабы и последствия.

Обработка данных в QGIS включает их корректировку, преобразование форматов, формирование отдельных слоёв и их визуализацию. Далее производится комплексный пространственный анализ: выделяются участки повышенного риска, создаются карты пожарной опасности по показателям рельефа и типам растительности, выполняется классификация территорий по вероятности возникновения пожаров. Важным преимуществом QGIS является возможность использования автоматизированных инструментов и геообработки, что позволяет выполнять многокритериальные оценки в сжатые сроки.

Следующий этап – построение прогнозных моделей. В зависимости от сложности задачи могут применяться статистические

методы, алгоритмы машинного обучения или комбинированные подходы. QGIS поддерживает интеграцию с внешними библиотеками Python, что открывает возможности для использования современных методов прогнозирования. Модели проходят обязательную валидацию – результаты сравниваются с фактическими данными, оценивается точность прогноза, корректируются критерии и параметры.

На основании полученных данных формируются практические рекомендации: определяются зоны повышенного внимания, разрабатываются меры по предотвращению пожаров, выбираются приоритетные направления патрулирования, усиливается контроль за наиболее уязвимыми территориями. Картографические материалы, созданные в QGIS, используются для планирования мероприятий по тушению пожаров, организации взаимодействия между подразделениями, а также для информационной поддержки руководящего состава.

Использование QGIS в деятельности МЧС не ограничивается только пожарами. Система активно применяется при моделировании паводков, анализе последствий сильных осадков, прогнозировании зон возможных затоплений, оценке устойчивости территорий, мониторинге изменений рельефа, расчёте рисков для критически важных объектов. Возможность интегрировать QGIS с дистанционным зондированием Земли, метеорологическими сервисами и внешними базами

данных делает её универсальным инструментом, способным расширять функционал по мере необходимости.

Несмотря на широкие возможности QGIS и её значительный вклад в повышение качества анализа природных и техногенных рисков, важно учитывать, что данная система изначально создавалась как универсальная платформа для обработки пространственных данных, а не как специализированный инструмент для оперативного управления силами и средствами. Это определяет её функциональные ограничения, особенно заметные в контексте задач МЧС России, связанных с логистикой, маршрутизацией спецтехники и моделированием перемещений крупномасштабных группировок.

QGIS позволяет визуализировать дорожную сеть, рассматривать состояние инфраструктуры, загружать данные о закрытых участках дорог или зонах ограничения движения, однако инструменты оперативного управления транспортом, автоматической маршрутизации спецтехники в реальном времени, формирования колонн или контроля отклонений от маршрутов в ней отсутствуют. Она не поддерживает работу с телеметрией, не интегрирована с системами мониторинга транспорта (ГЛОНАСС/ЭРА-ГЛОНАСС), не способна рассчитывать схемы переброски сил в условиях динамически меняющейся обстановки, что является критически важным для реагирования на крупные чрезвычайные ситуации.

Таким образом, QGIS может служить эффективным средством анализа территории,

оценки рисков и формирования прогнозных карт, но остаётся недостаточно приспособленной для решения задач тактического и оперативного управления. Отсутствие встроенных инструментов по моделированию перемещения подразделений, автоматизированному планированию маршрутов и координации действий в реальном времени объясняет, почему эта система применяется преимущественно для аналитических задач, а не как основа для управления большой группировкой сил РСЧС. В отличие от неё, специализированные ведомственные решения, такие как КИС УСС или системные комплексы НЦУКС, ориентированы на интеграцию с диспетчерскими службами, мониторинг транспорта и поддержку принятия решений при переброске сил.

### Геоинформационная система «Аксиома ГИС»

Геоинформационная система «Аксиома» является одним из отечественных программных продуктов, постепенно внедряемых в деятельность подразделений МЧС России (рис. 7).

Она создавалась как универсальный инструмент пространственного анализа, ориентированный на работу государственных структур, которым требуются российские программные решения, не зависящие от зарубежных платформ. В последние годы «Аксиома» активно позиционируется как перспектива постепенной импортозаметы существующих ГИС и как платформа, способная обеспечить интеграцию с системами мониторинга, аналитическими комплексами и ведомственными базами данных.

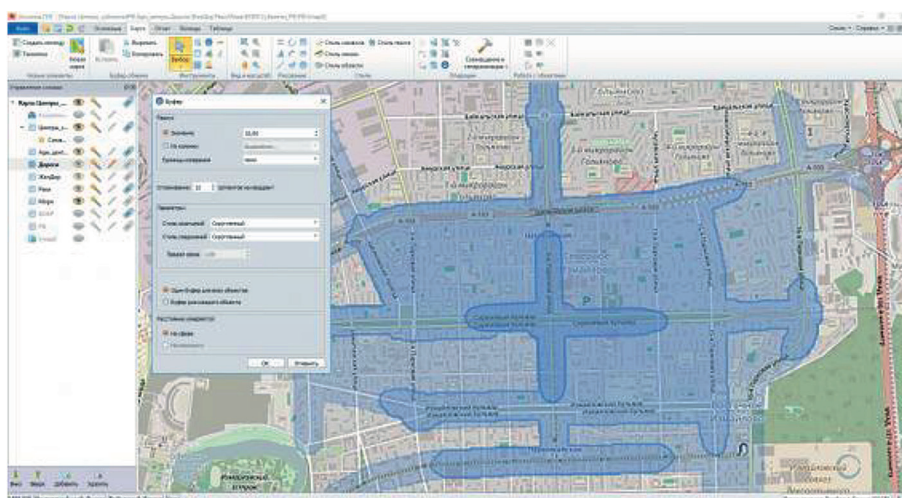


Рис. 7. Интерфейс «Аксиома ГИС»

Одним из ключевых преимуществ «Аксиомы» является её отечественное происхождение, что обеспечивает устойчивость к санкционным ограничениям, возможность адаптации исходного кода под ведомственные нужды и интеграцию с существующими государственными информационными системами. Именно по этой причине система получила распространение в ряде территориальных органов МЧС и используется, в том числе, в НЦУКС для отображения оперативной обстановки. Внутри Национального центра ГИС «Аксиома» применяется как вспомогательная картографическая платформа, позволяющая быстро визуализировать данные, поступающие из других источников, включая QGIS, специализированные ГИС и собственные аналитические модули МЧС России.

Функционал «Аксиомы» охватывает стандартные задачи базового геоинформационного анализа: отображение картографических данных, создание тематических слоёв, просмотр спутниковых снимков, подготовку картосхем, нанесение оперативной информации, а также работу с топографической основой. Система поддерживает обмен геоданными и позволяет загружать материалы различных форматов, что обеспечивает относительную гибкость при взаимодействии с внешними источниками информации. В практической деятельности она используется для картографирования зон чрезвычайных ситуаций, формирования схем подтоплений и анализа рельефа.

Однако по своим аналитическим возможностям «Аксиома» заметно уступает как QGIS, так и специализированным комплексам, например, «Атласу опасностей и рисков». В системе ограничен набор инструментов пространственного анализа, отсутствуют развитые модули моделирования сценариев развития чрезвычайных ситуаций, нет встроенных алгоритмов прогнозирования опасных процессов или расчётов поражающих факторов.

Кроме того, функционал по работе с большими массивами данных реализован в более упрощённом виде, что снижает удобство использования при сложных аналитических задачах, связанных с учётом множества параметров территории.

Особенно заметными становятся ограничения «Аксиомы» в области задач, связанных с оперативным управлением и планированием

перемещения сил и средств. В отличие от специализированных систем мониторинга транспорта или тех же платформ, которые применяются в структуре КИС УСС Москвы, «Аксиома» не обладает встроенными инструментами автоматической маршрутизации, моделирования колонн, расчёта доступности территорий, анализа транспортной сети в условиях разрушенной инфраструктуры или оперативного контроля за перемещением подразделений. Она не интегрирована с системами ГЛОНАСС в режиме реального времени и не предназначена для тактического управления крупной группировкой сил РСЧС.

При этом система развивается, расширяется перечень картографических слоёв, улучшаются средства визуализации, появляются модули для работы с ведомственными базами, усиливается интеграция с платформами мониторинга и аналитическими инструментами МЧС. Перспективы её использования во многом связаны с переходом государственной системы управления на отечественные программные решения и стремлением сформировать единый технологический контур обработки геоданных. Несмотря на существующие ограничения, «Аксиома» выполняет важную роль в качестве платформы, обеспечивающей картографическое сопровождение оперативной информации и позволяющей осуществлять визуализацию данных в ведомственной среде.

ГИС «Аксиома» относится к числу перспективных отечественных решений, способных обеспечить выполнение базовых задач картографирования и визуализации обстановки. Однако её текущие функциональные возможности остаются ограниченными в контексте задач оперативного управления, прогнозирования ЧС и особенно – моделирования перемещения сил и средств. Это подчёркивает необходимость её дальнейшего развития и интеграции со специализированными подсистемами, а также обосновывает потребность в создании нового ГИС-модуля, нацеленного именно на решение задач логистики и распределения ресурсов в условиях крупных чрезвычайных ситуаций.

### Выводы

Проведённый анализ существующих геоинформационных систем, используемых в МЧС России, демонстрирует выраженную фрагментарность применяемых систем и отсутствие



единой интегрированной платформы, способной охватить весь спектр задач, возникающих при ликвидации чрезвычайных ситуаций. Отдельные ГИС – такие как «Атлас опасностей и рисков», QGIS, «Экстремум», система «Термоточки», специализированные комплексы мониторинга транспорта и отечественная ГИС «Аксиома» – успешно решают локальные задачи: мониторинг, прогнозирование, визуализацию оперативной обстановки, анализ рисков, обработку космических данных, оценку поражающих факторов или формирование отчётности.

Однако ни одна из существующих систем не обеспечивает полноценную поддержку стратегического и оперативного управления крупной группировкой сил и средств. Они не способны автоматически моделировать перемещение подразделений, рассчитывать маршруты с учётом разрушенной инфраструктуры, анализировать транспортную доступность, формировать логистические схемы переброски техники, определять потребность в ресурсах с учётом динамики ЧС или проводить сценарный анализ вариантов развёртывания группировки.

Отдельные элементы такой функциональности присутствуют в различных платформах, но не объединены в единую систему, работающую в реальном времени и способную поддерживать принятие решений на региональном и федеральном уровнях. На примере паводка на Дальнем Востоке в 2013 году видно, что управление десятками тысяч спасателей, тысячами единиц техники, авиацией

и плавсредствами велось в условиях крайне изменчивой обстановки. Задачи по переброске сил выполнялись вручную, опираясь на опыт оперативных дежурных, разрозненные данные, телефонные доклады и картографические материалы, не связанные в единую вычислительную среду.

Тем самым проявляется ключевой системный разрыв: ведомство располагает богатым набором инструментов мониторинга и оценки обстановки, но не имеет специализированной ГИС, ориентированной на логистику сил РСЧС, моделирование их перемещения и планирование действий при масштабных чрезвычайных ситуациях. Это создаёт методологический и технологический вакуум, который особенно заметен при ЧС федерального уровня, где требуется согласованная работа нескольких субъектов Федерации, десятков ведомств и тысяч подразделений.

В совокупности выявленные ограничения подтверждают актуальность разработки специализированного программного решения, способного объединить картографическую основу, аналитические модели и инструменты логистического планирования в рамках единой платформы. Такая система должна обеспечивать оперативное моделирование перемещения сил и средств, прогнозировать изменения доступности территорий и поддерживать выработку решений в реальном времени, что позволит перейти от классической реактивной схемы управления к проактивной, основанной на точных расчётах и пространственном анализе.

### Литература

1. Арефьева Е. В. Защита в чрезвычайных ситуациях МЧС России // Баринов А. В., Бобарико А. В. Ермаков С. И., Панченков В. В., Полевой В. Г., Ткаченко П. Н., Треушков И. В., Юхин А. Н. / Издание 2-е, переработанное. – М.: АГЗ МЧС России, 2018. – 400 с.
2. Бабенышев, С. В. Информационные технологии поддержки принятия решений в чрезвычайных ситуациях: учебное пособие / С. В. Бабенышев, Е. Н. Матеров. – Железногорск: ФГБОУ ВО Сибирская пожарно-спасательная академия ГПС МЧС России, 2024. – 145 с.
3. Блиновская Я. Ю. Введение в геоинформационные системы: учебное пособие / Я. Ю. Блиновская, Д. С. Задоя. – Второе издание. – Москва: ФОРУМ: ИНФРА-М, 2023. – 112 с.
4. Гасимова Р. В., Рязанцева Л. Т. Информационные технологии в управлении безопасностью жизнедеятельности. – Воронеж: ВГТУ, 2018.
5. Епишкин Е. В. Комплексная информационная система мониторинга и управления силами и средствами / Е. В. Епишкин // Современные технологии обеспечения гражданской обороны и ликвидации последствий чрезвычайных ситуаций. – Москва, 2019. – С. 102–104.
6. Медеу А. Р., Благовещенский В. П., Карагулов Р. К. «Атлас природных и техногенных опасностей и рисков чрезвычайных ситуаций в Республике Казахстан» // Проблемы чрезвычайных ситуаций. – 2021.

7. Панов Д. В., Кудряшов А. Ю., Спиридонова А. Н., Бочкарева И. И. Использование геопортала открытых данных МЧС России для моделирования чрезвычайных ситуаций // Геодезия и картография. – 2024., С. 103–108.
8. Пашковская О. В., Потапенко И. А. Использование геоинформационных систем для предотвращения чрезвычайных ситуаций // Енисейская Арктика: сборник материалов Всероссийской научно-практической конференции. СибГУ им. М. Ф. Решетнева. Красноярск, 2021., С. 16–18.
9. Карапузиков А. А., Мураев Н. П. Применение инновационных технических средств в условиях затопления территорий // Правовая информатика. 2025, №3. С. 90-95. DOI:10.24412/1994-1404-2025-3-90-95.

## ANALYSIS OF EXISTING GEOGRAPHIC INFORMATION SYSTEMS USED IN THE MINISTRY OF EMERGENCY SITUATIONS OF RUSSIA AND THEIR ASSESSMENT FUNCTIONAL LIMITATIONS

Kurbanov S. N.<sup>1</sup>, Bezvesyla A. A.<sup>2</sup>, Grigoryan A. A.<sup>3</sup>

**Keywords:** emergency situations, spatial analysis, decision support, operational management, hazard monitoring, risk forecasting, rescue units.

### Abstract

**Objective:** to analyze the practice of using geographic information systems in the activities of the Ministry of Emergency Situations of Russia in the prevention and elimination of emergency situations, as well as to identify the functional limitations of existing solutions in the context of managing forces and means.

**Research method:** the methods of system analysis, comparative analysis and generalization of practical experience in the use of geographic information systems in the management bodies of the Ministry of Emergency Situations of Russia were used. In addition, the method of structural and functional analysis was used to assess the role of geoinformation technologies in the decision support system in emergency situations.

**Result:** regulatory documents, materials of scientific publications, as well as data reflecting the use of geographic information systems at the federal, regional and territorial levels of management are analyzed. Solutions, including the «Atlas of Hazards and Risks», the «Thermal Points» system, QGIS and «Axiom GIS», which make it possible to effectively solve the problems of identifying hazardous areas, predicting the development of adverse processes, assessing potential damage and information support of management bodies. At the same time, it is revealed that the existing geographic information systems are focused mainly on analytical and monitoring functions and do not fully provide automated planning and coordination of the movement of forces and means in large-scale emergencies. It is shown that the lack of a single specialized geoinformation platform that integrates logistics, transport accessibility analysis and group management reduces the effectiveness of response in a dynamically changing situation. The results obtained can be used in the development of promising information solutions to improve the stability of the RSChS management system.

**The practical value** of the work lies in a comprehensive analysis of the use of geographic information systems in the activities of the Ministry of Emergency Situations of Russia from the standpoint of managing forces and means and identifying their functional limitations in the elimination of large-scale emergencies.

### References

1. Aref`eva E. V. Zashhita v chrezvy`chajny`x situatsiyax MChS Rossii // Barinov A. V., Bobariko A. V., Ermakov S. I., Panchenkov V. V., Polevoj V. G., Tkachenko P. N., Treushkov I. V., Yuxin A. N. / Izdanie 2-e, pererabotannoe. – M.: AGZ MChS Rossii, 2018. – 400 s.
2. Babeny`shev S. V. Informatsionny`e tekhnologii podderzhki prinyatiya reshenij v chrezvy`chajny`x situatsiyax: uchebnoe posobie / S.V. Babeny`shev, E.N. Materov. – Zheleznogorsk: FGBOU VO Sibirskaya pozharno-spasatel`naya akademiya GPS MChS Rossii, 2024. – 145 s.

1 Sultan N. Kurbanov, Lecturer of the Department of Information Systems and Technologies 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. Mikhailik, Khimki, Russia. E-mail: s.kurbanov@agz.50.mchs.gov.ru

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

3 Almita A. Grigoryan, Researcher of the Research Department of the Research Center of the Academy of Civil Protection of the Ministry of Emergency Situations of Russia named after Lieutenant General D. I. Mikhailik, Khimki, Russia. E-mail: a.grigoryan@agz.50.mchs.gov.ru

3. Blinovskaya Ya. Yu. Vvedenie v geoinformacionny`e sistemy`: uchebnoe posobie / Ya. Yu. Blinovskaya, D. S. Zadoya. – Vtoroe izdanie. – Moskva: FORUM: INFRA-M, 2023. – 112 s.
4. Gasy`mova R. V., Ryazanceva L. T. Informacionny`e texnologii v upravlenii bezopasnost`yu zhiznedeyatel`nosti. – Voronezh: VGTU, 2018.
5. Epishkin E. V. Kompleksnaya informacionnaya sistema monitoringa i upravleniya silami i sredstvami / E. V. Epishkin // Sovremennyy`e texnologii obespecheniya grazhdanskoj oborony` i likvidacii posledstvij chrezvy`chajny`x situacij. – Moskva, 2019. – S. 102–104.
6. Medeu A. R., Blagoveshhenskij V. P., Karagulov R. K. «Atlas prirodny`x i texnogenny`x opasnostej i riskov chrezvy`chajny`x situacij v Respublike Kazaxstan» // Problemy` chrezvy`chajny`x situacij. – 2021.
7. Panov D. V., Kudryashov A. Yu., Spiridonova A. N., Bochkareva I. I. Ispol`zovanie geoportala otkry`ty`x dannyx MChS Rossii dlya modelirovaniya chrezvy`chajny`x situacij // Geodeziya i kartografiya. – 2024., S. 103–108.
8. Pashkovskaya O. V., Potapenko I. A. Ispol`zovanie geoinformacionny`x sistem dlya predotvrashheniya chrezvy`chajny`x situacij // Enisejskaya Arktika: sbornik materialov Vserossijskoj nauchno-prakticheskoy konferencii. SibGU im. M. F. Reshetneva. Krasnoyarsk, 2021., S. 16–18.
9. Karapuzikov A. A., Muraev N. P. Primenenie innovacionny`x texnicheskix sredstv v usloviyax zatopleniya territorij // Pravovaya informatika. 2025, №3. S. 90-95. DOI:10.24412/1994-1404-2025-3-90-95.



# НЕМАТЕМАТИЧЕСКИЕ МЕТОДЫ В КРИПТОГРАФИИ (ЗАЩИЩЕННАЯ СВЯЗЬ НА ОСНОВЕ ОДНОРАНГОВОЙ MESH-СЕТИ)

Черепнёв М. А.<sup>1</sup>

DOI:10.21681/3034-4050-2026-1-72-77

**Ключевые слова:** шифрование, защита информации, одноранговые сети, децентрализованные системы, цифровая подпись, распределение ключей, аутентификация.

## Аннотация

**Цель работы** в анализе слабостей протоколов защиты информации в ТЗУ ВС РФ и разработке предложений по её усовершенствованию.

**Метод исследования** состоит в предложении использовать децентрализованную криптографию.

**Результаты исследования:** предложены некоторые новые методы защиты информации в условиях (временного) отсутствия удостоверяющего центра. Предлагаемые методы не используют трудно решаемые математические задачи (дискретное логарифмирование, факторизация, поиск наименьшего вектора в решетке и пр.). Предлагаются способы, похожие на физическую аутентификацию пользователя, но в цифровом варианте. Современные индивидуальные средства коммуникации позволяют это сделать. Кроме того предлагается использовать величину меш-сети в качестве фактора усиления стойкости связи составляющих её абонентов.

