

TELECOMMUNICATIONS AND COMMUNICATIONS

№ 3 (12) 2026

DOI: 10.21681/3034-4050

THEME OF THE ISSUE:

DIRECTIONS FOR THE DEVELOPMENT OF TROPOSPHERIC COMMUNICATION

WIRED COMMUNICATION DURING THE GREAT PATRIOTIC WAR

ТЕЛЕКОММУНИКАЦИИ и СВЯЗЬ

№ 3 (12) 2026

ТЕМА НОМЕРА:

НАПРАВЛЕНИЯ РАЗВИТИЯ ТРОПОСФЕРНОЙ СВЯЗИ

ПРОВОДНАЯ СВЯЗЬ В ГОДЫ ВЕЛИКОЙ ОТЕЧЕСТВЕННОЙ ВОЙНЫ

WWW.TELEMIL.RU

DOI: 10.21681/3034-4050



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



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

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

Главный редактор

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

Шеф-редактор

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

Попечительский совет

РУБИС Александр Анатольевич, к.т.н., заместитель начальника Главного управления связи ВС РФ по вооружению (председатель)

ПАНКОВ Роман Николаевич, к.ист.н., начальник ФГБУ «16 Центральный научно-исследовательский испытательный институт»

ХАРЧЕНКО Евгений Борисович, к.соц.н., доцент (секретарь)

Редакционная коллегия

АЧКАСОВ Николай Борисович, д.в.н., профессор, Санкт-Петербург

БЫЧКОВ Антон Вячеславович, д.в.н., доцент, Санкт-Петербург

БУЙНЕВИЧ Михаил Викторович, д.т.н., профессор, Санкт-Петербург

ГЛУШАНКОВ Евгений Иванович, д.т.н., профессор, Санкт-Петербург

ГРУДИНИН Игорь Владимирович, д.в.н., профессор, Санкт-Петербург

ИВАНОВ Сергей Александрович, д.т.н., Санкт-Петербург

КОЗАЧОК Александр Васильевич, д.т.н., доцент, Орел

КОСТОГРЫЗОВ Андрей Иванович, д.т.н., профессор, Москва

КУЗИН Павел Игоревич, к.т.н., доцент, Санкт-Петербург

МАКАРЕНКО Сергей Иванович, д.т.н., профессор, Санкт-Петербург

МАРКОВ Алексей Сергеевич, д.т.н., доцент, Москва

НОВИКОВ Евгений Александрович, д.т.н., доцент, Санкт-Петербург

ПРИВАЛОВ Андрей Андреевич, д.в.н., профессор, Санкт-Петербург

ПЫЛИНСКИЙ Максим Валерьевич, д.т.н., профессор, Белоруссия

РЫЖОВ Геннадий Борисович, д.в.н., профессор, Москва

САВИЩЕНКО Николай Васильевич, д.т.н., профессор, Санкт-Петербург

СТАРОДУБЦЕВ Юрий Иванович, д.в.н., профессор, Санкт-Петербург

ФЕДЮНИН Павел Александрович, д.т.н., профессор, Воронеж

ФИНЬКО Олег Анатольевич, д.т.н., профессор, Краснодар

ЦИМБАЛ Владимир Анатольевич, д.т.н., профессор, Серпухов

ЧЕРНЫШОВ Михаил Викторович, д.т.н., профессор, Санкт-Петербург

Учредитель и издатель

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

Над номером работали:

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

Подписано к печати 15.04.2026 г.

Общий тираж 120 экз. Цена свободная

Адрес: 141006, г. Мытищи Московской обл., 1-й Рупасовский пер.

E-mail: editor.tis@yandex.ru, тел.: +7 (985) 939-75-01

Требования, предъявляемые к рукописям, размещены на сайте: <https://telemil.ru/>

СОДЕРЖАНИЕ

СИСТЕМНЫЙ АНАЛИЗ СИСТЕМ ВОЕННОГО НАЗНАЧЕНИЯ

СОСТОЯНИЕ И НАПРАВЛЕНИЯ РАЗВИТИЯ ТРОПОСФЕРНОЙ СВЯЗИ В СИСТЕМЕ ВОЕННОЙ СВЯЗИ ВООРУЖЕННЫХ СИЛ

Иванов В. Г., Лукьянчик В. Н., Баширов С. Ю..... 2

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ АЛГОРИТМА ПОДСТРОЙКИ КОЭФФИЦИЕНТОВ АДАПТИВНОЙ АНТЕННОЙ РЕШЕТКИ

Цветков Д. Е., Федоров П. Н..... 13

ПРИНЦИПЫ ПОСТРОЕНИЯ ПАЙПЛАЙНОВ С ДИНАМИЧЕСКОЙ АРХИТЕКТУРОЙ И АГЕНТНЫМ УПРАВЛЕНИЕМ

Лукашенко В. И., Изотов Д. Ю..... 21

МЕТОД КОНТЕКСТНОЙ ВЕРИФИКАЦИИ СОБЫТИЙ ПРИ КОНТРОЛЕ БЕЗОПАСНОСТИ РАСПРЕДЕЛЁННОЙ ИОТ-ПОДСИСТЕМЫ

Андреев И. А., Липатников В. А., Тарасенко С. Е..... 29

ИНФОРМАЦИОННЫЕ СИСТЕМЫ

ПРОГРАММНЫЙ КОМПЛЕКС ДЛЯ ПОИСКА И ИДЕНТИФИКАЦИИ СИГНАЛОВ ДЛЯ SDR НА ОСНОВЕ ПЛАТФОРМЫ GNU RADIO

Баймаков Д. А., Ткачев Д. Ф., Воробьев П. В..... 40

ВОЕННЫЕ СИСТЕМЫ УПРАВЛЕНИЯ, СВЯЗИ И НАВИГАЦИИ

АЛГОРИТМЫ ЗОНДИРОВАНИЯ ЛАЗЕРНОЙ ЛОКАЦИОННОЙ СТАНЦИЕЙ БЕСПИЛОТНОГО ЛЕТАТЕЛЬНОГО АППАРАТА МАЛОГО КЛАССА

Козирацкий А. Ю., Чёгин А. В., Гревцев А. И..... 49

ВОЗМОЖНОСТИ И ПЕРСПЕКТИВЫ ПРИМЕНЕНИЯ ТЕХНОЛОГИЙ РОЕВОГО ИНТЕЛЛЕКТА В СИСТЕМАХ СВЯЗИ ВОЕННОГО НАЗНАЧЕНИЯ

Яговитов Д. С., Вдовченко Н. Ю..... 57

АРХИТЕКТУРА СЕТИ ОТКРЫТОЙ АВТОМАТИЧЕСКОЙ ТЕЛЕФОННОЙ СВЯЗИ, ПОСТРОЕННОЙ С ПРИМЕНЕНИЕМ ПИРИНГОВЫХ ТЕХНОЛОГИЙ, И ПРЕДЛОЖЕНИЯ ПО ЕЕ ЗАЩИТЕ

Ашлапов М. В., Елисеев Д. И..... 64

ВОЕННАЯ ЭЛЕКТРОНИКА, АППАРАТУРА КОМПЛЕКСОВ ВОЕННОГО НАЗНАЧЕНИЯ

ОБНАРУЖЕНИЕ ДРОНОВ ПРОТИВНИКА С ПОМОЩЬЮ ПОИСКОВОЙ АППАРАТУРЫ, УСТАНОВЛЕННОЙ НА ОТЕЧЕСТВЕННЫХ БЕСПИЛОТНЫХ ЛЕТАТЕЛЬНЫХ АППАРАТАХ

Ахмедов Э. М., Асадов Х. Г., Алиева Х. С..... 69

ОПТИМИЗАЦИЯ ФУНКЦИОНИРОВАНИЯ ПЕРЕДОВЫХ ПУНКТОВ ТЕХНИЧЕСКОГО ОБЕСПЕЧЕНИЯ КАК ФАКТОР ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ ОБСЛУЖИВАНИЯ СИСТЕМ СВЯЗИ И АСУ

Курочка В. С., Колодяжный П. А., Юшин А. И..... 74

РОЛЬ МАСКИРОВКИ И ИМИТАЦИИ ЭЛЕМЕНТОВ СИСТЕМЫ СВЯЗИ ВОЕННОГО НАЗНАЧЕНИЯ

Агафонов Д. А., Козырев В. В., Лапин Г. В..... 83

НАША ИСТОРИЯ

ОЦЕНКА РАБОТЫ ВОЕННО-ПОЛЕВЫХ СРЕДСТВ ПРОВОДНОЙ СВЯЗИ В ГОДЫ ВЕЛИКОЙ ОТЕЧЕСТВЕННОЙ ВОЙНЫ

Шенгура В. Н..... 89

СОСТОЯНИЕ И НАПРАВЛЕНИЯ РАЗВИТИЯ ТРОПОСФЕРНОЙ СВЯЗИ В СИСТЕМЕ ВОЕННОЙ СВЯЗИ ВООРУЖЕННЫХ СИЛ

Иванов В. Г.¹, Лукьянчик В. Н.², Баширов С. Ю.³

DOI:10.21681/3034-4050-2026-3-2-12

Ключевые слова: система связи, тропосферная связь, военная связь, тропосферная станция, загоризонтное распространение, развитие связи.

Аннотация

Цель работы: проведение ретроспективного анализа развития тропосферной связи в Вооруженных силах, выработка практических предложений по развитию средств тропосферной связи в настоящее время с учетом технологического развития и опыта организации связи в специальной военной операции.

Метод исследования: методологическую основу исследования составила общая теория систем, теория военной связи, теория открытых систем с использованием методов системного анализа.

Результаты исследования: проведен анализ развития средств тропосферной связи в Вооруженных силах СССР, их состояние в Российской Федерации и в армиях стран НАТО в настоящее время. Выработаны предложения по способу применения «точка-многоточка» и основным направлениям совершенствования военных тропосферных станций.

Научная новизна заключается в разработке обоснованных направлений развития средств тропосферной связи с учетом требований по обеспечению управления и технологического развития средств военной связи.

1. Введение

Развитие способов и средств высокотехнологичной вооружённой борьбы требует постоянного развития и совершенствования систем управления войсками и оружием, её технической основы – систем связи различного уровня управления.

Современные системы связи в условиях угрозы и ведения масштабных и войн и вооружённых конфликтов с применением высокоточного оружия, оружия массового поражения, в том числе и на новых физических принципах, должны гарантированно обеспечивать обмен большими объемами информации органам военного управления в любых условиях обстановки. С учётом прогнозируемого большого территориального размаха районов боевых действий, сложного рельефа местности, ожидаемого повреждения большинства кабельных линий связи, к системам беспроводной связи предъявляются новые требования в части значительного увеличения длины линий, интервалов связи, пропускной способности, а также к развед- и помехозащищенности.

Для обеспечения требований по организации беспроводной связи дальней связи в войсках

связи Вооруженных Сил применяются тропосферные средства связи, при этом их тактико-технические характеристики существенно уступают современным образцам тропосферных станций, применяемых в армиях стран НАТО. При этом анализ применения средств военной связи показывает [1, 2], что перенос основной нагрузки мобильных систем военной связи в космос (активное применение средств спутниковой связи) может негативно сказаться на управлении войсками в случае уничтожения спутников, в итоге управление группировками в удаленных районах и действующих на больших расстояниях будет существенно затруднено. И тропосферная связь может стать резервным средством связи. Следовательно, необходимо организовывать и обеспечивать дальнейшее развитие и совершенствование средств и комплексов тропосферной связи, обеспечивающих устойчивую связь в условиях действий войск (сил) на большом удалении, а также в условиях сложного рельефа и деструктивных воздействий противника.

В условиях сложной политической обстановки в мире, экономических санкций при создании новых средств и комплексов связи не должно

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

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

3 **Баширов Сергей Юрьевич**, заместитель начальника управления Главного управления связи Вооруженных Сил Российской Федерации. г. Москва, Россия. E-mail: wasj2006@yandex.ru

быть ошибок в принятии решения, какие средства связи нужны войскам в современной войне, при этом актуальным вопросом является всесторонняя историческая реконструкция развития и изучения накопленного многолетнего опыта разработки и организации производства отечественных образцов средств тропосферной связи военного назначения и их активное применения в период с 1960 по 2000 г.

Тропосферная связь, как новый вид военной связи, имеет относительно короткую историю. В СССР работы по разработке технологий тропосферной связи стартовали с первых теоретических и экспериментальных изысканий, посвящённых изучению дальнего загоризонтного распространения радиоволн в дециметровом диапазоне [3].

На основании результатов комплексного научно-исследовательского анализа была сформулирована теоретическая база процессов запредельного распространения ультракоротких волн в тропосфере, обусловленных рассеятельным и отражательным взаимодействием радиосигнала с неоднородностями нижних слоев атмосферы. Установленная регулярность, в противовес эпизодическому характеру явления, подтверждает стабильность тропосферной связи, что открывает перспективы для проектирования высокоскоростных систем за горизонтом. Данные системы способны обеспечить значительно большие дистанции передачи по сравнению с существующими радиорелейными линиями прямой видимости. Следовательно, тропосферная связь имеет существенное преимущество перед радиорелейной связью прямой видимости, поскольку обеспечивает высокоскоростную связь между ПУ без дополнительных ретрансляций на значительно (в 3–6 раз) большем расстоянии – до 200 км, включая труднодоступные и сильнопересечённые территории, в том числе и в районах Крайнего Севера. В случае,

когда требуется обеспечить управление на расстоянии, превышающем интервал связи, тропосферные станции могут работать в режиме ретрансляции информации.

Технология тропосферной связи основана на отражении сигнала от тропосферы – нижнего слоя атмосферы (высотой в полярных областях 8–10 км, в умеренных широтах – 10–12 км, на экваторе – 16–18 км), вследствие чего возможно распространение волн за пределы горизонта (рис. 1) [3, 4].

При дальнем регулярном тропосферном распространении определяющую роль играют неоднородности Q тропосферы в объеме V , образованном при пересечении телесных углов характеристик направленности передающей и приемной антенн (рис. 1). Тропосферные неоднородности действуют как естественные пассивные ретрансляторы, вторичное излучение которых можно характеризовать некоторой диаграммой направленности. Для компенсации ослабления радиосигнала в тропосфере требуется наличие значительного запаса мощности передающих устройств, высокой чувствительности приемников и большого коэффициента усиления антенн для обеспечения удовлетворительного соотношения сигнал/шум на приемном конце радиолинии [3, 4].

Тропосферная связь обеспечивается ценой больших энергетических затрат (использованием мощных передатчиков, больших остро-направленных антенн и чувствительных приемников), так как эффективность рассеяния и отражения УКВ неоднородностями тропосферы весьма низка.

Особенностью тропосферной связи являются также суточные и сезонные изменения уровня высокочастотного сигнала на трассах. Кроме быстрых и медленных замираний напряженность поля имеет отчетливо выраженную зависимость от времени суток и времени года.

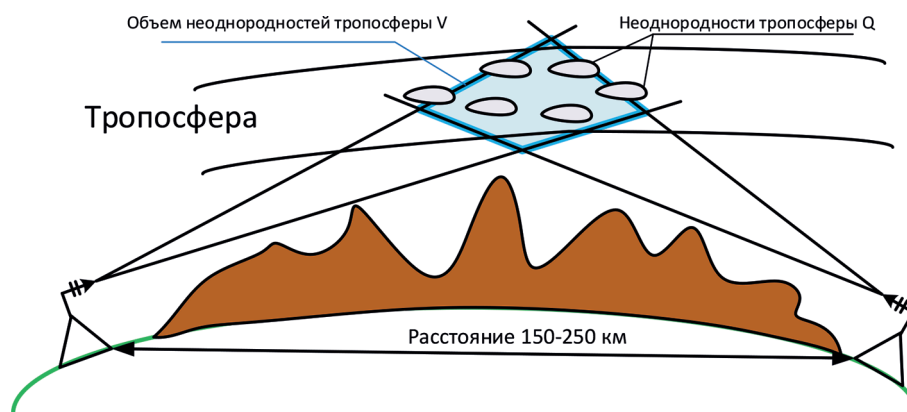


Рис. 1. Принцип тропосферной связи

Необходимо отметить, что на интервале тропосферной линии днем уровень энергии сигнала в точке приема ниже, чем ночью. Суточные изменения мощных сигналов проявляются значительно больше, чем слабых сигналов.

Учитывая особенности дальней тропосферной связи с учетом рассеяния и отражения волн и другие факторы, оказывавшие влияние на распространение высокочастотного сигнала, проводимые научные исследования и опытно-конструкторские работы, а также ведущиеся отечественные разработки и за рубежом в области создания тропосферных средств в середине XX столетия способствовали появлению разработок в области создания тропосферных станций в СССР.

Анализ развития средств военной тропосферной связи [1,2] позволил определить основные этапы ее развития:

1-й этап (аналоговый) (1959–1974) с принятием на вооружение первых отечественных военных аналоговых тропосферных станций Р-121, Р-122, Р-133, Р-408, Р-410;

2-й этап (аналого-цифровой) (1974–1986) с принятием на вооружение первой аналого-цифровой станции Р-412 в 1974 г.;

3-й этап (начальный цифровой) (1986–2000) с принятием на вооружение тропосферных станций Р-417, Р-423-1, Р-423-2;

4-й этап (цифрового развития) (2000 г. – по настоящее время) с принятием на вооружение тропосферных станций Р-423АМ.

Первые тактико-технические задания на проведение опытно-конструкторских работ по

созданию средств тропосферной связи были подготовлены [1, 2].

Анализ литературы [1, 2, 3] показал, что развитие тропосферной связи осуществлялось под руководством начальника связи Войск противовоздушной обороны СССР, который поставил задачу на проведение первых опытно-конструкторских работ (ОКР) по созданию средств тропосферной связи, и уже в период 1957–1959 гг. были выполнены ОКР по созданию первых отечественных военных средств тропосферной связи Р-121 (шифр «Фрегат») и Р-122 (шифр «Лодка») (рис. 2), эксплуатация которых выявила много недостатков, что позволило в короткие сроки создать более совершенные тропосферные станции.

В 1962 году была принята на вооружение новая тропосферная станция Р-133 (шифр «Корвет»), работающая в диапазоне частот 4257–4382 МГц и обеспечивающая устойчивую связь на дальности связи 150–250 км, а также многоканальная станция Р-408 (шифр «Баклан»), которая обеспечивала 6 каналов в диапазоне частот на дальности 120 км, которая выпускалась в мобильном (Р-408М) и стационарном (Р-408С) исполнении (рис. 3).

Набирающая популярность тропосферная связь обеспечила в период 1964–1967 гг. проведение опытно-конструкторских работ (ОКР) по созданию Р-410 (шифр «Атлет») (рис. 3). Станция обеспечивала работу в диапазоне 476–525 МГц и 576–625 МГц и позволяла строить одноинтервальные линии протяженностью 150–200 км и девятиинтервальные линии протяженностью до 1200 км.



Тропосферная радиорелейная станция Р-121 (шифр «Фрегат»)

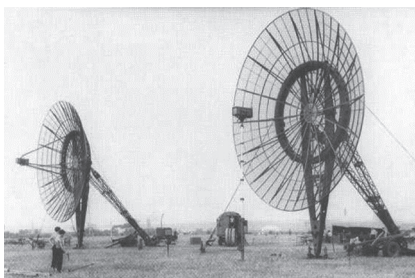


Тропосферная радиорелейная станция Р-122 (шифр «Лодка»)

Рис. 2. Первые военные тропосферные станции СССР



Тропосферная станция Р-133
(шифр «Корвет»)



Тропосферная станция Р-408
(шифр «Баклан»)



Тропосферная станция Р-410
(шифр «Атлет»)

Рис. 3. Военные тропосферные станции СССР

На основе опыта применения тропосферных станций, постоянно осуществлялись работы по повышению их тактико-технических характеристик с целью увеличения канальной емкости и уменьшения массогабаритных показателей. Так в период 1970–1974 гг. на основе Р-410 была разработана и принята на вооружение тропосферная станция Р-420 (шифр «Атлет-Д»), в которой была увеличена мощность передатчиков в 7 раз, применена новая питающая электро-станция на 100 кВт, что позволило увеличить дальность интервала в 1,6 раза и составила 400 км, а протяжённость тропосферной линии связи достигла 2500 км.

Для обеспечения устойчивой связи в интересах Объединённых вооружённых сил государств Варшавского договора потребовалась разработка многоканальной высокоскоростной станции тропосферной связи нового типа. Эти работы были связаны с необходимостью повышения разведзащищённости линий связи и их безопасности, так как спутниковый ресурс связи был ограничен по количеству выделяемых каналов и по пропускной способности [2]. И уже в 1974 году началось серийное производство самой распространённой аналого-цифровой тропосферной станции Р-412 (шифр «Тропа») 4438–4555 МГц и 4630–4750 МГц, которая выпускалась в нескольких модификациях: Р-412А, Р-412Ф, Р-412Б, Р-412С (рис. 4). Р-412 обеспечивала построение одноинтервальной линии связи до 200 – 250 км на скоростях передачи цифрового потока: 1,2; 2,4; 4,8; 9,6; 48 кбит/с. Диаметр двух антенн был уменьшен до 2,5 м, а мощность на выходе передающего устройства увеличена до 600 Вт.

К концу семидесятых годов был создан парк второго поколения тропосферных станций и сформировалась концепция их использования в полевой и стационарной системе связи Вооружённых сил:

- малоканальные – для построения сетей прямой связи (сетей командования) в тактическом, оперативно-тактическом и оперативном

звеньях управления всех видов Вооружённых сил;

- многоканальные – для построения опорных сетей и многоинтервальных линий в оперативном и стратегическом звеньях управления всех видов Вооружённых сил, а также стационарных территориальных сетей связи.

В 1980 году была разработана и в 1986 году принята на вооружение мобильная 60-канальная тропосферная станция для обеспечения связи в стратегическом звене управления Р-417 (шифр «Багет»), применение которой позволило осуществлять построение многоинтервальной тропосферной линии связи до 2000 км с интервалами по 200–250 км с канальной скоростью 480 кбит/с (рис. 5).



Рис. 4. Тропосферная станция Р-412



Рис. 5. Тропосферная станция Р-417



Тропосферная станция Р-423-1



Тропосферная станция Р-423-2А

Рис. 6. Тропосферные станции семейства «Бриг»

В рамках ОКР была разработана многоканальная цифровая тропосферная станция Р-423-1 (шифр «Бриг-1») (рис. 6) оперативного звена управления с пропускной способностью от 48 кбит/с до 2 Мбит/с.

Развитие тропосферной станции Р-423-1 осуществлялось в рамках ОКР «Бриг-2», в 1985 г. первая станция Р-423-2А комплекса «Бриг-2А» успешно прошла государственные испытания и была принята на вооружение в 1988 г.

На базе тропосферной станции Р-423-2А было разработано 9 модификаций (5 – для Сухопутных войск, 2 – для РВСН, 2 – для войск ПВО) [1, 2].

Благодаря применению средств и технологий тропосферной связи значительно расширились возможности систем управления и связи соединений и сил СССР при ведении боевых действий, а также в труднодоступных и отдалённых районах страны и за её пределами. Об этом свидетельствует практика боевого применения ограниченного контингента советских войск в условиях высокогорной и пересечённой местности в Демократической Республике Афганистан (1979–1989 гг.) [2].

В 90-х годах прошлого столетия развитие военной тропосферной связи не осуществлялось: НИИ, КБ и предприятия промышленности, не имея заказов от Министерства обороны, закрыли ранее начатые работы.

В первой половине 2000-х годов в Красноярске (ФГУП «НПП «Радиосвязь») была проведена модернизация ТРССт Р-423-2А по расширению рабочего диапазона частот, модернизации передатчика мощностью 300 Вт, увеличению канальной скорости до 2 Мбит/с. На ее основе был разработан комплекс «Сосник» (контейнерный вариант ТРССт Р-423-АМК (2005 г.), малогабаритная перевозимая ТРССт Р-423-ПМ (2008 г.) и вариант ТРССт на автомобильном шасси Р-423-АМ (2009 г.) (рис. 7).

Все тропосферные станции комплекса «Сосник» работают в диапазоне от 4400 до 5000 МГц с разбивкой на два диапазона: от 4400 до 4630 МГц и от 4770 до 5000 МГц. Для борьбы с быстрыми замираниями кроме последовательного многочастотного сигнала используется пространственно-разнесённый приём. Станции обеспечивают передачу группового потока со скоростями 64, 256, 512 и 2048 кбит/с.

Рассматривая мобильные тропосферные станции, нельзя не упомянуть о созданной в 1963 году стационарной ТРССт «Горизонт-М» и в последующем ТР-120 (рис. 8) с системой «Аккорд» для борьбы с быстрыми замираниями сигнала методом частотного разнесения (за счет одновременной передачи информации на разных эквидистантных частотах с последующим сложением) [1]. Протяженность интервала связи составляла – 300–400 км, линии – более 10000 км.



Р-423АМК



Р-423ПМ



Р-423АМ

Рис. 7. Тропосферные станции семейства «Сосник»



Рис. 8. Тропосферная станция TP-120

Сравнительные характеристики тропосферных станций различных поколений приведены в таблице 1.

Представленный ретроспективный анализ тропосферных станций показал, что базовыми недостатками современных тропосферных средств связи являются: отсутствие портативных и малогабаритных решений; большие габариты аппаратных машин, демаскирующие их на местности; низкая пропускная способность; большое время развертывания и вхождения в связь.

Таблица 1.

Сравнительные характеристики тропосферных станций

Тип станции	Диапазон частот, МГц	Дальность связи на интервале, км	Число каналов / скорость передачи, кбит/с	Транспортные единицы	Мощность передатчика, Вт
Горизонт-М	0,821–0,853; 0,969–0,997	120–450	60 ТФ	стационарная	2×3000, 2×5000
TP-120	0,821–0,853; 0,969–0,997	200–300	120 ТЧ	стационарная	2×5000
P-133	3200–3400	150–200	2ТФ	«Урал-375А» – 1	2×1000
P-408М	475–625	до 180	24 ТФ	«ЗИЛ-157» – 4	2×1000
P-410М	476–525; 576–625	100–160	12–24 ТФ	«ЗИЛ-131» – 3, «УРАЛ-375» – 1, прицепы – 4	2×700
P-412	4200–4440	150	3–6 ТФ; до 48 кбит/с	«Урал-375Д» – 2, «ЗИЛ-131» – 1	2×1000
P-412	4200–4440	150	3–6 ТФ; до 48 кбит/с	«Урал-375Д» – 2, «ЗИЛ-131» – 1	2×1000
P-417	4435–4555; 4630–4750	до 390	60 ТЧ; до 2048 кбит/с	«КАМАЗ-4310» – 5, прицепы – 4	4×1500
P-420 P-420М	476–525; 576–625	до 420	24 ТФ или 480 кбит/с	«Урал-4320» – 4, «ЗИЛ-131» – 2, прицепы – 4	2×5000
P-423-1М	4435–4555; 4630–4075	300–150	48–2048 кбит/с	«КАМАЗ-4310» – 3, прицепы – 2	2×1500
P-423-2А	4435–4555; 4630–5000	до 145	до 480 кбит/с	«КАМАЗ-4310» – 1, прицеп – 1	2×300
P-423-2Б	4435–4555; 4630–5000	до 90	до 240 кбит/с	МТ-ЛБу	1×300
P-423-2БТ	4435–4555; 4630–5000	до 90	до 240 кбит/с	БТР-80	1×300
P-423-2Р	4435–4555; 4630–5000	220–200	2,4–9,6 кбит/с	МАЗ-543В	2×300
P-423-2УС	4435–4555; 4630–5000	300–140	2,4–240 кбит/с	стационарная	4×1000
P-423-АМК	4400–5000	170–125	256–2048 кбит/с	контейнер	2×300
P-423-АМ	4400–5000	170–125	256–2048 кбит/с	«Урал-4320»	2×300
P-423-ПМ	4400–5000	145–105	64–256 кбит/с	2 модуля, общ. масса ≈ 180 кг	1×100

Также тропосферные средства связи широко используются в зарубежных странах таких как США, Великобритания, Норвегия, Франция, Япония, Китай, при этом совершенными являются средства тропосферной связи США. Технической основой повышения эффективности перспективных средств тропосферной связи является стремление к использованию современных информационных радиотехнологий в тропосферной связи [4, 5].

В настоящее время в армиях развитых стран НАТО активно осуществляется развитие и применение мобильных военных тропосферных станций (табл. 2).

Учитывая достоинства средств тропосферной связи, их роль, место и значение при организации связи для управления войсками необходимо наряду с заданием оперативно-технических и тактико-технических требований, обосновать перспективный унифицированный цифровой комплекс, сочетающий в себя возможности для работы в сложных условиях комплексного противодействия.

Разработку и создание тропосферных станций нового поколения необходимо осуществлять из концептуальных положений развития системы связи Вооруженных Сил с учетом опыта организации связи в ходе СВО по обеспечению

Таблица 2.

Сравнительные характеристики тропосферных станций НАТО

Тропосферная станция COMET CS67PLUS	Тропосферная станция AN/TRC-245	Автоматический тропосферный терминал TROPOLINE 240
		
Страна-изготовитель		
США	США	Норвегия
Диапазон частот		
нижний: 4,40 ГГц – 4,65 ГГц, верхний: 4,75 ГГц – 5,00 ГГц	нижний: 4,40 ГГц – 4,65 ГГц, верхний: 4,75 ГГц – 5,00 ГГц	4,4–5,0 ГГц
Канальная скорость		
946 Кбит/с – 210 Мбит/с	100 Мбит/с – 210 Мбит/с	до 200 Мбит/с
Дальность связи		
до 250 км	до 200 км	до 150 км
Время развертывания		
Один оператор за 15 мин.	Двумя операторами за 30 мин.	Двумя операторами за 20 мин.
Антенна		
С сегментированным отражателем из углеродного волокна диаметром 2,4 м	Параболический отражатель с прямым фокусом 2,4 м. в надувном радиолокаторе	С сегментированным отражателем из углеродного волокна диаметром 2,4 м со встроенной пневматической мачтой
Особенности		
Для обеспечения максимальной пропускной способности используется технология адаптивного кодирования и модуляции на основе глубокого обучения (Adaptive Coding Modulation).	Для использования в суровых условиях, обеспечивает высокопроизводительную тактическую связь по прямой видимости (LOS) и за пределами линии видимости (BLOS)	Интеллектуальный блок управления с датчиками ориентации для автоматического наведения

связи в сложной помеховой обстановке в условиях действия средств РЭБ противника, быстрого обнаружения станций (аппаратных) и их излучения, применения высокоточных средств поражения. Следовательно, разрабатывать ТРСт нужно с учётом технологического развития связи и способов организации связи в видах и родах ВС РФ в границах территории РФ для повседневной деятельности, на особый период и в ходе ведения боевых действий с возможностью их применения в экстремальных условиях. В различных вариантах исполнения, для полевого – мобильные перевозимые в автомобилях типа «Буран» или «Тигр» и в стационарном – с возможностью их размещения на стационарных объектах в защищённых сооружениях с учетом обеспечения их живучести.

В основе технологических решений необходимо найти такие, которые будут способны удовлетворить требования по потребляемой мощности электроэнергии, массогабаритным показателям, размерам АФУ, частотному диапазону, высокой пропускной способности и простоте применения. В технологическую основу ТРСт нужно закладывать перспективные технологии, например: технологии помехозащиты адаптивной компенсации помех (АКП) и фазоманипулированных широкополосных сигналов (ФМ-ШП) и метод режекции (подавления мешающих сигналов), использование режима временного дуплекса, использования широкополосных неперестраиваемых усилителей мощности, методы модуляции несущего колебания – ВРК-ОФ-Мн-ШПС, ЧВМ-4, ДОФМ (ОФМ) [6, 7].

Важное значение имеет и такое техническое решение, как применение комбинированного разнесения: частотного и пространственного, то есть по существу технологии MIMO с возможностью передачи нескольких потоков данных

одновременно с использованием множества антенн [8, 9]. При этом образуются статистически независимые каналы, которые эффективно разделены друг от друга. Применение данной технологии имеет ряд важных преимуществ (достоинств), которые делают её незаменимой в современных системах военной связи, в том числе и при создании перспективных средств тропосферной связи. Основными из них являются:

- увеличение пропускной способности за счет передачи нескольких потоков данных одновременно с использованием нескольких антенн и тем самым многократно увеличивается пропускная способность канала связи, что приводит к более быстрой и эффективной передаче данных;
- повышение скорости передачи данных благодаря возможности одновременной трансляции нескольких потоков данных (технология MIMO);
- улучшенная надёжность связи при использовании нескольких приёмопередающих антенн в конструкции. Это позволяет снизить вероятность возникновения ошибок при передаче данных;
- применение MIMO помогает эффективно использовать доступный спектр частот для передачи данных и тем самым сокращает время передачи.

Особую значимость представляют цифровые антенные решётки (ЦАР), с помощью которых возможно проводить электрическое сканирование несколькими лучами и на различных частотах. ЦАР обеспечивает получение высокой направленности излучения с помощью объединенных в систему слабонаправленных антенных элементов (АЭ) (вибраторов, щелей, спиралей и т. п.), возбуждаемых токами с заданным

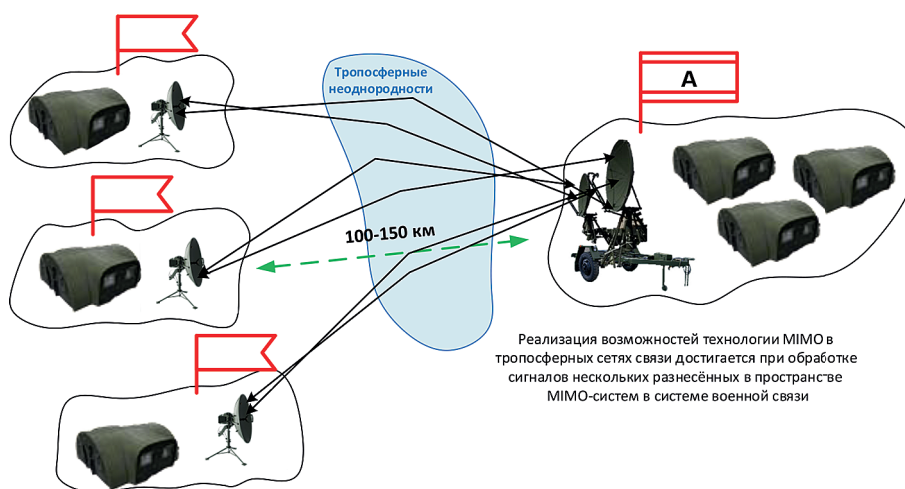


Рис. 9. Способ организации тропосферной связи на основе технологии MIMO

соотношением амплитуд и фаз [4, 6, 7]. ЦАР позволяет изменять направления излучения главного лепестка электронным способом, за счет перераспределения токов и фаз в АЭ. Структура построения ЦАР является унифицированной и инвариантной к аппаратной зависимости процедур обработки сигналов и упрощает их адаптацию под определенный стандарт функционирования с заменой лишь программного обеспечения.

Цифровое формирование лучей диаграммы направленности позволяет эффективно реализовать динамическую оптимизацию обслуживаемой зоны покрытия на основе оперативного перенацеливания цифровых приемных лучей по группам корреспондентов в зависимости от территориального распределения абонентов связи [4].

Применение ЦАР в сочетании с принципом ММО позволяет решить задачу функционирования ТРСт в условиях многолучевого распространения радиоволн и связанных с ним явлений, а также обеспечить высокую скорость передачи данных. Основным условием применения технологии ММО в ТРСт является стационарность среды распространения радиоволн на заданном интервале времени. Возможным шагом к реализации ТРСт с ЦАР является применение когнитивной технологии, когда мощность передатчика расходуется на самую оптимальную частоту, на которой в данный момент наилучшее прохождение на трассе. Рабочая частота как бы «блуждает» в некоторой полосе частот. Достаточно использовать полосу 32 МГц (в диапазоне 4,4–5,0 ГГц), в которой размещается 8 независимых частот с шагом 4 МГц, через каждые 10 мс определяется самая «оптимальная» из этих восьми частот, и очередной пакет информации передается на этой частоте. В когнитивной ТРСт непрерывно анализируются условия распространения радиоволн на трассе с определением самой оптимальной частоты.

Реализация высокотехнологичных ТРСт может быть решена на основе применения метода мультиплексирования с ортогональным частотным разделением (OFDM) для построения широкополосных систем цифровой радиосвязи по каналам с многолучевым распространением сигналов, которая позволяет эффективно бороться с частотно-селективными замираниями и обеспечивать высокую спектральную эффективность, скорость и достоверность передачи информации, устойчивость к узкополосным помехам [9, 10]. Наиболее перспективным вариантом из OFDM для тропосферных систем связи является с кодовым разделением каналов

COFDM. Применение в ТРСт OFDM модема с турбо-кодированием со скоростью от 1/2 до 1/5 позволит реализовать одновременное пространственное и частотное разнесение на двух несущих частотах (четырёхкратное разнесение) [9, 10].

С 2022 года отечественной промышленностью начато производство тропосферной станций «Гроза-1.5» в диапазоне 4,5–5 ГГц, рассчитанной на передачу данных со скоростью до 50 Мбит/с (рис. 10) [11]. Данная ТРСт обеспечивает устойчивую связь между двумя корреспондентами и предоставление высокоскоростного доступа в интернет в районах Крайнего Севера, там, где нет возможности проложить оптоволоконный или телефонный кабель. Тропосферная станция «Гроза-1.5» может функционировать и в режиме радиорелейной связи. Но весьма существенным преимуществом станции являются её массогабаритные показатели: антенна диаметром 1,5 м с усилителем мощности и модемом, что обеспечивает высокую мобильность и малые массогабаритные показатели, что и необходимо при организации связи в современных операциях.



Рис. 10. Тропосферная станция «Гроза-1.5»

Основными направлениями по совершенствованию военных тропосферных станций следует считать:

- создание единого для Вооружённых сил типа тропосферных станций в составе: мобильной возимой (с возможностью развертывания одним-двумя операторами), автомобильной (на базе защищенных машин типа «Буря», «Тигр», «Феникс») и стационарной;
- использование в составе оборудования ТРСт быстроразворачиваемых АМУ, со сменными сегментированными отражателями из легкого металлического сплава или углеродного волокна с диаметром от 1,2 до 2,4 м с системой автоматического наведения;

- увеличение пропускной способности тропосферной связи до 200 Мбит/с и более путем применения новых сигнально-кодовых конструкций модемного устройства с искусственным интеллектом;
- увеличение дальности связи на интервале до 400 км при использовании мобильных ТРСт на автомобильном шасси;
- использование методов помехозащиты, обеспечивающих увеличение значения коэффициента помехозащиты до величины 40–50 дБ;
- использование типового оборудования с интерфейсами Ethernet 10/100/1000 Мбит/с (RJ45);
- размещение оборудования малогабаритных ТРСт в составе линейных комплексных аппаратных связи с реализацией одновременной многонаправленной работы, в том числе с унификацией по механизмам РРВ (режим прямой видимости (до 50 км и более), дифракционный режим (50–100 км), тропосферный режим 100–200 км) с адаптацией пропускной способности;
- создание интеллектуальной системы управления автоматизации процессов развертывания АМУ, юстировки антенн на корреспондента, ведения связи, включения/выключения режима и методов помехозащиты, контроля качества связи и адаптации параметров оборудования;

- простота в развертывании и эксплуатации.

В заключение хотелось бы отметить, что при организации связи на дальность до 500 км мобильные тропосферные линии более эффективны по показателю затрат (количество транспортных единиц, количество обслуживающего персонала, стоимость оборудования) по сравнению с радиорелейными, спутниковыми и волоконно-оптическими линиями.

Создание новых средств тропосферной связи обеспечит развитие научных школ и восстановление утраченных компетенций в области тропосферной связи, даст импульс развития научно-производственных предприятий России занимающихся производством тропосферных станций.

Значительные размеры территории Российской Федерации, сложные климатические и природные условия, сложные географические условия предполагаемых театров военных действий определяют неоспоримые (в отдельных случаях уникальные) преимущества тропосферной связи по сравнению с другими родами связи и показывают ее значимость и востребованность в системах военной связи уже сегодня.

В тропосферных станциях аккумулированы три рода связи: тропосферная, радиорелейная и спутниковая, что подтверждает необходимость дальнейшего развития тропосферной связи как важного рода связи в военной связи.

Литература

1. Базовые средства, комплексы и системы военной связи: энциклопедический справочник. Т. 1 / Под ред. профессора Г. И. Азарова. – Мытищи: 16 ЦНИИИ МО РФ, 2005. – 119 с.
2. Антропов Д. А. Радиорелейная связь в системах управления отечественных группировок войск (сил): становление и развитие // Военно-исторический журнал. – 2023. – № 1. – С. 85–98.
3. Гусятинский И. А., Немировский А. С., Соколов А. В., Троицкий В. Н. Дальняя тропосферная радиосвязь – М.: Связь, 1968. – 248 с.
4. Анисимов В. Г., Мырова Л. О. Обоснование оптимальных способов построения перспективных тропосферных станций // T-Comm: Телекоммуникации и транспорт. – 2019. – Т. 13. – № 5. – С. 21–27.
5. Иванов В. Г. Теория и практика построения и обеспечения функционирования системы связи специального назначения с учётом технологического развития и опытов вооруженных конфликтов / Монография В. Г. Иванов. – М.: Красная Звезда, 2025. – 304 с.
6. Луферчик П. В., Луферчик А. В., Галеев Р. Г., Богатырев Е. В., Штро П. В. Повышение энергетических характеристик модема тропосферной связи // Успехи современной радиоэлектроники. – 2022. – № 76 (5). – С. 50–54.
7. Воробьев Н. А., Луферчик П. В., Штро П. В., Богатырев Е. В. Исследование характеристик нестационарности тропосферного канала связи // Журнал Ural Radio Engineering Journal. – 2023. – № 7 (2). – С. 123–136.
8. Мацков А. А., Перспективы использования линий загоризонтной связи // А. А. Мацков, В. В. Серов, Л. И. Чернобельский // Электросвязь. – 2006. – № 8. – С. 33–38.
9. Слюсар В. И., Масесов Н. А. Оценка граничных возможностей пространственного уплотнения каналов тропосферной связи в режиме мульти-ММО / В. И. Слюсар, Н. А. Масесов // XV Международная научно-техническая конференция «Информационные системы и технологии (ИСТ–2009)» Нижегородский государственный технический университет им. Р. Е. Алексеева, 2009. – С. 90–92.
10. Луферчик П. В., Комаров А. А., Штро П. В., Конев А. Н. Разработка адаптивной системы связи на основе OFDM для тропосферного и радиорелейного канала // Известия ЮФУ. Технические науки. – 2022. – № 4. – С. 244–250.
11. Михайлина Е. О. Использование новых технологий в тропосферной системе связи // Новые информационные технологии в научных исследованиях: материалы XXX Всероссийской научно-технической конференции студентов, молодых ученых и специалистов. Издательство ИП Коняхин А. В. (Book Jet). – 2025. – С. 140–141.

STATE AND DIRECTIONS OF DEVELOPMENT OF TROPOSPHERIC COMMUNICATIONS IN THE SYSTEM OF MILITARY COMMUNICATIONS OF THE ARMED FORCES

Ivanov V. G.⁴, Lukyanchik V. N.⁵, Bashirov S. Y.⁶

Keywords: communication system, tropospheric communication, military communication, tropospheric station, over-the-horizon propagation, communication development.

Abstract

The purpose of the work: to conduct a retrospective analysis of the development of tropospheric communications in the Armed Forces, to develop practical proposals for the development of tropospheric communication facilities at the present time, taking into account technological development and experience in organizing communications in a special military operation.

Research method: the methodological basis of the research is the general theory of systems, the theory of military communications, the theory of open systems using the methods of system analysis. The reliability of the results is ensured by the practical implementation of the directions of development of tropospheric communication in the military communications system of the Armed Forces attached in the article.

Results of the study: the analysis of the development of tropospheric communication facilities in the Armed Forces of the USSR, their state in the Russian Federation and in the armies of NATO countries at the present time has been carried out. Proposals have been developed on the method of application of «point-to-multipoint» and the main directions for improving military tropospheric stations.

Scientific novelty: consists in the development of substantiated directions for the development of tropospheric communications, taking into account the requirements for ensuring the management and technological development of military communications.

References

1. Bazovye sredstva, komplekсы i sistemy voennoj svyazi: ehnciklopedicheskiy spravochnik. T. 1. / Pod red. professora G. I. Azarova. Mytishchi: 16 CNII MO RF, 2005. – P. 119.
2. Antropov D. A. Radiorelejnyaya svyaz' v sistemah upravleniya otechestvennykh gruppirovok vojsk (sil): stanovlenie i razvitiye // Voенno-istoricheskij zhurnal. – 2023. – No 1. – Pp. 85–98.
3. Gusyatinskiy I. A., Nemirovskiy A. S., Sokolov A. V., Troickiy V. N. Dal'nyaya troposfernaya radiosvyaz'. M.: Svyaz', 1968. – P. 248.
4. Anisimov V. G., Myrova L. O. Obosnovanie optimal'nykh sposobov postroeniya perspektivnykh troposfernykh stancij // T-Comm: Telekommunikacii i transport. – 2019. – Vol. 13. – No 5. – Pp. 21–27.
5. Ivanov V. G. Teoriya i praktika postroeniya i obespecheniya funkcionirovaniya sistemy svyazi special'nogo naznacheniya s uchytom tehnologicheskogo razvitiya i opytov vooruzhennykh konfliktov / Monografiya V. G. Ivanov. – M.: Krasnaya Zvezda, 2025. – P. 304.
6. Luferchik P. V., Luferchik A. V., Galeev R. G., Bogatyrev E. V., Shtro P. V. Povyshenie ehnergeticheskikh harakteristik modema troposfernoj svyazi // Uspehi sovremennoj radioehlektroniki. – 2022. – No 76 (5). – Pp. 50–54.
7. Vorob'ev N. A., Luferchik P. V., Shtro P. V., Bogatyrev E. V. Issledovanie harakteristik nestacionarnosti troposfernogo kanala svyazi // Zhurnal Ural Radio Engineering Journal. – 2023. No 7 (2). – Pp. 123–136.
8. Mackov A. A., Perspektivy ispol'zovaniya linij zagorizontnoj svyazi // A. A. Mackov, V. V. Serov, L. I. Chernobel'skij // Ehlektrosvyaz'. – 2006. – No 8. – Pp. 33–38.
9. Slyusar V. I., Masesov N. A. Ocenka granichnykh vozmozhnostej prostranstvennogo uplotneniya kanalov troposfernoj svyazi v rezhime mul'ti-MIMO / V. I. Slyusar, N. A. Masesov // XV Mezhdunarodnaya nauchnotehnicheskaya konferenciya «Informacionnye sistemy i tehnologii (IST-2009)» Nizhegorodskij gosudarstvennyj tehničeskij universitet im. R. E. Alekseeva, 2009. – Pp. 90–92.
10. Luferchik P. V., Komarov A. A., Shtro P. V., Konev A. N. Razrabotka adaptivnoj sistemy svyazi na osnove OFDM dlya troposfernogo i radiorelejnogo kanala // Izvestiya YUFU. Tehničeskije nauki. – 2022. – No 4. – Pp. 244–250.
11. Mihajlina E. O. Ispol'zovanie novykh tehnologij v troposfernoj sisteme svyazi // Novye informacionnye tehnologii v nauchnykh issledovaniyakh: materialy XXX Vserossijskoj nauchno-tehničeskoj konferencii studentov, molodyh uchenykh i specialistov / Izdatel'stvo IP Konyahin A. V. (Book Jet). – 2025. – Pp. 140–141.

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

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

6. **Sergey Yu. Bashirov**, Deputy Head of the Department of the Main Directorate of Communications of the Armed Forces of the Russian Federation. Moscow, Russia. E-mail: wasj2006@yandex.ru

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ АЛГОРИТМА ПОДСТРОЙКИ КОЭФФИЦИЕНТОВ АДАПТИВНОЙ АНТЕННОЙ РЕШЕТКИ

Цветков Д. Е.¹, Федоров П. Н.²

DOI:10.21681/3034-4050-2026-3-13-20

Ключевые слова: диаграмма направленности, пространственная фильтрация, весовые коэффициенты, алгоритмы адаптации, безопорные алгоритмы, методы подпространств, матрица ковариации, математическое моделирование, подавление помех, робастность.

Аннотация

Цель работы состоит в анализе и разработке математической модели алгоритма адаптации весовых коэффициентов для адаптивных антенных решеток (ААР), а также в оценке его эффективности при подавлении сложных пространственно-распределенных радиопомех.

Методы исследования: математическое и имитационное моделирование в программной среде MatLab, а также методы матричной алгебры, теории случайных процессов и статистической радиотехники для расчета корреляционных матриц и весовых векторов. Для оценки качества пространственной фильтрации использовался сравнительный анализ вычислительной сложности классических градиентных методов и селективности современных робастных безопорных алгоритмов при различных угловых распределениях источников помех.

Результаты исследования показали, что для мобильных систем с жесткими ограничениями аппаратных ресурсов наиболее эффективным является алгоритм наименьших средних квадратов (LMS), который благодаря линейной вычислительной сложности обеспечивает уверенное формирование глубоких нулей в направлении источников помех. При этом установлено, что в условиях априорной неопределенности и отсутствия опорного сигнала классические методы теряют работоспособность, что требует перехода к безопорным алгоритмам. Моделирование сложных многокомпонентных помех выявило критическую уязвимость стандартного метода LCMV к ошибкам пеленгации, приводящую к эффекту самоподавления полезного сигнала. Для решения этой проблемы успешно протестирован модифицированный робастный алгоритм RAIS-LCMV. Испытания доказали, что его применение в стационарных режимах инициализации позволяет итеративно реконструировать фактический вектор направленности на основе глубокого анализа собственных векторов ковариационной матрицы. Это полностью исключает эффект самоподавления и гарантирует формирование многолучевых глубоких провалов диаграммы направленности точно на источники комбинированных помех, сохраняя при этом максимальный коэффициент передачи в направлении целевого сигнала.

Практическая ценность исследования заключается в комплексном обосновании гибридного подхода к пространственной фильтрации, объединяющего высокоточную инициализацию решетки робастным алгоритмом RAIS-LCMV в стационарном режиме с последующим переходом на малозатратные градиентные методы в динамике. Математически доказана эффективность данного подхода для устранения эффекта самоподавления сигнала в условиях многокомпонентного радиоэлектронного противодействия.

Введение

Стремительное развитие современных радиотехнических систем, включая комплексы радиолокации, сети мобильной связи поколений 5G/6G и системы радиоэлектронной борьбы (РЭБ), требует принципиально новых подходов к помехозащищенности. Традиционные методы частотной и временной фильтрации оказываются недостаточно эффективными в условиях плотного электромагнитного спектра и преднамеренных широкополосных воздействий. Решением этой проблемы стало массовое внедрение адаптивных антенных решеток (ААР).

Антенная решётка представляет собой набор идентичных антенных элементов, определенным образом размещённых в пространстве. Ключевое отличие ААР от классических фазированных антенных решеток (ФАР) заключается в наличии полнофункционального цифрового диаграммообразующего устройства (блок пространственной обработки сигнала) и встроенных математических алгоритмов оптимизации (рис. 1). Главная особенность таких систем – это способность автоматически и в реальном времени изменять свои пространственные характеристики (адаптировать форму диаграммы направленности) для

¹ Цветков Дмитрий Евгеньевич, оператор научной роты, Военная академия связи им. Маршала Советского Союза С. М. Будённого. Санкт-Петербург, Россия. E-mail: tsvetkovde123@gmail.com

² Федоров Павел Николаевич, старший научный сотрудник НИО-4 Военной академии связи им. Маршала Советского Союза С.М. Будённого. Санкт-Петербург, Россия. E-mail: fedorovpn1@yandex.ru

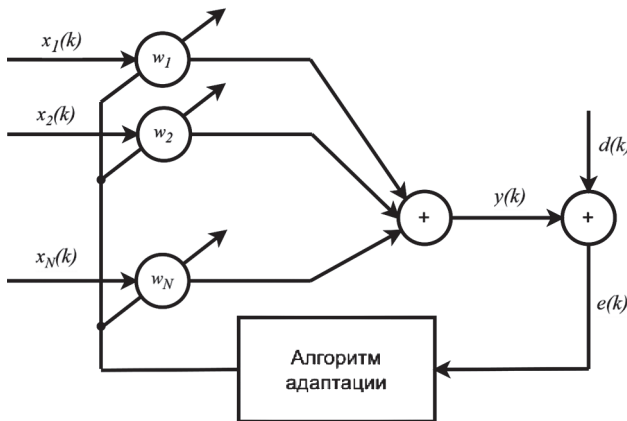


Рис. 1. Структурная схема адаптивной антенной решетки

максимизации отношения сигнал/помеха+шум (SINR).

Архитектура современной цифровой ААР состоит из нескольких фундаментальных компонентов.

Во-первых, это сама геометрия решетки: линейная, плоская или конформная. Для исключения эффекта появления дифракционных максимумов или «ложных лепестков» расстояние между соседними элементами обычно выбирается равным половине длины волны ($\lambda/2$).

Во-вторых, приемопередающие модули: каждый антенный элемент связан со своим независимым радиочастотным трактом, включающим маломощный усилитель, аналого-цифровой преобразователь (АЦП) и цифровой квадратурный демодулятор.

В-третьих, высокопроизводительный цифровой сигнальный процессор или ПЛИС, который непосредственно реализует сложные алгоритмы вычисления весовых коэффициентов.

