I семинар научной школы профессора С. И. Макаренко

Сборник тезисов
докладов конференции

г. Санкт-Петербург
20-21 декабря 2025 г.

Санкт-Петербургский государственный
электротехнический университет «ЛЭТИ»
им. В. И. Ульянова (Ленина)

I СЕМИНАР НАУЧНОЙ ШКОЛЫ ПРОФЕССОРА С. И. МАКАРЕНКО

Сборник тезисов докладов конференции

г. Санкт-Петербург, 20-21 декабря 2025 г.

Электронное текстовое издание

Санкт-Петербург
Наукоемкие технологии
2026

УДК 001.8+004+621.39+623
ББК 381+384+388+397+68
П26

Составитель:

Сергей Иванович Макаренко, доктор технических наук, профессор,
Санкт-Петербургский государственный электротехнический
университет «ЛЭТИ» имени В. И. Ульянова (Ленина)
(г. Санкт-Петербург)

Рецензенты:

Илья Евгеньевич Афонин, кандидат технических наук, доцент,
Краснодарское высшее военное авиационное училище летчиков (г. Краснодар);

Максим Сергеевич Иванов, кандидат технических наук, Военный учебно-научный
центр Военно-воздушных сил «Военно-воздушная академия имени
проф. Н. Е. Жуковского и Ю. А. Гагарина» (г. Воронеж);

Роман Леонидович Михайлов, доктор технических наук, доцент,
Военный университет радиоэлектроники (г. Череповец)

П26 I семинар научной школы профессора С. И. Макаренко: сборник тезисов докладов конференции; г. Санкт-Петербург, 20-21 декабря 2025 года / сост. С. И. Макаренко. – СПб.: Наукоемкие технологии, 2026. – 132 с. – URL: https://publishing.intelgr.com/archive/I-seminar-nauchnoi-shkoli-professora-S-I-Makarenko.pdf.

Сборник составлен на основе материалов докладов участников конференции «I семинар научной школы профессора С. И. Макаренко», прошедшей в г. Санкт-Петербург 20-21 декабря 2025 года. Основной площадкой проведения конференции выступил Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» имени В. И. Ульянова (Ленина). Заседания конференции были посвящены обсуждению результатов исследований резидентов научной школы, выработке рекомендаций по подготовке к защите докторантов, соискателей, адъюнктов и аспирантов, а также анализу наиболее актуальных тенденций развития науки, техники и практики.

Издание адресовано научным работникам, докторантам, адъюнктам, аспирантам, студентам и специалистам, ведущим исследования в профильных областях, по которым работает научная школа С. И. Макаренко.

УДК 001.8+004+621.39+623
ББК 381+384+388+397+68

Научное издание

I семинар научной школы профессора С. И. Макаренко

Сборник тезисов докладов конференции

г. Санкт-Петербург, 20-21 декабря 2025 года

Электронное текстовое издание

Материалы изданы в авторской редакции
Опубликовано с оригинал-макета, подготовленного составителем
Главный редактор *В. М. Коровин*

Подписано к использованию 27.04.2026.
Объем издания – 4,5 Мб.

Издательство «Наукоемкие технологии»
ООО «Корпорация «Интел Групп»
https://publishing.intelgr.com
E-mail: publishing@intelgr.com
Тел.: +7 (812) 945-50-63
Интернет-магазин издательства:
https://shop.intelgr.com/

Сведения о конференции

Конференция «I семинар научной школы профессора С. И. Макаренко» прошла в очном режиме и в режиме видеоконференцсвязи на нескольких секциях, которые были сформированы на 7 площадках в разных организациях в 5 городах:

1. Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» имени В. И. Ульянова (Ленина) (г. Санкт-Петербург) – руководитель секции Макаренко С. И.;
2. Военная академия связи имени маршала Советского Союза С. М. Буденного (г. Санкт-Петербург) – руководитель секции Медведев А. А.;
3. Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича (г. Санкт-Петербург) – руководитель секции Владыко А. Г.;
4. Военный университет радиоэлектроники (г. Череповец) – руководитель секции Михайлов Р. Л.;
5. Военный учебно-научный центр Военно-воздушных сил «Военно-воздушная академия имени проф. Н. Е. Жуковского и Ю. А. Гагарина» (г. Воронеж) – руководитель секции Иванов М. С.;
6. Краснодарское высшее военное авиационное училище лётчиков имени Героя Советского Союза А. К. Серова (г. Краснодар) – руководитель секции Афонин И. Е.;
7. Государственное бюджетное учреждение здравоохранения Запорожской области «Медицинский информационно-аналитический центр» (г. Мелитополь) – руководитель секции Касаткин Ф. Ю.

Основной организатор конференции: Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» имени В. И. Ульянова (Ленина) (г. Санкт-Петербург), кафедра информационной безопасности.

Основное место и время проведения: г. Санкт-Петербург, 20-21 декабря 2025 года.

Сборник тезисов докладов конференции опубликован издательством «Наукоемкие технологии» (г. Санкт-Петербург).

Организационный комитет конференции

Председатель оргкомитета конференции – руководитель семинара научной школы:

1. *Макаренко Сергей Иванович*, д.т.н., профессор, СПбГЭТУ «ЛЭТИ» имени В. И. Ульянова (Ленина), Военная академия связи имени маршала Советского Союза С. М. Буденного (г. Санкт-Петербург).

Члены оргкомитета:

2. *Михайлов Роман Леонидович*, д.т.н., доцент, Военный университет радиоэлектроники (г. Череповец);
3. *Иванов Максим Сергеевич*, к.т.н., Военный учебно-научный центр Военно-воздушных сил «Военно-воздушная академия имени проф. Н. Е. Жуковского и Ю. А. Гагарина» (г. Воронеж);
4. *Дисенов Артур Амангалиевич*, к.т.н., доцент, Военный учебно-научный центр Военно-воздушных сил «Военно-воздушная академия имени проф. Н. Е. Жуковского и Ю. А. Гагарина» (г. Воронеж);
5. *Владыко Андрей Геннадьевич*, к.т.н., доцент, Санкт-Петербургский государственный университет телекоммуникаций имени проф. М. А. Бонч-Бруевича (г. Санкт-Петербург);
6. *Афонин Илья Евгеньевич*, к.т.н., доцент, Краснодарское высшее военное авиационное училище лётчиков имени Героя Советского Союза А. К. Серова (г. Краснодар);
7. *Понамарев Алексей Валерьевич*, к.т.н., Краснодарское высшее военное авиационное училище лётчиков имени Героя Советского Союза А. К. Серова (г. Краснодар);
8. *Медведев Алексей Александрович*, Военная академия связи имени маршала Советского Союза С. М. Буденного (г. Санкт-Петербург);
9. *Касаткин Феликс Юрьевич*, Государственное бюджетное учреждение здравоохранения Запорожской области «Медицинский информационно-аналитический центр» (г. Мелитополь).

Секретарь конференции:

10. *Кривоносова Наталья Викторовна*, Санкт-Петербургский государственный университет телекоммуникаций имени проф. М. А. Бонч-Бруевича (г. Санкт-Петербург).

Содержание

УДК 001.8+004+621.39+623

Направления исследований, основные результаты и достижения научной школы профессора С. И. Макаренко

Макаренко С. И.

В тезисе представлены основные направления исследований научной школы проф. С. И. Макаренко за последние годы, изложены фундаментальные результаты, указаны наиболее значимые публикации, а также обзорно сформулированы пути дальнейшей работы.

Ключевые слова: *научная школа, научное направление, исследование, система связи, спутниковая система связи, радиоэлектронный мониторинг, радиоэлектронная борьба, информационная безопасность, информационное противоборство, робототехнический комплекс, беспилотный летательный аппарат, безэкипажное судно, безэкипажный катер, автономный необитаемый аппарат, интероперабельность, воздушно-космическая оборона, противовоздушная оборона, военное искусство.*

Фактически научная школа (НШ) проф. С. И. Макаренко активно начала формироваться в период после 2020 г., когда совместные исследования с большим количеством учеников, переросли в системную работу по их защите и внедрению результатов исследований в реальные научно-исследовательские и опытно-конструкторские работы (НИОКР). Наша НШ является «боковой ветвью» всероссийской НШ «Защита информационных ресурсов систем управления войсками от иностранных технических разведок», ведущей исследования под руководством д.в.н. проф. Ю. И. Стародубцева, научного консультанта С. И. Макаренко по докторской диссертации, самобытному и неординарному ученому, поражающему глубиной и масштабом своих научных замыслов. Кроме того, на направления исследований и общую методологию их проведения в нашей НШ повлияли: к.т.н. доцент А. В. Кихтенко; к.т.н. проф. А. В. Баженов; д.т.н. проф. П. А. Будко; д.т.н. проф. В. И. Владимиров; д.т.н. проф. А. Г. Ломако; д.т.н. проф. Е.А. Новиков; д.т.н. проф. В. П. Пашинцев; д.т.н. проф. Г. И. Линец; д.т.н. проф. А. И. Яшин; д.т.н. проф. А. Я. Олейников; к.в.н. К. В. Козлов и в наибольшей степени – д.т.н. проф. В. И. Курносов. Именно эти люди во многом способствовали становлению и развитию нашей НШ.

Разнообразие тематических направлений нашей НШ не позволяет их объединить в рамках какого-либо одного наименования, поэтому пока наша НШ именуется по имени ее создателя. В дальнейшем, возможно, мы сформулируем некое адекватное наименование, интегрально объединяющее все тематики наших исследований, например, «Информационные технологии. Безопасность. Обороноспособность». Так же отметим, что некоторые «доброжелатели» высказывали мнение, что наша НШ «не настоящая» т. к. не имеет официально за-

---

Статья (тезис) опубликована в сборнике докладов конференции:
I семинар научной школы профессора С. И. Макаренко. Сборник тезисов докладов конференции. г. Санкт-Петербург, 20-21 декабря 2025 года. – СПб.: Наукоемкие технологии, 2026.

регистрированного статуса. Вместе с тем, сейчас, официальная регистрация НШ в России производиться либо в рамках конкретной организации (например, СПбГЭТУ «ЛЭТИ» или НИУ ИТМО), либо в рамках конкретного города (например, такую регистрацию в рамках г. Санкт-Петербург ведет городской комитет по науке и высшей школе). Однако наша НШ вышла далеко за рамки отдельной организации или города и приобрела поистине всероссийский размах – сейчас наша НШ включает специалистов, которые служат и работают в 7 организациях в 5 городах России.

1. Основные направления исследований научной школы и полученные результаты

Традиционно наша НШ ведет исследования по нескольким основным тесно взаимосвязанным между собой направлениям:

1) разработка и исследование космических систем, в т. ч. спутниковых систем связи (ССС);
2) разработка и исследование систем радиоэлектронного мониторинга (РЭМ) и радиоэлектронной борьбы (РЭБ);
3) вопросы информационной безопасности (ИБ) и информационного противоборства (ИПб);
4) вопросы организации связи и автоматизации управления робототехническими комплексами (РТК);
5) исследование вопросов интероперабельности;
6) вопросы воздушно-космической обороны (ВКО) в т. ч. вопросы противовоздушной обороны (ПВО) и вопросы разработки систем защиты объектов (СЗО) от беспилотных летательных аппаратов (БпЛА).
7) исследование изменений в военном искусстве;
8) другие частные вопросы.

Рассмотрим эти направления более подробно.

1.1. Разработка и исследование космических систем в т.ч. ССС

В 2010-2020-х гг. С. И. Макаренко и Р. Л. Михайлов долгое время работали над вопросами создания ССС, а также модернизации космической инфраструктуры Российской Федерации (РФ). Мы принимали участие в модернизации космодрома «Байконур», создании космодрома «Восточный», а также в проектных работах по ряду космических систем – «Приморка», «ЕССС-3», «Сфера», «Эфир», «Мегафон-1440», создание бортовой и наземной аппаратуры для космических систем специального назначения (СН). При этом во основу многих отечественных решений был положен глубокий анализ ССС ведущих зарубежных стран (ВЗС). Результаты этого анализа были обобщены в монографиях: «Описательные модели систем спутниковой связи как космического эшелона телекоммуникационных систем специального назначения» [1], «Системы спутниковой связи общего пользования и специального назначения» [2]. При этом значимые наработки в области создания помехоустойчивой подсистемы маршрутизации информационных потоков в наземно-космических системах

связи (СС) были обобщены в монографии «Помехозащищенность транспортных сетей связи специального назначения» [3]. В настоящее время наша НШ временно «отошла» от активного исследования космических вопросов, однако уверен, возобновление масштабных космических проектов в России, например, таких как программа «Сфера», вернет нас «в космос» где мы могли бы быть востребованы с исследованием вопросов обеспечения интероперабельности космических систем, разработкой протоколов маршрутизации для низкоорбитальных ССС, комплексирования и с системами дистанционного зондирования Земли (ДЗЗ) в части ретрансляции информации, разработкой подсистемы управления орбитальной группировками (ОГ) на сетевых принципах, а также для решения других актуальных задач.

1.2. Разработка и исследование систем РЭМ и РЭБ

Вопросы РЭМ и РЭБ применительно к СС СН традиционно являлись значимой областью научных интересов С. И. Макаренко, Р. Л. Михайлова и М. С. Иванова. По данному направлению нами были опубликованы следующие монографии, обобщающие результаты наших исследований: «Помехозащищенность систем связи с псевдослучайной перестройкой рабочей частоты» [4]; «Помехозащищенность транспортных сетей связи специального назначения» [3]; «Информационное противоборство и радиоэлектронная борьба в сетецентрических войнах начала XXI века» [5]; «Радиоэлектронная борьба в вооруженных силах США» [6], «Модели системы связи в условиях преднамеренных дестабилизирующих воздействий и ведения разведки» [7], а также концептуальный анализ отечественных исследований в области информационных конфликтов [73], применительно к системам различной природы.

В настоящее время наиболее активным исследователем вопросов РЭМ и РЭБ в составе НШ является Р. Л. Михайлов. В 2010-х гг. он активно изучал вопросы комплексного использования электромагнитного спектра в интересах координации совместного применения средств РЭМ, РЭБ и СС СН. Данное направление исследований отражено в цикле статей [8-13]. В 2022 г. Р. Л. Михайлов обобщил свои результаты по этой тематике и защитил докторскую диссертацию. В настоящее время Р. Л. Михайлов занялся исследованиями различных аспектов повышения эффективности функционирования систем наблюдения за источниками радиоизлучений со своими учениками – Д. В. Цулуном, И. Ю. Мальгиным и А. А. Павонским. Предварительные результаты исследований этих аспектов опубликованы в статьях [14-15].

С. И. Макаренко продолжает исследования в области исследования динамических информационных конфликтов между системами РЭМ, РЭБ/ИПб и СС СН. По результатам этих исследований опубликована монография «Модели системы связи в условиях преднамеренных дестабилизирующих воздействий и ведения разведки» [7], а также статьи [16-18]. В рамках развития этого направления исследований в 2025 г. А. С. Мамончикова защитила кандидатскую диссертацию по оценке защищенности СС СН в условиях воздействия РЭМ и РЭБ. При этом система «СС СН – РЭМ – РЭБ» была формализована и исследована как трехсторонний динамический информационный конфликт, выявлены би-

фуркации и фазовые состояния такого конфликта, сформулированы стратегии действия СС СН, ведущих к выигрышу в конфликте.

Вопросы использования средств РЭМ и РЭБ в составе ударных эшелонов средств воздушно-космического нападения (СВКН) при проведении ударных операций США и стран НАТО исследовались С. И. Макаренко, И. Е. Афониным и С. В. Петровым и были опубликованы в работах [19, 20].

С началом специальной военной операции (СВО) на Украине весьма актуальными стали вопросы РЭМ и РЭБ в отношении ССС Starlink, С. И. Макаренко изучал эти вопросы, а результаты его исследований опубликованы в статье [21].

1.3. Вопросы ИБ и ИПб

Вопросы ИБ и ИПб применительно к СС СН традиционно являлись значимой областью научных интересов С. И. Макаренко, а также основной областью исследований Г. Е. Смирнова, М. Ф. Савельева, А. В. Касьянова и Н. В. Кривоносовой. По данному направлению нами были опубликованы следующие монографии: «Информационное противоборство и радиоэлектронная борьба в сетецентрических войнах начала XXI века» [5]; «Аудит безопасности критической инфраструктуры специальными информационными воздействиями» [22]; а также учебные пособия: «Принципы построения и функционирования аппаратно-программных средств телекоммуникационных систем – Сетевые операционные системы и принципы обеспечения информационной безопасности в сетях» [23]; «Аудит безопасности критической информационной инфраструктуры» [24].

Одним из основных разрабатываемых направлений нашей НШ в области ИБ является разработка теоретических основ ведения аудита ИБ практическими средства и способами – проведения тестирования на проникновение. По результатам исследования этих вопросов были опубликованы монография [22] и статьи [25, 26]. В 2023 г. Г. Е. Смирнов защитил первую в России кандидатскую диссертацию [27] по разработке научно-методического обоснования проведения тестирования на проникновение – выбора тестовых информационно-технических воздействий (ИТВ), с учетом затрат на их проведение, минимизации проверяемых объектов и их свойств, а также максимизации обнаруживаемого потенциального ущерба. Важными направлениями развития этих исследований являются:

а) совершенствование научно-методического аппарата оценки эффективности тестирования на проникновение;
б) интеграция зарубежного опыта в отечественные наработки по аудиту ИБ; создание новых тестовых ИТВ, ориентированных на проверку отдельных уязвимостей или каких-либо специализированных объектов информатизации;
в) использования для формирования сценариев тестирования на проникновение систем искусственного интеллекта (ИИ);

г) разработка киберполигонов для отработки средств и способов как тестирования на проникновения, так и обеспечения защищенности информационной инфраструктуры;
д) исследование эффективности использования ложных информационных ресурсов для отвлечения на них ИТВ злоумышленников.

Для изучения этих вопросов в СПбГЭТУ «ЛЭТИ» им. В. И. Ульянова (Ленина) в период с 2021 г. по 2026 г. были поставлены и выполнены учебные научно-исследовательские работы (НИР) и выпускные квалификационные работы (ВКР) в которых приняли участие более десятка студентов: В. Ф. Абдулова, А. И. Иванов, В. Насонов, А. А. Никулин, Л. А. Богданова, Л. В. Егер, Д. Д. Маслевцов, Е. В. Писуков, К. Ю. Чулаев, М. Егоров, Е. А. Шостак.

Другим важным направлением нашей НШ в области ИБ является разработка теоретических основ создания стегосетей и развития теоретического базиса стеганографии. Еще в 2014 г. С. И. Макаренко опубликовал концептуальную статью «Эталонная модель взаимодействия стеганографических систем и обоснование на ее основе новых направлений развития теории стеганографии» [28], в которой впервые высказал идею о возможности формирования высокоскоростных скрытых сетей передачи мультимедийных данных, с поддержкой режимов передачи мудьтимедийных данных (видео, звук, изображения) в режиме реального времени. В развитие этой идеи в СПбГЭТУ «ЛЭТИ» им. В. И. Ульянова (Ленина) в период с 2019 г. по 2026 г. были проведены учебные НИР и ВКР по разработке частных практических (программных и математических) решений в области стегосетей, в которых приняли участие студенты: А. Ю. Коротова, И. О. Кущ, Ю. С. Галлямова, Т. Х. Х. Фан, Д. М. Чан, П. В. Саков. Переход от практики к дальнейшим теоретическим исследованиям по созданию стегосетей «подхватили» докторант М. Ф. Савельев и его «собратья» по этому направлению исследований – во-первых, в части разработки моделей и методов формирования стегосетей, скрытой маршрутизации и обеспечения качества обслуживания в них, во-вторых, в части разработки моделей и методов скрытой передачи конфиденциальной мультимедийной информации в стегосетях. Пока в рамках исследования этих вопросов наработано относительно небольшое число результатов, некоторые из которых были опубликованы в статьях [29-33].

Еще одним важным направлением в области ИБ, разрабатываемым С. И. Макаренко, является исследование вопросов информационно-психологической безопасности – влияние способов социальной инженерии, способов информационно-психологического воздействия (ИПВ) на корректность работы операторов, эффективность человеко-машинных интерфейсов (ЧМИ) и, в целом, на эффективность функционирования организационно-технических систем (ОТС). Частично эти вопросы изложены в монографиях «Информационное противоборство и радиоэлектронная борьба в сетецентрических войнах начала XXI века» и «Аудит безопасности критической инфраструктуры специальными информационными воздействиями» [5, 22] и многократно обсуждались С. И. Макаренко с ведущими специалистами по этой тематике в стране – В. И. Емелиным и С. Ф. Сергеевым, однако, эти вопросы еще не нашли своего глубокого исследования. Пока по этой тематике в СПбГЭТУ «ЛЭТИ» им.

В. И. Ульянова (Ленина) в 2024 г. выполнена только одна студенческая работа Е. Е. Ларионовой [29] по оценке влияния нарушения «визуабилити» web-интерфейсов на информационно-психологическую безопасность пользователей.

Отдельным направлением работы НШ является приложение исследований С. И. Макаренко в области информационных конфликтов в применении к области ИПб. В частности, использование наработанных результатов [16-18] для исследования ИПб в части ведения «вирусных войн», когда объектами, которые и запускают вирусы и защищаются от них, являются стороны, находящиеся в различной степени конфликтности друг с другом. При этом как вирусы, так и средства противодействия им представляются как мультиагенные системы, динамически распространяющиеся по сети на основе принципов биологической эволюции. Такое исследование на соискание ученой степени кандидата технических наук выполняется Н. В. Кривоносовой, и мы ожидаем, что в относительно ближайшее время оно будет завершено и вынесено на защиту.

Еще одним, несколько отдельно отстоящим от основных направлений исследований нашей НШ, являются исследования А. В. Касьянова по оценке эффективности генераторов случайных чисел и разработке способов повышения их «случайности». Эти исследования А. В. Касьянов проводит совместно с проф. А. Ю. Гришенцевым, а их результаты опубликованы в работах [30-32]. Мы также ожидаем, что в ближайшее время А. В. Касьянов оформит свои результаты в виде диссертации на соискание ученой степени кандидата технических наук и успешно защитит ее.

1.4. Вопросы организации связи и автоматизации управления РТК

Опыт применения РТК, в частности БпЛА, безэкипажных судов (БЭС), автономных необитаемых подводных аппаратов (АНПА), наземных безэкипажных транспортных средств (БЭТС), в специальной военной операции (СВО) на Украине, показал высокую актуальность вопросов организации связи с ними, а также автоматизации управления ими. По этому вопросу исследования ведут: С. И. Макаренко, М. С. Иванов, А. Г. Владыко, а также их учениками и коллегами.