**Научная новизна** состоит в разработке новых протоколов децентрализованной криптографии, позволяющих понизить нагрузку на центральный узел и повысить функциональность и стойкость в работе сети в целом.

## Введение

Для сетей связи тактического звена предложена система защищенной связи на основе одноранговой mesh-сети. В этом случае совокупная цена оборудования становится значительно меньше, а сама сеть надежнее. При этом уничтожение узлов связи одноранговой сети становится неэффективным с точки зрения противника, так как не наносит ущерба работе связи. Кроме того, современные средства военной связи используют спутники связи, количество которых в нашей стране не велико, а кроме того, эти спутники являются уязвимыми для средств поражения противника. Как будет показано дальше, предложенная система способна самостоятельно определять переход абонентов в режим работы под контролем (захват противником).

Важным свойством надежных систем защиты информации является теоретико-информационный характер стойкости. Подобный характер стойкости можно получить и с помощью децентрализованной криптографии. Одна из первых работ на эту тему [3] дала толчок к построению крипто протоколов с совершенно новыми свойствами. Мы будем использовать эти идеи и некоторое их развитие

совместно с более старыми [4] методами защиты информации.

## Решение поставленной задачи

Рассмотрим схему децентрализованного шифрования на основе разделения открытого текста на пороговой схеме с последующей рассылкой разными маршрутами через списки доверия. Проверка совпадения на получателе исключает возможность подделки. Значит чем больше сеть, тем такая схема более стойкая. Она позволяет повысить стойкость до теоретико-информационного уровня. Упрощая пороговую схему до генерации случайных строк и их XOR-а со строкой передаваемого открытого текста, получим новый протокол сетевого шифрования. Поскольку выбор из некоторого набора строк половины этих строк может быть осуществлен перебором экспоненциального объема, то фиксированный такой выбор может быть взят в качестве общего ключа шифрования. При этом открытый текст будет XOR-ом выбранных строк. Конечно, если атакующий может читать весь трафик отправителя или получателя, или узла сети, где возможно собрать все необходимые строки, то дешифровка сводится к экспоненциальному перебору общего ключа шифрования.

<sup>1</sup> Черепнёв Михаил Алексеевич, доктор физико-математических наук, профессор кафедры информационной безопасности факультета ВМК МГУ имени М. В. Ломоносова. г. Москва, Россия. E-mail: cherepniov@gmail.com



Однако, если коммутация в сети устроена так, что траектории пересылки выбранных строк не пересекаются, то для сбора всех таких строк потребуется контроль над частью всех таких траекторий. Если эти траектории выбираются с некоторой долей случайности, то это, фактически, потребует контроля над всей сетью. Однако, чем больше сеть, тем сложнее ее полностью контролировать.

Новыми проблемами в криптографии являются: сетевая работа per-to-per протоколов, перегрузки узлов в централизованных сетях. Поэтому модель нарушителя при получении доказательства сетевой стойкости должна рассматривать атаку сети на выделенного клиента. Принцип децентрализованной стойкости всей сети должен содержать требование: для несанкционированного доступа к информации нужно сломать защиту каждого. Кроме того, должна быть обеспечена независимость от транспорта (сети) и клиентского программного обеспечения. При этом известные трудно решаемые задачи (факторизация, дискретное логарифмирование, решение нелинейных систем алгебраических уравнений от многих переменных и т.д.) остаются основой криптографической стойкости.

Ускоренное решение криптографических задач (обращение односторонних функций) может быть получено не только с помощью квантового компьютера, но и с помощью конвейерных, векторных и других специальных вычислителей. Поэтому одной из важных задач является построение и использование теоретически (а не вычислительно) стойких методов. В том числе не дешифруемых протоколов.

Децентрализованное шифрование на основе разделения шифр текста на пороговой схеме с последующей рассылкой разными маршрутами через списки доверия. Проверка совпадения на получателе.

Данный протокол использует сетевую структуру сети для поднятия уровня стойкости до теоретико-информационного уровня. А именно, упрощаем пороговую схему до генерации  $n$  случайных строк и XOR-а половины из них со строкой зашифрованного текста.

Количество выборов без учета порядка из  $n$  строк половины равно

$$C_n^{n/2} \approx 2^n \sqrt{\frac{2}{\pi n}}$$

(данная оценка получена с помощью формулы Стирлинга). Поэтому, если номера

использованных в суммировании строк считать секретным ключом, то угадать их среди всех передаваемых строк экспоненциально трудно. В тоже время если противнику удастся перехватить не все используемые строки, то он получает лишь случайную строку. То есть в этом случае имеется теоретически не дешифруемый протокол.

Оценки на трудоемкость метода «грубой силы» – экспоненциальные. Значит, чем больше сеть, тем такое шифрование более стойкое.

Для повышения стойкости с помощью программно-конфигурируемых сетей можно предусмотреть, чтобы указанные выше маршруты передачи отдельных строк не пересекались, а также распределить пересылку по времени, по частотным диапазонам, по различным сетям, с использованием ранее пересланных кому-то случайных строк или зашифрованных строк секретной информации; псевдослучайных строк, полученных на основе общего секретного ключа и т.д. То есть часть строк может вообще не передаваться, а быть общим секретом.

Другой способ увеличить стойкость криптопротоколов, не прибегая к трудно решаемым математическим задачам – это оцифровка физической аутентификации. При этом для получения объективной оцифрованной информации можно эффективно использовать клавиатуру, микрофон, а также квантовые сенсоры [1] (датчики движения, анализаторы химических событий, точечные термометры, атомные часы и т.д.). Данные с этих устройств (см. например [2]), подписанные секретным ключом абонента и снабженные меткой времени (которую нельзя модифицировать незаметно) и открытым ключом, могут составить портрет абонента, достаточный для его (или его открытого ключа) автоматической аутентификации (динамическая аутентификация). Естественно, чем больше различных способов анализа состояния абонента, тем более стойкая аутентификация может быть построена с их использованием. Повторному использованию аутентифицирующей информации помешают метки времени, которые нельзя модифицировать незаметно (защищенные метки времени).

Доверие в сети может распространяться и с помощью непосредственно физической аутентификации, поддержанной в течение некоторого периода метками времени. Распространение информации в сети при помощи

правила «рукопожатий» позволит охватить всех.

Объективное наблюдение за абонентом со стороны нескольких «доверенных» абонентов. Одиночного абонента труднее аутентифицировать. А вот если у него имеется доверенное окружение (например, имеющее с ним общие секретные ключи, находящееся с ним в постоянном контакте, на прямой видимости и т.д.) то подтверждающая информация от разных членов окружения подтверждает аутентификацию абонента (коллективная аутентификация).

Постоянный автоконтакт, обеспечивающий поддержку непрерывной аутентификации, также повышает стойкость. Эта оцифровка обычного протокола переключки на поверке в воинских частях или переключки «Ау» в условиях ограниченной видимости. В этом случае по голосу (а в нашем случае могут быть использованы и другие, в том числе квантовые и нано датчики [1]) можно не только аутентифицировать абонента, но и узнать его статус.

Отметим еще важную особенность рассматриваемого подхода. Если абонент пересылает (и получает) передающему устройству информацию в зашифрованном виде, то такая система остается стойкой при использовании любого иностранного оборудования и программного обеспечения с единственным условием выполнения транспортной функции. Поэтому, использование для пересылки зашифрованных сообщений оборудования разных производителей одновременно, с проверкой совпадения передаваемого сообщения на получателе, повышает стойкость. Предварительное зашифрование и расшифрование должно производиться на отечественном доверенном оборудовании (индивидуальном шифраторе).

Рассмотрим конкретный пример. Пусть имеется подразделение из 50 бойцов, которые отправляются на боевое задание. Первоначально у каждой пары есть свой симметричный ключ для шифрованной связи. Всего 2500 различных ключей. Пусть, для простоты, у каждого имеется однотипная рация, устройство которой позволяет в каждый момент времени связаться с 10 бойцами своей группы. При этом возможен захват каждой рации в работающем состоянии в течение периода времени (такт, например 2–4 минуты) противником с вероятностью  $p$ .

Задача состоит в обеспечении секретной связи, стойкой с некоторой вероятностью, достаточной для безопасной передачи координат объектов на линии боевого соприкосновения.

Средства для решения указанной задачи следующие:

1. Целенаправленный аутентифицирующий запрос, состоящий в анализе статических и динамических персональных данных. Статические (неизменяемые) персональные данные включают секретный ключ. Динамические – это результаты наблюдения за бойцом со стороны его окружения, результаты работы квантовых и наносенсоров, аудио, SMS, фото; все с метками времени (простановка этих меток – это отдельная задача, которая в данной статье не рассматривается). Анализ может подвергаться почерк бойца при наборе с клавиатуры, характер его движений (это по своей природе тоже симметричные ключи, которые, однако, трудно «отделить от человека», воспроизвести). Пусть анализатор (например искусственный интеллект) определяет по этим признакам «свой-чужой» с вероятностью  $p_1$ .
2. Запрос-переключка осуществляется один раз в 2–4 минуты. Опрашивает случайного доступного абонента (равновероятно) на предмет адекватности отклика. Адекватность понимается в смысле «небольшого» отличия от предыдущего отклика того же абонента. Это можно реализовать, например, при помощи вычисления хеша от кода сообщения. Опуская подробности, имеем, что «небольшое» отличие в сообщениях дает для них одно и то же кодовое слово. Например, если кодовое расстояние вдвое больше «небольшого», а расстояние от сообщений до соответствующих кодовых слов в четыре раза меньше кодового расстояния. Пусть вероятность определить своего в результате такого запроса неверно равна  $p_2$ .
3. Целенаправленный запрос окружения передающего абонента на результаты запросов-переключки и физической аутентификации. Вероятность реализации (возможность) опросить хотя бы одного из окружения за 2–4 минуты равна  $p_3$ .
4. Построение нового секретного ключа:
  - а) с использованием старых ключей;

- б) с использованием запросов п. 1–3;  
 в) с использованием посредников в сети.  
 5. Режим теоретически не дешифруемой передачи (при возможности создания большого числа непересекающихся маршрутов).

Пункты 1–3 выбраны так, чтобы не допустить перегрузки сети. Пункты 1 и 3 описывают вызовы по мере необходимости конкретной связи и, поэтому, не сильно увеличивают трафик. Для реализации пункта 2, при условии, что переключки двусторонняя, достаточно задействовать каждый из 2500 двусторонних каналов с вероятностью 0,1. То есть в среднем, нагрузка на сеть оценивается в 250 пересылок за такт.

Оценим вероятность как функцию времени. Пусть  $T$  – количество прошедших интервалов (тактов) между переключками.

Вероятность ошибки в определении своего целенаправленного запроса вида 1 и 3 в первом такте, при условии, что все опрашиваемые рации не захвачены, не больше, чем

$$\begin{aligned} P &= p \sum_{i=0, \dots, 10} C_{10}^i \left(\frac{9}{10}\right)^i \left(\frac{p_2}{10}\right)^{10-i} (1-p_1)(1-p_3) = \\ &= p(1-p_1)(1-p_3) \left(\frac{9+p_2}{10}\right)^{10} = \\ &= p(1-p_1)(1-p_3) \left(1 - \frac{1-p_2}{10}\right)^{10} \approx \\ &\approx (1-p_1)(1-p_3)e^{-(1-p_2)}. \end{aligned}$$

В общем случае получаем примерно тоже, умноженное на

$$\sum_{i=0, \dots, 10} C_{10}^i p^{10-i} (1-p)^i = 1.$$

Для двух тактов аналогично получим

$$\begin{aligned} p(1-p)P + p(1-p_1)(1-p_3)^2 e^{-2(1-p_2)} \approx \\ \approx p(1-p_1)(x+x^2)(1-p)^2, \\ x = \frac{(1-p_3)e^{-(1-p_2)}}{1-p}. \end{aligned}$$

В общем случае для  $T$  тактов имеем:

$$p(1-p_1) \frac{1-x^T}{1-x} (1-p)^T,$$

что дает величину, пропорциональную  $(1-p)^T$  при растущем  $T$ , так как в нетривиальном случае всегда выполнено:  $(1-p_3)e^{-(1-p_2)} < 1$ . Заметим, что множитель  $(1-p)^T$  при растущем  $T$  пропорционален вероятности того, что никто из бойцов не будет захвачен, что в нашей модели происходит с вероятностью, стремящейся к нулю. Таким образом, вероятность того, что захваченный воин будет принят за своего в нашей модели незначительно отличается

от вероятности того, что он вообще будет захвачен.

Для оценки эффективности п. 4 достаточно потребовать, чтобы граф двусторонней связи был двусвязным. Двусвязный граф – это связный и неделимый граф, то есть удаление любой вершины не приведет к потере связности. Теорема Уитни утверждает, что граф двусвязен тогда и только тогда, когда между любыми двумя его вершинами есть как минимум два непересекающихся пути.

Для п. 5 заметим следующее: данный протокол использует сетевую структуру коммутации для поднятия уровня стойкости с теоретико-сложностного (для вскрытия требуются большие вычисления) до теоретико-информационного (вычислительная мощность не облегчает вскрытия) уровня. А именно, генерируем  $n$  случайных строк и XOR-сумму их со строкой зашифрованного текста.

Генерируем еще  $n-1$  случайных строк. Перемешиваем получившиеся строки и посылаем адресату по сети разными маршрутами в разное время. При этом, некоторые пересылки могут быть заменены на ссылки на ранее переданные кому-то строки секретной или открытой информации. Количество выборов без учета порядка из  $2n$  строк  $n+1$  нужной для получения шифртекста, равно

$$C_{2n}^{n+1} \approx \frac{2^{2n}}{\sqrt{\pi n}}.$$

Поэтому, если номера использованных в суммировании строк считать секретным ключом, то угадать их среди всех передаваемых строк экспоненциально трудно. В то же время, если противнику удастся перехватить не все используемые в суммировании строки, то он получает лишь случайную строку. То есть в этом случае имеется теоретически не дешифруемый протокол.

### Заключение

Децентрализованная криптография во многом приходит на смену криптографии двусторонних протоколов. Новые направления в криптографии, используемые в таких технологиях как «Блокчейн», могут быть расширены для применения в системах защиты сетевого взаимодействия. При этом стойкость может возрасти с ростом количества абонентов в сети и выходить на теоретико-информационный уровень. Эта стойкость может не зависеть от оборудования, используемого для работы в сети. Перегрузки

центральных узлов и атаки на них в децентрализованных сетях отсутствуют. Кроме того, такие решения позволяют получить доселе невозможные свойства: противодействие атакам типа «человек посередине», удаленная

аутентификация незнакомых абонентов, невозможность блокировки отдельных абонентов, определение статуса «доверенный свой», определение режима «работа под контролем» и т.д.

### Литература

1. Букашкин С. А., Черепнёв М. А. Квантовые устройства в криптографии INJOIT, Vol. 11, No 1 (2023), p. 104–108
2. Букашкин С. А., Черепнёв М. А. Принцип децентрализации в системах защищенной связи. Сборник материалов XIII межведомственной научной конференции «Актуальные направления развития систем обеспечения безопасности объектов государственной охраны и охраняемых объектов, специальной связи для нужд органов государственной власти и специального информационного обеспечения государственных органов.» февраль 2023г., Орел.
3. Nakamoto, Satoshi<sup>2</sup>: «Bitcoin: A Peer-to-Peer Electronic Cash System» Available: [www.bitcoin.org/bitcoin.pdf](http://www.bitcoin.org/bitcoin.pdf).
4. Черепнев М. А. Криптографические протоколы / М. А. Черепнев; Московский государственный университет имени М. В. Ломоносова, Факультет вычислительной математики и кибернетики. – Москва: МАКС Пресс, 2018. – 2, 125 с. – ISBN 978-5-89407-592-1. – Текст: непосредственный.

## NON-MATHEMATICAL METHODS IN CRYPTOGRAPHY (SECURE COMMUNICATION BASED ON A PEER-TO-PEER MESH NETWORK)

Cherepnev M. A.<sup>3</sup>

**Keywords:** encryption, information protection, peer-to-peer networks, decentralized systems, digital signature, key distribution, authentication.

### Abstract

**The purpose of the work** is to analyze the weaknesses of information security protocols in the technical intelligence of the Armed Forces of the Russian Federation and to develop proposals for its improvement.

**The research method** consists in proposing the use of decentralized cryptography.

**Results:** some new methods of information protection in the (temporary) absence of certification authority have been proposed. The proposed methods do not use mathematical problems that are difficult to solve (discrete logarithm, factorization, search for the smallest vector in a lattice, etc.). Methods similar to physical user authentication are proposed, but in a digital version. Modern individual means of communication allows you to do this. It is proposed to use the value of the network mesh as a factor in strengthening the communication stability of its subscribers.

**The scientific novelty** lies in the development of new protocols of decentralized cryptography, which reduce the load on the central node and increase the functionality and stability of the network as a whole.

### References

1. Bukashkin S. A., Cherepnyov M. A. Kvantovye ustroystva v kriptografii INJOIT, Vol. 11, No 1 (2023), p. 104–108
2. Bukashkin S. A., Cherepnyov M. A. Princip decentralizatsii v sistemakh zashchishhennoj svyazi. Sbornik materialov XIII mezhvedomstvennoj nauchnoj konferencii «Aktual'ny'e napravleniya razvitiya sistem obespecheniya bezopasnosti ob'ektov gosudarstvennoj ohrany i ohranyaemyx ob'ektov, special'noj svyazi dlya nuzhd organov gosudarstvennoj vlasti i special'nogo informacionnogo obespecheniya gosudarstvennyx organov.» fevral' 2023 g., Orel.

2 Satoshi Nakamoto (англ. Satoshi Nakamoto) — псевдоним человека или группы людей, разработавших протокол криптовалюты биткойн и создавших первую версию программного обеспечения, в котором этот протокол был реализован. Было предпринято несколько попыток раскрыть реальную личность или группу, стоящую за этим именем, но ни одна из них не была успешной.

3 Mikhail A. Cherepnev, Doctor of Physical and Mathematical Sciences, Professor, Department of Information Security, Faculty of Computer Science, Lomonosov Moscow State University, Moscow, Russia. E-mail: [cherepniyov@gmail.com](mailto:cherepniyov@gmail.com)



3. Nakamoto, Satoshi: «Bitcoin: A Peer-to-Peer Electronic Cash System». Available: [www.bitcoin.org/bitcoin.pdf](http://www.bitcoin.org/bitcoin.pdf)
4. Cherepnev, M. A. Kriptograficheskie protokoly` / M. A. Cherepnev; Moskovskij gosudarstvenny`j universitet imeni M. V. Lomonosova, Fakul'tet vychislitel'noj matematiki i kibernetiki. - Moskva: MAKS Press, 2018. – 2, 125 s. – ISBN 978-5-89407-592-1. – Tekst : neposredstvenny'j.



# КРИТЕРИИ ЭФФЕКТИВНОСТИ ПОЛЕВОЙ СИСТЕМЫ ЭЛЕКТРОСНАБЖЕНИЯ

Асанин А. В.<sup>1</sup>, Иванов В. Г.<sup>2</sup>, Иванишко А. Н.<sup>3</sup>

DOI:10.21681/3034-4050-2026-1-78-87

**Ключевые слова:** эффективность системы, критерии системы, напряжение, мощность, часовой расход.

## Аннотация

**Цель работы:** обоснование критериев эффективности полевой системы электроснабжения специального назначения.

**Метод исследования:** методологическую основу исследования составила общая теория систем с использованием методов системного анализа. Достоверность результатов обеспечивается корректностью постановок задач, адекватностью применяемых методов исследования решаемым задачам и непротиворечивостью полученных результатов данным предшествующих исследований, согласованностью полученных теоретических оценок с результатами аналитических расчетов.

**Результаты исследования:** выбраны и обоснованы критерии эффективности полевой системы электроснабжения. В качестве экономического критерия эффективности системы принят часовой расход топлива, критерий технической эффективности оценивается суммой объемов и масс элементов полевой системы электроснабжения. За комплексный (обобщенный) технико-экономический критерий принято время непрерывной работы. Данный критерий позволяет оценить экономический и технический уровень устройств полевой системы электроснабжения, сопоставить их с функциональными возможностями и определить их целесообразный предел совершенствования.