Основной физический принцип работы ААР базируется на явлении пространственной интерференции электромагнитных волн. Управление формой луча осуществляется посредством комплексного взвешивания. Когда электромагнитные волны, принимаемые каждым элементом решетки, после цифрового сдвига фаз программно совмещаются в фазе для определенного угла прихода, они интерферируют конструктивно. В результате происходит когерентное сложение (синтез остронаправленного главного лепестка). Если же фазы не совпадают, волны гасят друг друга (деструктивная интерференция). Интеллектуально манипулируя амплитудой и фазой каждого канала, система формирует глубокие «нули» (зоны подавления до $-30...-50$ дБ) диаграммы направленности точно в направлениях источников активных помех [1, 2].

Математический аппарат пространственной фильтрации

Способность динамически перестраивать диаграмму направленности достигается путем перемножения вектора входных сигналов $X(t)$ на комплексный весовой вектор

$$W = [w_1, w_2, \dots, w_N]^T, \quad (1)$$

где N – количество элементов антенной решетки.

В общем виде модель принимаемого сигнала можно описать векторно-матричным уравнением:

$$X(t) = A(\theta)S(t) + \sum_{i=1}^K A(\theta_i)J_i(t) + N(t), \quad (2)$$

где $A(\theta)$ – вектор пространственной направленности полезного сигнала $S(t)$, приходящего с угла θ ; $J_i(t)$ – сигналы K независимых источников помех; $N(t)$ – вектор шума приемников (аддитивный белый гауссовский шум).

Выходной сигнал системы формируется как скалярное произведение вектора весов и вектора принятых сигналов (в эрмитовом сопряжении):

$$y(t) = W^H X(t). \quad (3)$$

Фундаментальной математической задачей всех алгоритмов пространственной адаптации является поиск такого оптимального вектора W_{opt} , который минимизирует среднеквадратическую ошибку (СКО) между выходным сигналом $y(t)$ и некоторым известным эталонным сигналом $d(t)$. Эта задача описывается классическим уравнением Винера-Хопфа:

$$W_{opt} = R_{xx}^{-1} r_{xd}, \quad (4)$$

где $R_{xx} = E[X(t)X^H(t)]$ – пространственная корреляционная матрица входных сигналов; $r_{xd} = E[X(t)d^*(t)]$ – вектор взаимной корреляции между входным вектором и эталонным сигналом.

На практике точное вычисление уравнения Винера-Хопфа затруднено из-за необходимости обращения матрицы R_{xx} . Поэтому используются адаптивные методы, которые были проанализированы в ходе исследования: LMS, SMI и RLS.

Алгоритм SMI (Sample Matrix Inversion) использует метод прямой оценки, который вычисляет приближенную (выборочную) матрицу ковариации:

$$\hat{R} = \frac{1}{K} \sum_{n=1}^K X(n)X^H(n), \quad (5)$$

на ограниченном временном окне в K отсчетов, а затем напрямую обращает её:

$$W_{SMI} = \hat{R}^{-1} r_{xd}. \quad (6)$$

Хотя SMI обеспечивает чрезвычайно высокую скорость сходимости (достаточно $2N$ отсчетов),

алгоритм обладает кубической вычислительной сложностью $O(N^3)$ из-за операции обращения матрицы. При большом числе элементов ААР это делает его непрактичным, к тому же алгоритм крайне чувствителен к сингулярности (числовой обусловленности) матрицы [3].

Алгоритм RLS (Recursive Least Squares) использует лемму об обращении матриц для рекурсивного обновления обратной корреляционной матрицы без прямого вычисления обратной матрицы на каждом такте. Математический аппарат включает вычисление калмановского вектора усиления $k(n)$ и пересчет матрицы с использованием «параметра забывания» λ (где $0 < \lambda \leq 10 < \lambda \leq 1$). Параметр забывания позволяет алгоритму адаптироваться к нестационарным каналам: чем меньше λ , тем быстрее система «забывает» старые данные. Сложность RLS составляет $O(N^2)$, что делает его оптимально сбалансированным с точки зрения скорости и сложности вычисления, однако для высокоскоростных боевых комплексов ресурсов процессора все еще может не хватать [4].

Алгоритм LMS (Least Mean Squares) обладает наименьшей вычислительной мощностью. Он представляет собой итеративную процедуру стохастического градиентного спуска. Вместо работы с полными матрицами, он использует мгновенные оценки градиента [5]. Ошибка вычисляется по формуле

$$e(n) = d(n) - y(n). \quad (7)$$

Обновление весовых коэффициентов выполняется по выражению:

$$W(n+1) = W(n) + \mu X(n)e^*(n), \quad (8)$$

где μ – параметр шага адаптации.

Вычислительная сложность алгоритма линейна $O(N)$. Ключевой проблемой LMS является выбор шага μ : слишком большое значение приведет к расходимости алгоритма, а слишком малое – к критически медленной сходимости: алгоритм не успеет перестроиться при быстром движении источника помехи. Медленная сходимость особенно проявляется при работе с сильно коррелированными сигналами (когда число обусловленности корреляционной матрицы велико). Однако в условиях ограниченных ресурсов и энергопотребления (например, беспилотные аппараты), LMS является оптимальным выбором с точки зрения применения на БПЛА [6, 7, 8].

Имитационное моделирование алгоритма LMS в среде MatLab

Для верификации теоретических выкладок и детального анализа переходных процессов в программной среде MatLab была создана

развернутая имитационная модель ААР. Была смоделирована эквидистантная решетка, состоящая из 4 антенных элементов с шагом $d = \lambda/2$. Соотношение сигнал/шум (SNR) было установлено на уровне 10 дБ, а отношение помеха/шум (INR) – на уровне 30 дБ (мощная подавляющая помеха).

В разработанной модели полезный (управляющий) сигнал был зафиксирован под углом 30° относительно нормали решетки. Направленная широкополосная помеха программно меняла угол прихода в азимутальном диапазоне от 0° до 360° . Для оценки качества адаптации анализировалась глубина формируемых нулей и уровень боковых лепестков.

Результаты моделирования подтвердили высокую эффективность LMS для задач пространственной фильтрации. На полярных и декартовых графиках отчетливо видно, как система в реальном времени подстраивает веса под меняющуюся обстановку. При удаленном расположении сигнала помехи (например, азимут 210°) алгоритм уверенно формирует глубокий нуль с коэффициентом подавления, достигающим -35 дБ относительно максимума главного лепестка (рис. 2). При этом сигнал управления не искажается и сохраняет максимальный коэффициент направленного действия по направлению своего прихода (азимут 30°).

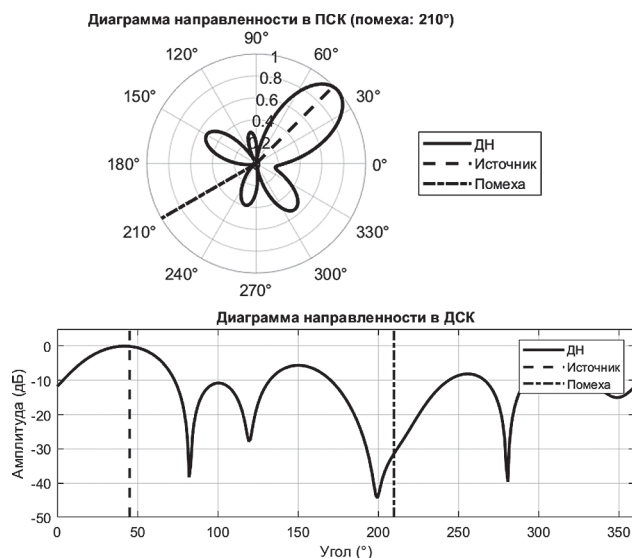


Рис. 2. Диаграмма направленности при угле прихода сигнала помехи 210°

Особый интерес представляло моделирование сложных граничных условий. При сближении пеленга помехи с направлением на полезный сигнал (например, при направлении прихода помехи 15° и направлении прихода сигнала управления с 30°), формирование

классического «глубокого нуля» становится физически невозможным из-за конечной ширины главного лепестка (определяемой апертурой антенны). В этом случае алгоритм переходит в режим компромиссной оптимизации: глубина нуля уменьшается, но уровень диаграммы направленности в направлении полезного сигнала все равно поддерживается выше, чем в направлении помехи (рис. 3). Это гарантирует сохранение связи даже при плотном сближении источников.

Наихудший теоретический результат алгоритм LMS продемонстрировал при абсолютном совпадении углов прихода помехи и полезного сигнала. В этом случае пространственное разнесение отсутствует, уровни приема совпадают, и ААР теряет способность отфильтровать помеху пространственным методом (рис. 4). Подавление в таком сценарии может быть реализовано только за счет временной или поляризационной селекции. Впрочем, на практике вероятность столь точного совпадения векторов крайне мала.

Безопорные алгоритмы: работа в условиях априорной неопределенности

Несмотря на стабильность и легкость LMS, его применение обусловлено жестким требованием – наличием в приемнике копии эталонного сигнала $d(n)$. В реальных системах, например, при внезапном воздействии РЭБ, глубоких многолучевых замираниях или в системах радиоразведки, когда параметры сигнала противника неизвестны, опорный сигнал недоступен. В таких случаях классические методы становятся

неработоспособными, что диктует переход к классу безопорных алгоритмов адаптации.

Безопорные алгоритмы базируются исключительно на статистических, пространственно-временных свойствах общего принимаемого сигнала и не нуждаются в обучающей последовательности. Основной целью таких алгоритмов является минимизация выходной мощности шумов и помех при строгом сохранении чувствительности (коэффициента передачи) антенной системы в предполагаемом направлении прихода полезного сигнала.

Среди обширного семейства безопорных методов можно выделить несколько фундаментальных направлений:

1. Алгоритмы на основе постоянства огибающей (Constant Modulus Algorithm, CMA). Используют априорную информацию о статистике модуляции полезного сигнала (например, что сигнал имеет фазовую модуляцию PSK/QAM и его амплитуда должна быть постоянной). Алгоритм штрафует любые отклонения огибающей от константы, тем самым подавляя интерференционные помехи.
2. Алгоритмы максимизации энтропии и методы высших порядков. Анализируют статистику распределения сигнала, опираясь на то, что сумма независимых сигналов (помех) стремится к гауссовскому распределению. Максимизация аномалий данного распределения позволяет выделить полезный сигнал из шума.
3. Методы подпространств. Это класс алгоритмов высокого разрешения (родственный методам MUSIC и ESPRIT). Они основаны

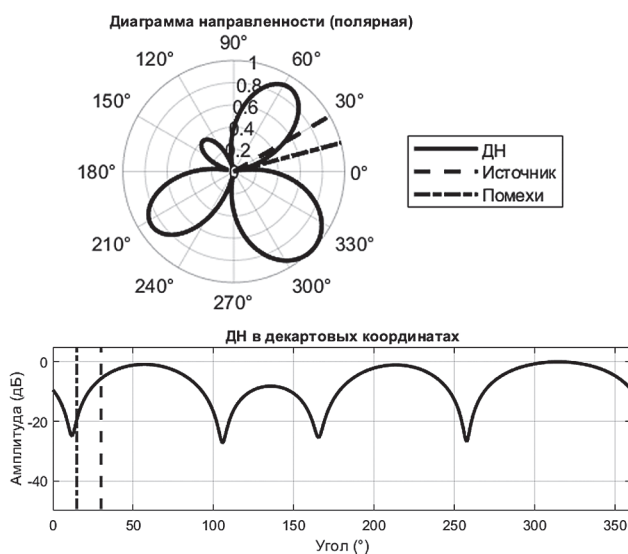


Рис. 3. Диаграмма направленности при угле прихода сигнала помехи 35°

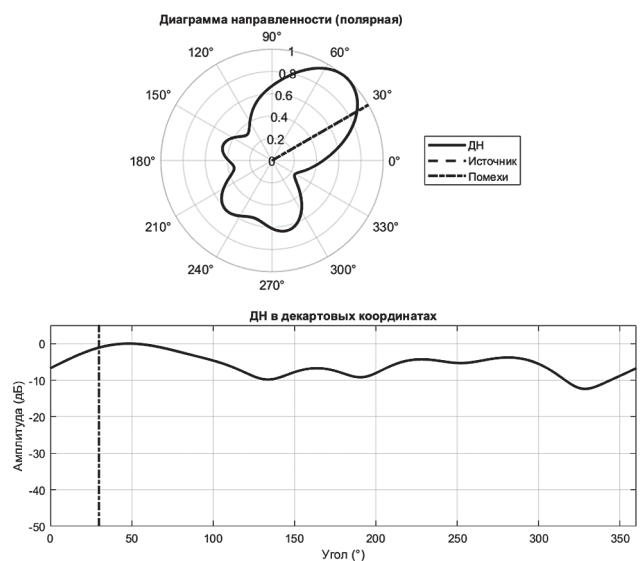


Рис. 4. Диаграмма направленности при угле прихода сигнала помехи 30°

на спектральном (сингулярном) разложении корреляционной матрицы R_{xx} на собственные векторы и собственные значения. Пространство сигналов математически разделяется на ортогональные друг другу сигнальное подпространство и шумовое подпространство. Адаптация весовых коэффициентов производится так, чтобы проекция вектора весов на шумовое подпространство была максимальной, а на помеховое – минимальной. Методы подпространств обладают феноменальной селективностью, однако спектральное разложение матрицы $O(N^3)$ критически увеличивает вычислительную нагрузку [8, 9, 10].

К наиболее распространенному и практичному классу безопорных алгоритмов относятся методы минимальной дисперсии, основанные на градиентном спуске. Адаптация весов в них осуществляется путём поэтапной корректировки вектора в направлении антиградиента выбранной функции стоимости. Благодаря относительной простоте, эти методы отлично ложатся на архитектуру ПЛИС. Результаты моделирования безопорного градиентного алгоритма в MatLab продемонстрировали устойчивую сходимость (рис. 5) и подтвердили, что геометрия решетки выступает ключевым фактором: плоские решетки сходятся быстрее линейных в условиях 3D-распределения помех.

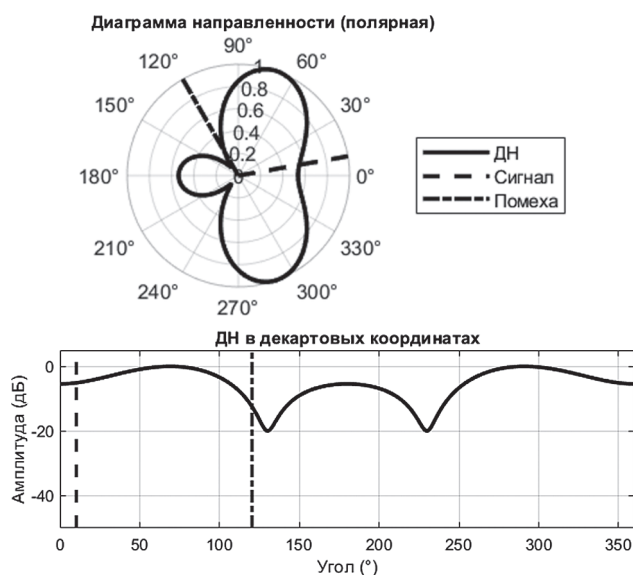


Рис. 5. Результат работы алгоритма градиентного спуска

Логическим продолжением исследования стало моделирование работы безопорной ААР в условиях сложных комбинированных помех, где эфир загрязняется несколькими мощными независимыми передатчиками с разных азимутов. Варьировались мощности источников и их угловое

распределение. Анализ показал, что увеличение количества помех усложняет многомерную топологию функции стоимости (появляются локальные минимумы) и требует применения адаптивного шага μ . Тем не менее, имитационная модель успешно продемонстрировала формирование нескольких глубоких нулей, доказав способность системы решать задачи многолучевого подавления (рис. 6).

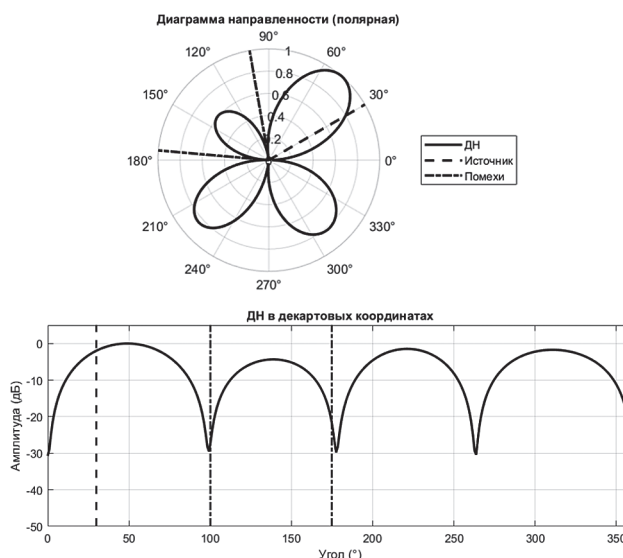


Рис. 6. Диаграмма направленности ААР при воздействии двух сигналов помех

Финальные испытания: Алгоритмы LCMV и робастный RAIS-LCMV

Завершающим этапом исследования стали финальные испытания разработанной имитационной модели в условиях стационарной многокомпонентной помеховой обстановки с применением алгоритмов класса минимальной дисперсии с линейными ограничениями – LCMV (Linearly Constrained Minimum Variance).

Математическая суть LCMV заключается в решении задачи условной оптимизации: необходимо минимизировать общую выходную мощность антенны $W^H R_{xx} W \rightarrow \min$, соблюдая при этом набор жестких линейных ограничений:

$$C^H W = f, \quad (9)$$

где C – матрица ограничений, содержащая вектор направленности на цель; f – вектор откликов (единичный, чтобы гарантировать, что сигнал с заданного направления пройдет без ослабления).

Однако у классического LCMV есть фундаментальный недостаток – возможный эффект самоподавления полезного сигнала. Если априорная информация об угле прихода полезного сигнала хотя бы на доли градуса отличается от реальной (например, из-за неточности

калибровки антенны, многолучевости или деформации корпуса носителя), алгоритм воспримет полезный сигнал как помеху и направит на него глубокий ноль.

Для преодоления этой уязвимости в модели был рассмотрен модифицированный алгоритм RAIS-LCMV (Robust Adaptive Iterative Steering LCMV). Робастность (повышенная устойчивость) в нем достигается за счет итеративной математической реконструкции фактического вектора направленности на основе анализа собственных векторов ковариационной матрицы, а также применения методов диагонального нагружения корреляционной матрицы, что сглаживает ошибки целеуказания [11, 12].

В рамках испытаний алгоритм RAIS-LCMV рассматривался как основной режим инициализации системы в стационарных условиях (до начала движения подвижного носителя ААР). В стационарном режиме отсутствует эффект Доплера и быстрая смена углов, что позволяет накопить объемную статистическую выборку, рассчитать корреляционную матрицу без искажений и выполнить итеративное уточнение вектора. Результаты испытаний со сценариями воздействия нескольких разнонаправленных помеховых станций доказали высочайшую эффективность подхода: RAIS-LCMV полностью исключил эффект самоподавления полезного сигнала, продемонстрировав предельно глубокие нули в зонах помех.

Заключение

В представленной работе был проведен всесторонний анализ алгоритмов пространственно-временной обработки сигналов для цифровых адаптивных антенных решеток. Разработанная

на базе среды MatLab математическая имитационная модель позволила детально исследовать физику формирования диаграммы направленности и оценить поведение системы в сложной электромагнитной обстановке.

Доказано, что для систем, функционирующих в динамичном режиме с жесткими ограничениями на вычислительные мощности (бортовые системы БПЛА, тактические радиостанции), алгоритм стохастического градиентного спуска LMS является оптимальным выбором. Он гарантирует уверенное подавление одиночных и групповых помех с вычислительной сложностью всего $O(N)$.

С другой стороны, вскрыта проблематика априорной неопределенности, когда отсутствие опорного сигнала требует внедрения безопорных алгоритмов. Выполненный анализ методов подпространств и алгоритмов минимальной дисперсии показал их высокий потенциал, но выявил проблему критической уязвимости классического LCMV к ошибкам пеленгации (эффект самоподавления).

Успешная реализация и тестирование робастного алгоритма RAIS-LCMV предлагает элегантное решение этой проблемы. Его применение признано наиболее целесообразным для стационарных режимов инициализации радиотехнических комплексов: он с высокой точностью оценивает параметры эфира и реконструирует векторы направленности, формируя глубокие защитные барьеры-нули против сложных комбинированных помех. Синтез рассмотренных методов открывает широкие перспективы для создания гибридных, высокоинтеллектуальных систем радиосвязи и радиолокации нового поколения.

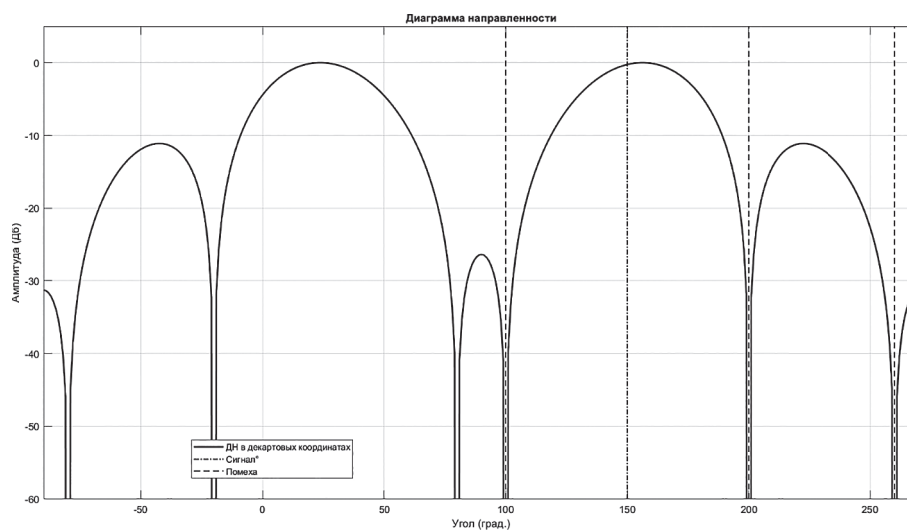


Рис. 7. Диаграмма направленности ААР при применении алгоритма RAIS-LCMV

Литература

1. Звонарев В. В., Питрин А. В., Попов А. С. Методика расчета коэффициента направленного действия адаптивной антенной решетки при наличии помех // Изв. вузов. Приборостроение, 2025. – Т. 68. – № 3. – С. 198–206.
2. An Adaptive Five-Element Array Antenna Based on Miniaturised Polarisation-Insensitive Absorptive Metamaterial for Anti-Jamming Applications / G. Wang, X. Tang, F. Huang [et al.] // IET Microwaves Antennas & Propagation, 2025. – Vol. 19. – No. 1. – P. e70056.
3. Shima, K. Data-Aided SMI Algorithm Using Common Correlation Matrix for Adaptive Array Interference Suppression / K. Shima, K. Maruta, Ch. Ju. Ahn // IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2021. – Vol. E104.A. – No 2. – Pp. 404–411.
4. Кащенко И. Е. Регуляризация RLS-алгоритма для адаптивных систем ввода цифровых предсказаний / И. Е. Кащенко, А. П. Павлов // Радиотехника, 2024. – Т. 88. – № 1. – С. 141–148.
5. An efficient normalized LMS algorithm / A. Zerguine, Ja. Ahmad, M. Moinuddin [et al.] // Nonlinear Dynamics, 2022. – Vol. 110. – No. 4. – Pp. 3561–3579.
6. Praneet R. J., Kumar C. A., Rajendra N. A novel sign variable step size LMS (SiVSS-LMS) algorithm for adaptive beamforming // CSIT, 2020. – 8 (4). – Pp. 377–384.
7. Бойко И. А., Глушанков Е. И., Лялина А. Ж. Алгоритмы адаптивной обработки сигналов в геостационарных системах // Труды учебных заведений связи, 2025. – Т. 11. – № 5. – С. 74–83.
8. Wnuk, M. Adaptive Antenna Array Control Algorithm in Radiocommunication Systems // Algorithms, 2024. – Vol. 17. – No 2. – P. 81.
9. Глушанков Е. И., Царик И. В., Царик В. И. Пространственно-распределенная технология адаптивного формирования диаграммы направленности антенной решетки // Научные известия, 2022. – № 29. – С. 165–170.
10. Чистяков В. А. Алгоритм адаптивной фильтрации помех в цифровых антенных решетках спутниковой связи // Труды МАИ, 2019. – В. 105. – С. 100–113.
11. Meng, Zh. Robust widely linear beamforming using estimation of extended covariance matrix and steering vector / Zh. Meng, W. Zhou, S. Gazor // Eurasip Journal on Wireless Communications and Networking, 2020. – Vol. 2020. – No 1. – Pp. 1–20.
12. Guo X., Chu L., Li B. Robust Adaptive LCMV Beamformer Based on an Iterative Suboptimal Solution. // Radioengineering, 2015. – Vol. 24. – No 2. – P. 572–581.

MATHEMATICAL MODEL OF THE ALGORITHM FOR ADJUSTING THE COEFFICIENTS OF THE ADAPTIVE ANTENNA ARRAY

Tsvetkov D. E.³, Fedorov P. N.⁴

Keywords: radiation pattern, spatial filtering, weight coefficients, adaptation algorithms, unsupported algorithms, subspace methods, covariance matrix, mathematical modeling, interference suppression, robustness.

Abstract

The aim of the work is to analyze and develop a mathematical model of the algorithm for adapting weight coefficients for adaptive antenna arrays (AAR), as well as to assess its effectiveness in suppressing complex spatially distributed radio interference.

The research method is mathematical and simulation modeling in the MatLab software environment, as well as methods of matrix algebra, theory of random processes and statistical radio engineering for calculating correlation matrices and weight vectors. To assess the quality of spatial filtering, a comparative analysis of the computational complexity of classical gradient methods and the selectivity of modern robust unsupported algorithms at different angular distributions of sources was used interference.

The results of the study showed that for mobile systems with severe hardware resource constraints, the least mean squares (LMS) algorithm is the most effective, which, due to linear computational complexity, provides a confident formation of deep zeros in the direction of interference sources. At the same time, it was established that under conditions of a priori uncertainty and the absence of a reference signal, classical methods lose their performance, which requires a transition to unsupported algorithms. Simulation of complex multi-component interference revealed a critical vulnerability of the standard LCMV method to direction finding errors, leading to the effect of self-rejection of the desired signal. To solve this problem, the modified robust RAIS-LCMV algorithm was successfully tested. The tests proved that its use in stationary initialization modes makes it possible to iteratively reconstruct the actual directional vector based on an in-depth analysis of the eigenvectors of the covariance matrix. This completely eliminates the effect of self-rejection and ensures that multipath deep dips are generated precisely to the sources of combined interference, while maintaining the maximum transmission ratio in the direction of the target signal.

³ **Dmitry E. Tsvetkov**, operator of the scientific company, Military Academy of Communications named after Marshal of the Soviet Union S. M. Budyonny. St. Petersburg, Russia. E-mail: tsvetkovde123@gmail.com

⁴ **Pavel N. Fedorov**, Senior Researcher of the Research Institute-4 of the Military Academy of Communications named after Marshal of the Soviet Union S. M. Budyonny. St. Petersburg, Russia. E-mail: fedorovpn1@yandex.ru

The practical value of the study lies in the comprehensive substantiation of a hybrid approach to spatial filtering, which combines high-precision lattice initialization by the robust RAIS-LCMV algorithm in a stationary mode with the subsequent transition to low-cost gradient methods in dynamics. The effectiveness of this approach for eliminating the effect of signal self-suppression in conditions of multicomponent electronic countermeasures is mathematically proved.

References

1. Zvonarev V. V., Pitrin A. V., Popov A. S. Metodika rascheta koehfficienta napravlennoogo dejstviya adaptivnoj antennoj reshetki pri naliczii pomeh // Izv. vuzov. Priborostroenie, 2025. – V. 68. – No 3. – Pp. 198–206.
2. An Adaptive Five-Element Array Antenna Based on Miniaturised Polarisation-Insensitive Absorptive Metamaterial for Anti-Jamming Applications / G. Wang, X. Tang, F. Huang [et al.] // IET Microwaves Antennas & Propagation, 2025. – Vol. 19. – No. 1. – P. e70056.
3. Shima, K. Data-Aided SMI Algorithm Using Common Correlation Matrix for Adaptive Array Interference Suppression / K. Shima, K. Maruta, Ch. Ju. Ahn // IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2021. – Vol. E104.A. – No 2. – Pp. 404–411.
4. Kashchenko I. E. Regularizaciya RLS-algoritma dlya adaptivnyh sistem vvoda cifrovyyh predyskazhenij / I. E. Kashchenko, A. P. Pavlov // Radiotekhnika, 2024. – V. 88. – No 1. – Pp. 141–148.
5. An efficient normalized LMS algorithm / A. Zerguine, Ja. Ahmad, M. Moinuddin [et al.] // Nonlinear Dynamics, 2022. – Vol. 110. – No. 4. – Pp. 3561–3579.
6. Praneet R. J., Kumar C. A., Rajendra N. A novel sign variable step size LMS (SiVSS-LMS) algorithm for adaptive beamforming // CSIT, 2020. – 8 (4). – Pp. 377–384.
7. Bojko I. A., Glushankov E. I., Lyalina A. Zh. Algoritmy adaptivnoj obrabotki signalov v geostacionarnyyh sistemah // Trudy uchebnyh zavedenij svyazi, 2025. – V. 11. – No 5. – Pp. 74–83.
8. Wnuk, M. Adaptive Antenna Array Control Algorithm in Radiocommunication Systems // Algorithms, 2024. – Vol. 17. – No 2. – P. 81.
9. Glushankov E. I., Carik I. V., Carik V. I. Prostranstvenno-raspredeleonnaya tehnologiya adaptivnogo formirovaniya diagrammy napravlennosti antennoj reshetki // Nauchnye izvestiya, 2022. – No 29. – Pp. 165–170.
10. Chistyakov V. A. Algoritmy adaptivnoj fil'tracii pomeh v cifrovyyh antennyh reshetkah sputnikovoy svyazi // Trudy MAI, 2019. – V.105. – Pp. 100–113.
11. Meng, Zh. Robust widely linear beamforming using estimation of extended covariance matrix and steering vector / Zh. Meng, W. Zhou, S. Gazor // Eurasip Journal on Wireless Communications and Networking, 2020. – Vol. 2020. – No 1. – Pp. 1–20.
12. Guo X., Chu L., Li B. Robust Adaptive LCMV Beamformer Based on an Iterative Suboptimal Solution // Radioengineering, 2015. – Vol. 24. – No 2. – P. 572–581.



ПРИНЦИПЫ ПОСТРОЕНИЯ ПАЙПЛАЙНОВ С ДИНАМИЧЕСКОЙ АРХИТЕКТУРОЙ И АГЕНТНЫМ УПРАВЛЕНИЕМ

Лукашенко В. И.¹, Изотов Д. Ю.²

DOI:10.21681/3034-4050-2026-3-21-28

Ключевые слова: динамические пайплайны, агентное управление, адаптивная архитектура, самоорганизация, масштабируемость, декомпозиция задач.

Аннотация

Цель работы: обосновать методологический подход к построению пайплайнов с динамической архитектурой, управляемых автономными программными агентами, способными адаптироваться к изменяющимся условиям выполнения задач.

Метод исследования: метод исследования сочетает принципы модульного проектирования, теорию много-агентных систем и методы имитационного моделирования для анализа поведения динамических пайплайнов.

Результаты исследования: представлен формализованный подход к описанию жизненного цикла агентов, их взаимодействия и эволюции топологии пайплайна, что позволяет осуществлять моделирование различных сценариев функционирования системы в условиях внешних возмущений. Сформулированы научно обоснованные принципы проектирования агентно-управляемых архитектур, включая критерии выбора granularity агентов, стратегии коммуникации и механизмы принятия решений. Эти аспекты будут положены в основу дальнейшего развития фреймворков для построения адаптивных систем обработки данных.

Научная новизна: обоснован принцип построения пайплайнов с динамической архитектурой и агентным управлением, рассматриваемые как взаимодополняющие механизмы адаптации.

Введение

В современном мире, где объемы обрабатываемых данных растут экспоненциально, а требования к скорости и качеству принятия решений ужесточаются, важность гибких и адаптивных вычислительных архитектур становится очевидной. Традиционные статические пайплайны обработки данных, характеризующиеся жестко заданной последовательностью операций, все чаще оказываются неспособными эффективно реагировать на изменения входных потоков, вариативность вычислительных ресурсов и динамические требования бизнес-процессов [1, 2].

Интеграция принципов динамической архитектуры и агентного управления представляет собой перспективное направление развития распределенных систем. Динамическая архитектура позволяет пайплайну изменять свою структуру в процессе выполнения: добавлять или исключать этапы обработки, перенаправлять потоки данных, масштабировать компоненты в зависимости от нагрузки [3, 4]. Агентное управление, в свою очередь, обеспечивает децентрализованное принятие решений, где автономные программные агенты координируют

свою деятельность для достижения общих целей системы^{3,4}[5].

Для обоснования эффективности проектируемых динамических пайплайнов применяется множество методов оценки. В основном анализ проводится на основе метрик производительности, задержек, использования ресурсов и отказоустойчивости, что позволяет использовать результаты при разработке промышленных решений. Ключевой характеристикой таких систем является адаптивность – способность изменять поведение и структуру в ответ на внешние и внутренние стимулы^{5,6}[6, 7]. Адаптивность косвенно определяет живучесть системы, т.е. способность сохранять работоспособность при частичных отказах компонентов или изменении условий функционирования.

В статье [8] рассматривается метод оркестрации микросервисов на основе правил и событий. В отличие от предыдущего примера, здесь предлагается алгоритм динамического перепланирования потоков данных, используя метрики загрузки узлов, приоритеты задач и ограничения по времени. Математические модели и программная реализация позволяют анализировать

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

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

3 Wooldridge M. An Introduction to Multiagent Systems // M. Wooldridge. 2nd ed. / Chichester: Wiley, 2009. – 488 p.

4 Weiss G. Multiagent Systems: A Modern Approach to Distributed Artificial Intelligence / G. Weiss // Cambridge: MIT Press, 2000. – 640 p.

5 Huebscher M. C. A Survey of Autonomic Computing: Degrees, Models, and Applications / M. C. Huebscher, J. A. McCann // ACM Computing Surveys, 2008. – Vol. 40. – No 3. – Article 7. – DOI: 10.1145/1380584.1380585.

6 Kephart J. O. The Vision of Autonomic Computing / J. O. Kephart, D. M. Chess // Computer, 2003. – Vol. 36. – No 1. – Pp. 41–50. – DOI: 10.1109/MC.2003.1160055.

зависимость показателей эффективности от различных параметров, таких как частота поступления задач и доступность вычислительных ресурсов. Эти методы обеспечивают точную оценку производительности системы, но требуют значительных вычислительных ресурсов и сложных моделей для анализа.

Таким образом, оценка адаптивности и эффективности динамических пайплайнов с агентным управлением является важным параметром устойчивости и, как следствие – надежности системы, и в современных условиях создания и проектирования новых распределенных архитектур является актуальным направлением исследования. Гипотеза настоящего исследования заключается в предположении, что адаптивность динамических пайплайнов с агентным управлением может быть количественно оценена с использованием марковских моделей при допущении о стационарности вероятностей переходов между состояниями агентов, а предложенный подход к расчету позволяет выявлять критические точки структуры и прогнозировать поведение системы при внешних возмущениях с приемлемой для инженерной практики точностью. В качестве инструментария исследования выступает комплекс методов, включающий теорию многоагентных систем для описания поведения автономных сущностей, аппарат цепей Маркова для формализации переходов между состояниями, а также среду имитационного моделирования на платформе Python с использованием библиотек `numpy` и `matplotlib` для реализации вычислительных экспериментов и визуализации полученных зависимостей. Этому вопросу и посвящена данная статья.

Анализ предмета исследования и постановка задачи

Анализ существующих подходов к построению адаптивных пайплайнов показывает, что они в основном основаны на предопределенных правилах переконфигурации или реактивных механизмах масштабирования. Основным их недостатком является то, что они не учитывают семантическую связность между этапами обработки, т.е. насколько изменения в одном компоненте влияют на эффективность работы всей системы, и как адаптировать поведение агентов при изменении контекста выполнения задач.

Основополагающей частью работы является математическая модель оценки адаптивности сложных систем с децентрализованным управлением [9]:

$$S = \{A_1, A_2, \dots, A_n\}, n \in N, \quad (1)$$

где S – система, а каждый агент A_i характеризуется:

- вектором состояния $x_i(t) \in R^{d_i}$;
- вектором управления $u_i(t) \in R^{m_i}$;
- входным сигналом среды $y_i(t) \in R^{p_i}$;
- функцией полезности $J_i(x_i, u_i, y_i)$.

В данной статье предложена математическая модель построения пайплайнов, которая учитывает влияние динамических факторов на координацию между агентами системы. Особенностью модели является учет стохастического характера поступления задач и вариативности времени выполнения операций, что формализуется через случайный процесс поступления заявок с интенсивностью $\lambda(t)$ и случайное время обслуживания $\tau_i e(\mu_i)$ для каждого агента.

На основе предложенной формализации можно выделить два фундаментальных принципа построения динамических пайплайнов с агентным управлением. Первый принцип – декомпозиции на автономные агенты – заключается в разбиении вычислительного процесса на множество слабосвязанных сущностей (агентов), каждая из которых обладает собственным вектором состояния $x_i(t)$ и функцией полезности J_i . Это обеспечивает модульность, масштабируемость и возможность децентрализованной адаптации. Второй принцип – вероятностной связанности – утверждает, что взаимодействие между агентами не является детерминированным, а характеризуется вероятностями успешного перехода p_{ij} . Данный принцип позволяет учитывать стохастическую природу внешней среды (сбои, задержки, перегрузки) при оценке устойчивости всей цепочки обработки.

В условиях воздействия внешних возмущений на элементы вычислительной системы надежность узлов и каналов связи не является абсолютной: задержки могут происходить как из-за перегрузки ресурсов, так и под воздействием сетевых проблем. Поэтому каждый компонент пайплайна оценивается вероятностью его нормального функционирования в заданный момент времени $p_i(t) = P$ (агент A_i работает исправно в момент t).

Физически это означает вероятность того, насколько стабильно данный агент выполняет свои функции при текущей нагрузке. Вероятностная мера надежности может выражаться как вероятность завершения задачи в срок $P(T_i \leq T_{\text{дедлайн}})$ или другими показателями, имеющими иной физический смысл.

Использование равновесных состояний в поведении агентов позволило применить марковские модели, что значительно упростило процесс вычислений и повысило оперативность оценки

адаптивности пайплайна. Это стало возможным благодаря тому, что наш подход позволяет рассчитывать вероятность успешного завершения цепочки обработки, где каждый переход между состояниями имеет определенную вероятность. Формально, пусть $S = \{s_1, s_2, \dots, s_m\}$ – множества состояний пайплайна, а $P = [p_{ij}]$ – матрица переходных вероятностей, где p_{ij} – переход состояний. Тогда вектор стационарных вероятностей $\pi = \pi P$ при условии $\sum_i \pi_i = 1$. Формула полной вероятности используется для вычисления вероятности успешного исхода в серии зависимых событий, где каждый этап имеет два возможных результата: успешное завершение с вероятностью p_i или необходимость перепланирования с вероятностью $q_i = 1 - p_i$ [10]. Вероятность успешного прохождения всей цепочки из k этапов вычисляется как $P_{\text{успешн}} = \prod_i p_i$, а математическое ожидание числа попыток составляет $E[N] = \sum_{i=1}^k \frac{1}{p_i}$. Такой метод обеспечивает возможность отслеживания состояния пайплайна в реальном времени и предоставляет более простой и эффективный инструмент для анализа системы.

Поэтому в работе рассматривается обобщенное понятие адаптивной связности как взаимосвязи между агентами, образующими динамически перестраиваемую и самоорганизующуюся структуру пайплайна. Такой подход расчета адаптивности обусловлен необходимостью оперативного восстановления цепочек обработки в случае их нарушения на критических участках, вызванного внешними возмущениями или внутренними сбоями архитектуры [11, 12]. Данный способ позволяет не только вычислить адаптивность, т.е. способность к реконфигурации, но и оценить устойчивость восстановленных цепочек и вероятность успешной обработки информационных потоков. Кроме того, анализ адаптивной связности помогает выявлять узкие места системы, прогнозировать поведение при различных сценариях нагрузки и разрабатывать эффективные методы ее оптимизации [13, 14]. Таким образом, модель является многофункциональной, определяющей адаптивность, надежность, устойчивость и работоспособность сложных пайплайнов в зависимости от физического смысла показателя модели.

На платформе Python с использованием фреймворка симуляции агентов был разработан программный код, который позволяет рассчитывать адаптивность пайплайна для заданного числа агентов n и различных значений k , представляющих минимальное количество успешных переходов для завершения задачи. Программа также вычисляет среднее время выполнения для всех сценариев, которое меньше

или больше определенного значения t . Итоговый результат представляет собой график зависимости адаптивности от параметров системы, что обеспечивает наглядность и удобство анализа.

Таким образом, в работе предложен научный подход к анализу адаптивности пайплайнов с использованием марковских моделей и имитационного моделирования в программной среде Python. Этот подход позволяет упростить расчеты и повысить оперативность оценки адаптивности в условиях динамического поведения агентов.

В рамках данной работы анализируется вычисление адаптивности для динамически перестраиваемого и равновесного пайплайна. В таких условиях применима модель цепей Маркова, поскольку вероятности переходов между состояниями агентов считаются стационарными, а каждый элемент системы может взаимодействовать с другими через определенные протоколы.

Формула полной вероятности используется для вычисления вероятности успешного исхода в серии зависимых событий, где каждый этап имеет возможные результаты:

$$P(A) = \sum_{i=1}^n P(H_i) \cdot P(A|H_i), \quad (2)$$

где $P(A)$ – вероятность успешного завершения пайплайна; $P(H_i)$ – вероятность нахождения системы в состоянии i ; $P(A|H_i)$ – условная вероятность успеха при условии состояния i ; n – количество возможных состояний системы.

Вероятность перехода между состояниями можно вычислить по формуле:

$$P_{ij} = \frac{\lambda_{ij}}{\sum_k \lambda_{ik}}, \quad (3)$$

где λ_{ij} – интенсивность перехода из состояния i в состояние j .

Представленная математическая модель позволяет вычислить вероятность того, что из n последовательных этапов обработки будет достигнуто успешное завершение при вероятностях переходов P_{ij} , т.е. определить устойчивость цепочки агентов в отдельности. Для определения среднего значения адаптивности пайплайна будем использовать ее усредненное значение по множеству сценариев, тогда формализованную постановку задачи можно записать в следующем виде:

$$\dot{A} = \frac{1}{M} \sum_{m=1}^M \left(\prod_{t=1}^{T_m} P_{\text{success}}^{m,t} \right). \quad (4)$$

Ограничения и условия: $0 \leq P \leq 1$, $n > 0$, $0 < k \leq n$, T_m – длительность сценария m .

Полученная математическая модель позволяет вычислить усредненное значение адаптивности, если известна архитектура пайплайна и вероятностные характеристики переходов между состояниями агентов.

Анализ адаптивности пайплайнов

Анализ адаптивности пайплайнов с агентным управлением основан на использовании марковских моделей, что позволяет упростить расчеты в силу математической стройности модели, а следовательно, повысить оперативность оценки в условиях динамического поведения агентов.

Основным предположением данного подхода является наличие стационарных вероятностей переходов между состояниями агентов [15, 16]. Такое ограничение имеет преимущество в оценке адаптивности пайплайнов любой размерности, однако ограничивает рамки применимости модели, которые связаны с типом обрабатываемых данных, требованиями к задержкам и видам внешних возмущений. В таких условиях адаптивность пайплайна определяется как взаимосвязь между агентами, формирующая динамически перестраиваемую и самоорганизующуюся структуру обработки.

На платформе Python был разработан программный код, который позволяет рассчитывать адаптивность пайплайна для заданного числа агентов n и различных значений k , представляющих минимальное количество успешных переходов для завершения задачи. Программа также вычисляет среднее время выполнения для всех сценариев, которое меньше или больше определенного значения t . Итоговый результат представляет собой график зависимости адаптивности от параметров системы, что обеспечивает наглядность и удобство анализа.

Алгоритм расчета адаптивности пайплайна с агентным управлением приведен на рисунке 1. Он включает следующие процедуры:

1. Ввод параметров: запрос количества агентов n , минимального количества успешных переходов k , матрицы вероятностей переходов P_{ij} .
2. Расчет адаптивности: для каждого сценария нагрузки и каждого значения k вычисляется вероятность успешного завершения с использованием марковской модели. Далее определяются средние значения адаптивности для различных диапазонов времени выполнения.
3. Визуализация результатов: строится график зависимости средней адаптивности от вероятности успешных переходов для различных значений k . Затем линейный график зависимости адаптивности от количества агентов для различных стратегий координации.

Для реализации вышеописанного алгоритма были написаны основные фрагменты кода на Python с использованием библиотек `numpy` для матричных вычислений и `matplotlib` для визуализации. Этот алгоритм и код позволяют оперативно анализировать адаптивность пайплайнов, используя простые и понятные методы вычислений. Полученные результаты предоставляют значимые данные для оценки адаптивности, позволяя учесть стохастическую природу процессов обработки.

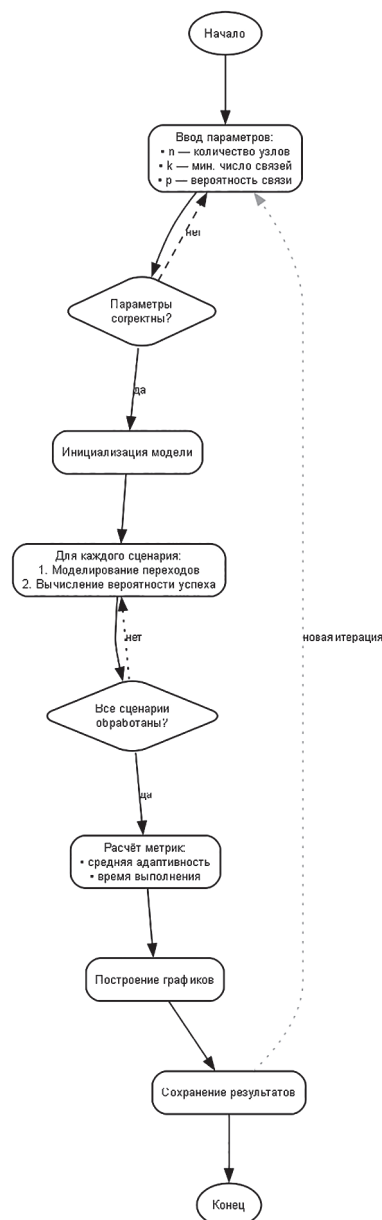


Рис. 1. Блок-схема алгоритма программы

Результаты исследований адаптивности пайплайна с десятью агентами от количества успешных переходов и значений вероятности

перехода между состояниями приведены на рисунке 2. Анализ полученных зависимостей показывает, что при вероятностном подходе к оценке показателя адаптивности фрагмента пайплайна его нормированное значение уменьшается по сравнению с оценкой по детерминированным методикам.

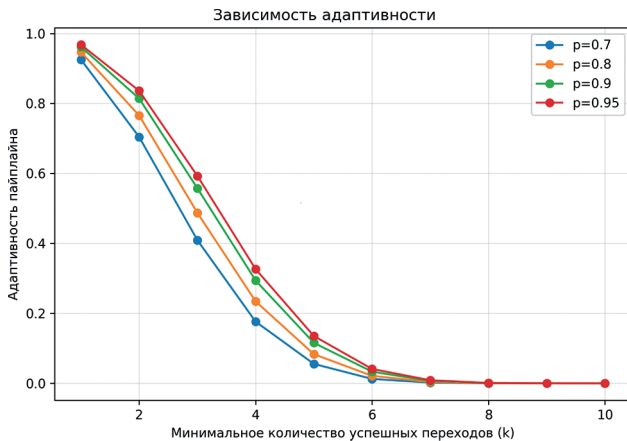


Рис. 2. График зависимости адаптивности от k для различных вероятностей переходов

Анализ полученных зависимостей показывает, что при вероятностном подходе к оценке показателя адаптивности фрагмента пайплайна его нормированное значение уменьшается по сравнению с оценкой по классическим методикам. Это связано с тем, что при наличии перехода между состояниями вес связи не равен единице, как в детерминированном подходе, а имеет вероятностный характер (меньше или равен единице), так как отражает степень воздействия внешних факторов на агентов пайплайна, что отражает реальную действительность.

С уменьшением значения вероятности успешного перехода между состояниями показатель адаптивности уменьшается, т.е. снижается устойчивость системы по причине внешних возмущений на ее элементы.

При увеличении количества агентов в пайплайне, но ограничении на число успешных переходов между ними (например, по причине ограничений пропускной способности или других факторов) даже при высокой вероятности переходов показатель адаптивности значительно снижается.

Также необходимо отметить, что в полностью связанной структуре пайплайна из 10 агентов показатель адаптивности уменьшился на 36 % по сравнению с детерминированной оценкой. Этот эффект связан с тем, что несмотря на практически гарантированные переходы в сложных системах с увеличением числа агентов возрастает

количество возможных путей отказа. Поэтому даже небольшие отклонения в вероятностях переходов оказывают существенное влияние на общую адаптивность. Этот результат доказывает тот факт, что чем сложнее структура пайплайна, тем большая надежность должна быть у каналов взаимодействия между агентами.

Полученные результаты демонстрируют важность учета надежности отдельных переходов в сложных системах. Анализ качества межагентных зависимостей позволит выявлять критически слабые места пайплайна, оптимизировать его структуру и на конечном этапе разрабатывать стратегии повышения устойчивости системы.

Вторая часть программы позволяет проводить анализ адаптивности пайплайна в зависимости от количества переходов, превышающих или недостающих до требуемого (заданного) значения. Этот этап особенно важен для аналитической работы, так как позволяет не только определить точную вероятность успешного завершения, но и рассчитать средние значения вероятностей для меньших и больших значений переходов. Такая детализация дает возможность формировать более точные и обоснованные выводы об архитектуре системы обработки. Полученные диаграммы адаптивности пайплайна на рисунке 3 предоставляют значимые данные для оценки, учитывая стохастическую природу процессов.

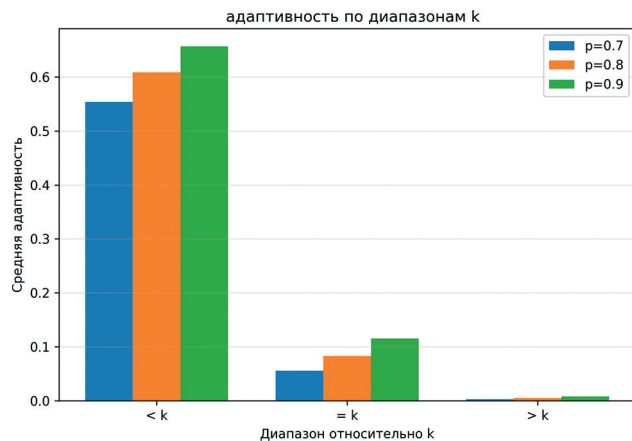


Рис. 3. Средняя адаптивность для менее, точно и более k успешных переходов

Анализ свидетельствует о том, что адаптивность не является фиксированным (детерминированным) значением, а представляет собой стохастический процесс, зависящий от множества факторов, таких как вероятность внешних возмущений, количество агентов и характер связей между ними. Для аналитической работы данная диаграмма более значима, так как

по ней определяется точная вероятность, а также средняя для меньших и больших значений. Это позволяет сделать более точное оценочное заключение по архитектуре системы обработки и способствует глубокому пониманию поведения сложных пайплайнов в различных условиях, что важно для проектирования устойчивых и эффективных структур.

Заключение

Разработанная математическая модель оценки и анализа адаптивности пайплайнов с динамической архитектурой и агентным управлением отражает значительный потенциал для оценки устойчивости и работоспособности систем в условиях внешних возмущений. В рамках настоящего исследования был предложен методологический подход, основанный на использовании марковских моделей, который позволяет упростить расчеты и повысить оперативность оценки адаптивности при наличии стационарных вероятностей переходов между состояниями агентов.

Основной целью исследования являлось создание простой, но адекватной модели оценки адаптивности и разработка программного обеспечения для её расчёта. Реализованная модель базируется на сформулированных в работе принципах: декомпозиции на автономные агенты, обеспечивающих необходимую гибкость архитектуры, и вероятностной связанности, позволяющей учитывать влияние внешних возмущений на надежность взаимодействий. Необходимо заметить, что предложенная методология оценки адаптивности пайплайна позволяет оценить устойчивость системы в целом в рамках способности к реконфигурации при внешних воздействиях на элементы, но она не дает информации о других свойствах системы, например, таких как семантическая согласованность данных, качество промежуточных результатов, энергоэффективность вычислений и т.п.

Очевидно, что в реальных условиях вероятности переходов между состояниями не могут быть одинаковыми из-за множества факторов, таких как различия в характеристиках оборудования, разнообразие во внешних условиях и типах возмущений. Однако принятое допущение о стационарных вероятностях переходов позволило разработать базовый алгоритм и программную реализацию, которая служит фундаментом для дальнейших исследований и расширений.

Полученные результаты исследований могут быть положены в основу научного обоснования и сравнительного анализа адаптивности пайплайнов различной сложности, в том числе распределенных, а также для проведения ситуационного анализа устойчивости систем к внешним воздействиям и оперативной оценки деформации цепочек обработки. Аналитическая работа с результатами оценки системных показателей позволит определять слабые звенья пайплайна, задавать научно обоснованные требования к вероятностным показателям элементов и формулировать точные оценочные заключения по адаптивности системы в различных условиях функционирования, что важно для проектирования устойчивых и эффективных архитектур.