Вопросы интеграции управления БпЛА, используемых Военно-воздушными силами (ВВС), в имеющийся контур управления пилотируемых летательных аппаратов (ЛА) исследовались М. С. Ивановым, его учениками и коллегами: А. В. Понаморевым, А. В. Шушковым, С. В. Смирновым, А. С. Васильченко, А. В. Аганесовым. В частности, в интересах повышения скорости обмена данными были проведены работы по модификации и адаптации коммерческих технологий связи 4.5G и 5G, а также технологий многократного использования радиоресурса в ССС к использованию в перспективных сетях воздушной радиосвязи (СВРС) управления пилотируемыми ЛА и БпЛА. Частные результаты этих исследований были опубликованы в работах [74-77] и оформлены в виде кандидатских диссертаций на соискание ученой степени кандидата технических наук, которые были успешно защищены – С. В. Смирновым и А. С. Васильченко в 2021 г., А. В. Понаморевым в 2022 г., А. В. Шушковым в 2023 г. Результаты этих исследований были взаимоувязаны между собой и опубликованы

в монографии «Модели, методы и методики повышения скорости обмена данными в сетях воздушной радиосвязи управления авиацией ВВС» [33]. Вышеуказанные частные результаты были интегрально обобщены в докторской диссертации М. С. Иванова, посвященной решению проблемы разработки научно-методического аппарата (НМА) повышения скорости обмена данными в СВРС за счет динамического, взаимоувязанного и многоуровневого использования пространственного, энергетического, сигнального, частотного, временного и топологического ресурсов на физическом, канальном и сетевом уровнях модели OSI (Open Systems Interconnection), которая была успешна защищена в 2025 г. Дальнейшим развитием исследований М. С. Иванова являются работы на соискание ученой степени кандидата технических наук А. А. Медведева, А. А. Тхакахова и Е. А. Ковалева. А. А. Медведев в своих исследованиях решает задачу рационального распределения ограниченного радиоресурса СВРС между большим количеством управляемых БпЛА при их совместных действиях, а также с учетом автоматического (на основе ИИ) и автоматизированного (дистанционного, оператором) режимов управления БпЛА. А. А. Тхакахов развивает НМА управления БпЛА при наличии ограничений на зоны их применения с учетом фактора огневого противодействия и РЭБ. Е. А. Ковалев решает задачу создания ложного сигнального навигационного поля в зоне применения БпЛА в интересах повышения их живучести. Мы ожидаем, что в относительно ближайшее время А. А. Медведев, А. А. Тхакахов и Е. А. Ковалев оформят свои результаты в виде диссертаций и успешно защитят их.

Вопросы организации связи с БЭТС в интересах управления ими в составе информационно-дорожной инфраструктуры в соответствии с концепцией V2X (Vehicle-to-Everything) изучает А. Г. Владыко и его ученики – П. В. Плотников и Г. И. Тамбовцев. Они, в рамках своих исследований, планируют объединить существующие разработки в области беспилотного транспорта, в сфере ИИ, в граничных и туманных вычислениях, в маршрутизации вычислительных задач, а также решения логистических задач для интеллектуального маршрутного управления БЭТС и формирования соответствующей информационно-дорожной инфраструктуры. Пока еще эти исследования далеки от завершения, а наиболее значимыми работами по этому направлению исследований являются статьи [34-36].

Вопросу формирования обобщенной информационно-логистической инфраструктуры обеспечения связью РТК различного типа и базирования в интересах управления ими посвящена концептуальная работа [37]. В данной работе С. И. Макаренко, А. Г. Владыко и А. А. Нестров предложили концепцию бесшовного информационного взаимодействия РТК как между собой, так и с информационно-логистической инфраструктурой наземно-дорожного, наземно-воздушного, морского и космического базирования, с учетом фактора интероперабельности. При этом, однако, эта тематика пока еще в недостаточной степени проработана и еще ждет своего глубокого исследователя.

Проблемные вопросы использования РТК не ограничиваются исключительно связными аспектами. Существующий принцип управления «один РТК – один оператор», является настоящим «каменным веком» при текущем развитии

НМА автоматизации. Групповое применение РТК при совместном их использовании требует создание полноценной автоматизированной системы управления (АСУ), интегрирующей в себя вопросы планирования использования РТК, мониторинга окружающего пространства, маршрутного управления РТК, режимами работы как РТК, так и их полезной нагрузкой. Замысел по созданию АСУ БпЛА при решении этих вопросов изложен в работе [38]. Замысел по созданию АСУ БЭС изложен в работе [39].

Члены нашей НШ входят в состав межведомственной рабочей группы «по управлению и передаче данных в области создания многосферных РТК» и активно реализуют свои наработки в проектах профильных предприятий промышленности – АО «Концерн «Созвездие», ЗАО «Институт телекоммуникаций», ПАО «Интелтех», АО «НПП «Полет», ООО «НПП «Прима», ООО «СТЦ».

1.5. Вопросы интероперабельности

Вопросами интероперабельности наша НШ занялась с «подачи» проф. А. Я. Олейникова в 2019 г. Интероперабельность – способность двух или более систем бесшовной обмениваться информацией между собой и использовать полученную информацию. В рамках исследований по интероперабельности А.Я. Олейниковым была сформирована большая научная группа в которую входят представители организаций Российской академии наук (РАН), учебных заведений и организаций промышленности – ИРЭ РАН, ФИЦ ИУ РАН, СПб ФИЦ РАН, ВАГШ, 3 ЦНИИ, 27 ЦНИИ, ВАС, ВКА, СПбГЭТУ «ЛЭТИ» и др. В период с 2019 по 2025 г. было опубликовано более десятка статей по тематике интероперабельности, в которых изложены результаты, полученные нашей НШ за авторством С. И. Макаренко, Т. Е. Черницкой и О. С. Соловьевой. Эти результаты были обобщены в двух стандартах – ГОСТ Р 59796-2021 и ГОСТ Р 55062-2021, в двух монографиях «Интероперабельность организационно-технических систем» [40], «Интероперабельность человеко-машинных интерфейсов» [41], а также в справочнике «Термины и определения в области интероперабельности» [42].

В настоящее время исследования в области интероперабельности продолжаются – С. И. Макаренко ведет работу в подгруппе «Интероперабельность» ТК-22 РосСтандарта по разработке ГОСТов по протоколам связи и управления БпЛА, А. Н. Карутин – по разработке принципов интероперабельности по объединению существующих ССС, систем ДЗЗ и спутниковой радионавигационной системы (СРНС) в единую интегрированную космическую систему [43], А. А. Нестеров и М. А. Ходаковский – по разработке количественных методик оценки различных аспектов и параметров технической интероперабельности [44, 45], А. В. Малеева – по разработке методики обеспечения интероперабельности баз данных уязвимостей информационных систем [46].

Наша НШ является активным участником межведомственной рабочей группы «по повышению статуса проблемы интероперабельности РФ» и активно работает в рамках этой группы с Минобрнауки, Минцифры, Мипромторгом, Минобороны России, а также с РАН, различными комиссиями и советами.

Кроме того, наша НШ по тематике интероперабельности активно взаимодействует со специалистами других организаций, ведущих активные исследования по интероперабельности информационных систем СН, космических и авиационных систем, а также РТК – А. Е Федоровым, Д. А. Мосиным, И. В. Скрипниковым, В. Р. Миловым, А. В. Ананьевым, С. В. Козловым и др. Мы уверены, что проблема интероперабельности является новой еще не до конца изученной областью, а за исследованиями в этой области большое будущее!

1.6. Вопросы ВКО в т. ч. вопросы формирования ПВО и вопросы разработки СЗО от БпЛА

Вопросы ВКО/ПВО традиционно являлись значимой областью научных интересов С. И. Макаренко, И. Е. Афонина, Р. Л. Михайлова, А. А. Дисенова. В последнее время к этой группе исследователей присоединились новые специалисты – К. В. Козлов, Н. А. Куприянов, А. А. Потапов, П. А. Бирюков, А. В. Старостин, С. В. Петров, А. А. Тхакаков. Актуальность исследований по вопросам ВКО/ПВО обусловлены уязвимым состоянием этих систем, выявленным СВО и их неспособностью эффективно бороться с новыми типами угроз – БпЛА и ракетами высокоточного оружия (ВТО). Исследования ведутся по нескольким направлениям, которые представлены далее.

Во-первых, это анализ новых типов угроз для систем ВКО/ПВО, оценка изменений руководящих документов США и стран НАТО, тенденций развития СВКН. По этому направлению опубликована монография «Быстрый глобальный удар: ретроспективный анализ концепции, вероятный сценарий нанесения, состав сил и средств, последствия и приоритетные мероприятия по противодействию» [47]. В данной работе С. И. Макаренко, И. Е. Афонин и Р. Л. Михайлов показывают, что в соответствии с новыми руководящими документами США основную угрозу для России представляют не межконтинентальные баллистические ракеты (МБР) и баллистические ракеты подводных лодок (БРПЛ), на защиту от которых до сих пор ориентирована отечественная система ВКО, а главным образом. крылатые ракеты (КР) воздушного и морского базирования, а также БпЛА. В рамках формирования актуальной описательной модели СВКН противника нашей НШ была начата работа над циклом статей «Средства воздушно-космического нападения ведущих зарубежных стран» [48-50]. В настоящее время работа над описательной моделью продолжается, а по ее окончании планируется издание еще одной монографии. В рамках выработки перспективных решений по новой архитектуре системы ПВО в условиях нового типа угроз – БпЛА и КР, на основе анализа исследований США С. И. Макаренко и А. В. Старостиным была опубликована концептуальная статья «Противовоздушная оборона страны от ударов беспилотных летательных аппаратов и крылатых ракет: новые угрозы, проблемные вопросы, технико-экономический анализ вариантов архитектуры» [51]. Проблематика, обозначенная в этой статье, послужила началу последующих исследований нашей НШ.

Во-первых, это исследования в области повышения устойчивости системы ВКО при нанесении ударов СВКН противником в новых условиях. Исследования по этой тематике ведет И. Е. Афонин, в рамках подготовки докторской

диссертации, его ученик – С. В. Петров, в рамках подготовки кандидатской диссертации, а также С. И. Макаренко и Р. Л. Михайлов. К настоящему времени ими разработана концептуальная модель конфликта «система ВКО – СВКН» [52], оценены состав сил и средств, а также боевые потенциалы конфликтующих сторон [53], разработана модель устойчивости системы управления ВКО с учетом многообразия факторов разведки и дестабилизирующего воздействия со стороны СВКН [54], сформированы предложения по внедрению адаптивно-сетевой структуры системы управления ВКО, гибко реагирующей на поражение или подавление ее элементов [55]. Некоторые из этих результатов вошли в учебное пособие [78]. В дальнейших исследованиях предполагается развить результаты С. И. Макаренко по динамическому моделированию конфликтов, но применительно к конфликту «система ВКО – СВКН», а также сформировать технические решения по реализации такой адаптивно-сетевой структуры на практике – протоколы устойчивой маршрутизации информационных потоков в системе управления ВКО, протоколы децентрализованного резервирования и оперативного восстановления информационного состояния узлов системы и проч.

В-третьих, это другое направление докторских исследований, которое ведет А. А. Дисенов. Как показано в вышеуказанной статье [51], наиболее сложным аспектом противодействия системы ПВО новым типам угроз является мониторинг воздушного пространства всей страны с целью обнаружения низковысотных и низкоскоростных целей – БпЛА и КР. В этой связи, цель А. А. Дисенова – формирование пассивной системы мониторинга воздушного пространства страны на основе интегральной вторичной и третичной обработки радиоданных от различных РЭМ-датчиков, получаемых в режимах «отражение» и «на просвет» от внешних (некооперируемых) источников радиоизлучения (ИРИ) наземного, воздушного и космического базирования. Пока это направление все еще находится в проработке, а значимые результаты еще пока не опубликованы. Вместе с тем это направление имеет большой потенциал т. к. позволит обеспечить формирование новой эффективной и дешевой системы разведки и контроля воздушного пространства нашего Отечества.

Отдельным актуальным направлением исследований является разработка облика и состава технических средств СЗО от БпЛА. С. И. Макаренко еще в 2016 г. стоял у истоков разработки технических решений по созданию СЗО от БпЛА, результаты которых были опубликованы в монографии «Противодействие БПЛА» [56] в 2020 г., когда этой проблеме еще не уделялось никакого внимания. Помимо С. И. Макаренко исследованиями в этом направлении занимаются К. В. Козлов, А. А. Медведев и А. А. Тхакахов. В настоящее время, по итогам проработки системотехнических проектов по созданию реальных интегрированных СЗО для объектов топливно-энергетического комплекса (ТЭК) готовиться издание монографии «Автоматизированная система защиты объектов от БпЛА», выход которой запланирован на 2026 г. В дальнейших планах – разработка моделирующего комплекса для исследования состава СЗО от БпЛА и местоположения его элементов в целях оптимизации по критерию «эффективность – стоимость».

1.7. Исследование изменений в военном искусстве

Военные конфликты начала XXI в., в особенности начало СВО, запустили процесс пересмотра некоторых положений военного искусства. Преобладание гибридных действий в военной стратегии отдельных государств, внедрение сначала сетецентрических принципов управления, а затем и ИИ, массовое использование БпЛА и БЭС в боевых действиях – все это требует обобщения, осмысления и использования в практике обороны нашей Родины.

В рамках этого направления исследований наша НШ опубликовала монографию «Сетецентрическая война – принципы, технологии, примеры и перспективы» [57] в 2018 г. А в 2025 г. приняла участие в подготовке фундаментальной монографии «Модели военных, боевых и специальных действий» [58], которая была издана под редакцией академика РАН Д. А. Новикова, и в настоящее время является, наверное, наиболее полным и новейшим изданием по НМА моделирования соответствующих конфликтных процессов. В рамках развития этой работы Д. А. Новиков и В. В. Шумов предложили издать серию монографий, каждая из которых была бы посвящена военному противоборству в отдельной сфере ведения войны. В рамках подготовки такой монографии по моделированию боевых действий в воздухе С. И. Макаренко и И. Е. Афонин опубликовали статью «Моделирование боевых действий авиации и оценки их эффективности – анализ работ, моделей, актуальных направлений исследований» [59], которая содержит первую часть моделей, относящихся к ведению боевых действий в воздухе авиацией. Вторая часть, посвященная вопросам моделирования ведения противоборства в воздухе силами ПВО, сейчас находится в разработке.

Использование гибридного противоборства, сложные отношения в геополитике, привели к исследованию вопросов конфликтного взаимодействия множества сторон при которой эти стороны в отношении своих оппонентов реализуют различные степени конфликтности – работа [60].

Широкое использование БпЛА в практике боевых действий СВО, необходимость осмысления опыта их применения как нового высокоточного тактического оружия, разработки и внедрения новых тактических приемов и способов боевых действий с их использованием, формирование новых воинских формирований, вооруженных БпЛА – все это также является областью интересов нашей НШ. По этому направлению исследований были изданы статьи [61-63] и исследование этих вопросов за счет обобщения опыта СВО продолжается.

Судя по опыту СВО, Ирано-Американо-Израильского и Палестино-Израильского военных конфликтов, важным вопросом современных военных действий является заблаговременное вскрытие массированных переброс вооружения, военной и специальной техники (ВВСТ), осуществляемое противником с целью подготовки к агрессии и развертывания наступательных порядков. В рамках этого направления Р. Л. Михайловым и А. А. Потаповым была издана монография «Система управления стратегическими перебросками вооруженных сил США» [64].

Еще одним вопросом, который является незаслуженно упущенным отечественной военной наукой является использование ИИ в военном деле. В то время как на западе вышло уже более десятка англоязычных монографий по этой тематике, глубокие открытые работы по этой проблематике в нашем Отечестве отсутствуют. Восполняя это пробел С. И. Макаренко опубликовал в 2025 г. концептуальную работу «Искусственный интеллект и когнитивное оружие, как стратегический тип вооружений в войнах будущего» [65], в которой обобщил зарубежные взгляды на использование ИИ в военном деле, указал на проблемные аспекты игнорирования этого направления исследований в РФ и предложил мероприятия по ликвидации наметившегося российского отставания в этой области. Уверен, что в связи с революционным развитием ИИ, вопросы его использования в военном деле еще ждут своих исследователей!

1.8. Другие частные вопросы

Область научных интересов нашей НШ не ограничивается вышеуказанными направлениями. Среди нас есть талантливые и работоспособные товарищи, которые ведут свои оригинальные исследования. К ним можно отнести Ф. Ю. Касаткина и Н. В. Медведева.

Ф. Ю. Касаткин занимается вопросами исследований интегральных показателей качества, которые не могут быть оценены путем линейной свертки частных параметров, а требуют особого подхода – некомпенсаторного агригирования, когда в интегральной оценке учитывается сложная взаимосвязь частных параметров между собой. Основные результаты Ф. Ю. Касаткина опубликованы в работах [66, 67]. Несмотря на то, что разработанный подход в рамках своей кандидатской диссертации Ф. Ю. Касаткин применяет для оценки качества оказания услуг центрами обработки вызовов, полученные результаты обладают поистине фундаментальной универсальностью применимости к оценке качества любых сложно-взаимосвязанных многопараметрических процессов и систем.

Н. В. Медведев долгое время являлся конструктором тренажерной техники и область его нынешних интересов – формирование кандидатской диссертации по разработке научно-обоснованных технических и технологических решений создания учебно-тренажерных средств с целью повышения полноты и оперативности освоения специальной техники ее эксплантатами.

Мы ожидаем, что в относительно ближайшее время Ф. Ю. Касаткин и Н. В. Медведев оформят свои результаты в виде диссертаций и успешно защитят их.

2. Просветительская, публикационная, редакционная, диссертационная, экспертная и преподавательская работа

2.1. Научно-методическая работа

В 2023 г. С. И. Макаренко стал экспертом Высшей аттестационной комиссии (ВАК) при Министерстве науки и высшего образования РФ. Получив опыт процесса экспертизы диссертационных работ в высшем органе государственной научной аттестации, с целью методической помощи соискателям уче-

ных степеней, а также их научным руководителям и членам администраций диссоветов сначала С. И. Макаренко, следуя новомодным тенденциям, завел блог на портале Дзен «Сергей Макаренко: советы эксперта ВАК» [68], а в дальнейшем издал научно-методическое пособие «Оформление и защита кандидатской диссертации по техническим наукам» в двух книгах [69, 70]. Книги прошли рецензирование у многих опытных экспертов ВАК, при этом в подготовке этого пособия приняли участие многие члены нашей НШ. На основе этого пособия наш коллега – эксперт ВАК П. А. Будко организовал проведение цикла семинаров «Как подготовить и защитить диссертацию», который он проводит в масштабах Государственной корпорации «Ростех», что во многом способствует увеличению научного потенциала этой корпорации. В настоящее время готовится к изданию аналогичное методическое руководство для докторантов, отдельные выдержки из которого публикуются в разделе «Докторская диссертация» [71] блога «Сергей Макаренко: советы эксперта ВАК». Выпуск вышеуказанных пособий и участие в семинарах для соискателей – это большой и важный вклад нашей НШ в дело повышения научного потенциала нашего Отечества.

Помимо этого, в 2025 г. с учетом опыта подготовки вышеуказанных пособий был обновлен и переиздан «Справочник научных терминов и математических обозначений» [72], в который вошло большое количество терминов, без которых невозможна не одна диссертационная работа: «научный результат», «научная новизна», «актуальность», «практическая значимость», «метод», «методика», «подход» и проч.

2.2. Публикационная и редакционно-экспертная работа

Наша НШ широко представлена в отечественных наукометрических рейтингах, что говорит о высокой востребованности результатов наших исследований академическим сообществом РФ и значимым вкладом НШ в научный потенциал нашей Родины:

- С. И. Макаренко входит в ТОП-10 наиболее цитируемых отечественных ученых рейтинга Российского индекса цитирования (РИНЦ) в тематических областях «Связь» и «Военное дело»;
- А. Г. Владыко входит в ТОП-100 наиболее цитируемых отечественных ученых рейтинга РИНЦ в тематической области «Связь»;
- Р. Л. Михайлов входит в ТОП-100 наиболее цитируемых отечественных ученых рейтинга РИНЦ в тематической области «Военное дело»;
- И. Е. Афонин входит в ТОП-200 наиболее цитируемых отечественных ученых рейтинга РИНЦ в тематической области «Военное дело»;
- М. С. Иванов входит в ТОП-200 наиболее цитируемых отечественных ученых рейтинга РИНЦ в тематической области «Связь».

Члены нашей НШ активно вовлечены в экспертно-редакционную деятельность. По состоянию на 2025 г. ученые НШ входят в состав редакций следующих журналов, в которых осуществляют активное рецензирование статей:

- Системы управления, связи и безопасности (включен в Перечень ВАК по научным специальностям: 1.2.2, 2.2.13, 2.2.14, 2.2.15, 2.3.1, 2.3.5, 2.3.6, 6.0.0);
- Техника средств связи (включен в Перечень ВАК по научным специальностям: 2.2.13, 2.2.14, 2.2.15, 2.3.1, 2.3.5, 2.3.6, имеется закрытая версия журнала);
- Труды учебных заведений связи (включен в Перечень ВАК по научным специальностям 1.2.2, 2.2.6, 2.2.13, 2.2.14, 2.2.15, 2.2.16, 2.3.1, 2.3.6);
- Техника радиосвязи (включен в Перечень ВАК по научным специальностям: 1.3.4, 2.2.13, 2.2.14);
- Эргодизайн (включен в Перечень ВАК по научным специальностям: 2.3.4, 5.3.3);
- Телекоммуникации и связь (имеется закрытая версия журнала);
- Научная мысль (рецензируемый закрытый журнал);
- Информационные технологии и телекоммуникации;
- Интеллектуальные технологии на транспорте;
- Вестник СПбГУТ.

2.3. Диссертационно-экспертная работа

Наша НШ активно участвует в подготовке нового поколения ученых. Члены нашей НШ входят в состав 6 диссоветов в 5 организациях, и активно принимают участие в защитах диссертаций по следующим научным специальностям и отраслям наук:

- 1.2.2. Математическое моделирование, численные методы и комплексы программ (технические науки);
- 2.2.13. Радиотехника, в том числе системы и устройства телевидения (технические науки);
- 2.2.14. Антенны, СВЧ-устройства и их технологии (технические науки);
- 2.2.15. Системы, сети и устройства телекоммуникаций (технические науки);
- 2.3.1. Системный анализ, управление и обработка информации, статистика (технические науки);
- 2.3.6. Методы и системы защиты информации, информационная безопасность (технические науки);
- группа специальностей 6.0.0 (технические и военные науки).

Разветвленная сеть научных контактов, высокое качество проведения исследований и диссертационно-экспертной работы, создает соискателям нашей НШ широкие возможности по адаптации своих результатов под спектр вышеуказанных научных специальностей, оформлению и защиты своих диссертаций.

2.4. Преподавательская работа

Члены нашей НШ ведут активную научную и преподавательскую работу в следующих вузах России:

- Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» имени В. И. Ульянова (Ленина) (г. Санкт-Петербург);
- Военно-космическая академия имени А. Ф. Можайского (г. Санкт-Петербург);
- Военная академия связи имени маршала Советского Союза С. М. Буденного (г. Санкт-Петербург);
- Санкт-Петербургский государственный университет телекоммуникаций имени проф. М. А. Бонч-Бруевича (г. Санкт-Петербург);
- Военный университет радиоэлектроники (г. Череповец);
- Военный учебно-научный центр Военно-воздушных сил «Военно-воздушная академия имени проф. Н. Е. Жуковского и Ю. А. Гагарина» (г. Воронеж);
- Краснодарское высшее военное авиационное училище лётчиков имени Героя Советского Союза А. К. Серова (г. Краснодар).