**Научная новизна:** заключается в разработке обоснованных критериев эффективности полевой системы электроснабжения специального назначения с учетом ее применения для электроснабжения полевых средств связи военного назначения.

## Введение

Система электроснабжения является неотъемлемой и составной частью подвижных объектов связи [1] (рис. 1), и является подсистемой более высокой по иерархии системы, поэтому исследования эффективности полевой системы электроснабжения (ПСЭС) должны проводиться на основе системного анализа. Для этого необходимо выбрать и обосновать критерии эффективности, которые формализуются на основе технико-экономических показателей типовых средств электроснабжения и источников вторичного электропитания (ИБЭП).

При всех возможных обстоятельствах выбора критерия он должен удовлетворять вполне определенным требованиям:

- отражать основное назначение системы и соответствовать цели исследования;

- количественно измерять эффективность системы;
- быть критичным к параметрам системы;
- должен быть наглядным и по возможности просто определяемым;
- иметь, по возможности, четкий физический смысл.

Принципиально важным в методологическом плане является учет принадлежности ПСЭС конкретному подвижному объекту связи. Это положение вытекает из основного принципа системного анализа, состоящего в том, что эффективность того или иного технического средства может рассматриваться лишь в определенной среде, под которой понимаются условия применения, предъявляемые требования и накладываемые ограничения [1, 2]. Это означает, что при выборе критериев эффективности ПСЭС необходимо

1 Асанин Антон Викторович, кандидат технических наук, доцент, декан инженерного факультета, Федеральное государственное бюджетное военное образовательное учреждение высшего образования «Академия гражданской защиты Министерства Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий имени генерал-лейтенанта Д. И. Михайлика», г. Химки, Россия. E-mail: asanin-anton@mail.ru

2 Иванов Василий Геннадьевич, доктор военных наук, доцент, профессор кафедры информатики и вычислительной техники, Федеральное государственное бюджетное военное образовательное учреждение высшего образования «Академия гражданской защиты Министерства Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий имени генерал-лейтенанта Д. И. Михайлика» г. Химки, Россия. E-mail: wasj2006@yandex.ru

3 Иванишко Александр Николаевич, начальник группы главного управления связи Вооруженных Сил Российской Федерации, г. Москва, Россия. E-mail: GUS\_1@mail.ru



Рис. 1. Функциональные элементы системы электроснабжения специального назначения

вводить в них параметры, характеризующие условия применения подвижных объектов связи по назначению.

### Основная часть

Система преобразования энергии и ее составные элементы в частности двигатели внутреннего сгорания (ДВС), электроагрегаты (ЭГ), кабельное распределительное оборудование (КРО) и ИВЭП аппаратуры связи оцениваются множеством показателей. При этом в соответствии с принципом однозначности, сформулированным в [1,2], критерий эффективности должен быть представлен в виде одного показателя, зависящего от всех необходимых параметров. Вместе с тем, следуя методологическим основам исследования эффективности ПСЭС, необходимо выделить такие показатели или группу показателей, которые отвечали бы исследованиям эффективности ПСЭС. При этом значения эффективности определяются не только показателями самой ПСЭС, но и показателями применения средств связи.

Функционирование ПСЭС связано с расходом топлива [3] на выработку полезной энергии для аппаратуры связи (АС) и технических

средств обеспечения обитаемости (ТСОО), на тепловые потери энергии. В общем случае экономические затраты выражаются стоимостью разработки, и производства подвижных объектов связи, материалоемкостью элементов системы и средствами, расходуемыми в процессе функционирования (эксплуатации) объекта, в частности, горюче-смазочными материалами. Стоимость системы в условиях выполнения подвижными объектами связи специальных задач. Показатель стоимости может рассматриваться как ограничение при выборе возможных реализаций элементов системы. Помимо этого, система должна характеризоваться показателями технического уровня ее элементов, которые войдут в критерий технической эффективности. Комплексный (обобщенный) критерий эффективности системы должен отражать влияние функционирования ПСЭС на выполнение подвижными объектами связи специальных задач по обеспечению связи в полном объеме.

Исходя из вышеизложенного, в качестве экономического критерия эффективности системы предлагается использовать часовой расход топлива ( $m_T$ ), аналитическое выражение которого представлено в следующем виде:

$$m_{TC} = \frac{P_{ac}}{\eta_{dvc} \times Knc_T \times P'_{эT}} \quad (1)$$

где:

- $P_{ac}$  – мощность потребления аппаратуры связи и технических средств обеспечения обитаемости;
- $\eta_{dvc}$  – КПД ДВС;
- $Knc_T$  – общий коэффициент преобразования тепловой энергии;
- $P'_{эT}$  – эквивалентная удельная энергия 1-го килограмма топлива [кВт\*ч/кг].

$$Knc_T = \prod_{i=1}^K Kn_i = \prod_{i=1}^K \eta_i, \quad (2)$$

где:  $\eta_i$  – КПД  $i$ -го элемента СПЭ.

Исследования, проведенные в работах [1, 4], показали, что общий коэффициент преобразования тепловой энергии ( $Knc_T$ ) зависит от совокупности параметров, которые характеризуют поток электрической энергии, при этом исследовался функционал вида:

$$Knc_T = F \{Uc, Uni, Pi_{ac}, Pac, \varepsilon_{ex}, \varepsilon_2, Un\phi_i\}, \quad (3)$$

где:

- $Uc$  – напряжение на выходе ИЭЭ;
- $Uni$  – напряжение  $i$ -й цепи электропитания в АС;
- $Pi_{ac}$  – мощность  $i$ -й цепи электропитания в АС или ТСОО;
- $Pac$  – мощность потребляемая АС и ТСОО;
- $\varepsilon_{ex}$  – коэффициент кратности изменения напряжения в электрической сети (ИЭЭ);
- $\varepsilon_2$  – коэффициент кратности изменения напряжения на выходе ИЭЭ, или стабилизированных ИВЭП;
- $Un\phi_i$  – напряжение пульсаций на выходе сглаживающего фильтра выпрямителя.

Анализ используемых в устройствах (ДВС, ЭГ, КРО, ИВЭП) показывает, что КПД каждого устройства зависит, прежде всего, от номинальной мощности, напряжения и тока, за исключением в ДВС. По известным значениям КПД серийно выпускаемых устройствах согласно [3, 5], были получены аналитические выражения зависимостей КПД устройств от их номинальной мощности. В (2.4...2.7) эти выражения представлены в общем виде:

$$\eta_{i_2} = a_1 + \varepsilon_1 \times \left( \frac{Pac}{\prod_{i=1}^{K-1} Kno_i} \right); \quad (4)$$

$$\eta_{i_2} = a_2 + \varepsilon_2 \times \left( \frac{Pac}{lac \times \prod_{i=1}^{K-1} Kno_i} \right); \quad (5)$$

$$\eta_{3_3} = \varepsilon_3 \times \left( \frac{Pac}{\prod_{i=1}^{K-1} Kno_i} \right)^\alpha; \quad (6)$$

$$\eta_{i_4} = a_4 = const, \quad (7)$$

где:

- $a_i, \varepsilon_i$  [1/Вт] – постоянные коэффициенты аппроксимации;
- $\alpha$  – степенной показатель;
- $Kno_i$  – общий коэффициент преобразования энергии, равный произведению  $\eta_i$  –  $*K_{M_i}$ ,  $K_{M_i}$  – коэффициент мощности.

Коэффициент  $K_M$  каждого  $i$ -го устройства системы определяется из выражения:

$$K_{M_i} = \cos \varphi \times K_{Ii} \times K_{Iiv}, \quad (8)$$

где:  $\cos \varphi$  – коэффициент сдвига фазы между током и напряжением;  $K_{Ii}, K_{Iiv}$  – коэффициенты искажения формы тока и напряжения.

В свою очередь, составляющие, входящие в выражение (8) были определены, как:

$$\cos \varphi_1 = c_1 + d_1 \times \left( \frac{Pac}{\prod_{i=1}^K \eta_i} \right); \quad (9)$$

$$\cos \varphi_2 = d_2 \times (\varepsilon_{BX}); \quad (10)$$

$$Ku_{i1} = \frac{1}{\sqrt{1 + Kr^2}}; \quad (11)$$

$$Ku_{i2} = d_2 \times (\varepsilon_{BX}); \quad (12)$$

$$Ku_{i3} = c_2 = const; \quad (13)$$

$$Ku_{U1} = \frac{1}{\sqrt{1 + Kr^2}} 1/\sqrt{(1 + Kr^2)}; \quad (14)$$

$$Ku_{U2} = d_2 \times (\varepsilon_{BX}), \quad (15)$$

где:  $c, d$  – постоянные коэффициенты аппроксимации;  $K_r$  – коэффициент гармоник искаженной формы тока и напряжения.

Конкретные выражения КПД и реактивных составляющих устройств, входящих в ПСЭС приведены в табл. 1.

Наличие реактивных составляющих в ПСЭС приводит к увеличению потерь тепловой энергии, падению напряжения на реактивных



Таблица 1.

## Элементы полевой системы электроснабжения и их характеристики

№ п/п	Тип преобразователя	Вид преобразователя	Перечень технико-экономических показателей	Расчеты, формулы и соотношения
1	2	3	4	5
1.	Двигатель внутреннего сгорания карбюраторный	Химическую энергию топлива в механическую	$m_T, \dot{q}_{ЭФ}, P_{ЭТ}, V_{об}, M_{об}$	$m_T = \frac{P_{ас}}{\eta_{авс} \times P'_{ЭТ}}, \dots \eta_{ЭФ} = 0,17 \dots 0,24;$ $P_{эм} = 11862 \text{ Вт} \times \text{ч/кг};$ $V_{об} = 403 \times \log(P_{эф}) - 2976;$ $M_{об} = 171 \times \log(P_{эф}) - 576.$
2.	Двигатель внутреннего сгорания дизельный	Химическую энергию топлива в механическую	$m_T, \dot{q}_{ЭФ}, P_{ЭТ}, V_{об}, M_{об}$	$m_T = \frac{P_{ас}}{\eta_{авс} \times P'_{ЭТ}}, \dots \eta_{ЭФ} = 0,25 \dots 0,35;$ $P_{эм} = 12560 \text{ Вт} \times \text{ч/кг};$ $V_{об} = 800,2 \times \log(P_{эф}) - 1358;$ $M_{об} = 407 \times \log(P_{эф}) - 1447.$
3.	Электродвигатель переменного тока	Магнитную энергию в электрическую посредством механической	$\eta_{ЭГ}, V_{ЭГ}, M_{ЭГ}$	$\eta_{ЭГ} = 0,542 \times (P_H)^{0,0476};$ $V_{ЭГ} = 188,2 \times \log(P_H) - 597;$ $M_{ЭГ} = 189,6 \times \log(P_H) - 603.$
4.	Электродвигатель постоянного тока	Магнитную энергию в электрическую посредством механической	$\eta_{ЭГ}, V_{ЭГ}, M_{ЭГ}$	$\eta_{ЭГ} = 0,715 + 0,67 \times 10^{-5} \times P_H;$ $V_{ЭГ} = 16 + 0,003 \times P_{ЭГ};$ $M_{ЭГ} = 5,3 + 0,008 \times P_{ЭГ}.$
5.	Бензиновый электроагрегат переменного тока	Химическую энергию топлива в электрическую	$V_{БЭА}, M_{БЭА}$	$V_{БЭА} = 8,38 \times (P_H)^{0,512};$ $M_{БЭА} = 1,51 \times (P_H)^{0,606}.$
6.	Дизельный электроагрегат переменного 3ф тока	Химическую энергию топлива в электрическую	$V_{ДЭА}, M_{ДЭА}$	$V_{ДЭА} = 1987 \times \log(P_H) - 6933;$ $M_{ДЭА} = 1570 \times \log(P_H) - 5400.$
7.	Электроустановка с отбором мощности	Магнитную энергию в электрическую посредством механической	$M_{ЭУ}$	$M_{ЭУ} = 190 \times \log(P_H) - 600.$
8.	Коммутационно-распределительное оборудование переменного 3ф тока	Транзит электроэнергии от ЭА к ИВЭП АС	$\eta_{КРО}, V_{КРО}, M_{КРО}$	$\eta_{КРО} = 0,95;$ $V_{КРО} = K_V \times P_{КРО};$ $M_{КРО} = K_M \times P_{КРО}.$
9.	Коммутационно-распределительное оборудование постоянного тока	Транзит электроэнергии от ЭА к ИВЭП АС	$\eta_{КРО}, V_{КРО}, M_{КРО}$	$\eta_{КРО} = 0,95, \text{ при токе до } 100 \text{ А};$ $\eta_{КРО} = 0,9, \text{ при токе свыше } 100 \text{ А};$ $V_{КРО} = K_V \times P_{КРО};$ $M_{КРО} = K_M \times P_{КРО}.$
10.	Стабилизатор напряжения переменного 1ф тока типа СОС	Стабилизация переменного напряжения	$\eta_{СОС}, \cos \phi_{мп},$ $\cos \phi_{вх}, K_{ui}, K_M, \varepsilon_{вх},$ $\varepsilon_2, V_{СОС}, M_{СОС}$	$\eta_{СОС} = 0,35 + 0,125 \times \log(P_H);$ $\cos \phi_{мп} = 0,428 + 0,191 \times \log(P_с);$ $\cos \phi_{вх} = 0,98;$ $K_{ui} = \frac{I_1}{\sqrt{I_1^2 + I_2^2 + \dots + I_g^2}};$ $K_M = \cos \phi_{мп} \times \cos \phi_{вх} \times K_{ui} = 0,7;$ $\varepsilon_{вх} = 1,3; \varepsilon_2 = 1,05;$ $V_{СОС} = 40 + 0,0135 \times P_H;$ $M_{СОС} = 50 + 0,016 \times P_H.$

1	2	3	4	5
11.	Стабилизатор напряжения переменного 3ф тока типа СТС	Стабилизация переменного напряжения	$\eta_{СТС}, \cos\varphi_{mp}, K_M, \varepsilon_{\text{вх}}, \varepsilon_2, V_{СТС}, M_{СТС}$	$\eta_{СТС} = 0,394 + 0,115 \times \log(P_H);$ $\cos\varphi_{mp} = 0,818 + 0,016 \times \log(P_2);$ $K_M = 0,75; \varepsilon_{\text{вх}} = 1,3; \varepsilon_2 = 1,05;$ $V_{СТС} = 80 + 0,0065 \times P_H;$ $M_{СТС} = 85 + 0,0105 \times P_H.$
12.	Стабилизатор напряжения переменного 1ф тока типа СТО	Стабилизация переменного напряжения	$\eta_{СТО}, K_M, \varepsilon_{\text{вх}}, \varepsilon_2, V_{СТО}, M_{СТО}$	$\eta_{СТО} = 0,639 + 0,05 \times \log(P_H);$ $K_M = 0,85; \varepsilon_{\text{вх}} = 1,3; \varepsilon_2 = 1,05;$ $V_{СТО} = 40 + 0,008 \times P_H;$ $M_{СТО} = 35 + 0,005 \times P_H.$
13.	Стабилизатор напряжения переменного 3ф тока типа СТТ	Стабилизация переменного напряжения	$\eta_{СТТ}, K_M, \varepsilon_{\text{вх}}, \varepsilon_2, V_{СТТ}, M_{СТТ}$	$\eta_{СТТ} = 0,387 + 0,12 \times \log(P_H);$ $K_M = 0,85; \varepsilon_{\text{вх}} = 1,3; \varepsilon_2 = 1,05;$ $V_{СТТ} = 60 + 0,005 \times P_H;$ $M_{СТТ} = 50 + 0,005 \times P_H.$
14.	Линейный стабилизатор напряжения постоянного тока	Стабилизация постоянного напряжения	$\eta_{ЛСН}, \varepsilon_H, V_{ЛСН}, M_{ЛСН}$	$\eta_{ЛСН} = \frac{1}{\varepsilon_{\text{вх}} \times (1 + \delta_{ЭК})};$ $P_H = \frac{P_{\text{рас}}}{[\varepsilon_{\text{вх}} \times (1 + \delta_{ЭК}) - 1]};$ $\delta_{ЭК} = \frac{U_{K\text{эmin}} + Unc}{U_H}; \varepsilon_H = 1;$ $V_{ЛСН} = K_V \times P_H \times [\varepsilon_1 \times (1 + \delta_{ЭК}) - 1];$ $M_{ЛСН} = K_M \times P_H \times [\varepsilon_1 \times (1 + \delta_{ЭК}) - 1].$
15.	Сетевой трансформаторный выпрямитель 1ф исполнения	Трансформирование, выпрямление переменного 1ф тока и сглаживание выпрямленного напряжения	$\eta_{СТВ0}, \cos\varphi_{mp}, K_{И1}, K_M, K_{ИЛП}, \varepsilon_{\text{вх}}, \varepsilon_2, V_{СТВ0}, M_{СТВ0}$	$\eta_{СТВ0} = 0,403 + 0,126 \times \log(P_H);$ $\cos\varphi_{mp} = 0,428 + 0,191 \times \log(P_2);$ $K_{И1} = 0,88; K_M = \cos\varphi_{mp} \times K_{И1};$ $K_{ИЛП} = 0,32/0,675/0,9^2);$ $\varepsilon_{\text{вх}} = 1,3; \varepsilon_2 = 1,05;$ $V_{СТВ0} = 4 + 0,009 \times P_H;$ $M_{СТВ0} = 7 + 0,048 \times P_H.$
16.	Сетевой трансформаторный выпрямитель 3ф исполнения	Трансформирование, выпрямление переменного 3ф тока и сглаживание выпрямленного напряжения	$\eta_{СТВм}, \cos\varphi_{mp}, K_{И1}, K_M, K_{ИЛП}, \varepsilon_{\text{вх}}, \varepsilon_2, V_{СТВм}, M_{СТВм}$	$\eta_{СТВм} = 0,404 + 0,107 \times \log(P_H);$ $\cos\varphi_{mp} = 0,818 + 0,016 \times \log(P_2);$ $K_{И1} = 0,9; K_M = \cos\varphi_{mp} \times K_{И1};$ $K_{ИЛП} = 0,74/0,95^3); \varepsilon_{\text{вх}} = 1,3; \varepsilon_2 = 1,05;$ $V_{СТВм} = 30 + 0,037 \times P_H;$ $M_{СТВм} = 32 + 0,025 \times P_H.$
17.	Сетевой трансформаторный выпрямитель 1ф исполнения	Трансформирование, выпрямление переменного 1ф тока и сглаживание, стабилизация выпрямленного напряжения	$\eta_{СТВCo}, K_M, K_{ИЛП}, \varepsilon_{\text{вх}}, \varepsilon_2, V_{СТВCo}, M_{СТВCo}$	$\eta_{СТВCo} = 0,218 + 0,187 \times \log(P_H);$ $K_M = 0,85; K_{ИЛП} = 0,6;$ $\varepsilon_{\text{вх}} = 1,3; \varepsilon_2 = 1,05;$ $V_{СТВCo} = 25 + 0,052 \times P_H;$ $M_{СТВCo} = 15 + 0,078 \times P_H.$
18.	Сетевой трансформаторный выпрямитель 3ф исполнения	Трансформирование, выпрямление переменного 3ф тока и сглаживание, стабилизация выпрямленного напряжения	$\eta_{СТВСм}, K_M, K_{ИЛП}, \varepsilon_{\text{вх}}, \varepsilon_2, V_{СТВСм}, M_{СТВСм}$	$\eta_{СТВСм} = 0,281 + 0,145 \times \log(P_H);$ $K_M = 0,65/0,85^4); K_{ИЛП} = 0,62/0,68^5);$ $\varepsilon_{\text{вх}} = 1,3; \varepsilon_2 = 1,05;$ $V_{СТВСм} = 20 + 0,1 \times P_H;$ $M_{СТВСм} = 30 + 0,033 \times P_H.$