Перспективами дальнейшего развития является совершенствование модели и программного обеспечения для оценки не только структурной, но и семантической адаптивности. Дальнейшая разработка принципов агентного управления, в частности, переход от стационарных к динамическим вероятностям переходов и внедрение механизмов обучения агентов, позволит учитывать более сложные сценарии функционирования пайплайнов. Это обеспечит более точные прогнозы производительности и надежности систем в реальных условиях эксплуатации, что имеет важное значение в условиях быстро меняющейся технологической среды и растущих требований к адаптивным системам обработки данных.

Литература

1. Вернер Х., Ламп Дж. Паттерны интеграции корпоративных приложений / Х. Вернер, Дж. Ламп. – М.: Вильямс, 2020. – 672 с.
2. Richardson C. Microservices Patterns: With examples in Java / C. Richardson // Shelter Island: Manning Publications, 2018. – P. 520.
3. Balalaie A. Microservices Architecture Enables DevOps: Migration to a Cloud-Native Architecture / A. Balalaie, A. Heydarnoori, P. Jamshidi // IEEE Software, 2016. – Vol. 33. – No 3. – Pp. 42–52. – DOI: 10.1109/MS.2016.64.
4. Soldani J. The Pains and Gains of Microservices: A Systematic Grey Literature Review / J. Soldani, D. A. Tamburri, W.-J. van den Heuvel // Journal of Systems and Software, 2018. – Vol. 146. – Pp. 215–232. – DOI: 10.1016/j.jss.2018.09.082.
5. Goonatilake S. T. Past, Present and Future Trends in Multi-Agent System Technology / S. T. Goonatilake, B. Hettige // Journal Européen des Systèmes Automatisés, 2022. – Vol. 55. – No. 6. – Pp. 723–739.
6. Smith E. LILLIE: Information extraction and database integration using linguistics and learning-based algorithms / E. Smith, D. Papadopoulos, M. Braschler, K. Stockinger // Information Systems, 2022. – Vol. 105. – DOI: 10.1016/j.is.2021.101938.

7. Голиков В. А. Исследование ключевых архитектурных паттернов микросервисов: теоретический анализ их роли в построении отказоустойчивой информационной системы / В. А. Голиков, М. В. Янаева, Н. Т. Рудник. – СПб: Информационно-управляющие системы, 2023. – № 4. – С. 28–37.
8. Абросимов Л. И. Методы проектирования и анализа производительности распределенных вычислительных сетей / Л. И. Абросимов. – М: Университетская книга, 2023. – 256 с.
9. Qiang S. The Nonlinear Mathematical Modeling and Optimization of Distributed Control in Complex Systems / S. Qiang // Journal of Advances in Engineering and Technology, 2025. – Vol. 2. – Pp. 34–42. – DOI: 10.62177/jaet.v2i1.152.
10. Wang Y., et al. A multi-level action coupling reinforcement learning approach for online two-stage flexible assembly flow shop scheduling // Journal of Manufacturing Systems, 2024. – Vol. 76. – Pp. 351–370.
11. Liu C. A Survey on Workflow Management and Scheduling in Cloud Computing / C. Liu, C. Yang, X. Fan [et al.] // IEEE Transactions on Services Computing, 2022. – Vol. 15. – No 4. – Pp. 2178–2197. – DOI: 10.1109/TSC.2020.3047462.
12. Calheiros R. N. CloudSim: A Toolkit for Modeling and Simulation of Cloud Computing Environments and Evaluation of Resource Provisioning Algorithms / R. N. Calheiros, R. Ranjan, A. Beloglazov [et al.] // Software: Practice and Experience, 2011. – Vol. 41. – No 1. – Pp. 23–50. – DOI: 10.1002/spe.995.
13. Sun S. Integrated data-driven topology reconstruction and risk-aware reconfiguration for resilient power distribution systems under incomplete observability / S. Sun, N. Li, L. Zhang, D. Zhao, D. Lun, L. Feng // Scientific Reports, 2025. – Vol. 15. – P. 30661. – DOI: 10.1038/s41598-025-15440-8.
14. Sahu A. ARM-IRL: Adaptive Resilience Metric Quantification Using Inverse Reinforcement Learning / A. Sahu, V. Venkataramanan, R. Macwan // AI, 2025. – Vol. 6. – No 5. – P. 103. – DOI: 10.3390/ai6050103.
15. Meylahn J. M. Quantifying the Likelihood of Learning Collusive Strategy Equilibria / J. M. Meylahn // Chaos: An Interdisciplinary Journal of Nonlinear Science, 2025. – Vol. 35. – No 8. – P. 083106. – DOI: 10.1063/5.0281443.
16. Шелухин О. И. Модели и методы управления в многоагентных системах / О. И. Шелухин, А. В. Осин. – М.: ФИЗМАТЛИТ, 2018. – 288 с.

PRINCIPLES OF BUILDING PIPELINES WITH DYNAMIC ARCHITECTURE AND AGENT-BASED MANAGEMENT

Lukashenok V. I.⁷, Izotov D. Yu.⁸

Keywords: dynamic pipelines, agent-based management, adaptive architecture, self-organization, scalability, task decomposition.

Abstract

The purpose of the work is to substantiate a methodological approach to building pipelines with dynamic architecture, controlled by autonomous software agents capable of adapting to changing conditions of task performance.

Research method: the research method combines the principles of modular design, the theory of multi-agent systems, and simulation modeling methods to analyze the behavior of dynamic pipelines.

Results of the study: a formalized approach to the description of the life cycle of agents, their interaction and evolution of the pipeline topology is presented, which makes it possible to simulate various scenarios of the system's functioning under conditions of external disturbances. Scientifically based principles for the design of agent-driven architecture have been formulated, including criteria for selecting agent granularity, communication strategies, and decision-making mechanisms. These aspects will form the basis for the further development of frameworks for building adaptive data processing systems.

Scientific novelty: the principle of building pipelines with dynamic architecture and agent-based control, considered as complementary adaptation mechanisms, is substantiated.

References

1. Verner H., Lamp Dzh. Patterny integracii korporativnyh prilozhenij / H. Verner, Dzh. Lamp // М.: Vil'yams, 2020. – P. 672.
2. Richardson C. Microservices Patterns: With examples in Java / C. Richardson // Shelter Island: Manning Publications, 2018. – P. 520.
3. Balalaie A. Microservices Architecture Enables DevOps: Migration to a Cloud-Native Architecture / A. Balalaie, A. Heydarnoori, P. Jamshidi // IEEE Software, 2016. – Vol. 33. – No 3. – Pp. 42–52. – DOI: 10.1109/MS.2016.64.
4. Soldani J. The Pains and Gains of Microservices: A Systematic Grey Literature Review / J. Soldani, D. A. Tamburri, W.-J. van den Heuvel // Journal of Systems and Software, 2018. – Vol. 146. – Pp. 215–232. – DOI: 10.1016/j.jss.2018.09.082.
5. Goonatilleke S. T. Past, Present and Future Trends in Multi-Agent System Technology / S. T. Goonatilleke, B. Hettige // Journal Européen des Systèmes Automatisés, 2022. – Vol. 55. – No. 6. – Pp. 723–739.

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

⁸ Danil Yu. Izotov, Researcher, Research Center, Military Academy of Communications. St. Petersburg, Russia. E-mail: daniil.izotov.1999@mail.ru

6. Smith E. LILLIE: Information extraction and database integration using linguistics and learning-based algorithms / E. Smith, D. Papadopoulos, M. Braschler, K. Stockinger // *Information Systems*, 2022. – Vol. 105. – DOI: 10.1016/j.is.2021.101938.
7. Golikov V. A. Issledovanie klyuchevykh arhitekturnykh patternov mikroservisov: teoreticheskij analiz ih roli v postroenii otkazoustojchivoj informacionnoj sistemy / V. A. Golikov, M. V. Yanaeva, N. T. Rudnik. – SPb: Informacionno-upravlyayushchie sistemy, 2023. – No 4. – Pp. 28–37.
8. Abrosimov L. I. Metody proektirovaniya i analiza proizvoditel'nosti raspredelennykh vychislitel'nykh setej / L. I. Abrosimov // M.: Universitetskaya kniga, 2023. – P. 256.
9. Qiang S. The Nonlinear Mathematical Modeling and Optimization of Distributed Control in Complex Systems / S. Qiang // *Journal of Advances in Engineering and Technology*, 2025. – Vol. 2. – Pp. 34–42. – DOI: 10.62177/jaet.v2i1.152.
10. Wang Y., et al. A multi-level action coupling reinforcement learning approach for online two-stage flexible assembly flow shop scheduling // *Journal of Manufacturing Systems*, 2024. – Vol. 76. – Pp. 351–370.
11. Liu C. A Survey on Workflow Management and Scheduling in Cloud Computing. / C. Liu, C. Yang, X. Fan [et al.] // *IEEE Transactions on Services Computing*, 2022. – Vol. 15. – No 4. – Pp. 2178–2197. – DOI: 10.1109/TSC.2020.3047462.
12. Calheiros R. N. CloudSim: A Toolkit for Modeling and Simulation of Cloud Computing Environments and Evaluation of Resource Provisioning Algorithms / R. N. Calheiros, R. Ranjan, A. Beloglazov [et al.] // *Software: Practice and Experience*, 2011. – Vol. 41. – No 1. – Pp. 23–50. – DOI: 10.1002/spe.995.
13. Sun S. Integrated data-driven topology reconstruction and risk-aware reconfiguration for resilient power distribution systems under incomplete observability / S. Sun, N. Li, L. Zhang, D. Zhao, D. Lun, L. Feng // *Scientific Reports*, 2025. – Vol. 15. – P. 30661. – DOI: 10.1038/s41598-025-15440-8.
14. Sahu A. ARM-IRL: Adaptive Resilience Metric Quantification Using Inverse Reinforcement Learning / A. Sahu, V. Venkataramanan, R. Macwan // *AI*, 2025. – Vol. 6. – No 5. – P. 103. – DOI: 10.3390/ai6050103.
15. Meylahn J. M. Quantifying the Likelihood of Learning Collusive Strategy Equilibria / J. M. Meylahn // *Chaos: An Interdisciplinary Journal of Nonlinear Science*, 2025. – Vol. 35. – No 8. – P. 083106. – DOI: 10.1063/5.0281443.
16. Sheluhin O. I. Modeli i metody upravleniya v mnogoagentnykh sistemah / O. I. Sheluhin, A. V. Osin. – M.: FIZMATLIT, 2018. – P. 288.



МЕТОД КОНТЕКСТНОЙ ВЕРИФИКАЦИИ СОБЫТИЙ ПРИ КОНТРОЛЕ БЕЗОПАСНОСТИ РАСПРЕДЕЛЁННОЙ IoT-ПОДСИСТЕМЫ

Андреев И. А.¹, Липатников В. А.², Тарасенко С. Е.³

DOI:10.21681/3034-4050-2026-3-29-39

Ключевые слова: интернет вещей, IoT, ESP32, MQTT, контроль безопасности, контекстная верификация событий, периферийные узлы, серверная обработка данных, виртуальный помощник, адаптивный режим контроля.

Аннотация

Цель работы: повышение защищённости распределённой IoT-подсистемы контроля безопасности за счёт разработки метода контекстной верификации событий и адаптивного выбора режима контроля безопасности при взаимодействии периферийных узлов на базе ESP32 с сервером виртуального помощника.

Метод исследования: использованы методы формализации событийного контура распределённой IoT-подсистемы, построения показателя доверия к событию на основе идентификационных, временных, процессных, состоянийных и ресурсных факторов, а также накопительной оценки аномальности событийного потока. Для проверки предложенного подхода применён модельный вычислительный эксперимент, основанный на генерации последовательностей событий доступа, телеметрии и управляющих воздействий. Сравнительная оценка выполнена по отношению к базовым статическим и пороговым методам контроля безопасности.

Результаты исследования: предложен метод контекстной верификации событий, основанный на совместном учёте идентификационных, временных, процессных и ресурсных факторов; разработано правило накопительной оценки аномальности и адаптивного выбора режима контроля безопасности; сформирован и исследован прикладной сценарий распределённой IoT-подсистемы с двумя узлами ESP32 и серверной обработкой данных; показано, что предложенный подход превосходит базовые статические и пороговые методы по вероятности ложного допуска и полноте выявления некорректных событий, особенно при распределённой во времени аномальной активности.

Научная новизна заключается в разработке метода контекстной верификации событий при контроле безопасности распределённой IoT-подсистемы, учитывающего контекст возникновения события, накопительную оценку аномальности и адаптивный выбор режима контроля безопасности в условиях ограниченных ресурсов периферийных узлов и серверно-периферийной архитектуры обработки данных.

Введение

Интернет вещей является одним из наиболее динамично развивающихся направлений современной цифровой инфраструктуры. Рост числа подключённых устройств, их гетерогенность, распределённый характер взаимодействия и тесная связь с физической средой формируют новые классы киберугроз. В документах NIST подчёркивается, что IoT-системы требуют специальных подходов к обеспечению безопасности, поскольку сочетают сетевую связность, ограниченные ресурсы и высокую вариативность сценариев применения [1–2].

Одной из ключевых проблем является обеспечение защищённости распределённых IoT-подсистем контроля безопасности, в которых события доступа, телеметрии и управляющих

воздействий обрабатываются в реальном времени. Для таких подсистем недостаточно только сетевой фильтрации или статической проверки идентификаторов, поскольку допустимость события определяется временным контекстом, контекстом развития процесса и текущим состоянием системы. Современные исследования показывают, что жёстко заданные модели авторизации плохо адаптируются к динамичным и гетерогенным IoT-средам, а развитие access control идёт в сторону гибридных и адаптивных подходов [3–5]. Дополнительную сложность создаёт широкое распространение MQTT, где атаки могут быть связаны не только с сетевыми аномалиями, но и с нарушением логики прикладного процесса [6–7].

В связи с этим актуальна разработка метода контроля безопасности, объединяющего

1 **Андреев Илья Андреевич**, оператор научной роты, Военная академия связи им. Маршала Советского Союза С. М. Будённого. Санкт-Петербург, Россия. E-mail: andreev.ilia.1984@mail.ru

2 **Липатников Валерий Алексеевич**, заслуженный деятель науки РФ, доктор технических наук, профессор, старший научный сотрудник научно-исследовательского центра, Военная академия связи им. Маршала Советского Союза С. М. Будённого. Санкт-Петербург, Россия. E-mail: lipatnikovanl@mail.ru

3 **Тарасенко Станислав Евгеньевич**, старший научный сотрудник научно-исследовательского центра, Военная академия связи им. Маршала Советского Союза С. М. Будённого. Санкт-Петербург, Россия. E-mail: s.tar.my@mail.ru

контекстную верификацию событий, накопительный анализ аномальности и адаптивный выбор режима контроля безопасности.

Целью работы является повышение защищённости распределённой IoT-подсистемы управления за счёт разработки метода контекстной верификации событий и адаптивного выбора режима контроля безопасности.

Для достижения цели в статье решаются следующие задачи: анализ существующих подходов к контролю доступа и выявлению аномалий в IoT-среде; формализация событийного контура; разработка показателя доверия к событию; разработка правила накопительной оценки аномальности; разработка правила выбора режима контроля безопасности; проведение экспериментальной оценки предложенного подхода.

Анализ существующих подходов и обзор литературы

Проблематика контроля доступа и защиты ресурсов в IoT подробно рассмотрена в обзорных работах последних лет. В частности, в исследовании S. Ravidas и соавт. показано, что для IoT-систем требования к механизмам авторизации формируются под влиянием масштабируемости, интероперабельности, малых вычислительных затрат, динамичности и необходимости учитывать специфику конкретного приложения. Авторы подчёркивают, что не существует единственного универсального решения для всех IoT-сценариев, а выбор механизма авторизации должен опираться на свойства конкретной архитектуры и среды функционирования [3].

В обзоре M. S. Ahsan и A.-S. K. Pathan доступ к ресурсам в IoT рассматривается как одна из центральных проблем безопасности, а сами модели доступа делятся на *conventional* и *advanced*. Авторы отмечают, что классические модели, основанные на ролях, атрибутах, доверии или отношениях, нередко оказываются недостаточно гибкими в условиях высокой динамичности и гетерогенности IoT-среды, тогда как новые подходы всё чаще используют гибридные механизмы, машинное обучение и иные способы адаптации к изменяющимся условиям [5].

Среди работ, наиболее близких к рассматриваемой тематике, следует выделить исследования по *context-aware access control*. В обзоре A. S. M. Kayes и соавт. показано, что в распределённых *cloud/fog*-средах решения о доступе должны учитывать не только статические атрибуты субъектов и объектов, но и релевантные контекстные условия [8]. Развивая этот подход, R. Kalaria и соавт. предложили *fog-based adaptive context-aware access control framework*, в котором

принятие решений переносится ближе к конечным узлам сети, а сами политики адаптируются к изменениям контекста и поведения доступа. Показано, что использование *fog*-узлов позволяет сократить задержку обработки и уменьшить зависимость от централизованного облачного контура [9].

Одновременно с этим в исследованиях по IoT security отмечается, что *edge/fog*-уровень должен рассматриваться не только как вычислительное расширение облака, но и как самостоятельный уровень защиты. В работе I. Butun и соавт. подчёркивается, что *fog computing* может выступать промежуточным security layer, обеспечивающим обработку и защиту данных до их передачи в облачную инфраструктуру [10]. Это особенно важно для систем, в которых задержка реакции и доступность критичны для безопасного функционирования.

Отдельное направление исследований связано с выявлением аномалий и вторжений в MQTT-ориентированных IoT-сетях. В статье M. A. Khan и соавт. предложена DNN-модель для intrusion detection в MQTT-based IoT, а также проведено сравнение с классическими ML-моделями на публичных MQTT-датасетах. Авторы показывают, что MQTT-брокер и связанные с ним публикации/подписки являются мишенью для DoS, MitM, intrusion и других атак [6].

Для воспроизводимых исследований важную роль играют специализированные наборы данных. Работа H. Hindy и соавт. посвящена MQTT-IoT-IDS2020 и показывает полезность packet-based, uni-flow и bi-flow признаков для выявления атак в MQTT-сетях. Авторы подчёркивают, что для MQTT-based IDS требуется учитывать особенности самого протокола и структуры потока, а не только общие сетевые признаки [11]. В свою очередь, I. Vaccari и соавт. представили MQTTset – специализированный датасет, включающий как легитимный, так и вредоносный MQTT-трафик, опубликованный в форматах PCAP и CSV. Авторы указывают на ограниченность ранее доступных IoT-датасетов и обосновывают необходимость именно MQTT-ориентированного корпуса данных [12].

С практической точки зрения существенна не только точность выявления угроз, но и применимость метода на периферийных узлах. В работе A. Mudgerikar и соавт. предложена device-edge split IDS, где сбор системных признаков осуществляется на устройстве, а основные вычисления выносятся на edge-server, что позволяет снизить накладные расходы на IoT-устройство [13]. Аналогичная линия прослеживается и в исследовании B. Asulba и соавт., где classical one-class ML

algorithms оцениваются по detection performance, execution time и memory на Raspberry Pi как репрезентативной edge-платформе [14].

Особый интерес представляет работа P. Empl и соавт., в которой предложен process-aware подход к intrusion detection в MQTT networks. Авторы обосновывают, что IoT application layer protocols несут дополнительную contextual information, а значит, могут использоваться для восстановления и анализа процессов, лежащих за отдельными сообщениями. Предложенный framework MISSION объединяет distributed tracing, aggregation of MQTT flows и process mining, позволяя выявлять аномалии уже на уровне отклонения от допустимого процесса, а не только на уровне отдельных пакетов или статистических признаков [7].

Подход к динамическому обнаружению киберугроз в распределённых системах Интернета вещей с использованием генеративных моделей представлен в [15], а методы обеспечения и повышения защищённости сетей при прогнозировании стратегий вторжений и многоэтапных атаках рассмотрены в [16–17].

Таким образом, анализ литературы показывает наличие трёх взаимосвязанных исследовательских направлений: моделей доступа и контекстно-зависимой авторизации в IoT; методов выявления аномалий и вторжений в MQTT-ориентированных сетях; edge/fog-подходов, ориентированных на снижение накладных расходов и повышение оперативности реакции.

Однако существующие работы обычно концентрируются либо на доступе, либо на intrusion detection, либо на resource-aware deployment. При этом в меньшей степени исследован подход, который объединяет контекстную допустимость события, накопительную оценку аномальности и адаптивный выбор режима контроля безопасности в рамках единого метода для распределённой IoT-подсистемы мониторинга и управления. Именно этот пробел и определяет постановку задачи настоящей работы.

Постановка задачи

Рассмотрим распределённую IoT-подсистему мониторинга и управления, состоящую из множества периферийных узлов, сенсоров, исполнительных устройств, коммуникационного брокера и серверного контура обработки событий. Такое представление согласуется с подходом NIST, в котором IoT-система трактуется как совокупность сетевых компонентов, обладающих интерфейсами, возможностями восприятия и воздействия на физическую среду, обработки и передачи данных [1, 2].

Структура исследуемой распределённой IoT-подсистемы мониторинга и управления, соответствующая рассматриваемому прикладному сценарию, представлена на рисунке 1.

В прикладной реализации исследуемая распределённая IoT-подсистема включала два периферийных узла на базе ESP32 и серверный контур виртуального помощника. Первый узел

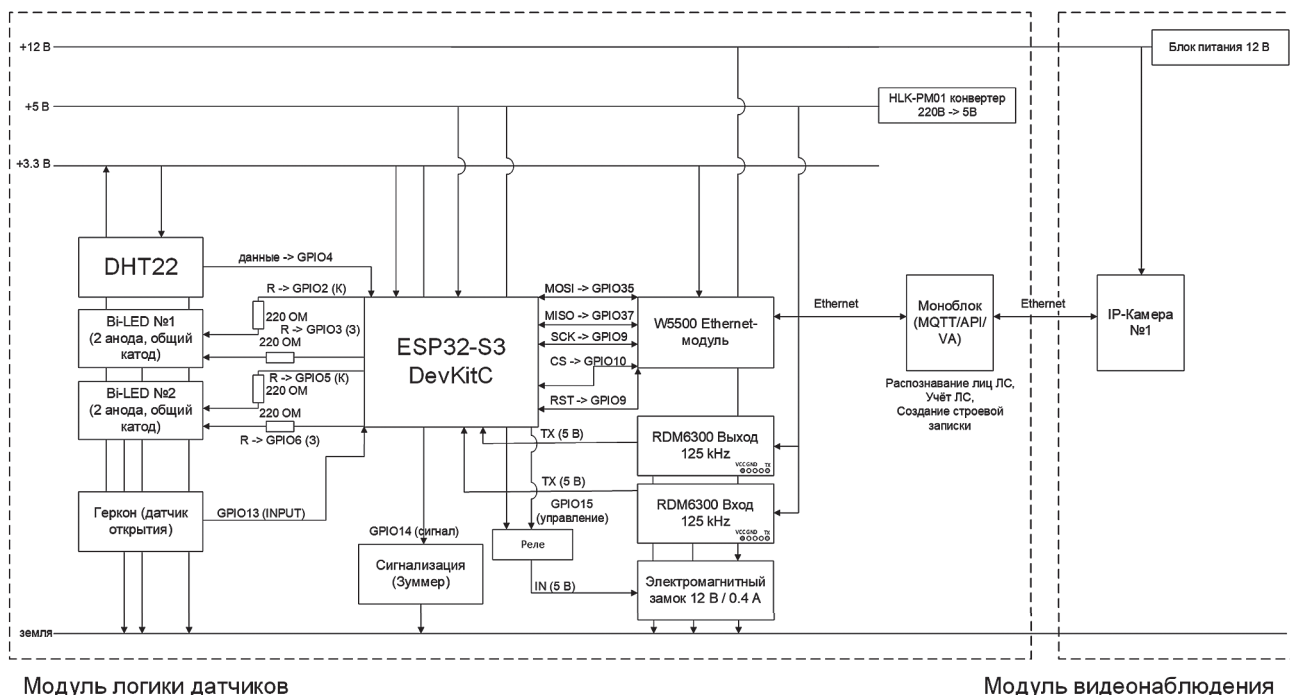


Рис. 1. Структурная схема исследуемой распределённой IoT-подсистемы мониторинга и управления

обеспечивал обработку событий доступа и состояния исполнительных устройств, второй – обработку телеметрических и управляющих сообщений. Сервер виртуального помощника выполнял агрегацию поступающих данных, журналирование событий и поддержку принятия решений в соответствии с реализуемой логикой контроля безопасности.

Пусть в дискретные моменты времени $t = 1, 2, \dots$ в систему поступают события:

$$e_t = \langle id_t, \tau_t, d_t, s_t, r_t, h_t \rangle, \quad (1)$$

где id_t – идентификатор источника события; τ_t – временная метка; d_t – тип события или направление действия; s_t – текущее логическое состояние системы; r_t – вектор ресурсных параметров узла; h_t – информация о предшествующей последовательности событий.

Практическая реализация исследуемой распределённой IoT-подсистемы в двух вариантах размещения периферийных узлов представлена на рисунке 2.



Рис. 2. Практическая реализация распределённой IoT-подсистемы контроля безопасности: слева – вариант установки в роте; справа – вариант установки в технопарке

В рассматриваемой постановке события могут соответствовать операциям доступа, публикациям в MQTT-темы, командам управления исполнительными устройствами, телеметрическим сообщениям и иным действиям, значимым для функционирования подсистемы.

Традиционный подход к принятию решения о допустимости события может быть представлен в виде функции:

$$u_t = F(id_t), \quad (2)$$

где решение определяется, по существу, только фактом наличия идентификатора в разрешённом множестве или удовлетворением простому набору статических правил. Такой подход прост в реализации, но не учитывает ни временную согласованность события, ни допустимость его появления в текущем процессе, ни изменение

состояния системы, ни ресурсные ограничения узла. В результате он может приводить как к ложным допускам, так и к ложным блокировкам. Для устранения указанного недостатка требуется перейти от статической проверки отдельных событий к их контекстной верификации. Для этого вводится показатель доверия к событию:

$$T_t = w_1 f_{id}(e_t) + w_2 f_{ime}(e_t) + w_3 f_{seq}(e_t) + w_4 f_{state}(e_t) + w_5 f_{res}(e_t), \quad (3)$$

где f_{id} характеризует корректность идентификатора источника; f_{ime} – временную допустимость события; f_{seq} – согласованность с предшествующей последовательностью; f_{state} – соответствие текущему состоянию системы; f_{res} – учёт ресурсного состояния узла; w_i – весовые коэффициенты, удовлетворяющие условию

$$\sum_{i=1}^5 w_i = 1, w_i \geq 0. \quad (4)$$

Одного только значения T_t недостаточно, если вредоносная активность проявляется не единственным отклонением, а устойчивой последовательностью пограничных или слабо аномальных событий. Поэтому дополнительно вводится накопительная оценка аномальности:

$$A_t = \max\{0, \lambda A_{t-1} + (1 - T_t) - v\}, \quad (5)$$

где $\lambda \in [0, 1]$ – коэффициент памяти, v – параметр отсечения фоновых отклонений.

На основе значения A_t формируется режим контроля безопасности:

$$M_t = \begin{cases} M_1, & A_t < \theta_1 \\ M_2, & \theta_1 \leq A_t < \theta_2, \\ M_3, & A_t \geq \theta_2 \end{cases} \quad (6)$$

где M_1 – нормальный режим; M_2 – усиленный контроль; M_3 – ограничительный режим; θ_1, θ_2 – пороговые значения, $\theta_1 < \theta_2$.

Тогда итоговое решение о допустимости события определяется уже не только самим событием, но и текущим режимом контроля:

$$u_t = G(e_t, T_t, A_t, M_t). \quad (7)$$

Таким образом, задача исследования заключается в разработке метода контекстной верификации событий и адаптивного выбора режима контроля безопасности, обеспечивающего снижение вероятности ложного допуска некорректных событий и повышение полноты их выявления при сохранении допустимой задержки принятия решения и приемлемой вычислительной стоимости. В качестве критерия эффективности принимается достижение превосходства

предложенного метода над базовыми статическими правилами по совокупности показателей:

- вероятности ложного допуска;
- вероятности ложной блокировки;
- полноты выявления некорректных событий;
- средней задержки принятия решения;
- вычислительной стоимости.

Метод контекстной верификации событий

Предлагаемый метод предназначен для принятия решения о допустимости событий в распределённой IoT-подсистеме мониторинга и управления на основе совместного учёта идентификационных, временных, процессных, состоянийных и ресурсных факторов. В отличие от статических правил, ориентированных преимущественно на проверку принадлежности источника разрешённому множеству, предлагаемый подход рассматривает событие как элемент развивающегося событийного процесса. Такая постановка соответствует современным представлениям о необходимости context-aware и process-aware анализа в IoT-средах [5, 7–9].

1. Общая схема метода

Метод включает три основных этапа: нормализацию события, вычисление контекстных признаков и формирование интегрального показателя доверия с последующей передачей результата в модуль накопительной оценки аномальности и выбора режима контроля безопасности. Нормализация позволяет привести различные типы входных сообщений к единому представлению, что особенно важно для MQTT-ориентированного обмена, где в общем потоке совместно присутствуют события доступа, телеметрии и управления. Такой переход от отдельных сообщений к интерпретируемым событиям согласуется с подходами, ориентированными на MQTT flow analysis и process-aware detection [7, 11–12].

2. Контекстные признаки события

Для каждого события формируется набор частных признаков допустимости. Идентификационный признак $f_{id}(e_i) \in [0,1]$ характеризует корректность источника события. Максимальные значения соответствуют зарегистрированным и согласованным с политикой системы источникам. Значимость контроля идентификации и логического доступа к интерфейсам соответствует базовым IoT cybersecurity capabilities, выделяемым NIST [2].

Временной признак $f_{time}(e_i) \in [0,1]$ отражает временную допустимость события и учитывает принадлежность события допустимому временному окну, а также ограничения на межсобытийные интервалы. Признак согласованности

последовательности $f_{seq}(e_i) \in [0,1]$ показывает, насколько событие соответствует допустимому порядку развития процесса. Его важность для MQTT-сетей подтверждается исследованиями по process-aware intrusion detection [7]. Признак согласованности состояния $f_{state}(e_i) \in [0,1]$ оценивает совместимость события с текущим состоянием системы. Ресурсный признак $f_{res}(e_i) \in [0,1]$ учитывает состояние узла, канала и доступного вычислительного бюджета. Этот фактор особенно важен для resource-constrained IoT/edge-среды [10, 13–14].

3. Агрегирование частных оценок

Интегральный показатель доверия к событию вычисляется как взвешенная сумма частных функций по выражению (3). Такое представление обеспечивает интерпретируемость метода: снижение итогового доверия можно объяснить вкладом конкретных факторов. Весовые коэффициенты задаются на этапе настройки системы и могут определяться экспертно либо уточняться по результатам модельного эксперимента.

4. Правило первичного решения

По значению T_i формируется первичная оценка допустимости события:

$$\hat{u}_i = \begin{cases} 1, & T_i \geq \delta, \\ 0, & T_i < \delta, \end{cases} \quad (8)$$

где δ – порог базовой контекстной допустимости.

Однако использование только порога δ недостаточно в случае медленно развивающейся вредоносной активности, состоящей из последовательности пограничных событий. Поэтому величина T_i используется не как окончательное решение, а как входной параметр для накопительной оценки аномальности, описанной в разделе 5.

5. Свойства метода

Предлагаемый метод является контекстно-зависимым, интерпретируемым и масштабируемым по набору учитываемых признаков. Кроме того, он совместим с edge/fog-развёртыванием, поскольку вычисление отдельных признаков может быть распределено между устройством, брокером и периферийным сервером, что согласуется с device-edge split архитектурой IDS для IoT [13].

Адаптивный выбор режима контроля безопасности

Контекстная верификация отдельного события позволяет оценить его локальную допустимость, однако не всегда обеспечивает выявление устойчивой вредоносной активности. На практике многие атаки в распределённых IoT-средах проявляются как последовательность

частично допустимых или слабо аномальных действий. Поэтому в предлагаемом подходе используется накопительная оценка аномальности и адаптивный выбор режима контроля безопасности.

1. Накопительная оценка аномальности

Для учёта инерции событийного процесса вводится переменная аномальности A_t , вычисляемая по выражению (5). Если текущее событие имеет высокую контекстную допустимость, значение A_t остаётся близким к нулю. При поступлении серии событий с пониженным доверием аномальность накапливается. Это позволяет перейти от реакции на единичное отклонение к выявлению устойчивого аномального паттерна, что более адекватно отражает природу MQTT-ориентированных атак [6–7].

2. Режимы контроля безопасности

Предполагается, что подсистема функционирует в одном из трёх режимов (6). Режим M_1 соответствует штатному функционированию и минимальному набору проверок. Режим M_2 характеризуется усилением контроля и повышением строгости анализа. Режим M_3 является ограничительным и предполагает блокировку низкодоверенных событий, а также применение более консервативной политики принятия решений.

3. Правило адаптации

Итоговое решение о допустимости события определяется функцией (7), где режим M_t задаёт текущую строгость контроля. Это означает, что одинаковое значение T_t может приводить к различным решениям в зависимости от накопленной аномальности процесса. Тем самым механизм является адаптивным и изменяет политику контроля не по фиксированному расписанию, а в зависимости от текущего состояния событийного потока.

4. Учёт ресурсных ограничений

Выбор режима контроля безопасности должен учитывать не только уровень аномальности, но и доступный ресурсный бюджет узла, поскольку усиление контроля не должно вызывать неприемлемую деградацию производительности в IoT- и edge-среде [9–10, 13–14]. Для этого может быть введено ограничение:

$$C(M_t) \leq B_t, \quad (9)$$

где $C(M_t)$ – вычислительная стоимость режима, B_t – доступный ресурсный бюджет. В случае дефицита ресурсов система может усиливать только критические проверки, сохраняя приемлемые задержки обработки.

Экспериментальное исследование

Целью экспериментального исследования явилась оценка эффективности предложенного

метода контекстной верификации событий и адаптивного выбора режима контроля безопасности по сравнению с базовыми правилами принятия решения в распределённой IoT-подсистеме мониторинга и управления.

В отличие от натурного стендового эксперимента, в данной работе используется модельный вычислительный эксперимент, основанный на генерации и анализе событийных последовательностей, имитирующих функционирование MQTT-ориентированной IoT-подсистемы. Такой подход представляется допустимым для предварительной проверки метода, поскольку в современных исследованиях по безопасности IoT и MQTT широко используются симулированные сетевые сценарии, синтетические и полусинтетические датасеты, а также имитационные модели атак [6, 11, 12, 14]. При этом для MQTT-сетей в литературе уже представлены как специализированные датасеты, так и исследования, ориентированные на packet-based, flow-based и process-aware анализ [7, 11–12].

Серверный контур обработки и визуализации событий, используемый в прикладной реализации исследуемой подсистемы, представлен на рисунке 3.

1. Схема модельного эксперимента

В рамках эксперимента моделировалась распределённая IoT-подсистема с учётом структуры подсистемы, представленной на рисунке 1, включающая:

- источники событий доступа;
- публикации телеметрических и управляющих сообщений;
- события изменения состояния объекта;
- команды исполнительным устройствам;
- ограниченный ресурсный профиль периферийного узла.

Модельный сценарий формировался на основе архитектуры прикладной реализации, в которой два узла ESP32 передавали события в серверный контур виртуального помощника, обеспечивавший централизованную обработку данных и поддержку решений по контролю безопасности.

Каждое событие описывалось вектором e_t (1), использованным в разделе 3. Для моделирования были сформированы последовательности событий двух типов:

1. Нормальные последовательности, соответствующие допустимой логике функционирования подсистемы.
2. Аномальные последовательности, содержащие отклонения одного или нескольких видов.

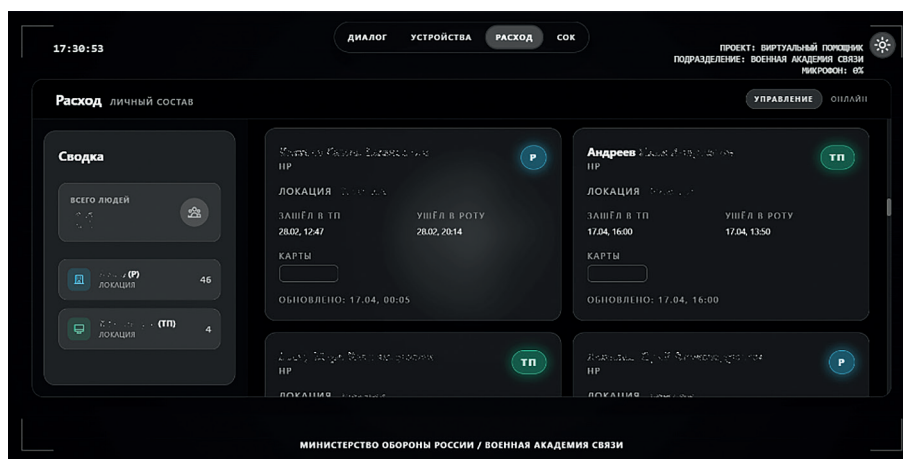


Рис. 3. Интерфейс серверного контура виртуального помощника для обработки и визуализации событий распределённой IoT-подсистемы

В вычислительном эксперименте рассматривались следующие классы аномалий:

- повтор разрешающего события в недопустимом временном окне;
- нарушение допустимой последовательности действий;
- управляющая команда вне корректного состояния системы;
- событие от формально допустимого источника в нетипичном контексте;
- серия пограничных событий, каждое из которых по отдельности не является грубым нарушением, но в совокупности образует устойчивую аномальную активность.

Последний класс особенно важен, поскольку именно он позволяет проверить преимущество предлагаемого накопительного механизма над простыми статическими правилами.

2. Сравнимые методы

Для оценки были использованы три варианта принятия решения.

Метод 1. Статическая проверка идентификатора (Baseline-1): событие считается допустимым, если идентификатор источника принадлежит разрешённому множеству u_i (1) по выражению (2).

Метод 2. Пороговая контекстная проверка без накопления (Baseline-2): для события вычисляется показатель доверия T_i , однако окончательное решение принимается только по порогу δ , без учёта накопления аномальности: u_i (2) по выражению (8).

Метод 3. Предлагаемый метод: используется показатель доверия T_i , накопительная оценка аномальности A_i и адаптивный выбор режима контроля безопасности u_i (3) по выражению (7).

Таким образом, сравнение позволяет оценить вклад двух элементов:

- контекстной верификации по сравнению со статической проверкой;
- накопительной адаптации по сравнению с разовой пороговой контекстной проверкой.

3. Параметры эксперимента

В рамках модельного исследования было сгенерировано 12000 событий, объединённых в 600 сценариев по 20 событий в каждом. Из них:

- 360 сценариев относились к нормальному функционированию;
- 240 сценариев включали один или несколько типов аномалий.

Доля аномальных сценариев была выбрана повышенной по сравнению с реальной эксплуатационной средой для получения более выраженной сравнительной картины качества методов. Для обеспечения воспроизводимости в каждом сценарии использовались одинаковые правила генерации последовательностей, а варьировались только временные интервалы, текущие состояния и структура допустимых или недопустимых переходов. При моделировании были использованы следующие параметры предложенного метода: $w_1 = 0,22$, $w_2 = 0,18$, $w_3 = 0,24$, $w_4 = 0,21$, $w_5 = 0,15$; $\delta = 0,60$, $\lambda = 0,72$, $\nu = 0,08$, $\theta_1 = 0,35$, $\theta_2 = 0,70$.

Выбор весов отражает более высокую значимость процессной согласованности и состояния системы по сравнению с ресурсным фактором, что соответствует характеру исследуемой задачи.

4. Метрики оценки

Для оценки эффективности использовались следующие показатели:

- FAR – вероятность ложного допуска некорректного события;
- FRR – вероятность ложной блокировки корректного события;

- *Recall* – полнота выявления некорректных событий;
- *Precision* – точность выявления некорректных событий;
- F_1 – гармоническое среднее точности и полноты;
- t_{avg} – средняя задержка принятия решения на одно событие;
- c_{rel} – относительная вычислительная стоимость метода.

Использование не только quality-метрик, но и временных/ресурсных показателей согласуется с современными исследованиями по edge-ориентированным IoT-методам, где эффективность должна рассматриваться совместно с вычислительной стоимостью [13–14].

5. Результаты сравнения методов

Результаты модельного вычислительного эксперимента приведены в таблице 1.

Из таблицы 1 следует, что простой статический подход характеризуется наименьшими вычислительными затратами, однако имеет наибольшую вероятность ложного допуска. Это означает, что проверка только по идентификатору не обеспечивает требуемого уровня защищенности в условиях контекстно-зависимых нарушений.

Переход к пороговой контекстной проверке без накопления аномальности приводит к заметному снижению *FAR* и росту полноты выявления. Однако этот вариант по-прежнему недостаточно устойчив к сериям пограничных событий, поскольку не учитывает их накопительный эффект. Предлагаемый метод показывает

наилучшие значения *Recall* и F_1 , а также минимальный *FAR*. Это указывает на более высокую способность выявлять некорректные события при меньшем числе опасных пропусков. При этом наблюдается умеренный рост *FRR* и вычислительной стоимости по сравнению с более простыми подходами, что является ожидаемой платой за повышение защищенности.

6. Анализ результатов по типам аномалий

Для более детальной оценки были отдельно рассмотрены результаты по различным типам аномальных сценариев. Они приведены в таблице 2.

Наибольшее различие наблюдается для серии пограничных событий. Для данного класса аномалий статическая проверка и даже разовая контекстная верификация демонстрируют ограниченную эффективность, так как отдельные события по отдельности могут не пересекать установленный порог аномальности. Предлагаемый метод, благодаря использованию накопительной переменной A_t , выявляет такие сценарии существенно лучше. Именно этот результат подтверждает целесообразность введения адаптивного режима контроля безопасности: он позволяет учитывать не только локальное качество текущего события, но и характер развития процесса во времени.

7. Влияние накопительного механизма и обсуждение результатов

Дополнительная проверка показала, что рациональные значения коэффициента памяти λ лежат в диапазоне 0,6–0,75: при меньших значениях снижается чувствительность метода

Таблица 1.

Сравнение методов принятия решения по основным показателям

Метод	<i>FAR</i>	<i>FRR</i>	<i>Recall</i>	<i>Precision</i>	F_1	t_{avg}	c_{rel}
Baseline-1: статическая проверка идентификатора	0,173	0,041	0,781	0,812	0,796	0,19	1,00
Baseline-2: контекстная проверка без накопления	0,091	0,058	0,872	0,884	0,878	0,43	1,84
Предлагаемый метод	0,049	0,064	0,931	0,918	0,924	0,67	2,41

Таблица 2.

Полнота выявления по типам аномальных сценариев

Тип аномалии	Baseline-1	Baseline-2	Предлагаемый метод
Нарушение временного окна	0,69	0,86	0,91
Нарушение последовательности событий	0,62	0,84	0,93
Команда в недопустимом состоянии	0,74	0,88	0,94
Нетипичный контекст при допустимом источнике	0,71	0,82	0,90
Серия пограничных событий	0,55	0,67	0,96

к распределённым во времени аномалиям, а при больших возрастает число ложных блокировок. Это подтверждает целесообразность использования накопительного механизма как средства выявления устойчивых аномальных паттернов.

Результаты эксперимента показывают, что учёт контекстных признаков сам по себе повышает качество принятия решения по сравнению со статической проверкой идентификатора. Наибольший прирост достигается за счёт введения накопительной оценки аномальности и адаптивного режима контроля, что особенно заметно в сценариях, где вредоносная активность распределена во времени и маскируется под последовательность частично допустимых действий. При этом рост вычислительной стоимости остаётся ограниченным и не приводит к неприемлемому увеличению задержки обработки событий, что согласуется с требованиями edge-ориентированных решений [13–17].

8. Вывод по результатам экспериментального исследования

Результаты модельного вычислительного эксперимента показывают, что предложенный метод контекстной верификации событий и адаптивного выбора режима контроля безопасности превосходит базовые статические и пороговые подходы по ключевым показателям защищённости. Наиболее существенное улучшение достигается по вероятности ложного допуска и полноте выявления некорректных событий, особенно в сценариях с распределённой во времени аномальной активностью. Следовательно, цель статьи может считаться достигнутой в рамках проведённого модельного исследования.

Заключение

В статье рассмотрена задача повышения защищённости распределённой IoT-подсистемы

специального назначения в условиях киберугроз, нестационарности событийного потока и ограниченных ресурсов периферийных узлов. Показано, что статические правила проверки событий и решения, основанные только на идентификаторе источника, недостаточны для выявления сложных контекстно-зависимых нарушений.

Предложен метод контекстной верификации событий при контроле безопасности, в котором допустимость события определяется на основе идентификационных, временных, процессных, состояний и ресурсных факторов. В развитие этого подхода введён механизм накопительной оценки аномальности и адаптивного выбора режима контроля безопасности, позволяющий учитывать не только текущее событие, но и характер развития событийного процесса во времени.

В рамках модельного вычислительного эксперимента показано, что предложенный метод превосходит базовые статические и пороговые подходы по вероятности ложного допуска и полноте выявления некорректных событий, особенно в сценариях с распределённой во времени аномальной активностью. Полученные результаты позволяют сделать вывод о достижении поставленной цели работы – повышении защищённости распределённой IoT-подсистемы за счёт разработки метода контекстной верификации событий и адаптивного выбора режима контроля безопасности.

Перспективы дальнейших исследований связаны с уточнением процедуры настройки весовых коэффициентов и пороговых параметров, а также с расширением метода на более сложные распределённые IoT/IoRT-сценарии с несколькими взаимосвязанными контурами принятия решений.

Литература

1. Hogan M., Piccarreta B. Interagency Report on the Status of International Cybersecurity Standardization for the Internet of Things (IoT). Gaithersburg: National Institute of Standards and Technology, 2018. – P. 185. – DOI: 10.6028/NIST.IR.8200.
2. Fagan M., Megas K. N., Scarfone K., Smith M. IoT Device Cybersecurity Capability Core Baseline. Gaithersburg: National Institute of Standards and Technology, 2020. – P. 23. – DOI: 10.6028/NIST.IR.8259A.
3. Ravidas S., Lekidis A., Paci F., Zannone N. Access control in Internet-of-Things: A survey // Journal of Network and Computer Applications, 2019. – Vol. 144. – Pp. 79–101. – DOI: 10.1016/j.jnca.2019.06.017.
4. Ragothaman K., Wang Y., Rimal B., Lawrence M. Access Control for IoT: A Survey of Existing Research, Dynamic Policies and Future Directions // Sensors, 2023. – Vol. 23. – No 4. – Art. 1805. – DOI: 10.3390/s23041805.
5. Ahsan M. S., Pathan A.-S. K. A Comprehensive Survey on the Requirements, Applications, and Future Challenges for Access Control Models in IoT: The State of the Art // IoT, 2025. – Vol. 6. – Art. 9. – DOI: 10.3390/iot6010009.
6. Khan M. A., Khan M. A., Jan S. U., Ahmad J., Jamal S. S., Shah A. A., Pitropakis N., Buchanan W. J. A Deep Learning-Based Intrusion Detection System for MQTT Enabled IoT // Sensors, 2021. – Vol. 21. – Art. 7016. – DOI: 10.3390/s21217016.
7. Empl P., Böhm F., Pernul G. Process-Aware Intrusion Detection in MQTT Networks // Proceedings of the Fourteenth ACM Conference on Data and Application Security and Privacy (CODASPY '24). Porto, Portugal, 2024. – Pp. 91–102. – DOI: 10.1145/3626232.3653271.

8. Kayes A. S. M., Rahayu W., Dillon T., Chang E. A Survey of Context-Aware Access Control Mechanisms for Cloud and Fog Networks: Taxonomy and Open Research Issues // *Sensors*, 2020. – Vol. 20. – No 9. – Art. 2464. – DOI: 10.3390/s20092464.
9. Kalaria R., Kayes A. S. M., Rahayu W., Pardede E., Shahraki A. S. Adaptive context-aware access control for IoT environments leveraging fog computing // *International Journal of Information Security*, 2024. – Vol. 23. – Pp. 3089–3107. – DOI: 10.1007/s10207-024-00866-4.
10. Butun I., Sari A., Österberg P. Hardware Security of Fog End-Devices for the Internet of Things // *Sensors*, 2020. – Vol. 20. – No. 20. – Art. 5729. – DOI: 10.3390/s20205729.
11. Hindy H., Bayne E., Bures M., Atkinson R., Tachtatzis C., Bellekens X. Machine Learning Based IoT Intrusion Detection System: An MQTT Case Study (MQTT-IoT-IDS2020 Dataset) // *arXiv*, 2020. arXiv:2006.15340.
12. Vaccari I., Chiola G., Aiello M., Mongelli M., Cambiaso E. MQTTset, a New Dataset for Machine Learning Techniques on MQTT // *Sensors*, 2020. – Vol. 20. – No 22. – Art. 6578. – DOI: 10.3390/s20226578.
13. Mudgerikar A., Sharma P., Bertino E. Edge-Based Intrusion Detection for IoT devices // *ACM Transactions on Management Information Systems*, 2020. – Vol. 11. – No. 4. – Art. 18. – DOI: 10.1145/3382159.
14. Asulba B., Souto P. F., Almeida L. Bringing IoT Intrusion Detection to the Edge // *Proceedings of the 8th International Conference on Future Networks & Distributed Systems (ICFNDS '24)*. Marakech, Morocco, 2024. New York: ACM, 2024. – P. 10. – DOI: 10.1145/3726122.3726166.
15. Котенко И. В., Саенко И. Б., Липатников В. А., Андреев И. А. Метод динамического обнаружения киберугроз в распределенных системах Интернета вещей на основе генеративных моделей // *Прикладная информатика*. – 2026. – Т. 21. – № 2. – С. 102–118. – DOI: 10.37791/2687-0649-2026-21-2-102-118.
16. Липатников В. А., Шевченко А. А., Косолапов В. С., Сокол Д. С. Метод обеспечения информационной безопасности сети VoIP-телефонии с прогнозом стратегии вторжений нарушителя // *Информационно-управляющие системы*, 2022. – № 1. – С. 54–67. – DOI: 10.31799/1684-8853-2022-1-54-67.
17. Липатников В. А., Шевченко А. А., Мелехов К. В., Ткачев Д. Ф. Методика повышения защищенности сети передачи данных объектов критической информационной инфраструктуры при многоэтапных атаках // *Информационно-управляющие системы*, 2024. – № 1. – С. 44–55. – DOI: 10.31799/1684-8853-2024-1-44-55.

METHOD OF FIELD VERIFICATION OF EVENTS IN SECURITY CONTROL OF A DISTRIBUTED IoT SUBSYSTEM

Andreev I. A.⁴, Lipatnikov V. A.⁵, Tarasenko S. E.⁶

Keywords: Internet of Things, IoT, ESP32, MQTT, security control, field verification of events, edge nodes, server data processing, virtual assistant, adaptive control mode.

Abstract

The aim of the work is to improve the security of the distributed IoT security control subsystem by developing a method for field verification of events and adaptive selection of the security control mode when interaction between edge nodes based on ESP32 and the virtual assistant server.

Research method: the methods of formalizing the event circuit of the distributed IoT subsystem, constructing an indicator of confidence in an event based on identification, time, process, state and resource factors, as well as cumulative assessment of the anomalousness of the event flow were used. To test the proposed approach, a model computational experiment based on the generation of sequences of access events, telemetry and control actions was used. A comparative assessment was carried out in relation to the basic static and threshold methods of safety control.

Results of the study: a method of field verification of events based on the joint consideration of identification, time, process and resource factors is proposed; a rule for cumulative anomaly assessment and adaptive selection of the security control mode is developed; an applied scenario of a distributed IoT subsystem with two ESP32 nodes and server data processing is formed and investigated; it is shown that the proposed approach surpasses the basic static and threshold methods for the probability of false tolerance and completeness of detection of invalid events, especially in the case of anomalous activity distributed over time.

The scientific novelty lies in the development of a method for field verification of events in the security control of a distributed IoT subsystem, taking into account the context of the event, cumulative anomaly assessment and adaptive selection of the security control mode in conditions of limited resources of peripheral nodes and server-edge architecture of data processing.