Высокий научный потенциал членов нашей НШ и разветвленная географическая сеть позволяет нам неустанно трудиться в масштабах всей России для подготовки будущих поколений инженеров, ученых и офицеров!

Литература

1. Михайлов Р. Л. Описательные модели систем спутниковой связи как космического эшелона телекоммуникационных систем специального назначения. Монография. – СПб.: Наукоемкие технологии, 2019. – 150 с.
2. Макаренко С. И. Системы спутниковой связи общего пользования и специального назначения. Монография. – СПб.: Наукоемкие технологии, 2025. – 222 с.
3. Михайлов Р. Л. Помехозащищенность транспортных сетей связи специального назначения. Монография. – Череповец: ЧВВИУРЭ, 2016. – 128 с.
4. Макаренко С. И., Иванов М. С., Попов С. А. Помехозащищенность систем связи с псевдослучайной перестройкой рабочей частоты. Монография. СПб.: – Свое издательство, 2013. – 166 с.
5. Макаренко С. И. Информационное противоборство и радиоэлектронная борьба в сетецентрических войнах начала XXI века. Монография. – СПб.: Наукоемкие технологии, 2017. – 546 с.
6. Михайлов Р. Л. Радиоэлектронная борьба в Вооруженных силах США: военно-теоретический труд. – СПб.: Наукоемкие технологии, 2018. – 131 с.
7. Макаренко С. И. Модели системы связи в условиях преднамеренных дестабилизирующих воздействий и ведения разведки. Монография. – СПб.: Наукоемкие технологии, 2020. – 337 с.
8. Михайлов Р. Л. Анализ подходов к формализации показателя информационного превосходства на основе теории прогнозирования и управления рисками // Системы управления, связи и безопасности. 2017. № 3.

С. 98-118. URL: http://sccs.intelgr.com/archive/2017-03/05-Mikhailov.pdf (дата обращения 04.02.2026).

9. Михайлов Р. Л. Двухуровневая модель координации подсистем радиомониторинга и радиоэлектронной борьбы // Наукоемкие технологии в космических исследованиях Земли. 2018. Т. 10. № 2. С. 43-50. DOI: 10.24411/2409-5419-2018-10040

10. Михайлов Р. Л. Динамическая модель информационного конфликта информационно-телекоммуникационных систем специального назначения // Системы управления, связи и безопасности. 2020. № 3. С. 238-251. DOI: 10.24411/2410-9916-2020-10309.

11. Михайлов Р. Л. Модель информационных контактов устройств телекоммуникаций информационно-телекоммуникационной системы специального назначения со средствами наблюдения и воздействия противостоящей стороны // Труды учебных заведений связи. 2020. Т. 6. № 3. С. 17-27. DOI: 10.31854/1813-324X-2020-6-3-17-27

12. Михайлов Р. Л. Новый базовый подход и методика оценивания информационного превосходства в информационном конфликте // Инфокоммуникационные технологии. 2021. Том 19. № 1. С. 7-20. DOI: 10.18469/ikt.2021.19.1.01

13. Михайлов Р. Л., Ганиев А. Н., Ефремов А. В. Модели и методы динамической координации подсистем информационно-телекоммуникационной системы специального назначения в условиях информационного конфликта // Системы управления, связи и безопасности. 2021. № 5. С. 136-179. DOI: 10.24412/2410-9916-2021-5-136-179

14. Михайлов Р. Л., Цулун Д. В. Применение алгоритмов поиска кратчайших путей при формировании маршрута полета беспилотного летательного аппарата // Информационные технологии и телекоммуникации. 2023. Том 11. № 1. С. 26-38. DOI: 10.31854/2307-1303-2023-11-1-26-38

15. Мальгин И. Ю. Моделирование траекторного сигнала радиолокационной станции космического базирования // Физика, техника и технология сложных систем (ФТТСС-2025): тезисы докладов Всероссийской с международным участием молодежной научно-практической конференции (Ярославль, 23 апреля - 07 мая 2025 г.). – Ярославль, 2025. – С. 110-111.

16. Макаренко С. И. Динамическая модель двунаправленного информационного конфликта с учетом возможностей сторон по наблюдению, захвату и блокировке ресурса // Системы управления, связи и безопасности. 2017. № 1. С. 60-97. DOI: 10.24411/2410-9916-2017-10106

17. Макаренко С. И. Игровая модель информационного конфликта системы связи с системой дестабилизирующих воздействий // Автоматизация процессов управления. 2020. № 4 (62). С. 61-74. DOI: 10.35752/1991-2927-2020-4-62-61-74

18. Макаренко С. И., Мамончикова А. С. Модель динамического многостороннего информационного конфликта с различными стратегиями участников // Радиопромышленность. 2021. Т. 31. № 2. С. 35-48. DOI: 10.21778/2413-9599-2021-31-2-35-48

19. Афонин И. Е., Макаренко С. И., Петров С. В. Описательная модель комплексов разведки, используемых для вскрытия системы воздушно-космической обороны и целеуказания при нанесении удара средствами воздушно-космического нападения // Системы управления, связи и безопасности. 2021. № 1. С. 190-214. DOI: 10.24411/2410-9916-2021-10108

20. Афонин И. Е., Макаренко С. И., Петров С. В. Описательная модель подсистемы радиоэлектронного подавления в составе средств воздушно-космического нападения, используемых для нарушения функционирования элементов системы воздушно-космической обороны // Системы управления, связи и безопасности. 2021. № 2. С. 76-95. DOI: 10.24412/2410-9916-2021-2-76-95

21. Макаренко С. И. Помехозащищенность наземных абонентских терминалов системы спутниковой связи Starlink // Системы управления, связи и безопасности. 2023. № 2. С. 81-101. DOI: 10.24412/2410-9916-2023-2-81-101

22. Макаренко С. И. Аудит безопасности критической инфраструктуры специальными информационными воздействиями. Монография. – СПб.: Наукоемкие технологии, 2018. – 122 с.

23. Макаренко С. И., Ковальский А. А., Краснов С. А. Принципы построения и функционирования аппаратно-программных средств телекоммуникационных систем: учебное пособие. Часть 2: Сетевые операционные системы и принципы обеспечения информационной безопасности в сетях. – СПб.: Наукоемкие технологии, 2020. – 357 с.

24. Макаренко С. И. Аудит безопасности критической информационной инфраструктуры. Учебное пособие. – СПб.: Наукоемкие технологии, 2023. – 122 с.

25. Макаренко С. И. Критерии и показатели оценки качества тестирования на проникновение // Вопросы кибербезопасности. 2021. № 3 (43). С. 43-57. DOI: DOI: 10.21681/2311-3456-2021-3-43-57.

26. Макаренко С. И., Смирнов Г. Е. Анализ стандартов и методик тестирования на проникновение // Системы управления, связи и безопасности. 2020. № 4. С. 44-72. DOI: 10.24411/2410-9916-2020-10402.

27. Смирнов Г. Е. Методика обоснования тестовых воздействий при анализе защищенности объекта информатизации на основе графоаналитических методов. Дис. … канд. техн. наук по спец. 2.3.6 – «Методы и системы защиты информации, информационная безопасность». – СПб.: ПГУПС, 2022. – 159 с.

28. Макаренко С. И. Эталонная модель взаимодействия стеганографических систем и обоснование на ее основе новых направлений развития теории стеганографии // Вопросы кибербезопасности. 2014. № 2 (3). С. 24-32.

29. Ларионова Е. Е. Методика эмпирического исследования и комплекс тестовых Web-интерфейсов для анализа информационно-психологической безопасности информационно-управляющих систем в условиях преднамеренного воздействия злоумышленника на интероперабельность человеко-машинных интерфейсов. Вып. квалиф. работа по спец. 10.05.01 «Компьютерная безопасность». – СПб.: СПбГЭТУ «ЛЭТИ» им. В. И. Ульянова (Ленина), 2024. – 70 с.

30. Касьянов А. В. Проблема анализа генераторов (псевдо-) случайных чисел // Научно-технический вестник Поволжья. 2024. № 7. С. 292-298.

31. Касьянов А. В., Витчак И. Д., Еремук В. В. Минимальная длина битовых последовательностей для асимптотических статистических тестов в криптографии // Правовая информатика. 2025. № 4. С. 79-85. DOI: 10.24412/1994-1404-2025-4-79-85

32. Касьянов А. В. Периодичность генераторов случайных чисел, построенных на вычислительной машине // Современная наука: актуальные проблемы теории и практики. Серия: Естественные и технические науки. 2025. № 7. С. 112-116. DOI: 10.37882/2223-2966.2025.07.20

33. Иванов М. С., Макаренко С. И. Модели, методы и методики повышения скорости обмена данными в сетях воздушной радиосвязи управления авиацией Военно-воздушных сил. Монография. – СПб.: Наукоемкие технологии, 2025. – 532 с.

34. Плотников П. В., Тамбовцев Г. И., Владыко А. Г. Математическая модель многокритериальной балансировки параметров V2X-систем // Информатика и автоматизация. 2026. Т. 25. № 1. С. 16-48. DOI: 10.15622/ia.25.1.1

35. Vladyko A., Plotnikov P., Tambovtsev G. Simulation-based evaluation of V2X system with variable computational infrastructure // Network. 2025. Vol. 5. Iss. 1. P. 4.

36. Плотников П. В., Владыко А. Г. Анализ подходов к оптимизации V2X-систем: кластеризация, граничные и туманные вычисления // Труды учебных заведений связи. 2024. Т. 10. № 3. С. 7-22. DOI: 10.31854/1813-324X-2024-10-3-7-22

37. Владыко А. Г., Нестеров А. А., Макаренко С. И. Актуальные вопросы и перспективные направления обеспечения интероперабельности робототехнических комплексов различного типа и базирования на основе технологии Robot-to-Everything // Техника средств связи. 2024. № 3 (167). С. 18-30. DOI: 10.24412/2782-2141-2024-3-18-30

38. Макаренко С. И., Козлов К. В. Автоматизированная система управления беспилотными летательными аппаратами при совместном решении ими специальных задач // Системы управления, связи и безопасности. 2025. № 1. С. 131-155. DOI: 10.24412/2410-9916-2025-1-131-155

39. Макаренко С. И., Козлов К. В. Автоматизированная система управления совместными действиями морских робототехнических комплексов, безэкипажных судов и катеров // Системы управления, связи и безопасности. 2026. № 1. С. 1-34. DOI: 10.24412/2410-9916-2026-1-001-034.

40. Макаренко С. И. Интероперабельность организационно-технических систем. Монография. – СПб.: Наукоемкие технологии, 2024. – 313 с.

41. Макаренко С. И. Интероперабельность человеко-машинных интерфейсов. Монография. – СПб.: Наукоемкие технологии, 2023. – 185 с.

42. Макаренко С. И. Термины и определения в области интероперабельности. Справочник. – СПб.: Наукоемкие технологии, 2023. – 41 с.

43. Макаренко С. И., Карутин А. Н. Перспективы и проблемные вопросы обеспечения интероперабельности интегрированных космических систем // Системы управления, связи и безопасности. 2021. № 4. С. 228-247. DOI: 10.24412/2410-9916-2021-4-228-247

44. Нестеров А. А. Оценка уровня готовности систем к взаимодействию на техническом уровне интероперабельности // ИТ-Стандарт. 2024. № 3 (40). С. 97-109.

45. Нестеров А. А., Макаренко С. И., Черницкая Т. Е. Количественная оценка вероятности нарушения требований информационной безопасности в модели интероперабельности организационно-технических систем // Техника средств связи. 2025. № 2 (170). С. 9-25. DOI: 10.24412/2782-2141-2025-2-9-25

46. Малеева А. В. Методика обеспечения интероперабельности баз данных уязвимостей. Вып. квалиф. работа по спец. 10.05.01 «Компьютерная безопасность». – СПб.: СПбГЭТУ «ЛЭТИ» им. В. И. Ульянова (Ленина), 2023. – 41 с.

47. Афонин И. Е., Макаренко С. И., Михайлов Р. Л. Быстрый глобальный удар: ретроспективный анализ концепции, вероятный сценарий нанесения, состав сил и средств, последствия и приоритетные мероприятия по противодействию. Монография. – СПб.: Наукоемкие технологии, 2022. – 174 с.

48. Афонин И. Е., Макаренко С. И., Михайлов Р. Л. Средства воздушно-космического нападения ведущих зарубежных стран. Часть 1. межконтинентальные баллистические ракеты // Системы управления, связи и безопасности. 2024. № 1. С. 138-190. DOI: 10.24412/2410-9916-2024-1-138-190

49. Афонин И. Е., Макаренко С. И., Михайлов Р. Л., Куприянов Н. А., Потапов А. А. Средства воздушно-космического нападения ведущих зарубежных стран. Часть 2. Баллистические ракеты подводных лодок // Системы управления, связи и безопасности. 2024. № 4. С. 223-286. DOI: 10.24412/2410-9916-2024-4-223-286

50. Афонин И. Е., Дисенов А. А., Черепанов Д. А., Макаренко С. И., Михайлов Р.Л. Средства воздушно-космического нападения ведущих зарубежных стран. Часть 3. Баллистические ракеты большой дальности // Системы управления, связи и безопасности. 2025. № 3. С. 170-215. DOI: 10.24412/2410-9916-2025-3-170-215

51. Макаренко С. И., Старостин А. В. Противовоздушная оборона страны от ударов беспилотных летательных аппаратов и крылатых ракет: новые угрозы, проблемные вопросы, технико-экономический анализ вариантов архитектуры // Системы управления, связи и безопасности. 2024. № 2. С. 86-148. DOI: 10.24412/2410-9916-2024-2-086-148

52. Афонин И. Е. Концептуальная модель конфликта системы воздушно-космической обороны и средств воздушно-космического нападения // Системы управления, связи и безопасности. 2025. № 3. С. 1-34. DOI: 10.24412/2410-9916-2025-3-001-034

53. Афонин И. Е., Макаренко С. И., Михайлов Р. Л. Описательная модель боевых потенциалов сторон в конфликте системы воздушно-космической обороны со средствами воздушно-космического нападения // Системы

управления, связи и безопасности. 2022. № 3. С. 41-66. DOI: 10.24412/2410-9916-2022-3-41-66

54. Афонин И. Е., Макаренко С. И., Петров С. В. Модель оценивания устойчивости системы управления воздушно-космической обороной в конфликте со средствами воздушно-космического нападения // Системы управления, связи и безопасности. 2023. № 3. С. 227-266. DOI: 10.24412/2410-9916-2023-3-227-266

55. Афонин И. Е., Петров С. В., Макаренко С. И. Переход к адаптивно-сетевой структуре системы управления воздушно-космической обороной, как один из основных путей повышения ее устойчивости // Воздушно-космические силы. Теория и практика. 2021. № 19. С. 159-178.

56. Макаренко С. И. Противодействие беспилотным летательным аппаратам. Монография. – СПб.: Наукоемкие технологии, 2020. – 204 с.

57. Макаренко С. И., Иванов М. С. Сетецентрическая война – принципы, технологии, примеры и перспективы. Монография. – СПб.: Наукоемкие технологии, 2018. – 898 с.

58. Авербух Ю. В., Афонин И. Е., Васин А. А., Галяев А.А., Дащенко А. Ю., Косарев А. Е., Макаренко С. И., Новиков Д. А., Ромашев Ю. С., Сидоренко А. А., Цыганов Н. И., Чернов И. В., Шумов В. В., Якушенко Е. И. Модели военных, боевых и специальных действий / под ред. Д. А. Новикова. – М.: ЛЕНАНД, 2025. – 528 с.

59. 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

60. Макаренко С. И., Афонин И. Е., Копичев О. А., Мамончикова А. С. Обобщенная модель Ланчестера, формализующая конфликт нескольких сторон // Автоматизация процессов управления. 2021. № 2 (64). С. 66-76. DOI: 10.35752/1991-2927-2021-2-64-66-76

61. Бирюков П. А., Тимохин А. А., Макаренко С. И. Бригады сухопутных войск, вооруженные беспилотными летательными аппаратами: обоснование создания, предложения по их структуре, способам боевого применения и техническому обеспечению с учетом опыта специальной военной операции на Украине // Системы управления, связи и безопасности. 2024. № 2. С. 43-70. DOI: 10.24412/2410-9916-2024-2-043-070

62. Макаренко С. И. Преодоление позиционного тупика в современных боевых действиях за счет массированного применения беспилотных летательных аппаратов // Воздушно-космические силы. Теория и практика. 2024. № 32. С. 25-42.

63. Макаренко С. И., Медведев А. А., Зеленов А. В. Усовершенствованный способ десантно-штурмовых действий с применением беспилотных летательных аппаратов // Воздушно-космические силы. Теория и практика. 2025. № 35. С. 17-30.

64. Михайлов Р. Л., Потапов А. А. Система управления стратегическими переброскаами вооруженных сил США. Монография. – СПб.: Наукоемкие технологии, 2024. – 134 с

65. Макаренко С.И. Искусственный интеллект и когнитивное оружие, как стратегический тип вооружений в войнах будущего // Системы управления, связи и безопасности. 2025. № 4. С. 47-67. DOI: 10.24412/2410-9916-2025-4-047-067

66. Касаткин Ф. Ю. Некомпенсаторная интегральная оценка качества работы центров обработки вызовов // Системы управления, связи и безопасности. 2025. № 4. С. 200-243. DOI: 10.24412/2410-9916-2025-4-200-243

67. Касаткин Ф. Ю. Об эффективном виде функции качества во взаимоотношениях заказчика и поставщика продукции военного назначения // Системы управления, связи и безопасности. 2025. № 3. С. 232-268. DOI: 10.24412/2410-9916-2025-3-232-268

68. Сергей Макаренко: советы эксперта ВАК // Дзен [Электронный ресурс]. 2025. – URL: https://dzen.ru/mak_serg (дата доступа 10.12.2025).

69. Макаренко С. И. Оформление и защита кандидатской диссертации по техническим наукам. Часть 1. – СПб.: Наукоемкие технологии, 2024. – 420 с.

70. Макаренко С. И. Оформление и защита кандидатской диссертации по техническим наукам. Часть 2. – СПб.: Наукоемкие технологии, 2025. – 356 с.

71. Докторская диссертация. Сергей Макаренко: советы эксперта ВАК // Дзен [Электронный ресурс]. 2025. – URL: https://dzen.ru/suite/67037eb1-a280-43e3-990a-63586b4df586 (дата доступа 10.12.2025).

72. Макаренко С. И. Справочник научных терминов и математических обозначений. – СПб.: Наукоемкие технологии, 2025. – 348 с.

73. Макаренко С. И., Михайлов Р. Л. Информационные конфликты - анализ работ и методологии исследования // Системы управления, связи и безопасности. 2016. № 3. С. 95-178. DOI: 10.24411/2410-9916-2016-10304

74. Иванов М. С., Понаморев А. В., Макаренко С. И. Моделирование трафика, передаваемого в канале управления летательным аппаратом при управлении им в процессе выполнения специальных задач. Часть 1. модель интенсивности нестационарного трафика на различных этапах полета // Системы управления, связи и безопасности. 2021. № 6. С. 120-147. DOI: 10.24412/2410-9916-2021-6-120-147

75. Васильченко А. С., Иванов М. С., Малышев В. А. Формирование полетных зон беспилотных летательных аппаратов по степени устойчивости управления ими в условиях применения средств противовоздушной обороны и радиоэлектронного подавления // Системы управления, связи и безопасности. 2019. № 4. С. 262-279. DOI: 10.24411/2410-9916-2019-10410

76. Смирнов С. В., Макаренко С. И., Иванов М. С., Попов С. А. Единая сеть воздушной радиосвязи управления авиацией с АК РЛДН основанная на децентрализованном принципе ретрансляции информационных потоков // Инфокоммуникационные технологии. 2018. Т. 16. № 1. С. 57-68. DOI: 10.18469/ikt.2018.16.1.06

77. Федосеев В. Е., Иванов М. С. Методика и результаты анализа потенциальной помехоустойчивости приема цифрового сигнала на фоне

манипулированной структурной помехи // Вестник Воронежского государственного технического университета. 2010. Т. 6. № 11. С. 108-111.

78. Медведев В. И., Снытkин И. И., Афонин И. Е., Коновальцев Э. В. Радиоэлектронное оборудование воздушных судов. Часть 1 Основы теории передачи информации. основные принципы и методы радиолокации. Учебное пособие. – Краснодар: Краснодарское высшее военное авиационное училище летчиков им. А.К. Серова, 2023. – 249 с.

Информация об авторе

Макаренко Сергей Иванович – доктор технических наук, профессор. Профессор кафедры информационной безопасности. Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» имени В.И. Ульянова (Ленина). Область научных интересов: сети и системы связи; радиоэлектронная борьба; информационное противоборство; системы и комплексы вооружения. E-mail: mak-serg@yandex.ru

Адрес: 197376, Россия, Санкт-Петербург, ул. Профессора Попова, 5.

УДК 623.646:623.746.4-519

Средства противовоздушной обороны малой дальности ведущих зарубежных стран в вооруженных конфликтах XXI века

Тхакахов А. А.

В статье представлен системный анализ средств противовоздушной обороны малой дальности, применяемых противником для уничтожения беспилотных летательных аппаратов. На основе вооруженных конфликтов в Сирии, Ливии и специальной военной операции, детально исследованы тактико-технические характеристики зенитных комплексов противника, включая турецкие системы Hisar-A и Korkut, а также немецкий IRIS-T, американский Tempest и украинскую разработку «Шершень». Рассмотрены особенности их боевого применения и технические параметры, определяющие эффективность поражения беспилотных летательных аппаратов.

***Ключевые слова**: противовоздушная оборона, противовоздушная оборона малой дальности, беспилотные летательные аппараты, Сирия, Ливия, специальная военная операция.*

Развитие беспилотных летательных аппаратов (БПЛА) и их массированное применение в вооруженных конфликтах последних лет обусловили необходимость создания эффективных средств противовоздушной обороны, способных противодействовать данному классу целей [1]. Особую значимость приобретают комплексы противовоздушной обороны (ПВО) малой дальности, предназначенные для непосредственного прикрытия войск и объектов от ударов с воздуха. Целью настоящей работы является систематизация и анализ сведений о тактико-технических характеристиках и особенностях применения средств ПВО малой дальности противника в вооруженных конфликтах в Сирии, Ливии и в ходе специальной военной операции.

Эффективность поражения беспилотных летательных аппаратов средствами ПВО определяется совокупностью факторов, связанных с физическими характеристиками целей. Малоразмерные БПЛА обладают эффективной площадью рассеяния от 0,01 до 0,1 м², что сопоставимо с аналогичным показателем крупных птиц и существенно затрудняет их обнаружение радиолокационными средствами [2]. Низкая тепловая сигнатура, особенно у аппаратов с электрическими двигателями, делает их слабовидимыми для инфракрасных головок самонаведения. Кроме того, способность БПЛА совершать полет на предельно малых высотах с использованием рельефа местности дополнительно снижает возможности их обнаружения и сопровождения [2].