1	2	3	4	5
19.	Преобразователь постоянного напряжения стабилизированный дискретного исполнения	Преобразование и стабилизация постоянного напряжения	$\eta_{ПНС}, \varepsilon_{\text{вх}}, \varepsilon_2, K_{И.ТР}, V_{ПНС}, M_{ПНС}$	$\eta_{ПНС} = 0,503 + 0,186 \times \log(U_H);$ $\varepsilon_{\text{вх}} = 1,3; \varepsilon_2 = 1,05;$ $K_{И.ТР} = \frac{I_1}{\sqrt{\varepsilon_{\text{вх}} \times \pi}};$ $V_{ПНС} = Ku \times P_H; M_{ПНС} = Km \times P_H.$
20.	Преобразователь напряжения дискретного исполнения	Преобразование постоянного напряжения	$\eta_{ПН}, \varepsilon_{\text{вх}}, \varepsilon_2, K_{И.ТР}, V_{ПН}, M_{ПН}$	$\eta_{ПН} = \frac{U_H}{1,22 \times U_H + 0,553};$ $K_{И.ТР} = 1; \varepsilon_{\text{вх}} = 1,3; \varepsilon_2 = 1,05;$ $V_{ПН} = Ku \times P_H; M_{ПН} = Km \times P_H.$
21.	Выпрямитель с бестрансформаторным входом 1ф	Преобразование переменного 1ф напряжения в постоянное	$\eta_{ВБВ}, \varepsilon_{\text{вх}}, \varepsilon_2, K_B, K_{И.и}, K_M, V_{ВБВ}, M_{ВБВ}$	$\eta_{ВБВ1} = 0,8 + 0,04 \times \log(U_H);$ $\varepsilon_{\text{вх}} = 1,3; \varepsilon_2 = 1,05; K_B = 0,9; K_{И.и} = 0,7;$ $K_M = K_B \times K_{И.и} = 0,63;$ $V_{ВБВ} = Ku \times P_H; M_{ВБВ} = Km \times P_H.$
22.	Выпрямитель с бестрансформаторным входом 3ф	Преобразование переменного 3ф напряжения в постоянное	$\eta_{ВБВ}, \varepsilon_{\text{вх}}, \varepsilon_2, K_B, K_{И.и}, K_M, V_{ВБВ}, M_{ВБВ}$	$\eta_{ВБВ3} = 85; \varepsilon_{\text{вх}} = 1,3; \varepsilon_2 = 1,05;$ $K_B = 0,95; K_{И.и} = 0,8; K_M = 0,76;$ $V_{ВБВ} = Ku \times P_H; M_{ВБВ} = Km \times P_H.$
23.	Стабилизатор напряжения постоянного тока микромодульного исполнения	Стабилизация постоянного напряжения	$\eta_{МЛНС}, \varepsilon_H, V_{МЛНС}, M_{МЛНС}$	$\eta_{МЛНС} = \frac{1}{\varepsilon_{\text{вх}} \times (1 + \delta_{ЭК})};$ $P_H = \frac{P_{\text{рас}}}{[\varepsilon_{\text{вх}} \times (1 + \delta_{ЭК}) - 1]};$ $V_{МЛНС} = Kv \times P_H \times [\varepsilon_1 \times (1 + \delta_{ЭК}) - 1];$ $M_{МЛНС} = Km \times P_H \times [\varepsilon_{\text{вх}} \times (1 + \delta_{ЭК}) - 1].$
24.	Стабилизатор напряжения микромодульного исполнения	Преобразование и стабилизация постоянного напряжения	$\eta_{МПСН}, \varepsilon_{\text{вх}}, \varepsilon_2, V_{МПСН}, M_{МПСН}$	$\eta_{МПСН} = 0,728 + 0,098 \times \log(U_H);$ $\varepsilon_{\text{вх}} = 1,3; \varepsilon_2 = 1,05;$ $V_{МПСН} = Ku \times P_H; M_{МПСН} = Km \times P_H.$
25.	Микровыпрямитель с бестрансформаторным микромодульного исполнения	Преобразование переменного напряжения в постоянное	$\eta_{МВБВ}, K_M, \varepsilon_{\text{вх}}, \varepsilon_2, V_{МВБВ}, M_{МВБВ}$	$\eta_{МВБВ} = 0,628 + 0,099 \times \log(U_H);$ $\varepsilon_{\text{вх}} = 1,3; \varepsilon_2 = 1,05; K_M = 0,83;$ $V_{МВБВ} = Ku \times P_H; M_{МВБВ} = Km \times P_H.$
26.	Устройства гарантированного питания с щелочными АБ		$V_{АБщ}, M_{АБщ}$	$V_{АБщ} = 13,4 + 0,02 \times P_H;$ $M_{АБщ} = 0,581 + 0,187 \times P_H.$
27.	Устройства гарантированного питания с кислотными АБ		$V_{АБК}, M_{АБК}$	$V_{АБК} = 1,3 + 0,07 \times P_H;$ $M_{АБК} = 0,136 \times P_H - 2,34.$

элементах, перегрузке генератора, снижению нагрузки на ДВС, к созданию предпосылок искажения формы кривой напряжения на зажимах генератора и, тем самым, к увеличению мощности искажений. Анализ разработок существующих СЭС и ИВЭП показывает, что реактивные составляющие, как правило, при этом не оцениваются. Избыточность по мощности при этом обычно компенсируется выбором более мощного электроагрегата, что приводит к увеличению потребления топлива и ухудшению МГП системы. Поэтому исследование ПСЭС по снижению избыточных МГП,

а значит и реактивных составляющих является необходимым условием повышения эффективности системы. Эти показатели необходимо отнести к критерию технической эффективности, которые оцениваются суммой объемов и масс элементов ПСЭС.

$$V_C = \sum_{i=1}^n V_{i_{уэз}} + \sum_{j=1}^m V_{j_{кпо}} + \sum_{y=1}^k V_{y_{уээн}}; \quad (16)$$

$$M_C = \sum_{i=1}^n M_{i_{уэз}} + \sum_{j=1}^m M_{j_{кпо}} + \sum_{y=1}^k M_{y_{уээн}}. \quad (17)$$

Массогабаритные показатели ИЭЭ, КРО и ИВЭП зависят, в основном, от номинальной мощности нагрузки. В соответствии с этим, объем и масса каждого элемента системы выражены через  $P_{ac}$ .

$$V_1 = \pm m_1 + n_1 \times \left( \frac{P_{i_{ac}}}{1} \right); \quad (18)$$

$$V_2 = \pm m_2 + n_2 \times \left( \frac{P_{i_{ac}}}{Kno_1} \right); \quad (19)$$

$$V_3 = \pm m_3 + n_3 \times \log \left( \frac{\sum_1^n P_{i_{ac}}}{Kno_1 \times Kno_2} \right); \quad (20)$$

$$V_4 = n_4 \times \left( \frac{\sum_1^n P_{i_{ac}}}{Kno_1 \times Kno_2 \times Kno_3} \right)^\alpha, \quad (21)$$

где  $Kno$  – общий коэффициент преобразования энергии в  $i$ -м элементе СПЭ.

Расчетные соотношения массы каждого элемента системы имеют аналогичный вид, что и для объема в (18)–(21).

Общим параметром, характеризующим связь экономического и технических показателей ПСЭС с показателями подвижных объектов связи является мощность потребления АС и ТСОО  $P_{ac}$ . Однако более полно эта связь может быть установлена с помощью комплексного (обобщенного) показателя. Наиболее распространенным приемом формирования обобщенного критерия эффективности является представление его в аддитивной или мультипликативной форме. При этом зачастую используется метод экспертных оценок, когда для каждого из формируемых показателей (частных критериев) определяется «вес» в сравнении с другими. Недостатками таких критериев эффективности являются субъективизм экспертов, утрата наглядности и физического смысла обобщенного показателя. Поэтому необходим такой обобщенный показатель, в котором частные показатели имеют аналитическое выражение.

Основной задачей подвижных объектов связи в условиях боевых действий является выполнение ими своих функций в полном объеме в течение времени проведения боевой операции ( $t_{on}$ ). Это достигается непрерывным функционированием подвижных объектов связи за этот промежуток времени. Согласно [1,3], функционирование подвижных объектов связи является циклическим. При этом установлены подготовительный и основной циклы функционирования. На подготовительном цикле подвижных объектов связи приводится в состояние выполнения боевых

задач (производится ремонт поврежденных узлов, или замена на работоспособные, проводятся регламентные работы, техническое обслуживание, заправка топливом). Основным циклом функционирования характеризуется выполнением подвижных объектов связи боевых задач в течении  $t_{on}$ , который обеспечивается качеством функционирования ПСЭС. Время  $t_{on}$  устанавливается нормативными документами или приказами и является величиной заданной. Так, например, для подвижных объектов связи тактического звена управления (в ПУС КП МСП)  $t_{on}$  составляет 120 часов.

Результат функционирования подвижных объектов связи напрямую связан с непрерывной работой ПСЭС и, в первую очередь, ИЭЭ и определяется временем непрерывной работы ПСЭС ( $t_{HP}$ ). Этот показатель является одним из важных временных показателей и задается в требованиях технического задания на разработку ПСЭС подвижных объектов связи. Для ПСЭС время  $t_{HP}$  определяется следующим выражением:

$$t_{HP} = \frac{M_{m3}}{m_T}, \quad (22)$$

где  $M_{m3}$  – масса запаса топлива, предназначенная для ИЭЭ.

В существующих СЭС ПОС запас топлива определяется емкостью топливного бака ИЭЭ. Как показано в работах [1,2], запас  $M_{m3}$  обеспечивает непрерывную работу ИЭЭ в течение 8–12 часов, что значительно меньше  $t_{on}$ , вследствие чего, возможны перерывы в электропитании подвижных объектов связи из-за отсутствия топлива. Перерывы в электропитании подвижных объектов связи также могут вызывать и отказы в ПСЭС, но в данной работе надежность показатели считаются заданными и будут введены в ограничения при разработке математической модели и выборе наиболее эффективного варианта ПСЭС. Это оправданно тем, что рассматриваемый отрезок времени  $t_{on}$  в десятки раз меньше, чем заданная наработка на отказ (Тос) СЭС, которая для подвижных объектов связи тактического звена управления составляет 1500–2000 часов. При таких соотношениях, когда  $t_{on} \ll \text{Тос}$ , отказы маловероятны, и вследствие этого надежность показатели в обобщенный показатель вводить нецелесообразно. Из вышеизложенного следует, что для организации непрерывного функционирования ПСЭС необходима неоднократная и своевременная дозаправка топливом в течении  $t_{on}$ :

$$N_3 = \frac{t_{on}}{tp_3}, \quad (23)$$



где:  $tp_3$  – время работы ИЭЭ на одной заправке топливом;  $N_3$  – количество заправок.

При  $tp_3 = t_{HP} = t_{on}$  результат функционирования ПСЭС соответствует идеальному случаю (при одной исходной заправки топливом). Но практически, в настоящее время это невозможно, так как запас топлива в подвижных объектах связи для ПСЭС ограничен емкостью топливного бака ИЭЭ. Количество резервного топлива, доставляемого с базы снабжения в район боевых действий для объектов военной техники, в том числе и ПСЭС подвижных объектов связи, определяется нормативными документами и составляет в тактическом звене управления половине всей заправки топливом. При этом дозаправка резервным топливом организуется в соединении 1-2 раза в сутки. Поэтому увеличение исходного запаса топлива в подвижных объектах связи является важным условием повышения эффективности ПСЭС и, как следует из (22), этот запас топлива увеличивает время непрерывной работы системы в пределах времени  $t_{on}$ . Исходя из (22), можно утверждать, что время непрерывной работы ПСЭС является одним из важных обобщенных показателей, связывающих систему преобразования энергии с подвижными объектами связи. Но необходимый запас топлива может размещаться в подвижных объектах связи в том случае, если для него имеется соответствующий запас полезного объема и массы. В существующих подвижных объектах связи со встраиваемыми электроагрегатами такой запас отсутствует из-за громоздких габаритов и массы ВЭА и ИВЭП. Следовательно, необходимый объем и массу для размещения дополнительного топлива можно получить за счет совершенствования элементов ПСЭС, то есть улучшения их МГП и снижения потерь тепловой энергии.

Практика проектирования СЭС показывает, что компоновка ее составных элементов в подвижных объектах связи всегда связана с ограниченными возможностями в отношении их размещения, так как приоритетным оборудованием считается аппаратура связи. Следовательно, размещаемые в подвижных объектах связи элементы ПСЭС не должны превышать заданные значения объема и массы ( $V_{с.зад}$ ,  $M_{с.зад}$ ), которые устанавливаются для конкретных типов подвижных объектов связи. С учетом этого условия имеем следующие соотношения:

$$\begin{aligned} V_C &\leq V_{с.зад}, \\ M_C &\leq M_{с.зад}. \end{aligned} \quad (24)$$

Тогда объем и масса, отводимые для размещения топлива, определяются из выражения:

$$\begin{aligned} V_{m3} &= V_{с.зад} - V_C, \\ M_{m3} &= M_{с.зад} - M_C. \end{aligned} \quad (25)$$

где:  $V_C$  – объем, занимаемый элементами перспективной (усовершенствованной) СПЭ;  $M_C$  – суммарная масса элементов перспективной ПСЭС.

Подставляя (25) в (22), получим аналитическое выражение обобщенного критерия эффективности:

$$t_{HP} = \frac{M_{с.зад} - M_C}{m_T}, \quad (26)$$

где  $M_C$  – масса перспективной ПСЭС.

Из (26) следует, что обобщенный критерий  $t_{HP}$  объединяет экономический и технические показатели ПСЭС и в дальнейшем может трактоваться как обобщенный технико-экономический критерий, на основании которого можно проводить оценку эффективности ПСЭС и решать поставленную научную задачу.

### Заключение

Каждый из частных критериев эффективности, входящих в обобщенный критерий, отражает несопоставимые друг с другом значения, и может иметь противоречивые результаты, по которым наилучший вариант ПСЭС определить не удастся. Их взаимосвязь можно установить только косвенным путем, после тщательного исследования различных вариантов ПСЭС. С помощью обобщенного критерия эффективности ( $t_{HP}$ ) решаются эти противоречия и удается найти компромиссное решение. Выбранный обобщенный критерий (27) имеет простую форму и содержит глубокий физический смысл.

$$\begin{aligned} t_{HP} &= \frac{M_{m3}}{m_{TC}} = \frac{M_{с.зад} - M_C}{m_{TC}} = \\ &= \frac{y_T \times (V_{с.зад} - V_C)}{m_{TC}} = \max t_{HP}. \end{aligned} \quad (26)$$

Данный критерий позволяет оценить экономический и технический уровень устройств ПСЭС, сопоставить их с функциональными возможностями подвижных объектов связи и определить их целесообразный предел совершенствования. Эти обстоятельства позволяют говорить о правильном выборе обобщенного критерия технико-экономической эффективности.

### Литература

1. Электроснабжение телекоммуникационных систем, стационарных и полевых узлов связи / А. В. Мякотин, Д. Ю. Замазий, Е. А. Кордюков, Н. М. Мельников, Н. Г. Сысоев, Д. Б. Шляхтенко, под ред. А. В. Мякотина. – СПб.: ВАС, 2018. – 408 с.: ил.
2. Воробьев А. Ю. Электроснабжение компьютерных и телекоммуникационных систем. – М.: Эко-Трендз, 2002.
3. Романов Н. В., Алексашкин А. А. Энергетика для войск // Армейский сборник. 2021. № 8. С. 100-110.
4. Основные проблемы и перспективы развития АСЭС / Бартош В. В., Винограденко А. М., Веселовский А. П. // В сборнике: Проблемы технического обеспечения войск в современных условиях. Труды III Межвузовской научно-практической конференции. 2018. С. 136–140.
5. Железняков В. О., Матвеев Р. В., Мякотин А. В. Способ электроснабжения полевых объектов материально-технического обеспечения // В сборнике: Актуальные проблемы инфотелекоммуникаций в науке и образовании. Международная научно-техническая и научно-методическая конференция: сборник научных статей в 2 томах. под. ред. С. В. Бачевского, сост. А. Г. Владыко, Е. А. Аникевич, Л. М. Минаков. 2015. С. 1209–1215.

## CRITERIA FOR THE EFFICIENCY OF THE FIELD POWER SUPPLY SYSTEM

Asanin A. V.<sup>4</sup>, Ivanov V. G.<sup>5</sup>, Ivanishko A. N.<sup>6</sup>

**Keywords:** system efficiency, system criteria, voltage, power, hourly consumption.

### Abstract

**The purpose of the work** is to substantiate the criteria for the efficiency of a field power supply system for special purposes.

**Research method:** the methodological basis of the research is the general theory of systems using the methods of system analysis. The reliability of the results is ensured by the correctness of the problem statements, the adequacy of the applied research methods to the tasks to be solved and the consistency of the results obtained with the data of previous studies, the consistency of the theoretical estimates obtained with the results of analytical calculations.

**Results of the study:** the criteria for the efficiency of the field power supply system are selected and substantiated. As an economic criterion for the efficiency of the system, the hourly fuel consumption is taken, the criterion of technical efficiency is estimated by the sum of the volumes and masses of the elements of the field power supply system. The time of continuous operation is taken as a complex (generalized) technical and economic criterion. This criterion allows to assess the economic and technical level of field power supply devices power supply system, compare them with the functional capabilities and determine their expedient limit of improvement.

**Scientific novelty:** consists in the development of substantiated criteria for the efficiency of a field power supply system for special purposes, taking into account its use for power supply of field military communications.

### References

1. Jelektrosnabzhenie telekommunikacionnyh sistem, stacionarnyh i polevyh uzlov svjazi / A. V. Mjakotin, D. Ju. Zamazij, E. A. Kordjukov, N. M. Mel'nikov, N. G. Sysoev, D. B. Shljahtenko, pod red. A. V. Mjakotina. – SPb.: VAS, 2018. – 408 s.: il.
2. Vorob'ev A. Ju. Jelektrosnabzhenie komp'juternyh i telekommunikacionnyh sistem. – M.: Jeko-Trendz, 2002.
3. Romanov N. V., Aleksashkin A. A. Jenergetika dlja vojsk // Armejskij sbornik. 2021. № 8. S. 100–110.

4 Anton V. Asanin, Ph.D. of Technical Sciences, Associate Professor, Dean of the Faculty of Engineering, Federal State Budgetary Military Educational Institution of Higher Education «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. Mikhaylik», Khimki, Russia. E-mail: asanin-anton@mail.ru

5 Vasily G. Ivanov, Dr.Sc. of Military Sciences, Associate Professor, Professor of the Department of Informatics and Computer Engineering, Federal State Budgetary Military Educational Institution of Higher Education «Academy of Civil Protection of the Ministry of the Russian Federation for Civil Defense, Emergencies and Elimination of Consequences of Natural Disasters named after Lieutenant General D. I. Mikhailik», Khimki, Russia. E-mail: wasj2006@yandex.ru

6 Alexander N. Ivanishko, Head of the Group of the Main Communications Directorate of the Armed Forces of the Russian Federation, Moscow, Russia. E-mail: GUS\_1@mil.ru

4. Osnovnye problemy i perspektivy razvitija ASJeS / Bartosh V. V., Vinogradenko A. M., Veselovskij A. P. // V sbornike: Problemy tehničeskogo obespečenija vojsk v sovremennyh uslovijah. Trudy III Mezhvuzovskoj nauchno-praktičeskoj konferencii. 2018. S. 136–140.
5. Zheleznjakov V. O., Matveev R. V., Mjakotin A. V. Spособ jelectrosnabzhenija polevyh ob#ektov material'no-tehničeskogo obespečenija // V sbornike: Aktual'nye problemy infotelekkommunikacij v nauke i obrazovanii. Mezhdunarodnaja nauchno-tehničeskaja i nauchno-metodičeskaja konferencija: sbornik nauchnyh statej v 2 tomah. pod. red. S. V. Bachevskogo, sost. A. G. Vladyko, E. A. Anikevich, L. M. Minakov. 2015. S. 1209–1215.



# ИСПОЛЬЗОВАНИЕ ДОПОЛНЕННОЙ РЕАЛЬНОСТИ В ПРОЦЕССЕ ОБУЧЕНИЯ В ВЫСШИХ УЧЕБНЫХ ЗАВЕДЕНИЯХ

Магера М. А.<sup>1</sup>

DOI:10.21681/3034-4050-2026-1-88-95

**Ключевые слова:** интерактивные образовательные технологии, трехмерная визуализация, пространственное мышление, персонализация обучения, системы управления обучением, когнитивная нагрузка, учебная аналитика, вовлечённость студентов, виртуальные лаборатории, мобильные приложения, смешанная реальность.