4 **Ilya A. Andreev**, Operator of the scientific company, Military Academy of Communications named after Marshal of the Soviet Union S. M. Budyonny. St. Petersburg, Russia. E-mail: andreev.ilia.1984@mail.ru

5 **Valery A. Lipatnikov**, Honored Scientist of the Russian Federation, Doctor of Technical Sciences, Professor, Senior Researcher of the Research Center, Military Academy of Communications named after Marshal of the Soviet Union S. M. Budyonny. St. Petersburg, Russia. E-mail: lipatnikovanl@mail.ru

6 **Stanislav E. Tarasenko**, Senior Researcher, Research Center, Military Academy of Communications named after Marshal of the Soviet Union S.M. Budyonny. St. Petersburg, Russia. E-mail: s.tar.my@mail.ru

References

1. Hogan M., Piccarreta B. Interagency Report on the Status of International Cybersecurity Standardization for the Internet of Things (IoT). Gaithersburg: National Institute of Standards and Technology, 2018. – P. 185. – DOI: 10.6028/NIST.IR.8200.
2. Fagan M., Megas K. N., Scarfone K., Smith M. IoT Device Cybersecurity Capability Core Baseline. Gaithersburg: National Institute of Standards and Technology, 2020. – P. 23. – DOI: 10.6028/NIST.IR.8259A.
3. Ravidas S., Lekidis A., Paci F., Zannone N. Access control in Internet-of-Things: A survey // Journal of Network and Computer Applications, 2019. – Vol. 144. – Pp. 79–101. – DOI: 10.1016/j.jnca.2019.06.017.
4. Ragothaman K., Wang Y., Rimal B., Lawrence M. Access Control for IoT: A Survey of Existing Research, Dynamic Policies and Future Directions // Sensors, 2023. – Vol. 23. – No 4. – Art. 1805. – DOI: 10.3390/s23041805.
5. Ahsan M. S., Pathan A.-S. K. A Comprehensive Survey on the Requirements, Applications, and Future Challenges for Access Control Models in IoT: The State of the Art // IoT, 2025. – Vol. 6. – Art. 9. – DOI: 10.3390/iot6010009.
6. Khan M. A., Khan M. A., Jan S. U., Ahmad J., Jamal S. S., Shah A. A., Pitropakis N., Buchanan W. J. A Deep Learning-Based Intrusion Detection System for MQTT Enabled IoT // Sensors, 2021. – Vol. 21. – Art. 7016. – DOI: 10.3390/s21217016.
7. Empl P., Böhm F., Pernul G. Process-Aware Intrusion Detection in MQTT Networks // Proceedings of the Fourteenth ACM Conference on Data and Application Security and Privacy (CODASPY '24). Porto, Portugal, 2024. – Pp. 91–102. – DOI: 10.1145/3626232.3653271.
8. Kayes A. S. M., Rahayu W., Dillon T., Chang E. A Survey of Context-Aware Access Control Mechanisms for Cloud and Fog Networks: Taxonomy and Open Research Issues // Sensors, 2020. – Vol. 20. – No 9. – Art. 2464. – DOI: 10.3390/s20092464.
9. Kalaria R., Kayes A. S. M., Rahayu W., Pardede E., Shahraki A. S. Adaptive context-aware access control for IoT environments leveraging fog computing // International Journal of Information Security, 2024. – Vol. 23. – Pp. 3089–3107. – DOI: 10.1007/s10207-024-00866-4.
10. Butun I., Sari A., Österberg P. Hardware Security of Fog End-Devices for the Internet of Things // Sensors, 2020. – Vol. 20. – No. 20. – Art. 5729. – DOI: 10.3390/s20205729.
11. Hindy H., Bayne E., Bures M., Atkinson R., Tachtatzis C., Bellekens X. Machine Learning Based IoT Intrusion Detection System: An MQTT Case Study (MQTT-IoT-IDS2020 Dataset) // arXiv, 2020. arXiv:2006.15340.
12. Vaccari I., Chiola G., Aiello M., Mongelli M., Cambiaso E. MQTTset, a New Dataset for Machine Learning Techniques on MQTT // Sensors, 2020. – Vol. 20. – No 22. – Art. 6578. – DOI: 10.3390/s20226578.
13. Mudgerikar A., Sharma P., Bertino E. Edge-Based Intrusion Detection for IoT devices // ACM Transactions on Management Information Systems, 2020. – Vol. 11. – No. 4. – Art. 18. – DOI: 10.1145/3382159.
14. Asulba B., Souto P. F., Almeida L. Bringing IoT Intrusion Detection to the Edge // Proceedings of the 8th International Conference on Future Networks & Distributed Systems (ICFNDS '24). Marakech, Morocco, 2024. New York: ACM, 2024. – P. 10. – DOI: 10.1145/3726122.3726166.
15. Kotenko I. V., Saenko I. B., Lipatnikov V. A., Andreev I. A. Metod dinamicheskogo obnaruzheniya kiberugroz v raspredelennyh sistemah Interneta veshchej na osnove generativnyh modelej // Prikladnaya informatika, 2026. – Vol. 21. – No. 2. – Pp. 102–118. – DOI: 10.37791/2687-0649-2026-21-2-102-118.
16. Lipatnikov V. A., Shevchenko A. A., Kosolapov V. S., Sokol D. S. Metod obespecheniya informacionnoj bezopasnosti seti VoIP-telefonii s prognozom strategii vtorzenij narushitelya // Informacionno-upravlyayushchie sistemy, 2022. – No 1. – Pp. 54–67. – DOI: 10.31799/1684-8853-2022-1-54-67.
17. Lipatnikov V. A., Shevchenko A. A., Melehov K. V., Tkachev D. F. Metodika povysheniya zashchishchennosti seti peredachi dannyh ob'ektov kriticheskoy informacionnoj infrastruktury pri mnogoehapnyh atakah // Informacionno-upravlyayushchie sistemy, 2024. – № 1. – Pp. 44–55. – DOI: 10.31799/1684-8853-2024-1-44-55.



ПРОГРАММНЫЙ КОМПЛЕКС ДЛЯ ПОИСКА И ИДЕНТИФИКАЦИИ СИГНАЛОВ ДЛЯ SDR НА ОСНОВЕ ПЛАТФОРМЫ GNU RADIO

Баймаков Д. А.¹, Ткачев Д. Ф.², Воробьев П. В.³

DOI:10.21681/3034-4050-2026-3-40-48

Ключевые слова: программно-определяемое радио, GNU Radio, USRP B210, обнаружение БПЛА, спектральный анализ, Python-блоки, идентификация сигналов, база сигнатур.

Аннотация

Цель работы: создание законченного решения, позволяющего в реальном времени сканировать заданные диапазоны частот, автоматически фиксировать превышения порогового уровня мощности, определять параметры обнаруженных сигналов и идентифицировать их на основе предварительно сформированной базы сигнатур.

Результаты исследования: создан программно-аппаратный стенд для мониторинга электромагнитной обстановки в диапазонах работы каналов управления беспилотных летательных аппаратов (БПЛА) с использованием технологии программно-определяемого радио (SDR). Стенд реализован на базе приёмника USRP B200/B210 и открытой среды GNU Radio, развёрнутой в виртуальной машине Oracle VirtualBox. Подробно описаны этапы построения потокового графа обработки сигналов, разработки встроенных Python-блоков для порогового детектирования, измерения центральной частоты и ширины спектра, а также создания базы сигнатур с функцией автоматической идентификации. Приведены ключевые фрагменты программного кода и результаты экспериментальной проверки системы. Обсуждаются факторы, влияющие на точность измерений, и перспективы дальнейшего развития комплекса.

Практическая ценность заключается в создании целостной архитектуры программного комплекса, объединяющей в реальном времени спектральный анализ, измерение параметров сигнала и его идентификацию на основе базы сигнатур с использованием только открытых программных средств и доступного SDR-оборудования.

Введение

Беспилотные летательные аппараты (БПЛА) широко используют для управления и передачи телеметрии нелегализуемые диапазоны частот 2,4 ГГц, 5,8 ГГц, а также 433 МГц и 900 МГц [1]. Обнаружение и идентификация таких сигналов в реальной электромагнитной обстановке является актуальной задачей как для целей безопасности объектов, так и для противодействия несанкционированному применению дронов [2]. Технология программно-определяемого радио (SDR) предоставляет гибкий инструмент для построения недорогих и перестраиваемых систем радиомониторинга [3]. В отличие от традиционных аппаратных анализаторов спектра, SDR-приёмник в связке с открытым программным обеспечением позволяет не только визуализировать спектр, но и реализовывать произвольные алгоритмы цифровой обработки сигналов, адаптированные под конкретную задачу [4].

Целью настоящей работы является разработка законченного программного решения, позволяющего в реальном времени сканировать заданные диапазоны частот, автоматически фиксировать превышения порогового уровня мощности, определять центральную частоту и ширину полосы обнаруженного излучения, а также сохранять спектрограммы в базу данных с возможностью последующей идентификации вновь появляющихся сигналов. В статье последовательно описан процесс создания такого комплекса на базе приёмопередатчика USRP B200/B210 и среды GNU Radio, включая установку драйверов, построение потокового графа, разработку специализированных Python-блоков и реализацию подсистемы хранения и сравнения сигнатур.

Аппаратная и программная основа стенда

В качестве SDR-приёмника использовалось устройство Ettus Research USRP B200 (в дальнейшем применим и B210), подключаемое

1 **Баймаков Данил Алексеевич**, оператор научной роты Военной академии связи им. Маршала Советского Союза С. М. Буденного. Санкт-Петербург, Россия. E-mail: baymakovdaniil@gmail.com

2 **Ткачев Дмитрий Федорович**, начальник научно-исследовательского отдела научно-исследовательского центра Военной академии связи им. Маршала Советского Союза С. М. Буденного. Санкт-Петербург, Россия. E-mail: dimas.portnoy@inbox.ru

3 **Воробьев Павел Владимирович**, научный сотрудник научно-исследовательского отдела научно-исследовательского центра Военной академии связи им. Маршала Советского Союза С. М. Буденного. Санкт-Петербург, Россия. E-mail: pvorobyev98@gmail.com

к персональному компьютеру через интерфейс USB 3.0. Приёмник обеспечивает непрерывный частотный диапазон от 70 МГц до 6 ГГц и мгновенную полосу пропускания до 56 МГц, что с запасом перекрывает каналы управления большинства коммерческих БПЛА⁴. Для калибровки и тестовых излучений применялся передатчик HackRF One, способный генерировать немодулированную несущую или FM-тон в диапазоне 1 МГц – 6 ГГц.



Рис. 1. Аппаратная часть стенда

Обработка сигналов выполняется в среде GNU Radio, выбранной благодаря открытой архитектуре, богатой библиотеке стандартных блоков и возможности расширения функционала с помощью модулей на Python⁵. Установка производилась в два этапа:

1. На хост-системе (Windows) устанавливался менеджер пакетов Conda и дистрибутив Radioconda, включающий все необходимые зависимости Python.
2. Основная работа велась в виртуальной машине Oracle VirtualBox с образом instant-gnuradio на базе Linux, что обеспечило корректное взаимодействие с драйверами UHD (USRP Hardware Driver).

После подключения USRP B200 и активации компонента Cypress Westbridge в настройках виртуальной машины устройство определялось в GNU Radio как `uhd.usrp_source`, готовое к использованию в потоковых графах.

Программная часть комплекса построена по двухуровневой архитектуре. Ядром является граф обработки сигналов, сгенерированный в GNU Radio Companion в виде Python-класса `Base_detection`. Этот класс обеспечивает ряд действий:

1. Настройка и запуск приёмника USRP с заданными центральной частотой, частотой дискретизации и коэффициентом усиления.
2. Преобразование потока комплексных отсчётов в спектр мощности с помощью БПФ.
3. Визуализация спектра и «водопада» в реальном времени.
4. Вызов встроенных Python-блоков для анализа спектра.

Поверх этого низкоуровневого слоя работает управляющее приложение `MyEnhancedApp`, которое наследует класс `Base_detection` и расширяет его функциональность:

1. Обрабатывает сообщения от блоков-детекторов.
2. Ведёт базу данных известных сигналов в формате JSON.
3. Реализует логику записи фрагментов IQ-данных при обнаружении нового сигнала.
4. Предоставляет графический интерфейс для отображения результатов идентификации и управления записью.

Такая архитектура позволила отделить базовую функциональность SDR от высокоуровневой логики приложения, что значительно упростило разработку и отладку.

Настройка параметров сканирования: ширина полосы и частотное разрешение

Одной из ключевых особенностей разработанного комплекса является возможность гибкой настройки параметров сканирования в зависимости от решаемой задачи. В текущей конфигурации ширина анализируемой полосы составляет 2,4 МГц, что достаточно для обнаружения большинства узкополосных сигналов, однако для полноценного захвата широкополосных сигнатур БПЛА (например, каналов управления с FHSS, занимающих до 20 МГц) этого может оказаться недостаточно. В то же время прямое увеличение полосы обзора ведёт к росту вычислительной нагрузки и снижению частотного разрешения, что негативно сказывается на точности измерения параметров сигнала.

Основными переменными, определяющими ширину полосы сканирования и разрешение спектрограммы, являются `samp_rate` (частота дискретизации, Гц) и `fft_length` (размер блока БПФ). Ширина отображаемого спектра равна `samp_rate`, а частотное разрешение (расстояние между соседними бинами) вычисляется как отношение `samp_rate / fft_length`. Например, при `samp_rate = 2,4e6` и `fft_length = 2048` разрешение составляет около 1,17 кГц, а общая полоса – 2,4 МГц. Если требуется расширить полосу

⁴ Ettus Research. USRP B200/B210 Product Overview. URL: <https://www.ettus.com>

⁵ GNU Radio Documentation. URL: <https://wiki.gnuradio.org>

до 10 МГц, необходимо увеличить `samp_rate` до 10e6, однако при сохранении `fft_length = 2048` разрешение упадёт до 4,88 кГц, что может затруднить идентификацию узкополосных компонент сигнала. Для компенсации этого эффекта следует пропорционально увеличить `fft_length` (например, до 8192), что восстановит прежнее разрешение, но потребует больше вычислительных ресурсов.

Дополнительно в коде присутствует переменная `bandwidth`, задающая полосу пропускания аналогового фильтра USRP (по умолчанию 10e6). При изменении `samp_rate` рекомендуется синхронизировать `bandwidth` с новой частотой дискретизации, чтобы избежать алиасинга. Все перечисленные переменные доступны для редактирования в секции `#Variables` файла `Base_detection.py` и могут быть изменены как вручную, так и через графический интерфейс GNU Radio Companion.

Таким образом, выбор параметров сканирования сводится к поиску компромисса между шириной обзора, точностью измерений и вычислительной нагрузкой на компьютер. Практика показала, что для большинства задач обнаружения БПЛА оптимальным является соотношение `samp_rate = 10e6`, `fft_length = 8192`, обеспечивающее полосу 10 МГц при разрешении около 1,22 кГц, что приемлемо для идентификации типовых сигнатур.

Теоретические аспекты обнаружения сигналов БПЛА

Прежде чем перейти к описанию программных блоков, кратко рассмотрим факторы, влияющие на эффективность обнаружения сигналов БПЛА.

Большинство современных дронов используют для управления и передачи видео диапазоны 2,4 ГГц (2,400–2,4835 ГГц) и 5,8 ГГц (5,725–5,850 ГГц). Некоторые модели применяют 433 МГц (например, Chitwan QW350-02) или 868/915 МГц (Autel EVO II) [5]. Каналы управления часто используют широкополосные сигналы с псевдослучайной перестройкой рабочей частоты (FHSS) или расширением спектра, что требует от системы мониторинга достаточной мгновенной полосы пропускания и высокой чувствительности.

Мощность теплового шума на входе приёмника определяется выражением:

$$P_{\text{ш}} = k \cdot T \cdot B \cdot K_{\text{ш}}, \quad (1)$$

где k – постоянная Больцмана; T – шумовая температура, B – ширина полосы, $K_{\text{ш}}$ – коэффициент шума [6].

Таким образом, при расширении полосы в k раз мощность шума возрастает в k раз, что при фиксированной мощности сигнала приводит к снижению отношения сигнал/шум (SNR) на $10 \log_{10}(k)$ дБ. С другой стороны, для корректного воспроизведения широкополосных сигналов необходимо, чтобы полоса пропускания приёмника была не меньше ширины спектра сигнала. В разработанном комплексе частота дискретизации выбрана равной 2,4 МГц, что обеспечивает компромисс между чувствительностью и достаточной полосой обзора для обнаружения большинства каналов управления БПЛА.

Отношение сигнал/шум и точность измерений. Как показано в работах [7, 8], SNR напрямую влияет на точность измерения навигационных параметров и, как следствие, на точность позиционирования. В контексте данной задачи SNR определяет надёжность детектирования сигнала и точность определения его центральной частоты и ширины полосы. Для повышения SNR в программном комплексе применяется накопление спектров (интегрирование) и сглаживание скользящим средним.

Потоковый граф GNU Radio и пользовательские блоки

Потоковый граф, реализованный в классе `Base_detection`, включает следующие ключевые блоки:

1. `uhd.usrp_source` — источник IQ-отсчётов от USRP.
2. `stream_to_vector` и `keep_one_in_n` — преобразование потока в векторы и децимация для снижения вычислительной нагрузки.
3. `fft_vcc` — вычисление спектра мощности с использованием окна Блэкмана-Харриса для уменьшения растекания спектра.
4. `complex_to_mag_squared` и `moving_average` — вычисление квадрата модуля и сглаживание для получения усреднённого спектра.
5. `nlog10_ff` — перевод в логарифмический масштаб (дБ).
6. `qtgui_vector_sink_f` и `qtgui_waterfall_sink_c` — визуализация спектра и водопада.

Для реализации специфических функций детектирования и анализа сигналов были разработаны три встроенных Python-блока.

Блок `bandwidth_detector` является центральным элементом анализа. На вход он получает вектор спектральных отсчётов в дБ, а на выходе формирует сообщения с параметрами обнаруженного сигнала. Основные методы блока:

1. `estimate_noise_floor` — оценивает уровень шума как медианное значение спектра, что обеспечивает устойчивость к выбросам.

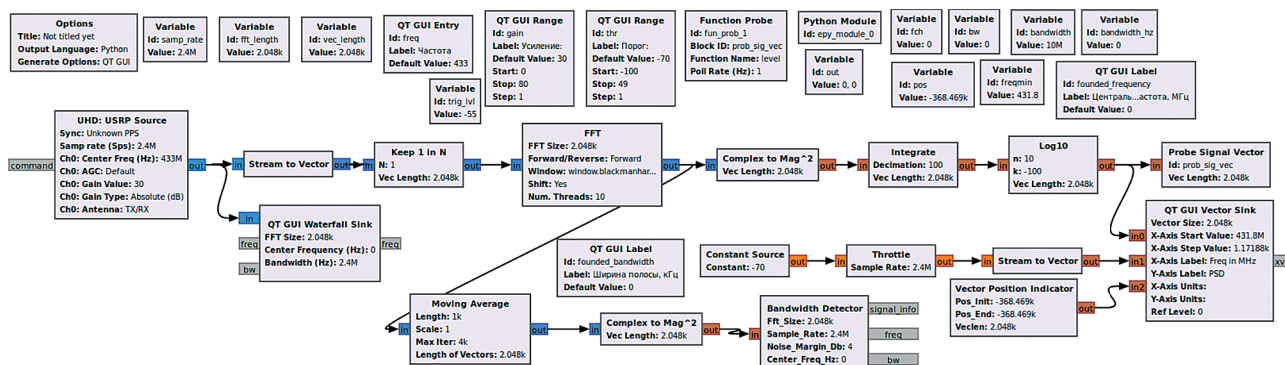


Рис. 2. Поточковый граф программы

2. `detect_signal_center` – находит индекс бина с максимальной амплитудой и сравнивает его с заданным порогом `threshold_db`.
3. `find_signal_bandwidth` – от найденного центра ищет границы влево и вправо до тех пор, пока значение не опустится ниже уровня `noise_floor + noise_margin_db`. Разность граничных частот, умноженная на частотное разрешение, даёт ширину полосы.

Блок публикует сообщения через порты `bw` и `freq`, передавая словарь с полями `bandwidth_hz`, `center_freq_hz`, `snr_db` и др. Ниже приведён фрагмент метода обнаружения центра сигнала:

```
python
def detect_signal_center(self,
spectrum_db):
    peak_bin = np.argmax(spectrum_db)
    if spectrum_db[peak_bin] > self.
threshold_db:
        return peak_bin
    return None
```

В модуле `ery_module_0` реализована вспомогательная функция `detect`, используемая для инициализации переменных в `Base_detection`. Она выполняет поиск каналов в спектре, мощность которых превышает порог, и возвращает частоту первого обнаруженного канала и его длину в бинах. Для уточнения центра используется средневзвешенное значение индексов с весами, равными мощностям:

```
python
def avg_freq_pwr(data):
    total_power = np.sum(data)
    if total_power == 0: return 0
    indices = np.arange(len(data))
    return np.sum(indices * data) /
total_power
```

Блок `ery_block_0` генерирует вектор-маску, в которой заданный диапазон индексов (от `pos_init` до `pos_end`) заполняется значением 1000, а остальные элементы — -1000. Маска используется для визуального выделения на спектре

полосы обнаруженного сигнала (зелёная линия на графике).

Name	Size	Modified	Star
Base_detection.py	18.9 kB	Yesterday	☆
BD_Launcher.py	14.1 kB	Yesterday	★
BD_Launcher.py.bak	13.2 kB	Mon	☆
epy_block_0.py	2.3 kB	Yesterday	☆
epy_block_1.py	3.9 kB	Yesterday	☆
epy_module_0.py	3.3 kB	Yesterday	☆
__pycache__	4 items	Yesterday	☆
Signal_recording.grc	39.8 kB	Mon	☆

Рис. 3. Составляющие элементы программы

Алгоритм обнаружения и измерения параметров сигнала

Полный цикл обработки одного кадра спектра выглядит следующим образом:

1. Поток IQ-отсчётов с выхода USRP буферизуется в вектор длиной `fft_length` (2048).
2. Выполняется БПФ с окном Блэкмана – Харриса, вычисляется квадрат модуля, производится сглаживание и логарифмирование.
3. Полученный спектр в дБ подаётся на вход блока `bandwidth_detector` и одновременно отображается на графике.
4. Блок `bandwidth_detector` оценивает шум, ищет пик выше порога и определяет границы сигнала.

Если сигнал обнаружен, блок публикует сообщение с параметрами.

Приложение MyEnhancedApp получает сообщение, обновляет информационную панель и, если сигнал не найден в базе, активирует кнопку записи.

Экспериментальная проверка с тестовым FM-тоном шириной 200 кГц на частоте 434,8 МГц показала, что центральная частота определяется с погрешностью не более ± 2 кГц, а ширина

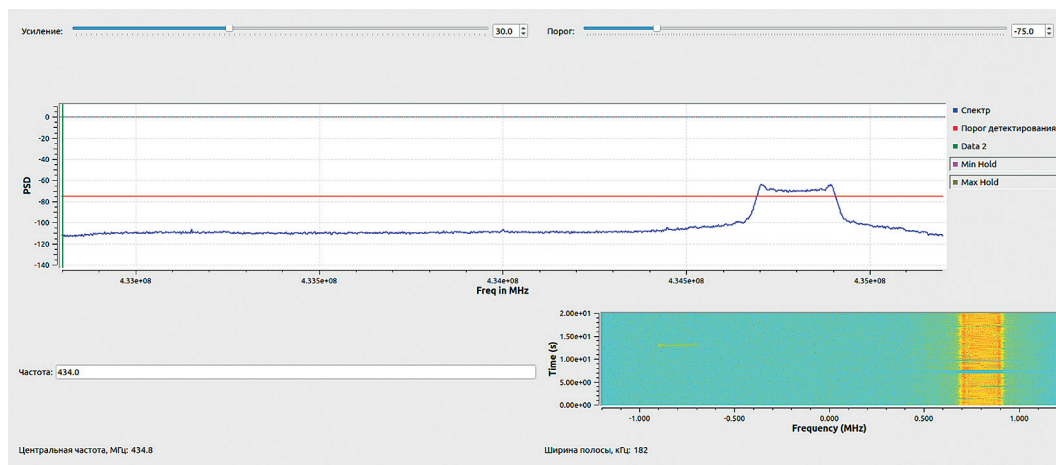


Рис. 4. Проверка работоспособности программы на определение параметров сигнала

полосы – с точностью около 5 %. Погрешность обусловлена конечной крутизной спадов спектра реального сигнала и дискретностью БПФ.

База данных сигналов и алгоритм идентификации

Для решения задачи идентификации была разработана подсистема хранения и сопоставления сигнатур, реализованная в классе MyEnhancedApp.

Каждая запись в базе описывается классом KnownSignal (dataclass) и содержит поля: id, name, center_freq_hz, bandwidth_hz, а также допуски freq_tolerance_hz (по умолчанию 5 кГц) и bw_tolerance_hz (30 кГц).

Класс SignalDatabase управляет списком сигналов в памяти и синхронизирует его с JSON-файлом на диске. При запуске приложения база загружается, а при добавлении нового сигнала – автоматически сохраняется.

При поступлении параметров обнаруженного сигнала вызывается метод find_matching_signal, который последовательно сравнивает частоту и ширину полосы с каждой записью. Если разности не превышают допусков, сигнал считается известным. Ниже представлен фрагмент кода метода сопоставления:

```
python
def find_matching_signal(self,
center_freq_hz, bandwidth_hz):
    for signal in self.signals:
        if abs(center_freq_hz - signal.
center_freq_hz) <= signal.freq_
tolerance_hz \
        and abs(bandwidth_hz - signal.
bandwidth_hz) <= signal.bw_ tolerance _
hz:
        return signal
    return None
```

Такой подход устойчив к небольшим погрешностям измерений и естественным флуктуациям параметров сигнала.

Механизм записи и пополнения базы

При обнаружении сигнала, отсутствующего в базе, оператору предоставляется возможность записать 100-миллисекундный фрагмент IQ-данных и сохранить его в базу. Для этого в MyEnhancedApp реализованы:

1. file_sink – блок GNU Radio, подключаемый параллельно к выходу USRP и управляемый программно.
2. record_timer – таймер Qt, ограничивающий длительность записи.
3. Диалоговое окно с полем ввода имени сигнала.

После завершения записи временный файл temp_signal.dat переименовывается в signal_<id>_<name>.dat, а параметры сигнала добавляются в JSON-базу. Такой подход позволяет накапливать библиотеку сигнатур, которую в дальнейшем можно использовать для автоматической идентификации типов БПЛА.

```
1 [
2 {
3   "id": 6,
4   "name": "Test1",
5   "center_freq_hz": 433450000.0,
6   "bandwidth_hz": 5000.0,
7   "freq_tolerance_hz": 30000,
8   "bw_tolerance_hz": 100000
9 },
10 {
11   "id": 7,
12   "name": "Test2",
13   "center_freq_hz": 432850000.0,
14   "bandwidth_hz": 5000.0,
15   "freq_tolerance_hz": 30000,
16   "bw_tolerance_hz": 100000
17 },
18 {
19   "id": 8,
20   "name": "Test3",
21   "center_freq_hz": 433740500.0,
22   "bandwidth_hz": 53000.0,
23   "freq_tolerance_hz": 30000,
24   "bw_tolerance_hz": 100000
25 }
26 ]
```

Рис. 5. Содержимое JSON-файла базы сигналов

Экспериментальные результаты

Работоспособность комплекса проверялась в лабораторных условиях с использованием генератора HaskRF и реальных сигналов БПЛА.

Основные достигнутые характеристики:

1. Диапазон сканирования: 70 МГц – 6 ГГц (ограничен возможностями USRP).
2. Мгновенная полоса анализа: 2,4 МГц (может быть увеличена ценой снижения чувствительности).

3. Пороговая чувствительность: около -100 дБм при полосе 200 кГц (с накоплением 100 спектров).

4. Точность определения центральной частоты: ± 2 кГц.

5. Погрешность измерения ширины полосы: не более 5 % для сигналов с крутыми фронтами.

Как показано в [8, 10], увеличение полосы пропускания ведёт к снижению SNR и, как следствие, к росту вероятности ошибок. В нашем

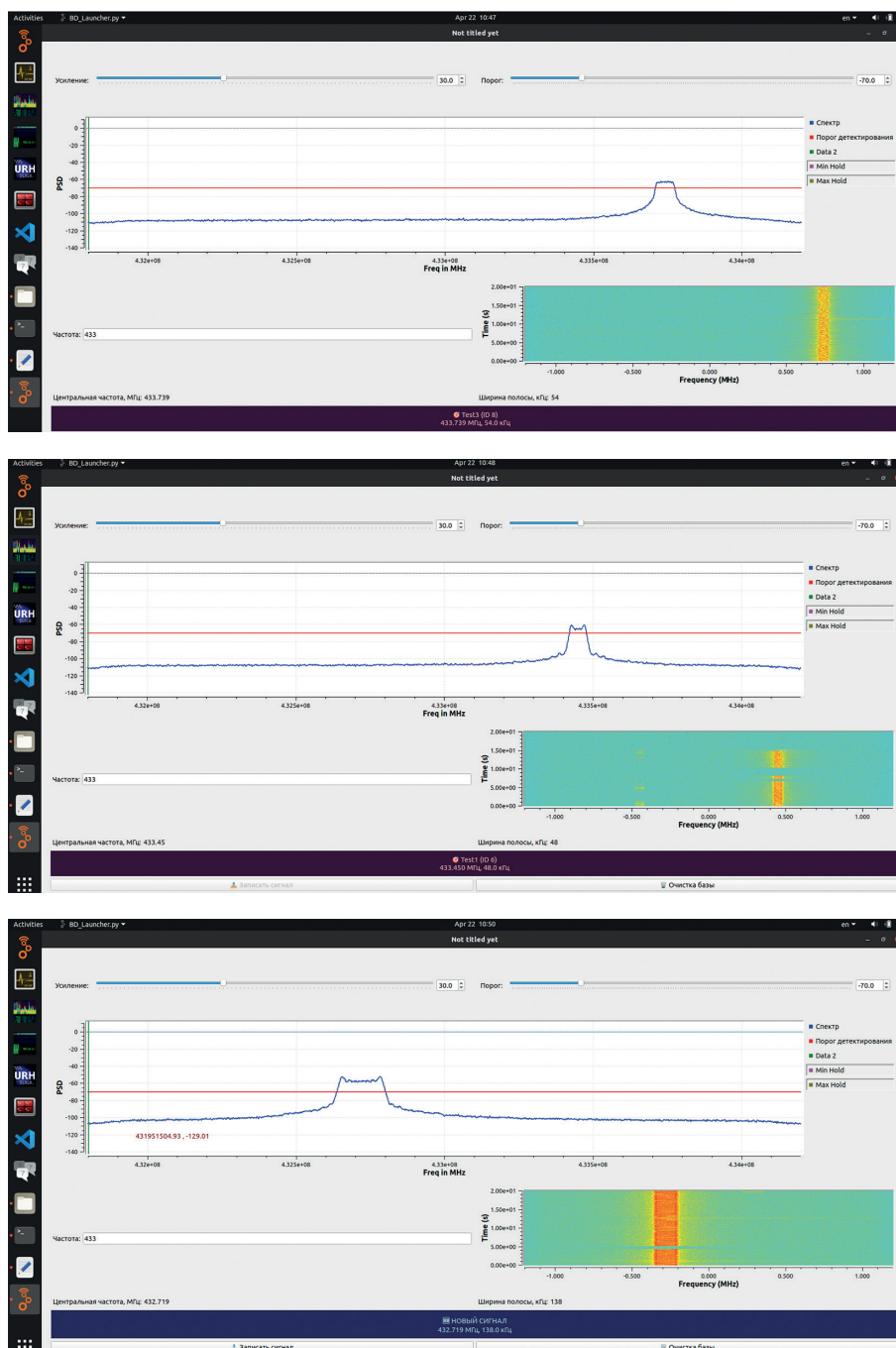


Рис. 6. Проверка работоспособности идентификации сигналов

комплексе выбор частоты дискретизации 2,4 МГц и размера БПФ 2048 даёт частотное разрешение около 1,17 кГц, что достаточно для различения каналов управления большинства дронов. При необходимости повышения точности можно увеличить длину БПФ или уменьшить полосу обзора, сузив фильтр.

В ходе эксперимента были записаны сигналы нескольких типов. При повторном появлении сигнала программа корректно идентифицировала его как известный, отобразив на информационной панели имя и ожидаемые параметры. Для неизвестного сигнала, сгенерированного HackRF, было предложено сохранить его в базу с произвольным именем.

В отличие от традиционных спектроанализаторов, предлагаемый комплекс не только визуализирует спектр, но и автоматически измеряет параметры сигнала и ведёт базу сигнатур. По сравнению с коммерческими системами радиомониторинга его стоимость на порядок ниже, а открытая архитектура позволяет адаптировать алгоритмы под конкретные задачи.

В результате эксперимента (рис. 6) была проведена проверка алгоритма идентификации сигналов. При излучении первых двух сигналов из базы (рис. 5) они были определены программой как известные, а также выведены их исходные параметры. При излучении ранее неизвестного сигнала программа даёт возможность его сохранить, предоставляя кнопку «Записать сигнал» активной.

Направления дальнейшего развития

Созданный программно-аппаратный комплекс представляет собой законченное решение для радиомониторинга, но его потенциал может быть расширен в следующих направлениях:

Автоматизация записи: реализация полностью автоматического режима, при котором любой новый сигнал записывается без участия оператора.

Углублённый анализ: переход от сравнения по двум параметрам к корреляционному анализу спектров или использованию классификаторов на основе машинного обучения для повышения точности идентификации.

Интеграция с системами противодействия: дополнение комплекса блоком подавления (jammer) и алгоритмом автоматического сопровождения цели.

Распределённая сеть мониторинга: синхронизация нескольких SDR-приёмников по сигналам GPS PPS для реализации TDoA-пеленгации [9, 10].

Заключение

В результате выполненной работы с нуля разработан и экспериментально апробирован программно-аппаратный комплекс на основе открытой среды GNU Radio и SDR-приёмника USRP B200/B210, предназначенный для решения задач поиска, измерения параметров и идентификации сигналов БПЛА. Последовательно решены задачи развёртывания виртуализированного программного окружения, построения потокового графа обработки сигналов в GNU Radio Companion, создания специализированных встроенных блоков на языке Python для порогового детектирования, автоматического определения центральной частоты и ширины спектра, а также реализации подсистемы хранения и сопоставления сигнатур в формате JSON с пользовательским интерфейсом управления записью.

Экспериментальные испытания подтвердили работоспособность и устойчивость предложенных алгоритмов. Комплекс обеспечивает мониторинг в диапазоне 70 МГц – 6 ГГц с мгновенной полосой анализа 2,4 МГц (расширяемой до 10 МГц при сохранении приемлемого частотного разрешения порядка 1,2 кГц), точность определения центральной частоты ± 2 кГц и погрешность измерения ширины полосы не более 5 %. Достигнутая пороговая чувствительность составляет около -100 дБм в полосе 200 кГц, что достаточно для обнаружения каналов управления большинства коммерческих БПЛА. Функция идентификации на основе базы сигнатур с допусками по частоте и ширине полосы показала корректное распознавание ранее записанных сигналов в условиях лабораторных экспериментов.

Научная значимость работы заключается в демонстрации целостной архитектуры программного SDR-решения, объединяющего в реальном времени спектральный анализ, извлечение параметров сигналов и их идентификацию исключительно на базе открытого программного обеспечения и доступного аппаратного обеспечения. Практическая ценность состоит в создании недорогого и гибкого инструмента радиомониторинга, который может быть использован как в исследовательских целях, так и в качестве основы для построения специализированных систем обнаружения БПЛА.

К ограничениям текущей реализации следует отнести ручной режим инициализации записи новых сигналов, фиксированные допуски при идентификации, а также зависимость вычислительной нагрузки от выбранной частоты дискретизации и длины БПФ. Дальнейшее развитие комплекса предполагает внедрение

автоматического режима пополнения базы сигнатур, применение методов машинного обучения для повышения точности идентификации за счёт анализа формы спектра, интеграцию с модулями подавления (jammer) и синхронизацию нескольких приёмников по сигналам GPS PPS для реализации разностно-дальномерной

пеленгации (TDoA). Полученные результаты подтверждают перспективность использования технологий SDR и открытых программных платформ для создания эффективных и экономичных систем радиомониторинга в интересах противодействия несанкционированному применению беспилотных летательных аппаратов.

Литература

1. Лысов А. В. Основные характеристики БПЛА, используемые на поле боя. – СПб: Лаборатория ППШ, 2024. – 357 с.
2. Боев Н. М. Анализ радиолиний связи с беспилотными летательными аппаратами // Вестник СибГАУ, 2012. – № 2. – С. 86–91.
3. Костин М. С., Ярлыков А. Д. Архитектурно-конфигурируемые SDR-технологии радиомониторинга и телеметрии. – М.: Инфра-Инженерия, 2021. – 147 с.
4. Галкин В. А. Основы программно-конфигурируемого радио. – М.: Горячая линия – Телеком, 2013. – 372 с.
5. Робенков Д. Н., Демченко А. А. Построение системы связи с беспилотным летательным аппаратом // СПб-ГУПС, 2023. – С. 278–280.
6. Шалаев А. А. Оценка фактических значений отношения сигнал/шум в радионавигационных системах на основе экспериментальных данных // Crede Experto, 2025. – № 4. – С. 60–75.
7. Арефьев Р. О., Скрипник О. Н., Арефьева Н. Г. Опыт использования программно-определяемых GNSS приёмников // Crede Experto, 2022. – № 1. – С. 88–99.
8. Семенко А. И., Бокла Н. И., Домрачева Е. А. Определение помехозащищённости телекоммуникационных систем с многопозиционным фазоманипулированным сигналом // Доклады АН ВШ РФ, 2017. – № 2 (35). – С. 97–106.
9. Гилев И. В., Канавин С. В. Программа автоматизации определения местоположения мобильного источника радиоизлучения с использованием приемника программно-определяемого радио // Вестник Воронежского института МВД России, 2025. – № 3. – С. 150–161.
10. Арзуманян А. Г., Севоян О. Ж., Гомцян О. А. Синхронная система обработки и передачи данных с привязкой к шкале единого мирового времени // Информационные технологии и телекоммуникации, 2016. – Т. 4. – № 2. – С. 12–19.

SOFTWARE PACKAGE FOR SEARCHING AND IDENTIFYING SIGNALS FOR SDR BASED ON THE GNU RADIO PLATFORM

Baymakov D. A.⁶, Tkachev D. F.⁷, Vorobyov P. V.⁸

Keywords: software-defined radio, GNU Radio, USRP B210, UAV detection, spectral analysis, Python blocks, signal identification, signature database.

Abstract

The goal of the work is to create a complete solution that allows scanning specified frequency ranges in real time, automatically recording exceedances of the threshold power level, determining the parameters of the detected signals and identifying them based on a pre-formed database of signatures.

Results of the study: a hardware and software stand has been created for monitoring the electromagnetic environment in the operating ranges of unmanned aerial vehicles (UAV) control channels using software-defined radio (SDR) technology. The test bench is implemented on the basis of the USRP B200/B210 receiver and the GNU Radio open environment deployed in the Oracle VirtualBox virtual machine for threshold detection, measurement of the center frequency and spectrum width, as well as the creation of a signature database with an automatic identification function. The key fragments of the program code and the results of the experimental verification of the system are presented. Factors affecting the accuracy of measurements and prospects for further development of the complex are discussed.

The practical value lies in the creation of an integral architecture of the software package that combines in real time spectral analysis, measurement of signal parameters and its identification based on a database of signatures using only open software and available SDR equipment.

⁶ **Danil A. Baymakov**, operator of the scientific company of the Military Academy of Communications named after Marshal of the Soviet Union S. M. Budyonny. St. Petersburg, Russia. E-mail: baymakovdanil@gmail.com

⁷ **Dmitry F. Tkachev**, Head of the Research Department 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: dimas.portnoy@inbox.ru

⁸ **Pavel V. Vorobyov**, Researcher of the Research Department 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: pvorobyev98@gmail.com

References

1. Lysov A. V. Osnovnye harakteristiki BPLA, ispol'zuemye na pole boya. – SPb: Laboratoriya PPSH, 2024. – P. 357.
2. Boev N. M. Analiz radiolinij svyazi s bespilotnymi letatel'nymi apparatami // Vestnik SibGAU, 2012. – No 2. – Pp. 86–91.
3. Kostin M. S., Yarlykov A. D. Arhitekturno-konfiguriruemye SDR-tehnologii radiomonitoringa i teletmetrii. – M.: Infra-Inzheneriya, 2021. – P. 147.
4. Galkin V. A. Osnovy programmno-konfiguriruемого radio. – M.: Goryachaya liniya – Telekom, 2013. – P. 372.
5. Roenkov D. N., Demchenko A. A. Postroenie sistemy svyazi s bespilotnym letatel'nym apparatom // SPbGUPS, 2023. – Pp. 278–280.
6. Shalaev A. A. Ocenka fakticheskikh znachenij otnosheniya signal/shum v radionavigacionnykh sistemah na osnove ehksperimental'nykh dannykh // Crede Experto, 2025. – No 4. – Pp. 60–75.
7. Aref'ev R. O., Skrypnik O. N., Aref'eva N. G. Opyt ispol'zovaniya programmno-opredelyaemykh GNSS priyomnikov // Crede Experto, 2022. – No 1. – Pp. 88–99.
8. Semenko A. I., Bokla N. I., Domracheva E. A. Opredelenie pomehozashchishchennosti telekommunikacionnykh sistem s mnogopozicionnym fazomanipulirovannym signalom // Doklady AN VSh RF, 2017. – No 2 (35). – Pp. 97–106.
9. Gilev I. V., Kanavin S. V. Programma avtomatizatsii opredeleniya mestopolozheniya mobil'nogo istochnika radio-izlucheniya s ispol'zovaniem priemnika programmno-opredelyaemogo radio // Vestnik Voronezhskogo instituta MVD Rossii, 2025. – No 3. – Pp. 150–161.
10. Arzumanyan A. G., Sevoyan O. Zh., Gomcyan O. A. Sinhronnaya sistema obrabotki i peredachi dannykh s privyazkoj k shkale edinogo mirovogo vremeni // Informacionnye tehnologii i telekommunikatsii, 2016. – V. 4. – No 2. – Pp. 12–19.



АЛГОРИТМЫ ОБРАБОТКИ СИГНАЛА ПРИ ЗОНДИРОВАНИИ ЛАЗЕРНОЙ ЛОКАЦИОННОЙ СТАНЦИЕЙ ЛЕТАТЕЛЬНОГО АППАРАТА

Козирацкий А. Ю.¹, Чёнгин А. В.², Гревцев А. И.³

DOI:10.21681/3034-4050-2026-3-49-56

Ключевые слова: лазерная локация, гетеродин, максимальное правдоподобие, оценка амплитуды, оценка частоты, квадрокоптер, обнаружение.

Аннотация

Цель работы: разработка алгоритмов обнаружения и оценок параметров отраженного сигнала от вращающихся винтов беспилотного летательного аппарата малого класса при зондировании лазерной локационной станцией гетеродинного типа.

Метод исследования: метод максимального правдоподобия.

Результаты: разработаны алгоритмы обнаружения и оценок параметров отраженного от вращающихся винтов сигнала при зондировании лазерной локационной станцией гетеродинного типа беспилотного летательного аппарата малого класса. Процесс формирования оценок является многоитерационным вследствие подстройки фазового фронта гетеродина. Оценки формируются на всем протяжении подстройки фазового фронта и хранятся в буферном устройстве. Наиболее правдоподобной считается та оценка, у которой амплитуда больше. Алгоритмы позволяют по входным реализациям получить исходные данные для методики формирования идентификации подсистемой лазерной разведки беспилотных летательных аппаратов малого класса лазерной локационной станцией гетеродинного типа. Предложенные алгоритмы позволяют оптимальным образом оценить амплитуду и частоту биений на выходе фотоприемного устройства с учетом подстройки фазового фронта гетеродина, а также определить статистические характеристики полученных оценок, что в свою очередь позволяет сформировать требования к параметрам подсистемы разведки воздушного пространства на основе использования лазерной локационной станции гетеродинного типа.

Научная новизна: алгоритмы обнаружения и оценки параметров входных сигналов, необходимых для идентификации подсистемой лазерной разведки беспилотных летательных аппаратов малого класса в воздушном пространстве, отличаются от известных введением дополнительной процедуры подстройки фазового фронта гетеродина.

Введение

Существующие способы борьбы с квадрокоптерами включают средства радиоэлектронной борьбы (РЭБ), предназначенные для подавления каналов управления и навигации, кинетические средства поражения (стрелковое оружие, зенитные комплексы, сетемётные устройства). Стрелковое оружие, зенитные комплексы малоэффективны против малоразмерных БПЛА, а применение средств РЭБ не гарантирует физического уничтожения цели и может быть бесполезно, в случае если квадрокоптер управляется по оптоволоконному каналу. В этой связи лазерные системы поражения представляют особый интерес как высокоточные, быстронаводимые средства, обеспечивающие направленное энергетическое воздействие на элементы конструкции квадрокоптера.

Применение одиночных источников импульсного лазерного излучения (ИИ) большой мощности сопряжено с рядом физических и технических ограничений. При достижении плотности мощности излучения превышающих порог пробоя атмосферы возникает ионизация среды распространения (воздуха), что приводит к формированию плазменного канала, рассеянию и расфокусировке излучения, снижению эффективности передачи энергии к цели. Кроме того, экстремальные требования к одному лазерному излучателю (по пиковой мощности, термостабильности и ресурсу) усложняют конструкцию системы, повышают её стоимость и снижают надёжность.

В источниках [1, 2] обоснован способ пространственного сложения электромагнитных излучений когерентных источников. Способ

¹ Козирацкий Александр Юрьевич, доктор технических наук, профессор, профессор кафедры радиотехники и антенно-фидерных устройств военного учебно-научного центра Военно-воздушной академии им. профессора Н. Е. Жуковского и Ю. А. Гагарина. Воронеж, Россия. E-mail: sashfish@bk.ru

² Чёнгин Александр Владимирович, адъюнкт военного учебно-научного центра Военно-воздушной академии им. профессора Н. Е. Жуковского и Ю. А. Гагарина. Воронеж, Россия. E-mail: alexsvist168@mail.ru

³ Гревцев Александр Иванович, кандидат технических наук, доцент, заместитель начальника кафедры радиотехники и антенно-фидерных устройств военного учебно-научного центра Военно-воздушной академии им. профессора Н. Е. Жуковского и Ю. А. Гагарина. Воронеж, Россия. E-mail: grevtsev.sanche@yandex.ru

направлен на физическое поражение (плавление, поджигание конструктивных элементов) БЛА малого класса за счет накопления энергии от импульсных последовательностей отдельных лазерных источников. В работе [3] описана методика поражения БЛА малого класса пространственно-распределенной системой источников направленной энергии большой мощности. Ключевая идея заключается в том, что при использовании отдельных источников излучения имеется возможность настроить систему так, чтобы пиковая мощность в отдельных лучах, формируемых каждым ИИ, была ниже порога интенсивности, приводящей к ионизации среды распространения, обеспечивая при этом максимально возможную мощность в точке сложения импульсов (на БЛА), при заданных начальных энергетических параметрах излучателей. Кроме того, для достижения минимального времени поражения имеется возможность увеличения количества ИИ, следствием чего является увеличение мощности излучения в точке сложения импульсов. На рисунке 1 представлен вариант применения пространственно-распределенной системы направленной энергии.

Решение

В предложенной пространственно-распределенной системе направленной энергии в качестве поражающих элементов решено применять лазеры на CO_2 , поскольку основными компонентами конструктивных элементов БЛА являются полимеры, у которых коэффициент поглощения

излучения с длиной волны 10,6 мкм составляет $5 \cdot 10^3 - 1 \cdot 10^4 \text{ см}^{-1}$. Благодаря очень малой глубине проникновения энергия концентрируется в тонком поверхностном слое, что обеспечивает быстрый локальный перегрев и эффективное термическое разрушение материала при минимальных энергетических затратах по сравнению с лазерами видимого и ближнего ИК-диапазона. Для обоснования режима работы источников излучения проанализировано поведение полимерных материалов, при различных длительностях импульсов воздействия. У полимерного материала есть характерное время тепловой релаксации – десятки миллисекунд. Это время, за которое тепло, внесённое в тонкий поверхностный слой, успевает заметно распространиться вглубь и частично рассеяться. Если импульсы приходят реже, чем это время (например, десятки герц), поверхность между ними ощутимо остывает. Тогда нагрев становится пульсирующим, и значительная часть энергии теряется из-за охлаждения между импульсами. В этом режиме рост средней температуры замедляется. Когда частота повышается так, что пауза между импульсами становится существенно меньше времени тепловой релаксации (несколько миллисекунд против десятков миллисекунд), поверхность уже не успевает остывать. Импульсы начинают эффективно накапливать температуру, и нагрев по своему характеру практически не отличается от непрерывного излучения той же средней мощности. Минимальная частота, при которой наблюдается такой эффект,

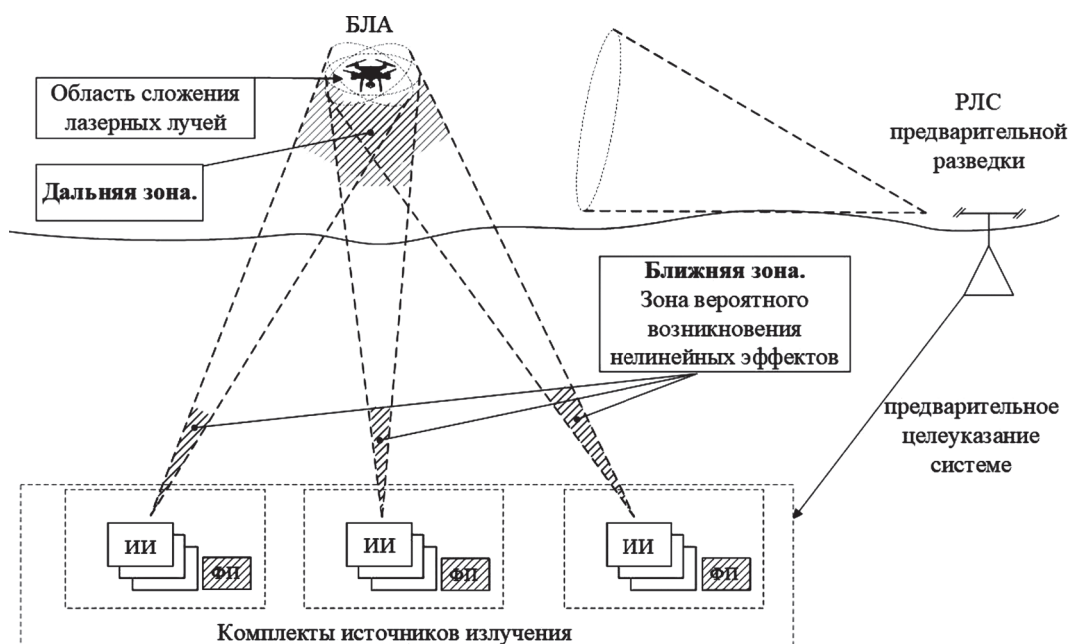


Рис.1. Пространственно-распределенная система направленной энергии

составляет 200 Гц при длительности импульсов 100 мкс. Учитывая это, определен режим работы ИИ. Резонатор ИИ должен работать в режиме импульсной накачки. Работа в данном режиме обеспечивает требуемые параметры излучения, не подвергая отдельные источники излучения экстремальным нагрузкам, что обеспечивает надежность.

Для достижения поставленной цели – поражения БПЛА – системе разведки необходимо решить задачу обнаружения его в воздушном пространстве, а именно идентифицировать цель как БПЛА малого класса и отличить от других объектов, например птиц. На основе способа, представленного в работе [4], для обеспечения эффективного функционирования приемопередающей аппаратуры подсистемы разведки на основе лазерной локационной станции гетеродинного типа предлагается идентифицировать БПЛА малого класса, по оценке параметров отраженного зондирующего лазерного излучения от вращающихся лопастей винтов. Предлагаемое решение отличается от известных введением в конструкцию фотоприемного устройства, с последующей оценкой амплитуды и частоты биений на выходе. Это позволяет по оценкам величин амплитуды и частоты фототоков с выхода фотоприемного устройства определить вращение винтов, способствующее повышению вероятности правильного обнаружения системы разведки воздушного пространства.

Для анализа отраженного от вращающихся винтов сигнала требуется разработка алгоритмов приема и определения его параметров, позволяющих наилучшим образом выделить полезный сигнал на фоне непреднамеренных естественных помех и собственных шумов, а также произвести наиболее точные оценки требуемых информационных параметров, ошибки определения которых не будут существенно понижать эффективность обнаружения и идентификации объекта.

Для принятия решения о том, что цель является квадрокоптером необходимо знать частоту вращения лопастей винтов. Для примера, чтобы рассчитать количество оборотов винтов БПЛА малого класса, можно использовать формулу: обороты в минуту = $KV \times$ вольтаж аккумулятора (где KV – это коэффициент, который показывает, сколько оборотов в минуту сделает двигатель на каждый поданный на него вольт напряжения без нагрузки). Например, если мотор с маркировкой 2400KV и используется стандартный 4S аккумулятор (полный заряд – 16,8 В), то $2400 \times 16,8 = 40320$ оборотов в минуту – с такой скоростью двигатель будет вращаться при

полном газе. Таким образом, частота вращения лопастей винта, который установлен на данном типе мотора, будет составлять 1344 Гц (для винта с двумя лопастями). Рассмотрим общую схему функционирования подсистемы разведки БПЛА малого класса, представленную на рисунке 2.

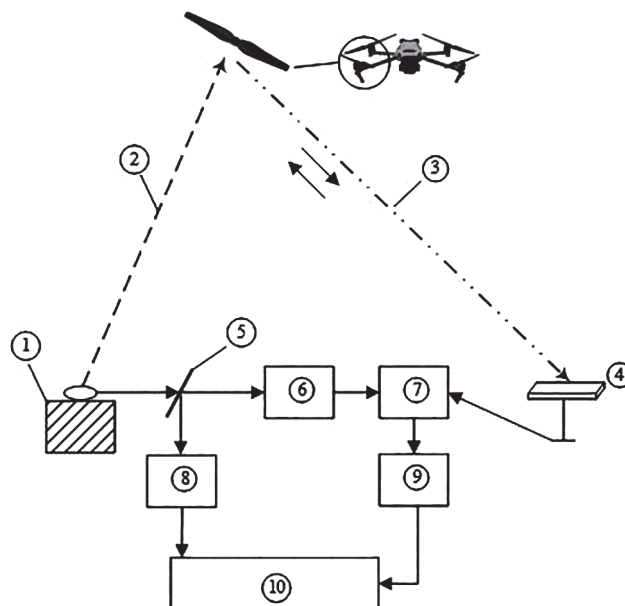


Рис. 2. Цикл разведки воздушной цели

Подсистема функционирует следующим образом. Квантовый генератор 1 формирует в направлении разведки поток импульсного лазерного излучения 2. Сгенерированное излучение поступает в передающую оптическую систему, часть мощности при помощи полупрозрачного зеркала 5 поступает на вход опорного фотодетектора (ОФД) 8. На выходе ОФД формируется управляющее напряжение, запускающее измеритель временных интервалов (ИВИ) в устройстве обработки сигналов 10.