Статья (тезис) опубликована в сборнике докладов конференции:
I семинар научной школы профессора С. И. Макаренко. Сборник тезисов докладов конференции. г. Санкт-Петербург, 20-21 декабря 2025 года. – СПб.: Наукоемкие технологии, 2026.

В 2020 году в ходе Сирийского конфликта турецкие вооруженные силы, проводившие операцию «Весенний щит» в Идлибской зоне деэскалации, применяли современные средства противовоздушной обороны для прикрытия своих войск и поддержки оппозиционных группировок.

Турецкий зенитный ракетный комплекс Hisar-A, разработанный компанией Aselsan и принятый на вооружение в 2019 году, предназначен для поражения воздушных целей на малых высотах. Комплекс был развернут турецкими войсками в Сирии для противодействия сирийской авиации и беспилотным летательным аппаратам правительственных войск [3].

Основные тактико-технические характеристики комплекса Hisar-A [3]:

– дальность поражения целей – до 15 км;

– максимальная высота поражения – до 5 км;

– минимальная высота поражения – 50 м;

– скорость поражаемых целей – до 300 м/с;

– время реакции – 5-8 с;

– вероятность поражения БПЛА одной ракетой – 0,7-0,8.

Зенитная управляемая ракета комплекса имеет длину 3,5 м, диаметр корпуса 0,16 м и массу 150 кг. Боевая часть осколочно-фугасного типа массой 15 кг оснащена неконтактным лазерным взрывателем. Ракета оснащена инфракрасной головкой самонаведения, обеспечивающей захват цели на дальности до 10 км. Система наведения комбинированная: на начальном участке – инерциальная с радиокомандной коррекцией, на конечном – пассивное инфракрасное самонаведение.

Комплекс может функционировать как автономно, так и в составе единой системы ПВО, получая целеуказание от радиолокационных станций (РЛС). Время развертывания комплекса не превышает 15 минут, время свертывания – 10 минут.

Турецкие вооруженные силы также развертывали в Сирии зенитные самоходные установки Korkut, предназначенные для поражения воздушных целей на малых высотах. Установка создана на базе бронетранспортера FNSS ACV-30 и оснащена спаренной 35-мм автоматической пушкой [3].

Технические характеристики установки Korkut [3]:

– дальность поражения – до 4 км;

– максимальная высота поражения – до 3 км;

– скорострельность – 1100 выстрелов в минуту;

– боезапас – 400 снарядов;

– скорость сопровождения целей – до 60 градусов в секунду.

Установка оснащена РЛС обнаружения с дальностью действия до 20 км и оптико-электронной системой сопровождения. Данные установки использовались для прикрытия наземных подразделений от ударов беспилотных летательных аппаратов и вертолетов противника.

Конфликт в Ливии в 2019-2020 годах характеризовался активным применением беспилотных летательных аппаратов обеими сторонами. Правительство

национального согласия (ПНС), поддерживаемое Турцией, использовало турецкие системы ПВО, в то время как силы маршала Х. Хафтара применяли китайские ударные БПЛА [1].

По данным открытых источников, Турция поставила ПНС зенитные ракетные комплексы Hisar, специально доработанные для повышения эффективности против беспилотных летательных аппаратов. Модернизация включала установку дополнительных средств обнаружения и систем радиоэлектронной борьбы, интегрированных в единый комплекс ПВО [1].

Доработанные комплексы Hisar получили усовершенствованную систему управления огнем, адаптированную для работы по малоразмерным целям с малой эффективной поверхностью рассеяния. Повышена чувствительность радиолокационных средств обнаружения, в алгоритмы обработки информации внесены изменения, позволяющие селектировать БПЛА на фоне естественных помех.

Кроме того, в Ливию были поставлены турецкие зенитные самоходные установки Korkut, предназначенные для поражения маловысотных целей. Данные установки развертывались для прикрытия ключевых объектов инфраструктуры и позиций правительственных войск [1].

Силы маршала Х. Хафтара активно применяли китайские ударные беспилотные летательные аппараты Wing Loong II, однако сами не имели современных средств ПВО для противодействия турецким БПЛА. Основу их системы противовоздушной обороны составляли зенитные артиллерийские установки советского производства и переносные зенитные ракетные комплексы [1].

Зенитные артиллерийские установки ЗУ-23-2 (калибр 23 мм, дальность до 2,5 км) и переносные зенитные ракетные комплексы «Стрела-2» и «Игла» (дальность до 4 км, высота до 3 км) обладали низкой эффективностью против современных ударных БПЛА, действовавших на средних высотах.

Информационное обеспечение системы ПВО ПНС осуществлялось с использованием самолета дальнего радиолокационного обнаружения Boeing E-7, поставленного одной из стран НАТО. Данный самолет, оборудованный радиолокационной станцией Northrop Grumman MESA с активной фазированной антенной решеткой, способен обнаруживать и сопровождать до 180 воздушных целей на дальности до 370 км [1].

Создание интегрированной системы ПВО, объединившей турецкие зенитные комплексы Hisar, средства РЭБ Koral и самолет дальнего радиолокационного обнаружения E-7, позволило ПНС в короткие сроки уничтожить несколько китайских ударных БПЛА Wing Loong I и Wing Loong II, действовавших на стороне сил маршала Х. Хафтара.

Специальная военная операция предоставила уникальные данные о применении современных западных и украинских средств ПВО малой дальности против российских беспилотных летательных аппаратов.

Зенитный комплекс IRIS-T (Infra Red Imaging System – Tail/Thrust Vector Controlled) представляет собой семейство зенитных управляемых ракет и ком-

плексов, разработанное немецкой компанией Diehl Defence. По данным Министерства обороны Украины, на вооружении Вооруженных сил Украины (ВСУ) находятся девять комплексов IRIS-T двух модификаций: малой дальности (SLS) и средней дальности (SLM) [4].

Модификация IRIS-T SLS предназначена для непосредственного прикрытия войск на передовой. Дальность поражения воздушных целей составляет до 12 км, максимальная высота поражения — до 8 км. Комплекс способен эффективно поражать беспилотные летательные аппараты различных классов, крылатые ракеты, самолеты и вертолеты [5]. Самоходная установка базируется на гусеничном шасси двухзвенного вездехода BvS10, что обеспечивает высокую проходимость по пересеченной местности.

Зенитная управляемая ракета комплекса имеет длину 2,94 м, диаметр корпуса 0,127 м и массу 87,4 кг. Боевая часть осколочно-фугасного типа массой 11,4 кг оснащена активным лазерным взрывателем. Ракета оснащена инфракрасной головкой самонаведения, захватывающей цель на конечном участке траектории. На начальном этапе полета наведение осуществляется по радиокомандам с радиолокационной коррекцией. Максимальная скорость ракеты достигает 3 махов, перегрузка при маневрировании – до 60 единиц [5].

Основным средством обнаружения комплекса является радиолокационная станция CEAFAR GBMMR, способная функционировать совместно с немецкой РЛС TRML-4D производства Hensoldt. Радиолокационная станция TRML-4D работает в диапазоне частот 4-8 ГГц, обеспечивает обнаружение целей на дальности до 250 км при секторе обзора 360° и способна сопровождать до 1500 целей одновременно [6].

Особенностью боевого применения IRIS-T SLS является его способность работать автономно благодаря наличию собственной радиолокационной станции обнаружения. Это позволяет оперативно развертывать комплекс на неподготовленных позициях и использовать его для прикрытия войск на марше без необходимости интеграции в стационарную систему ПВО.

Зенитный комплекс Tempest является новейшей мобильной системой ПВО малого радиуса действия, разработанной американской компанией V2X. Впервые применение данного комплекса в зоне специальной военной операции зафиксировано в начале 2026 года [7].

Комплекс построен на шасси коммерческого багги модели Polaris RZR, усиленного для боевых условий. На машине размещены компактная радиолокационная станция обнаружения и две пусковые установки управляемых ракет AGM-114L Longbow Hellfire. Дальность поражения беспилотных летательных аппаратов составляет до 8 км. Применяемые ракеты оснащены активными радиолокационными головками самонаведения миллиметрового диапазона, что обеспечивает реализацию принципа «выстрелил-забыл» [8].

Ракета AGM-114L Longbow Hellfire имеет длину 1,63 м, диаметр корпуса 0,178 м и массу 49 кг. Боевая часть осколочно-фугасного типа массой 8 кг обеспечивает гарантированное поражение беспилотных летательных аппаратов

среднего класса. Ракета оснащена инерциальной системой наведения на начальном участке траектории и активной радиолокационной головкой самонаведения миллиметрового диапазона (94 ГГц) на конечном участке [9].

Технические характеристики комплекса включают возможность работы в условиях подавления сигналов спутниковой навигации GPS (Global Positioning System) благодаря использованию инерциальной системы наведения. Радиолокационная станция комплекса обеспечивает обнаружение целей на дальности до 15 км и их автоматическое сопровождение.

Особенностью тактического применения Tempest является его высокая мобильность и малое время нахождения на огневой позиции, не превышающее 5 минут от момента обнаружения цели до пуска ракет. Это позволяет комплексу эффективно противодействовать внезапным налетам российских БПЛА, оперативно перемещаясь в угрожаемые районы и избегая ответного огня.

Украинский зенитный комплекс «Шершень» представляет собой мультикалиберный зенитный ракетный комплекс, разработанный компанией «Радионикс», входящей в Национальную Ассоциацию Оборонной Промышленности Украины [10].

Главной конструктивной особенностью комплекса является универсальная пусковая установка, совместимая с пятью типами ракет, включая советские образцы Р-27, западные боеприпасы и перспективные украинские разработки. Пусковая установка имеет модульную конструкцию, позволяющую осуществлять съем пускового блока с шасси с помощью системы мультилифт и размещать его на земле как автономный огневой объект [10].

В состав комплекса входят пункт управления радарной станции, пусковые установки, пуско-заряжающие машины и транспортно-зарядные машины. Комплекс не привязан к конкретному типу радиолокационной станции и может интегрироваться с различными РЛС, включая украинскую систему «Кречет», получающую информацию от различных источников обнаружения [10].

При применении ракет Р-27ЕТ1 с тепловыми головками самонаведения дальность поражения воздушных целей не превышает 20 км, что позволяет классифицировать «Шершень» как средство ПВО малой дальности. Ракета Р-27ЕТ1 имеет длину 4,08 м, диаметр корпуса 0,23 м и массу 350 кг, включая боевую часть массой 39 кг. Инфракрасная головка самонаведения обеспечивает захват цели на дальности до 15 км.

По заявлениям разработчиков, комплекс обладает существенно меньшей стоимостью по сравнению с зарубежными аналогами, что потенциально позволяет обеспечить массовое производство и насыщение войск данными средствами ПВО [11]. Интеграция с различными типами ракет позволяет использовать имеющиеся запасы советских боеприпасов, что критически важно в условиях ограниченных ресурсов.

Системный анализ применения средств противовоздушной обороны малой дальности противником в вооруженных конфликтах в Сирии, Ливии и специальной военной операции показывает, что противник активно развивает как

западные (IRIS-T, Tempest), так и собственные разработки (турецкий Hisar-A, украинский «Шершень»). Рассмотренные комплексы обладают различными тактико-техническими характеристиками и представляют серьезную угрозу для российских беспилотных летательных аппаратов.

Наиболее совершенные средства ПВО противника (IRIS-T SLS, Tempest) способны эффективно поражать малоразмерные цели благодаря современным системам наведения и высокой мобильности. Украинский комплекс «Шершень» представляет собой наиболее экономичное решение с возможностью применения различных типах ракет, что обеспечивает гибкость применения в различных условиях боевой обстановки.

Полученные данные могут служить основой для моделирования боевой эффективности российских БПЛА в условиях противодействия современных средств ПВО противника.

Литература

1. Афонин И. Е., Макаренко С. И., Петров С. В., Привалов А. А. Анализ опыта боевого применения групп беспилотных летательных аппаратов для поражения зенитно-ракетных комплексов системы противовоздушной обороны в военных конфликтах в Сирии, в Ливии и в Нагорном Карабахе // Системы управления, связи и безопасности. 2020. № 4. С. 163-191.

2. Макаренко С. И. Противодействие беспилотным летательным аппаратам. Монография. – Санкт-Петербург: Наукоемкие технологии, 2020. – 204 с.

3. В битве за Идлиб Турция опробовала против России новое оружие // Московский комсомолец: [Электронный ресурс]. 2020. – URL: https://www.mk.ru/politics/2020/03/07/v-bitve-za-idlib-turciya-oprobovala-protiv-rossii-novoe-oruzhie.html (дата обращения: 24.02.2026).

4. Минобороны назвало количество зенитных комплексов IRIS-T у ВСУ и их особенности // Диалог.UA [Электронный ресурс]. 2025. – URL: https://www.dialog.ua/war/326136_1766749708 (дата обращения: 24.02.2026).

5. Ukraine received the first IRIS-T SLS air defense system // Мілітарний: [Электронный ресурс]. 2026. – URL: https://militarnyi.com/en/news/ukraine-received-the-first-iris-t-sls-air-defense-system/ (дата обращения: 24.02.2026).

6. Ukraine will receive two IRIS-T air defense systems from Germany by the end of the year // Мілітарний [Электронный ресурс]. 2026. – URL: https://militarnyi.com/en/news/ukraine-will-receive-two-iris-t-air-defense-systems-from-germany-by-the-end-of-the-year/ (дата обращения: 24.02.2026).

7. Систему ПВО, тайно привезенную из США на Украину, показали на видео // Российская газета [Электронный ресурс]. 2026. – URL: https://rg.ru/2026/01/14/poiavilos-video-s-sistemoj-pvo-tajno-peredannoj-ssha-ukraine.html (дата обращения: 24.02.2026).

8. Украина представила американскую противобеспилотную систему Tempest для ночных операций // Vietnam.vn [Электронный ресурс]. 2026. – URL:

https://www.vietnam.vn/ru/ukraine-he-lo-vu-khien-chong-uav-tempest-do-my-che-tao-trong-tac-chien-ban-dem (дата обращения: 24.02.2026).

9. Ukraine Deploys US-Made Tempest Counter-Drone System in Combat for First Time // Army Recognition [Электронный ресурс]. 2026. – URL: https://www.armyrecognition.com/news/army-news/2026/ukraine-deploys-us-made-tempest-counter-drone-system-in-combat-for-first-time2 (дата обращения: 24.02.2026).

10. ЗРК «Шершень». Проект мультикалиберного комплекса ПВО разработали в Украине // Online.ua [Электронный ресурс]. 2026. – URL: https://news.online.ua/ru/zrk-sersen-proekt-multikalibernogo-kompleksa-pvo-razrabotali-v-ukraine-901392/ (дата обращения: 24.02.2026).

11. В Украине разработали комплекс ПВО «Шершень»: на нем уже испытали 5 типов ракет // УНИАН [Электронный ресурс]. 2026. – URL: https://www.unian.net/weapons/pvo-ukraina-razrabotala-zrk-shershen-na-kotorom-uzhe-ispytali-5-tipov-raket-13286790.html (дата обращения: 24.02.2026).

Информация об авторе

Тхакахов Алим Артурович – соискатель ученой степени кандидата технических наук. Адъюнкт научно-исследовательского центра. Военная академия связи. Область научных интересов: беспилотные летательные аппараты, маршрутизация беспилотных летательных аппаратов, разведзащищенность систем управления. E-mail: thakahov.98@bk.ru

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

УДК 623.61

Особенности обеспечения разведывательной защищенности и живучести полевых узлов связи пунктов управления на основе опыта специальной военной операции

Медведев А. А.

В работе рассмотрен опыт ведения боевых действий в военных конфликтах последних десятилетий, указывающий на ряд проблем в обеспечении живучести полевых узлов связи пунктов управления. Сформулированы основные пути повышения разведывательной защищённости в условиях активного применения противником средств видовой разведки.

Ключевые слова: *разведывательная защищённость, живучесть, полевой узел связи, пункт управления, БпЛА, средства воздушной разведки.*

Опыт применения Вооружённых Сил (ВС) Российской Федерации (РФ) в контртеррористических операциях и боевых действиях (БД) сформировал соответствующие способы ведения борьбы с противником, но изменившаяся тактика действий в условиях особенностей проведения специальной военной операции (СВО) указывает на ряд проблем в тактических действиях войск.

Массовое использование беспилотных летательных аппаратов (БпЛА) привело к новым формам и способам ведения БД. В целях получения преимущества «на поле боя» противник активно использует средства радио- и радиотехнической разведки (РРТР), оптико-электронной (ОЭР) и радиолокационной разведок (РЛР), размещаемых на летательных аппаратах (БпЛА), тем самым увеличивая вероятность вскрытия местоположения пунктов управления (ПУ) и их узлов связи (УС) средствами воздушной разведки за счёт использования интегрированных комплексов мониторинга на основе БпЛА.

В результате продвижения российских войск вглубь территории противника пункты управления (ПУ) развертываются в непосредственной близости к линии боевого соприкосновения (ЛБС). ПУ представляют собой совокупность сооружений или транспортных средств, оснащённых средствами управления и системами жизнеобеспечения, предназначенными для обеспечения деятельности должностных лиц органов военного управления, их функционального взаимодействия при подготовке и ведении боевых действий. При этом условия СВО привели к тому, что существующие требования по развертыванию ПУ и использованию средств связи его УС частично устарели и подвергаются пересмотру «на ходу» в процессе ведения БД. При этом эмпирически введенные на СВО улучшения, в части развертывания ПУ и организации связи в них, должны быть узаконены «де юре» за счёт внесения изменений в соответствующие руководящие документы.

Статья (тезис) опубликована в сборнике докладов конференции:
I семинар научной школы профессора С. И. Макаренко. Сборник тезисов докладов конференции. г. Санкт-Петербург, 20-21 декабря 2025 года. – СПб.: Наукоемкие технологии, 2026.

В целях повышения разведывательной защищённости ПУ и соответственно снижения вероятности нанесения противником удара по нему, выполняются мероприятия по повышению временной и энергетической скрытности УС в составе ПУ путем ограничений, вводимых на использование средств связи, например, на использование радиосредств малой и средней мощности, размещенных на командно-штабных машинах (КШМ). Такие радиосредства применяются только в тыловых районах и, как правило, исключительно в целях оповещения. В сложившихся на СВО условиях ведения БД спутниковые средства связи, ранее считавшиеся вспомогательным элементом УС для работы в условиях мирного времени, сегодня являются основным средством связи в зоне СВО. Они обеспечивают высокую пространственную скрытность УС за счёт малого угла диаграммы направленности (ДН) антенны и низкого энергетического уровня боковых лепестков ДН.

Активное использование в зоне СВО единой сети электросвязи (ЕСЭ) на основе проводных линий связи в интересах различных ведомств, частично разрешило проблемы организации взаимодействия подразделений различной ведомственной принадлежности, обусловленные трудностями несовместимости или ограниченными возможностями взаимодействия, наличием разнотипной аппаратуры и средств связи. Это потребовало применения не только штатных средств связи, но и средств связи двойного назначения, что позволило сформировать дополнительное множество основных и резервных каналов связи для межвидового применения войск (сил), что, в свою очередь, также повысило их разведывательную защищённость от средств РРТР воздушной разведки противника.

Ещё одним из ключевых факторов обеспечения разведывательной защищённости является запрещение формирования новых фортификационных сооружений в районе развёртывания УС и использование для развертывания ПУ и УС естественных укрытий местности. Это обусловлено тем, что любые изменения местности являются важными демаскирующими признаками для средств видовой разведки противника. При необходимости возведения дополнительных сооружений для ПУ или УС инженерные работы проводятся частично или скрытно, под видом повседневных ремонтно-строительных (восстановительных) работ, которые позволяют замаскировать выполнение необходимых задач для организации управления и связи.

Обобщая изложенное, можно сделать следующие выводы:

1) проводимые мероприятия по защите полевых УС ПУ от различных видов оружия имели шаблонный характер, в низкой степени соответствующий современным способам БД, что вскрылось только после начала СВО;
2) приобретённый опыт ведения БД в СВО на Украине, в Сирии и в других военных конфликтах позволил сделать вывод о необходимости оперативного перестроения системы связи в тактическом звене управления, а также о необходимости изменения способов применения подразделений связи в интересах повышения их разведывательной защищённости от средств видовой разведки противника;

3) в районах БД требуется внедрение возимых средств связи ввиду высокой оперативности вскрытия местонахождения полевых УС ПУ видовой разведкой противника;
4) ремонт и восстановление аппаратуры средств связи должны предусматривать возможность ее замены «блочным» способом, то есть путём замены неисправных блоков на работоспособные, что повысит оперативность восстановления аппаратуры связи и, как следствие, живучесть УС ПУ;
5) ограниченность типажа и номенклатуры средств тактического звена управления формирует для противника возможности идентификации УС по их принадлежности к ПУ, а соответственно повышает вероятность применения по УС ПУ высокоточного оружия (ВТО);
6) средства связи на транспортной базе не должны иметь отличительных видовых демаскирующих признаков, позволяющих определить их принадлежность к подразделениям связи. Обеспечение этого существенно повысит разведывательную защищённость УС для средств видовой разведки противника, а, следовательно, и живучесть УС как при развёртывании (стоянке), так и на марше, поскольку именно УС представляют собой наиболее вероятную цель поражения со стороны ВТО противника;
7) вышеуказанные мероприятия по повышению разведывательной защищённости и живучести УС целесообразно закрепить «де юре» путем внесения изменений и дополнений в руководящие документы, а также в план перспективного развития войск связи;
8) требуется организация подготовки и переподготовки специалистов связи для обучения работе на перспективных средствах связи;
9) необходимо обеспечить создание технических условий для взаимодействия средств связи всех министерств и ведомств, участвующих в БД в рамках межвидовой группировки.

Вышеуказанные мероприятия обеспечат повышение разведзащищённости полевого УС ПУ от средств разведки воздушного базирования, что, в свою очередь, снизит вероятность вскрытия их местоположения и нанесения по ним удара ВТО противника, а, следовательно, повысит живучесть ПУ. Повышение живучести ПУ окажет непосредственное положительное влияние на устойчивость и непрерывность управления личным составом, техникой и оружием, что позволит повысить эффективность ведения БД в таких новых условиях, сложившихся в ходе СВО.

Литература

1. Ворогушин Е. Б., Савушкин Н. И. Военная энциклопедия. Т. 1. – М.: Воениздат, 1997. – 147 с.

2. Иванов В. Г., Симоненко И. В., Озарчук В. С. и др. Узлы связи пунктов управления: учебник по дисциплине «Тактико-специальная подготовка» – СПб.: СПбПУ им. Петра Великого, 2019. – С. 13–47.

3. Рыльков П. Ф. На международном военно-техническом форуме «АРМИЯ-2024» ГУС ВС РФ определяет дальнейший вектор развития системы связи. // Красная звезда. 2024. – URL: http://redstar.ru/v-formate-kruglogo-stola/ (дата обращения 20.10.2024).