## Аннотация

**Цель работы:** анализ и разработка методики использования дополненной реальности (AR) в высшем образовании, позволяющей количественно оценивать влияние AR-инструментов на учебные результаты студентов, их когнитивную нагрузку и вовлечённость, а также в выработке рекомендаций по внедрению AR в учебный процесс.

**Метод исследования:** для проверки эффективности предложенной методики применён смешанный исследовательский дизайн: квази-эксперимент с контрольной группой, использовавшей традиционные учебные материалы, и экспериментальной группой студентов на практико-ориентированных курсах. Использовались до- и пост-тесты (уровни воспроизведения, применения, переноса знаний), стандартизированные опросники, сбор логов взаимодействия, а также качественные интервью преподавателей и студентов.

**Результаты исследования:** показали, что обучение с AR-инструментами значительно повышает нормированный прирост знаний по сравнению с традиционными материалами, а также ускоряет освоение процедурных навыков. При умеренной плотности AR-оверлеев субъективная когнитивная нагрузка и время выполнения заданий снижались. AR-подход стимулировал большую вовлечённость студентов и автономность обучения, что приводило к лучшей ретенции материалов. Эти тенденции сохранялись в разных дисциплинах.

**Научная новизна:** заключается в разработке воспроизводимого подхода к исследованию с применением xAPI-логирования для объективного сбора и анализа данных о взаимодействии студентов с AR-контентом. Кроме того, в ходе работы получены эмпирически обоснованные рекомендации по дизайну AR-интерфейсов, определяющие оптимальную плотность и типы информационных оверлеев для снижения когнитивной нагрузки и повышения удобства восприятия информации. Наконец, сформулированы практические рекомендации по эффективной интеграции AR-контента в учебный процесс, учитывающие особенности учебных дисциплин и позволяющие максимально использовать дидактический потенциал дополненной реальности в высшем образовании.

## Введение

Традиционные методы обучения часто не обеспечивают достаточной связи теории с практикой. Лекционные занятия и статичные учебники затрудняют понимание сложных явлений и структур, особенно пространственных или динамических, а лабораторные практикумы ограничены оборудованием и ресурсами. В таком контексте дополненная реальность (AR) выступает перспективным решением: она позволяет «наложить» интерактивные 3D-объекты и анимации на реальные объекты и среды, создавая безопасную «песочницу» для экспериментов. AR-проекты

поддерживают более интуитивное восприятие, активируют пространственное мышление и делают обучение более персонализированным. Поскольку современные студенты хорошо знакомы с мобильными устройствами и AR-приложениями, это открывает новые возможности обучения.

Под AR мы понимаем технологии, которые дополняют реальное пространство виртуальной информацией, например текстом, графикой, 3D-моделями, аудио/видео, в реальном времени [1]. В отличие от полностью виртуальной реальности (VR), где пользователь «окутан» цифровым миром, AR сохраняет

<sup>1</sup> Магера Марина Александровна, младший научный сотрудник, Военная академия связи, Санкт Петербург, Россия. E-mail: chapa1999@mail.ru



центральность физического окружения, лишь обогащая его слоем дополнительных данных. Понятие смешанной реальности (MR) обычно подразумевает динамическое взаимодействие реальных и виртуальных объектов, где пользователь может манипулировать и тем, и другим [2]. Технологии AR делятся по носителю: мобильная AR работает на смартфонах/планшетах, AR-HMD (head-mounted display) реализуется через очки или шлемы. Несмотря на различия в устройствах, основная цель одна: улучшить восприятие и понимание учебного материала путём наглядной визуализации и интерактивности.

Анализ литературы выявляет несколько ограничений текущих подходов. Во-первых, существует разрыв между теорией и практикой: студенты часто не имеют возможности безопасно и недорого воспроизводить сложные или опасные эксперименты, например, химические реакции, биологические диссекции, что снижает мотивацию и эффективность обучения. AR-технологии могут моделировать такие сценарии визуально и интерактивно, позволяя «практиковаться» без риска. Во-вторых, традиционные материалы плохо демонстрируют скрытые процессы и 3D-структуры, такие как молекулярное строение, анатомия органов. AR в реальном времени визуализирует «невидимое», что упрощает понимание.

Современные исследования подтверждают, что AR-поддержка обучения ведёт к лучшим результатам. AR-модели, совмещённые с реальным миром, создают более наглядную и симуляционную среду: динамическая визуализация облегчает интерпретацию сложных концепций и стимулирует активное усвоение материала [3]. AR-инструкции способствуют индивидуализации обучения, коллаборативному решению задач и развитию критического мышления. Кроме того, мобильные AR-приложения позволяют студентам учиться в любое удобное время, что повышает вовлечённость. Эти преимущества делают AR перспективным средством повышения эффективности обучения в вузах.

Цель работы: разработать и эмпирически обосновать методику применения дополненной реальности в высшем образовании, позволяющую количественно оценивать влияние AR-инструментов на учебные результаты, когнитивную нагрузку и вовлечённость студентов, а также разработать рекомендации по внедрению AR в учебный процесс.

Объект исследования: учебные действия студентов на лабораторных и практико-ориентированных курсах в вузах.

Предмет исследования: влияние конфигурации AR-интерфейса и сценариев использования дополненной реальности на ключевые показатели эффективности обучения: прирост знаний, когнитивная нагрузка, вовлечённость студентов.

### Решение поставленной задачи

Литература последнего десятилетия демонстрирует разнообразные положительные эффекты AR-поддержки. Во-первых, AR улучшает понимание трехмерных и абстрактных структур. Например, сложные молекулярные модели или анатомические объекты, трудные для изучения на плоских изображениях, становятся доступнее через интерактивные 3D-оверлеи. Методы на основе дополненной реальности повышают освоение пространственных отношений: учащиеся лучше понимают топографию и географию с помощью AR-песочницы, а в математике AR помогает визуализировать геометрические фигуры. Во-вторых, AR-технологии повышают развитие процедурных навыков. Например, в медицине симуляция операций или визуализация физиологических процессов через AR позволяют практиковаться без риска для пациентов. В курсе инженерии интерактивные инструкции по сборке оборудования становятся более наглядными. В результате обучающиеся демонстрируют более высокую точность выполнения практических заданий и лучшую переносимость знаний в реальные ситуации.

Объяснение эффективности AR лежит в теоретических моделях обучения. Согласно когнитивной теории мультимедиа (Mayer) [4], совмещение слов и изображений в пространственной близости снижает когнитивную нагрузку обучаемых. Дополненная реальность естественным образом следует принципам split-attention и modality effect [5], представляя информацию в разных модальностях и в контексте реального окружения. Согласно принципам конструктивизма и социально-конструктивистского подхода, усвоение знаний наиболее эффективно происходит в процессе активного конструирования смыслов обучающимся в контексте специфической деятельности и социального взаимодействия [6].

AR-инструменты создают «мир на лодках», где студент сам открывает правила

и закономерности, а преподаватель выступает наставником или помощником.

На сегодняшний день доступны разные платформы для разработки AR-контента:

- Мобильная AR: Google ARCore и Apple ARKit предоставляют возможности обнаружения плоскостей, отслеживания движения (SLAM) и рендеринга 3D-графики для Android и iOS соответственно.
- Маркерная AR: системы вроде Vuforia распознают специальные метки и закрепляют виртуальные объекты на них.
- AR Foundation (Unity): позволяет писать один код, работающий с ARCore/ARKit одновременно.
- AR-HMD: шлемы и очки расширенной реальности (Microsoft HoloLens, Magic Leap, Meta 2) дают более погружающий опыт благодаря встроенным дисплеям и сенсорам.
- WebAR: использует браузер смартфона (например, через WebXR API) без установки приложений.

Несмотря на успешные кейсы использования AR, в литературе отмечаются существенные пробелы. Многие эмпирические работы – это простое сравнение дополненной реальности с традиционными методами без глубокого анализа механизмов воздействия. Чаще всего эксперименты проводились в узких дисциплинах, что ограничивает обобщаемость выводов. Существует недостаток исследований, оценивающих долгосрочные эффекты AR и ретенцию знаний. Также выявлен дефицит интегрированных метрик: большинство работ измеряют только результаты тестов, игнорируя комплексную оценку когнитивной нагрузки, пользовательского опыта и образовательной аналитики. Это указывает на необходимость стандартизированных протоколов и учёта качественных данных наряду с количественными метриками. Необходимо проведение кросс-дисциплинарных исследований и сравнение разных конфигураций AR, таких как мобильная, HMD, плотность оверлеев и т.д., в повторяемых экспериментах.

Наша AR-система собрана из нескольких ключевых блоков, которые работают вместе, чтобы превратить обучение в интерактивное приключение:

- Контент-модуль: содержит образовательные объекты, текстовые инструкции, интерактивные проверки и интерактивные пошаговые процедуры.

- AR-движок: реализует технологию отслеживания и отрисовку оверлеев. Оверлеи включают подсказки, аннотации, пометки, 3D-стрелки навигации и прочие интерактивные элементы поверх реальных объектов.
- Интеграция с LMS: система связана с платформой управления обучением через SSO для аутентификации. Задания и AR-контент загружаются из LMS, а результаты передаются обратно. В идеале используются стандарты xAPI/SCORM для трекинга обучения.
- Аналитика: ведётся логирование взаимодействий и формируется панель преподавателя для мониторинга прогресса. Данные экспортируются для статистической обработки.

Благодаря такой модульной архитектуре система легко подстраивается под разные учебные задачи. Вот несколько примеров:

- Виртуальная лаборатория: полноценная симуляция эксперимента на столе, где студенты манипулируют виртуальной аппаратурой и наблюдают результаты.
- Интерактивные пособия по оборудованию: AR-навигатор по лабораторному оборудованию или расходникам: при наведении камеры на прибор появляются инструкции по его использованию, обозначаются важные детали.
- Навигация по кампусу: схематические AR-навигационные подсказки внутри зданий и кампуса для новых студентов, например маршрут до нужной аудитории, лаборатории или оборудования.
- Микропрактикумы с проверкой: небольшие пошаговые тренажёры, например сборка цепи, разборка механизма, где после каждого шага AR-оверлей оценивает правильность и выдаёт подсказку.

Таким образом, модульная архитектура позволяет гибко подбирать компоненты в зависимости от учебной задачи.

Исследование реализуется в рамках смешанного дизайна (mixed methods): комбинируются количественные квази-эксперименты и качественные методы с участием двух групп студентов:

- контрольная группа осваивает материал с использованием традиционных средств обучения;
- экспериментальная группа занимается по аналогичной программе, но с применением дополненной реальности.

Для повышения валидности и минимизации эффекта начальных различий между группами планируется применить перекрёстный дизайн. После первого этапа эксперимента группы поменяются условиями обучения, что позволит каждому участнику попробовать оба формата и обеспечит более надежное сравнение.

Для чистоты эксперименты необходимо выбрать 2–3 разных направления. Это позволит оценить, насколько универсальны выявленные эффекты от применения AR, и проверить переносимость методики между разными предметными областями.

В качестве инструментария можно использовать как мобильные AR-приложения, так и AR-HMD. Контент хранится в едином репозитории. Разрабатываются чек-листы для преподавателей с описанием процедур и критериев оценки.

Процедура эксперимента включает в себя несколько этапов: сначала всем участникам проводится тест для определения базового уровня знаний, далее обе группы проходят обучение: одна с AR, другая – традиционно, затем обе группы сдают тест для выявления количества полученных знаний. Спустя 2–4 недели проводится повторный тест, который оценивает, насколько хорошо усвоенный материал сохраняется в долговременной памяти и воспроизводится через определенный промежуток времени после обучения. Между тестами студенты заполняют опросники и участвуют в интервью о восприятии технологий.

Учебные результаты анализируются на основе результатов тестирования, которые разбиваются по уровню сложности вопросов. Вычисляется нормированный прирост для количественного сравнения эффективности обучения. Также оценивается длительность получения навыка и результаты теста по удержанию материала в долгосрочной памяти.

Помимо этого, собираются объективные данные во время выполнения заданий: время на задачу, число ошибок или неудачных попыток, количество запросов подсказок. Если возможно, собираются тепловые карты фокуса внимания, чтобы понять, какие элементы интерфейса привлекают внимание.

Существуют следующие метрики для получения качественно-количественных характеристик [7]:

- когнитивная нагрузка: многомерный опросник, широко используемый для оценки восприятия нагрузки.

- юзабилити и опыт: SUS (10-вопросный опросник) дает общую оценку удобства системы. Дополнительно можно применять UEQ (User Experience Questionnaire) для оценки UX-параметров.
- мотивация: IMI (Intrinsic Motivation Inventory) измеряет интерес, чувство компетентности, выбор поведения, расслабленность и внутреннюю мотивацию.
- присутствие/иммерсивность: IPQ (Igroup Presence Questionnaire) или похожие шкалы оценивают ощущение «эффекта присутствия» в смешанной среде.

С помощью лог взаимодействия собираются данные системного журнала, такие как число щелчков, длительность сессий, последовательности переходов между этапами. Эти данные используются для построения временных диаграмм и расчёта комплаенса (насколько студенты соблюдали последовательность инструкций).

Ключевым аспектом проектирования эффективных интерфейсов дополненной реальности является минимизация эффекта расфокусирования внимания. Для этого элементы контента, такие как текстовые пояснения и схемы, следует размещать в непосредственной близости от соответствующих объектов в физическом пространстве. Такой подход позволяет снизить избыточную когнитивную нагрузку, возникающую при необходимости перераспределять внимание между разрозненными источниками информации.

Важную роль играет соблюдение умеренной плотности оверлеев. Чтобы избежать визуальной перегрузки, интерфейс должен содержать только необходимые подсказки и аннотации, которые могут быть активированы по требованию пользователя или раскрываться поэтапно. Этот принцип тесно связан с концепцией пошагового раскрытия сложности, согласно которой сложную информацию следует представлять постепенно. Начинать рекомендуется с базовых уровней, последовательно переходя к более сложным заданиям и моделям, а также предоставляя адаптивные подсказки и подсветку ключевых элементов для поддержки пользователя.

Для обеспечения интуитивной понятности интерфейса необходимо придерживаться единого визуального языка. Это подразумевает использование согласованных иконок, графических обозначений и цветовых кодировок, где, например, один и тот же цвет

последовательно обозначает определенный тип объектов или функций. Дополнительную ясность в восприятии трехмерных сцен вносят наглядные указатели глубины, такие как тени, которые упрощают оценку расстояний.

Указанные принципы находятся в полном соответствии с когнитивно-психологическими рекомендациями в области мультимедийного обучения и направлены на минимизацию лишней нагрузки на рабочую память пользователя.

Для технической реализации образовательных AR-приложений рекомендуется использовать проверенный технологический стек. В качестве базовой платформы оптимальным выбором является Unity в связке с фреймворком AR Foundation, что обеспечивает кроссплатформенную разработку с одновременной поддержкой ARCore для Android и ARKit для iOS. Для сценариев, основанных на маркерах, может быть задействован специализированный движок Vuforia, в то время как для web-ориентированных решений подходят технологии WebAR, такие как фреймворк three.js в связке со стандартом WebXR.

Обеспечение воспроизводимости исследований и легкости развертывания требует формирования комплексного пакета воспроизводимости. Для каждого AR-сценария целесообразно хранить конфигурационные файлы в форматах JSON или YAML, которые описывают последовательность шагов и условия их выполнения, а также фиксировать версии используемого программного обеспечения и плагинов. Дополнительную открытость и проверяемость результатов обеспечивает размещение в открытых репозиториях исходного кода, сопровождаемого наборами тестовых данных, включающих учебный контент и примеры для валидации.

Для глубокой интеграции в образовательный процесс необходима связь AR-платформы с системами управления обучением (LMS), такими как Moodle или Canvas, через специализированные плагины. Автоматизировать сбор данных о взаимодействии студентов позволяет стандарт xAPI, с помощью которого действия обучающихся записываются в хранилище учебных записей (Learning Record Store). Это позволяет автоматически выгружать результаты обучения, такие как пройденные уровни сложности или ответы на встроенные квизы, в электронные зачетные книжки и карточки успеваемости.

Крайне важной составляющей разработки являются вопросы этики и безопасности. Участие студентов в любых активностях должно быть строго добровольным и основываться на принципе информированного согласия, а собираемые в процессе данные – обязательно анонимизироваться. Для минимизации рисков для здоровья, таких как «киберболезнь», следует ограничивать продолжительность сессий, обеспечивать высокую плавность графики и ограничивать интенсивность виртуальных движений. Наконец, необходимо обеспечивать доступность AR-контента для лиц с различными ограничениями, предусматривая альтернативные текстовые описания, субтитры и механизмы управления, не требующие точных жестов.

Проведенное исследование продемонстрировало ряд статистически значимых преимуществ применения дополненной реальности в высшем образовании. В экспериментальных группах наблюдалось значительное повышение успеваемости по сравнению с контролем. Студенты осваивали лабораторные процедуры быстрее и с меньшим количеством ошибок благодаря интерактивному визуальному контенту (что согласуется с другими исследованиями эффективности AR [8]).

При оптимальном дизайне интерфейса участники сообщали о меньшей умственной нагрузке. Таким образом, умеренная информационная плотность AR-оверлеев уменьшает субъективную когнитивную нагрузку и время выполнения учебных задач становится ниже, чем в контрольной группе.

Также был зафиксирован выраженный рост вовлеченности и внутренней мотивации. AR-сессии демонстрировали более высокие оценки по IMI и IPQ – студенты были более мотивированы и чувствовали себя «погружёнными» в процесс. Это совпадает с данными о повышении интереса и удержании информации при использовании AR [9]. Улучшилась и долговременная ретенция материала.

Полученные эффекты проявлялись во всех исследованных дисциплинах – химии, анатомии и информационных технологиях, – что говорит о широком кросс-дисциплинарном потенциале AR-технологий. Тем не менее, наибольший эффект наблюдался в практико-ориентированных дисциплинах.

Эти результаты демонстрируют, что применение AR-инструментов действительно даёт



количественные и качественные улучшения в обучении студентов вузов.

Несмотря на положительные результаты, необходимо отметить ряд ограничений, влияющих на внешнюю валидность работы. Хотя эксперимент охватил несколько дисциплин и типов устройств, остаётся вопрос о переносимости результатов на иные контексты, например, гуманитарные или публицистические дисциплины, где AR чаще используется иначе. Важно проверить, сохраняются ли эффекты на разных возрастных группах и уровнях подготовки.

Среди ключевых ограничений текущего исследования — его выборочный охват, обусловленный доступными ресурсами. Кроме того, нельзя полностью исключать потенциальное влияние эффекта новизны, когда использование AR-устройства могло искусственно повысить краткосрочную вовлечённость участников экспериментальной группы. Существенным барьером для широкого внедрения остается и проблема доступности оборудования, поскольку не все студенты имеют персональные AR-шлемы (HMD), что создаёт риски образовательного неравенства.

Проектирование образовательных AR-интерфейсов сопряжено с определёнными рисками, ключевым из которых является перегрузка пользователя информацией и визуальными эффектами. Чрезмерно плотная графика может вызвать усталость или «киберболезнь». Во избежание этого рекомендуются короткие сессии (10–15 мин) с перерывами, простые эффекты перехода, а также тестирование контента на разных пользователях.

Для успешной интеграции технологий дополненной реальности в учебный процесс рекомендуется использовать модель минимально жизнеспособного модуля (MVP). Рекомендуемая продолжительность цикла внедрения составляет 4–6 недель. В течение этого периода формируется конкретная учебная цель, создается базовый AR-контент, который может быть ограничен одной ключевой 3D-моделью, проводится необходимый инструктаж преподавателей и осуществляется пилотное тестирование с последующей сборкой обратной связи.

Реализация подобных проектов требует формирования междисциплинарной команды, где каждый участник вносит свой вклад

в общий результат. Преподаватель фокусируется на методической составляющей и содержательном наполнении модуля. Методист или координатор обеспечивает соответствие разработки образовательным стандартам и принципам педагогического дизайна. 3D-дизайнер отвечает за создание качественных и педагогически релевантных моделей, в то время как разработчик осуществляет их интеграцию в функциональное AR-приложение. Критически важную роль играет лаборатория или служба технической поддержки, которая обеспечивает проект необходимым оборудованием — смартфонами или AR-очками.