Отраженный сигнал 3 от цели поступает на вход приемной оптической системы 4. Принимаемое оптическое излучение преобразуется в электрический сигнал фотодетектором 7, осуществляется его фотосмещение с опорным сигналом, поступившим с линии задержки 6, полученный сигнал усиливается и поступает на вход порогового детектора (ПД) 9. В случае превышения установленного порогового значения, на выходе ПД формируется управляющий сигнал, останавливающий ИВИ.

Далее в устройстве обработки сигналов происходит оценивание вибрационных параметров. Таким образом происходит обнаружение вибрирующих объектов с использованием лазерной локационной станции гетеродинного типа.

Схема передачи части энергии передающего канала для гетеродинирования представлена на рисунке 3 [5, 6].

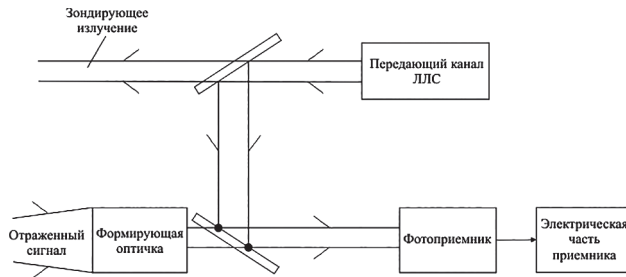


Рис. 3. Схема гетеродинирования

По результатам разведки принимается решение, попадает ли обнаруженный объект под заданные параметры или нет, на основе чего принимается решение о воздействии в указанный сектор источниками излучения из состава пространственно-распределенной системы направленной энергии.

Целью работы является разработка алгоритмов обнаружения и оценки параметров сигнала при зондировании лазерной локационной станцией беспилотного летательного аппарата малого класса.

Таким образом, результаты указанных исследований в области лазерной локации повышают достоверность решения о факте обнаружения и идентификации квадрокоптера лазерной локационной станцией гетеродинного типа. Связка высокоточной лазерной локации с многоканальным лазерным поражающим устройством формирует единый информационно-энергетический комплекс, обеспечивающий полный цикл – от обнаружения и сопровождения квадрокоптера до его выведения из строя.

Алгоритм оценки амплитуды биений, возникающих на выходе фотоприемного устройства

Полагая, что при решении задачи обнаружения принято решение о наличии полезного сигнала на выходе ФП, произведем оценку амплитуды биений [7–9].

Для получения параметров вибрации необходимо осуществлять подстройку фазового фронта лазера гетеродина. Оценки амплитуды биений с выхода ФП формируются непрерывно. Из совокупности полученных значений оцениваемого параметра за время подстройки фазового фронта гетеродина, наиболее правдоподобной считается амплитуда, у которой уровень энергии выше. Рассмотрим алгоритм получения оценки амплитуды биений сигнала за один такт.

Пусть в принимаемой смеси

$$x(t) = s(t, A) + n(t), \quad 0 \leq t \leq T \quad (10)$$

информационный сигнал описывается следующим выражением

$$s(t, A) = A \cdot S_0(t) \cos[2\pi\Delta f + \varphi], \quad (11)$$

где $S_0(t)$ – огибающая сигнала единичной амплитуды; φ – случайная фаза; $n(t)$ – белый шум с постоянной спектральной плотностью $F_n(\omega) = N_0/2$; T – интервал наблюдения; $\int_0^T S_0^2(t) dt = E_0$ – энергия единичной огибающей радиосигнала.

Функционал правдоподобия параметра A имеет вид:

$$F(A) = \text{const} \cdot \exp\left[-\frac{A^2 E_0}{2N_0}\right] \cdot I_0\left(\frac{2AZ}{N_0}\right), \quad (12)$$

где $I_0(x)$ – модифицированная функция Бесселя первого рода нулевого порядка; Z – огибающая корреляционной функции.

$$Z = \sqrt{\left[\int_0^T x(t) \cdot S_0(t) \cdot \cos(\omega_0 t) dt\right]^2 + \left[\int_0^T x(t) \cdot S_0(t) \cdot \sin(\omega_0 t) dt\right]^2}. \quad (13)$$

Уравнение правдоподобия:

$$\begin{aligned} \frac{d \ln F(\hat{A})}{d \hat{A}} &= \exp\left[-\frac{\hat{A}^2 E_0}{2N_0}\right] \cdot I_0\left(\frac{2AZ}{N_0}\right) + \\ &+ \exp\left[-\frac{\hat{A}^2 E_0}{2N_0}\right] \cdot I_0\left(-\frac{2\hat{A}Z}{N_0}\right) \cdot \frac{2Z}{N_0} = 0. \end{aligned} \quad (14)$$

В (14) $I_0\left(-\frac{2\hat{A}Z}{N_0}\right) = I_1\left(\frac{2\hat{A}Z}{N_0}\right)$ – модифицированная функция Бесселя первого рода первого порядка.

Из (14) определяется оценка амплитуды

$$\hat{A} = \frac{\left(\frac{2Z}{N_0}\right) \cdot I_1\left(\frac{2AZ}{N_0}\right)}{\left(\frac{E_0}{N_0}\right) \cdot I_0\left(\frac{2AZ}{N_0}\right)}. \quad (15)$$

Множитель $I_1(x) / I_0(x)$ нелинейно зависит от x и изменяется от 0 до 1 при изменении x от 0 до ∞ . Однако уже при $x \geq 3$ $I_1(x) / I_0(x) \approx 1$, поэтому справедливо равенство

$$\hat{A} = \frac{2Z}{N_0}. \quad (16)$$

На рисунке 4 в соответствии с (16) приведена структурная схема устройства оптимальной оценки амплитуды сигнала.

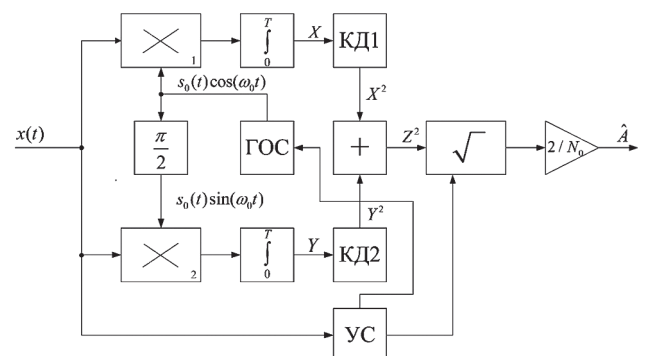


Рис. 4. Структурная схема устройства оптимальной оценки амплитуды

Дисперсию оценки амплитуды можно получить из анализа структуры апостериорной вероятности, если воспользоваться асимптотическим разложением модифицированной функции Бесселя первого рода нулевого порядка.

$$\begin{aligned} P_{PS}(A) &= \text{const} \cdot F(\lambda) = \text{const} \cdot \exp\left[-\frac{A^2 E_0}{2N_0}\right] \cdot I_0\left(\frac{2AZ}{N_0}\right) = \\ &= \text{const} \frac{1}{\sqrt{2\pi}} \left(\frac{2AZ}{N_0}\right)^{-1/\lambda} e^{-\left(\frac{A^2 E_0}{2N_0} - \frac{2AZ}{N_0}\right)} = \\ &= \text{const} \frac{1}{\sqrt{2\pi} \sigma_A} \cdot e^{-\left(\frac{(A - \hat{A})^2}{2\sigma_A^2}\right)}, \end{aligned} \quad (17)$$

где дисперсия оценки амплитуды сигнала имеет вид:

$$\sigma_A^2 = \frac{N_0}{E_0}. \quad (18)$$

Таким образом, для формирования оценки амплитуды биений в ФП необходимо осуществлять подстройку фазового фронта гетеродина. Кроме того, из (18) следует, что потенциальная точность оценки амплитуды тем выше, чем больше энергия сигнала относительно шума.

Алгоритм оценки частоты биений, возникающих на выходе фотоприемного устройства

Для определения вращения винтов помимо оценки амплитуды биений сигнала на выходе ФП необходимо знание их частоты. Пускай произведено обнаружение сигнала, необходимо произвести оценку частоты биений. Для формирования правдоподобной оценки необходимо осуществлять подстройку фазового фронта гетеродина [10]. Рассмотрим алгоритм формирования оценки частоты биений сигнала на выходе ФП за один такт.

Пусть сигнал описывается аналитическим выражением вида

$$S(t, \Delta f) = S_0(t) \cos[2\pi(f_0 - f)t + \varphi], \quad 0 \leq t \leq T \quad (19)$$

в принимаемой смеси

$$x(t) = S(t, \Delta f) + n(t) \quad (20)$$

содержит информацию о смещении частоты Δf . Для этого случая сигнальная функция примет вид:

$$\begin{aligned} y_c(\Delta f) &= \frac{2}{N_0} \int_0^T S_0^2(t) \cdot \cos[2\pi(f_0 - \Delta f_0)t + \varphi] \cdot \\ &\cdot \cos[2\pi(f - \Delta f)t + \varphi] dt = \\ &= \frac{1}{N_0} \int_0^T S_0^2(t) \cdot \cos(2\pi(f - \Delta f_0)t) dt. \end{aligned} \quad (21)$$

Первая и вторая производные (21)

$$y'_c(\Delta f) = \frac{1}{N_0} \int_0^T t S_0^2(t) \cdot \sin(f - \Delta f_0) dt, \quad (22)$$

$$y'_c(\Delta f) = \frac{1}{N_0} \int_0^T t S_0^2(t) \cos(f - \Delta f_0) dt. \quad (23)$$

При $\Delta f = \Delta f_0$, где Δf_0 – истинное значение смещения частоты,

$$\begin{aligned} y'_c(\Delta f) &= -\frac{1}{N_0} \int_0^T t^2 S_0^2(t) dt = \\ &= -\frac{2E}{N_0} \cdot \frac{\int_0^T t^2 S_0^2(t) dt}{\int_0^T S_0^2(t) dt} = \frac{2E}{N_0} \cdot \alpha^2, \end{aligned} \quad (24)$$

где

$$\int_0^T t^2 S_0^2(t) dt = 2E, \quad \alpha^2 = \frac{\int_0^T t^2 S_0^2(t) dt}{\int_0^T S_0^2(t) dt}$$

имеет размерность круговой частоты в квадрате.

Следовательно, дисперсия оценки смещения действительной частоты примет вид

$$\sigma_f^2 = \frac{\sigma_{\alpha}^2}{(2\pi)^2} = \frac{1}{\left(\frac{2E}{N_0}\right) \cdot \alpha^2 (2\pi)^2} = \frac{1}{\left(\frac{2E}{N_0}\right) \cdot T_{\text{эк}}^2}, \quad (25)$$

где $T_{\text{эк}} = 2\pi\alpha$ – эквивалентная длительность сигнала.

Из (25) следует, что потенциальная точность оценки смещения частоты тем выше, чем больше отношение энергии сигнала к спектральной плотности шума и эквивалентная длительность.

Многоканальный вариант структурной схемы оптимальной оценки частоты представлен на рисунке 5.

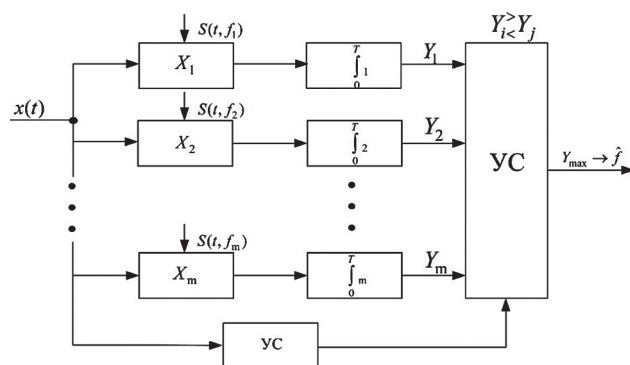


Рис. 5. Многоканальный вариант структурной схемы оптимальной оценки частоты

Основным достоинством данной схемы является быстродействие. Отраженный сигнал распределяется по всем каналам. Каждый канал настроен на свою частоту. С выхода устройства сравнения будет определяться номер канала и значение частоты. Каналы могут настраиваться, используя априорную информацию.

Алгоритм оценки амплитуды и частоты биений, возникающих на выходе фотоприемного устройства

Обобщенная структурная схема устройства оценки амплитуды и частоты биений представлена на рисунке 6 [11].

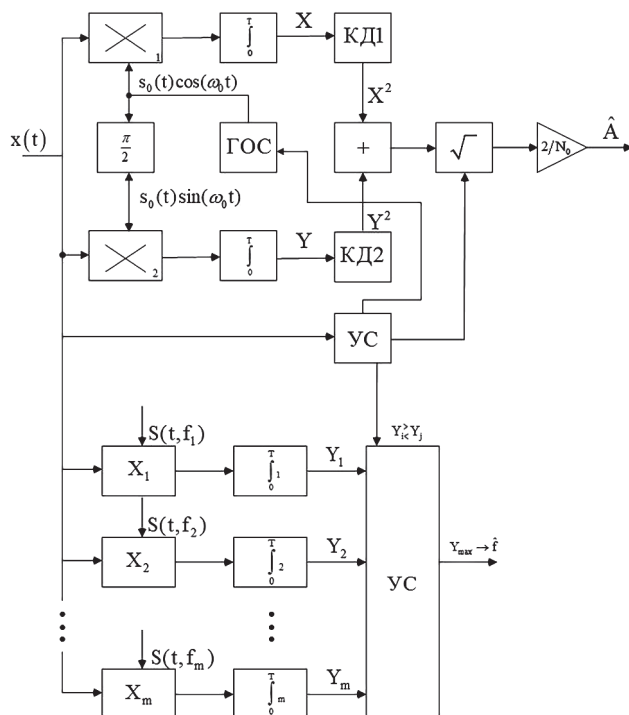


Рис.6. Обобщенная структурная схема устройства формирования оценок амплитуды и частоты биений

Заключение

В результате проведенного исследования разработаны алгоритмы обнаружения и оценивания параметров отражённого сигнала от вращающихся винтов беспилотного летательного аппарата малого класса при зондировании лазерной локационной станцией гетеродинного

типа, основанные на методе максимального правдоподобия. В отличие от известных решений, процедура оценивания организована как последовательный процесс формирования совокупности промежуточных оценок амплитуды и частоты биений на всём интервале фазовой подстройки гетеродина и последующим выбором наиболее правдоподобной реализации по критерию максимальной амплитуды, что повышает устойчивость алгоритма к фазовым искажениям и улучшает качество приёма отражённого сигнала. Получены аналитические выражения и оценки, позволяющие количественно определить их точностные показатели и сформировать обоснованные требования к параметрам фотоприёмного устройства и чувствительности подсистемы лазерной разведки. Показано, что использование оценок частоты биений, обусловленных вращением лопастей, обеспечивает формирование информативных признаков, достаточных для идентификации беспилотных летательных аппаратов малого класса и их различения с объектами иной природы.

Тем самым предложенные алгоритмы обеспечивают получение достоверной информации о наличии и параметрах цели, позволяют классифицировать обнаруженный объект как беспилотный летательный аппарат малого класса на основе оценок частоты и амплитуды отражённого сигнала, на основании чего принимается решение о применении пространственно-распределённой системы направленной энергии.

Литература

1. Патент на изобретение РФ № 2857752, Способ пространственного сложения электромагнитных излучений когерентных источников / Чёнгин А. В., Козирацкий А. Ю., Смынтына О. В., Гревцев А. И., Кусакин О. В., Капитанов В. В. (RU); опубл. 06.03.2026, Бюл. № 7. – М.: ФИПС, 2026.
2. Козирацкий А. Ю., Чёнгин А. В. Способ пространственного сложения электромагнитных излучений когерентных источников // XXV Международная НПК: Информатика: проблемы, методы, технологии: материалы конференции (12–13 февраля 2025 г.) / Воронежский государственный университет. – Воронеж: Издательско-полиграфический центр Воронежского государственного университета, 2025. – С. 1177–1184.
3. Методический подход к энергетическому расчету пространственно-распределённой системы сложения мощностей когерентных источников оптического диапазона длин волн // Радиолокация, навигация, связь: сборник трудов XXXI Международной научно-технической конференции (г. Воронеж, 15–17 апреля 2025 г.): в 6 т. / Воронежский государственный университет; АО «Концерн Созвездие». – Воронеж: Издательский дом ВГУ, 2025. – Т. 3. – С. 8–15. Козирацкий А.Ю., Чёнгин А.В., Смынтына О.В.
4. Патент на изобретение РФ № 2791818, Способ обнаружения вибрирующих объектов, основанный на анализе интерференционной картины, получаемой с использованием лазерных локационных станций гетеродинного типа / Дрынкин Д. А., Смынтына О. В., Петухов А. Г. (RU); опубл. 07.03.2023, Бюл. № 3. – М.: ФИПС, 2023.
5. Дрынкин Д. А. Предложение по использованию лазерной локационной станции гомодинного типа при селекции вибрирующих объектов / Козирацкий А. Ю., Петухов А. Г. // Материалы Междун. науч.-техн. конф. «Радиолокация, навигация, связь». – Воронеж: АО «Концерн «Созвездие», 2023. – С. 209–216.
6. Алгоритм работы лазерной локационной станции гомодинного типа при селекции вибрирующих объектов / Козирацкий А. Ю., Смынтына О. В. // Материалы Междун. науч.-практ. конф. «Современное состояние и перспективы развития систем связи и РТО в управлении авиацией. Научные чтения им А. С. Попова. – Воронеж: ВУНЦ ВВС «ВВА», 2023. – С. 54–58.

7. Дрынкин Д. А. Формирование вибрационного портрета // Свидетельство о государственной регистрации программы для ЭВМ RU № 2022680198, 28.10.2022. Заявка от 24.10.2022.
8. Дрынкин Д. А. Программа расчета вибрационных характеристик лоцируемых объектов // Свидетельство о государственной регистрации программы для ЭВМ RU № 2022685469, 23.12.2022. Заявка от 12.12.2022.
9. Дрынкин Д. А. Программа оценки амплитуды биений сигнала на выходе элемента матричного фотоприемного устройства // Свидетельство о государственной регистрации программы для ЭВМ RU № 2024616090, 15.03.2024. Заявка от 01.03.2024.
10. Дрынкин Д. А. Программа оценки частоты биений сигнала на выходе элемента матричного фотоприемного устройства // Свидетельство о государственной регистрации программы для ЭВМ RU № 2024615704, 12.03.2024. Заявка от 01.03.2024.
11. Дрынкин Д. А. Программа синтеза вибрационного изображения на основе оценок амплитуд и частот биений сигналов с элементов матричного фотоприемного устройства // Свидетельство о государственной регистрации программы для ЭВМ RU № 2024615946, 14.03.2024. Заявка от 01.03.2024.

ALGORITHMS FOR SIGNAL PROCESSING DURING AIRCRAFT LASER DETECTION

Koziratsky A. Y.⁴, Chengin A. V.⁵, Grevtsev A. I.⁶

Keywords: laser LAN, heterodyne, maximum likelihood, amplitude estimation, frequency estimation, quadcopter, detection.

Abstract

The aim of the work is to develop algorithms for detecting and estimating the parameters of the reflected signal from the rotating propellers of a small-class unmanned aerial vehicle when sounding with a heterodyne-type laser radar station.

Research method: maximum likelihood method.

Results: algorithms for detecting and estimating the parameters of the signal reflected from rotating propellers when sounding a small-class unmanned aerial vehicle by a heterodyne-type laser radar station have been developed. The process of generating estimates is multiiterative due to tuning the local oscillator phase front. Estimates are generated throughout the phase front tuning and are stored in a buffer device. The most plausible estimate is the one with a larger amplitude. Algorithms allow to obtain initial data from input implementations for the method of generating identification by the laser reconnaissance subsystem of small-class unmanned aerial vehicles by a laser radar station heterodyne type. The proposed algorithms make it possible to optimally assess the amplitude and frequency of beats at the output of the photodetector, taking into account the tuning of the local oscillator phase front, as well as to determine the statistical characteristics of the estimates obtained, which in turn makes it possible to form requirements for the parameters of the airspace reconnaissance subsystem based on the use of a heterodyne-type laser radar station.

Scientific novelty: the algorithms for detecting and evaluating the parameters of input signals necessary for the identification of small-class unmanned aerial vehicles in the airspace by the laser reconnaissance subsystem differ from those known by the introduction of an additional procedure for tuning the local oscillator phase front.

References

1. Patent na izobretenie RF № 2857752, Sposob prostranstvennogo slozheniya ehlektromagnitnyh izluchenij kogerentnyh istochnikov / Chyongin A. V., Kozirackij A. Yu., Smyntyna O. V., Grevtsev A. I., Kusakin O. V., Kapitanov V. V. (RU); opubl. 06.03.2026, Byul. No 7. – M.: FIPS, 2026.
2. Kozirackij A. Yu., Chyongin A. V. Sposob prostranstvennogo slozheniya ehlektromagnitnyh izluchenij kogerentnyh istochnikov // XXV Mezhdunarodnaya NPK: Informatika: problemy, metody, tehnologii: materialy konferencii (12–13 fevralya 2025 g.) / Voronezhskij gosudarstvennyj universitet. – Voronezh: Izdatel'sko-poligraficheskij centr Voronezhskogo gosudarstvennogo universiteta, 2025. – Pp. 1177–1184.
3. Metodicheskij podhod k ehnergeticheskomu raschetu prostranstvenno-raspredelennoj sistemy slozheniya moshchnostej kogerentnyh istochnikov opticheskogo diapazona dlin voln // Radiolokaciya, navigaciya, svyaz': sbornik trudov XXXI Mezhdunarodnoj nauchno-tehnicheskoy konferencii (g. Voronezh, 15–17 aprelya 2025 g.): v 6 t. – Voronezhskij gosudarstvennyj universitet; AO «Koncern Sozvezdie». – Voronezh : Izdatel'skij dom VGU, 2025. – T. 3. – Pp. 8–15. Kozirackij A. Yu., Chyongin A. V., Smyntyna O. V.

⁴ **Alexander Yu. Koziratsky**, Dr.Sc. of Technical Sciences, Professor, Professor of the Department of Radio Engineering and Antenna-Feeder Devices of the Military Training and Research Center of the Air Force Academy named after Professor N. E. Zhukovsky and Yu. A. Gagarin. Voronezh, Russia. E-mail: sashfish@bk.ru

⁵ **Alexander V. Chengin**, Adjunct of the Military Training and Research Center of the Air Force Academy named after Professor N. E. Zhukovsky and Yu. A. Gagarin. Voronezh, Russia. E-mail: alexsvist168@mail.ru

⁶ **Alexander I. Grevtsev**, Ph.D. of Technical Sciences, Associate Professor, Deputy Head of the Department of Radio Engineering and Antenna-Feeder Devices of the Military Training and Research Center of the Air Force Academy named after Professor N. E. Zhukovsky and Yu. A. Gagarin. Voronezh, Russia. E-mail: grevtsev.sanche@yandex.ru

4. Patent na izobretenie RF № 2791818, Sposob obnaruzheniya vibriruyushchih ob'ektov, osnovannyj na analize interferencionnoj kartiny, poluchaemoj s ispol'zovaniem lazernyh lokacionnyh stancij geterodinnogo tipa / Drynkin D. A., Smyntyna O. V., Petuhov A. G. (RU); opubl. 07.03.2023, Byul. No 3. – M.: FIPS, 2023.
5. Drynkin D. A. Predlozhenie po ispol'zovaniyu lazernoj lokacionnoj stancii gomodinno tipa pri selekcii vibriruyushchih ob'ektov / Kozirackij A. Yu., Petuhov A. G. // Materialy Mezhdun. nauch.-tehn. konf. «Radiolokaciya, navigaciya, svyaz'». – Voronezh: AO «Koncern «Sozvezdie», 2023. – Pp. 209–216.
6. Algoritm raboty lazernoj lokacionnoj stancii gomodinno tipa pri selekcii vibriruyushchih ob'ektov / Kozirackij A. Yu., Smyntyna O. V. // Materialy Mezhdun. nauch.-prakt. konf. «Sovremennoe sostoyanie i perspektivy razvitiya sistem svyazi i RTO v upravlenii aviatsii. Nauchnye chteniya im. A. S. Popova. – Voronezh: VUNC VVS «VVA», 2023. – Pp. 54–58.
7. Drynkin D. A. Formirovanie vibracionnogo portreta // Svidetel'stvo o gosudarstvennoj registracii programmy dlya EHVM RU № 2022680198, 28.10.2022. Zayavka ot 24.10.2022.
8. Drynkin D. A. Programma rascheta vibracionnyh harakteristik lociruemyh ob'ektov // Svidetel'stvo o gosudarstvennoj registracii programmy dlya EHVM RU № 2022685469, 23.12.2022. Zayavka ot 12.12.2022
9. Drynkin D. A. Programma ocenki amplitudy bienij signala na vyhode ehlementa matrichnogo fotopriemnogo ustrojstva // Svidetel'stvo o gosudarstvennoj registracii programmy dlya EHVM RU № 2024616090, 15.03.2024. Zayavka ot 01.03.2024.
10. Drynkin D. A. Programma ocenki chastoty bienij signala na vyhode ehlementa matrichnogo fotopriemnogo ustrojstva // Svidetel'stvo o gosudarstvennoj registracii programmy dlya EHVM RU № 2024615704, 12.03.2024. Zayavka ot 01.03.2024.
11. Drynkin D. A. Programma sinteza vibracionnogo izobrazheniya na osnove ocenok amplitud i chastot bienij signalov s ehlementov matrichnogo fotopriemnogo ustrojstva // Svidetel'stvo o gosudarstvennoj registracii programmy dlya EHVM RU № 2024615946, 14.03.2024. Zayavka ot 01.03.2024.



ВОЗМОЖНОСТИ И ПЕРСПЕКТИВЫ ПРИМЕНЕНИЯ ТЕХНОЛОГИЙ РОЕВОГО ИНТЕЛЛЕКТА В СИСТЕМАХ СВЯЗИ ВОЕННОГО НАЗНАЧЕНИЯ

Яговитов Д. С.¹, Вдовченко Н. Ю.²

DOI:10.21681/3034-4050-2026-3-57-63

Ключевые слова: искусственный интеллект, децентрализованное управление, оптимизация, искусственные спутники Земли, центр обработки данных.

Аннотация

Цель исследования: состоит в определении возможностей применения технологий роевого интеллекта в процессах функционирования систем связи военного назначения и формулировании выводов о перспективах проведения дальнейших исследований в этом направлении.

Метод исследования: теоретический (синтез, индукция).

Результат: концепция роевого интеллекта реализуема в комплексах связи и автоматизации управления связью систем связи военного назначения, а также теоретически обоснована для проработки вопросов перспективного развития существующих автоматизированных систем управления, из чего можно заключить, что направление исследований применения роевого интеллекта в интересах обеспечения надежного (устойчивого, помехоустойчивого), доступного, управляемого и безопасного функционирования систем связи военного назначения является актуальным.

Практическая ценность: полученные знания о технологиях роевого интеллекта могут быть использованы при постановке тактико-технических заданий на перспективные образцы вооружения, военной и специальной техники по линии ответственности Главного управления связи Вооруженных сил Российской Федерации.

Введение

Роевой интеллект – это раздел искусственного интеллекта, изучающий коллективное поведение децентрализованных самоорганизующихся систем³. Название происходит из аналогии наблюдения за поведением насекомых (муравьями, пчелами, термитами, рыбами), которые, будучи простыми особями, совместно решают сложные задачи (поиск кратчайшего пути к еде, выбор места основания нового гнезда) без участия в принятии решений единого центра управления [1].

Под технологиями роевого интеллекта (ТРИ), соответственно, можно понимать комплекс технологических решений, направленных на создание информационных систем, в функционирование которых заложены принципы роевого интеллекта.

К основным принципам функционирования ТРИ относятся:

- 1) **децентрализация** – отсутствие единого центра принятия решений, таким образом, любой агент (узел) может выйти из строя без угрозы отказа в функционировании всей колонии (роя);
- 2) **автономность** – каждый агент роя функционирует самостоятельно, но в составе группы (роя);
- 3) **стигмергия** – взаимодействие агентов происходит через изменение состояния окружающей среды и получения от неё реакционного действия (например, муравьи оставляют феромонные следы);
- 4) **простота правил** – стратегия сложного глобального поведения колонии (роя) является следствием реализации простых действий, заложенных в функционирование каждого агента.

Концептуальная схема одной из возможных реализаций ТРИ, построенной на принципах

¹ Яговитов Данила Сергеевич, кандидат технических наук, начальник лаборатории ФГБУ «16 ЦНИИИ» Минобороны России. Мытищи, Россия. E-mail: daniila.yagovitov@mail.ru

² Вдовченко Наталья Юрьевна, младший научный сотрудник ФГБУ «16 ЦНИИИ» Минобороны России. Мытищи, Россия. E-mail: natashok120391@mail.ru

³ Впервые в нашей стране коллективным поведением занимался Варшавский В. И. (Варшавский В. И. Коллективное поведение автоматов. М.: Наука, 1973. 408 с. ISBN 978-5-0000-0000-0). Были и его более ранние публикации на эту тему, однако в моей памяти они не сохранились, хотя я и был с ним дружен вплоть до его отъезда из страны.

Виктор Ильич Варшавский опередил свое время, и должного внимания эти исследования не получили. В годы перестройки научные исследования в России практически не финансировались, и он вместе со своими сотрудниками и семьей переехал в 1993 г. в Японию по приглашению японской стороны и работал до 2000 г. в Университете Айдзу, Айдзу-Вакамацу – профессор, заведующий лабораторией проектирования компьютерной логики, а с 2002–2003 гг. в компании «Технологии нейронных сетей», Бней-Брак, Израиль (заведующий отделом логического управления). Умер в Израиле 3 января 2005 г. (прим. редактора).

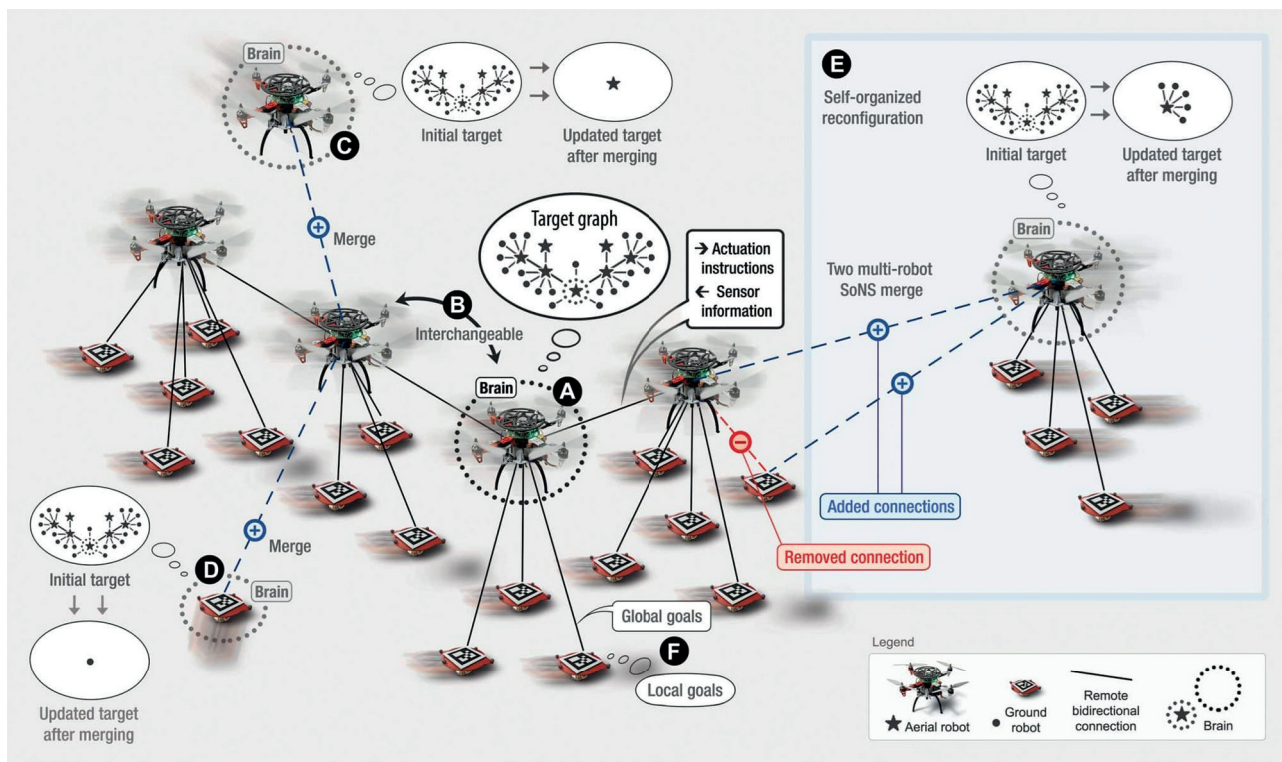


Рис. 1. Схема самоорганизующейся нервной системы

архитектуры нервной системы человека – самоорганизующаяся нервная система – приведена на рисунке 1⁴.

Постановка задачи

Задача исследования состоит в том, чтобы на основе анализа основных направлений применения ТРИ в системах связи (СС) гражданского и (если это осуществимо) военного назначений (ВН) определить степень возможности их практической реализации в последних и на основе полученных знаний сформулировать выводы о перспективности проведения дальнейших исследований в направлении реализации ТРИ в комплексах связи и автоматизации (КСА) ВН.

Направления применения ТРИ в системах связи гражданского и военного назначений

В КСА гражданского и военного назначений ТРИ применимы для решения задач управления, где централизованные алгоритмы обладают низкой скоростью сходимости, потребляют большое количество вычислительных ресурсов или уязвимы для компьютерных атак противника.

К основным направлениям применения ТРИ для решения указанных задач можно отнести следующие варианты использования.

⁴ Ученые построили роевой интеллект на принципах архитектуры нервной системы человека. – URL: <https://naked-science.ru/article/hi-tech/roevoy-intellekt> (дата обращения: 24.03.2026)

1. Динамическая маршрутизация в распределенных пакетных сетях (NGN⁵, MANET⁶, IoT⁷)

В основе функционирования алгоритмов традиционных протоколов маршрутизации в пакетных сетях заложены механизмы рассылки информации о доступных маршрутах (векторов расстояний в протоколе BGP⁸) или проверки состояния линии связи между соседними сетевыми устройствами (технология link-state в протоколе OSPF⁹), что в условиях динамично меняющейся обстановки по связи в территориально и/или иерархически распределенных сетях создает дополнительные накладные расходы пропускной способности каналов связи. Для нивелирования указанных недостатков классических подходов к управлению трафиком может использоваться оптимизация на основе муравьиной колонии

⁵ NGN (англ. Next Generation Networks), сети следующего/нового поколения – мультисервисные сети связи, ядром которых являются опорные IP-сети, поддерживающие полную или частичную интеграцию услуг передачи речи, данных и мультимедиа. Реализуют принцип конвергенции услуг электросвязи.

⁶ MANET (англ. Mobile Ad hoc Network) – беспроводные децентрализованные самоорганизующиеся сети, состоящие из мобильных устройств, способных устанавливать соединения между произвольными узлами. Каждое такое устройство может независимо передвигаться в любых направлениях, и, как следствие, часто разрывать и устанавливать соединения с соседями.

⁷ IoT (англ. Internet of Things) – концепция сети передачи данных между физическими объектами («вещами»), оснащёнными встроенными средствами и технологиями для взаимодействия друг с другом или с внешней средой.

⁸ BGP (англ. Border Gateway Protocol) – протокол динамической маршрутизации граничного (внешнего) шлюза (англ. Exterior Gateway Protocol, EGP) между несколькими автономными системами.

⁹ OSPF (англ. Open Shortest Path First) – протокол динамической маршрутизации внутреннего шлюза (англ. Interior Gateway Protocol, IGP), использующий для нахождения кратчайшего пути алгоритм Дейкстры внутри одной автономной системы.

(англ. Ant Colony Optimization, ACO): искусственные агенты-муравьи (зонды-пакеты) блуждают по сети; достигая адресата, они возвращаются к источнику, откладывая виртуальный «феромон» вдоль пройденного пути [2].

Так, на рисунке 2 (1) показано, как первый муравей находит источник пищи (F) любым способом (а), а затем возвращается к гнезду (N), оставив за собой тропу из «феромонов» (b). Затем муравьи выбирают один из четырёх возможных путей, затем укрепляют его следом из «феромонов» и делают «привлекательным» для других особей (рис. 2 (2)). Наконец, муравьи выбирают кратчайший маршрут, так как «феромоны», оставленные вдоль более длинных путей, быстрее исчезают (рис. 2 (3)).

Таким образом, чем лучше сетевые показатели качества отобранного агентами-муравьями маршрута от источника к получателю, тем больше «феромона» вдоль него накапливается. И напротив, если показатели качества маршрута ухудшаются с течением времени (растут задержки прохождения пакетов, деградирует пропускная способность или повышается степень её утилизации), «феромон» испаряется (удаляется), и агенты-муравьи начинают поиск новых, оптимальных с точки зрения обеспечения сетевых показателей качества маршрута. В итоге сеть становится т.н. «самоисцеляющейся» (англ. self-healing) и адаптивной к перегрузкам в автоматическом режиме.

Указанный подход реализован в программно-техническом комплексе (ПТК) управления и обеспечения информационной безопасности транспортной сети ВН, опытный образец которого получен в ходе одной из опытно-конструкторских работ (ОКР) по линии ответственности

Главного управления связи Вооруженных сил Российской Федерации, для решения задачи оптимальной прокладки оптических кабельных линий связи.

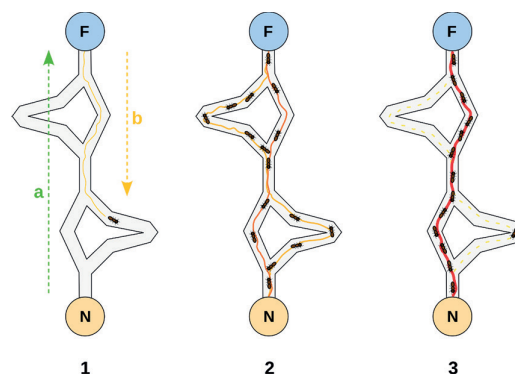


Рис. 2. Иллюстрация шагов оптимизации на основе муравьиной колонии

Эффект от реализации указанной ТРИ для СС ВН: повышение надежности (устойчивости) и пропускной способности.

2. Оптимизация ресурсов в радиосетях 5 и 6 поколений

Концепция открытой архитектуры сети радиодоступа (англ. Open Radio Access Network, O-RAN)¹⁰, предложенная консорциумом O-RAN Alliance¹¹, предполагает создание унифицированной сети радиодоступа 5G/6G со стандартизированными интерфейсами и протоколами взаимодействия между компонентами (рис. 3).

¹⁰ Open RAN (O-RAN) Reference Architecture. — <https://www.techplayon.com/open-ran-o-ran-reference-architecture/> (дата обращения 23.03.2026)

¹¹ Международная организация, основанная в 2018 г. с целью переосмысления архитектуры сетей радиодоступа и объединяющая операторов мобильной связи, производителей оборудования, технологические компании и научно-исследовательские институты.

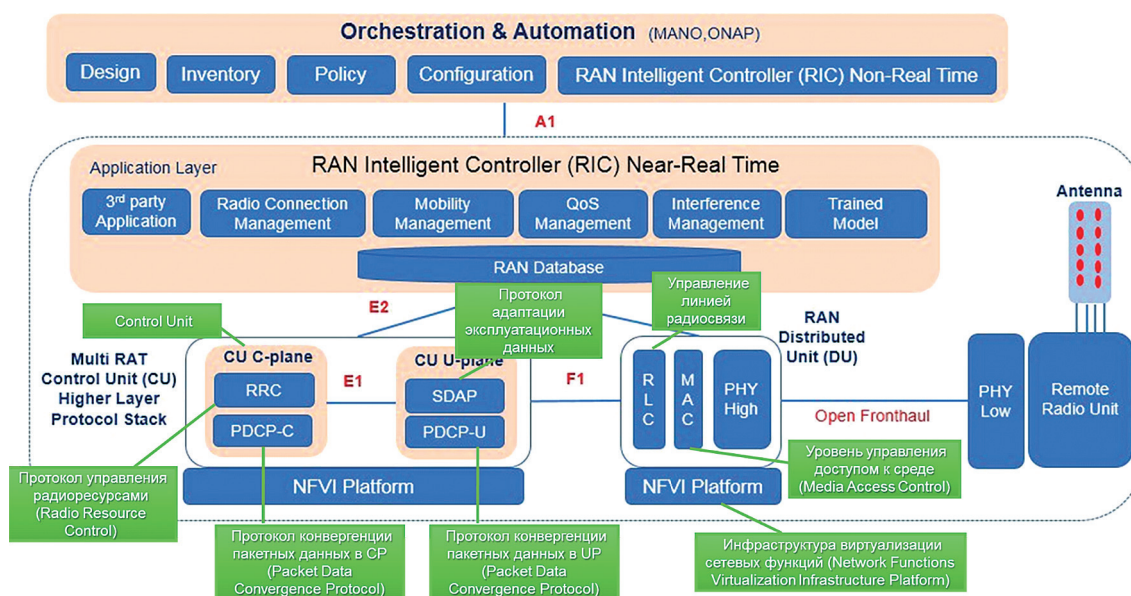


Рис. 3. Архитектура O-RAN

Такие преимущества от реализации концепции O-RAN, как наличие гибкости и масштабируемости развертывания и управления, свободы выбора оператором поставщиков компонентов ввиду стандартизации и унификации интерфейсов и протоколов наделяет оператора возможностью самостоятельного добавления новой специализированной функциональности в части управления сетями радиодоступа, в том числе на основе ТРИ.

Так, каждую базовую станцию (или её логический сегмент) возможно представить как агента. С использованием метода **оптимизации роя частиц** (англ. Particle Swarm Optimization, PSO) [3], моделирующего многоагентную систему, где агенты-частицы перемещаются в направлении оптимальных решений в пространстве поиска, обмениваясь при этом информацией с соседями (рис. 4), станции могут осуществлять согласованную настройку углов наклона антенно-мачтовых устройств, мощность излучения, частотно-территориальное планирование в целях минимизации помех друг для друга и максимизации области радиопокрытия.

Примечательно, что для функционирования PSO не требуется вычисления точного градиента оптимизируемой функции, которая, в свою очередь, может быть выражена нелинейно-многочленным уравнением.

Эффект от реализации указанной ТРИ для СС ВН: повышение надежности (устойчивости), пропускной способности и доступности.

3. Управление лазерной межспутниковой связью в мегасозвездиях искусственных спутников Земли

Такие проекты западных компаний, как Starlink и OneWeb, представляют собой классический

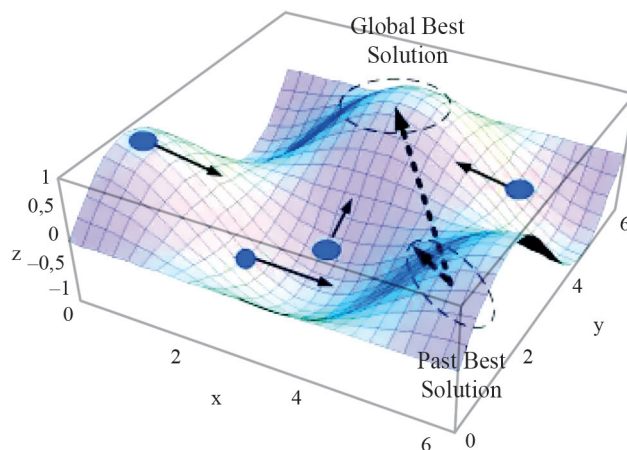


Рис. 4. Фрагмент процесса поиска глобального максимума (global best solution) с использованием оптимизации роя частиц

«рой» из тысяч аппаратов – искусственных спутников Земли (ИСЗ) – на низкой околоземной орбите (НОО) (рис. 5)¹².

Используя принципы ТРИ, ИСЗ способны в автоматическом режиме сформировать динамическую mesh-сеть¹³ на НОО, выбирая оптимальные направления установления лазерной межспутниковой связи, например, обходя при родные атмосферные помехи, зоны функционирования станций радиоэлектронного подавления противника или исключая из информационного обмена ИСЗ, уходящие в тень Земли. Результатом такой автоматизации является обеспечение глобального покрытия ареала

¹² Моделирование возможностей связи комплекса Starlink. – URL: <https://habr.com/ru/companies/ruvds/articles/704580/?code=8e75be7e21976ca697a3f3bc63a66c0e&state=te1W5HD3UjJ5KHXMGL7uZd&hl=en> (дата обращения: 24.03.2026)

¹³ Сетевая топология компьютерной сети, построенная на принципе ячеек, в которой рабочие станции сети соединяются друг с другом и способны принимать на себя роль коммутатора для остальных участников.

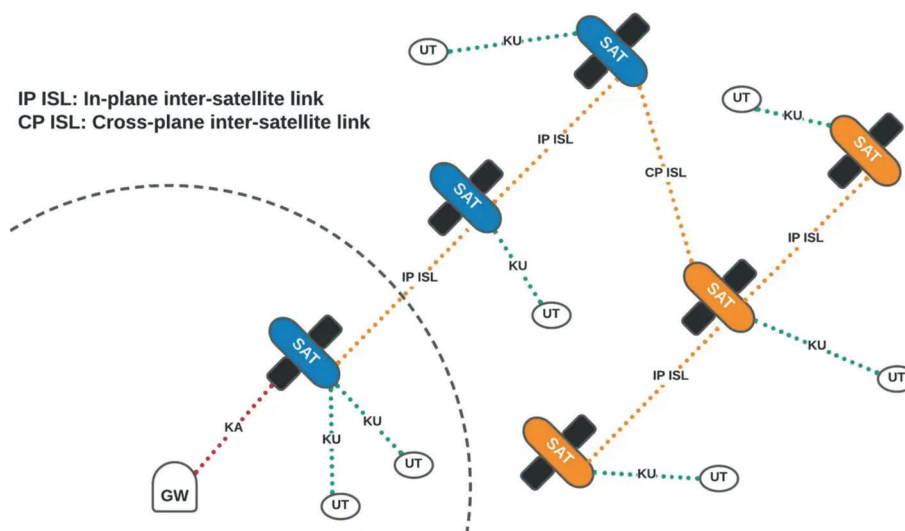


Рис. 5. Схема организации внутриорбитальной (IP ISL) и межорбитальной (CP ISL) лазерной межспутниковой связи группировки ИСЗ Starlink

потребителей инфокоммуникационных услуг с требуемым (заданным) качеством.

Эффект от реализации указанных ТРИ для СС ВН: повышение пропускной способности, надежности (устойчивости) и доступности.

4. Обеспечение безопасности передачи данных в сетях связи

Небольшие программные зонды-агенты (сетевые «пауки») с заданной периодичностью могут осуществлять сканирование сети передачи данных на предмет обнаружения аномальной обстановки по связи. Если один агент обнаруживает аномалию, например, DDoS-атаку¹⁴ или распространение вредоносного программного обеспечения, он меняет свое поведение («метит» среду). Другие агенты, проходя мимо (сканируя те же области сети), «видят» эту метку и начинают локально активировать защитные меры, изолируя зараженный сегмент сети и не дожидаясь команды от администратора.

Эффект от реализации указанных ТРИ для СС ВН: повышение надежности (помехоустойчивости).

5. Управление нагрузкой в центрах обработки данных

В крупных центрах обработки данных (ЦОД), в том числе военного назначения, оператору требуется динамически перемещать виртуальные машины, контейнеры и потоки данных между серверами, решая в каждый момент времени оптимизационную задачу о распределении вычислительных мощностей между границей сети и ядром (облаком). ТРИ позволяют виртуальным агентам находить наименее загруженные сетевые устройства, перемещая вычислительную

нагрузку ближе к потребителю инфокоммуникационных услуг (принцип edge computing) в реальном времени, снижая тем самым энергопотребление ЦОД в целом.

Эффект от реализации указанных ТРИ для СС ВН: повышение надежности (устойчивости) и доступности.

6. Управление нагрузкой в транспортных сетях связи

В ядре транспортных сетей связи применим подход к мультиагентному управлению обслуживаемой сетью нагрузки, когда совокупность управляющих сущностей – интеллектуальных агентов – размещенных в подсистеме автоматизированного управления связью, сканируя сеть в «узких» местах и используя механизмы обучения с подкреплением¹⁵ (рис. 6 [4]), в автоматическом режиме и масштабе времени, близком к реальному, вырабатывают единую оптимальную стратегию по определению маршрутов прохождения трафика и выделения для этого пропускной способности каналов связи. Критерием же указанной оптимизации является обеспечение требуемого (заданного) качества инфокоммуникационных(-ой) услуг(-и).

Концепция ТРИ в части мультиагентного подхода в совокупности с механизмами обучения с подкреплением может быть предложена в тактико-техническом задании на доработку (модернизацию) программно-аппаратного комплекса автоматизированной системы управления (АСУ) СС ВН.

Эффект от реализации указанных ТРИ для СС ВН: повышение пропускной способности, надежности (устойчивости) и управляемости.

¹⁴ DDoS (англ. distributed denial-of-service attack), распределенная атака типа «отказ в обслуживании» – атака на вычислительную систему в целях её отказа, т. е. создания таких условий, при которых авторизованные пользователи системы не смогут получить доступ к предоставляемым системным ресурсам (услугам), либо этот доступ будет затруднён.

¹⁵ Англ. Reinforcement Learning, RL – это метод машинного обучения, в котором агент (обучаемая система) учится принимать оптимальные решения через взаимодействие со средой. В отличие от классического обучения с учителем, где модель обучается на готовых примерах, RL осуществляется по принципу совершения агентом проб и ошибок.



Рис. 6. Схема взаимодействия агента и окружения в парадигме обучения с подкреплением

Заключение

Концептуально реализация ТРИ представляет собой переход от централизованного управления связью с единым центром принятия решений на управление к децентрализованному, когда в сети функционирует множество интеллектуальных «агентов», каждый в своей зоне ответственности принимает локальное решение и транслирует его другим участникам процесса управления. Таким образом, формируется распределенная когнитивная сеть, что является особенно актуальным в условиях развития сетей 6 поколения, где предполагается, что сеть будет представлять собой не простую совокупность сетевых устройств, объединенных каналами связи различной природы, а «сенсорным организмом»,

состоящим из миллионов автономных устройств (виртуальных или реальных датчиков), которые обладают способностью автоматической самоорганизации из-за наличия физической невозможности обработать большой объем управляющих сигналов централизованно.

Концепция ТРИ реализуема в КСА СС ВН: некоторые метаэвристики уже применяются в опытных образцах ПТК, а также теоретически обоснована [4] для проработки вопросов перспективного развития существующих АСУ, из чего можно заключить, что направление исследований применения ТРИ в интересах обеспечения надежного (устойчивого, помехоустойчивого), доступного, управляемого и безопасного функционирования СС ВН является актуальным.

Литература

1. Старков И. А. Методы роевого интеллекта / И. А. Старков // Наука молодых: сборник статей Межрегиональной молодежной научной конференции, посвященной памяти Ф. А. Бабушкина, Сыктывкар, 29–30 мая 2025 г. – Сыктывкар: Сыктывкарский государственный университет им. Питирима Сорокина, 2025. – С. 9–12. – EDN EPIXIH.
2. A. Coloni, M. Dorigo et V. Maniezzo Distributed Optimization by Ant Colonies, actes de la première conférence européenne sur la vie artificielle, Paris, France, Elsevier Publishing, 1991. – Pp. 134–142.
3. Kennedy J., Eberhart R. (1995). Particle Swarm Optimization. Proceedings of IEEE International Conference on Neural Networks, 1995. – Vol. IV. – Pp. 1942–1948.
4. Применение модели марковского процесса принятия решений с целью обеспечения своевременности обслуживания мультисервисного трафика в домене программно-конфигурируемой инфокоммуникационной сети специального назначения / Д. С. Яговитов, М. И. Рафальская, Д. А. Несвит, И. В. Образцов // Современное состояние и перспективы развития инфокоммуникационных сетей связи специального назначения: Сборник материалов научно-практической конференции, Санкт-Петербург, 23 марта 2023 г. – СПб: Федеральное государственное казенное военное образовательное учреждение высшего образования «Военная академия связи им. маршала Советского Союза С. М. Буденного» Министерства обороны Российской Федерации, 2023. – С. 137–144. – EDN JESIAA.

OPPORTUNITIES AND PROSPECTS FOR THE USE OF SWARM INTELLIGENCE TECHNOLOGIES IN MILITARY COMMUNICATION SYSTEMS

Yagovitev D. S.¹⁶, Vdovchenko N. Yu.¹⁷

Keywords: artificial intelligence, decentralized control, optimization, artificial Earth satellites, data processing center.

Abstract

The purpose of the research is to determine the possibilities of using swarm intelligence technologies in the processes of functioning of military communication systems and to formulate conclusions about the prospects for further research in this direction.

Research method: theoretical (synthesis, induction).

Result: the concept of swarm intelligence is implemented in communication and automation of communication control systems for military purposes, and is also theoretically substantiated for the study of the issues of the future development of existing automated control systems, from which it can be concluded that the direction of research on the use of swarm intelligence in the interests of ensuring reliable (stable, noise-resistant), accessible, controllable and safe operation of military communication systems is relevant.

¹⁶ **Danila S. Yagovitev**, Ph.D. of Technical Sciences, Head of the Laboratory of the 16th Central Research Institute of the Ministry of Defense of the Russian Federation. Mytishchi, Russia. E-mail: danila.yagovitev@mail.ru

¹⁷ **Natalia Yu. Vdovchenko**, Junior Researcher, 16th Central Research Institute of the Ministry of Defense of the Russian Federation. Mytishchi, Russia. E-mail: natashok120391@mail.ru

Practical value: the knowledge gained about swarm intelligence technologies can be used in setting tactical and technical tasks for promising models of weapons, military and special equipment under the responsibility of the Main Communications Directorate of the Armed Forces of the Russian Federation.