4. Макаренко С. И. Модели системы связи в условиях преднамеренных дестабилизирующих воздействий и ведения разведки. Монография. – СПб.: Наукоемкие технологии, 2020. – 337 с.

5. Афонин И. Е., Макаренко С. И., Петров С. В. Модель оценивания устойчивости системы управления воздушно-космической обороной в конфликте со средствами воздушно-космического нападения // Системы управления, связи и безопасности. 2023. № 3. С. 227–266. DOI: 10.24412/2410-1916-2023-3-227-266.

6. Дудко С. М., Морару А. А., Смелов А. Е. К вопросам живучести пунктов управления общевойсковых формирований тактического звена // Военная мысль. 2023. № 10. С. 60–68.

7. Вольхин С. Д., Пустошкин М. М. Повышение эффективности применения средств и комплексов связи путем проведения мероприятий по обеспечению живучести // Телекоммуникации и связь. 2025. № 4 (7). С. 52–58.

8. Гусева А. С., Дурнев Р. А., Кудряшов А. С., Свиридок Е. В. Оценка эффективности систем противодействия массированному применению мини - БПЛА: методические основы // Известия Российской академии ракетных и артиллерийских наук. 2021. № 1 (116). С. 57–61.

Информация об авторе

Медведев Алексей Александрович – соискатель учёной степени кандидата наук. Адъюнкт научно-исследовательского центра. Военная академия связи. Область научных интересов: военные системы связи; пункты управления и узлы связи; разведывательная защищённость систем управления; живучесть полевых узлов связи; организация связи. E-mail: aleksey750rus@mail.ru

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

УДК 621.391

Методы, модели и методики повышения скорости обмена данными в сетях воздушной радиосвязи

Иванов М. С.

В статье кратко рассмотрены основные результаты, полученные автором в рамках работы над диссертацией на соискание ученой степени доктора технических наук.

Ключевые слова: *сеть воздушной радиосвязи, авиация, сетевые ресурсы, скорость обмена данными, модели, методики, методы.*

В последнее время наметилась тенденция увеличения интенсивности эксплуатации летательных аппаратов (ЛА) авиации специального назначения (АСН) при выполнении специальных целевых задач (СЦЗ), которая обусловлена прежде всего, широким применением беспилотных летательных аппаратов (БЛА), действующих в зонах повышенной опасности для человека (при контроле техногенных аварий на объектах атомной и химической промышленности, лесных пожаров, контроля и мониторинга государственной границы и т.д.), а также совместным применением пилотируемых ЛА и групп БЛА.

Одновременно с возрастанием интенсивности применения ЛА АСН выявляются проблемные технические аспекты их эксплуатации и управления:

Несоответствие принципов организации связи в сетях воздушной радиосвязи (СВРС) управления пилотируемыми ЛА и БЛА АСН требованиям по скорости передачи данных на пункты управления (ПУ), в частности, в СВРС используется директивный способ назначения частотно-временных ресурсов для отдельных каналов управления ЛА в СВРС, что не позволяет адаптивно распределять частотно-временные ресурсы среди абонентов в СВРС. Предварительные исследования показали, что подобное назначение ресурсов для каналов управления ЛА в СВРС не учитывает изменения интенсивности передаваемого по ним трафика (команд управления и данных воздушной обстановки) на различных этапах полета ЛА и характера выполняемых ими СЦЗ, что ведет к снижению своевременности передачи команд управления на ЛА и, как следствие, – снижению эффективности управления ЛА.

Высокие требования по оперативности управления ЛА и особенно БЛА, своевременности передачи данных и команд на борт, скорости передачи как отдельных каналов управления, так и СВРС в целом.

Необходимость применения АСН в удаленных регионах необорудованных связной инфраструктурой. Примерами такого применения АСН является выполнение СЦЗ по тушению лесных пожаров, проведения мониторинга и кон-

---

Статья (тезис) опубликована в сборнике докладов конференции:
I семинар научной школы профессора С. И. Макаренко. Сборник тезисов докладов конференции. г. Санкт-Петербург, 20-21 декабря 2025 года. – СПб.: Наукоемкие технологии, 2026.

троля функционирования нефте-газо добывающих предприятий, поиск и спасание экипажей, терпящих бедствие, мониторинг и контроль границы и т.д.

Большое количество разнородной авиации и БЛА – как новый вид ЛА, которые активно применяются в настоящее время для проведения наблюдения и контроля обстановки, требуют от автоматизированной системы управления способности управлять как большим количеством ЛА, так и оперативности управления, что ведет к повышенным требованиям по скорости обмена данными в сети управления и необходимости создания единой связной инфраструктуры.

Как показывает опыт проведения специальной военной операции (СВО), для выполнения СЦЗ привлекаются ЛА подведомственные Министерству обороны, Министерству чрезвычайных ситуаций, Федеральной службе безопасности и т.д., при этом применяемые в настоящее время в АСН комплексы средств связи не отвечают современным требованиям по скорости обмена данными, а автоматизированные системы управления (АСУ) неспособны одновременно управлять необходимым количеством ЛА. Объем трафика, циркулирующего в СВРС возрастает в разы, что требует высокой скорости обмена данными как в каналах управления ЛА, так и в СВРС обмена данными и информационного обеспечения.

Широкий класс решаемых задач АСН актуализирует вопросы разработки перспективных комплексов и средств связи для организации оперативного управления авиацией и повышения скорости обмена данными в СВРС.

При этом авиация Военно-воздушных сил, решающая в настоящее время задачи СВО на Украине, а также отстаивание геополитических интересов за пределами РФ (Сирия, Африканские страны, Киргизия, Таджикистан, Армения) также нуждается в перспективных комплексах средств связи, позволяющих решать боевые задачи в условиях противодействия современному виду оружия, разработанному странами НАТО.

Вместе с тем, технологические решения для формирования многоканальных СВРС как в существующей аппаратуре передачи данных воздушного эшелона, так и в специализированных командных радиолиниях управления в настоящее время отсутствуют.

Существующий научно-методический аппарат (НМА) теории радиосвязи не учитывает и не реализует повышение скорости обмена данными в СВРС за счет избыточности ресурсов сети на физическом, канальном и сетевом уровнях модели OSI (OSI – Open Systems Interconnection), отсюда отсутствует единый комплекс управления средствами связи от физического (антенны, радиостанции) до сетевого (маршрутизаторы) уровней, который бы обеспечивал рациональное распределение сетевых ресурсов и, как следствие, достижение супремума скорости обмена данными в сети.

То есть необходимость повышения скорости обмена данными в СВРС:

– для выполнения требований по оперативности управления ЛА и особенно БЛА, своевременности передачи данных и команд на борт ЛА, скорости передачи как отдельных каналов управления, так и СВРС в целом;

– для обеспечения связи с АСН в удаленных регионах необорудованных связной инфраструктурой;
– для реализации концепции сетецентрического управления и организации единого информационного пространства позволяет сформулировать актуальную прагматическую цель исследования – повышение скорости обмена данными в сетях воздушной радиосвязи авиации специального назначения.

Таким образом, в области повышения скорости обмена данными в сетях воздушной радиосвязи АСН имеет место проблемная ситуация между необходимостью повышения скорости обмена данными в сетях воздушной радиосвязи АСН и невозможностью такого повышения скорости на основе существующего научно-методического аппарата.

Для решения представленной проблемной ситуации получены:

1. Комплекс модели и методики обмена данными в СВРС на физическом уровне с использованием избыточности энергетического и сигнального ресурсов сети [1-3].

2. Комплекс моделей и методик обмена данными в СВРС на канальном уровне с использованием избыточности временного и частотного ресурсов сети [4-7].

3. Комплекс моделей и методики обмена данными в СВРС на сетевом уровне с использованием избыточности топологического ресурса сети [8-12].

4. Методы повышения скорости обмена данными в СВРС АСН [13, 14].

5. Научно обоснованные технические предложения по повышению скорости обмена данными в существующих и перспективных бортовых комплексах связи, а также другие научные результаты [15, 16].

Каждый из полученных результатов обладает научной новизной хорошо доказанной в работах автора, а разработанные научно обоснованные технические предложения позволяют повысить скорость обмена данными в СВРС на 77-293% и уменьшить время задержки передачи трафика в канале связи до 0,05 с. Структурная схема проведённых исследований представлена на рис. 1.

1) Комплекс модели и методики обмена данными в СВРС на физическом уровне с использованием избыточности сигнального ресурса сети отличается от известных тем, что основан на расчете энергетического бюджета радиолинии с последующим учетом полученного энергетического ресурса для реализации информационно емких конструкций сигналов и повышения скорости кодирования (сигнальный ресурс) при организации связи с коммутацией пакетов, что на более высоких уровнях (канальном и сетевом) позволяет обосновать новые, ранее не используемые режимы функционирования СВРС.

2) Комплекс моделей и методик обмена данными в СВРС на канальном уровне с использованием избыточности временного и частотного ресурсов сети отличается от известных тем, что введены новые параметры, формальные операции и расчетные соотношения, которые впервые используют параметры функционирования физического уровня модели OSI, такие как энергетический выигрыш в отношении «сигнал/шум+помеха» и скорость обмена данными, полученные за счет применения технологии адаптивного кодирования и модуляции.

Введены новые формализованные факторы, параметры и формальные операции, учитывающие нестационарность реального трафика и зависимость интенсивности информационного обмена от этапа полета ЛА, а также новые расчетные отношения по экстраполяции интенсивности трафика для последующего формирования прогнозного значения необходимой скорости обмена данными на заданном цикле управления ЛА. Введенные в комплекс новые параметры, формальные операции и расчетные отношения позволяют обосновать создание избыточности временного ресурса за счет реализации адаптивного изменения длительности паузы захвата канала множественного доступа, учитывая специфику организации управления ЛА при выполнении целевой задачи с учетом этапности полета, с последующим выделением необходимого числа дополнительных частотных каналов абонентам с высокой интенсивностью информационного обмена для передачи трафика с требуемым качеством обслуживания, что впоследствии на сетевом уровне формализует ранее неучтенные и нереализованные режимы функционирования СВРС.

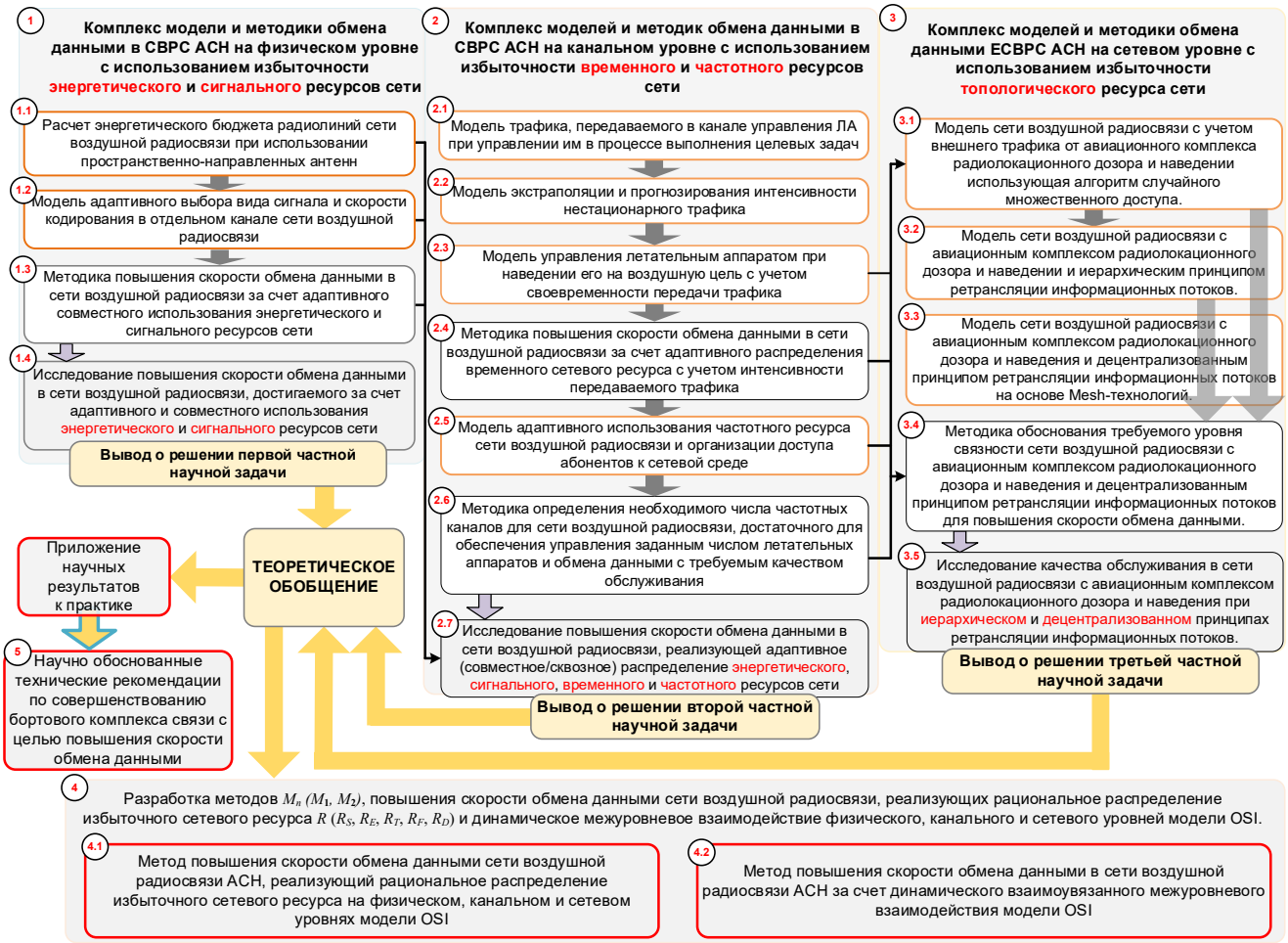

Рис. 1. Структурная схема проведенных исследований

3) Комплекс моделей и методики обмена данными в СВРС на сетевом уровне с использованием избыточности топологического ресурса сети отличается от известных тем, что введены новые параметры, формальные операции и расчетные соотношения, которые впервые учитывают параметры функциониро-

вания физического и канального уровней модели OSI, а именно, энергетический выигрыш в отношении «сигнал/шум+помеха» и скорость обмена данными, полученные за счет применения технологии адаптивного кодирования и модуляции, нестационарность интенсивности информационного обмена пункта управления и ЛА на различных этапах полета с реализацией экстраполяции прогнозного значения необходимой скорости обмена данными на заданном цикле управления ЛА с последующим выделением дополнительных частотных каналов абонентам с высокой интенсивностью информационного обмена. Введенные в комплекс новые параметры, формальные операции и расчетные отношения позволяют обосновать: создание избыточности топологического ресурса за счет формализованного учета новых параметров функционирования единой СВРС на основе алгоритма случайного множественного доступа; новую структуру СВРС АСН, в которой центральным элементом является авиационный комплекс радиолокационного дозора и наведения, а периферийные СВРС объединены на основе Mesh-технологии; требуемый показатель связности для нижнего уровня двухуровневой сети связи с учетом особенностей управления АСН; топологические структуры сети связи группового управления авиацией, такие как: централизованная (используемая в настоящее время) и децентрализованная (перспективная) на основе Mesh-сетей, а также формализовать ранее неучтенные и нереализованные режимы функционирования СВРС.

4) Методы повышения скорости обмена данными в СВРС АСН, основанные на рациональном динамическом взаимоувязанном межуровневом использовании сетевых ресурсов, отличаются тем, что впервые теоретически обобщают ранее разработанные модели и методики физического, канального и сетевого уровней модели OSI, которые формируют и реализуют избыточные сетевые ресурсы на физическом, канальном и сетевом уровнях модели OSI, а именно энергетический, сигнальный, частотно-временной и топологический. Впервые введены новые параметры и формальные операции, которые учитывают и реализуют рациональное распределение полученной (выработанной) избыточности сетевых ресурсов на различных уровнях модели OSI, введены расчетные выражения по динамическому взаимоувязанному межуровневому взаимодействию параметров функционирования модели сети с физического до сетевого уровня. Впервые в интегральном виде, комплексно, во взаимосвязи с параметрами функционирования СВРС на различных уровнях модели OSI методы реализуют повышение скорости обмена данными за счет рационального распределение созданных сетевых ресурсов и динамическое взаимоувязанное межуровневое взаимодействие созданной избыточности в виде параметров функционирования модели сети с физического до сетевого уровня.

5) Научно обоснованные технические предложения по повышению скорости обмена данными в существующих и перспективных бортовых комплексах связи, отличающиеся от известных тем, что они основаны на разработанных моделях, методиках и методах, и предлагают ранее нереализованные режимы функционирования существующих и перспективных комплексов связи, реализованные применительно к различным уровням модели OSI.

В научном исследовании с целью развития теории радиосвязи решена научная проблема, состоящая в разработке элементов научно-методического аппарата повышения скорости обмена данными в СВРС за счет динамического, взаимоувязанного и межуровневого использования избыточного энергетического, сигнального, частотного, временного и топологического ресурсов на физическом, канальном и сетевом уровнях модели OSI.

Выводы

К основным выводам по результатам научного исследования относятся следующие.

1) Повышение скорости обмена данными в СВРС может быть реализовано за счет рационального распределения избыточного сетевого ресурса:

- физического уровня – энергетического и сигнального ресурса (использование антенных систем с пространственно-направленными диаграммами направленности, обеспечивающими энергетический выигрыш в «сигнал/шум+помеха» на входе приемника; информационно высокоемких сигнальных конструкций; адаптивной смены сигнально-кодовых конструкций);
- канального уровня – временного и частотного ресурсов (применение адаптивного распределения временного ресурса в части доступа абонентов к каналу множественного доступа; выделение дополнительных частотных каналов абонентам с большой интенсивностью информационного обмена);
- сетевого уровня – топологического ресурса (использование MESH-техно-логии – технологии оптимизации структуры сети), с учетом межуровневого динамического взаимодействия параметров функционирования модели OSI в целом.

2) Использование на ЛА и ПУ направленных антенных систем позволяет достичь существенного выигрыша по значению «сигнал/шум+помеха» принимаемого сигнала. Расчет показал, что при рассматриваемых исходных данных использование фазированных антенных решеток позволяет обеспечить приблизительный энергетический выигрыш в бюджете радиолинии 8 дБ относительно кольцевой антенной решетки, 13 дБ относительно параболической антенны на опорно-поворотном устройстве и 15 дБ относительно нескольких переключаемых антенн с диаграммой направленности 60°.

3) Адаптивное распределение сигнального ресурса СВРС основано на предложенных в научном исследовании вариантах применения технологии адаптивного кодирования и модуляции, ориентированной на адаптивный к помеховым условиям выбор вида сигнала и скорости помехоустойчивого кодирования в отдельном частотном канале СВРС с учетом различных моделей распространения радиоволн – гауссовской, райевской и рэлеевской, что позволяет повысить скорость передачи данных в условиях благоприятной сигнально-помеховой обстановки в отдельных каналах СВРС на 77-293% для гауссовской, райевской и рэлеевской моделей распространения радиоволн.

4) Адаптивное распределение частотного ресурса СВРС основано на перераспределении числа каналов сети, выделяемых каждому ЛА, что, с учетом интенсивности формируемого ЛА трафика, позволяет, во-первых, обеспечить требуемое качество обслуживания для передаваемого в режиме реального времени трафика аудио- и видеоданных, во-вторых, обеспечить гибкое перераспределение частотного ресурса СВРС, в виде отдельных частотных каналов, в пользу тех ЛА, которые формируют трафик с наибольшей интенсивностью. Достигаемые при этом показатели качества обслуживания трафика равны $T_{зад} \leq 0{,}05$ с.

5) Многоканальный режим обслуживания абонентов, с одной стороны – требует увеличения количества частотных каналов, используемых каждым абонентом, а с другой стороны, за счет использования технологии адаптивного кодирования и модуляции скорость передачи каждого отдельного канала значительно возрастает. В результате достигается экономия частотного ресурса СВРС в благоприятных сигнально-помеховых условиях. При рассматриваемых исходных данных для организации многоканальной СВРС, обслуживающих абонентов с требуемым качеством, требуется полоса частот от 55 до 140 МГц, когда с фиксированными сигнально-кодовыми режимами от 105 до 220 МГц.

6) Одновременное использование в СВРС технологии адаптивного кодирования и модуляции и многоканального обслуживания абонентов позволяет значительно увеличить скорости передачи данных. Для рассматриваемых исходных данных моделирование показало, что обеспечивается увеличение значений суммарной максимальной потенциально достигаемой скорости обмена данными с одним ЛА до 617,4 Мбит/с (64QAM, R=7/8) для СВРС с каналами шириной 20 МГц.

7) Переход к децентрализованному информационному обмену на основе Mesh-технологий и использование перспективных средств связи сохранит зависимость пропускной способности информационного направления связи (ИНС) от числа периферийных СВРС. Однако наблюдается существенный выигрыш в пропускной способности ИНС, проходящих через Mesh-сегмент от 20% до 120%.

Повышение пропускной способности отдельных ИНС позволяет обеспечить больший диапазон пропускной способности СВРС в целом и повысить количество одновременно обслуживаемых абонентов в диапазоне от 2 до 9 раз для современного авиационного оборудования.

Разработанные в научном исследовании модели, методики, методы и научно обоснованные технические предложения рекомендуются к использованию организациями, ведущими военно-научное сопровождение работ в оборонно-промышленном комплексе при разработке технических и тактико-технических заданий на перспективные НИОКР в области авиационной радиосвязи, а также конструкторами БКС и управления авиацией при разработке нового телекоммуникационного оборудования с повышенной скоростью обмена данными.

К дальнейшим направлениям исследований можно отнести разработки методик и моделей повышения скорости обмена данными в СВРС, объединенной воздушно-космической и наземно-воздушной сетях радиосвязи, а также решения вопросов создания и организации единой наземно-воздушно-космической сети связи для сетецентрического управления войсками на театре военных действий в

едином информационном пространстве. К отдельным направлениям исследований стоит отнести разработку моделей и методик автоматического управления связью и ресурсами связи.

Литература

1. Иванов М. С., Шушков А. В., Макаренко С. И. Повышение скорости передачи данных в сети воздушной радиосвязи управления летательными аппаратами за счет адаптивного использования энергетического, сигнального и частотного сетевых ресурсов. Часть 1. Модели и методика повышения скорости передачи данных // Системы управления, связи и безопасности. 2023. № 1. С. 125–219.

2. Иванов М. С., Шушков А. В., Макаренко С. И. Повышение скорости передачи данных в сети воздушной радиосвязи управления летательными аппаратами за счет адаптивного использования энергетического, сигнального и частотного сетевых ресурсов. Часть 2. Исследование достигаемого повышения скорости передачи данных // Системы управления, связи и безопасности. 2023. № 1. С. 220–243.

3. Иванов М. С., Афонин И. Е., Макаренко С. И. Повышение устойчивости автоматизированной системы управления комплекса с беспилотными летательными аппаратами в условиях воздействия средств физического поражения и радиоэлектронного подавления // Системы управления, связи и безопасности. 2022. № 2. С. 92–134.