Экономическое обоснование проекта требует тщательного анализа затрат и ожидаемого эффекта. К первоначальным инвестициям относятся закупка устройств, разработка цифрового контента и обучение персонала. Но при повторном использовании моделей и масштабировании на новые курсы эти инвестиции окупаются за счёт сокращения штучных опытов и повышения качества обучения. Создание библиотеки AR-моделей по предмету снижает дальнейшие расходы. Отчетность на базе xAPI поможет аргументировать ценность AR для администрации учебного заведения.

### Заключение

В работе предложена комплексная методика интеграции дополненной реальности в высшее образование, подкреплённая теоретическими выкладками, моделью эксперимента и конкретными рекомендациями. Показано, что AR-технологии позволяют преодолеть разрыв между теоретической и практической подготовкой студентов, делая обучение более наглядным, безопасным и мотивирующим. Полученные результаты подтверждают эффективность AR для повышения успеваемости, снижения когнитивной нагрузки и роста вовлечённости.

Направления дальнейших исследований: включают разработку адаптивных подсказок с искусственным интеллектом (персонализированных наставников), расширение аналитики для автоматической диагностики навыков и интеграцию AR с AI-тренерами и автогенерацией учебного контента. Таким образом, AR имеет потенциал стать не просто дополнением, но неотъемлемой частью современных цифровых образовательных экосистем.

### Литература

1. Маслова Ю. А., Белов Ю. С. Технологии дополненной реальности // E-Scio. 2022. № 2(65), С. 313-322.
2. Паскова А. А. Особенности применения иммерсивных технологий виртуальной и дополненной реальности в высшем образовании // Вестник Майкопского государственного технологического университета. 2022. № 3, С. 83–92.
3. Итинсон К. С. Перспективы и возможности применения инновационных интерактивных технологий: дополненная реальность в обучении студентов в высших учебных учреждениях // БГЖ. 2020. № 1(30), С. 67–70.
4. Барашян В. К., Симонова О. Б. Теория мультимедийного обучения Майера. Теория и практика // Гуманитарные и Социальные науки. 2024. № 4. С. 133–138. DOI: 10.18522/2070-1403-2024-105-4-133-138
5. Хлыбова М. А. Анализ принципов мультимедийного обеспечения электронного обучения // Проблемы современного педагогического образования. 2024. № 85-1. С. 364–366.
6. Трухачева Н. В., Пупырев Н. П., Кирколуп Е. Р. Конструктивизм и его основные идеи в качестве руководящих принципов разработки учебных программ // Преподаватель XXI век. 2017. № 1-1. С. 158–166.
7. Buchner J., Buntins K., Kerres M. The Impact of Augmented Reality on Cognitive Load and Performance: A Systematic Review // Journal of Computer Assisted Learning. – 2021. – Т. 38, № 1, С. 285–303.
8. Данилова Т. В., Бурыкина М. Ю., Крамарева И. Е. Использование виртуальной и дополненной реальности в высшем образовании // Управление образованием: теория и практика. 2024, № 14, С. 133–142.
9. Chang H.-Y., Binali T., Liang J.-C., Chiou G.-L., Cheng K.-H., Lee S. W.-Y., Tsai C.-C. Ten Years of Augmented Reality in Education: A Meta-Analysis of (Quasi-) Experimental Studies // Computers & Education. – 2022. – Т. 191, С. 104641.

## THE USE OF AUGMENTED REALITY IN THE PROCESS OF LEARNING IN HIGHER EDUCATIONAL INSTITUTIONS

**Magera M. A.<sup>2</sup>**

**Keywords:** *interactive educational technologies, three-dimensional visualization, spatial thinking, personalization of learning, learning management systems, cognitive load, educational analytics, student engagement, virtual laboratories, mobile applications, mixed reality.*

### Abstract

**The purpose of the work** is to analyze and develop a methodology for using augmented reality (AR) in higher education, which allows to quantify the impact of AR tools on students' learning outcomes, their cognitive load and involvement, as well as to develop recommendations for the implementation of AR in the educational process.

**Research method:** to test the effectiveness of the proposed methodology, a mixed research design was used: a quasi-experiment with a control group using traditional educational materials and an experimental group of students on practice-oriented courses. Pre- and post-tests (levels of reproduction, application, transfer of knowledge), standardized questionnaires, collection of interaction logs, as well as high-quality interviews of teachers and students.

**Results of the study:** showed that learning with AR tools significantly increases the normalized growth of knowledge compared to traditional materials and also accelerates the development of procedural skills. With a moderate density of AR overlays, subjective cognitive load and task completion time decreased. The AR approach stimulated greater student engagement and autonomy of learning, which led to better retention of materials. These trends persisted across disciplines.

**The scientific novelty** consists in the development of a reproducible approach to the study using xAPI-logging for the objective collection and analysis of data on the interaction of students with AR content. In addition, in the course of the work, empirically substantiated recommendations on the design of AR interfaces were obtained, determining the optimal density and types of information overlays to reduce cognitive load and increase the convenience of perceiving information recommendations for the effective integration of AR content into the educational process, taking into account the specifics of academic disciplines and allowing you to maximize the didactic potential of augmented reality in higher education.

<sup>2</sup> Marina A. Magera, Junior Researcher, Military Academy of Communications, St. Petersburg, Russia. E-mail: chapa1999@mail.ru

### References

1. Maslova Ju. A., Belov Ju. S. Tehnologii dopolnennoj real'nosti // E-Scio. 2022. № 2(65), S. 313–322.
2. Paskova A. A. Osobennosti primeneniya immersivnyh tehnologij virtual'noj i dopolnennoj real'nosti v vysshem obrazovanii // Vestnik Majkopskogo gosudarstvennogo tehnologicheskogo universiteta. 2022. №3, S. 83–92.
3. Itinson K. S. Perspektivy i vozmozhnosti primeneniya innovacionnyh interaktivnyh tehnologij: dopolnennaja real'nost' v obuchenii studentov v vysshih uchebnyh uchrezhdenijah // BGZh. 2020. № 1(30), S. 67–70.
4. Barashjan V. K., Simonova O. B. Teorija mul'timedijnogo obuchenija Majera. Teorija i praktika // Gumanitarnye i Social'nye nauki. 2024. № 4. S. 133–138. DOI: 10.18522/2070-1403-2024-105-4-133-138/
5. Hlybova M. A. Analiz principov mul'timedijnogo obespechenija jelektronnogo obuchenija // Problemy sovremennogo pedagogicheskogo obrazovanija. 2024. № 85-1. S. 364–366.
6. Truhacheva N. V., Pupyrev N. P., Kirkolup E. R. Konstruktivizm i ego osnovnye idei v kachestve rukovodjashih principov razrabotki uchebnyh programm // Prepodavatel' XXI vek. 2017. № 1-1. S. 158–166.
7. Buchner J., Buntins K., Kerres M. The Impact of Augmented Reality on Cognitive Load and Performance: A Systematic Review // Journal of Computer Assisted Learning. – 2021. – T. 38, № 1, S. 285–303.
8. Danilova T. V., Burykina M. Ju., Kramareva I. E. Ispol'zovanie virtual'noj i dopolnennoj real'nosti v vysshem obrazovanii // Upravlenie obrazovaniem: teorija i praktika. 2024, № 14, S. 133–142.
9. Chang H.-Y., Binali T., Liang J.-C., Chiou G.-L., Cheng K.-H., Lee S. W.-Y., Tsai C.-C. Ten Years of Augmented Reality in Education: A Meta-Analysis of (Quasi-) Experimental Studies // Computers & Education. – 2022. – T. 191, S. 104641.



# ПОДВИЖНЫЙ УЗЕЛ СВЯЗИ НАРОДНОГО КОМИССАРИАТА СВЯЗИ СССР: ОПЫТ СТРОИТЕЛЬСТВА ОБЪЕКТА 04, ФОРМИРОВАНИЯ И ПРИМЕНЕНИЯ ПОЕЗДА СВЯЗИ № 1

Шептура В. Н.<sup>1</sup>

DOI:10.21681/3034-4050-2026-1-96-107

**Ключевые слова:** система военной связи, объект связи, поезд связи, Народный комиссариат связи СССР, Главное управление связи Красной армии.

## Аннотация

**Целью статьи** является обобщение исторического опыта строительства и боевого применения объекта 04 (поезда связи № 1) и формулирование выводов и предложений по его использованию в современных условиях.

**Метод исследования** историко-генетический, предполагает последовательное изучение исторических фактов, их обобщение и выработка практических предложений и рекомендаций, актуальных для современного процесса развития системы и войск связи.

**Результаты исследования:** в статье изучен опыт сооружения подвижного узла связи Народного комиссариата связи СССР (объект 04), формирования и применения поезда связи № 1 в годы Великой Отечественной войны. Особое внимание в публикации уделено обобщению материалов архивных источников по организационным и техническим особенностям создания подвижного узла связи на базе железнодорожного подвижного состава. Обобщен опыт создания, формирования и применения подвижного узла связи стратегического звена управления и выработаны практические рекомендации по совершенствованию боевого применения войск связи.

**Научная новизна и практическая полезность** заключается в том, что впервые введены в научный оборот архивные материалы по строительству Объекта 04 (поезда связи № 1) и проведено описание выполнения им первой боевой задачи по обеспечению связи Генеральному штабу Красной армии.

## Введение

Неудачи Красной армии в начальный период Великой Отечественной войны показали, что связь играет важную роль в обеспечении управления войсками, организации взаимодействия между воинскими частями, соединениями и объединениями и имеет фундаментальное значение для успеха в военных действиях [1, с. 73, 74].

Динамика ведения боевых действий, быстрота изменения оперативной обстановки, решение самостоятельных задач, возлагаемых на отдельно действующих в тылу и на флангах воинских формирований, вызвали объективную необходимость поиска путей для создания мобильных, надежных и типовых средств связи [2, 152–155]. Вместе с тем разработка новых средств связи, по своим тактико-техническим характеристикам соответствующих требованиям управления войсками, задачам, масштабу, уровню материально-технического

обеспечения и маневренному характеру ведения военных действий, потребовала определения наиболее целесообразных способов их боевого применения в системе связи объединения [3].

Заметим, что вопросам организации и обеспечения связи в годы войны и применения подвижных узлов связи пунктов управления в настоящее время посвящено целый ряд работ [4, 5, 6, 7], однако в них не рассмотрен опыт сооружения подвижного узла связи Народного комиссариата связи СССР – объекта 04 (поезда связи № 1) и особенности его технической эксплуатации. Данная статья приоткрывает завесу таинственности по созданию данного объекта связи, его формированию как воинской части – поезда связи № 1, сыгравшей важную роль в обеспечении связи Генеральному штабу Красной армии и обогатившей теорию и практику военной связи и применения воинских формирований связи.

<sup>1</sup> Шептура Владимир Николаевич, кандидат военных наук, доцент, член-корреспондент Российской академии ракетных и артиллерийских наук, старший научный сотрудник Научно-исследовательского института (военной истории) Военной академии Генерального штаба Вооруженных Сил Российской Федерации, г. Москва, Россия. E-mail: sheptura\_vn@mail.ru



### Строительство объекта 04

Седьмого июля 1941 г. народный комиссар связи СССР И. Т. Пересыпкин обратился к председателю Государственного комитета обороны СССР И. В. Сталину с докладной запиской о необходимости создания дополнительного резерва связи и организации подвижного узла связи (поезда связи) [8, с. 457–472]<sup>2</sup>. На следующий день (8 июля) постановлением Государственного Комитета обороны СССР (ГКО) № ГКО-59-сс было принято решение о сооружении подвижного узла связи, содержащего комплекс автономных телеграфных, телефонных и радиосредств связи, смонтированных в железнодорожном составе с приданной энергобазой и необходимыми средствами для развертывания линейно-кабельных подходов. Непосредственное строительство объекта связи, как единого комплексного сооружения, было поручено Народному комиссариату связи СССР (НКС). Срок завершения основных монтажных и строительных работ определялся в течение 25 суток. Подвижный железнодорожный состав, переоборудованный для нужд подвижного узла связи, так же, как и энергобазу, в соответствии с постановлением ГКО должен был представить Народный комиссариат путей сообщения (НКПС) в течение 10 суток (рис. 1)<sup>3</sup>.

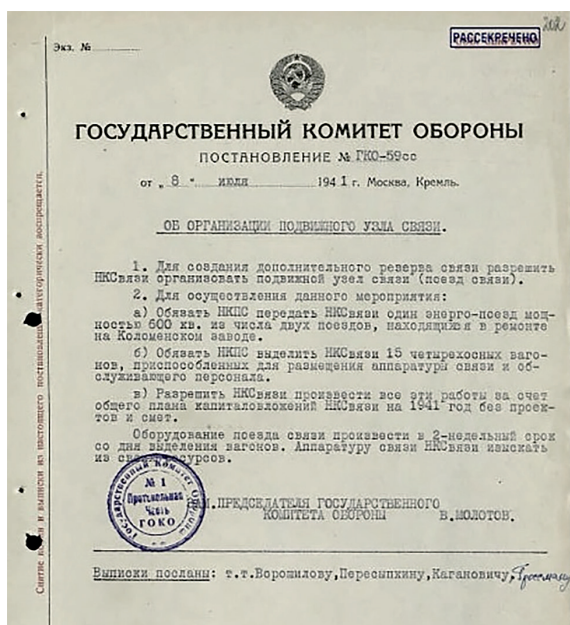


Рис. 1. Постановление Государственного Комитета обороны СССР от 8 июля 1941 г. № ГКО-59-сс «Об организации подвижного узла связи»

- 2 Российский государственный архив социально-политической истории (РГАСПИ). Ф. 644. Оп. 2. Д. 2. Л. 93, 94.  
3 РГАСПИ. Ф. 644. Оп. 1. Д. 1. Л. 202.

Перед связистами была поставлена сложная задача – в кратчайшие сроки создать мощный, быстро развертываемый подвижный узел связи, отвечающий своими тактико-техническими свойствами всем условиям ведения войны. При этом необходимо было учесть специфические особенности боевого применения такого подвижного узла связи:

- функционирование объекта связи не должно осуществляться вблизи населенных пунктов или промышленных центров с достаточными по мощности и стабильности источниками энергии;
- большая уязвимость энергетических объектов в условиях интенсивности воздействия средств воздушного нападения противника<sup>4</sup>.

9 июля 1941 г. приказом НКС № 39-с была организована Дирекция строительства Объекта 04 (поезда связи № 1). Основной задачей Дирекции являлось своевременное выполнение постановления ГКО. Сооружение необычного объекта (подвижного узла связи – поезда связи № 1) осуществлялось в г. Москве и на железнодорожной станции Гжель Казанской железной дороги. Причем, строительство поезда разрешалось осуществлять без предварительного утверждения проекта и сметной документации. По существу, все работы производились по эскизным рабочим чертежам и наброскам, выдаваемым инженерно-техническому составу подрядных организаций, непосредственно в цехах, на месте – по ходу самой работы.

Монтажные работы по основным техническим узлам производились монтерами, техниками и инженерами следующих организаций:

- радиоузел – работниками треста «Радиострой»<sup>5</sup>;
- телеграф, телефонный узел и узел генераторный и аккумуляторный – работниками треста «Межгорсвязьстрой»<sup>6</sup>;
- энергобаза – работниками завода «Динамо» [9, с. 411]<sup>7</sup>;
- подвижный железнодорожный состав – работниками завода НКПС им. 1905 года.

4 Центральный архив Министерства обороны Российской Федерации (ЦАМО РФ). Ф. 71. Оп. 12177. Д. 17. Л. 254.

5 Всесоюзный государственный трест по проектированию, строительству и монтажу радиостанций (Радиострой) Радиопромышленности Народного комиссариата связи СССР.

6 Всесоюзный государственный трест строительства сооружений междугородной проволочной связи Народного комиссариата связи СССР.

7 Московский электромашиностроительный завод «Динамо» им. С.М. Кирова Главного управления электромашиностроительной промышленности СССР Народного комиссариата электростанций СССР.

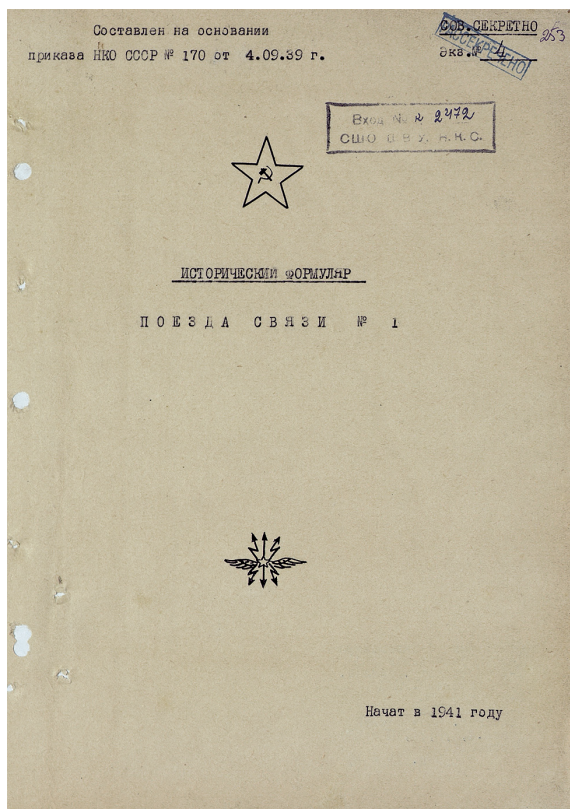


Рис. 2. Обложка Исторического формуляра поезда связи № 1. ЦАМО РФ. Ф. 71. Оп. 12177. Д. 17. Л. 253.

В Историческом формуляре поезда связи № 1 отмечено, что: «...Указанные сроки монтажа были выдержаны благодаря широко развернутому фронту параллельно ведущихся работ и исключенной напряженной работе коллектива Строительства, трудовой энтузиазм которого являлся частицей общего подъема, отражая как в капле воды поток трудовых подвигов великих дней Отечественной войны» (рис. 2)<sup>8</sup>.

По завершении монтажных работ начался период механической регулировки аппаратуры и контрольной проверки электрических цепей. Подвижной состав, оборудованный в соответствии с требованиями Дирекции строительства, НКПС предоставил для монтажа к 25 июля. Ровно через 15 суток с момента получения переоборудованного подвижного состава (т.е. к 10 августа 1941 г.) Дирекцией строительства были закончены

основные монтажные и строительные работы по всему комплексу сооружения.

В 06.00 11 августа 1941 г. приехавшим на место строительства – станцию Гжель, заместителю НКО И. Т. Пересыпкину и заместителю НКС А. А. Конюхову, Дирекция строительства представила законченный монтажом и оборудованный всеми основными средствами связи Объект 04.

15 августа 1941 г. Метростроем НКПС была предоставлена подвижная электростанция, предназначенная в качестве основного источника энергоснабжения поезда и вспомогательной тяговой силы.

Приданная поезду энергобаза включала:

- один тепловоз типа ЭЛ-46 с двигателем дизеля мощностью 1025 л.с. и генератором на 635 кВт;
- один вагон с высоковольтным и низковольтным распределительным устройствами;
- один вагон со вспомогательным оборудованием;
- один вагон-цистерну для горючих и смазочных материалов;
- один жилой вагон для обслуживающего персонала, переоборудованный и приспособленный под штаб поезда.

Всего поезд по окончании строительного-монтажных работ включал в своем составе один тепловоз и 25 четырехосных вагонов (рис. 3).

При сооружении Объекта 04 были применены передовые технологические, технические и производственные решения, которыми обладали в то время советские инженеры и практики строительства общегосударственной сети связи. Особенностью строительства

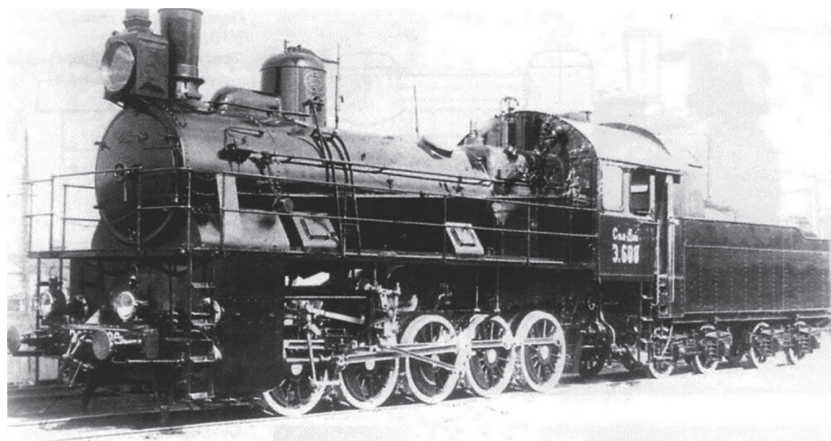


Рис. 3. Тепловоз серии Эл

<sup>8</sup> ЦАМО РФ. Ф. 71. Оп. 12177. Д. 17. Л. 660.