References

1. Starkov I. A. Metody roevogo intellekta / I. A. Starkov // Nauka molodyh: sbornik statej Mezhhregional'noj molodezhnoj nauchnoj konferencii, posvyashchennoj pamyati F. A. Babushkina, Syktyvkar, 29–30 maya 2025 goda. – Syktyvkar: Syktyvkarskij gosudarstvennyj universitet im. Pitirima Sorokina, 2025. – S. 9–12. – EDN EPIXIH.
2. A. Coloni, M. Dorigo et V. Maniezzo Distributed Optimization by Ant Colonies, actes de la première conférence européenne sur la vie artificielle, Paris, France, Elsevier Publishing, 1991. Pp. 134–142.
3. Kennedy J., Eberhart R. Particle Swarm Optimization. Proceedings of IEEE International Conference on Neural Networks, 1995. – Vol. IV. – Pp. 1942–1948.
4. Primenenie modeli markovskogo processa prinyatiya reshenij s cel'yu obespecheniya svoevremennosti obsluzhivaniya mul'tiservisnogo trafika v domene programmno-konfiguriruemoj infokommunikacionnoj seti special'nogo naznacheniya / D. S. Yagovitev, M. I. Rafal'skaya, D. A. Nesvit, I. V. Obrazcov // Sovremennoe sostoyanie i perspektivy razvitiya infokommunikacionnyh setej svyazi special'nogo naznacheniya: Sbornik materialov nauchno-prakticheskoy konferencii, Sankt-Peterburg, 23 marta 2023 g. – SPb: Federal'noe gosudarstvennoe kazennoe voennoe obrazovatel'noe uchrezhdenie vysshego obrazovaniya «Voennaya akademiya svyazi im. marshala Sovetskogo Soyuza S. M. Budennogo» Ministerstva oborony Rossijskoj Federacii, 2023. – S. 137–144. – EDN JESIAA.



АРХИТЕКТУРА СЕТИ ОТКРЫТОЙ АВТОМАТИЧЕСКОЙ ТЕЛЕФОННОЙ СВЯЗИ, ПОСТРОЕННОЙ С ПРИМЕНЕНИЕМ ПИРИНГОВЫХ ТЕХНОЛОГИЙ, И ПРЕДЛОЖЕНИЯ ПО ЕЕ ЗАЩИТЕ

Ашлапов М. В.¹, Елисеев Д. И.²

DOI:10.21681/3034-4050-2026-3-64-68

Ключевые слова: телефонная связь, услуги телефонии, коммутация пакетов, кластер, аппаратные шлюзы, безопасность телефонной связи, аудиоконференц-связь.

Аннотация

Цель работы: анализ архитектуры пиринговой сети открытой автоматической телефонной связи и предложений по обеспечению защиты речевого и сигнального трафика.

Метод исследования: системный подход применен для анализа архитектуры сети пиринговой автоматической телефонной связи, на основе которого разработаны предложения по защите речевого и сигнального трафика в сети открытой телефонной связи.

Результаты исследования: рекомендуется применять аппаратно-программные средства обеспечения безопасности открытой телефонной связи.

Научная новизна: определяется глубиной обоснования применения пиринговых технологий для построения сетей открытой телефонной связи и рассмотрения особенностей обеспечения безопасности передачи речевого и сигнального трафика в такой сети.

Введение

В современных условиях ведения боевых действий ключевое значение приобретает обеспечение своевременного и достоверного информационного обмена между должностными лицами на всех уровнях управления. Учитывая, что по-прежнему основой их информационного взаимодействия остается телефонная связь, решение вопросов доведения услуг телефонии непосредственно до линии боевого соприкосновения войск становится крайне важным [1, 2].

Одним из наиболее актуальных направлений совершенствования сети передачи данных в тактическом звене управления является развертывание на полевых пунктах управления сети открытой автоматической телефонной связи с использованием автоматических телефонных станций (далее – АТС) с поддержкой пиринговой технологии – АТС «Пирс» (рис. 1).

АТС «Пирс» обладает возможностью обеспечить услугами телефонной связи до 1000 IP-абонентов по протоколу сети с коммутацией пакетов SIP, а также 8 аналоговых абонентов. Кроме того, станция предоставляет большое количество дополнительных видов обслуживания, к которым относятся аудиоконференцсвязь,



Рис. 1. Внешний вид АТС «Пирс»

речевое оповещение, голосовой информатор, переадресация и другие.

Архитектура пиринговой сети открытой телефонной связи. Понятие кластера

В пиринговой архитектуре отсутствует выделенный центральный сервер, вместо этого каждый узел сети – будь то IP-телефон, программный клиент или шлюз – обладает достаточным уровнем интеллекта для самостоятельной маршрутизации вызовов [3]. Сигнальная информация передается по протоколу SIP, а медиапоток – по протоколу RTP, при этом обмен происходит непосредственно между узлами. Основными

¹ Ашлапов Михаил Владимирович, кандидат технических наук, доцент кафедры Военной академии связи. Санкт-Петербург, Россия. E-mail: mvashlapov@mail.ru

² Елисеев Дмитрий Иванович, кандидат технических наук, доцент, доцент кафедры Военной академии связи. Санкт-Петербург, Россия. E-mail: dimone73@mail.ru

преимуществами такой архитектуры являются высокая отказоустойчивость и масштабируемость. Поскольку нет центрального сервера, выход из строя одного из узлов не приводит к полному коллапсу всей телефонной сети. Добавление новых абонентов не требует увеличения мощностей центрального сервера, а прямая передача медиапотока минимизирует задержки и джиттер, что критически важно для поддержания качества обслуживания пользователей (QoS).

Ключевой особенностью архитектуры сети открытой телефонной связи, построенной с применением АТС «ПИРС», является возможность работы станций в кластере.

Кластер – понятие из области вычислительных сетей. В общем случае это группа серверов, объединенных высокоскоростными каналами связи и представляющих, с точки зрения пользователя, единый аппаратный ресурс³. Таким образом, кластер – это объединение не менее двух серверов на базе одинаковых процессоров под управлением одной операционной системы, имеющих общий доступ к носителям информации, используемым в кластере.

Работа вычислительных серверов в структуре кластера позволяет:

- скоординированно использовать общий ресурс серверов, входящих в кластер;
- осуществлять взаимный контроль работы серверов;
- осуществлять обмен данными о конфигурации серверов.
- кластер серверов отличается от обычной схемы резервирования:
- воспринимается пользователем как один сервер;
- управляется как единая система;
- обладает более высокой надежностью по сравнению с «клиент-серверной» архитектурой;
- имеет общую файловую систему.

Кластер АТС «ПИРС» представляет собой совокупность нескольких децентрализованных станций, развернутых в составе распределенной сети и пространственно разнесенных на значительной территории в зоне ответственности соединения (группировки, части). Для абонентов вся совокупность децентрализованных станций является единой АТС с точки зрения предоставляемых услуг связи, номерной емкости и аппаратного резервирования.

По принципам функционирования кластер АТС «ПИРС» во многом повторяет серверный кластер. Основу кластера составляет «пиринговая

сеть», технология которой основывается на модели «Peer-to-Peer» (англ. – «равный-к-равному»). Указанная архитектура в значительной степени отличается от общепринятой в настоящее время архитектуры информационного обмена «клиент-сервер», на которой построены классические системы телефонии и коммуникаций.

Peer-to-Peer (P2P) представляет собой модель обмена информацией, в которой подключенные к сети узлы (пиры) обеспечивают непосредственную связь друг с другом и взаимный обмен информационными ресурсами. Особенностью технологии является то, что в ее состав входят равноправные узлы пиринговой сети. Центральная управляющая АТС (центральный блок) в пиринговой сети отсутствует, а в качестве узлов выступают все устройства пиринговой АТС.

Преимуществами архитектуры пиринговой телефонной сети по сравнению с традиционными сетями «клиент-сервер» являются способность неограниченного расширения сети, не требующая затрат централизованных ресурсов, высокая производительность и отказоустойчивость при любом количестве и сочетании доступных узлов. АТС «ПИРС» одного или даже разных типов (с аналоговыми окончаниями FXS, FXO, цифровыми интерфейсами E1 и др.) могут объединяться по сети передачи данных, образуя единую архитектуру пиринговых АТС с единым номерным планом, функциональностью дополнительных видов обслуживания (сервисами) и с общими физическими интерфейсами и каналами связи [1].

На сетевом уровне основную роль в организации автоматической телефонной связи посредством IP-сети играют маршрутизаторы, определяющие пути доставки данных до станций в составе кластера и до пользователей с определенным IP-адресом. Каждая пиринговая АТС имеет интерфейс Ethernet, посредством которого осуществляется подключение к транспортной сети связи, поиск других пиринговых АТС по IP-адресам, авторизация по специальному протоколу и логическое объединение с образованием кластера. Указанный алгоритм обеспечивает объединение в единую сеть ресурсов всех подключаемых устройств.

Пиринговая АТС «ПИРС» работает с различными оконечными устройствами. Это могут быть аналоговые телефонные аппараты и SIP-телефоны, некоторые из которых («Спектр-О», «Fanvil», Kirisun DH200 и др.) имеют встроенные профили автоматических настроек в системе.

Отличительными особенностями архитектуры телефонного кластера, построенного на основе АТС «Пирс», являются высокая отказоустойчивость и возможность информационного обмена в открытом сегменте сети передачи данных

3 АО «Линтех». Пиринговая система унифицированных коммуникаций Symway: официальная документация / АО «Линтех». – М., 2024. – Режим доступа: <https://www.symway.com>

Минобороны России, в том числе принимающим участие в специальной военной операции (так, по состоянию на 2025 год в группировках войск применялись более 1500 станций).

Вариант архитектуры сети открытой телефонной связи, построенной по принципу комплексного взаимодействия АТС «ПИРС», в составе распределенного кластера с классическими SIP серверами показан на рисунке 2.

Кроме АТС «ПИРС» в составе сети могут использоваться практически любые коммутаторы малой емкости, например, АТС П-380К из состава комплекса «Поле». По своей сути, АТС «ПИРС» будет являться шлюзом для объединения различных автоматических и ручных телефонных станций и предоставления им ресурсов кластера.

Однако именно децентрализация порождает уникальный профиль угроз. В отличие от централизованной АТС, где безопасность можно обеспечить на периметре одного сервера, в пиринговой сети каждый узел потенциально является точкой входа для злоумышленника. Это усложняет задачу администрирования и повышает вероятность атаки на кластер. Ключевые угрозы включают:

1. Перехват сигнальной информации: SIP-сообщения, такие как INVITE, ACK и BYE, передаются в открытом виде без шифрования (SIPS), что позволяет злоумышленнику, имеющему доступ к сетевому сегменту, перехватывать информацию о номерах абонентов, времени звонков и общем статусе линий [4].
2. Подмена абонента (Spoofing): отсутствие строгой взаимной аутентификации узлов позволяет злоумышленнику зарегистрироваться

в сети под видом легитимного абонента и инициировать вызовы от его имени, что может привести к разглашению конфиденциальной информации.

3. Атаки на доступность (DoS/DDoS): узлы пиринговой сети часто функционируют на обычных рабочих станциях или серверах, которые имеют меньше вычислительных ресурсов по сравнению со специализированными серверами программных АТС. Целенаправленная атака на конкретный узел способна вывести его из строя.
4. Уязвимости программного обеспечения: распределение функционала пиринговой АТС между множеством оконечных устройств делает процесс обновления программного обеспечения и применения инструментов безопасности сложной и трудоемкой задачей. Наличие уязвимости в клиентском ПО на одном узле может стать причиной компрометации всего сегмента сети [5].

Для нейтрализации этих угроз необходим комплексный подход, который включает обеспечение конфиденциальности и целостности как сигнального, так и медиа-трафика.

На сегодняшний день для обеспечения безопасности передаваемой информации в глобальных сетях общего пользования достаточно широко применяются технологии OpenVPN, для защиты каналов применяются технологии IPsec, аппаратные шлюзы и связка TLS+SRTP. Выбор решения определяется криптографическими алгоритмами, архитектурой сети, статусом сертификации и применимостью в инфраструктуре сетей связи специального назначения.

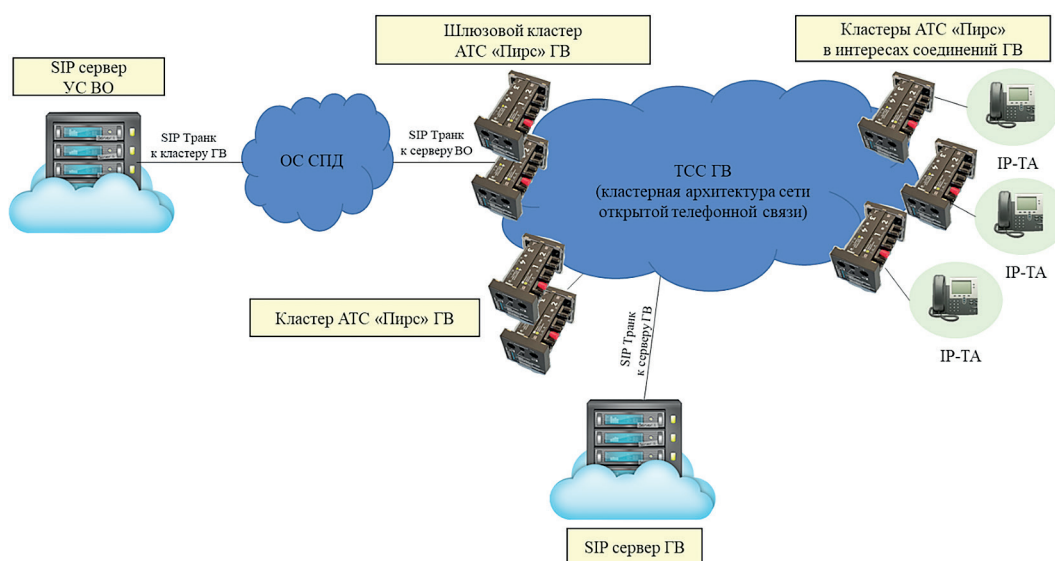


Рис. 2. Вариант архитектуры сети открытой телефонной связи ГВ

Криптографические механизмы и сертификация

OpenVPN – программное решение с открытым кодом, использующее библиотеку OpenSSL и протоколы TLS [6]. Оно поддерживает алгоритмы типа AES-256, но не имеет встроенной поддержки алгоритмов ГОСТ РФ и отдельных сертификатов ФСТЭК или ФСБ. Использование OpenVPN в сетях передачи данных специального назначения возможно только в составе сертифицированной конфигурации, что требует затрат на экспертизу.

IPsec, интегрированный на сетевом уровне ОС, шифрует заголовки пакетов, скрывая служебную информацию. Однако его применение в сетях передачи данных специального назначения требует сертификации всей системы, так как стандартные реализации не являются сертифицированными СКЗИ⁴.

В свою очередь АПКШ «Континент» является сертифицированным аппаратно-программным комплексом (имеет сертификаты ФСТЭК и ФСБ). Комплекс гарантирует использование алгоритмов ГОСТ РФ (например, ГОСТ Р 34.12-2015) и защищает от вторжений через публичные сети. Наличие сертификатов делает «Континент» приоритетным выбором для применения на сетях связи специального назначения, в которых передается информация с ограничительными пометками^{5,6}.

Архитектурные особенности и надежность

Архитектура OpenVPN (пользовательский уровень, UDP) обуславливает недостаток – неустойчивость туннелей. При разрыве соединения требуется повторное установление сеанса протокола TLS, что занимает время и приводит к обрыву сеансов. Сравнительная оценка показывает, что время восстановления туннеля OpenVPN может достигать 5–10 секунд, что недопустимо для телефонии и приводит к потере пакетов RTP.

IPsec (уровень ядра, IKEv2) обладает повышенной отказоустойчивостью [7]. Протокол поддерживает быстрое переключенное и мобильность (MOBIKE), минимизируя простой до менее чем 1 секунды. АПКШ «Континент» обеспечивает максимальную стабильность за счет аппаратных криптографических модулей и кластеризации. В то время как программные решения зависят от ресурсов операционной системы, аппаратные шлюзы обеспечивают переключение за миллисекунды⁶.

Для защиты речевого трафика используется связка TLS+SRTP. В отличие от IPsec, SRTP не шифрует заголовки RTP, но обеспечивает конфиденциальность медиапотока. Это решение эффективно для VoIP, но не заменяет VPN-технологии для защиты сетевого уровня.

На основе проведенного анализа можно сделать вывод, что для обеспечения безопасности открытой телефонной связи, как один из вариантов (рис. 3), может быть использована архитектура с каскадной схемой защиты услуг телефонной связи, как для сетей, построенных по классической клиент серверной архитектуре, так и для распределенных пиринговых сетей.

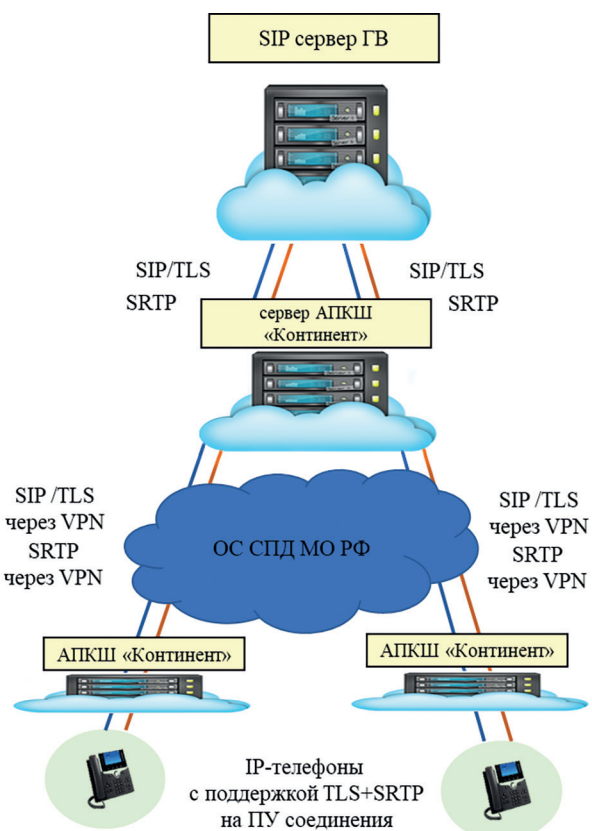


Рис. 3. Вариант архитектуры сети открытой телефонной связи с каскадной защитой услуг

Заключение

Очевидно, что для обеспечения защиты информации в сетях открытой телефонной связи наиболее предпочтительным решением является АПКШ «Континент» благодаря сертификации и поддержке ГОСТ РФ. Применение протокола IPsec рекомендуется как временное решение для защиты данных благодаря надежности туннелей. Применение OpenVPN для защиты голосового трафика не является приоритетным решением из-за проблем с устойчивостью

⁴ Федеральная служба по техническому и экспортному контролю. Требования к средствам криптографической защиты информации для обеспечения безопасности персональных данных при их передаче в сетях связи общего пользования: приказ ФСТЭК России от 11.02.2013 № 21. – М.: 2013. – 18 с.

⁵ ГОСТ Р 34.12-2015. Информационная технология. Криптографическая защита информации. Блочные шифры. – Введ. 2016-01-01. – М.: Стандартинформ, 2015. – 24 с.

⁶ АПКШ «Континент»: руководство администратора безопасности / ЗАО «Код Безопасности». – 4-е изд. – М.: 2022. – 156 с.

и отсутствия сертификации. В дополнение к выбранным решениям целесообразно применять каскадную схему защиты услуг телефонной связи

TLS+SRTP, которая обеспечивает шифрование непосредственно голосового и сигнального трафика.

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. – 304 с.
2. Кузина Е. И., Панкин А. А., Потапов И. А., Назаров А. Д. Особенности организации служебной телефонной связи на пунктах управления // Телекоммуникации и связь. – 2026. – № 1 (10). – С. 52–58.
3. Черемисин Д. Г., Мкртчян В. Р. Принципы построения пиринговых сетей // Международный научный журнал «Символ науки». – 2023. – № 6. – С. 31–32.
4. Яценко П. В. Безопасность VoIP-телефонии: угрозы и методы защиты // Информационная безопасность телекоммуникаций. – 2018. – № 3. – С. 45–52.
5. Петров В. К. Уязвимости программного обеспечения IP-телефонии // Защита информации. Инсайд. – 2021. – № 2. – С. 30–35.
6. Решетников С. Н. Применение TLS для защиты сигнализации SIP // Электросвязь. – 2023. – № 1. – С. 40–45.
7. Олифер В., Олифер Н. Компьютерные сети. Принципы, технологии, протоколы: Юбилейное издание, дополненное и исправленное // СПб.: Питер, 2024. – 1008 с.

ARCHITECTURE OF AN OPEN AUTOMATIC TELEPHONE NETWORK BUILT USING PEER-TO-PEER TECHNOLOGIES, AND PROPOSALS FOR ITS PROTECTION

Ashlapov M. V.⁷, Eliseev D. I.⁸

Keywords: telephony, telephony services, packet switching, cluster, hardware gateways, telephony security, audio conferencing.

Abstract

The purpose of the work is to analyze the architecture of a peer-to-peer network of open automatic telephone communication and proposals to ensure the protection of voice and signaling traffic.

Research method: the system approach is applied to the analysis of the architecture of the peer-to-peer automatic telephone network, on the basis of which proposals for the protection of voice and signal traffic in the open telephone network have been developed.

Results of the study: it is recommended to use hardware and software to ensure the security of open telephony.

Scientific novelty: the author determines the depth of substantiation of the use of peer-to-peer technologies for the construction of open telephone networks and consideration of the features of ensuring the security of voice and signal traffic transmission in such a network.

References

1. Ivanov V.G. Teoriya i praktika postroeniya i obespecheniya funkcionirovaniya sistemy svyazi special'nogo naznacheniya s uchytom tehnologicheskogo razvitiya i opytov vooruzhennykh konfliktov / monografiya V. G. Ivanov. – M.: Krasnaya Zvezda, 2025. – P. 304.
2. Kuzina E. I., Pankin A. A., Potapov I. A., Nazarov A. D. Osobennosti organizatsii sluzhebnoj telefonnoj svyazi na punktakh upravleniya // Telekommunikatsii i svyaz'. – 2026. – No 1 (10). – Pp. 52–58.
3. Cheremisin D. G., Mkrtychyan V. R. Principy postroeniya piringovykh setej // Meghdunarodnyi nauchnyi jurnal «Simvol nauki». – 2023. – No 6. – Pp. 31–32.
4. Yashchenko P. V. Bezopasnost' VoIP-telefonii: ugrozy i metody zashchity // Informacionnaya bezopasnost' telekommunikatsij. – 2018. – No 3. – Pp. 45–52.
5. Petrov V. K. Uyazvimosti programmnoho obespecheniya IP-telefonii // Zashchita informatsii. Insajd. – 2021. – No 2. – Pp. 30–35.
6. Reshetnikov S. N. Primenenie TLS dlya zashchity signalizatsii SIP // Ehlektrosvyaz'. – 2023. – No 1. – Pp. 40–45.
7. Olifer V., Olifer N. Komp'yuternye seti. Principy, tehnologii, protokoly: Yubilejnoe izdanie, dopolnennoe i ispravlennoe // SPb.: Piter, 2024. – P. 1008.

7 **Mikhail V. Ashlapov**, Ph.D. of Technical Sciences, Associate Professor of the Department of the Military Academy of Communications. St. Petersburg, Russia. E mail: mvashlapov@mail.ru

8 **Dmitry I. Eliseev**, Ph.D. of Technical Sciences, Associate Professor, Associate Professor of the Department of the Military Academy of Communications. St. Petersburg, Russia. E mail: dimone73@mail.ru

ОБНАРУЖЕНИЕ ДРОНОВ ПРОТИВНИКА С ПОМОЩЬЮ ПОИСКОВОЙ АППАРАТУРЫ, УСТАНОВЛЕННОЙ НА ОТЕЧЕСТВЕННЫХ БЕСПИЛОТНЫХ ЛЕТАТЕЛЬНЫХ АППАРАТАХ

Ахмедов Э. М.¹, Асадов Х. Г.², Алиева Х. С.³

DOI:10.21681/3034-4050-2026-3-69-73

Ключевые слова: математическое моделирование, оптимизация, оптимизируемые функции, видеокамеры, показатель вероятности, распознавание объектов, вражеские объекты, горные поверхности, обнаружения.

Аннотация

Цель: решение задачи обнаружения вражеских дронов в полете с помощью отечественных БПЛА, оборудованных видеокамерой и термальной камерой.

Метод: используется метод математического моделирования и синтеза с помощью составленной вариационной оптимизационной задачи.

Результат: для оценки эффективности обнаружения дрона противника использована вероятностная мера обнаружения. Введен на рассмотрение интегральный показатель вероятности и сформулирована задача оптимизации этого показателя. Также введена оптимизируемая функция взаимосвязи вероятности обнаружения дрона видеокамерой и вероятности обнаружения термальной ИК-камерой.

Определено, что при линейном виде оптимизируемой функции вновь введенный интегральный показатель вероятности обнаружения достигает максимума. Показано, что полученный результат проводимой оптимизации действителен в случае поиска оптимизируемой функции в пределах подмножества непрерывных и дважды дифференцируемых функций, удовлетворяющих определенному ограничительному условию.

Практическая ценность: полученные результаты могут быть использованы при планировании современных методов ведения боя с применением беспилотных аппаратов, а также поиске заданных объектов на поверхности Земли, в том числе в горной местности.

Введение

Как отмечается в работе [1], беспилотные летательные аппараты (БПЛА) имеют широкую область применения, не ограничиваясь такими сферами как контроль чрезвычайных ситуаций, безопасность границ, оценка состояния водных ресурсов, картографирование природных объектов, археологические и геологические исследования. Важной областью применения БПЛА также является контроль за состоянием дорожного транспортного движения [2], и в особенности в горной местности [3]. Как было отмечено в работе [3], эффективный контроль за состоянием дорожного движения может быть обеспечен только с помощью групповых полетов БПЛА на разных участках дорожной сети. Важность и значение группового применения БПЛА для выполнения различных задач также подчеркивается в работе [4]. Согласно этой работе, групповые полеты БПЛА позволяют расширить поле обзора поиска наземных объектов, увеличить

количество контролируемых пикселей на поверхности Земли. Не менее интересной областью применения БПЛА является их совместное функционирование с наземными беспилотными системами в целях контроля за поведением скопления людей [5]. Следует отметить, что широко распространенной областью применения БПЛА является обнаружение и распознавание (идентификация) объектов на поверхности Земли [6].

Следует отметить, что чрезвычайно широкая сфера применения дронов, включающая как гражданские, так и военные области, актуализировала задачу обнаружения самих БПЛА, запущенных во вражеских целях. Как указывается в работе [7], обнаружение дронов предусматривает решение таких задач как обнаружение объекта, отслеживание этого объекта и проведение классификации. С этой целью могут быть использованы RGB видеокамеры, специальные модули обнаружения для отличия их от птиц и различных воздушных баллонов.

¹ Ахмедов Эмиль Мехман оглы, аспирант Национального Аэрокосмического Агентства. Баку, Азербайджанская Республика. E-mail: emil.ahmadov@mail.ru

² Асадов Хикмет Гамид оглы, доктор технических наук, профессор, главный научный сотрудник НИИ Аэрокосмической информатики. Баку, Азербайджанская Республика. E-mail: asadzade@rambler.ru

³ Алиева Хумар Сабир гызы, кандидат технических наук, доцент, главный научный сотрудник НИИ Аэрокосмической информатики. Баку, Азербайджанская Республика. E-mail: khumar.aliyeva@maka.gov.az

На фоне отмеченной выше широкой области применения БПЛА безусловный интерес представляет их применения в целях обнаружения вражеских дронов. Указанная задача применения БПЛА безусловно отличается от вышеизложенных своей сложностью и системностью. Для решения данной задачи важно привлечение элементов системного анализа и элементов искусственного интеллекта. Следует отметить, что элементы теории нечетких множеств уже применяются в теории и практике при применении БПЛА для решения аналогичных задач [8]. Вместе с тем, важность привлечения методов системного анализа для решения указанной задачи неоспорима.

Материалы и методы

Как отмечается в работе [9], многоплановость работ по успешному функционированию БПЛА диктует необходимость формирования системного подхода к обеспечению успешной взаимосвязи привлекаемых для этой цели различных систем. Для этой цели предлагается использовать стандартные диаграммы функционирования привлеченных систем и подсистем БПЛА для дальнейшего использования их в объектно-ориентированной модели. Сообщается о разработке специального языка для обслуживания такой системы [9].

Также рассмотрены вопросы взаимосвязи такого языка со стандартными средствами моделирования, таких как MATLAB, и многокритериальных средств оптимизации, таких как MDAO. Примеры разработки и успешного использования подобных языков приведены в работах [10–14].

В работе [9] представлены диаграммы модельного представления функционирования БПЛА на разных уровнях обобщения. Блочные диаграммы БПЛА и подсистемы полезной нагрузки БПЛА представлены соответственно на рисунках 1 и 2.

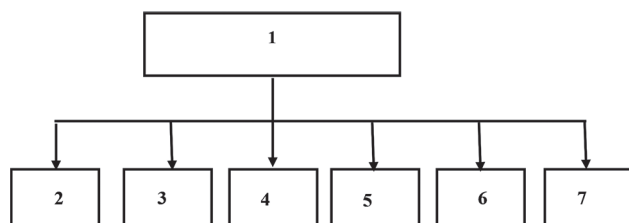


Рис. 1. Блочная диаграмма систем БПЛА [9]

1 – система БПЛА; 2 – контроль управляемой навигации; 3 – подсистема тяги; 4 – подсистема силовая; 5 – контроль полета БПЛА; 6 – рама БПЛА (механика); 7 – электронные узлы управления

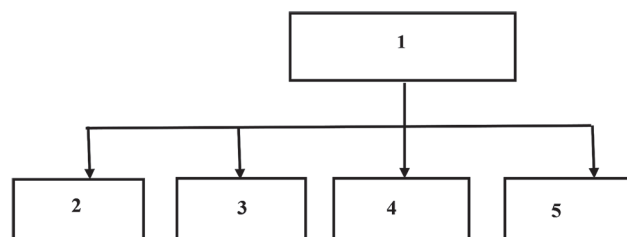


Рис. 2. Блочная диаграмма разведывательных компонент в полезной нагрузке БПЛА [9]

1 – полезная нагрузка; 2 – камера; 3 – инерциальное навигационное устройство; 4 – процессор; 5 – лидар

Применительно к поставленной в настоящей статье задаче обнаружения в полете вражеских дронов диаграмма функционирования БПЛА приведена на рисунке 3.

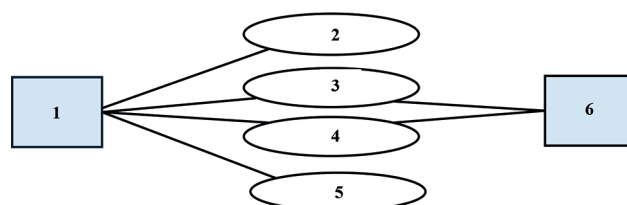


Рис. 3. Диаграмма функционирования разведывательного БПЛА, способного обнаружить вражеские дроны [9] с изменением

1 – БПЛА; 2 – перевозка оружия; 3 – разведка вражеских дронов; 4 – сбор разведывательной информации; 5 – атака без чрезвычайных случаев; 6 – контролирующий орган (наземная станция контроля)

Диаграмма состояний БПЛА, реализующей концепцию обнаружения и уничтожения вражеского БПЛА, приведена на рисунке 4.

Что касается средств и методов обнаружения в полете БПЛА вражеских дронов, то здесь можно воспользоваться результатами работы [6], в которой предлагается использование видеокамеры высокого разрешения и термальной ИК камеры для обнаружения различных объектов, представляющих определенную опасность (РТО – Possible Threat Objects).

Кадры, получаемые от видеокамеры и термальной камеры, обрабатываются по имеющимся признакам.

Проведем вероятностный анализ обнаружения вражеского дрона отдельно, используя видеокамеру и термальную ИК камеру. Обозначим общую вероятность обнаружения вражеского дрона как P_{Σ} , тогда P_{Σ} может быть вычислен как

$$P_{\Sigma} = P_v^{\alpha_1} \cdot P_T^{(1-\alpha_1)}, \quad (1)$$

где P_v – вероятность обнаружения вражеского дрона с помощью видеокамеры; P_T – вероятность обнаружения с помощью термальной камеры; α – весовой коэффициент.

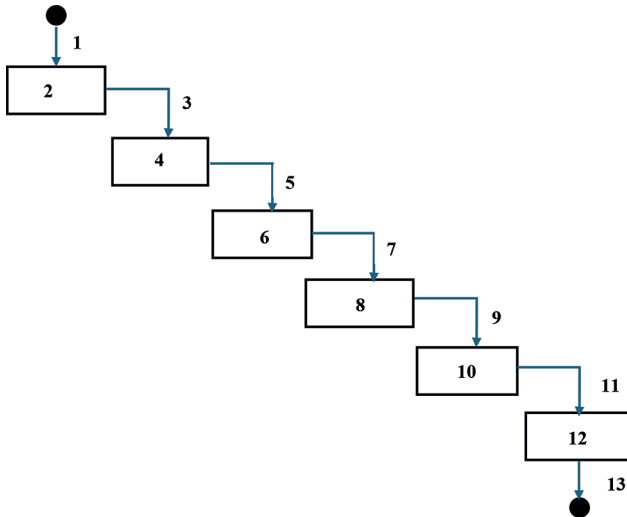


Рис. 4. Диаграмма состояний БПЛА по реализации концепции обнаружения и уничтожения вражеского дрона [9] с изменениями

1 – проверка безопасности; 2 – взлет; 3 – подъем на заданную высоту; 4 – избегание столкновений; 5 – приближение к цели; 6 – зарядка оружия; 7 – определение вражеского дрона; 8 – активизация сенсора разведки; 9 – комментарии от наземной станции контроля; 10 – атака вражеского дрона; 11 – вражеский дрон; 12 – путь возврата, выданный наземной станцией контроля; 13 – приземление

Введем на рассмотрение интегральный показатель обнаружения P_u , определяемый как

$$P_u = \int_0^{P_{Tmax}} P_v^\alpha \cdot P_T^{(1-\alpha)} dP_T. \quad (2)$$

При этом допускаем, что имеется некоторое множество вражеских дронов, тепловое излучения которых линейно изменяется от минимума до максимума, и соответственно P_T также изменяется от минимума до максимума.

Рассмотрим условия оптимизации предлагаемого показателя P_u .

Введем на рассмотрение следующую оптимизируемую функцию

$$P_v = \varphi(P_T). \quad (3)$$

С учетом выражений (2) и (3) получаем

$$P_u = \int_0^{P_{Tmax}} \varphi(P_T)^\alpha \cdot P_T^{(1-\alpha)} dP_T. \quad (4)$$

Для вычисления вида $\varphi(P_T)$, при которой P_u достигает экстремума, считая $\varphi(P_T)$ непрерывной и дважды дифференцируемой функцией, наложим на нее следующее ограничительное условие:

$$\int_0^{P_{Tmax}} \varphi(P_T) \cdot dP_T = c; c = const. \quad (5)$$

Заметим, что с учетом условия (5) поиск экстремума функционала (4) будем осуществлять по подклассу непрерывных и дважды дифференцируемых функций, в котором справедливо условие (5).

С учетом выражений (4) и (5) сформируем целевой функционал вариационной оптимизации F :

$$F = \int_0^{P_{Tmax}} \varphi(P_T)^\alpha \cdot P_T^{(1-\alpha)} dP_T - \lambda \left[\int_0^{P_{Tmax}} \varphi(P_T)^\alpha \cdot dP_T - c \right], \quad (6)$$

где λ – множитель Лагранжа.

Решение оптимизационной задачи (6) осуществим по методу Эйлера, согласно которому оптимизируемая функция $\varphi(P_T)_{opt}$ удовлетворяет следующему требованию

$$\frac{d\{\varphi(P_T)^\alpha \cdot P_T^{(1-\alpha)} dP_T - \lambda \varphi(P_T)\}}{d\varphi(P_T)} = 0. \quad (7)$$

Из условия (7) получаем

$$\alpha \varphi(P_T)^{\alpha-1} \cdot P_T^{(1-\alpha)} dP_T - \lambda = 0. \quad (8)$$

Из (8) находим

$$\varphi(P_T) = \sqrt[\alpha-1]{\frac{\lambda}{\alpha P_T^{(1-\alpha)}}}. \quad (9)$$

Выражение (9) можно записать в виде

$$P_v = \left(\frac{\lambda}{\alpha}\right)^{1/\alpha-1} \cdot P_T = k \cdot P_T, \quad (10)$$

где

$$P_v = \left(\frac{\lambda}{\alpha}\right)^{1/\alpha-1}; k = const. \quad (11)$$

Легко показать, что при выполнении условия (10) целевой функционал F достигает максимума, т. е. вражеский дрон может быть обнаружен с максимальной вероятностью. С этой целью можно воспользоваться признаком Лагранжа, который применительно к решаемой задаче означает, что исследуемый экстремум является максимумом в том случае, если производная выражения (8) по $\varphi(P_T)$ оказывается отрицательной величиной. Очевидно, что с учетом $\alpha \leq 1$ данное требование выполняется.

Что касается вычисления λ , то с этой целью можно воспользоваться выражениями (5) и (10).

Заключение

В отличие от известных работ, в которых обсуждаются вопросы обнаружения дронов с помощью наземных видеокамер и термальных камер, сформулирована и системно проанализирована задача обнаружения вражеских дронов с помощью БПЛА, оборудованного соответствующей аппаратурой. Определены оптимальные условия выбора характеристик используемых видео и термальных камер в вероятностном смысле, при которых вновь введенный

интегральный показатель вероятности обнаружения вражеского дрона достигает минимума. При этом заключение о наличии максимума оказывается верной при поиске вновь введенной

оптимизируемой функции $P_v = \varphi(P_T)$ в подклассе непрерывных и дважды дифференцируемых функций, удовлетворяющих определенному ограничительному условию.

Литература

1. Nabiyev N. M., Abdullayev A. A. The optimization of the Surveillance Capabilities of UAVs. Tuijin Jishu / Journal of Propulsion Technology. ISSN: 1001-4055. – Vol. 46. – No. 2 (2025). – Pp. 1212–1221.
2. Muhammad Arsalan Khan, Wim Ectors, Tom Bellemans, Davy Janssens and Geert Wets UAV-Based Traffic Analysis: A Universal Guiding Framework Based on Literature Survey. Transportation Research Procedia. 2017. 22:541-550. DOI:10.1016/j.trpro.2017.03.043.
3. Асатов Х. Г., Алиева Г. В., Гусейнов О. А. Анализ тягового режима при групповом полёте различных БПЛА при контроле за движением на горной автотрассе // Авиационная промышленность. – 2025. – № 1. – С. 46–50.
4. Pengnian Wu, Yixuan Li, Dong Xue. Multi-Target Tracking with Multiple Unmanned Aerial Vehicles Based on Information Fusion. Drones. November 2024. 8(12):704. DOI:10.3390/drones8120704.
5. Amirreza M. Khaleghi, Dong Xu, Sara Minaeian, Yifei Yuan, Jian Liu, Young-Jun Son. Analysis of UAV/UGV Control Strategies in a DDDAMS-based Surveillance System. May 2015. Industrial and Systems Engineering Research Conference 2015.
6. Eren Unlu, Emmanuel Zenou, Nicolas Riviere, Paul-Edouard Dupouy. An Autonomous Drone Surveillance and Tracking Architecture. Electronic Imaging. 2019(15):35-1-35-7. – DOI:10.2352/ISSN.2470-1173.2019.15.AVM-035.
7. Xing D., Unlu H. U., Evangeliou N., Tzes A. Drone Surveillance Using Detection, Tracking and Classification Techniques. Image Analysis and Processing. ICIAP 2022 Workshops. 4 August 2022. – Pp. 446–457. URL: https://doi.org/10.1007/978-3-031-13324-4_38.
8. M. Kontitsis, N. Tsurveloudis, K. Valavanis. A UAV Based Automated Airborne Surveillance System. IEEE International Conference on Robotics and Automation, 2004. – DOI: 10.1109/ROBOT.2004.1307132.
9. Niamat Ullah Ibne Hossain, Mostafa Lutfi, Ifaz Ahmed, Aditya Akundi and Daniel Cobb. Modeling and Analysis of Unmanned Aerial Vehicle System Leveraging Systems Modeling Language (SysML). Systems 2022, 10(6), 264. URL: <https://doi.org/10.3390/systems10060264>.
10. Dzielski J., Blackburn M. Implementing a Decision Framework in SysML Integrating MDAO Tools. INSIGHT. – 2018. – No 21. – Pp. 15–19.
11. Aprville L., de Saqui-Sannes P., Vingerhoeds R. An educational case study of using sysml and tool for unmanned aerial vehicles design. IEEE J. Miniatur. Air Space Syst. – 2020. – No 1. – Pp. 117–129.
12. Xing-hua L., Yun-feng C. Design of UAV flight control system virtual prototype using rhapsody and simulink. In Proceedings of the 2010 International Conference on Computer Design and Applications, Qinhuaangdao, China, 25–27 June 2010. – Pp. V3–V4.
13. Queiroz P., Braga R. Combining MARTE-UML, SysML and CVL to build unmanned aerial vehicles. In Proceedings of the Ninth International Conference on Software Engineering Advances, Nice, France, October 2014. – Pp. 334–340.
14. Макаренко С. И., Афонин И. Е. Моделирование боевых действий авиации и оценки их эффективности – анализ работ, моделей, актуальных направлений исследований // Системы управления, связи и безопасности. – 2024. – № 3. – С. 78–125. – DOI: 10.24412/2410-9916-2024-3-078-125.

DETECTION OF ENEMY DRONES USING SEARCH EQUIPMENT INSTALLED ON DOMESTIC UNMANNED AERIAL VEHICLES

Akhmedov E. M.⁴, Asadov Kh. G.⁵, Aliyeva Kh. S.⁶

Keywords: mathematical modeling, optimization, optimized functions, video cameras, probability indicator, object recognition, enemy objects, mountain surfaces, detections.

Abstract

Goal: solving the problem of detecting enemy drones in flight using domestic UAVs equipped with a video camera and a thermal camera.

Method: the method of mathematical modeling and synthesis is used using the compiled variational optimization problem.

⁴ **Ahmadov, Emil Mehman oglu**, postgraduate student of the National Aerospace Agency. Baku, Republic of Azerbaijan. E-mail: emil.ahmadov@mail.ru

⁵ **Asadov, Hikmet Hamid oglu**, Dr.Sc. of Technical Sciences, Professor, Chief Researcher of the Research Institute of Aerospace Informatics. Baku. Republic of Azerbaijan. E-mail: asadzade@rambler.ru

⁶ **Aliyeva, Khumar Sabir gizi**, Ph.D. of Technical Sciences, Associate Professor, Chief Researcher of the Research Institute of Aerospace Informatics. Baku. Republic of Azerbaijan. E-mail: khumar.aliyeva@maka.gov.az

Result: a probabilistic detection measure was used to assess the effectiveness of detecting an enemy drone. An integral probability indicator was introduced for consideration and the problem of optimizing this indicator was formulated. An optimized function of the relationship between the probability of detecting a drone by a video camera and the probability of detection by a thermal IR camera was also introduced.

It is determined that in the linear form of the optimized function, the newly introduced integral index of the probability of detection reaches its maximum. It is shown that the result of the optimization is valid in the case of searching for the function to be optimized within a subset of continuous and doubly differentiable functions that satisfy a certain restrictive condition.

Practical value: the results obtained can be used in planning modern methods of combat using unmanned aerial vehicles, as well as searching for specified objects on the Earth's surface, including in mountainous areas.

References

1. Nabiyeu N. M., Abdullayev A. A. The optimization of the Surveillance Capabilities of UAVs. Tuijin Jishu / Journal of Propulsion Technology. ISSN: 1001-4055. – Vol. 46. – No 02 (2025). – Pp.1212–1221.
2. Muhammad Arsalan Khan, Wim Ectors, Tom Bellemans, Davy Janssens. UAV-Based Traffic Analysis: A Universal Guiding Framework Based on Literature Survey. Transportation Research Procedia. 2017. 22:541-550. DOI:10.1016/j.trpro.2017.03.043.
3. Asadov H. G., Alieva G. V., Guseynov O. A. Analiz tyagovogo rezhima pri gruppovom polyote razlichnyh BpLA pri kontrole za dvizheniem na gornoj avtotrasse. «Aviacionnaya promyshlennost'». – 2025. – Pp. 46–50.
4. Pengnian Wu, Yixuan Li, Dong Xue. Multi-Target Tracking with Multiple Unmanned Aerial Vehicles Based on Information Fusion. Drones. November 2024. 8(12):704. DOI:10.3390/drones8120704.
5. Amirreza M. Khaleghi, Dong Xu, Sara Minaeian, Yifei Yuan, Jian Liu, Young-Jun Son. Analysis of UAV/UGV Control Strategies in a DDDAMS-based Surveillance System. May 2015. Industrial and Systems Engineering Research Conference 2015.
6. Eren Unlu, Emmanuel Zenou, Nicolas Riviere, Paul-Edouard Dupouy. An Autonomous Drone Surveillance and Tracking Architecture. Electronic Imaging. 2019(15):35-1-35-7. – DOI:10.2352/ISSN.2470-1173.2019.15.AVM-035.
7. Xing D., Unlu H. U., Evangeliou N., Tzes A. Drone Surveillance Using Detection, Tracking and Classification Techniques. Image Analysis and Processing. ICIAAP 2022 Workshops. 4 August 2022. – Pp. 446–457. URL: https://doi.org/10.1007/978-3-031-13324-4_38.
8. M. Kontitsis, N. Tsourveloudis, K. Valavanis. A UAV Based Automated Airborne Surveillance System. IEEE International Conference on Robotics and Automation, 2004. – DOI: 10.1109/ROBOT.2004.1307132.
9. Niamat Ullah Ibne Hossain, Mostafa Lutfi, Ifaz Ahmed, Aditya Akundi and Daniel Cobb. Modeling and Analysis of Unmanned Aerial Vehicle System Leveraging Systems Modeling Language (SysML). Systems 2022, 10(6), 264. URL: <https://doi.org/10.3390/systems10060264>.
10. Dzielski J., Blackburn M. Implementing a Decision Framework in SysML Integrating MDAO Tools. INSIGHT 2018, 21, Pp. 15–19.
11. Apvrille L., de Saqui-Sannes P., Vingerhoeds R. An educational case study of using sysml and tool for unmanned aerial vehicles design. IEEE J. Miniat. Air Space Syst. – 2020. – No 1. – Pp. 117–129.
12. Xing-hua L., Yun-feng C. Design of UAV flight control system virtual prototype using rhapsody and simulink. In Proceedings of the 2010 International Conference on Computer Design and Applications, Qinhuangdao, China, 25–27 June 2010. – Pp. V3–V4.
13. Queiroz P., Braga R. Combining MARTE-UML, SysML and CVL to build unmanned aerial vehicles. In Proceedings of the Ninth International Conference on Software Engineering Advances, Nice, France, October 2014. – Pp. 334–340.
14. Makarenko S. I., Afonin I. E. Modelirovanie boevyh dejstvij aviacii i ocenki ih ehffektivnosti – analiz rabot, modelej, aktual'nyh napravlenij issledovanij // Sistemy upravleniya, svyazi i bezopasnosti. – 2024. – No 3. – Pp. 78–125. – DOI: 10.24412/2410-9916-2024-3-078-125.



ОПТИМИЗАЦИЯ ФУНКЦИОНИРОВАНИЯ ПЕРЕДОВЫХ ПУНКТОВ ТЕХНИЧЕСКОГО ОБЕСПЕЧЕНИЯ КАК ФАКТОР ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ ОБСЛУЖИВАНИЯ СИСТЕМ СВЯЗИ И АСУ

Курочка В. С.¹, Колодяжный П. А.², Юшин А. И.³

DOI:10.21681/3034-4050-2026-3-74-82

Ключевые слова: восстановление техники связи, неисправность, трудоемкость, цикл ремонта, интенсивность ремонта, планирование ремонта, склады средств связи, QR-коды.

Аннотация

Цель работы: заключается в уточнении и обосновании комплексного подхода к совершенствованию подсистемы восстановления объединений путем оптимизации функционирования ППТО на основе методов математического моделирования.

Результаты исследования: выявлены основные проблемы организации восстановления техники связи и автоматизированных систем управления (ТС и АСУ) и методы их решения в условиях ведения современных операций и для оценки качества и планирования деятельности ремонтных органов объединений использованы основные технико-экономические показатели: трудоемкость видов ремонта для конкретных ТС и АСУ, продолжительность ремонтного цикла, интенсивность работ и фонд рабочего времени. Их аналитический расчёт служит основой для оценки производительности ремонтных ячеек передовых пунктов технического обеспечения (ППТО), определения требуемого количества таких пунктов, их организационной структуры и перечня выполняемых ремонтных операций. Приведено обоснование использования методов математического моделирования с целью определения рационального состава сил и средств ППТО объединения, в зависимости от складывающейся оперативной обстановки. Представлена схема планирования ремонтов на ППТО. Предложен способ повышения эффективности функционирования складов средств связи из состава ППТО за счет использования технологии QR-кодов. Разработан уточненный математический аппарат, который может быть использован в работе должностных лиц по ТОС и АСУ в ходе организации функционирования подсистемы восстановления ТС и АСУ в современных операциях.

Практическая полезность заключается в возможности использования уточненного математического аппарата отдельно или в составе автоматизированной системы управления техническим обеспечением связи и автоматизированных систем управления (ТОС и АСУ) в качестве инструмента поддержки принятия решения при организации восстановления ТС и АСУ в операции и формировании рационального варианта состава сил и средств ремонтных органов объединения.

Введение

В условиях современных операций элементы системы связи, используемые для развертывания системы управления объединения, подвергаются интенсивной эксплуатации, огневому воздействию противника и другим деструктивным факторам, что негативно влияет на обеспеченность войск исправной, боеготовой ТС и АСУ.

Для поддержания максимально возможной заданной обеспеченности войск работоспособными, готовыми к применению по назначению ТС и АСУ, развернута эшелонированная система ТОС и АСУ объединения. Важным элементом этой системы является подсистема восстановления, основным компонентом которой выступают ППТО. Оптимизация функционирования ППТО позволит значительно повысить эффективность системы ТОС и АСУ объединения.

Восполнение боевых потерь в ТС и АСУ возможно двумя путями:

- за счет подсистемы снабжения (поставка новых образцов взамен вышедших из строя);
- за счет подсистемы восстановления (ремонтно-восстановительные работы для приведения поврежденных образцов ТС и АСУ в исправное состояние и их последующего возвращения в строй).

При этом второй путь является более предпочтительным, так как при проведении ремонта замене подлежат только отказавшие части (блоки, узлы, агрегаты), стоимость которых значительно ниже стоимости всего образца [1]. Основные мероприятия восстановления выполняются развернутой сетью передовых пунктов технического обеспечения (ППТО). Задачами ППТО являются:

¹ Курочка Владимир Сергеевич, кандидат военных наук, доцент кафедры Военной академии связи. Санкт-Петербург, Россия. E-mail: Uprava223@mail.ru

² Колодяжный Петр Алексеевич, слушатель Военной академии связи. Санкт-Петербург, Россия. E-mail: petr2020.sev@mail.ru

³ Юшин Александр Иванович, кандидат технических наук, доцент кафедры Военной академии связи. Санкт-Петербург, Россия. E-mail: alyushin@yandex.ru

- обеспечение войск исправной техникой и имуществом связи;
- ремонт ТС и АСУ сложного текущего и среднего видов ремонта;
- обеспечение деятельности выездных ремонтных бригад (ВРБ) предприятий промышленности (ПП);
- накопление и содержание запасов ТС и АСУ и военно-технического имущества (ВТИ);
- взаимодействие с ПП по вопросам ремонта в рамках государственных контрактов, в том числе капитального, и исполнения гарантийных обязательств.

Оперативное развертывание ППТО в условиях проведения операций предусматривает создание единого комплекса, интегрирующего ремонтные посты, складские мощности для ТС и АСУ, ЗИП, ВТИ, а также выездные ремонтные отделения и подразделения охраны.

Методы определения рационального количества и состава ремонтных ячеек на ППТО при восстановлении ТС и АСУ

В современных операциях одной из главных причин снижения доступности работоспособной ТС и АСУ является деструктивное воздействие противника. При этом существуют и другие факторы, приводящие к выходу ТС и АСУ из строя (табл. 1). По этой причине основные усилия органов управления системой ТОС и АСУ должны быть направлены на поиск и использование всех доступных способов скорейшего дообеспечения войск работоспособной, готовой к применению ТС и АСУ. Одним из способов достижения этой цели является оптимизация функционирования ППТО.

В зависимости от возложенных задач и удаленности от линии боевого соприкосновения войск, ППТО могут иметь различный состав сил и средств. Основными элементами могут быть склад средств связи и посты по ремонту: телефонных аппаратов, радиостанций тактического звена управления, IT-оборудования, средств проводной связи, аккумуляторных батарей и зарядных устройств, станций спутниковой связи и др. (далее в тексте статьи, для краткости посты ремонта будут именоваться – ремонтными

ячейками). Каждая такая ремонтная ячейка укомплектовывается определенным количеством специалистов-ремонтников. Оптимизация количества и состава ремонтных ячеек критически важна, поскольку позволяет рационально распределить ремонтные мощности, сократить сроки восстановления ТС и АСУ, снизить эксплуатационные затраты на содержание ремонтной инфраструктуры и транспортировку агрегатов, вследствие чего – поддерживать требуемый уровень обеспеченности работоспособными, готовыми к применению по назначению ТС и АСУ.