4. Иванов М. С., Понаморев А. В., Макаренко С. И. Методика повышения скорости передачи данных в сети воздушной радиосвязи управления летательными аппаратами за счет адаптивного распределения сетевого частотно-временного ресурса с учетом интенсивности передаваемого трафика // Системы управления, связи и безопасности. 2022. № 1. С. 104–139.

5. Иванов М. С., Понаморев А. В., Макаренко С. И. Моделирование трафика, передаваемого в канале управления летательным аппаратом при управлении им в процессе выполнения специальных задач. Часть 1. Модель интенсивности нестационарного трафика на различных этапах полета // Системы управления, связи и безопасности. 2021. № 6. С. 120–147.

6. Иванов М. С., Понаморев А. В., Макаренко С. И. Моделирование трафика, передаваемого в канале управления летательным аппаратом при управлении им в процессе выполнения специальных задач. Часть 2. Экстраполяция и прогнозирование интенсивности нестационарного трафика // Системы управления, связи и безопасности. 2021. № 6. С. 148–172.

7. Иванов М. С. Повышение скорости передачи данных в каналах управления БЛА за счет экстраполяции трафика и прогнозирования интенсивности на следующий цикл управления // Вестник Воронежского института МВД России. 2023. №3. С. 207–216.

8. Иванов М. С., Макаренко С. И., Смирнов С. В., Попов С. А. Единая сеть воздушной радиосвязи управления авиацией с АК РЛДН основанная на иерархическом принципе ретрансляции информационных потоков // Системы управления, связи и безопасности. №3. 2018. С. 54–68.

9. Иванов М. С., Аганесов А. В., Макаренко С. И. Повышение пропускной способности объединенной воздушно-космической сети связи. Часть 1. Модели и методика повышения пропускной способности объединенной сети связи на основе использования Mesh-технологий // Системы управления, связи и безопасности. 2022. № 3. С. 183–259.

10. Иванов М. С., Аганесов А. В., Макаренко С. И. Повышение пропускной способности объединенной воздушно-космической сети связи. Часть 2. Исследование пропускной способности объединенной сети, и разработка алгоритма распределения информационных потоков для маршрутизатора узла сети связи воздушного эшелона // Системы управления, связи и безопасности. 2022. № 3. С. 260–285.

11. Иванов М. С., Аганесов А. В., Попов С. А. Повышение пропускной способности сети воздушно-космической радиосвязи за счет использования Mesh-технологий в системах межсетевого обмена // Теория и техника радиосвязи. 2016. № 2. С. 12–16.

12. Смирнов С. В., Макаренко С. И., Иванов М. С., Попов С. А. Единая сеть воздушной радиосвязи управления авиацией с АК РЛДН основанная на децентрализованном принципе ретрансляции информационных потоков // Инфокоммуникационные технологии. 2018. Т. 16. № 1. С. 57–68.

13. Иванов М. С. Метод повышения скорости обмена данными в сети Воздушной радиосвязи управления авиацией, реализующий динамическое межуровневое взаимодействие модели OSI // Вестник Воронежского института МВД России. 2024. №2. С. 98–109.

14. Иванов М. С. Метод повышения скорости обмена данными в сети воздушной радиосвязи управления авиацией, реализующий рациональное распределение избыточного сетевого ресурса // Телекоммуникации. 2024. № 1. С. 2–13.

15. Иванов М. С., Федосеев В. Е. Методика и результаты анализа потенциальной помехоустойчивости приема цифрового сигнала на фоне манипулированной структурной помехи // Вестник Воронежского технического университета. 2010. Том 6. № 11. С. 108–112.

16. Васильченко А. С., Иванов М. С., Малышев В. А. Формирование полетных зон беспилотных летательных аппаратов по степени устойчивости управления ими в условиях применения средств противовоздушной обороны и радиоэлектронного подавления // Системы управления, связи и безопасности. 2019. № 4. С. 262–279.

Информация об авторе

Иванов Максим Сергеевич – кандидат технических наук. Старший преподаватель кафедры эксплуатации бортового авиационного радиоэлектронного оборудования. ВУНЦ ВВС «Военно-воздушная академия имени проф. Н.Е. Жуковского и Ю.А. Гагарина». Область научных интересов: сети и системы авиационной радиосвязи. E-mail: point_break@rambler.ru

Адрес: 394074, Россия, Воронеж, Старых Большевиков, д. 54а.

УДК 623.612:623.746.4-519

Средства радиоэлектронной борьбы ведущих зарубежных стран в вооруженных конфликтах XXI века

Тхакахов А. А.

В статье проводится системный анализ средств радиоэлектронной борьбы, применяемых противником для противодействия беспилотным летательным аппаратам. На основе вооруженных конфликтов в Сирии, Нагорном Карабахе и специальной военной операции детально исследованы тактико-технические характеристики комплексов радиоэлектронной борьбы, их функциональные возможности и тактика применения. Рассмотрены турецкий комплекс Koral, израильские системы радиоэлектронной борьбы, а также украинские разработки «Ай-Петрі СВ», «Октава», «Дамба» и западные системы, поставляемые Вооруженным силам Украины. Материалы статьи могут быть использованы для обоснования требований по помехозащищенности каналов управления перспективных беспилотных летательных аппаратов.

Ключевые слова: *радиоэлектронная борьба, беспилотные летательные аппараты, Сирия, Нагорный Карабах, специальная военная операция, Koral, «Ай-Петрі СВ», «Октава», «Дамба».*

Современные вооруженные конфликты последнего десятилетия характеризуются масштабным применением беспилотных летательных аппаратов (БПЛА), что закономерно привело к интенсивному развитию средств противодействия, среди которых ключевое место занимают комплексы радиоэлектронной борьбы (РЭБ) [1]. Для обеспечения эффективного применения БПЛА необходимо глубокое понимание возможностей и особенностей функционирования средств РЭБ потенциального противника. Целью настоящей работы является систематизация и анализ сведений о тактико-технических характеристиках и тактике применения средств РЭБ в вооруженных конфликтах в Сирии, Нагорном Карабахе и в ходе специальной военной операции.

Средства радиоэлектронного подавления, ориентированные на борьбу с БПЛА, реализуют деструктивное воздействие по трем основным направлениям. Первое направление заключается в подавлении командных радиолиний управления, по которым осуществляется передача полетных заданий и команд оператора. Второе направление предусматривает воздействие на каналы спутниковой навигации, что приводит к нарушению определения БПЛА собственных координат. Третье направление включает информационно-техническое воздействие с целью перехвата управления или навязывания ложных режимов функционирования [2].

Энергетическая эффективность средств РЭБ убывает пропорционально квадрату расстояния, что определяет их применение в качестве средств ближнего рубежа обороны. При этом существенным недостатком является отсут-

Статья (тезис) опубликована в сборнике докладов конференции:
I семинар научной школы профессора С. И. Макаренко. Сборник тезисов докладов конференции. г. Санкт-Петербург, 20-21 декабря 2025 года. – СПб.: Наукоемкие технологии, 2026.

ствие гарантированной реакции БПЛА на радиоэлектронное подавление, поскольку при потере связи аппарат может перейти в автономный режим полета по заранее заложенной программе [2].

В ходе Сирийского конфликта турецкие вооруженные силы, поддерживавшие отдельные группировки оппозиции, активно применяли современные средства радиоэлектронной борьбы для подавления сирийских правительственных сил.

Турецкий комплекс радиоэлектронной борьбы Koral, разработанный компанией Aselsan, предназначен для подавления радиолокационных станций противника и создания помех системам ПВО. Комплекс был впервые применен в боевых условиях в ходе операции «Весенний щит» в Идлибской зоне деэскалации в 2020 году [3].

Комплекс Koral состоит из двух основных компонентов: станции радиоэлектронной разведки и станции постановки помех. Станция разведки осуществляет обнаружение, анализ и идентификацию сигналов радиолокационных станций противника в диапазоне частот от 2 до 18 ГГц. Время анализа сигнала не превышает 1 секунды, точность пеленгования составляет 1-2 градуса.

Станция постановки помех работает в том же частотном диапазоне и способна одновременно подавлять до 12 радиолокационных станций (РЛС) на дальности до 200 км. Мощность излучения составляет до 1 кВт в непрерывном режиме. Комплекс формирует как заградительные, так и прицельные помехи, адаптируясь к конкретным типам подавляемых РЛС.

По данным западных источников, применение комплексов Koral позволило турецкой стороне временно дезорганизовать работу сирийских радиолокационных станций советского производства, что обеспечило успешные действия ударных БПЛА Bayraktar TB2 против позиций правительственных войск [3].

Турецкие ударные БПЛА Bayraktar TB2, активно применявшиеся в Сирии, оснащались встроенными средствами радиоэлектронной разведки. Аппаратура, интегрированная в состав целевой нагрузки, позволяла обнаруживать работающие радиолокационные станции и определять их координаты с точностью до 50-100 м. Полученные данные передавались на наземный пункт управления и использовались для наведения ударных групп на позиции средств противовоздушной обороны (ПВО).

Конфликт в Нагорном Карабахе осенью 2020 года характеризовался массированным применением Азербайджаном беспилотных летательных аппаратов израильского производства под прикрытием средств радиоэлектронной борьбы [1].

По данным западных источников, Азербайджан применял израильские средства радиоэлектронной борьбы, поставленные в рамках военно-технического сотрудничества. Израильские комплексы РЭБ, точные характеристики которых остаются закрытыми, обеспечивали подавление радиолокационных станций и каналов связи армянских войск.

Особенностью израильских систем являлась их способность не только подавлять, но и имитировать работу средств связи противника, вводя в заблуждение армянские подразделения относительно реальной обстановки. Примене-

ние данных средств позволило азербайджанской стороне достичь тактической внезапности в первые дни конфликта.

Израильские барражирующие боеприпасы Harop, применявшиеся Азербайджаном, оснащались головками самонаведения, способными поражать работающие радиолокационные станции. Боеприпас имел комбинированную систему наведения, включающую пассивную радиолокационную головку для наведения на излучение РЛС и электронно-оптическую систему для визуального контроля. Дальность обнаружения работающих РЛС составляла до 100 км, время барражирования – до 6 часов [1].

Специальная военная операция предоставила уникальный материал для анализа реального противодействия БПЛА, поскольку Вооруженные силы Украины (ВСУ) применяют как западные, так и собственные разработки в области радиоэлектронной борьбы.

Комплекс «Ай-Петрі СВ» представляет собой украинский комплекс противодействия техническим разведкам, разработанный на отечественной элементной базе. Система предназначена для подавления каналов управления разведывательных БПЛА и ударных беспилотников типа «Шахед» в тактической глубине [4].

Технические характеристики комплекса включают работу в основных диапазонах частот управления БПЛА (433 МГц, 900 МГц, 2,4 ГГц) с возможностью постановки заградительных и прицельных помех. Мощность излучения составляет до 50 Вт в импульсном режиме, дальность эффективного подавления – до 10 км. Комплекс обладает временем развертывания, не превышающим 15 минут, и может функционировать как в автоматическом, так и в ручном режимах.

Принцип действия комплекса основан на анализе радиоэлектронной обстановки и автоматическом выборе оптимального типа помехи для подавления конкретного типа БПЛА. Встроенная библиотека сигнатур позволяет идентифицировать тип БПЛА по параметрам его излучения и формировать наиболее эффективную помеху. Первоначально система применялась для прикрытия артиллерийских расчетов и эвакуационных групп, однако в 2026 году зафиксировано ее использование для защиты воздушного пространства Киева [5].

В 2026 году на Харьковском направлении зафиксировано применение новых украинских комплексов РЭБ «Октава» и «Дамба» [6]. Указанные системы разработаны для решения тактических задач на передовой и предназначены для противодействия российским БПЛА различных классов [7].

Комплекс «Октава» функционирует в диапазоне частот 400-6000 МГц, что перекрывает основные каналы управления FPV-дронов и разведывательных БПЛА. Мощность излучения составляет до 100 Вт в непрерывном режиме, дальность эффективного подавления – до 15 км. Система способна одновременно создавать помехи по 8 целям и автоматически перестраивать частоту в зависимости от изменения параметров сигналов противника. Время реакции на изменение обстановки не превышает 0,5 секунды.

Комплекс «Дамба» специализируется на подавлении спутниковой навигации в диапазонах L1 (1575,42 МГц) и L2 (1227,6 МГц), что соответствует

сигналам GPS (Global Positioning System) и ГЛОНАСС. Мощность излучения достигает 200 Вт, зона подавления имеет радиус до 30 км. Оба комплекса интегрируются в общую систему противовоздушной обороны тактического звена и могут получать целеуказание от РЛС.

Особенностью применения «Октавы» и «Дамбы» является их размещение непосредственно на передовых позициях, что позволяет создавать локальные зоны подавления на направлениях предполагаемого применения российских БПЛА. Комплексы оснащены средствами автоматического обнаружения источников радиоизлучения и могут функционировать без участия оператора в автоматическом режиме.

В ходе специальной военной операции отмечено применение западных средств радиоэлектронной борьбы, поставляемых Украине в рамках военной помощи. Наибольшую угрозу представляют системы, способные не только осуществлять подавление, но и имитировать сигналы управления (спуфинг).

Американские комплексы РЭБ, поставленные Украине, включают средства для подавления каналов управления БПЛА в различных частотных диапазонах. По данным открытых источников, данные системы способны анализировать сигналы российских БПЛА и формировать помехи, оптимальные для подавления конкретных типов аппаратов. Дальность действия американских систем оценивается в 20-30 км, мощность излучения – до 500 Вт.

Британские системы радиоэлектронной борьбы, применяемые ВСУ, ориентированы на подавление спутниковой навигации и каналов связи в тактической глубине. Технические характеристики западных систем, как правило, закрыты, однако анализ открытых источников позволяет сделать вывод о наличии в их составе средств радиоразведки, способных оперативно вскрывать параметры сигналов российских БПЛА и адаптировать помехи под конкретные типы аппаратов.

Системный анализ применения средств радиоэлектронной борьбы противником в вооруженных конфликтах в Сирии, Нагорном Карабахе и специальной военной операции показывает, что средства РЭБ превратились в неотъемлемый элемент системы противодействия БПЛА. Противник активно развивает как собственные разработки (турецкий Koral, украинские «Ай-Петрі СВ», «Октава», «Дамба»), так и использует западные технологии.

Наиболее совершенные средства РЭБ противника способны не только подавлять, но и анализировать сигналы управления российских БПЛА, адаптируясь к изменению частотных параметров. Полученные данные могут служить основой для формирования требований к помехозащищенности каналов управления и связи, а также живучести перспективных беспилотных летательных аппаратов.

Литература

1. Афонин И. Е., Макаренко С. И., Петров С. В., Привалов А. А. Анализ опыта боевого применения групп беспилотных летательных аппаратов для поражения зенитно-ракетных комплексов системы противовоздушной обороны в военных конфликтах в Сирии, в Ливии и в Нагорном Карабахе // Системы управления, связи и безопасности. 2020. № 4. С. 163-191.

2. Макаренко С. И. Противодействие беспилотным летательным аппаратам. Монография. – СПб.: Наукоемкие технологии, 2020. – 204 с.

3. В битве за Идлиб Турция опробовала против России новое оружие // Московский комсомолец: [Электронный ресурс]. 2020. – URL: https://www.mk.ru/politics/2020/03/07/v-bitve-za-idlib-turciya-oprobovala-protiv-rossii-novoe-oruzhie.html (дата обращения: 24.02.2026).

4. БФ молодежной инициативы «Надія», Валерий Дубиль и Артем Чаплыгин доставили на восток РЭБы, средства питания и связи // Фокус: [Электронный ресурс]. 2025. – URL: https://focus.ua/ukraine/725534-bf-molodezhnoy-iniciativy-nadiya-valeriy-dubil-i-artem-chaplygin-dostavili-na-vostok-reby-sredstva-pitaniya-i-svyazi (дата обращения: 24.02.2026).

5. 15 комплексів РЕБ «Ай-Петрі» передадуть підрозділам, які захищають критичну інфраструктуру Києва – оборона України // Racurs.ua: [Электронный ресурс]. 2026. – URL: https://racurs.ua/ua/n212198-15-kompleksiv-reb-ay-petri-peredadut-pidrozdilam-yaki-zahyschaut-krytychnu-infrastrukturu.html (дата обращения: 24.02.2026).

6. В Харьковской области ВСУ задействуют новые комплексы РЭБ «Октава» и «Дамба» // Новости Mail.ru: [Электронный ресурс]. 2026. – URL: https://news.mail.ru/politics/69912028/ (дата обращения: 24.02.2026).

7. Полковник Геннадий Алехин: ВСУ опасаются броска на Харьков и укрепляют оборону за счет «Октавы» и «Дамбы» // Лента новостей Харькова: [Электронный ресурс]. 2026. – URL: https://kharkov-news.ru/society/2026/02/24/196454.html (дата обращения: 24.02.2026).

Информация об авторе

Тхакахов Алим Артурович – соискатель ученой степени кандидата технических наук. Адъюнкт научно-исследовательского центра. Военная академия связи. Область научных интересов: беспилотные летательные аппараты, маршрутизация беспилотных летательных аппаратов, разведзащищенность систем управления. E-mail: thakahov.98@bk.ru

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

УДК 004.722

Сокрытие данных на различных этапах их жизненного цикла

Савельев М. Ф., Абазина Е. С.

В статье представлена систематизация существующих направлений стеганографии в соответствии с жизненным циклом данных, а также определены направления, ранее не классифицированные, как стеганографические, однако фактически ими являющиеся. Определение методов и способов сокрытия по стадиям жизненного цикла данных расширяет научно-методический аппарат стеганографии.

3

Ключевые слова: *стеганография, стадии жизненного цикла, скрытое хранение данных, скрытая обработка данных, скрытое представление данных, скрытое размещение данных, скрытое уничтожение данных.*

Современные подходы к обеспечению безопасности и защиты информации [1, 2] с использованием программно-технических способов все чаще предусматривают не только возможность, но также желательность и даже необходимость применения стеганографических мер наравне с прочими мерами технической защиты информации.

Современная стеганография является отраслью знаний о сокрытии факта наличия информации, представленной цифровыми данными.

Основными целями стеганографии являются:

– сокрытие конфиденциальной информации;

– подтверждения авторского права обладателя защищаемой информации;

– подтверждение подлинности и целостности защищаемой информации.

Последние две цели преследуют методы и способы таких стеганографических направлений, как цифровые отпечатки (ЦО) и цифровые (стеганографические) водяные знаки (СВЗ/ЦВЗ) [3-8].

Сокрытие конфиденциальных данных с привлечением стеганографии осуществляется при их передаче, а также при хранении.

Эти процессы соответствуют одноименным этапам жизненного цикла (ЖЦ) данных, который также включает стадии формирования данных, сбора данных, обработки данных, представления и использования данных, уничтожения данных [9, 10]. Однако в существующих направлениях стеганографии стадии, кроме передачи и хранения, не отражены.

Между тем, в публикациях, посвященных кибербезопасности [11-13] встречаются упоминания методов сокрытия данных при реализации нарушителями различных видов атак.

В частности, стеганографические методы используются для решения следующих задач [11]:

Статья (тезис) опубликована в сборнике докладов конференции:
I семинар научной школы профессора С. И. Макаренко. Сборник тезисов докладов конференции. г. Санкт-Петербург, 20-21 декабря 2025 года. – СПб.: Наукоемкие технологии, 2026.

– обход цензуры – сокрытие источника медиа контента, несоответствующего нормам цензуры;

– альтернатива невзаимозаменяемыми токенами (non-fungible token – NFT) при аутентификации источника данных и подтверждении авторского права;

– в интересах кибератак.

Особенно широкое применение и развитие методы и способы стеганографии находят для реализации задачи реализации кибератак. Наиболее часто к сокрытию данных обращаются в следующих случаях [11-13]:

– встраивание вредоносных программ в файлы, не вызывающие подозрений, например, мультимедиа;

– использование стеганографии в программах-вымогателях на стадии извлечения данных;

– скрытное размещение исполнительного кода в пустых полях веб-страниц; сокрытия похищенных данных в изображениях;

– сокрытие веб-скиммеров в файлах векторной графики на платежных страницах интернет-магазинов;

– преодоление систем мониторинга и управления сетевыми ресурсами;

– камуфляж программного обеспечения (ПО);

– создание скрытых каналов утечки информации от законного пользователя;

– недекларированное хранение информации - маскировка данных одного формата под данные других форматов;

– скрытая передача управляющего сигнала;

– использование стеганографии для создания botnet-сетей в части сокрытия управления botnet-устройствами через вредоносное ПО злоумышленниками с центральных серверов (C&C) или в децентрализованной P2P-модели;

– использование стеганографии для Funkspiel («Радиоигры»), подход в которой аналогичен технологии command & control deception (имитация управления и контроля) и предусматривает захват C&C-серверов botnet-устройств с последующей передачей ложных команд для нейтрализации сети или сбора данных о злоумышленниках;

– стеганографическое отвлечение вычислительных мощностей и временных ресурсов злоумышленника на оперативную реагирование на генерируемые стегоконтейнеры (при условии временных и вычислительных затрат злоумышленника на обнаружение значительно больших, чем на их формирование у санкционированного источника стегоконтейнеров).

– стеганографическое отслеживание за счет внедрение стегометок для поимки злоумышленников в инфокоммуникационных системах по аналогии с подходом honeypot;

– умышленное запутывание исполняемого кода с целью сокрытия его недекларированного функционала;

– сокрытие дополнительных данных, регистрируемых системами чувств человека, незаметных для сознания, побуждающих к не осознанным действиям («25 кадр», раздражающие звуки, навязчивые фразы, образы и т.д., размещаемые в цифровых данных).

Таким образом, приведенные цели и задачи, решаемые средствами стеганографии демонстрируют принадлежность к ней компьютерной вирусологии, методов и техник информационно-психологического воздействия, обфускации кода и т.д. Это в свою очередь определяет необходимость пересмотра границ существующей стеганографии и расширения системы принятой классификации методов и способов сокрытия данных.

Обзор публикаций с упоминаниями сокрытия данных, используемом не только при передаче и хранении скрываемых данных, в совокупности с достаточно частым применением методов и способов стеганографии при реализации кибератак, позволяет сформулировать новые направления стеганографии, которые уже фактически существуют, но не определяются, как причастные к стеганографии. Такими направлениями являются:

– скрытое формирование данных;
– скрытая передача данных;
– скрытый сбор данных;
– скрытое хранение данных;
– скрытая обработка данных;
– скрытое уничтожение данных.

Для представленных направлений стеганографии очевидна возможность их применения для достижения не только целей безопасности информации, но и наоборот – для совершения различных атак на защищаемые данные. Реализация стеганографических методов и способов во многом определяется, будут ли они в дальнейшем применяться как разрешенные, санкционированные законодательством, или нет. В этой связи в терминология стеганографии требует расширения понятием субъект стеганографии – лицо, применяющее методы и способы стеганографии.

Соответственно субъекты стеганографии могут быть санкционированными, т.е. использующими стеганографию для достижения законных целей; и несанкционированными – применяющими стеганографию в обход закона, с его нарушением и для достижения приступных целей.