объекта связи являлось то, что подвижный узел связи представлял собой комплекс стационарных устройств различных видов связи, размещенных в железнодорожных вагонах, работающих на дальнее расстояние, с использованием мощных линейных сооружений существующих магистральных и местных сетей НКС и НКО, подготавливаемых к обслуживанию командного пункта фронта или армии.

По замыслу разработчиков поезд связи № 1 должен был обеспечивать телеграфную, телефонную и радиосвязь в любых условиях обстановки и применяться не только централизованно (в составе объекта связи), но и децентрализованно (отдельными элементами).

При этом от подвижного узла связи должностным лицам пункта управления телеграфная связь должна предоставляться:

- магистральная двухсторонняя, осуществляемая буквопечатающими аппаратами Бодо и СТ-35 по дуплексной схеме, с неограниченным радиусом действия при использовании трансляций;
- областная и местная, осуществляемая буквопечатающими аппаратами СТ-35 и по коду Морзе по симплексной схеме с радиусом действий до 600 км.

Одновременно на телеграфе может быть задействовано 8 дуплексных связей на двухкратных аппаратах Бодо, одна дуплексная и 5 симплексных связей на аппаратах СТ-35 и 2 полудуплексных связи и 8 симплексных, на аппаратуре Морзе. При необходимости любой из аппаратов Морзе или СТ-35 может быть заменен аппаратом Тремля или Шорина. Среднесуточный обмен обеспечивается порядка 6000 тридцатисловных телеграмм по аппаратуре Бодо, 1300 телеграмм по аппаратуре СТ-35 и 1000 телеграмм по аппаратуре Морзе<sup>9</sup>. Состав телеграфа представлен на рисунке 4.

При монтаже телефонного оборудования технологически закладывалась возможность обеспечения телефонной связи:

- междугородняя, осуществляемая через междугороднюю телефонную станцию и линейный аппаратный зал (ЛАЗ) поезда, с использованием каналов как тональной, так и высокой частоты с неограниченным радиусом действия на оборудованных трансляциями медных магистралях и действием в пределах области по стальным цепям;

- местная, в пределах населенного пункта по месту расположения поезда, осуществляемая через телефонную станцию ручного обслуживания (РТС) городского типа;
- внутренняя, для связи между собой подразделений поезда, осуществляемая через ту же и ряд коммутаторных установок специального назначения.

Производственная мощность междугородной телефонной связи определялась возмож-

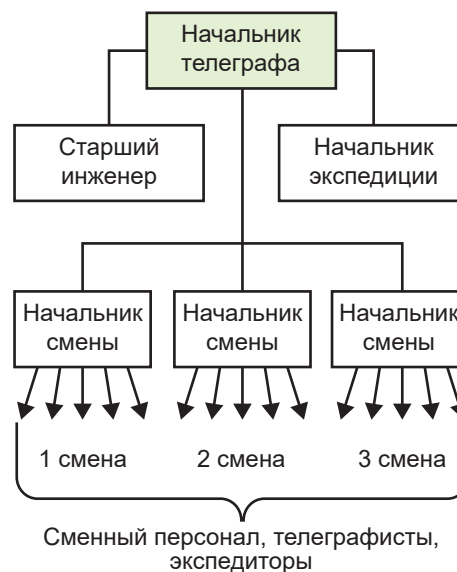


Рис. 4. Состав телеграфа поезда связи № 1

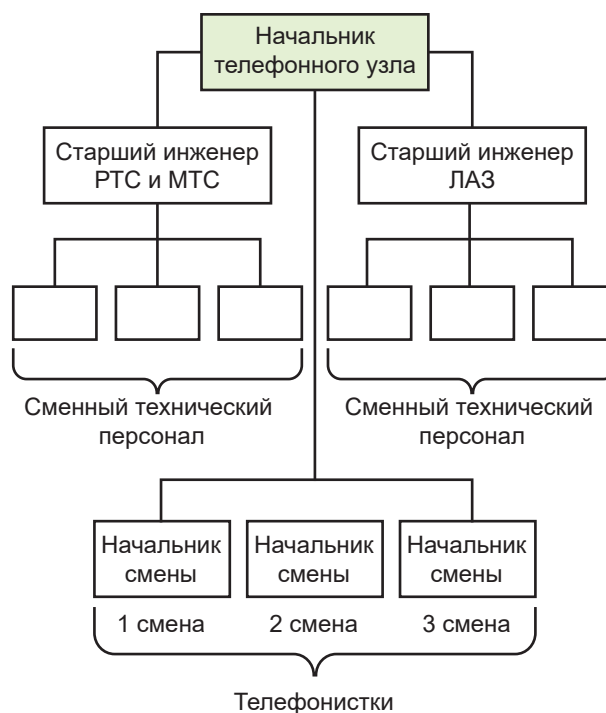


Рис. 5. Состав телефонного узла поезда связи № 1

9 ЦАМО РФ. Ф. 71. Оп. 12177. Д. 17. Л. 14.

ностью одновременного задействования на междугородной станции поезда до 20 связей. Эти связи могли осуществляться как целиком по физическим цепям, так и с использованием оборудуемых в ЛАЗ каналов. Пользование междугородной связью обеспечивалось любому абоненту РТС по заказной системе и 30 прямым абонентам МТС по системе немедленного соединения. При этом прямым абонентом МТС может быть как подчиненная телефонная станция, так и отдельное лицо, имеющее прямой аппарат ЦБ. Станция местной телефонной связи может принять до 500 внешних абонентов в радиусе до 8 км при кабельной телефонной сети. Состав телефонного узла представлен на рис. 5.

Большое значение при сооружении объекта было уделено техническим вопросам организации радиосвязи. Так, имеющимися в составе поезда радиосредствами предусматривалось строительство следующих линий радиосвязи:

- магистральная, осуществляемая передатчиками РК-15 и приемниками КТФ-1 или КВТ, допускающая быстрое действующий пишущий обмен, слуховой обмен и радиотелефонные переговоры с радиусом действия около 8000 км для телеграфного и 2000 км для телефонного обмена на приданных поезду антеннах. При использовании направленных антенн постоянного типа дальность действия радиосвязи может быть увеличена до пределов территории СССР;
- областная, осуществляемая передатчиками РК-1 и РАТ-1 и приемниками КВТ или Хаммерлунд, допускающие те же виды обмена в радиусе 2000 км для телеграфной и 500–600 км для телефонной работы;
- местная, осуществляемая приемо-передающей радиостанцией типа МРК-0,05Ф, в радиусе порядка 400 км для телеграфного обмена и 100 км для телефонных переговоров;
- специальная, допускающая ведение вещательных передач по любому передатчику и по местной сети проводного вещания с общей мощностью репродукторов до 500 Вт<sup>10</sup>.

Оборудование радиоузла поезда могло обеспечивать одновременную работу 2-х магистральных, 2-х областных и 1-го местного каналов передачи и 8 каналов приема (рис. 6).

<sup>10</sup> ЦАМО РФ. Ф. 71. Оп. 12177. Д. 17. Л. 14.

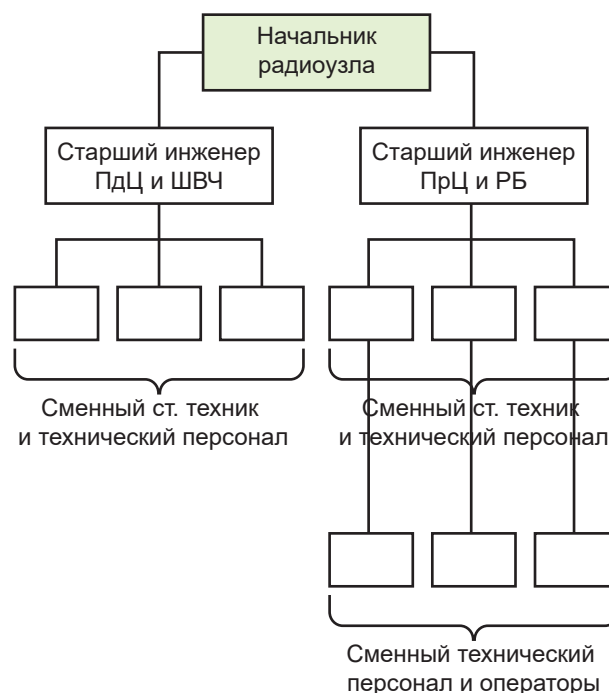


Рис. 6. Состав радиоузла поезда связи № 1

Работа радиоузла организовывалась произвольным сочетанием соответствующего количества видов радиосвязи, допускаемых наличием манипуляционной аппаратуры (табл. 1)<sup>10</sup>.

Таблица 1.  
Производственные возможности поезда связи № 1  
по ведению радиообмена

Виды радиообмена	Количество каналов манипуляции
Быстродействующий пишущий обмен	3
Слуховой обмен	4
Радиотелефонные переговоры	2
Радиовещание	2

В целом устойчивость работы подвижного узла связи при задействовании полного комплекса оборудования поезда обеспечивалась возможностью взаимного дублирования различных видов связи. Так, средства проводной связи на магистральной, областной и местной связях предусматривалось резервировать радиосвязями и наоборот. Телеграфная связь – дублировалась телефонной и наоборот. При этом не исключалась возможность автономной работы различных видов связи.



Подобный принцип резервирования был реализован в организации отдельных подразделений поезда связи № 1. Так, центральный коммутационный узел телеграфа и часть аппаратуры сосредоточенные в одном вагоне, дублировались резервным линейно-батареинным коммутатором и телеграфной аппаратурой, размещенными в другом вагоне. Выбытие из строя вагона с междугородной телефонной станцией не прекращало вовсе междугородной телефонной связи, организуемой в этом случае через резервный коммутатор в вагоне, где расположены ЛАЗ и РТС. Мощные радиопередатчики размещались в двух разных вагонах и полностью взаимозаменяемы. Энергоснабжение поезда собственной энергобазой резервировалось внешним электропитанием (рис. 7).

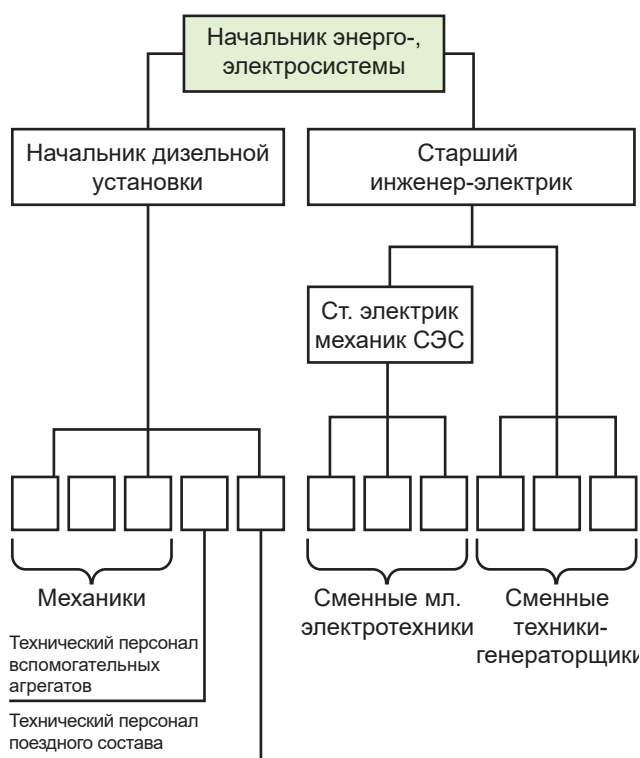


Рис. 7. Состав энерго-, электросистемы поезда связи № 1

Обеспечение максимальной подвижности поезда исключало возможность перевозки громоздкого линейного имущества связи (рис. 8). Поэтому устройство обходных линий (кольцевание), подводка к месту стоянки объекта шлейфов телеграфно-телефонных магистралей и кабелей местной (городской) телефонной сети, постройка соединительных

линий между поездом и существующими стационарными станциями связи, а также соединительных линий между приемным центром и радиобюро, было возложено на специальные батальоны связи или местные органы НКС и выполнялись их силами и средствами.

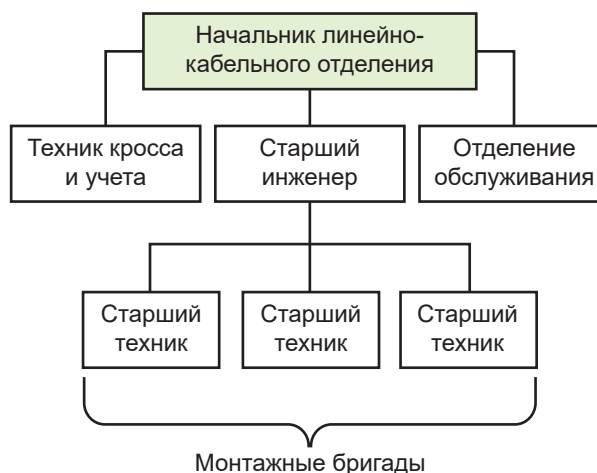


Рис. 8. Состав линейно-кабельного отделения поезда связи № 1

Необходимо отметить, что на протяжении всего периода проведения строительно-монтажных работ поезда И. Т. Пересыпкин оказывал большую практическую помощь и держал на жестком контроле сроки сооружения объекта связи.

В соответствии со штатом № 014/4, утвержденным 15 августа 1941 г. заместителем НКО армейским комиссаром 1-го ранга Е. А. Щаденко (рис. 9) основными подразделениями поезда связи № 1 являлись телеграф, телефонный узел, радио узел, энерго-электро система и линейно-кабельное отделение (рис. 10).



Рис. 9. Армейский комиссар 1-го ранга Е. А. Щаденко

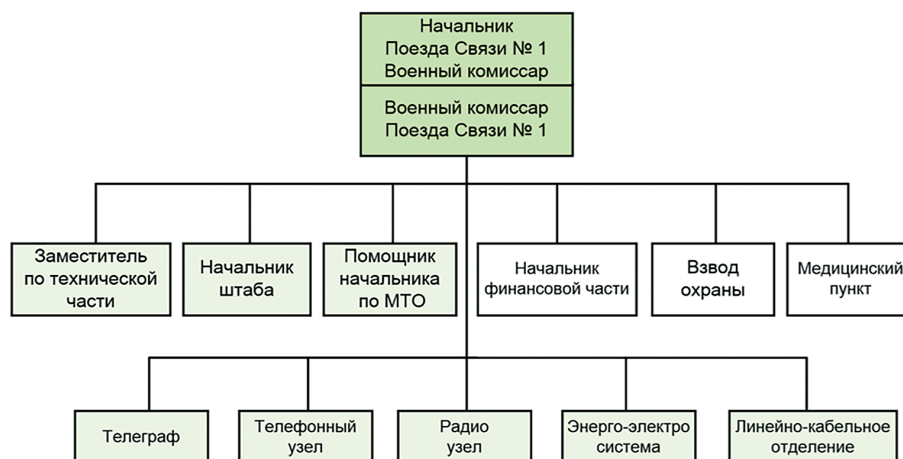


Рис. 10. Состав поезда связи № 1 (сентябрь 1941 г.)

В соответствии с приказом заместителя НКО И. Т. Пересыпкина и директивы Главного управления формирования и укомплектования войск Красной армии от 17 августа 1941 г. № 2-орг/5/5391 воинская часть была направлена для формирования в Приволжский военный округ в г. Пенза. В 24.00 25 августа поезд в полном составе отбыл со станции Гжель в свой первый рейс – в г. Пензу для формирования воинской части. В качестве официального наименования за воинской частью было закреплено уже привычное, хотя и не вполне точное, название «Поезд связи № 1». На протяжении всего периода формирования воинская часть находилась в непосредственном подчинении Центрального военного управления (ЦВУ) НКС и в состав какого-либо соединения не входила.

На основании предписания ЦВУ НКС от 23 августа 1941 г. № 989 формирование воинской части персонально было возложено на начальника строительства поезда связи военинженера 2 ранга В. И. Менделюкова (рис. 11).



Рис. 11. Начальник поезда связи № 1 военинженер 2 ранга В.И. Менделюков

Основными источниками формирования воинской части командным и начальствующим составом являлись Московские эксплуатационные и проектно-монтажные организации связи: проект «Связьстрой» дворца Советов<sup>11</sup>, на базе которого в свое время была организована Дирекция строительства Объекта 04; Московский центральный телеграф; трест «Радиострой» Главстройсвязи НКС.

Для формирования основного состава подразделений поезда связи № 1, по указанию ЦВУ НКС были использованы кадры управлений связи: Пензенской, Куйбышевской, Казанской и Саратовской областей. Данный состав был отобран через ЦВУ НКС в период с 24 августа по 18 сентября 1941 г. В это же время осуществлялось формирование и вспомогательных подразделений поезда: взвода охраны; части материально технического обеспечения, финансовой, санитарной и др. частей. Основными источниками формирования вспомогательных подразделений являлись Пензенский областной военный комиссариат и районные военные комиссариаты Пензенской области. В Пензе поезд дислоцировался в районе песчаного карьера (называемой пензенцами «Манчжурия») на вспомогательных путях, примыкающих к станции Пенза-III.

Необходимо отметить, что одновременно с формированием воинской части, продолжали выполняться пуско-наладочные работы и мероприятия, направленные на обеспечение технической готовности объекта. Так,

<sup>11</sup> Проект строительства высотного административного здания в Москве для проведения сессий Верховного Совета Союза ССР и массовых демонстраций. По плану архитектора Б. М. Иофана, высота Дворца Советов вместе с венчающей его стометровой статуей Владимира Ленина составляла 415 м. Дворец должен был стать центром новой советской Москвы и самым высоким зданием в мире, символизирующим победу социализма.

на базе произведенной на станции Гжель механической регулировки аппаратуры, осуществлялось устранение отдельных дефектов монтажа изделий, настройка комплексов оборудования (станций) и приемка их в эксплуатацию. Завершение настроечных и регулировочных работ по существу производилось уже формирующимся штатом поезда связи № 1, так как от строительно-монтажных организаций присутствовали лишь одиночные представители – преимущественно прорабы и старшие инженеры отдельных участков, оставленные для сдачи оборудования и инвентаря обслуживающего персонала.

Сочетание процессов формирования воинской части с основными настроечными работами было с организационной стороны наиболее напряженным периодом. Вместе с тем усложнение управленческих процессов в ходе ввода объекта в эксплуатацию существенно не повлияло на решение главной задачи – своевременного формирования воинской части. Это позволило одновременно с проведением опытной проверки оборудования и сдачей его в эксплуатацию, привить личному составу элементарные воинские навыки и закрепить оборудование поезда за ответственными должностными лицами. Кроме того, в это время персоналом поезда в первом приближении была изучена техника и осуществлено начальное освоение сложного и многообразного оборудования.

Формирование воинской части осуществлялось под руководством начальника поезда связи № 1 военинженера 2 ранга В. И. Менделюкова и военкома поезда связи № 1 старшего политрука Н. Т. Цыганкова (рис. 12).

Укомплектованность воинской части личным составом составляла около 85 % (табл. 2).

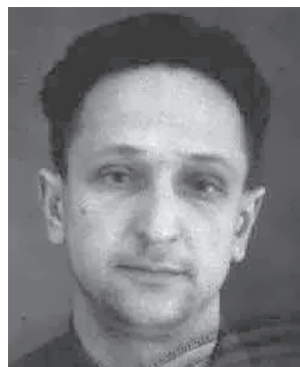


Рис. 12. Военком поезда связи № 1 старший политрук Н. Т. Цыганков

Приведенные в таблице 2 данные, показывают о достаточно высоком уровне укомплектованности воинской части личным составом. Также были укомплектованы и основные подразделения, за исключением начальствующего и руководящего технического персонала телеграфа, общий некомплект составлял 36 чел., в том числе: начальствующий состав (старший и средний) – 6 чел.; младший начальствующий состав – 1 чел.; рядовой состав – 29 чел.