В соответствии с ГОСТ 18322-2016⁴, система технического обслуживания и ремонта (ТО и Р) представляет собой организованную совокупность взаимосвязанных элементов: исполнителей, технических средств и документации. Ее предназначение – планомерное поддержание и восстановление качества эксплуатируемых изделий. На рисунке 1 отображена типовая структурная схема данной системы, иллюстрирующая взаимосвязи между ее компонентами [2].

Для наглядного представления технических мероприятий по восстановлению ТС и АСУ разработана систематизированная классификация видов ремонта (табл. 2). Критериями для дифференциации послужили: сложность работ, требуемые ресурсы, место выполнения и глубина восстановления технических характеристик. Выбор конкретного вида ремонтных мероприятий – текущего, среднего или капитального – осуществляется на основе комплексной диагностики технического состояния оборудования с учетом степени повреждения, характера неисправностей и расчетной трудоемкости восстановительных работ.

Стоит отметить, что капитальный ремонт включает в себя весь комплекс работ, предусмотренный для среднего ремонта, и выполняется преимущественно на заводах-изготовителях. В исключительных случаях, при подтвержденной технической разведкой нецелесообразности восстановления отдельных образцов, капитальный ремонт организуется в полевых условиях методом перекомпоновки – сборки работоспособных образцов техники из исправных компонентов

⁴ ГОСТ 18322-2016 Система технического обслуживания и ремонта техники. Термины и определения. М.: Стандартинформ, 2017. 16 с.

Таблица 1.

Перечень основных факторов, приводящих к выходу из строя ТС и АСУ

Виды отказов	Причины отказов
Одиночные	Износ, старение аппаратуры, недостатки конструкции и технологии, ударные нагрузки, перегрузки, ошибочные действия личного состава
Групповые	Преднамеренные воздействия (массированное применение ядерного, высокоточного или обычного оружия; электромагнитное воздействие). Природные явления (грозы, оползни, разливы рек, землетрясения, ураганы, обледенения и т. п.)



Рис. 1. Структурная схема ТО и Р

нескольких поврежденных единиц⁵ [3]. В качестве методики планирования ремонтных работ образцов ТС и АСУ, алгоритм которой отражен на структурной схеме, приведенной на рисунке 2 [2].

Стоит отметить, что капитальный ремонт включает в себя весь комплекс работ, предусмотренный для среднего ремонта, и выполняется преимущественно на заводах-изготовителях. В исключительных случаях, при подтвержденной технической разведкой нецелесообразности восстановления отдельных образцов, капитальный ремонт после дефектовки организуется в полевых условиях методом переком-

плектации – сборки работоспособных образцов техники из исправных компонентов нескольких поврежденных единиц⁶ [2]. В качестве методики планирования ремонтных работ образцов ТС и АСУ принимается алгоритм, который отражен на структурной схеме на рисунке 2 [2].

Для выполнения капитального ремонта по методу перекомплектации выездные ремонтные отделения и выездные ремонтные бригады предприятий промышленности. В ситуациях с нехваткой ресурсов данный подход, наравне с агрегатно-участковым восстановлением, распространяется также на проведение среднего

5 Агеев Е. В., Грашков С. А. Техническое обслуживание и ремонт машин в АПК: учебное пособие. – Курск: Курская ГСХА, 2019. – 185 с.

6 Агеев Е.В., Грашков С.А. Техническое обслуживание и ремонт машин в АПК: учебное пособие. Курск: Курская ГСХА, 2019. 185 с.

Таблица 2.

Сравнительная характеристика видов ремонта ТС и АСУ

Критерий	Текущий ремонт	Средний ремонт	Капитальный ремонт
Цель работ	Локализация отказов и оперативное восстановление базовой работоспособности	Восстановление эксплуатационных характеристик и тактико-технических показателей	Полное восстановление ресурса и заводских характеристик оборудования
Объём работ	Замена неисправных модулей и блоков из комплектов ЗИП	Демонтаж, дефектовка и замена узловых компонентов	Полная разборка, дефектовка всех элементов, комплексное восстановление
Место выполнения	Расчёты (экипажи), ППТО, с привлечением ВРБ ПП	ППТО, стационарные мастерские, полевые условия с ВРБ ПП	Специализированные ремонтные предприятия и заводы-изготовители
Технологические особенности	Регулировка и настройка после замены компонентов	Диагностика всех систем, испытания под эксплуатационной нагрузкой	Комплексные проверки, продолжительные испытания на надёжность
Специальные методы	–	–	Перекомплектация из нескольких неисправных образцов
Включаемые работы	–	Все операции текущего ремонта	Все операции среднего ремонта

ремонта. Дефектное оборудование отправляется на восстановление либо на ППТО, либо на заводские ремонтные базы. После ремонта компоненты поступают для пополнения запасов ЗИП промышленных предприятий, данный подход обеспечивает [2]:

- максимальное сокращение сроков ремонта и простоя ТС и АСУ в неисправном состоянии;
- уменьшение трудозатрат и времени на возвращение ТС и АСУ в строй за счет того, что снятые неисправные агрегаты и механизмы ремонтируются, как правило, на специализированных стационарных и подвижных ремонтных базах заводов-изготовителей;
- снижение требований к квалификации ремонтников, непосредственно восстанавливающих работоспособность ТС и АСУ.

Схема технологического процесса ремонта ремонтными ячейками на ППТО представлена на рисунке 3.

Эффективность работы ремонтных ячеек определяется их способностью осуществлять качественное и своевременное восстановление вышедших из строя ТС и АСУ в сроки, обеспечивающие сохранение боеспособности войск. Ключевыми техническими характеристиками, определяющими качество функционирования ремонтных подразделений, являются следующие показатели [2]:

1. Расчет трудоемкости ремонта T для заданного типа ТС и АСУ основан на агрегировании времени, необходимого для выполнения всей совокупности технологических операций. Показатель выражается в человеко-часах на единицу

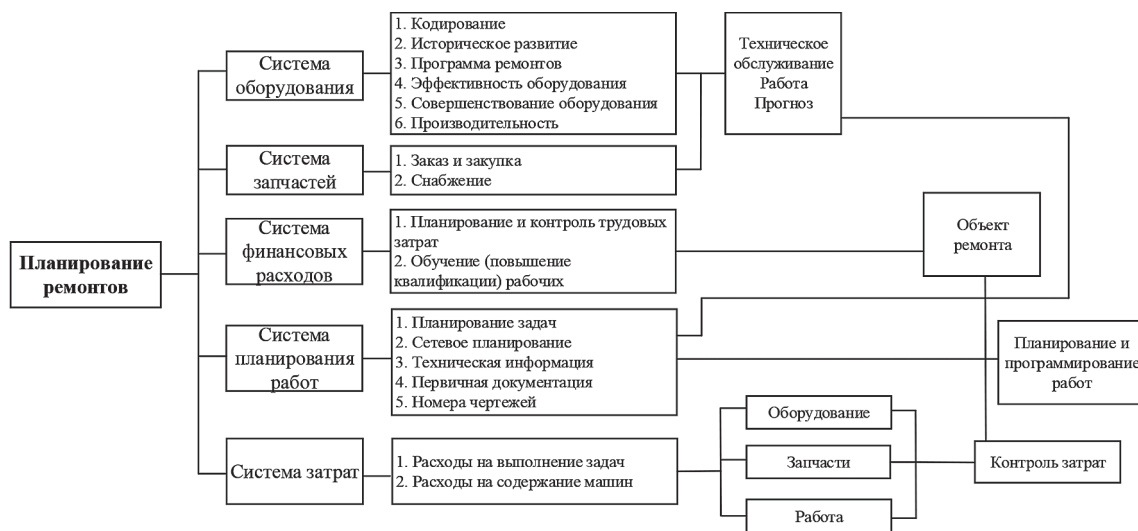


Рис. 2. Вариант структурной схемы планирования ремонтов

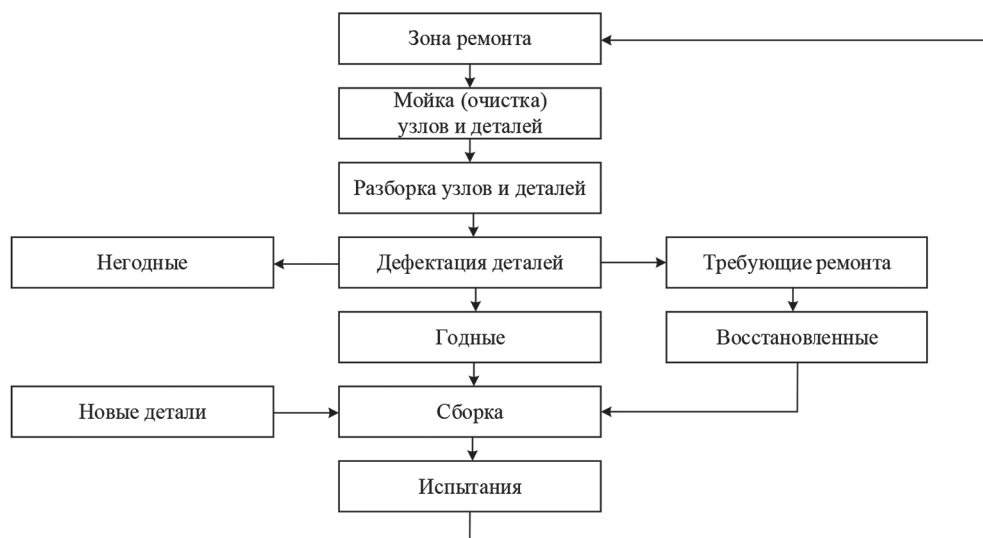


Рис. 3. Схема технологического процесса ремонта ремонтными ячейками ППТО

ремонтируемой техники и определяется по формуле:

$$T_{\text{тр}} = \sum_{i=1}^l \sum_{j=1}^{z_{\text{pm}}} \sum_{\xi=1}^{z_{\text{po}}} t_{\text{po } ij \xi},$$

где: t_{po} – норма времени на одну ремонтную операцию; $\xi = 1, 2, 3, \dots, z_{\text{po}}$ – индекс, имеющий значения от 1 до z_{po} , где z_{po} – общее число операций на рабочем месте; $j = 1, 2, 3, \dots, z_{\text{pm}}$ – число рабочих мест на каждом участке технологической линии ремонта; $i = 1, 2, 3, \dots, l$ – число ремонтных участков на технологической линии ремонта или в ремонтном органе [2].

2. Показатель длительности ремонтного цикла $T_{\text{цр}}$ характеризует минимально необходимое время для восстановления единицы техники. Он складывается из операционных затрат времени на всех этапах ремонта, организованных по принципу кратчайшего технологического пути, и определяется по формуле (в часах на единицу) [2]:

$$T_{\text{цр}} = \sum_{i=1}^{l_{\text{кп}}} t_{\text{цр } ij},$$

где: $i, j = 1, 2, 3, \dots, l_{\text{кп}}, z_{\text{pm}}^{\text{кп}}$ – показатель, определяющий количество этапов в ремонтном процессе, которое ТС и АСУ проходят по самому короткому технологическому маршруту – от начала ремонта до его окончания; $t_{\text{цр } ij}$ – представляет собой продолжительность ремонтного цикла для конкретной позиции в технологической цепи: i – номер участка, j – номер рабочего места на этом участке [2].

Количество параллельно работающих участков $z_{\text{пр}}$ определяется как разность между общим количеством рабочих мест (ремонтных участков) в органе z_{pm} и их минимально необходимым числом для обеспечения кратчайшего технологического маршрута:

$$z_{\text{пр}} = z_{\text{pm}} - z_{\text{pm}}^{\text{кп}}.$$

Таким образом, показатель $z_{\text{пр}}$ напрямую влияет на длительность ремонтного цикла $T_{\text{цр}}$: чем больше параллельно функционирующих мест, тем короче цикл и выше производительность ремонтного подразделения. Сам ремонтный цикл $T_{\text{цр}}$ представляет собой среднее время восстановления единицы техники в данном органе и может рассматриваться как математическое ожидание длительности цикла.

Анализ выявленной зависимости позволяет утверждать, что производительность ремонтного органа имеет прямую корреляцию с числом параллельно функционирующих участков $z_{\text{пр}}$. Основным следствием увеличения данного параметра является снижение общей длительности ремонтного цикла $T_{\text{цр}}$, что непосредственно ведет к росту операционной эффективности подразделения. Показатель $T_{\text{цр}}$, будучи средним

временем восстановления единицы техники, применяется в качестве математического ожидания длительности цикла и служит ключевой метрикой для планирования и оценки работы ремонтной службы.

3. Интенсивность ремонта μ – это параметр, количественно характеризующий скорость выполнения восстановительных работ в ремонтной ячейке, на участке или рабочем месте. Она определяется как величина, обратная средней продолжительности ремонтного цикла:

$$\mu = \frac{1}{T_{\text{цр}}}.$$

Таким образом, параметр μ описывает поток восстановления техники в рамках рассматриваемого ремонтного органа [2].

4. Под фондом рабочего времени $\Phi_{\text{рв}}$ понимается совокупный ресурс времени (в человеко-часах), доступный ремонтному подразделению при заданной организации труда и штатной численности личного состава. Данный фонд рассчитывается по формуле для различных плановых интервалов: смены, суток, недели, месяца или года [2]:

$$\Phi_{\text{рв}} = \left(t_{\text{рд}} \cdot K_{\text{рс}} \cdot D \cdot N_{\text{рем}} \cdot \frac{100 + \Pi_{\text{пр}}}{100} - T_{\text{обс}} \right) \cdot \frac{100 + \Pi_{\text{пв}}}{100},$$

где: $t_{\text{рд}}$ – длительность рабочей смены в часах; $K_{\text{рс}}$ – количество рабочих смен в течение суток; D – количество рабочих дней в расчетном периоде; $N_{\text{рем}}$ – численность мастеров и рабочих в одной смене; $\Pi_{\text{пр}}$ – средний уровень потерь рабочего времени, %; $T_{\text{обс}}$ – время на обслуживание оборудования ремонтной ячейки и его профилактические ремонты; $\Pi_{\text{пв}}$ – ожидаемый процент перевыполнения норм выработки специалистами-ремонтниками [2].

Величина фонда рабочего времени характеризует потенциальные возможности ремонтной ячейки по выполнению работ.

Представленная система показателей служит основой для оценки качественных параметров ремонтных ячеек и последующей оптимизации их количества и внутренней структуры. Определение трудоемкости ремонтных операций является первоочередной задачей и требует наличия детализированных перечней работ для ремонтов различной сложности: текущего, среднего и капитального. Формирование этих перечней должно базироваться на анализе прогнозируемых видов повреждений и отказов ТС и АСУ, а также учитывать фактическую обеспеченность ремонтной базы. Ключевыми факторами здесь выступают наличие специализированного оборудования, контрольно-измерительных приборов (КИА), технологической оснастки, инструмента, приспособлений и запасов запчастей ЗИП [2].

Непосредственное нормирование трудоемкости осуществляется эмпирическим путем – методом хронометражных замеров времени, затрачиваемого на каждую операцию в реальных условиях ремонта. Полученные таким образом временные нормы на отдельные работы (ремонтные операции) одновременно устанавливают и нормы выработки для личного состава.

На заключительном этапе проводится статистическая обработка данных хронометража, в результате которой определяются расчетные (нормативные) трудозатраты на каждый вид работ. Это позволяет агрегировать и получить суммарные нормы времени на проведение всего объема работ в рамках текущего, среднего и капитального ремонта для конкретного типа ТС и АСУ [3].

Исходными данными для планирования ресурсов (рабочих мест, участков и личного состава) служат перечни ремонтных работ и установленные средние нормы трудозатрат. На основе этой информации формируются локальные таблицы, регламентирующие затраты на все виды ремонтов (текущий, средний, капитальный) для каждого образца техники. Критическим ограничением при этом выступают предельные сроки ремонта. Таким образом, оптимизация времени восстановления ТС и АСУ заключается в таком рациональном планировании технологических операций, которое одновременно удовлетворяет этим нормативным требованиям, которое должно обеспечивать [4]:

- сбалансированное распределение трудозатрат между рабочими местами и ремонтными участками;
- параллельное выполнение работ в пределах одного участка и между различными участками.

Следует отметить, что показатель трудоемкости отражает лишь объем трудозатрат в человеко-часах, но не определяет фактическую продолжительность восстановительного процесса. Временные параметры выполнения ремонтных работ непосредственно характеризуются продолжительностью циклов соответствующих видов ремонта – текущего, среднего и капитального.

Продолжительность цикла восстановления ТС и АСУ формируется под влиянием двух ключевых факторов: оптимальной последовательности операций и совокупной трудоемкости работ. Эти параметры рассчитываются для каждого рабочего места, ремонтного участка и ППТО в целом на основе анализа кратчайшего технологического маршрута при стандартных условиях выполнения операций одним специалистом на единице оборудования. Следовательно, цикл ремонта на j -м месте $t_{црj}$ равен [2]:

$$t_{црj} = \sum_{\xi=1}^{z_{ро}^{кп}} t_{ро\xi}.$$

Параметр $z_{ро}^{кп}$ – число операций, входящих в минимальный по продолжительности технологический маршрут на рабочем месте, а $t_{ро\xi}$ – время выполнения ξ -й операции из этого маршрута.

Оптимальная технология ремонта требует согласования: номенклатура работ $z_{ро}^{кп}$, выполняемых одним человеком, должна быть идентична набору операций кратчайшего пути $z_{ро}^{кп}$. Если на рабочем месте с индексом j -м задействовано $N_{ремj}$ ремонтников, то цикл ремонта для этого места вычисляется по формуле

$$t_{црj} = \frac{t_{трj}}{N_{ремj}},$$

где $t_{трj}$ – трудоёмкость ремонта на j -м рабочем месте.

Следовательно, длительность цикла проведения текущего, среднего или капитального ремонта для указанного типа техники вычисляется по формуле [2]:

$$T_{тск} = \sum_{i=1}^l t_{црi} = \sum_{i=1}^l \sum_{j=1}^{z_{рм}} \frac{t_{трj}}{N_{ремj}},$$

где $z_{рм}$ – количество рабочих мест, задействованных на j -м ремонтном участке; l – общее число технологических участков, специализирующихся на ремонте данного типа ТС и АСУ в рамках рассматриваемого подразделения (бригады, цеха, органа).

Индексы t , c , k рассчитываются, соответственно, для текущего ($T_{цр}^t$), среднего ($T_{цр}^c$) и капитального ($T_{цр}^k$) ремонтов [2].

Продолжительность ремонтного цикла ТС и АСУ является ключевым показателем, определяющим период неработоспособности техники. Величина $T_{рц}$ служит интегральной технической характеристикой, отражающей эффективность как отдельной ремонтной ячейки, так и всей системы восстановления ППТО в целом.

Нормативы продолжительности циклов для всех видов ремонтов (текущего, среднего и капитального) устанавливаются на основе:

- экспериментальных данных, полученных методом хронометража технологических операций;
- статистического анализа производственных показателей действующих ремонтных мастерских ППТО объединения.

Данный подход обеспечивает формирование объективных временных нормативов, соответствующих реальным производственным возможностям ремонтных подразделений. Расчет требуемой численности ремонтного персонала для i -й ремонтной ячейки осуществляется на основе интегрального учета двух ключевых параметров: нормативной трудоемкости и плановой

продолжительности ремонтного цикла, что выражается следующей зависимостью:

$$N_{\text{рем } i} = \sum_{j=1}^{Z_{\text{рм}}} N_{\text{рем } j} = \sum_{j=1}^{Z_{\text{рм}}} \frac{t_{\text{тр } j}}{t_{\text{тц } j}},$$

где $j = 1, 2, 3, \dots, Z_{\text{рм}}$ – число рабочих мест в ремонтной ячейке; $N_{\text{рем } j}$ – число рабочих в j -м рабочем месте.

Общее число ремонтников на ППТО определяется по формуле:

$$N_{\text{ремППТО}} = \sum_{i=1}^l N_{\text{рем } i},$$

где $i = 1, 2, 3, \dots, l$ – число ремонтных ячеек [2].

На основании сформированных номенклатур работ для текущего, среднего и капитального ремонтов определяются ключевые параметры процесса восстановления технических средств, представленные в таблице 3.

Таким образом, качество и полнота разработки ремонтных перечней определяют эффективность всей системы восстановления ТС и АСУ. Данные перечни служат базисом для организации ремонтного производства, расчета производственных мощностей и оптимизации работы ремонтных ячеек ППТО.

Предложения по совершенствованию функционирования склада средств связи в составе ППТО

В современных условиях, характеризующихся высокой динамичностью операций, на первый

план выходит требование к минимизации сроков доведения материальных средств до войск. Одним из основных способов выполнения этого требования является технологическая модернизация процессов планирования и обеспечения, обусловленная общим трендом на технологизацию военной сферы.

Анализ опыта Специальной военной операции демонстрирует значительное расширение номенклатуры применяемых ТС и АСУ. В настоящее время парк техники воинских формирований включает не только штатные образцы военного назначения, но и средства связи двойного применения. Указанная тенденция, усугубляемая возрастающей интенсивностью информационного обмена в системах управления, приводит к постоянному росту номенклатурного перечня средств связи.

Достаточно сложным является процесс объективного непрерывного учета наличия и состояния ТС и АСУ, находящихся в войсках и на складах всех уровней, в режиме реального времени.

Организация обеспечения войск ТС и АСУ характеризуется высокой вероятностью ошибок, обусловленных человеческим фактором. Практика современных боевых действий подтверждает, что оперативность и обоснованность управленческих решений должностных лиц ТОС и АСУ, наряду с эффективной работой системы учета, являются критически важными факторами для:

Таблица 3.

Ключевые параметры процесса восстановления техники, определяемые на основе сформированных перечней работ

№	Ключевой параметр	Содержательное описание параметра
1	Трудоёмкость восстановления	Суммарная временная оценка, необходимая для выполнения полного комплекса восстановительных операций.
2	Материально-техническая база	Номенклатурный перечень требуемого оборудования, контрольно-измерительной аппаратуры, технологической оснастки, инструмента и запасных частей.
3	Технология восстановления	Обоснованная последовательность и методы выполнения ремонтных операций.
4	Длительность ремонтного цикла	Нормативная продолжительность полного цикла восстановления единицы техники.
5	Нормирование труда	Установленные нормы выработки для различных категорий ремонтного персонала.
6	Производственная интенсивность	Показатель, характеризующий мощность восстановительного потока по видам ремонтов.
7	Кадровый потенциал	Перечень требуемых специальностей, уровень их квалификации и расчетная производительность труда.

- бесперебойного снабжения соединений техническими средствами;
- устойчивого функционирования систем связи войсковых формирований.

Сложившаяся ситуация требует разработки комплексных мер по совершенствованию системы ТОС и АСУ, включая:

- внедрение автоматизированных систем поддержки принятия решений;
- создание защищенных от человеческих ошибок учетных механизмов;
- разработку стандартизированных процедур управления снабжением.

Данные меры позволят минимизировать риски сбоев в системе обеспечения и повысить устойчивость управления войсками в современных операциях.

В настоящее время существует огромное количество современных технологий, которые помогут оптимизировать организацию учета и снабжения ТС и АСУ. В рамках использования новых подходов к обработке информации и снижению рисков, связанных с ошибками личного состава, внедрение QR-кодов позволит повысить эффективность процессов учёта и снабжения за счёт автоматизации идентификации и отслеживания ТС и АСУ [5].

QR-код (от англ. Quick Response code – «быстрый отклик») – представляет собой матричный двумерный штрихкод, состоящий из чёрных модулей, расположенных в квадратной сетке на белом фоне. Он предназначен для быстрого считывания и декодирования информации с помощью фотокамер или специализированных сканеров.

В данном случае применение QR-кодов открывает возможности для:

- идентификации ТС и АСУ путём маркировки уникальными кодами, содержащими полные данные о характеристиках, истории эксплуатации и ссылки на документацию;
- автоматизации учёта за счёт мгновенного считывания кодов мобильными устройствами

для получения актуальной информации о ТС и АСУ (принадлежность к воинской части и материально ответственному лицу, количество и состояние экземпляров);

- мониторинга технического состояния ТС и АСУ и прослеживаемости цепочки поставок через интеграцию с блокчейн-технологиями, где каждый QR-код служит криптографическим хэшем для фиксации этапов жизненного цикла ТС и АСУ [5].

В общем случае создание единого реестра графических кодов обеспечивает сквозную прослеживаемость всех ТС и АСУ от производства до боевого применения, исключая ошибки учёта и несанкционированные изменения данных.

Заключение

Проведенное исследование позволило разработать подходы к повышению эффективности функционирования ППТО – важнейшего элемента системы ТОС и АСУ в условиях современных операций. Внедрение научно обоснованной методики расчета количественного и качественного состава ремонтных ячеек позволит существенно повысить возможности ППТО в области восстановления ТС и АСУ, вышедших из строя вследствие боевых повреждений и технических отказов.

Внедрение QR-кодов и единой системы базы данных складов средств связи в рамках системы ТОС и АСУ позволит совершенствовать процессы обеспечения войск. Мгновенное сканирование QR-кодов обеспечит достоверный мониторинг наличия и перемещения ТС и АСУ во всех звеньях управления в реальном масштабе времени, что позволит сократить временные затраты, минимизировать ошибки ручного ввода данных и уменьшить потребность в привлечении личного состава для выполнения логистических операций.

Таким образом, предложенные подходы имеют потенциал для значительного повышения эффективности ТОС и АСУ в условиях современных операций.

Литература

1. Дросс В. А., Фатьянова Е. В., Губская О. А. [и др.] Определение рационального количества личного состава для обслуживания и ремонта техники связи и АСУ // Известия Тульского государственного университета. Технические науки, 2022. – № 7. – С. 108–111. – DOI: 10.24412/2071-6168-2022-7-108-112.
2. Родионов Ю. В., Ломовских А. Е., Свиридов А. А., Январёв В. С., Север А. В., Рыбин Г. В. Методы определения количества и состава ремонтных бригад при восстановлении техники // Наука в Центральной России, 2023. – Т. 66. – № 6. – С. 123–134.
3. Ломовских А. Е., Томилов А. А., Баглаев А. А. Способ повышения технической готовности машин // Специальные вопросы моделирования систем и процессов, 2021. – С. 54–63.
4. Кравченко И. Н., Корнеев В. М., Захарова М. С., Ахметов Т. А. Методика выбора критериев оптимизации при формировании машинно-тракторных парков // Вестник Московского государственного агроинженерного университета им. В. П. Горячкина, 2016. – № 4 (74). – С. 41–46.

5. Курочка В. С., Бурлаков А. А., Ковалев В. В., Николаев В. Б. Пути совершенствования системы технического обеспечения связи и автоматизированных систем управления воинских формирований с использованием технологий блокчейн и QR-кодов в условиях современных операций // Вопросы оборонной техники. Серия 16: Технические средства противодействия терроризму, 2025. – № 3–4 (201–202). – С. 93–100.

OPTIMIZATION OF THE FUNCTIONING OF ADVANCED TECHNICAL SUPPORT POINTS AS A FACTOR IN IMPROVING THE EFFICIENCY OF MAINTENANCE OF COMMUNICATION SYSTEMS AND AUTOMATED CONTROL SYSTEMS

Kurochka V. S.⁷, Kolodyazhny P. A.⁸, Yushin A. I.⁹

Keywords: restoration of communication equipment, malfunction, labor intensity, repair cycle, repair intensity, repair planning, warehouses of communication equipment, QR codes.

Abstract

The purpose of the work is to clarify and substantiate an integrated approach to improving the subsystem for restoring associations by optimizing the functioning of the BPHE based on mathematical modeling methods.

Results of the study: the main problems of organizing the restoration of communication equipment and automated control systems (TS and ACS) and methods of their solution in the conditions of modern operations are revealed, and the main technical and economic indicators are used to assess the quality and plan the activities of the repair bodies of associations: labor intensity of types of repairs for specific vehicles and ACS, duration of the repair cycle, intensity of work and the fund of the worker time. Their analytical calculation serves as the basis for assessing the performance of repair cells of advanced technical support points (BPP), determining the required number of such points, their organizational structure and the list of repair operations performed. The substantiation of the use of mathematical modeling methods in order to determine the rational composition of the forces and means of the BPTO of the association, depending on the current operational situation, is given. A scheme for planning repairs at the BPHE is presented. A method is proposed to improve the efficiency of the functioning of communication warehouses from the BPTO through the use of QR code technology. A refined mathematical apparatus has been developed that can be used in the work of officials on TOC and ACS in the course of organizing the functioning of the vehicle and ACS recovery subsystem in modern operations.

Practical usefulness lies in the possibility of using the refined mathematical apparatus separately or as part of an automated control system for technical support of communications and automated control systems (TOS and ACS) as a tool to support decision-making when organizing the restoration of vehicles and automated control systems in the operation and forming a rational version of the composition of the forces and means of the repair bodies of the association.

References

1. Dross V. A., Fat'yanova E. V., Gubskaya O. A. [i dr.] Opredelenie racional'nogo kolichestva lichnogo sostava dlya obsluzhivaniya i remonta tekhniki svyazi i ASU // Izvestiya Tul'skogo gosudarstvennogo universiteta. Tekhnicheskie nauki, 2022. – No 7. – Pp. 108–111. – DOI: 10.24412/2071-6168-2022-7-108-112.
2. Rodionov Yu. V., Lomovskih A. E., Sviridov A. A., Yanvaryov V. S., Sever A. V., Rybin G. V. Metody opredeleniya kolichestva i sostava remontnykh brigad pri vosstanovlenii tekhniki // Nauka v Central'noj Rossii, 2023. – T. 66. – No 6. – Pp. 123–134.
3. Lomovskih A. E., Tomilov A. A., Baglaev A. A. Sposob povysheniya tekhnicheskoy gotovnosti mashin // Special'nye voprosy modelirovaniya sistem i processov, 2021. – Pp. 54–63.
4. Kravchenko I. N., Korneev V. M., Zaharova M. S., Ahmetov T. A. Metodika vybora kriteriev optimizatsii pri formirovani mashinno-traktornykh parkov // Vestnik Moskovskogo gosudarstvennogo agroinzhenernogo universiteta im. V. P. Goryachkina, 2016. – No 4 (74). – Pp. 41–46.
5. Kurochka V. S., Burlakov A. A., Kovalev V. V., Nikolaev V. B. Puti sovershenstvovaniya sistemy tekhnicheskogo obespecheniya svyazi i avtomatizirovannykh sistem upravleniya voinskih formirovaniy s ispol'zovaniem tekhnologii blokcheyn i QR-kodov v usloviyakh sovremennykh operatsiy // Voprosy oboronnoy tekhniki. Seriya 16: Tekhnicheskie sredstva protivodeystviya terrorizmu, 2025. – No 3–4 (201–202). – Pp. 93–100.

⁷ Vladimir S. Kurochka, Ph.D. of Military Sciences, Associate Professor of the Department of the Military Academy of Communications. St. Petersburg, Russia. E-mail: Uprava223@mail.ru

⁸ Petr A. Kolodyazhny, Student of the Military Academy of Communications, St. Petersburg, Russia. E-mail: petr2020.sev@mail.ru

⁹ Alexander I. Yushin, Ph.D. of Technical Sciences, Associate Professor of the Department of the Military Academy of Communications. St. Petersburg, Russia. E-mail: alyushin@yandex.ru

РОЛЬ МАСКИРОВКИ И ИМИТАЦИИ ЭЛЕМЕНТОВ СИСТЕМЫ СВЯЗИ ВОЕННОГО НАЗНАЧЕНИЯ

Агафонов Д. А.¹, Козырев В. В.², Лапин Г. В.³

DOI:10.21681/3034-4050-2026-3-83-88

Ключевые слова: пункт управления, полевой узел связи, радиоэлектронные средства, высокоточное оружие, разведывательно-ударный комплекс, беспилотный летательный аппарат.

Аннотация

Цель исследования заключается в рассмотрении основных путей организации ложных полевых узлов связи пунктов управления и решении задачи определения эффективности применения ложных целей.

Результат: рассмотрены основные мероприятия, применяемые для затруднения разведке выполнения задач по обнаружению и распознаванию объектов связи.

В статье представлены расчетные методы определения технико-экономической целесообразности оснащения ложными макетами элементов системы связи.

В ходе исследования было показано, что комплексные мероприятия по скрытию истинных и созданию ложных элементов полевых узлов связи в районах их размещения позволят осуществить эффективное противодействие средствам технической разведки. При этом убедительность мероприятий имитации достигается лишь при затратах, сопоставимых с затратами на развертывание и оборудование реальных элементов полевых узлов связи.

Практическая ценность заключена в предложенной методике расчета потребного количества макетов в составе штатной структуры частей и подразделений связи для имитации тех или иных реальных пунктов управления исходя из оперативно-тактической рациональности.

1. Введение

Для повышения устойчивости системы связи и ее компонентов требуется комплексный подход, объединяющий организационные и технические меры.

Соккрытие элементов системы и введение противника в заблуждение о ее составе, дислокации и боевых возможностях достигается через повышение маневренности подразделений, маскировку вооружения и техники, оснащение войск средствами имитации боевого порядка и работы средств связи и управления. Элементы системы связи обладают самыми явными демаскирующими признаками, полное устранение которых в настоящее время почти невозможно.

Опыт специальной военной операции показал, что маскировка является одним из важнейших факторов защиты от высокоточного оружия (ВТО), к которому в настоящее время можно отнести и беспилотные летательные аппараты (БПЛА), в том числе и FPV-дроны [1].

Принимая во внимание, что для повышения устойчивости функционирования системы связи и ее элементов необходимо применять комплексный подход, который включает

мероприятия организационного и технического характера [2]:

- создание средств обнаружения ВТО, особенно малогабаритных и низколетящих;
- создание единой системы предупреждения о применении противником ВТО;
- создание многоэшелонированной системы ПВО и ПРО, в том числе и единой системы «малого неба»;
- проведение мероприятий введения противника в заблуждение относительно размещения действующих элементов системы связи и средств связи;
- имитация излучения радиоэлектронных средств;
- наземная оборона подразделений и объектов системы управления и узлов связи в условиях действия наземных сил противника, в том числе диверсионно-разведывательных групп сил специальных операций противника.

Решение задач сокрытия элементов и введения противника в заблуждение относительно ее состава, размещения элементов и их боевых возможностей обеспечивается повышением маневренности подразделений, маскировкой вооружения и военной техники, оснащением

1 Агафонов Дмитрий Алексеевич, начальник научно-исследовательской лаборатории ФГБУ «16 Центральный научно-исследовательский испытательный институт» Минобороны России. Московская область, Мытищи, Россия. E-mail: invisibl78@yandex.ru

2 Козырев Валерий Васильевич, старший научный сотрудник научно-исследовательского отдела ФГБУ «16 Центральный научно-исследовательский испытательный институт» Минобороны России. Московская область, Мытищи, Россия. E-mail: kozirev4646@mail.ru

3 Лапин Григорий Викторович, заместитель начальника научно-исследовательского отдела ФГБУ «16 Центральный научно-исследовательский испытательный институт» Минобороны России. Московская область Мытищи, Россия. E-mail: lapingv@vk.com

войск средствами имитации (как элементов боевого порядка, так и средств имитации работы средств связи, управления и др.) [3]. Эффективное решение этих задач позволяет вывести из-под удара СВН противника часть подразделений (за счет того, что они могут быть не обнаружены в процессе предварительной разведки) и в определенной мере снизить наряды СВН и применяемого ими ВТО на обнаруженные подразделения (за счет перераспределения части наряда СВН на ложные позиции).

Оперативная (тактическая) маскировка является одним из основных видов оперативного (боевого) обеспечения и представляет собой комплекс взаимосвязанных организационных, технических мероприятий и практических действий штабов и войск, проводимых по единому замыслу и плану, направленных на обеспечение скрытности действий войск и обмана противника (введения его в заблуждение) относительно замысла предстоящих действий, наличия, расположения, состояния, боевой готовности и действий войск, а также направлений сосредоточения основных усилий.

Достижение скрытности осуществляется организацией и проведением мероприятий, направленных на предупреждение (исключение) утечки, уничтожения или искажения информации в соответствии с целями и замыслом маскировки.

Введение противника в заблуждение относительно замысла предстоящих действий осуществляется проведением комплекса мероприятий и практических действий по навязыванию ему ложного представления относительно намерений командования и истинного характера деятельности штабов, войск и военных объектов, показом положения, состояния и действий в соответствии с мерами обмана [4].

Мероприятия оперативной (тактической) маскировки должны соответствовать замыслу операции (боевых действий), проводиться непрерывно, активно, комплексно, с учетом возможностей разведки противника (иностранных спецслужб), предельно точно по месту и времени выполнения основных способов и приемов, отличаться разнообразием, убедительностью с учетом экономической целесообразности [5, 6].

Как показывает практика, наилучшая эффективность достигается за счет комплексного применения маскировки от различных видов разведки противника и организацией постоянных мероприятий. Основными способами маскировки являются скрытие, обеспечение режима секретности и безопасности связи и информации, противодействие средствам разведки

противника, демонстративные действия, имитация и дезинформация [5, 6]. Следовательно, имитация, наряду с демонстративными действиями и дезинформацией, является важным способом, обеспечивающим введение противника в заблуждение, которая заключается в воспроизведении демаскирующих признаков, присущих реальной деятельности войск и объектов, путем оборудования ложных районов и объектов, а также создания ложных элементов с учетом радиоэлектронной обстановки с использованием макетов вооружения и военной техники (ВВТ), устройства ложных инженерных сооружений и имитации излучения работающих РЭС.

Анализ литературы [5, 6] и практика войск позволили сформировать группы демаскирующих признаков объектов разведки (ОР), которые характеризуют [3]:

- а) физические свойства вещества ОР (теплопроводность, электропроводность, структура, твердость и т. д.);
- б) физические поля, создаваемые ОР (электромагнитное, акустическое, радиационное, гидроакустическое и т. д.);
- в) форму, цвет, размеры самого ОР и его элементов;
- г) пространственные признаки, характеризующие как координаты ОР в пространстве, так и их производные;
- д) наличие определенных связей в ОР между его элементами;
- е) результаты функционирования ОР (задымленность, запыленность, следы ОР на грунте, разработка грунта, последствия взрывов и стрельбы, загрязнение воды, воздуха, земли продуктами функционирования ОР).

Наиболее распространенными ОР, функционирующими в радиочастотном диапазоне длин волн, являются излучающие в пространство электромагнитные волны РЭС, входящие в состав образцов вооружения, военной и специальной техники (ВВСТ).

Маскировка становится критически важным способом сохранения боеспособности войск, особенно при скрытой передислокации, преодолении водных и наземных преград в условиях возросшей прозрачности поля боя, обусловленной активным применением противником современных средств видовой разведки (рис. 1) [1].

Уже на протяжении десятилетий полевые узлы связи, аппаратные и станции связи, их антенно-мачтовые устройства обладают самыми явными демаскирующими признаками, полное устранение которых в настоящее время почти невозможно (рис. 2).



Рис. 1. Маскировка аппаратных связи

Их скрытие связано с необходимостью применения дополнительного оборудования, сил и средств, которое в некоторых случаях является экономически затратно, например создание и развертывание дополнительных антенных мачт и т.д.

Предлагаемые мероприятия:

1. Использовать малогабаритные переносные средства связи, в том числе в первую очередь излучающие радиоэлектронные каналобразующие средства связи: радиорелейные станции, средства беспроводного широкополосного доступа, комбинированные тропосферные и радиорелейные станции и станции спутниковой связи, каждое из которых должно иметь в своем составе минимум два комплекта антенно-мачтовых устройств на каждый приемопередатчик с резервными высокочастотными фидерами. Мачты к указанному излучающим радиоэлектронным средствам связи также должны быть отдельными, перевозимыми любым транспортом и переносимыми для установки одним или двумя операторами.
2. Аппаратные связи должны не отличаться от боевых машин (базовые шасси должны быть типовыми) и иметь съёмное оборудование связи, при этом излучающие средства

выносить на максимальное расстояние от УС или ПУ.

Важнейшим мероприятием, позволяющим существенно затруднить разведке решение задач по обнаружению и распознаванию узлов (объектов) связи, является специальный показ (имитация и демонстративные действия) демаскирующих признаков, свойственных данному объекту или его состоянию [6]. Другими словами, должен реализовываться принцип, в соответствии с которым разведке надо показывать то, что хочет показать организатор управления и связи.

Имитация в качестве метода маскировки значительно увеличивает устойчивость системы управления и связи в условиях деструктивных воздействий противника, в первую очередь огневых, а также способствует снижению потерь среди соединений, воинских частей и подразделений.

Задача определения эффективности применения ложных целей

Для обеспечения правдоподобности ложных намерений командования, деятельности штабов, войск (сил) и военных объектов создаются ложные ПУ и их УС. Оборудуемые ложные объекты должны правдоподобно воспроизводить основные демаскирующие признаки действительных, в том числе имитировать характерные действия войск (сил), радиоэлектронную обстановку, работу средств связи с вышестоящими, подчиненными взаимодействующими штабами.

Состав средств, выделяемых для имитации ложных элементов системы связи, а также маскирующий обмен сообщениями и сигналами по своему характеру должны полностью соответствовать применяемым реальным средствам управления и связи, а также интенсивностью информационного потока и действиям личного состава по обеспечению их функционирования.

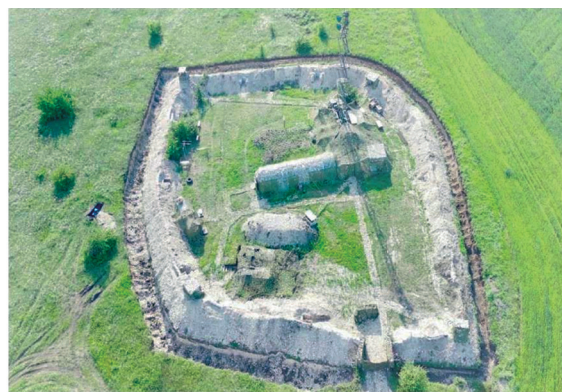
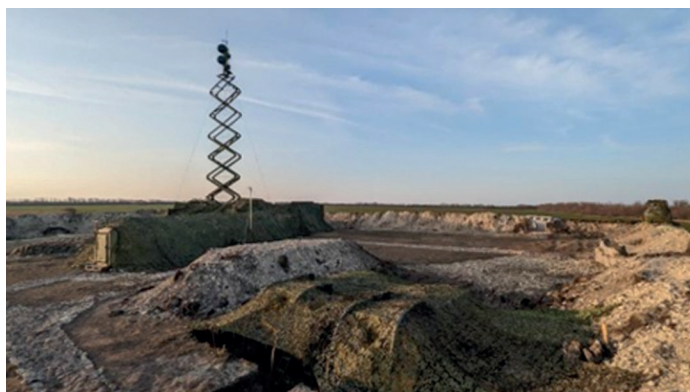


Рис. 2. Маскировка узла связи

Опыт современных конфликтов показывает, что существует возможность обнаружить местоположение, определить уровень и тип ПУ тактического звена или полевого ПУ объединения за 1,5–2 суток, основного ПУ объединения (группировки) – за 3–5 суток и нанести огневое поражение [6, 7].

Поэтому из-за высокой вероятности распознавания ложных элементов полевых узлов связи пунктов управления (ПУС ПУ) они должны осуществлять развертывание в единой системе подготовки пунктов управления как действующие ее элементы.

При этом подразделения, осуществляющие их развертывание, должны осуществлять все мероприятия защиты, скрытия и оборудования без учёта того, что развёртывают ложный элемент системы связи.

Для повышения живучести пунктов управления, находящихся в зоне поражения высокоточным оружием, УС необходимо располагать от группы управления на максимально возможном удалении, позволяющем обеспечить развертывание линий связи абонентской сети и сетей электропитания.

Организационно-техническую структуру ложных ПУС ПУ необходимо формировать с учетом применения излучающих средств, работы средств электроснабжения для создания правдоподобных радио- и тепловых карт объектов. Для этого предлагается использовать оставленные районы размещения ПУ. Для этого используется выведенная из строя техника связи, трофейная автомобильная и другая техника (двойного и гражданского назначения), а для защиты УС ПУ от ВТО применяются тепловые ловушки, уголковые отражатели.

Введение противника в заблуждение возможно путем создания видимости работ деятельности элементов УС и ПУ, которые будут заключаться в маневренных действиях с применением средств имитации и макетов радиоэлектронных средств (РЭС); время их применения должно соответствовать времени аналогичных действий имитируемых РЭС, что обеспечит требуемый уровень правдоподобности и временные интервалы функционирования ложных районов УС ПУ.

Для имитации основных элементов ПУС ПУ необходимо, наряду со штатными РЭС (аппаратными средствами, командно-штабными машинами (КШМ), машинами управления и т.п.), использовать их макеты, не связанные с радиоизлучениями (проводной связи, документального обмена, речевых сообщений и т.п.). При этом соотношение количества первых и вторых должно

определяться требуемой степенью правдоподобия имитации радиоэлектронной обстановки и работы средств связи [7].

С учетом определенных допущений будем полагать, что при выявлении средствами разведки реального ПУС (истинной позиции) на фоне нескольких ложных ПУС (ложной позиции) выход средств ВТО на реальный ПУС обеспечивается с вероятностью $P_{в.ин}$, а при выявлении ложного УС выход ВТО на этот ложный ПУС обеспечивается с вероятностью $P_{в.лп}$.

При количестве ложных позиций N_l полную группу событий можно записать следующим образом:

$$P_{в.ин} + N_l P_{в.лп} = 1. \quad (1)$$

Если все ложные позиции схожи с реальной позицией по внешним размерам, конфигурации, составу радиотехнических средств и излучательным характеристикам, то вероятности $P_{в.ин}$ и $P_{в.лп}$ можно считать равными. В таком случае вероятность $P_{в.ин}$ выхода средств воздушной тактики на истинную позицию с учетом наличия в данной области N_l ложных позиций рассчитывается по следующей формуле:

$$P_{в.ин} = \frac{1}{1 + N_l} \quad (2)$$

При вероятности поражения высокоточными боеприпасами объектов реального (функционирующего) УС $P_{вмо.ин}$ вероятность уничтожения этого ПУС при одном ударе ВТО $P_{ун.ин}$ с учетом выражения (2) будет определяться по формуле:

$$P_{ун.ин} = P_{вмо.ин} \frac{1}{1 + N_l} \quad (3)$$

Результаты расчетов, проведенных с использованием изложенного подхода, для различных значений $N_l P_{вмо.ин}$ приведены на графике (рис. 3).

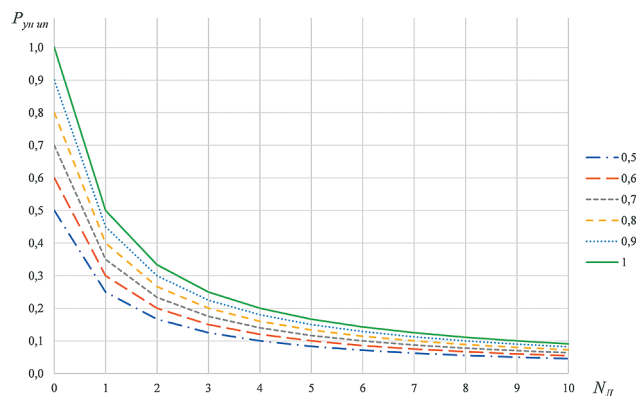


Рис. 3. График зависимости вероятности уничтожения ПУС от количества ложных позиций N_l

Расчеты показывают, что для обеспечения требуемой устойчивости функционирования действующего ПУС необходимо иметь не менее двух ложных. При этом данные позиции по своим внешним размерам, конфигурации, составу РЭС ложного ПУ, их излучательным (отражательным) свойствам должны быть идентичны реальным ПУС ПУ.

Поскольку вопросы оборудования и имитации жизнедеятельности ложных УС ПУ необходимо постоянно отрабатывать на тренировках и учениях, то средства имитации данных ПУС должны быть созданы и накоплены заранее.

Технико-экономическая целесообразность оснащения макетами ПУС промышленного производства определяется на основе сопоставления суммарных финансовых затрат, связанных с разработкой, производством и последующим содержанием (хранением и эксплуатацией) таких макетов с финансово-экономической оценкой разницы предполагаемого ущерба элементам ПУС в случае удара с применением средств ВТО при отсутствии макетов РЭС промышленного производства на ложных позициях.

Убедительность мероприятий имитации достигается лишь при затратах, сопоставимых с затратами на развертывание и оборудование реальных элементов системы связи.

Районы развертывания ложных ПУС необходимо оборудовать с таким расчетом, чтобы их можно было обнаружить и принять за действительные (рис. 4).

В составе ложных ПУС необходимо:

- широко использовать мобильные (переносные) средства связи (радиостанции, коммутаторы, планшеты и другие) во всех уровнях управления, которые менее подвержены деструктивному воздействию;
- использовать макеты со строгими, правильными формами и очертаниями реальных объектов связи и технического обеспечения;
- обеспечивать установку и функционирование макетов источников электроэнергии (станций электроснабжения), имеющих инфракрасное и акустическое излучение, заметно превышающее естественный фон;

- осуществлять имитацию кабельной и беспроводной распределительной сети между имитируемыми элементами УС;
- обеспечить изменение газового состава естественного фона местности для имитации жизнедеятельности объектов ложного УС.



Рис. 4. Применение военных объектов для развертывания ложных УС ПУ

При имитации элементов УС должна обеспечиваться высокая степень правдоподобия радиоэлектронной обстановки и работы средств связи.

Выводы

Опыт специальной военной операции и проведенные многочисленные учения последнего десятилетия показали, что маскировка должна осуществляться комплексно, по единому замыслу и плану с применением средств имитации и скрытия. Маскировка должна осуществляться постоянно, так как имеющиеся в настоящее время технические средства видовой разведки позволяют в короткие сроки идентифицировать элемент УС, средства связи. Должны проводиться мероприятия по организации маскирующего обмена сообщениями и сигналами, которые по своему характеру полностью соответствуют реальному.

Наличие штатных сил и средств маскировки позволит существенно повысить разведзащищенность элементов УС и ПУ.

Литература

1. Костарев С. В., Воробьев И. Г. Современные подходы к обеспечению разведывательной защищенности и живучести системы связи объединения в операциях (боевых действиях) // Военная мысль. – 2019. – № 11.
2. Иванов В. Г. Основы построения и оценки эффективности функционирования системы связи специального назначения в международном вооруженном конфликте на основе многосферной и конвергентной структуры ее элементов: Монография. – СПб.: ПОЛИТЕХ, 2023. – 298 с.
3. Макаренко С. И. Модели системы связи в условиях преднамеренных дестабилизирующих воздействий и ведения разведки. Монография. – СПб.: Научное издание, 2020. – 337 с.
4. Вольхин С. Д., Пустошкин М. М. Повышение эффективности применения средств и комплексов связи путем проведения мероприятий по обеспечению живучести // Телекоммуникация и связь. – 2025. – № 4 (7). – С. 52–58. – DOI:10.21681/3034-4050-2025-4-53-58.

5. Тишков В. В., Иванов В. Г., Лукьянчик В. Н. Обоснование облика построения перспективных комплексов и средств связи на основе опыта организации связи при проведении специальной военной операции // Военная мысль. – 2023. – № 9.
6. 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. – 304 с.
7. Белов А. В., Карапузов А. Н., Панкин А. А., Курочкин П. В., Кузин П. И. Моделирование состояния защиты информационных объектов // Известия Высшей военной школы Генерального штаба Вооружённых сил Республики Ангола. – 2025. – № 3. – С. 46–52.
8. Падишин С. А., Вольхин С. Д. Повышение живучести элементов системы связи группировки войск при выполнении мероприятий боевого обеспечения войск связи // Телекоммуникации и связь. – 2026. – № 1 (10). – С. 81–89. – DOI:10.21681/3034-4050-2026-1-81-89.

THE ROLE OF MASKING AND IMITATION OF ELEMENTS MILITARY COMMUNICATION SYSTEMS

Agafonov D. A.⁴, Kozyrev V. V.⁵, Lapin G. V.⁶

Keywords: command post, field communication center, radio-electronic means, high-precision weapons, reconnaissance and strike complex, unmanned aerial vehicle.

Abstract

The purpose of the research is to consider the main ways of organizing false field communication centers of command posts and to solve the problem of determining the effectiveness of the use of false targets.

Result: the main measures used to complicate the reconnaissance of the tasks of detecting and recognizing communication objects are considered.

The article presents calculation methods for determining the technical and economic feasibility of equipping communication system elements with false layouts.

In the course of the study, it was shown that comprehensive measures to conceal the true and create false elements of field communication centers in the areas of their deployment will make it possible to effectively counteract technical reconnaissance means. At the same time, the persuasiveness of simulation measures is achieved only at costs comparable to the costs of deploying and equipping real elements of field communication centers.

The practical value lies in the proposed methodology for calculating the required number of mock-ups as part of the standard structure of communication units and subdivisions to simulate certain real command posts based on operational and tactical rationality.