Очевидно, цели, в интересах достижения которых, субъекты стеганографии прибегают к тем или иным методам и способам различных стеганографических направлений, так же отличны [9-16].

Цели применения стеганографии для санкционированных субъектов стеганографии:

– обеспечение конфиденциальности данных;
– обеспечение доступности данных;
– обеспечение целостности данных;
– обеспечение подлинности (аутентификации) данных;
– обеспечение аутентификации отправителя (источника) данных;
– защита авторского права.

Цели применения стеганографии для несанкционированных субъектов стеганографии:

– атака на конфиденциальность данных;
– атака на доступность данных;

– атака на целостность данных;
– атака на подлинность данных;
– атака на аутентификацию отправителя (источника) данных;
– атака на защиту авторского права.

Взаимосвязь целей, субъектов и этапов жизненного цикла данных и направлений стеганографии достаточно прозрачна и представлена в таблице.

Таблица – Взаимосвязь целей, субъектов, этапов жизненного цикла данных и направлений стеганографии

Субъекты стеганографии	**Цели стеганографии**	**Направления стеганографии**	**Примеры реализации**
Этап ЖЦ данных - формирование данных			
санкционированные	обеспечение доступности данных	скрытое формирование данных	тихое резервирование
несанкционированные	атака на доступность данных		установка вредоносного ПО
Этап ЖЦ данных - передача данных			
санкционированные	обеспечение конфиденциальности данных	скрытая передача данных	сохранение в тайне факта передачи данных
несанкционированные	атака на конфиденциальность данных		несанкционированная передача (кража) данных
Этап ЖЦ данных - сбор данных			
санкционированные	обеспечение доступности данных	скрытый сбор данных	тихое резервирование, тихая диагностика и мониторинг
несанкционированные	атака на доступность данных, на доступность системы		несанкционированное накопление и анализ данных, анализ функционирования системы
Этап ЖЦ данных - хранение данных			
санкционированные	обеспечение конфиденциальности данных	скрытое хранение данных	сохранение в тайне факта хранения данных
несанкционированные	атака на конфиденциальность данных		размещение вредоносного ПО
Этап ЖЦ данных - обработка данных			
санкционированные	обеспечение доступности	скрытая обработка данных	тихое резервирование, мониторинг
несанкционированные	атака на доступность		тайное функционирование вредоносного по, управление botnet-устройствами
Этап ЖЦ данных - представление и использование данных			
санкционированные	обеспечение целостности, подлинности данных:	цифровые отпечатки	внедрение ЦО, СВЗ/ЦВЗ в защищаемые данные
	аутентификация источника данных, разделение «свой – чужой»		
	защита авторского права, разделение «свой – чужой»	цифровые водяные знаки	

Субъекты стеганографии	Цели стеганографии	Направления стеганографии	Примеры реализации
несанкционированные	атака на целостность, подлинность данных, аутентификацию источника данных	имитонавязывание	подмена, искажение данных
	атака на аутентификацию источника данных		подмена источника данных
	атака на авторское право		кража (присвоение) данных
Этап ЖЦ данных - уничтожение данных			
санкционированные	обеспечение доступности и конфиденциальности данных	Скрытое уничтожение данных	удаление вредоносного ПО
несанкционированные	атака на доступность и конфиденциальность данных		диверсии, удаление данных защищаемых данных, удаление артефактов функционирования данных

Для разных этапов ЖЦ данных методы и способы стеганографии, применяемые санкционированными и несанкционированными субъектами могут проявляться как в виде отдельного решения (самостоятельной программы) для этапа ЖЦ, так и быть реализованными совместно для нескольких этапов ЖЦ, а также совмещая функцию сокрытия с иными.

Так этап скрытого санкционированного формирования данных может быть совмещен с этапами скрытого хранения и (или) со скрытой передачей - при тихом резервном копировании (теневом копировании, непрерывной защите данных, облачном копировании, резервировании и хранении настроек сетевых устройств) [17-19].

Скрытое санкционированное формирование данных может быть совмещено со скрытым представлением данных – при формировании ЦО или СВЗ/ЦВЗ [3-8, 20-23] при обеспечении защиты целостности подлинности данных, а та-же тогда, когда стеганография используется для защиты авторства цифровых данных или права обладания данными [3-8, 20-23]. Совмещение процессов формирования и представления ЦО и СВЗ/ЦВЗ крайне актуально при использовании в качестве защищаемых данных данные реального времени, например, видеотрансляции и семинары с ограниченным участием.

Стеганографическое направление скрытый сбор данных в интересах санкционированных пользователей стеганографии как правило ориентирован для обеспечения безопасности защищаемой системы обработки (а также хранения и (или) обмена данными) путем мониторинга действий авторизованных пользователей и системных компонентов для обоснованного (документированного) определения внутренних нарушителей или обнаружения уязвимостей системы.

При использовании стеганографии несанкционированно скрытое формирование данных может быть совмещено со скрытым хранением вредоносного

ПО до момента его полной установки и исполнения функций и (или) со скрытой передачей данных. Примерами могут быть скрытая доставка вредоносного ПО (QuasarRAT, Remcos, StealC) [24], реализация многоступенчатой атаки с JPG (Remcos и AsyncRAT), создание скрытых каналов управления (C2 – command and control) и обход DPI (Deep Packet Inspection «глубокая инспекция пакетов»), где стеганография используется не только для доставки вредоносного ПО, но и для маскировки его последующей связи с управляющим сервером [25]. Подавляющее большинство троянских программ для удаленного доступа (RAT) и шпионского ПО обращаются к методам и способам скрытого формирования, хранения, сбора, представления и передачи данных: начиная от доставки вредоносного ПО и заканчивая скрытым уда-ленным включением средств видео и звукозаписи терминальных средств (смартфонов).

Скрытый сбор и обработка данных несанкционированными пользователями реализована в различном ПО, например в кейлоггерах (keyloggers), регистрирующей нажатие клавиш с последующим анализом для перехвата учетных данных из браузеров (Chrome, Edge, Firefox), а также с одновременным копированием содержимого буфера обмена [26]. К несанкционированным скрытым сбору и обработке данных также относится сбор сведений о работе системы (в том числе юридических лиц и государственных организаций и учреждений) и отправка на сервер злоумышленников, которые затем могут точечно атаковать компьютеры.

Стеганографические методы и способы, используемые на стадии ЖЦ уничтожения данных для санкционированных и несанкционированных пользователей зачастую реализованы в ПО-антагонистах, ведущих противоборство. Несанкционированное использование стеганографии на этом этапе ЖЦ данных может быть направленно так же на уничтожение любых данных, а также на уничтожение или подмену ЦО и СВЗ/ЦВЗ. Подделка ЦО может использоваться не только для кражи или подмены данных, но и для обхода систем безопасности. Например, злоумышленники подменяют параметры своего устройства, искажая ЦО, создавая таким образом тысячи фейковых аккаунтов в соцсетях или на маркетплейсах (мультиаккаунтинг), для обхода банковских системы фрод-мониторинга [27]. Атаки, связанные со скрытым подменой содержимого сайтов (дефейс, defacement), в том числе платежных реквизитов при выполнении оплат в интернете [28]. К направлению скрытого представления данных несанкционированными субъектами стеганографии могут быть атаки, направленные на манипулирование данными при обучении искусственного интеллекта (ИИ). Злоумышленник подменяет верные знания в интернете своим вымыслом, и ИИ, не имея надежных механизмов верификации, распространяет эту ложь, создавая огромные риски для репутации, финансов и даже здоровья людей.

Необходимо также отметить случаи использования стеганографии для скрытого сбора и обработки данных без нарушения закона, но и без осознанного согласия правообладателя данных. В таких ситуациях скрытый сбор данных выполняется в «сером» режиме: правообладатель данных соглашается на мониторинг и анализ данных без какого-либо ознакомления или анализа в совокупности условий. Примером являются случаи мониторинга облачными сервисами

и ПО, к которым обращается обладатель данных. Отчеты, представленные в [29], подтверждают сбор значительных объемов телеметрии Windows 10 и 11, включая данные об устройстве, производительности, установленном ПО, а также возможных режимах, истории браузера, анализах трафика.

Таким образом, методы и способы стеганографии применяются как санкционированными, так и несанкционированными субъектами стеганографии и реализуются на всех этапах жизненного цикла данных, что подтверждается публикациями, но не классифицируется как стеганографические направления. Сформулированные направления стеганографии по стадиям жизненного цикла данных расширяют научно-методический аппарат стеганографии и способствуют развитию методов и способов стеганографии.

Литература

1. Об информации, информационных технологиях и о защите информации. Федеральный закон РФ от 27.07.2006 № 149-ФЗ // Официальный интернет-портал правовой информации [Электронный ресурс]. – URL: http://pravo.gov.ru/proxy/ips/?docbody&nd=102108264 (дата обращения: 10.12.2025).
2. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения – М.: Стандартинформ, 2008. – 7 с.
3. Грибунин В. Г., Костюков В. Е., Мартынов А. П., Николаев Д. Б., ФомченкоВ. М. Стеганографические системы. Критерии и методическое обеспечение: учеб.-метод. пособие / Под ред. д-ра техн. наук В. Г. Грибунина. – Саров: ФГУП «РФЯЦ-ВНИИЭФ», 2012. – 324 с.
4. Грибунин В. Г., Оков И. Н., Туринцев И. В. Цифровая стеганография. М.: Солон-Пресс, 2009. 272 с.
5. Коржик В. И., Красов А. В. Цифровая стеганография: Учебник. – М.: КноРус, 2023. – 323 с.
6. Макаренко С. И. Эталонная модель взаимодействия стеганографических систем и обоснование на ее основе новых направлений развития теории стеганографии. // Вопросы кибербезопасности. 2014. № 2(3). С. 24-32.
7. Абазина Е. С., Ерунов А. А. Цифровая стеганография: состояние и перспективы. // Вопросы кибербезопасности. 2016. № 2(3). С. 182-201.
8. Абазина Е. С., Цветков К. Ю. Концептуальная модель взаимодействия стегосистем передачи данных в составе эталонной модели взаимодействия открытых систем. // Труды Военно-космической академии имени А.Ф. Можайского. 2019. № 668. С. 70-80.
9. ГОСТ Р 59897-2021. Данные для систем искусственного интеллекта в образовании. Требования к сбору, хранению, обработке, передаче и защите данных. – М.: Стандартинформ, 2021. – 7 с.
10. Макаренко С. И. Интероперабельность организационно-технических систем: Монография. – СПб.: Наукоемкие технологии. 2024. – 313 с.
11. Что такое стеганография? Определение и описание // Касперский лаборатория: официальный сайт [Электронный ресурс]. 08.02.2023. – URL: https://www.kaspersky.ru/resource-center/definitions/what-is-steganography (дата обращения 10.12.2025).

10. Стеганография в XXI веке. Цели. Практическое применение. Актуальность // Хабр [Электронный ресурс]. 2015. – URL: https://habr.com/ru/articles/253045/ (дата обращения 10.12.2025).

13. Омельченко И. Когда спрятать недостаточно: как устроены атаки на системы тайной передачи информации // Хабр [Электронный ресурс]. 2025. – URL: https://habr.com/ru/companies/bastion/articles/882522/ (дата обращения 10.12.2025).

14. Рудниченко А. К. Применение простой стеганографии при передаче файлов в интернете // Молодой ученый. 2017. – № 3 (137). – С. 49-51. [Электронный ресурс]. 17.01.2017. – URL: https://moluch.ru/archive/137/38298/ (дата обращения 10.12.2025).

15. Колмаков М. В., Блинова Е. А. Особенности применения стеганографических методов в альтернативных потоках файловой системы NTFS // Материалы 69 науч.-техн. конф. учащихся, студентов и магистрантов. – Минск, 2018. – С. 9–13.

16. Стеганография в файловой системе // Хабр [Электронный ресурс]. 28.01.2026 – URL: https://habr.com/ru/articles/347604/ (дата обращения 28.01.2026).

17. R1Soft. Continuous Data Protection 3.0 – Standard Edition. [Электронный ресурс]. 2024. – URL: https://wiki.r1soft.com/pages/viewpagesrc.action%3FpageId=4461001.html (дата обращения 10.12.2025).

18. Enabling Volume Shadow Service (VSS) for Windows File System Backups // Commvault Long-Term Support Release 11.40 [Электронный ресурс]. 12.11.2025. – URL: https://documentation.commvault.com/2024e/commcell-console/enabling_volume_shadow_service_vss_for_windows_file_system_backups.html (дата обращения 10.12.2025).

19. Google Transparency Center. (2025). Google Photos Policies and Guidelines [Электронный ресурс]. – URL: https://transparency.google/intl/en_ph/our-policies/product-terms/google-photos/ (дата обращения 10.12.2025).

20. Ларионова К. Е., Губенко Н. Е. Система внедрения ЦВЗ в графические файлы на основе метода картера [Электронный ресурс]. 2009. – URL: https://masters.donntu.ru/2009/fvti/larionova/library/article1.htm (дата обращения 10.12.2025).

21. В США разработано новое средство обхода цензуры в интернете // Утро.ру – сайт новостей России и мира [Электронный ресурс]. 10.12.2025. – URL: https://utro.ru/news/2002/07/23/91143.shtml (дата обращения 23.07.2002).

22. Зотин А. Г., Проскурин А. В. Способы ускорения подготовки и встраивания цифрового водяного знака с использованием мобильных устройств на основе преобразования Арнольда и вейвлет-преобразования |// Программные продукты и системы. - Т. 38 №4. [Электронный ресурс]. – URL: https://www.swsys.ru/print/article_print.php?id=4834 (дата обращения 10.12.2025).

23. Крахмаль М. В., Завадская Т. В. Исследование метода встраивания цифровых водяных знаков на основе деления изображения–контейнера / материалы VI Международная научно–практическая конференция «Современные тенденции развития и перспективы внедрения инновационных

технологий в машиностроении, образовании и экономике», 13–14 мая 2019, г. Азов [Электронный ресурс]. 2019. – URL: https://masters.donntu.ru/2019/fknt/krakhmal/library/article1.htm (дата обращения 10.12.2025).

24. QuasarRAT через WinRAR CVE-2025-6218: стеганография в PNG // Revolution Conference – сайт ежегодной конференция, посвященная ИБ и ИТ-технологиям [Электронный ресурс]. 09.12.2025. – URL: https://cisoclub.ru/quasarrat-cherez-winrar-cve-2025-6218-steganografija-v-png/ (дата обращения 10.12.2025).

25. Авсентьев О. С., Бутов В. В., Цыганов К. А. Функциональная модель процесса реализации угроз безопасности информации с использованием скрытых стеганографических каналов внешним нарушителем // Безопасность информационных технологий. 2025. Т. 32. № 2. – URL: https://www.seqrite.com/ru/blog/steganographic-campaign-distributing-malware/ (дата обращения 10.12.2025).

26. Кейлогер // Википедия: свободная энциклопедия [Электронный ресурс]. 13.05.2019. – URL: https://ru.wikipedia.org/wiki/Кейлогер (дата обращения 10.12.2025).

27. Подмена отпечатка браузера (Fingerprint Spoofing) // multilogin: сайт управления аккаунтами [Электронный ресурс]. – URL: https://multilogin.com/ru-ru/glossary/fingerprint-spoofing/ (дата обращения 10.12.2025).

28. Что такое дефейс сайта и как защититься от подмены контента? // Solar: сайт услуг комплексной кибербезопасности [Электронный ресурс]. 30.06.2025. – URL: https://rt-solar.ru/space/blog/5632/ (дата обращения 10.12.2025).

29. Что Windows на самом деле знает о вас: разбираем телеметрию и конфиденциальность // Revienet – сайт новостей Microsoft и Windows [Электронный ресурс]. 12.07.2025. – URL: https://msreview.net/windows-10/chto-windows-na-samom-dele-znaet-o-vas-razbiraem-telemetriiu-i-konfidentcialnost.html (дата обращения 10.12.2025).

Информация об авторах

Савельев Максим Феликсович – кандидат технических наук, доцент. Начальник кафедры информационной безопасности. Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В. И. Ульянова (Ленина). Область научных интересов: безопасность информации, защита компьютерных систем и сетей, криптографические и стеганографические методы защиты информации. E-mail: mfsavelev@etu.ru

Адрес: 197022, Россия, г. Санкт-Петербург, ул. Профессора Попова 5Ф.

Абазина Евгения Сергеевна – кандидат технических наук, доцент. Доцент кафедры сетей и систем связи космических комплексов. Военно-космическая академия имени А. Ф. Можайского. Область научных интересов: стеганография, теория сигналов, перераспределение телекоммуникационного ресурса. E-mail: e.s.abazina@yandex.ru

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

УДК 623.20

Динамическая координация подсистем наблюдения и воздействия в информационном конфликте

Михайлов Р. Л

В статье приведены результаты проведенного исследования на соискание ученой степени доктора технических наук. Диссертация была защищена в 2022 году в одном из специальных диссертационных советов города Санкт-Петербурга, вследствие чего аспекты технической реализации ее результатов в данной статье отсутствуют, а сами результаты описаны сжато. Научным консультантом выступил тогда еще доцент С. И. Макаренко, что дает мне право гордиться принадлежностью к его научной школе.

Ключевые слова: *автоматизированная система управления, динамическая координация, распределение ресурсов, мониторинг, радиоподавление.*

Актуальность

Процессы конвергенции современных телекоммуникационных технологий, реализованных в ведомственных телекоммуникационных системах специального назначения (ТКС СН), с информационными технологиями ведомственных систем управления привело к созданию автоматизированных систем управления специального назначения (АСУ СН). В соответствии с подходом автора, принятом в рамках проведенного исследования, под АСУ СН понимаются территориально распределенные комплексы, состоящие из информационных устройств (ИУ) и устройств телекоммуникаций (УТ), а также соединяющие их каналы радиосвязи, обеспечивающие формирование, передачу, прием, хранение, поиск, отображение и обработку информации по заданным человеком алгоритмам и программам и предназначенные для предоставления пользователям в специальной сфере (под которой понимается сфера обороны страны, безопасности государства и обеспечения правопорядка [1]) различных информационных и телекоммуникационных продуктов и услуг. Пользователями АСУ СН выступают элементы в составе системы управления и основных (базовых) сил и средств, а также средства наблюдения и воздействия в составе соответствующих подсистем, при этом задачи оказания необходимых информационных услуг пользователям возлагаются на информационную систему (ИС) АСУ СН, а информационный обмен между указанными пользователями – на ТКС СН.

Специальная сфера использования АСУ СН подразумевает наличие конфликтных ситуаций, когда решение возложенных на соответствующие системы управления задач сопряжено с целенаправленным противодействием конфлик-

---

Статья (тезис) опубликована в сборнике докладов конференции:
I семинар научной школы профессора С. И. Макаренко. Сборник тезисов докладов конференции. г. Санкт-Петербург, 20-21 декабря 2025 года. – СПб.: Наукоемкие технологии, 2026.

тующей стороны. К субъектам конфликта в специальной сфере можно отнести государства, их союзы и коалиции; международные организации; негосударственные незаконные вооруженные формирования (НВФ) и организации террористической, экстремистской, радикальной политической и религиозной направленности (в том числе международные). Достижение преимущества в конфликте в специальной сфере достигается применением основных (базовых) сил и средств, примерами которых являются силы правопорядка, вооруженные силы и другие разноведомственные формирования специального назначения, обладающие средствами физического поражения (огневыми, оружием на новых физических принципах и т. д.). Управление данными силами и средствами осуществляется посредством принятия органами государственного управления (системой управления субъекта конфликта в специальной сфере) решения о порядке их применения и доведения до них этого решения, т. е. каждому эпизоду применения предшествует цикл управления, включающий в себя этапы сбора и обработки данных о состоянии, намерениях и действиях конфликтующей стороны; принятия решения на применение основных (базовых) сил и средств; доведение решения до основных (базовых) сил и средств, а также контроля результатов их применения. Эффективное применение основных (базовых) сил и средств сопряжено с необходимостью проводить данные этапы в рамках цикла управления ими быстрее, нежели другая сторона конфликта. При этом задачи сбора данных о состоянии, намерениях и действиях конфликтующей стороны возлагаются на средства наблюдения в составе соответствующей подсистемы, а затруднение выполнения аналогичных действий конфликтующей стороной – на средства из состава подсистемы воздействия.

Таким образом, на этапе сбора и обработки данных о состоянии, намерениях и действиях сторон в ходе конфликта в специальной сфере имеет место информационный конфликт между АСУ СН в их составе, достижение преимущества в котором способствует получению превосходства субъекта в конфликте в целом. Под информационным конфликтом АСУ СН в работе понимается процесс столкновения субъектов конфликта в различных сферах специальной деятельности на этапе сбора и обработки данных о состоянии, намерениях и действиях конфликтующей стороны, каждый из которых стремится к обеспечению упреждающего принятия решений в цикле управления основными (базовыми) силами и средствами и предпринимает действия по снижению аналогичных возможностей оппонента. Целью АСУ СН в информационном конфликте является достижение информационного превосходства, т. е. способности осуществлять непрерывный сбор сведений о конфликтующей стороне, их обработку, распределение потока достоверной информации в интересах применения основных (базовых) сил и средств, а также способность обеспечить упреждение выполнения аналогичных действий конфликтующей стороны. Достижение этой цели обеспечивается посредством информационных контактов средств наблюдения и воздействия с УТ из состава ТКС противостоящей АСУ СН.

Под информационным контактом средства наблюдения с УТ понимается процесс перехвата и несанкционированного доступа к информации в каналах связи между УТ в составе ТКС противостоящей стороны (нарушение свойства

конфиденциальности информации). Результатом подобного информационного контакта является собранный объем оперативной информации, которая в дальнейшем используется системой управления при принятии решений о применении основных (базовых) сил и средств. Под информационным контактом средства воздействия с УТ понимается процесс разрушения и блокирования информации в каналах связи между УТ противостоящей стороны (нарушают свойство доступности информации). Результатом подобного информационного контакта является потеря объема оперативной информации, необходимой системе управления конфликтующей стороны при принятии решений. Вследствие этого, совокупность УТ противостоящей стороны выступает как общий ресурс подсистем наблюдения и воздействия для реализации информационных контактов. Следует отметить, что одно и то же УТ не может одновременно служить объектом информационного контакта для средства наблюдения и средства воздействия. **В связи с этим, АСУ СН выступает как орган, координирующий подсистемы наблюдения и воздействия, задачами которого является определение рационального распределения между этими подсистемами УТ с целью обеспечения их эффективного применения в интересах достижения превосходства в информационном конфликте.**

Очевидно, что обеспечить информационное превосходство в информационном конфликте лишь за счет совершенствования отдельных подсистем АСУ СН с учетом несравнимо большего экономического потенциала противостоящих РФ в конфликте в специальной сфере субъектов, не представляется возможным. В этой связи в рамках проведенного исследования была выдвинута гипотеза о том, что динамическая координация подсистем наблюдения и воздействия АСУ СН позволит повысить эффективность использования в условиях информационного конфликта как этих подсистем, так и АСУ СН в целом, за счет получения синергетического эффекта, что обеспечит достижение информационного превосходства. Подтверждение данной гипотезы, по мнению автора, являлось актуальным для практики использования АСУ СН в условиях информационного конфликта.