Сформированный поезд связи № 1 являлся отдельной воинской частью, состоящей в резерве Главного Командования, и вводимой по его приказу в состав войск определенного фронта или армии с временным подчинением на этот период непосредственно начальнику связи фронта. Причем, в период нахождения в резерве, он подчинялся непосредственно начальнику 1-го управления ГУСКА.

### Выполнение первой боевой задачи

Шестого октября 1941 г. в 3 часа 30 мин. начальник поезда связи № 1 военинженер 2 ранга В. И. Менделюков по прямому телефону

Таблица 2.

Укомплектованность поезда связи № 1 личным составом

Категория личного состава	Командный начальствующий состав	Младший начальствующий состав	Рядовой состав	Всего
Положено по штату, чел.	53	14	171	238
Имеется по списку, чел.	52	13	137	202
Некомплект, чел.	1	1	34	36

от заместителя НКО И. Т. Пересыпкина получил распоряжение на выполнение **первой задачи** – произвести свертывание и убыть в 14.00 на станцию Куйбышев. Несмотря на впервые произведенное свертывание поезда, к 14.00 были закончены все работы, связанные с убытием воинской части, включая снятие 8-ми антенн и погрузку автомашин на платформы<sup>12</sup>.

На новое место назначения поезд прибыл утром 8 октября 1941 г. Обследование тупиковых веток и подъездных заводских путей г. Куйбышева и непосредственно прилегающих к нему районов, с целью размещения поезда, не дало положительных результатов. В течение восьми дней пребывания в Куйбышеве поезд находился на станционных путях [10].

15 октября начальником отдела передвижения войск Куйбышевской железной дороги было получено распоряжение, переданное в 13.30 начальнику воинской части о немедленной отправке поезда на ст. Арзамас. В 20.30 поезд в полном составе убыл со ст. Куйбышев и к 6 часам утра 18 октября прибыл на станцию Арзамас-II.

Переброска поезда со станции Куйбышев на станцию Арзамас-I рассматривалась командованием воинской части, как первый поход. Заместитель НКО И. Т. Пересыпкин лично интересовался переброской поезда на протяжении всего пути следования и был детально осведомлен о места нахождения поезда и возможностей его дальнейшего продвижения (рис. 8). Все это говорило о том, что в Арзамасе предстояло развертывание подвижного узла связи и организация его боевого применения по оперативным заданиям.



Рис. 13. Заместитель Народного комиссара обороны СССР И. Т. Пересыпкин

<sup>12</sup> ЦАМО РФ. Ф. 71. Оп. 12177. Д. 17. Л. 263.

В результате проведенной рекогносцировки в новом пункте дислокации было установлено, что на станциях Арзамас-II и Арзамас-I не имелось станционных и пакгаузных путей, пригодных для размещения поезда и развертывания его работы. Для обеспечения функционирования подвижного узла связи И. Т. Пересыпкин принял решение о строительстве специальной железнодорожной ветки, идущей непосредственно в лес. Данная ветка сооружалась у разъезда Соловейка, расположенного между станциями Арзамас-I и Арзамас-II. Такое решение было весьма удачным, так как давало возможность хорошей маскировки поезда от наблюдения с земли и воздуха, а также позволяло осуществить быстрый выход состава на любое из 4-х основных направлений: Москва, Горький, Казань, Рузавка, минуя маневрирование на загруженных станционных путях [11, с. 171].

Временно, до окончания постройки ветки, распоряжением заместителя НКО, переданного через военного коменданта станции Арзамас-II, поезд был размещен на станции Арзамас-I. Здесь перед командованием поезда была поставлена **первая боевая задача** – немедленно начать развертывание и к 06.00 19 октября войти в связь с корреспондентами по четырем основным направлениям: Москва, Куйбышев, Казань, Горький, а также с г. Арзамас. Эти связи предназначались для оперативного обслуживания Генерального штаба до ввода в действие стационарного узла связи Генерального штаба, а в последующем – должны были служить резервом при выходе из строя, по тем или иным причинам, стационарного узла связи.

Исключительная ответственность за своевременное и качественное выполнение **поставленной задачи по обеспечению связи Генеральному штабу**, сжатость сроков развертывания – 10 часов, мобилизовали коллектив воинской части. Основная работа по развертыванию подвижного узла связи, связанная с подключением к воздушным магистралям с большой плотностью линий связи, производилась в условиях полного затемнения. Уже к 04.00 19 октября все требуемые связи были установлены. Успешному решению этой задачи в условиях некомплекта личного состава телеграфа, способствовало детальное знание оборудования и технологии работы телеграфа начальником поезда связи



№ 1, руководившего по существу всеми работами по его развертыванию<sup>13</sup>.

Следует также отметить большую помощь, оказанную главным инженером Горьковского областного управления связи тов. Соколовым и начальником ЛТУ Арзамасского района тов. Малышевым, в решении всего комплекса работ, связанных с развертыванием и вхождением в связь.

В 20.00 19 октября подвижный узел связи посетил заместитель НКО И. Т. Пересыпкин. Им были осмотрены работавшие подразделения телеграфа и телефонного узла и дано указание начальнику поезда связи № 1 о дополнительном задействовании связей с Ростовом, Вологдой и Архангельском.

К утру 20 октября были установлены связи: Ростов через Куйбышев, Вологда через Горький и Архангельск через Казань. Кроме того, через Куйбышев была установлена связь с Воронежем.

Оперативная работа продолжалась вплоть до переезда поезда на специальную ветку, понижаясь в своей интенсивности по мере передачи связей и принятия нагрузки стационарным узлом связи Генерального штаба.

23 октября к 12.00 последние связи были переданы стационарному узлу и поезда связи № 1 отбыл на разъезд Соловейка на подготовленную для него ветку.

Этим закончилось выполнение подвижным узлом связи – поездом связи № 1, **первой боевой задачи** по обеспечению связи Генеральному штабу Красной армии.

В дальнейшем необычный подвижный узел связи выполнял важные задачи по обеспечению связи в интересах государственного и военного руководства страны. На завершающем этапе Второй мировой войны в период с 9 августа по 3 сентября 1945 г. поезд уже находился в составе действующей армии.

### Выводы

Проведенный анализ сооружения подвижного узла связи на базе железнодорожного

подвижного состава в годы войны, как резерва связи, показал необходимость принятия действенных мер по обеспечению мобильности системы связи и непрерывности управления войсками. Принятие решения о создании данного объекта связи принималось председателем Государственного комитета обороны СССР И. В. Сталиным и было выполнено в ограниченные сроки 25 суток, с привлечением ресурсов профильных наркоматов СССР.

Особенно важным является тот факт, что строительство поезда связи № 1 осуществлялось без проведения научно-исследовательских и опытно-конструкторских работ, конкурсных процедур, предварительного утверждения проекта и сметной документации. Все строительно-монтажные работы производились на основе имеющихся на то время отечественных технологических, технических и инженерных заделов непосредственно по ходу выполнения государственного задания. Окончание выполнения работ и их приемка осуществлялось в ходе формирования воинской части и проведения боевого слаживания.

Таким образом, строительство в кратчайшие сроки объекта связи и формирование воинской части – поезда связи № 1 – позволило Генеральному штабу Красной армии решать важные задачи по устойчивому, непрерывному, оперативному и скрытному управлению войсками в глубине территории страны.

Опыт сооружения Объекта 04, особенности его приемки и ввода в эксплуатацию, а также осуществление формирования необычной воинской части связи и проведение боевого слаживания подвижного узла связи, способного немедленно выполнять боевые задачи в сложных условиях Великой Отечественной войны требует всестороннего изучения и учета при строительстве и развитии системы и войск связи Вооруженных Сил Российской Федерации, в том числе в ходе проведения специальной военной операции.

### Литература

1. Пересыпкин И. Т. Связь в начальный период войны / Антология отечественной военной мысли. – М.: АП «Наука и образование», 2024. – 208 с.
2. Во имя Победы (80 лет Победы в Великой Отечественной войне 1941–1945 гг.) – М.: Граница, 2025. – 480 с.

3. Шептура В. Н. К вопросу о снабжении Красной армии средствами и имуществом связи накануне и в ходе Великой Отечественной войны (1941–1945 годы) // Социально-гуманитарная безопасность России. I Международная научно-практическая конференция, посвящённая 80-летию Великой Победы и Году защитника Отечества: материалы конференции / авторы-составители: Душин А. В., Каримов О. В., Мананникова М. В. – М.: РГУ нефти и газа (НИУ) им. И. М. Губкина, 2025. – С. 92–101.
4. 105 лет войскам связи Вооружённых Сил Российской Федерации: военно-исторический труд / Военно-исторический труд. – М.: АО «Красная Звезда», 2024. – 728 с.
5. Связь Красной армии в 1938–1942 гг.: уроки истории (научно-справочный труд). – М.: АО «Красная Звезда», 2022. – 724 с.
6. Жарский А. П., Свердел В. Ф., Шептура В. Н. Могло ли начало войны сложиться по-другому? По материалам служебных записок и воспоминаний начальников связи приграничных особых военных округов // Военно-исторический журнал. 2021. № 6. – С. 4–6.
7. Кукк К. И. Техника связи Великой Отечественной войны. – М.: Горячая линия – Телеком, 2020. – 138 с.
8. Народный комиссариат обороны СССР. 1941–1945 / Н. М. Васильев, В. Ф. Ворсин, В. В. Гаврищук, В. О. Дайнес и др. – М.: ИстЛит, 2025. – 616 с.
9. Тихонов С. Г. Оборонные предприятия СССР и России. В 2 т., т. 2. – М.: Том, 2010. – 608 с.
10. Шептура В. Н. О состоянии работы Куйбышевского отделения узла связи Наркомата обороны СССР в годы Великой Отечественной войны (по материалам проверки комиссией Главного управления связи Красной армии в период с 13 по 16 июня 1942 г.) // Память о прошлом – 2025. Военная история России – осмысление и сохранение исторической памяти: сборник научных трудов XIII Международного историко-архивного форума (Самара, 15–17 апреля 2025 г.): в 2 ч. Ч. 1. – Самара: РГА в г. Самаре, 2025. – С. 331–335.
11. Народный комиссариат связи СССР. 1941–1945. – М.: ИстЛит, 2023. – 688 с.

## MOBILE COMMUNICATIONS CENTER OF THE PEOPLE'S COMMISSARIAT OF COMMUNICATIONS OF THE USSR: EXPERIENCE IN THE CONSTRUCTION OF OBJECT 04, FORMATION AND APPLICATION OF THE COMMUNICATIONS TRAIN No. 1

*Sheptura V. N.<sup>14</sup>*

**Keywords:** *military communication system, communication facility, communications train, People's Commissariat of Communications of the USSR, Main Communications Directorate of the Red Army.*

### **Abstract**

**The purpose of** the article is to summarize the historical experience of the construction and combat use of Object 04 (communication train No 1) and to formulate conclusions and proposals for its use in modern conditions.

**The method of research** is historical and genetic, which involves the consistent study of historical facts, their generalization and the development of practical proposals and recommendations that are relevant to the modern process of development of the system and signal troops.

**Results:** the article examines the experience of constructing a mobile communication center of the People's Commissariat of Communications of the USSR (object 04), the formation and use of communication No 1 during the Great Patriotic War. Particular attention is paid to the generalization of materials from archival sources on the organizational and technical features of the creation of a mobile communication center on the basis of railway rolling stock. The experience of creating, forming and using a mobile communication

<sup>14</sup> Vladimir N. Sheptura, Ph.D. of Military Sciences, Associate Professor, Corresponding Member of the Russian Academy of Missile and Artillery Sciences, Senior Researcher of the Scientific Research Institute (Military History) of the Military Academy of the General Staff of the Armed Forces of the Russian Federation, Moscow, Russia. E mail: sheptura\_vn@mail.ru

center of the strategic command and control level is summarized and practical recommendations for improving the combat use of signal troops are developed.

**The scientific novelty and practical usefulness** lie in the fact that for the first time archival materials on the construction of Object 04 (communication train No 1) are introduced into scientific circulation and a description of the fulfillment of its first combat mission to provide communications to the General Staff of the Red Army is carried out.

### References

1. Peresy'pkin I. T. Svyaz' v nachal'ny'j period vojny' / Antologiya otechestvennoj voennoj my'sli. – M.: AP «Nauka i obrazovanie», 2024. – 208 s.
2. Vo'imya Pobedy' (80 let Pobedy' v Velikoj Otechestvennoj vojne 1941–1945 gg.) – M.: Granicza, 2025. – 480 s.
3. Sheptura V. N. K voprosu o snabzhenii Krasnoj armii sredstvami i imushhestvom svyazi nakanune i v xode Velikoj Otechestvennoj vojny' (1941–1945 gody') // Social'no-gumanitarnaya bezopasnost' Rossii. I Mezhdunarodnaya nauchno-prakticheskaya konferenciya, posvyashhyonnaya 80-letiyu Velikoj Pobedy' i Godu zashhitnika Otechestva: materialy' konferencii / avtory'-sostaviteli: Dushin A. V., Karimov O. V., Manannikova M. V. – M.: RGU nefti i gaza (NIU) im. I.M. Gubkina, 2025. – S. 92–101.
4. 105 let vojskam svyazi Vooruzhenny'x Sil Rossijskoj Federacii: voenno-istoricheskij trud / Voенно-istoricheskij trud. – M.: AO «Krasnaya Zvezda», 2024. – 728 s.
5. Svyaz' Krasnoj armii v 1938–1942 gg.: uroki istorii (nauchno-spravochny'j trud). – M.: AO «Krasnaya Zvezda», 2022. – 724 s.
6. Zharskij A. P., Sverdel V. F., Sheptura V. N. Moglo li nachalo vojny' slozhit'sya po-drugomu? Po materialam sluzhebny'x zapisok i vospominanij nachal'nikov svyazi prigranichny'x osoby'x voenny'x okrugov // Voенно-istoricheskij zhurnal. 2021. № 6. – S. 4–6.
7. Kuk K. I. Texnika svyazi Velikoj Otechestvennoj vojny'. – M.: Goryachaya liniya – Telekom, 2020. – 138 s.
8. Narodny'j komissariat oborony' SSSR. 1941–1945 / N. M. Vasil'ev, V. F. Vorsin, V. V. Gavrishhuk, V. O. Dajnes i dr. – M.: IstLit, 2025. – 616 s.
9. Tixonov S. G. Oboronny'e predpriyatiya SSSR i Rossii. V 2 t., t. 2. M.: Tom, 2010. – 608 s.
10. Sheptura V. N. O sostoyanii raboty' Kujby'shevskogo otdeleniya uzla svyazi Narkomata oborony' SSSR v gody' Velikoj Otechestvennoj vojny' (po materialam proverki komissiej Glavnogo upravleniya svyazi Krasnoj armii v period s 13 po 16 iyunya 1942 g.) // Pamyat' o proshlom – 2025. Voennaya istoriya Rossii – osmy'slenie i soxranenie istoricheskoy pamyati: sbornik nauchny'x trudov XIII Mezhdunarodnogo istoriko-arkhivnogo foruma (Samara, 15–17 aprelya 2025 g.): v 2 ch. Ch. 1. – Samara: RGA v g. Samare, 2025. – S. 331–335.
11. Narodny'j komissariat svyazi SSSR. 1941–1945. – M.: IstLit, 2023. – 688 s.



The journal is registered by the Federal Service for  
Supervision of Communications, Information Technology  
and Mass Communications.  
Registration Certificate  
PI № FS77-88069 от 16.08.2024

## Editor-in-Chief

Vasily IVANOV, Ph.D., Ass. Professor, Moscow

## Chairman of the Editorial Council

Alexander RUBIS, Ph.D., Moscow

## Assistant Editor-in-Chief

Grigory MAKARENKO, Senior Research Fellow, Moscow

## Editorial Board

Maxim PYLINSKY, Dr.Sc., Professor, Belarus  
Gennady RYZHOV, Dr.Sc., Professor, Moscow  
Yuri STARODUBTSEV, Dr.Sc., Professor, St. Petersburg  
Evgeny KHARCHENKO, Ph.D., Professor, Moscow  
Pavel Kuzin, Ph.D., Ass. Professor, Moscow

## Editorial board

Mikhail BUINEVICH, Dr.Sc., Professor, St. Petersburg  
Evgeny GLUSHANKOV, Dr.Sc., Professor, St. Petersburg  
Sergey IVANOV, Dr.Sc., St. Petersburg  
Alexander KOZACHOK, Dr.Sc., Ass. Professor, Orel  
Sergey KOROBKA, Dr.Sc., Moscow  
Andrey KOSTOGRYZOV, Dr.Sc., Professor, Moscow  
Sergey MAKARENKO, Dr.Sc., Professor, St. Petersburg  
Alexey MARKOV, Dr.Sc., Ass. Professor, Moscow  
Anatoly RYZHKOV, Dr.Sc., Professor, Moscow  
Nikolay SAVISHCHENKO, Dr.Sc., Professor, St. Petersburg  
Igor SIVAKOV, Dr.Sc., Moscow  
Vladimir TSIMBAL, Dr.Sc., Professor, Serpukhov  
Pavel Fedyunin, Dr.Sc., Professor, Voronezh  
Oleg FINKO, Dr.Sc., Professor, Krasnodar

## 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

## MILITARY CONTROL, COMMUNICATIONS AND NAVIGATION SYSTEMS

### PRINCIPLES OF INCREASING THE STABILITY OF THE DATA EXCHANGE NETWORK OF A LARGE GROUP OF UAVS BASED ON CLUSTERING OF ITS STRUCTURE

Derkach A. E., Limantseva E. V., Chudnov A. M. .... 2

### LOAD DISTRIBUTION IN MILITARY INFORMATION SYSTEMS

Allenov D. S., Kurbanov S. N. .... 8

### INNOVATIVE TECHNOLOGIES IN TELECOMMUNICATIONS AND THEIR IMPACT ON MILITARY COMMUNICATIONS

Ivanov V. G., Lukyanchik V. N., Kuzin P. I. .... 16

## SYSTEM ANALYSIS OF MILITARY SYSTEMS

### NETWORK TRAFFIC MONITORING IMPACT MODEL AND EFFICIENCY ON THE NETWORK DATA TRANSFERS

Simonova K. O. .... 33

### APPLICATION OF DIGITAL TWINS IN TELECOMMUNICATIONS SYSTEMS

Yarovoy R. V., Karganov V. V., Lukashenok V. I. .... 42

## INFORMATION SYSTEMS

### FEATURES OF THE ORGANIZATION OF BUSINESS TELEPHONE COMMUNICATION AT CONTROL ROOMS

Kuzina E. I., Pankin A. A., Potapov I. A., Nazarov A. D. .... 52

### ANALYSIS OF EXISTING GEOGRAPHIC INFORMATION SYSTEMS USED IN THE MINISTRY OF EMERGENCY SITUATIONS OF RUSSIA AND THEIR ASSESSMENT FUNCTIONAL LIMITATIONS

Kurbanov S. N., Bezvesyla A. A., Grigoryan A. A. .... 59

### NON-MATHEMATICAL METHODS IN CRYPTOGRAPHY (SECURE COMMUNICATION BASED ON A PEER-TO-PEER MESH NETWORK)

Cherepnev M. A. .... 72

## MILITARY ELECTRONICS, EQUIPMENT FOR MILITARY COMPLEXES

### CRITERIA FOR THE EFFICIENCY OF THE FIELD POWER SUPPLY SYSTEM

Asanin A. V., Ivanov V. G., Ivanishko A. N. .... 78

## TECHNOLOGIES FOR TRAINING CADETS OF MILITARY SPECIALTIES

### THE USE OF AUGMENTED REALITY IN THE PROCESS OF LEARNING IN HIGHER EDUCATIONAL INSTITUTIONS

Magera M. A. .... 88

## OUR STORY

### MOBILE COMMUNICATIONS CENTER OF THE PEOPLE'S COMMISSARIAT OF COMMUNICATIONS OF THE USSR: EXPERIENCE IN THE CONSTRUCTION OF OBJECT 04, FORMATION AND APPLICATION OF THE COMMUNICATION TRAIN NO. 1

Sheptura V. N. .... 96