References

1. Kostarev S. V., Vorob'yov I. G. Sovremennye podhody k obespecheniyu razvedyvatel'noj zashchishchennosti i zhivuchesti sistemy svyazi ob'edineniya v operatsiyah (boevykh dejstviyakh) // Voennaya mysl'. – 2019. – No 11.
2. Ivanov V. G. Osnovy postroeniya i ocenki ehffektivnosti funkcionirovaniya sistemy svyazi special'nogo naznacheniya v mezhdunarodnom vooruzhennom konflikte na osnove mnogosfernoj i konvergentnoj struktury ee ehlementov: Monografiya. – SPb.: POLITEH, 2023. – 298 p.
3. Makarenko S. I. Modeli sistemy svyazi v usloviyah prednamerennyh destabiliziruyushchih vozdeystvij i vedeniya razvedki. Monografiya. – SPb.: Naukoemkie tehnologii, 2020. – 337 p.
4. Vol'hin S. D., Pustoshkin M. M. Povyshenie ehffektivnosti primeneniya sredstv i kompleksov svyazi putem provedeniya meropriyatij po obespecheniyu zhivuchesti // Telekommunikacii i svyaz'. – 2025. – № 4 (7). – Pp. 52–58. – DOI:10.21681/3034-4050-2025-4-53-58.
5. Tishkov V. V., Ivanov V. G., Luk'yanchik V. N. Obosnovanie oblika postroeniya perspektivnykh kompleksov i sredstv svyazi na osnove opyta organizatsii svyazi pri provedenii special'noj voennoj operatsii // Voennaya mysl'. – 2023. – № 9.
6. Ivanov V. G. Teoriya i praktika postroeniya i obespecheniya funkcionirovaniya sistemy svyazi special'nogo naznacheniya s uchotom tehnologicheskogo razvitiya i opytov vooruzhennykh konfliktov: monografiya – M.: Krasnaya Zvezda, 2025. – 304 p.
7. Belov A. V., Karapuzov A. N., Pankin A. A., Kurochkin P. V., Kuzin P. I. Modelirovanie sostoyaniya zashchity informacionnykh ob'ektov. // Izvestiya Vyshej voennoj shkoly General'nogo shtaba Vooruzhennykh sil Respubliki Angola. – 2025. – No 3. – Pp. 46–52.
8. Padishin S. A., Vol'hin S. D. Povyshenie zhivuchesti ehlementov sistemy svyazi gruppirovki vojsk pri vypolnenii meropriyatij boevogo obespecheniya vojsk svyazi // Telekommunikacii i svyaz'. – 2026. – No 1 (10). – Pp. 81–89. – DOI:10.21681/3034-4050-2026-1-81-89.

4 **Dmitry A. Agafonov**, Head of the Research Laboratory of the 16th Central Research and Testing Institute of the Ministry of Defense of the Russian Federation. Moscow Region, Mytishchi, Russia. E-mail: invisibl78@yandex.ru

5 **Valery V. Kozyrev**, Senior Researcher, Research Department, Federal State Budgetary Institution «16 Central Research and Testing Institute» of the Ministry of Defense of the Russian Federation. Moscow Region, Mytishchi, Russia. E-mail: kozirev4646@mail.ru

6 **Grigory V. Lapin**, Deputy Head of the Research Department of the Federal State Budgetary Institution «16 Central Research and Testing Institute» of the Ministry of Defense of Russia, Moscow Region, Mytishchi, Russia. E-mail: lapingv@vk.com

ОЦЕНКА РАБОТЫ ВОЕННО-ПОЛЕВЫХ СРЕДСТВ ПРОВОДНОЙ СВЯЗИ В ГОДЫ ВЕЛИКОЙ ОТЕЧЕСТВЕННОЙ ВОЙНЫ

Шептура В. Н.¹

DOI:10.21681/3034-4050-2026-3-89-99

Ключевые слова: военная связь, средства проводной связи, Главное управление связи Красной армии.

Аннотация

Цель: обобщение исторического опыта изучения эксплуатации военно-полевых средств проводной связи в годы Великой Отечественной войны и формулирование выводов и предложений по его использованию в современных условиях.

Метод исследования: историко-генетический, предполагает последовательное изучение исторических фактов, их обобщение и выработку практических предложений и рекомендаций, актуальных для современного процесса развития системы и войск связи.

Результаты исследования: рассмотрен опыт эксплуатации средств проводной связи в годы Великой Отечественной войны. На основе материалов архивных источников в публикации раскрываются формы и способы работы межведомственной комиссии Главного управления связи Красной армии и предприятий промышленности в 1-м Украинском фронте. Обобщен опыт работы межведомственной комиссии по изучению опыта эксплуатации военно-полевых средств проводной связи в действующей армии и на его основе формирование практических рекомендаций по совершенствованию промышленного производства изделий и боевого применения войск связи.

Научная новизна материала заключается в том, что на основе новых архивных материалов о работе межведомственной комиссии Главного управления связи Красной армии и предприятий промышленности непосредственно в действующей армии проведено их обобщение и выработаны актуальные предложения для организации работы органов управления связью, научно-исследовательских организаций и предприятий оборонно-промышленного комплекса в зонах боевых действий.

Введение

В годы Великой Отечественной войны войсками связи был накоплен богатый практический опыт организации связи и применения средств связи для обеспечения управления войсками в боевых условиях. В третьем периоде войны Главным управлением связи Красной армии (ГУСКА) совместно с заинтересованными народными комиссариатами, прежде всего Наркоматом электропромышленности (НКЭП), была создана и апробирована на практике стройная система изучения опыта войск связи непосредственно в действующей армии [1, 9]. Одной из форм функционирования данной системы являлось направление в действующую армию комиссий по изучению опыта эксплуатации в войсках различных типов средств связи. По результатам работы комиссий ГУСКА вырабатывались предложения по применению средств связи, улучшению качественных характеристик эксплуатируемых технических изделий и организации разработки новых образцов техники связи [2, С. 325].

Так, приказом ГУСКА и НКЭП от 20/26 октября 1944 г. № 0119/3-590 была создана межведомственная комиссия по изучению опыта

эксплуатации военно-полевых проводных средств связи и оценки их работы в действующей армии (рис. 1)².

Совместным приказом определялся следующий состав комиссии: председатель – главный инженер Научно-испытательного института связи Красной армии (НИИС КА) по проводным средствам связи инженер-полковник Растокин И. М. (рис. 2), заместитель председателя – начальник 3 отдела 3 управления ГУСКА инженер-подполковник Старобинец Г. С., члены комиссии: начальник 2 отдела 1 управления ГУСКА полковник Мурашко В. В., начальник 2 отдела НИИС КА инженер-подполковник Маримонт Л. Б., главный конструктор завода № 1 НКО инженер-капитан Решетов К. А., начальник технического отдела 3 Главного управления НКЭП инженер-подполковник Голубцов И. Е., главный технолог завода № 681 НКЭП Горшков, начальник лаборатории ГСПЭИ-56³ НКЭП Альтерман⁴, старший инженер ГСПЭИ-56 НКЭП Федорович В. Н. и главный конструктор завода № 707 НКСП⁵ Судаков П. А.

² Центральный архив Министерства обороны Российской Федерации (ЦАМО РФ). Ф. 71. Оп. 12173. Д. 685. Л. 132–134.

³ Государственный союзный производственно-экспериментальный институт № 56.

⁴ Непосредственно после издания приказа № 0119/3-590 НКЭП в состав комиссии был введен старший инженер ГСПЭИ-56 НКЭП Стипаков И. С. вместо начальника лаборатории ГСПЭИ-56 НКЭП Альтермана.

⁵ Наркомат судостроительной промышленности.

¹ 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. Москва, Россия. E-mail: sheptura_vn@mail.ru

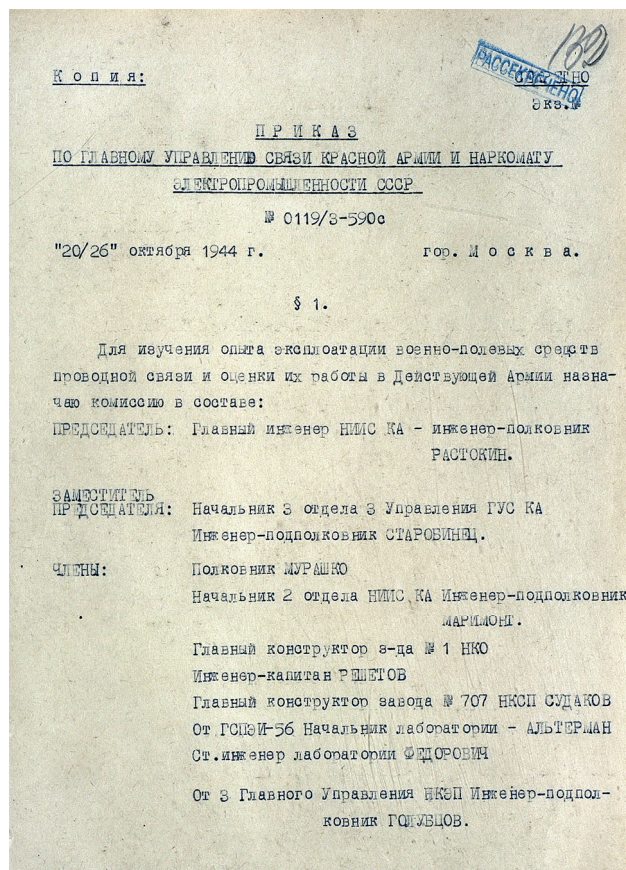


Рис. 1. Приказ ГУСКА и НКЭП от 20/26 октября 1944 г. №0119/3-590. ЦАМО РФ. Ф. 71. Оп. 12173. Д. 685. Л. 132–134



Рис. 2. Инженер-полковник Растокин И. М.

Маршал войск связи И. Т. Пересыпкин отдельным приказанием установил место поездки комиссии – 1-й Украинский фронт (рис. 3)⁶.

⁶ Центральный архив Министерства обороны Российской Федерации (ЦАМО РФ). Ф. 71. Оп. 12173. Д. 684. Л. 3.



Рис. 3. Маршал войск связи И. Т. Пересыпкин

Перед комиссией были поставлены следующие основные задачи:

- определить соответствие средств и имущества проводной связи требованиям организации связи и эксплуатации в сетях воинских частей и соединений;
- установить недостатки важнейших типов аппаратуры и имущества проводной связи, выявленные в процессе ее эксплуатации, а также на основе имеющихся отзывов, рекламаций и результатов испытаний;
- дать рекомендации по модернизации аппаратуры и имущества проводной связи и по разработке новых образцов, а также подготовить предложения о снятии со снабжения аппаратуры связи, технически устаревшей и не удовлетворяющей по своим тактико-техническим данным современным эксплуатационным требованиям.

В своей работе комиссии надлежало произвести осмотр на фронте аппаратуры и имущества проводных средств связи, собрать и изучить необходимые материалы войсковых частей и соединений, отзывы и рекламации, поступившие в ГУСКА и НИИС КА, провести необходимые измерения и испытания аппаратуры и линий связи и на основе всего этого дать обоснованную оценку каждого типа аппаратуры и имущества проводных средств связи.

Для обеспечения проведения на фронте необходимых испытаний и измерений, а также для передвижения членов комиссии, НИИС КА были выделены две подвижные лаборатории с минимально необходимой измерительной и испытательной аппаратурой. Одна лаборатория была оборудована в спецкузове, установленном на автомашине «Студебекер», а вторая –

на автомашине «Додж». В распоряжении председателя комиссии имелась автомашина «Виллис».

Организация работы комиссии

К работе комиссия приступила немедленно по получении приказа. В организационном плане ее деятельность по выполнению поставленных задач можно разделить на пять этапов.

Первый этап (с 27 октября по 5 ноября 1944 г.) – осуществлялось формирование комиссии, составлялись подробные перечни ее работы, уточнялись сведения о технических параметрах аппаратуры и имущества, подлежащих обследованию, также проводились подготовительные мероприятия по материально-техническому обеспечению выезда комиссии в войска 1-го Украинского фронта. Также в это время проводилась подготовка автомашин лаборатории и отправка их на фронт.

На **втором этапе** (с 5 ноября по 14 ноября 1944 г.) – был составлен подробный вопросник по оценке работы проводных средств связи и направлен начальникам управлений связи всех фронтов, произведена выборка основных норм и требований из технических условий на изделия, разработан подробный план работы комиссии на фронте и перечни вопросов для каждого члена комиссии по детальной проверке и осмотру аппаратуры.

В ходе **третьего этапа** – 14 ноября 1944 г., комиссия выехала на фронт и 19 ноября – прибыла в штаб фронта.

Непосредственная работа в воинских частях и соединениях 1-го Украинского фронта осуществлялась на четвертом этапе – с 19 ноября по 8 декабря 1944 г.

На **завершающем этапе** – состоялся отъезд комиссии из штаба фронта (9 декабря 1944 г.), прибытие в Москву (13 декабря), обработка материалов и составление отчета – 17 апреля 1945 г.

Для упорядочения работы по сбору и обобщению материалов, а также составления отчета и выводов по результатам работы комиссию разбили на три группы:

1-я группа – телефонных аппаратов, коммутаторов и центральных телефонных станций (ЦТС);

2-я группа – телеграфных аппаратов и военно-телеграфные станции (ВТС);

3-я группа – линейно-кабельных средств, аппаратуры дальней связи и вспомогательного имущества.

Секретарем комиссии был назначен инженер-подполковник Маримонт.

Распределение по группам личного состава комиссии и работников НИИС КА, выезжавших с комиссией на фронт, показано в таблице 1.

В связи с тем, что на 1-м Украинском фронте комиссия обследовала проводные средства связи и изучала опыт их эксплуатации в войсках связи двух армий, комиссия была разделена на две части: одна часть членов комиссии проводила работу в 13-й армии, а другая часть – в 60-й армии.

Группу членов комиссии, выезжавшую в 13-ю армию, возглавлял заместитель председателя комиссии инженер-подполковник Старобинец Г. С. В состав этой группы входили: инженер-подполковник Голубцов, инженер-майор Климов, инженер-майор Репина, старший техник-лейтенант Пшенин, инженер Горшков. Группу для работы в 60-й армии возглавлял полковник Мурашко В. В. В составе этой группы находились: инженер-подполковник Маримонт, инженер-капитан Решетов, инженер Федорович, инженер Судаков.

Инженер Стипаков И. С. все время находился в штабе фронта, на узле связи которого производил измерения и испытания воздушных и кабельных линий дальней связи. Кроме того, на него было возложено обследование усилителей ТООУ-Д⁷ и выезд на контрольно-измерительный пункт (КИП) № 094 (г. Жешув) для производства установки и пуска в эксплуатацию промежуточных телефонных усилителей ПНУ-42⁸.

7 Телефонный оконечный усилитель двустороннего действия ТООУ-Д. – М.: Воен. изд-во, 1944. – 16 с.

8 Промежуточный низкочастотный телефонный усилитель ПНУ-42. – М.: Воен. изд-во, 1945. – 32 с.

Таблица 1.

Распределение по группам личного состава комиссии и работников НИИС КА

Группа	Руководитель	Члены
№ 1	Инженер-подполковник Голубцов	Инженер-капитан Решетов; инженер-майор Репина, инженер Федорович
№ 2	Полковник Мурашко	Инженер-майор Климов, инженер Судаков
№ 3	Инженер-подполковник Маримонт	Старший техник-лейтенант Пшенин, инженер Горшков, инженер Стипаков

За время пребывания на 1-м Украинском фронте комиссия обследовала аппаратуру, имущество и линейно-кабельные сети в следующих штабах, воинских частях и соединениях: штабе фронта; 13-й и 60-й армиях; 15, 24, 28 и 102-м стрелковых корпусах; 181, 395, 302, 107-й стрелковых и 9-й пластунской дивизиях; 271, 714, 823-м стрелковых и 36-м пластуном полках; 865, 909, 575 и 968-м артиллерийских полках; четырех стрелковых батальонах; трех артиллерийских дивизионах.

Изучение и обследование средств связи проводилось путем непосредственного осмотра, проверки действия и проведения измерений технических параметров аппаратуры, имущества и линий на местах, а также путем бесед с офицерами и техническим составом обследуемых подразделений, воинских частей и соединений. При этом беседы проводились членами комиссии и представителями НИИС КА с начальниками связи всех степеней, начальниками узлов связи, начальниками ВТС и ЦТС, командирами батальонов, рот и взводов связи, механиками и техниками телеграфа и телефона, телеграфистками и телефонистками, линейными рабочими и надсмотрщиками.

Кроме того, руководством комиссии и групп был проведен ряд совещаний, позволивших обобщить способы и приемы боевого применения средств связи, вскрыть проблемные вопросы эксплуатации изделий и оказать практическую помощь в их использовании в боевых условиях, в том числе:

- командиров взводов эксплуатационных рот фронтовых воинских частей связи;
- командиров взводов фронтовых строительных воинских частей связи;
- в 102-м стрелковом корпусе с участием начальника связи корпуса, начальников связи трех дивизий, офицерского и технического состава отдельного батальона связи корпуса;
- в 74-м стрелковом корпусе с участием начальника связи корпуса, офицерского и технического состава отдельного батальона связи корпуса;
- в 24-м стрелковом корпусе с участием начальника связи 13-й армии, командования корпуса, начальника связи корпуса, офицерского и технического состава отдельного батальона связи корпуса;
- в 395-й стрелковой дивизии с участием начальников связи дивизии, стрелкового и артиллерийского полков, офицерского и технического состава воинских частей дивизии и полков.

Также комиссией был проведен анализ материалов, поступивших согласно директивному указанию ГУСКА от 11 ноября 1944 г. № 1084236 из Карельского, Ленинградского, 1, 2 и 3-го Прибалтийских, 1, 2 и 3-го Белорусских, 1, 2 и 4-го Украинских фронтов и отдельной Приморской армии. Необходимо отметить, что материалы фронтов поступали в распоряжение комиссии со значительным запозданием. Так, материалы 2-го Украинского фронта прибыли 24 февраля, а 4-го Украинского фронта – 5 марта 1945 г.

Комиссией также были изучены материалы выборочных испытаний аппаратуры, проведенных НИИС КА в 1943 и 1944 гг., рекламации и отзывы войск за 1944 г. [3, С. 55, 56].

Основные результаты работы комиссии

Собранные комиссией сведения по основным видам аппаратуры и имущества проводной связи, а также материалы фронтов, позволили комиссии дать оценку работы изделий, сделать выводы и выработать предложения, в соответствии с задачами, поставленными перед комиссией.

При анализе условий применения и эксплуатации телефонных аппаратов было установлено, что внутренняя телефонная связь в штабах фронтов осуществлялась по двухпроводным, в основном кабельным, линиям. Протяженность абонентских линий в сети внутренней связи фронтов составляла от нескольких метров до 2–5 км. Соединительные линии между подстанциями имели длину от нескольких сот метров до 8–12 км, а в отдельных случаях – до 20 км. Для соединительных линий применялись кабельные, шестовые и редко постоянные линии.

Количество контрольных постов на соединительных линиях между ЦТС и подстанциями обычно не превышало 3–4. При связи между абонентами различных подстанций в телефонном тракте обычно включались: 2 абонентских линии; одна (иногда 2) соединительная линия; 2 (иногда 3) индукторных коммутатора; до 4 (иногда до 5) контрольных телефонных аппарата с индукторным вызовом.

Дальняя телефонная связь в сетях фронтов в обороне осуществлялась по двухпроводным запикаренным цепям⁹. При этом в основном применялись постоянные линии связи со стальным проводом диаметром 3–4 мм, иногда 2,5 мм, нормального типа и со скрещенными проводами. Протяженность линии во фронтовых сетях

⁹ Запикаренная цепь – двухпроводная физическая цепь, уплотненная при помощи дифференциальных трансформаторов Пикара, по которой одновременно могла осуществляться одна телеграфная и одна телефонная связь.

в обороне составляла 40–160 км, при наступлении – могла достигать до 150 км, а в отдельных случаях – до 300 км. Постоянные линии иногда имели вставки шестовой линии протяженностью до 10–15 км.

В ходе наступления, при отставании настройки постоянной воздушной линии от перемещающегося штаба армии, осуществлялось наращивание постоянной линии связи шестовой линией. На второстепенных направлениях и при отсутствии постоянных линий связи применялись однопроводные и двухпроводные шестовые линии. Их максимальная протяженность не превышала 80–100 км.

Дальняя связь в сетях связи фронта осуществлялась по прямым линиям и через КИП. Практика войск показала, что на прямых линиях обычно включалось 2–3 индукторных коммутатора и два трансформатора Пикара. При связи через КИП, в случае использования обходных направлений, количество коммутаторов в телефонном тракте могло достигать до 4–5, а трансформаторов Пикара – 6–8.

Контрольные телефонные аппараты во фронтовых сетях включались на дальних линиях в служебный провод аппаратов СТ-35 или Морзе. Расстояние между контрольно-телефонными станциями (КТС) для различных условий составляло 6–15 км. Обычно число контрольных постов на проводе не превышало 2–4, а в отдельных случаях доходило до 8–10 и даже 12 (Ленинградский фронт). В случае отсутствия служебного провода контрольные посты чаще всего в цепи на постоянной основе не устанавливались, а включались для проверки линий через определенные промежутки времени (1-й Белорусский фронт). На двухпроводных телефонных линиях внутренней сети контрольные аппараты включались через 3–8 км, а их число на одну линию не превышало 3–4.

В сетях внутренней связи фронтов применялись в основном аппараты МБ с индукторным вызовом, а также аппараты ЦБ гражданского

типа. Аппараты АТС получили распространение только на двух фронтах – Карельском и Ленинградском. В отдельных случаях использовались аппараты ЕЕ-8А в режиме ЦБ (2-й Прибалтийский фронт).

Из аппаратов системы МБ наибольшее распространение получили импортные американские аппараты ЕЕ-8А. Эти аппараты обычно устанавливались у наиболее ответственных абонентов.

Аппараты УНА-ФИ применялись не везде и в небольших количествах. Как правило, устанавливались у абонентов внутренней сети, имеющих необходимость в выходе на дальние линии, а также в отдельных случаях использовались в качестве контрольных.

Аппараты УНА-И устанавливались у второстепенных абонентов, имеющих необходимость в использовании дальних оперативными линиями.

Аппараты с фоническим вызовом применялись только на однопроводных линиях связи для контрольной службы.

Комиссия установила, что абонентские аппараты в сети связи фронта устанавливались в большинстве случаев в жилых помещениях и отапливаемых блиндажах. На открытом воздухе аппараты использовались крайне редко (линейные надсмотрщики, посты охраны и т.д.). Относительная влажность в помещениях и блиндажах, согласно проведенных в штабе 1-го Украинского фронта измерений, колебалась от 60 до 97 %. Согласно присланных с различных фронтов материалам пределом нормального разряда элементов питания считалось напряжение 0,8–1,0 вольт.

По отзывам большинства фронтов у командования и крупных оперативных работников (командующий, начальник штаба, начальники отделов, диспетчера в звене воздушный полк – дивизия и т.д.) устанавливались от 4 до 6 телефонных аппаратов. Так, например, у начальника штаба 1-го Украинского фронта были установлены

Таблица 2.

Нагрузка полевых телефонных аппаратов во фронтовых, армейских, корпусных и дивизионных сетях (количество разговоров на аппарат в сутки)

Показатель	Фронт	Армия	Корпус	Дивизия
В обороне	30–60 (отдельные абоненты 75)	15–70 (отдельные абоненты 120)	20–30	12–30 (отдельные абоненты 120)
В наступлении	120–300 (отдельные абоненты 500)	15–90 (отдельные абоненты 210)	50–60	12–25 (отдельные абоненты 120)
Продолжительность разговора, мин.	6–10	3–8 (иногда до 20)	3–10	–

следующие телефонные аппараты: на коммутатор дальней связи; на коммутатор ЦБ; ВЧ; радиобюро; прямой с командующим. На 1, 2 и 3-м Прибалтийских фронтах количество устанавливаемых в одном месте аппаратов не превышало двух (дальняя и внутренняя связь). Данные по нагрузке полевых телефонных аппаратов приведены в таблице 2.

Анализ данных таблицы показывает, что интенсивность применения телефонной связи в ходе боевых действий была достаточно высокой, особенно в наступлении. Вместе с тем многообразие используемых типов различных телефонных аппаратов затрудняло их эксплуатацию и ремонт. Основными недостатками аппаратов отечественного производства являлись: «некультурное» внешнее оформление (изготовление корпуса в виде грубого деревянного ящика); неустойчивость в работе; недостаточный срок службы отдельных деталей (индуктор, микрофон и т.д.);

Комиссия подтвердила, что «принятое ГУСКА решение о ликвидации разнотипности имеющихся на снабжении полевых телефонных аппаратов и ориентация на аппарат с индукторным вызовом как основной тип для всей системы связи Красной армии сверху донизу соответствует требованиям фронтов»¹⁰. В качестве единого аппарата с индукторным вызовом для стрелковых, артиллерийских, танковых и авиационных воинских частей и соединений предлагалось принять аппарат ТАИ-43, который в основном удовлетворял по дальности действия, весу и габаритным размерам требованиям к эксплуатации изделий в боевых условиях.

Результаты обследования и собранные комиссией материалы по 1-му Украинскому фронту, а также материалы, полученные с других фронтов, позволили провести анализ эксплуатации в войсках коммутаторов малой и средней емкости, телеграфных аппаратов СТ-35 и Бодо, телефонно-телеграфных узлов и КИП, линейно-кабельных средств и линий связи.

Так, комиссия установила, что в воинских частях и соединениях действующей армии находилось большое количество разнообразных типов отечественных коммутаторов, а также трофейных немецких коммутаторов различной емкости (табл. 3)¹¹.

Эксплуатация коммутаторов ПК-30 в войсках показала, что при длительном пребывании их в условиях повышенной влажности наблюдается появление переходных разговоров на соседних шнуровых парах, выход из строя коммутаторных шнуров, коррозия громоотводов и ряд других дефектов, не обеспечивающих требуемую надежность, уверенную и устойчивую телефонную связь между абонентами. Поэтому комиссией было указано, что в выпускаемых промышленностью коммутаторах необходимо немедленно повысить эксплуатационную надежность, обратить особое внимание на влагостойкость, качество и срок службы основных полуфабрикатов коммутатора (шнуров, гнезд, штепселей и т.д.), а также устранить имеющиеся производственные дефекты.

Кроме того, комиссией было установлено, что телеграфные аппараты СТ-35 являлись основным типом аппаратуры, обеспечивающей телеграфную связь штабов фронтов между собой,

¹⁰ ЦАМО РФ. Ф. 71. Оп. 12173. Д. 685. Л. 110.

¹¹ ЦАМО РФ. Ф. 71. Оп. 12173. Д. 684. Л. 139.

Таблица 3.

Тактико-эксплуатационные сведения о применении телефонных коммутаторов

Наименование фронта	Центральная телефонная станция		Максимальная протяженность линий, км	
	Количество абонентов внутренней связи	Количество абонентов дальней связи	Внутренней связи	Дальней связи
Карельский	100–140 (ЦБ)	до 100	до 6	130
Ленинградский	100	60	–	80–130
1-й Прибалтийский	до 200 (МБ – 100; Р-60)	60	2–10	150–170
2-й Прибалтийский	100	60	5–6	50–70
3-й Прибалтийский	100 (МБ)	60	3–4	100
1-й Белорусский	100 (ЦБ)	60	–	70–90
3-й Белорусский	100 (МБ)	80	2–5	50–60
1-й Украинский	100–150 (ЦБ)	60	15	35

штаба фронта со штабом воздушной армии и с корпусами выведенными в резерв, штаба армии со штабами корпусов, а также для связей тылов фронта и армии. Так, из обследованных 48 телеграфных аппаратов данного типа на 1-м Украинском фронте все осмотренные аппараты были исправны, причем 33 аппарата работали на действующих связях, а 15 находились в резерве (табл. 4)¹².

По оценке специалистов аппараты СТ-35 показали себя с хорошей стороны, в полевых условиях работали надежно, отличались простотой в обслуживании, имели механическую прочность, обеспечивали требуемую скорость передачи и достаточную пропускную способность. Вместе с тем было отмечено, что начиная с 1942 г. промышленность снизила качество телеграфных аппаратов СТ-35 в сравнении с аппаратами довоенного выпуска. Это приводило к тому, что на узлах связи большое количество времени отводилось на ремонт и регулировку телеграфных аппаратов, выпущенных

¹² ЦАМО РФ. Ф. 71. Оп. 12173. Д. 684. Л. 167.

промышленностью в годы войны. Комиссия рекомендовала заводам повысить качество изготовления как аппаратов СТ-35 в целом, так и их отдельных узлов и деталей, доведя его до уровня мирного времени.

Отмечалось, что аппараты Бодо, как целостная система, на связях от Генерального штаба до штабов фронтов и армий полностью удовлетворяли требованиям эксплуатации как с оперативной, так и с технической точек зрения. Однако на узлах связи штабов фронтов и армий применялись главным образом аппараты Бодо гражданского типа, по своей конструкции не рассчитанные на работу в полевых условиях (табл. 5)¹³. Поэтому аппараты подвергались на месте переделкам и изменениям с целью частичного устранения их основных эксплуатационных недостатков.

В ходе обследования телефонно-телеграфных узлов связи комиссией было установлено, что в их состав входили следующие элементы: кросс; генераторная (в составе агрегатной

¹³ ЦАМО РФ. Ф. 71. Оп. 12173. Д. 684. Л. 145.

Таблица 4.

Распределение телеграфных аппаратов СТ-35 по заводам-изготовителям и годам выпуска (по материалам обследования в 1-ом Украинском фронте)

Завод изготовитель	Общее количество аппаратов	Из них выпуска				
		1940 г.	1941 г.	1942 г.	1943 г.	1944 г.
№ 209 НКСП [4, с. 22, 23]	7	—	7	—	—	—
№ 1 НКЭП (КЭМЗ) [5]	12	6	6	—	—	—
№ 647 НКЭП [4, с. 404]	16	—	—	—	16	—
№ 707 НКСП [4, с. 446, 447]	13	—	—	2	11	—
Итого	48	6	13	2	27	—

Таблица 5.

Количество аппаратов Бодо по отношению к общему числу аппаратов, работающих на узлах связи штабов фронтов

Наименование фронта	Удельный вес аппаратов Бодо, %			
	Гражданского типа	2БДА-40	2БД-2Г	2БДА-43
Карельский	90	—	10	—
Ленинградский	90	10	—	—
1-й Прибалтийский	65	—	35	—
2-й Прибалтийский	70	—	30	—
3-й Прибалтийский	60	—	15	25
1-й Белорусский	65	—	5	30
3-й Белорусский	95	—	—	5
1-й Украинский	80	—	20	—
Итого (в среднем)	75	Менее 5	15	Менее 10

и аккумуляторной); аппаратные Бодо и радио-Бодо, СТ-35, Морзе, переговарная, экспедиция, составляющие ВТС и телефонные станции (дальней и внутренней связи). При этом максимальная емкость узлов связи фронта (1-го Украинского и 3-го Белорусского) составляла 80 проводов (из них телефонно-телеграфных цепей – 30 и 20 проводов соответственно), 20 аппаратов Бодо, 30–35 аппаратов СТ-35 и Морзе, до 100 абонентов дальней связи, 200–250 абонентов внутренней телефонной связи. Время развертывания стационарного узла связи при наличии полностью подготовленных помещений составляло 8–12 часов, а с учетом оборудования помещений и устройства вводов постоянных линий – могло достигать 1,5–2 суток. Для подвижных узлов связи, смонтированных на автомашинах, время развертывания составляло 1,5–2 часа. Время свертывания стационарных узлов – 4–6 часов, подвижных – 1–1,5 часа¹⁴.

Комиссией было указано, что эксплуатацию телефонно-телеграфных узлов связи значительно затрудняло отсутствие типового промышленного коммутационно-соединительного и электропитающего оборудования, а также типовых отечественных бензоэлектрических агрегатов и зарядных станций. Также было обращено внимание на отсутствие типового промышленного коммутационно-соединительного оборудования для КИП, что приводит к усложнению эксплуатации и обслуживания линий проводной связи.

По результатам работы комиссия сделала ряд общих выводов.

Опыт применения проводной связи в действующей армии показал, что отечественная аппаратура и имущество проводной связи в основном соответствовали требованиям организации связи, эксплуатации изделий и использовались по прямому назначению. Однако имелись случаи *«оседания наиболее совершенной аппаратуры в высших штабах, что в значительной мере объясняется недостаточным количеством таких средств связи, поступающих в действующую армию (телефонные коммутаторы ПК-10, телеграфные аппараты Бодо полевого типа, вводные многожильные кабели, телефонные аппараты ТАИ-43 и ЕЕ-8А)»*¹⁵.

Отечественная аппаратура, изготовленная в довоенный период, имела вполне удовлетворительное качество, о чем свидетельствовал опыт длительной ее эксплуатации на фронте (телеграфные аппараты Бодо и СТ-35 завода № 209 НКСП, телефонные коммутаторы и аппараты завода «Красная Заря»). Качество

аппаратуры выпуска военного времени, особенно 1942 и 1943 гг., было значительно ниже и не в полной мере соответствовало требованиям эксплуатации в полевых условиях.

Комиссия установила, что военно-полевые кабели отечественного производства вполне удовлетворительны по качеству и не уступали кабелям довоенного выпуска, превосходя по качеству изоляции и оплетки импортные кабели.

В то же время офицеры обращали внимание на то, что войска связи не имели типового коммутационного соединительного оборудования для телеграфных станций и применяли оборудование, изготовленное или приспособленное кустарным образом на местах. Иностранная (импортная) аппаратура – американские телефонные аппараты отличались сравнительно высоким качеством изготовления, «культурным» внешним видом и достаточной устойчивостью в работе. Однако американские полевые кабели имели оплетку и изоляцию низкого качества, вследствие чего срок службы этих кабелей вдвое меньше срока службы кабелей отечественного производства.

Члены комиссии отмечали, что немецкая трофейная аппаратура имела весьма высокое качество изготовления и вполне надежно работала в полевых условиях. Вместе с тем по дальности действия полевые телефонные аппараты F-33 уступали отечественному аппарату ТАИ-43. Кроме того, несмотря на то, что трофейные немецкие полевые одножильные и многожильные кабели в работе зарекомендовали себя удовлетворительно, однако изоляция данных кабелей, изготовленная из пластмассы, со временем теряет гибкость и морозоустойчивость.

По заключению комиссии причинами недостаточно высокого качества отечественной аппаратуры проводной связи являются:

- низкое качество изготовления ряда деталей и узлов телефонной и телеграфной аппаратуры;
- дефекты сборки и регулировки аппаратуры, неправильная технологическая обработка деталей;
- неудовлетворительное качество ряда применяемых материалов, а также несоответствие материалов стандартам;
- низкое качество запасных частей и деталей, входящих в комплект аппаратуры;
- исключительно неудовлетворительное качество микрофонных и коммутаторных шнуров [6].

Вместе с тем члены комиссии отмечали, что разработанные ГУСКА требования действующих технических условий по большинству средств

14 ЦАМО РФ. Ф. 71. Оп. 12173. Д. 685. Л. 4.

15 ЦАМО РФ. Ф. 71. Оп. 12173. Д. 685. Л. 122.

проводной связи обеспечивали надлежащее качество, надежность и длительность действия аппаратуры в полевых условиях. Однако по некоторым средствам связи требования технических условий должны быть повышены (ящики телефонной аппаратуры, пековые изоляторы, катушки для кабеля, вводные кабели).

Опыт эксплуатации проводных средств показал необходимость модернизации телеграфных аппаратов СТ-35 и Бодо, телефонных коммутаторов ПК-30, телефонных аппаратов ТАИ-43, полевых кабелей ПТФ.

Комиссией было указано на крайнюю потребность в войсках связи действующей армии некоторых типов средств связи, образцы которых были разработаны, но серийное производство их не организовано, или крайне ограничено: телеграфные станции для фронтовых и армейских узлов связи (ЛВК 20/12 и кросс ТГСА в автомашинах); столы для транзитных связей; телефонные станции внутренней связи ЦБ-МБ для штабов крупных войсковых соединений; аппаратура дальней связи (установки ВЧ телефонирования, промежуточные и внутренние телефонные усилители); легкие полевые телефонные кабели ЛТФК, вводные кабели ТТФК, кабели питания КПТС; речные кабели ОРТФ и МРК; многожильные кабели ППК-4; линейное соединительное оборудование для узлов связи.

По результатам работы групп комиссии было обращено внимание на то, что опыт обеспечения связи в ходе войны показал необходимость создания новых типов средств проводной связи, в том числе: телеграфных буквопечатающих аппаратов (взамен аппарата Морзе); телеграфных коммутаторов для военно-телеграфных станций штабов корпусов; подвижных узлов связи крупных штабов; коммутационно-соединительного оборудования для КИП фронтовых и армейских сетей; аппаратуры уплотнения линий связи; транспортных средств и средств механизации для прокладки кабеля и повышения темпов строительства воздушных линий и других.

Комиссия предложила прекратить производство для ГУСКА телефонных аппаратов УНА-И, речного кабеля РТГ, деревянных катушек ТК-10 и номерных телефонных аппаратов гражданского образца.

Кроме того, комиссией особо была подчеркнута крайняя разнотипность аппаратуры проводной связи, находившейся в войсках, что затрудняло ее эксплуатацию, ремонт и подготовку обслуживающего персонала. Отмечалось, что аппаратура одного и того же наименования, выпускаемая различными заводами, имела множество не взаимозаменяемых узлов и деталей. Также указывалось на то, что во вновь

разрабатываемой аппаратуре стандартизация основных деталей и полуфабрикатов не предусматривалась. Единого органа, координирующего мероприятия промышленности и институтов нет, а необходимость межведомственной координации и взаимодействия в области стандартизации промышленного производства изделий очевидна. Это приводит к тому, что промышленность НКЭП и других наркоматов весьма медленно осуществляет намеченные мероприятия по повышению качества серийной продукции, крайне неохотно идет на модернизацию существующей аппаратуры, в основном проводя мероприятия, направленные только на упрощение производственного процесса. Разработка новых образцов ведется крайне медленно, а от производства ряда объектов промышленность отказывается в течение целого ряда лет.

В заключении комиссии было отмечено, что за годы войны Красная армия получила значительное количество новой аппаратуры проводной связи, по своим тактико-техническим данным удовлетворяющей требованиям фронта (ТАИ-43, ПК-10, ПК-30, К-10, телеграфные аппараты Бодо полевого типа, армейские трансляции, легкие полевые кабели и др.) [7, с. 146, 147]. В подавляющем большинстве эти средства связи были разработаны при участии НИИС КА и поставлены на серийное производство заводом № 1 НКО. В то же время 3-е управление НКЭП на подведомственных предприятиях освоило в серийном производстве только индукторные коммутаторы малой емкости К-10 и промежуточные усилители ПНУ-42. Исключением являлись заводы 5-го Главного управления НКЭП, создавшие ряд новых образцов линейно-кабельных средств и освоившие их в серийном производстве (ЛТФК, ППК-4, ТТФК, ОРТФ и др.). Несмотря на это, количественный выпуск средств проводной связи не удовлетворял текущей потребности действующей армии, а также не обеспечивал замену устаревших типов аппаратуры. Незначительное количество изготавливаемых индукторных коммутаторов малой емкости не обеспечивало перевод телефонной связи на единую индукторную систему вызова, а выпуск военно-полевых и специальных кабелей не удовлетворял потребности войск связи для развертывания проводных линий связи.

Большинство заводов, в том числе все заводы НКЭП, не изготавливали и не поставляли запасные части к выпускаемой аппаратуре, что создавало в войсках большой парк неисправной аппаратуры, требующей срочного ремонта.

Комиссия поставила вопрос о том, что научно-исследовательская и экспериментальная

база по разработке новой телефонной аппаратуры, средств дальней связи и линейно-кабельных средств в системе НКЭП слаба, а по телеграфной аппаратуре вообще отсутствовала. Для ликвидации этого крайне ненормального положения и обеспечения развития новых типов телефонно-телеграфного оборудования на уровне достижений зарубежной техники необходимо расширение существующего ГСПЭИ-56, Центральной кабельной лаборатории 5-го управления НКЭП, а также создание специализированного центрального бюро по телеграфии с обеспечением его надлежащей экспериментально-производственной базой.

Кроме того, комиссия полагала, что промышленности, производящей проводные средства связи, необходимо в кратчайший срок резко повысить качество выпускаемой продукции, обеспечить поставку изделий в Красную армию в требуемых количествах, внедрить в производство новые проводные средства связи и ускорить разработку опытных образцов аппаратуры.

Заключение

Таким образом, в ходе Великой Отечественной войны ГУСКА осуществлял постоянный поиск действенных форм и способов изучения, анализа и обобщения опыта эксплуатации средств связи в действующей армии. Организация работы межведомственной комиссии ГУСКА и предприятий промышленности на 1-м Украинском фронте позволила в боевых условиях определить степень соответствия средств и имущества проводной связи предъявляемым к ним требованиям, вскрыть эксплуатационные и производственные недостатки выпускаемых промышленностью изделий, а также дать практические рекомендации по совершенствованию аппаратуры и разработке новых образцов проводной связи.

Изучение опыта эксплуатации военно-полевых средств проводной связи и оценки их работы в годы войны в форме направления в действующую армию межведомственных комиссий является весьма актуальным в настоящее время.

Важность этого направления деятельности органов военного управления, подтверждается тем, что 6 марта 2026 г. Президент Российской Федерации провел совещание по вопросам оценки опыта и повышению эффективности использования военной техники в ходе специальной военной операции, на котором поставил задачи по его совершенствованию [8].

Накопленный в годы войны богатый практический опыт создания действенной системы по изучению опыта организации связи и эксплуатации средств связи в действующей армии, в современных условиях позволяет осуществлять постоянный контроль за функционированием системы военной связи, проводить детальный анализ технической эксплуатации средств связи, оперативно распространять в войсках связи передовой опыт по применению телекоммуникационного оборудования, своевременно вырабатывать меры по устранению выявленных недостатков, а также определять перспективные направления развития средств связи и совершенствования тактики боевого применения воинских частей и соединений связи. Особого внимания заслуживают такие способы изучения эксплуатации средств связи в воинских формированиях, как: составление опросных листов специалистов войск связи; осуществление непосредственного осмотра изделий с определением их технической готовности; проверка практических действий расчетов боевых постов на узлах связи по обеспечению связи; проведение необходимых измерений и испытаний аппаратуры и линий связи; проведение бесед с личным составом подразделений, воинских частей и соединений связи.

Рассмотренные в статье подходы по изучению опыта эксплуатации средств проводной связи в боевых условиях могут быть востребованы при организации работы органов управления связью и предприятий промышленности в ходе выполнения задач технического обеспечения связи и автоматизированных систем управления в зоне проведения специальной военной операции.

Литература

1. Шептура В. Н. К вопросу об изучении опыта организации связи и применения средств связи в действующей армии в годы Великой Отечественной войны (1941–1945 гг.) // Вестник Академии Военных наук. – 2025. – № 2. – С. 109–115.
2. Главное управление Связи Вооруженных Сил Российской Федерации: история создания и развития (1919–2019 гг.). – М.: Авиация и спорт, 2019. – 864 с.
3. 16 Центральный научно-исследовательский испытательный ордена Красной Звезды институт им. маршала войск связи А. И. Белова Министерства обороны Российской Федерации: 100 лет исследований, труда и побед, 1923–2023: [военно-исторический труд]. – СПб.: ПМБ, 2023. – 300 с.
4. Тихонов С. Г. Оборонные предприятия СССР и России. В 2 т., Т. 2. – М.: Том, 2010. – 608 с.

5. Оборонпром. Сайт истории оборонных предприятий СССР. – URL: <https://oboron-prom.ru/page,48,predpriyatiya-601-700.html> (дата обращения: 06.03.2026)
6. Ионов В. В., Шептура В. Н. Опыт работы военной приемки по увеличению поставок и обеспечению надежности средств связи в 1944–1945 годах // Вооружение и экономика. – 2025. – № 4 (74). – С. 48–53.
7. Пересыпкин И. Т. Связь СССР в Великой Отечественной войне / И. Т. Пересыпкин; Западный военный округ. – СПб.: ГАЛАРТ, 2014. – 388 с.
8. Сайт Президента России. – URL: <http://www.kremlin.ru/events/president/news/79272> (дата обращения: 06.03.2026).
9. Шептура В. Н. Подвижный узел связи народного комиссариата связи СССР: опыт строительства объекта 04, формирования и применения поезда связи № 1 // Телекоммуникации и Связь. – 2026. – № 1. – С. 96–107. DOI:10.21681/3034-4050-2026-1-96-107.

ASSESSMENT OF THE WORK OF MILITARY FIELD WIRE COMMUNICATION FACILITIES DURING THE GREAT PATRIOTIC WAR

Sheptura V. N.¹⁶

Keywords: military communications, wire communications, the Main Directorate of Communications of the Red Army.

Abstract

Objective: to summarize the historical experience of studying the operation of military field wire communication facilities during the Great Patriotic War and to formulate conclusions and proposals for its use in modern conditions.

The method of research is historical and genetic, which involves 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 of the research: the experience of the operation of wire communication facilities during the Great Patriotic War is considered. On the basis of the materials of archival sources, the publication reveals the forms and methods of work of the interdepartmental commission of the Main Directorate of Communications of the Red Army and industrial enterprises in the 1st Ukrainian Front. study of the experience of operating military field means of wire communication in the field army and, on its basis, the formation of practical recommendations for improving the industrial production of products and the combat use of signal troops.

The scientific novelty of the material lies in the fact that, on the basis of new archival materials on the work of the interdepartmental commission of the Main Directorate of Communications of the Red Army and industrial enterprises directly in the active army, their generalization was carried out and relevant proposals for the organization of the work of communications management bodies, research organizations and enterprises of the military-industrial complex in combat zones were developed.

References

1. Sheptura V. N. K voprosu ob izuchenii opyta organizatsii svyazi i primeneniya sredstv svyazi v dejstvuyushchej armii v gody Velikoj Otechestvennoj vojny (1941–1945 gg.) // Vestnik Akademii Voennyh nauk. – 2025. № 2. – С. 109–115.
2. Glavnoe upravlenie Svyazi Vooruzhennyh Sil Rossijskoj Federatsii: istoriya sozdaniya i razvitiya (1919–2019 gg.). – М.: Aviatsiya i sport, 2019. – 864 s.
3. 16 Central'nyj nauchno-issledovatel'skij ispytatel'nyj ordena Krasnoj Zvezdy institut imeni marshala vojsk svyazi A. I. Belova Ministerstva oborony Rossijskoj Federatsii: 100 let issledovanij, truda i pobed, 1923–2023: [voenno-istoricheskij trud]. – SPb.: PMB, 2023. – 300 s.
4. Tihonov S. G. Oboronnye predpriyatiya SSSR i Rossii. V 2 t., T. 2. – М.: Tom, 2010. 608 s.
5. Оборонпром. Сайт истории оборонных предприятий СССР. – URL: <https://oboron-prom.ru/page,48,predpriyatiya-601-700.html> (дата обращения: 06.03.2026)
6. Ионов В. В., Шептура В. Н. Опыт работы военной приемки по увеличению поставок и обеспечению надежности средств связи в 1944–1945 годах // Вооружение и экономика. – 2025. – № 4 (74). – С. 48–53.
7. Пересыпкин И. Т. Связь СССР в Великой Отечественной войне / И. Т. Пересыпкин; Западный военный округ. – СПб.: ГАЛАРТ, 2014. – 388 с.
8. Сайт Президента России. – URL: <http://www.kremlin.ru/events/president/news/79272> (дата обращения: 06.03.2026).
9. Sheptura V. N. Podvizhnyj uzel svyazi narodnogo komissariata svyazi SSSR: opyt stroitel'stva ob'ekta 04, formirovaniya i primeneniya poezda svyazi № 1 // Telekommunikatsii i Svyaz'. – 2026. – № 1. – Pp. 96–107. – DOI:10.21681/3034-4050-2026-1-96-107.

¹⁶ **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

TELECOMMUNICATIONS and COMMUNICATIONS

SCIENTIFIC PEER-REVIEWED JOURNAL

№ 3 (12) 2026

Published 6 times a year

The journal is registered by the Federal Service for
Supervision of Communications, Information Technology
and Mass Communications.

Registration Certificate
PI № FS77-88069 from 16/08/2024

Editor-in-Chief

Vasily IVANOV, *Dr.Sc., Professor, Moscow*

Assistant Editor-in-Chief

Grigory MAKARENKO, *Senior Research Fellow, Moscow*

Board of Trustees

Alexander RUBIS, *Ph.D., Deputy Head of the Main Directorate
of Communications of the Armed Forces of the Russian Federation
for Armament (Chairman)*

Roman PANKOV, *Ph.D., Head of the Federal State Budgetary
Institution 16 Central Research and Testing Institute*

Evgeny KHARCHENKO, *Ph.D, Ass. Professor (Secretary)*

Editorial Board

Nikolay ACHKASOV, *Dr.Sc., Professor, St. Petersburg*

Anton BYCHKOV, *Dr.Sc., Ass. Professor, St. Petersburg*

Mikhail BUINEVICH, *Dr.Sc., Professor, St. Petersburg*

Evgeny GLUSHANKOV, *Dr.Sc., Professor, St. Petersburg*

Igor GRUDININ, *Dr.Sc., Professor, St. Petersburg*

Sergey IVANOV, *Dr.Sc., Professor, St. Petersburg*

Alexander KOZACHOK, *Dr.Sc., Ass. Professor, Orel*

Andrey KOSTOGRYZOV, *Dr.Sc., Professor, Moscow*

Pavel KUZIN, *Ph.D., Ass. Professor, St. Petersburg*

Sergey MAKARENKO, *Dr.Sc., Professor, St. Petersburg*

Alexey MARKOV, *Dr.Sc., Professor, Moscow*

Evgeny NOVIKOV, *Dr.Sc., Ass. Professor, St. Petersburg*

Andrey PRIVALOV, *Dr.Sc., Professor, St. Petersburg*

Maxim PYLINSKY, *Dr.Sc., Professor, Belarus*

Gennady RYZHOV, *Dr.Sc., Professor, Moscow*

Nikolay SAVISHCHENKO, *Dr.Sc., Professor, St. Petersburg*

Yuriy STARODUBTSEV, *Dr.Sc., Professor, St. Petersburg*

Pavel FEDYUNIN, *Dr.Sc., Professor, Voronezh*

Oleg FINKO, *Dr.Sc., Professor, Krasnodar*

Vladimir TSYMBAL, *Dr.Sc., Professor, Serpukhov*

Mikhail CHERNYSHOV, *Dr.Sc., Professor, St. Petersburg*

Founder and publisher

Federal State Budgetary Institution
«16 Central Research and Testing Institute»
of the Ministry of Defense
of the Russian Federation

Signed to the press on 15/06/2026

The total circulation is 120 copies. The price is free

Postal address: 1st Rupasovsky lane, 1, 141006,
Mytishchi, Moscow region, Russia

E-mail: editor.tis@yandex.ru. Tel.: +7 (985) 939-75-01

The requirements for the manuscripts are posted
on the website: <https://telemil.ru/>

CONTENTS

SYSTEM ANALYSIS OF MILITARY SYSTEMS

STATE AND DIRECTIONS OF DEVELOPMENT OF TROPOSPHERIC COMMUNICATIONS IN THE SYSTEM OF MILITARY COMMUNICATIONS OF THE ARMED FORCES

Ivanov V. G., Lukyanchik V. N., Bashirov S. Y. 2

MATHEMATICAL MODEL OF THE ALGORITHM FOR ADJUSTING THE COEFFICIENTS OF THE ADAPTIVE ANTENNA ARRAY

Tsvetkov D. E., Fedorov P. N. 13

PRINCIPLES OF BUILDING PIPELINES WITH DYNAMIC ARCHITECTURE AND AGENT-BASED MANAGEMENT

Lukashenok V. I., Izotov D. Yu. 21

METHOD OF FIELD VERIFICATION OF EVENTS IN SECURITY CONTROL OF A DISTRIBUTED IOT SUBSYSTEM

Andreev I. A., Lipatnikov V. A., Tarasenko S. E. 29

INFOMATIONAL SYSTEMS

SOFTWARE PACKAGE FOR SEARCHING AND IDENTIFYING SIGNALS FOR SDR BASED ON THE GNU RADIO PLATFORM

Baymakov D. A., Tkachev D. F., Vorobyov P. V. 40

MILITARY CONTROL, COMMUNICATIONS AND NAVIGATION SYSTEMS

ALGORITHMS FOR SIGNAL PROCESSING DURING AIRCRAFT LASER DETECTION

Koziratsky A. Y., Chengin A. V., Grevtsev A. I. 49

OPPORTUNITIES AND PROSPECTS FOR THE USE OF SWARM INTELLIGENCE TECHNOLOGIES IN MILITARY COMMUNICATION SYSTEMS

Yagovitev D. S., Vdovchenko N. Yu. 57

ARCHITECTURE OF AN OPEN AUTOMATIC TELEPHONE NETWORK BUILT USING PEER-TO-PEER TECHNOLOGIES, AND PROPOSALS FOR ITS PROTECTION

Ashlapov M. V., Eliseev D. I. 64

MILITARY ELECTRONICS, EQUIPMENT FOR MILITARY COMPLEXES

DETECTION OF ENEMY DRONES USING SEARCH EQUIPMENT INSTALLED ON DOMESTIC UNMANNED AERIAL VEHICLES

Akhmedov E. M., Asadov Kh. G., Alieva Kh. S. 69

OPTIMIZATION OF THE FUNCTIONING OF ADVANCED TECHNICAL SUPPORT POINTS AS A FACTOR IN IMPROVING THE EFFICIENCY OF MAINTENANCE OF COMMUNICATION SYSTEMS AND AUTOMATED CONTROL SYSTEMS

Kurochka V. S., Kolodyazhny P. A., Yushin A. I. 74

THE ROLE OF MASKING AND IMITATION OF ELEMENTS MILITARY COMMUNICATION SYSTEMS

Agafonov D. A., Kozyrev V. V., Lapin G. V. 83

OUR HISTORY

ASSESSMENT OF THE WORK OF MILITARY FIELD WIRE COMMUNICATION FACILITIES DURING THE GREAT PATRIOTIC WAR

Sheptura V. N. 89