Таким образом, в области информационного конфликта в специальной сфере имеет место проблемная ситуация, между необходимостью достижения информационного превосходства в информационном конфликте АСУ СН и недостаточным уровнем развития теории управления, который не позволяет сформировать научно-обоснованные технические решения по динамической координации подсистем в составе наблюдения и воздействия в информационном конфликте. Цель исследования – повышение эффективности использования АСУ СН в условиях информационного конфликта. Объект исследования – АСУ СН. Предмет исследования – динамическая координация подсистем наблюдения и воздействия АСУ СН в условиях информационного конфликта.

Для достижения цели исследования, с учетом выбранного объекта и предмета исследования, было необходимо разрешить следующую научную проблему. Научная проблема – разработка научно-методического аппарата динамической координации подсистем наблюдения и воздействия АСУ СН в условиях информационного конфликта.

Постановка проблемы

Для формальной постановки и решения научной проблемы были введены обозначения, представленные в таблице 1.

Таблица 1 – Обозначения

Обозначение	Физический смысл обозначения
$\{m(t, p(t), v(t, p), u_1(t, p), u_2(t, p))\}_{2.1}$	– комплекс моделей динамической координации подсистем АСУ СН в условиях информационного конфликта;
$\{m(X, Y, p(t), t)\}_{2.2}$	– комплекс моделей распределения УТ противостоящей стороны в условиях информационного конфликта
$Mk_{1.4}(T_1, T_2, p(t), t)$	– методика оценивания информационного превосходства в информационном конфликте
Md	– метод
Mk	– методика
$p(t)$	– процесс информационного конфликта АСУ СН
t	– параметр времени
W_1	– множество управляющих воздействий на процесс информационного конфликта со стороны подсистемы наблюдения
W_2	– множество управляющих воздействий на процесс информационного конфликта со стороны подсистемы воздействия
$v(t, p)$	– стратегия АСУ СН в информационном конфликте
$u_1(t, p)$	– стратегия подсистемы наблюдения в информационном конфликте
$u_2(t, p)$	– стратегия подсистемы воздействия в информационном конфликте
X	– вектор (матрица) распределения УТ стороны 2 между подсистемами наблюдения и воздействия стороны
Y	– вектор (матрица) распределения УТ стороны 1 между подсистемами наблюдения и воздействия стороны 2
$P_{ИП}(Mk_{1.4})$	– показатель информационного превосходства в информационном конфликте, определяемый при помощи методики 1.4
$P_{ИП}^{треб}$	– требуемый уровень показателя информационного превосходства в информационном конфликте
$E(P_{ИП}^{треб})$	– показатель эффективности использования АСУ СН в условиях информационного конфликта при выполнении критерия обеспечения информационного превосходства

С учетом введенных обозначений проблема исследования формализовалась следующим образом: разработка комплекса моделей динамической координации подсистем АСУ СН в условиях информационного конфликта $\{m(t, p(t), v(t, p), u_1(t, p), u_2(t, p))\}_{2.1}$ и основанных на этих моделях методов динамической координации $\{Md_{3.1}, Md_{3.2}, Md_{3.3}\}$, а также комплекса методик $\{Mk_{3.4}, Mk_{3.5}, Mk_{3.6}, Mk_{3.7}, Mk_{3.8}, Mk_{3.9}\}$ для частных условий использования АСУ СН, которые бы обеспечивали

выполнение критерия информационного превосходства $P_{ИП} \geq P_{ИП}^{треб}$ при максимально достижимом значении показателя эффективности использования АСУ СН в условиях информационного конфликта $E(P_{ИП}^{треб})$:

$$\left(\left\{Md_{3.1}, Md_{3.2}, Md_{3.3}\right\} \middle| \left\{m(t, p(t), v(t, p), u_1(t, p), u_2(t, p))\right\}_{2.1} \rightarrow \right.$$

$$\rightarrow \left\{W_1, W_2, t\right\}) \times \left\{m_{2.2.1}\left(X, Y, p(t)\right), m_{2.2.2}\left(X, Y, p(t)\right)\right\} =$$

$$= \left\{Mk_{3.4}, Mk_{3.5}, Mk_{3.6}, Mk_{3.7}, Mk_{3.8}, Mk_{3.9}\right\} \rightarrow$$

$$\rightarrow P_{ИП}\left(Mk_{1.4}\right) \left| \begin{array}{l} P_{ИП}\left(Mk_{1.4}\right) \geq P_{ИП}^{треб} \\ E\left(P_{ИП}^{треб}\right) \rightarrow \max \end{array} \right. .$$

Модели и методы динамической координации подсистем наблюдения и воздействия АСУ СН

Учитывая обширность предметной области информационного конфликта в специальной сфере, а также разнообразие и развитие способов применения средств в составе подсистем наблюдения и воздействия, на основе проведенного анализа предметной области [2-12] были введены следующие рамки исследования:

1) новые условия, определяющие актуальность и практическую значимость исследования: развитие инструментария (средств и способов) обеспечения информационного превосходства, которые актуализировали аспекты использования АСУ СН в условиях информационного конфликта: ограниченная качеством подсистем наблюдения и воздействия эффективность функционирования АСУ СН и отсутствие технологии их динамической координации в интересах получения синергетического эффекта;
2) новые факторы, определяющие научную новизну исследования: учет динамического характера координации подсистем АСУ СН и формализация координирующих сигналов в виде распределения в каждый момент времени УТ для осуществления информационных контактов; учет вклада подсистемы наблюдения в снижение длительности сбора информации в цикле управления «своими» основными (базовыми) силами и средствами, а подсистемы воздействия – в увеличение длительности процесса сбора информации в цикле управления основными (базовыми) силами и средствами конфликтующей стороны, при этом данные факторы были взаимоувязано формализованы в виде процесса динамического двунаправленного информационного конфликта;
3) показатель информационного превосходства в информационном конфликте АСУ СН – вероятность информационного превосходства, характеризующий интегральное преимущество АСУ СН в длительности цикла управления основными (базовыми) силами и средствами, а именно – в снижении длительности процесса сбора данных о состоянии, намерениях и действиях конфликтующей стороны в интересах принятия решений о применении основных (базовых) сил и средств;

4) критерий обеспечения информационного превосходства в информационном конфликте АСУ СН – превышение вероятности информационного превосходства требуемого значения, при этом данное значение определяется вышестоящей системой управления (субъектом конфликта в специальной сфере) в диапазоне $[0{,}5; 0{,}9]$;
5) показатель эффективности использования АСУ СН в условиях информационного конфликта отражает синергетический эффект от динамической координации подсистем АСУ СН, выражающийся в снижении требуемого объема ресурса (УТ противостоящей стороны) в процессе его перевода в целевой эффект от использования АСУ СН (выполнение критерия обеспечения информационного превосходства в информационном конфликте);
6) информационный обмен между пользователями ТКС СН осуществляется по каналам радиосвязи, информационными услугами, предоставляемыми пользователям со стороны ИС АСУ СН, является решение расчетных задач при выработке стратегии применения средств подсистем наблюдения и воздействия в информационном конфликте;
7) рассматриваемый прототип АСУ СН – обобщенный вариант Единой системы управления тактического звена управления (ЕСУ ТЗ) в типовом составе программно-аппаратных комплексов связи и передачи данных (соответствуют ТКС), поддержки принятия решений (соответствуют ИС), а также средств мониторинга (соответствуют средствам подсистемы наблюдения) и средств радиоподавления (соответствуют средствам подсистемы воздействия).

Схема информационного конфликта АСУ СН с учетом принятых рамок исследования приобретет вид, представленный на рис. 1.

Общая последовательность проведенного исследования и взаимосвязь его результатов приведена на рис. 2.

На первом этапе был разработан методический аппарат оценивания информационного превосходства в информационном конфликте АСУ СН.

Для учета временных параметров конфликтного взаимодействия АСУ СН, был предложен новый базовый подход к формализации динамического информационного конфликта АСУ СН методами актуарной математики [13, 14], которые формализуют процессы конфликтного взаимодействия «страховая компания – клиент». Данный подход отличался от известных тем, что на более высоком теоретическом уровне обобщал известные работы в области динамического информационного конфликта, и в отличие от известных моделей типа «страховая компания-клиент» из теории актуарной математики, учитывал особенности конфликта АСУ СН как совокупности технических подсистем.

Предложенный подход к моделированию динамического информационного конфликта был использован для построения как общих (обобщающих уже существующие модели информационного конфликта), так и частных моделей информационных контактов УТ со средствами наблюдения и воздействия. Кроме того, на основе данного подхода разработана методика оценивания информационного превосходства в информационном конфликте

АСУ СН. Его приложение к моделированию динамического информационного конфликта методами актуарной математики позволило синтезировать соответствующую динамическую модель [15].

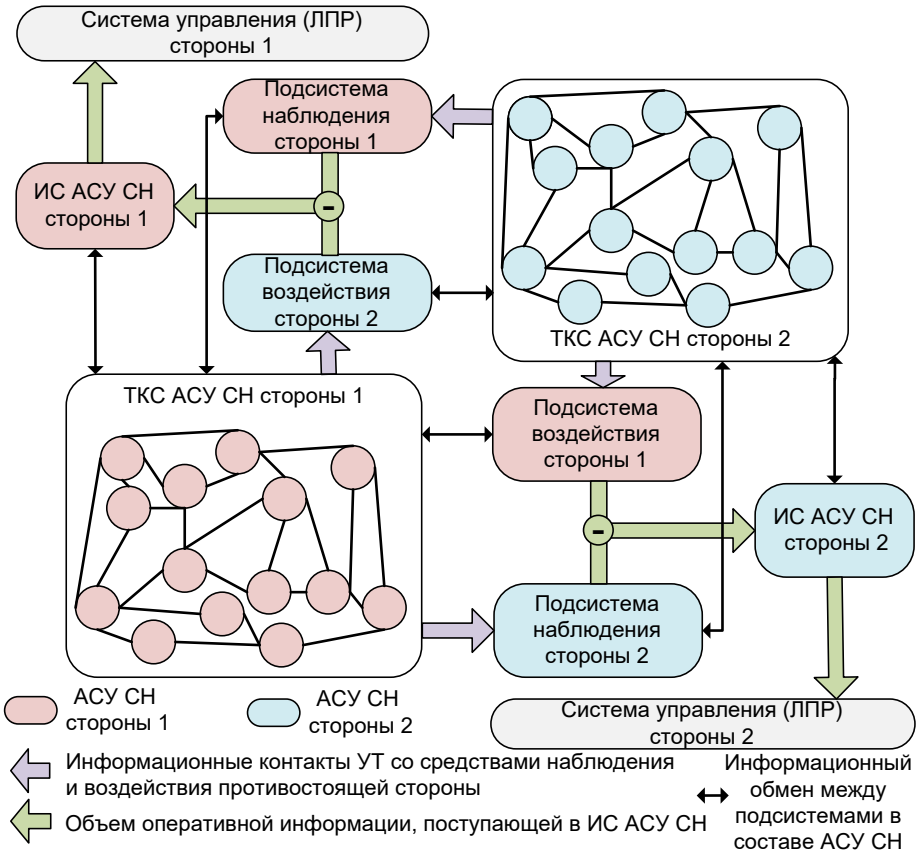

Рис. 1. Схема информационного конфликта АСУ СН с учетом принятых ограничений

На основе данной модели были исследован процесс накопления сторонами информационного конфликта информации, необходимой для принятия решения о применении основных (базовых) сил и средств. Проведенное исследование позволило обосновать пути достижения информационного превосходства на этапе сбора данных о состоянии, намерениях и действиях конфликтующей стороны цикла управления основными (базовыми) средствами.

Для исследования процессов отображения информационных контактов УТ со средствами наблюдения и воздействия в виде изменения общих объемов информации, требуемых сторонам для принятия решения о применении основных (базовых) сил и средств с требуемой достоверностью и формализации результатов этих информационных контактов с позиции снижения (для подсистемы наблюдения) «своего» времени сбора данных о состоянии, намерениях и действиях конфликтующей стороны и увеличения (для подсистемы воздействия) аналогичного показателя для последней была разработана модель информационных контактов устройств телекоммуникации АСУ СН со средствами наблюдения и воздействия противостоящей стороны [16].

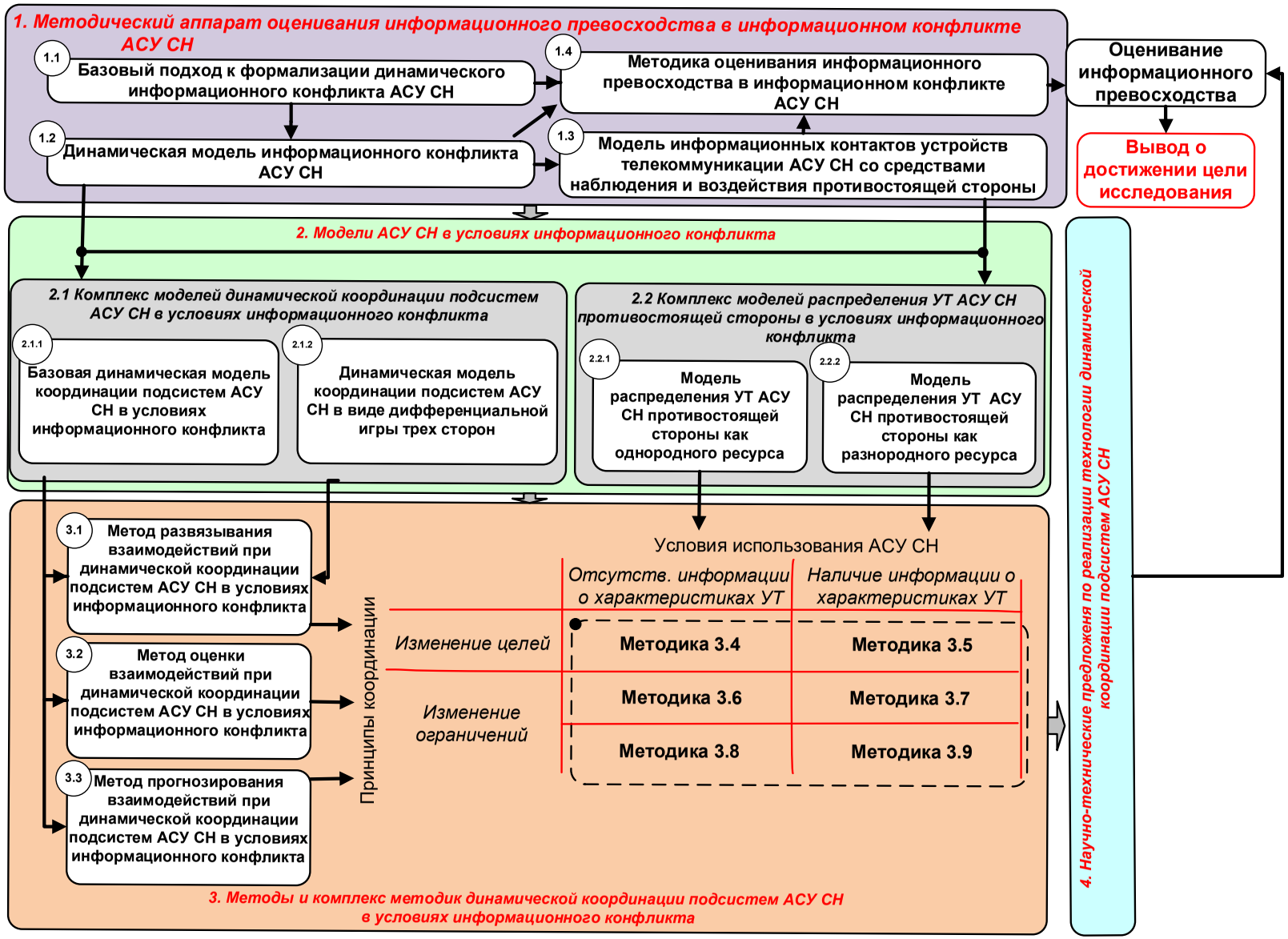

Рис. 2. Общая последовательность исследования

На основе результатов исследования вышеуказанных моделей была разработана методика оценивания информационного превосходства в информационном конфликте АСУ СН [17]. В рамках методики производится оценивание информационного превосходства одной из сторон информационного конфликта по показателю вероятности достижения информационного превосходства в информационном конфликте АСУ СН $P_{ИП}$. Введение данного показателя обусловлено тем, что существующие показатели оценивают исключительно качество подсистем АСУ СН и не подходят в качестве критериальной оценки эффективности использования АСУ СН в информационном конфликте как системы в целом. Еще одной отличительной чертой данной методики, которая составляет ее научную новизну, является использование в качестве исходных данных интенсивности процессов сбора и обработки информации конфликтующих сторон для последующего принятия решения о применении основных (базовых) сил и средств и математические ожидания приростов данных процессов для каждой из сторон конфликта.

Итоговое теоретическое обобщение разработанных моделей и методик позволило сформулировать общий вывод о том, что **рост отношения интенсивностей процессов сбора данных о состоянии, намерениях и действиях конфликтующей стороны оказывает большее влияние на изменение показателя вероятности информационного превосходства в информационном конфликте АСУ СН нежели отношение их математических ожиданий.** Таким образом, достижение информационного превосходства в информационном конфликте АСУ СН достигается, в первую очередь, рациональным распределением УТ АСУ СН между подсистемами наблюдения и воздействия, а не усовершенствованием качества самих технических средств в составе данных подсистем.

На втором этапе были разработаны модели АСУ СН в условиях информационного конфликта. На основе динамической модели информационного конфликта АСУ СН и модели информационных контактов УТ АСУ СН со средствами наблюдения и воздействия противостоящей стороны с целью конкретизации условий достижения информационного превосходства в информационном конфликте АСУ СН при динамической координации подсистем АСУ СН был разработан комплекс моделей динамической координации подсистем АСУ СН в условиях информационного конфликта. Состав комплекса:

- базовая динамическая модель координации подсистем АСУ СН в условиях информационного конфликта [18-20];
- динамическая модель координации подсистем АСУ СН в виде дифференциальной игры трех сторон [21, 22];
- модель ТКС при координации подсистем АСУ СН [23].

В интересах учета условий использования АСУ СН, связанных с наличием или отсутствием информации о характеристиках УТ АСУ СН в информационном конфликте, и с целью конкретизации подходов к формализации стратегий рационального распределения УТ АСУ СН был разработан комплекс моделей распределения УТ АСУ СН противостоящей стороны в условиях информационного конфликта [24-26], включающий в себя:

– модель распределения УТ АСУ СН противостоящей стороны как однородного ресурса;
– модель распределения УТ АСУ СН противостоящей стороны как разнородного ресурса.

В дальнейшем, на основе комплекса моделей динамической координации подсистем АСУ СН в условиях информационного конфликта были предложены методы и комплекс методик динамической координации подсистем АСУ СН в условиях информационного конфликта.

Разработанными методами динамической координацией являлись:

1) Метод развязывания взаимодействий при динамической координации подсистем АСУ СН в условиях информационного конфликта [27].
2) Метод оценки взаимодействий при динамической координации подсистем АСУ СН в условиях информационного конфликта [28].
3) Метод прогнозирования взаимодействий при динамической координации подсистем АСУ СН в условиях информационного конфликта [29].

Теоретическая общность и универсальность разработанных методов динамической координации подсистем АСУ СН доказывается тем, что каждый из них, в частных условиях, будучи приложенным к различным моделям распределения УТ АСУ СН противостоящей стороны, сводится к конкретным частным методикам, которые в рамках исследования были объединены в комплекс методик динамической координации подсистем АСУ СН (рис. 3).

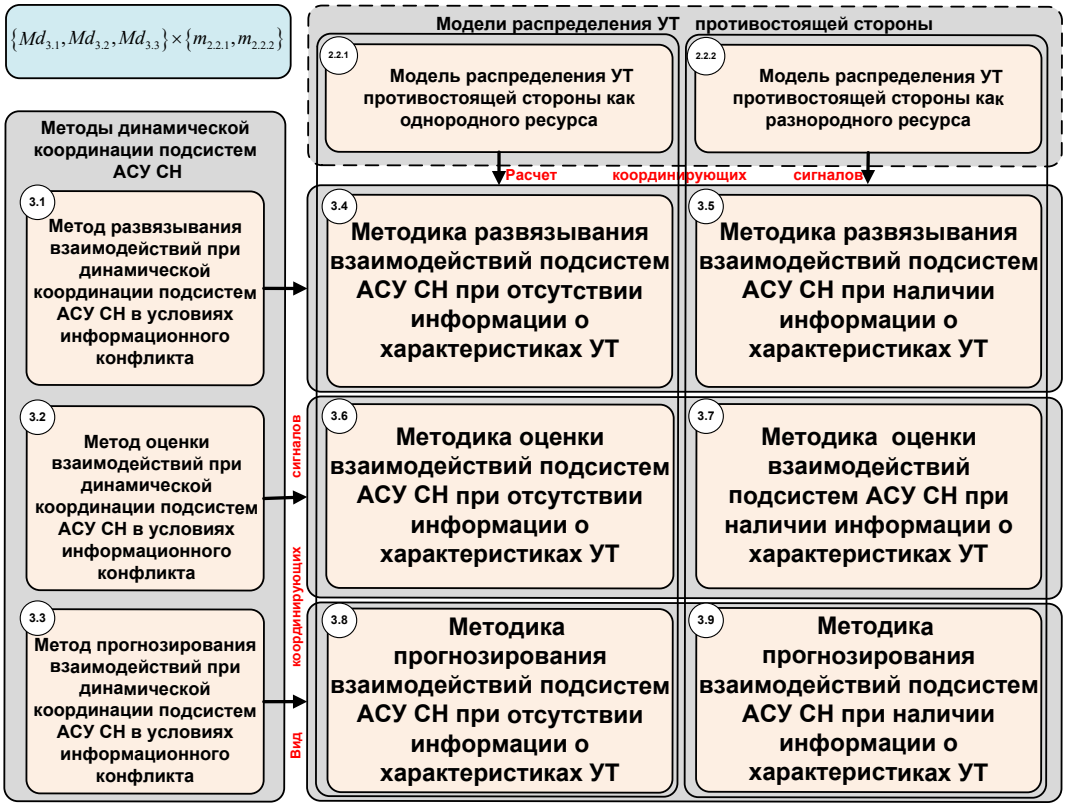

Рис. 3. Схема синтеза методик динамической координации подсистем АСУ СН

С учетом данных условий обосновано отношение предпочтительности применения методов динамической координации подсистем, которое сохраняется и применительно к частным методикам на их основе при постоянных условиях применения АСУ СН в информационном конфликте, т. е. рассмотрении УТ АСУ СН либо как однородного, либо как разнородного ресурса.

На заключительном этапе были разработаны научно-технические предложения по реализации технологии динамической координации подсистем АСУ СН, а также проведено имитационное моделирование типового сценария информационного конфликта прототипа объекта исследования (ЕСУ ТЗ) и аналогичной системы зарубежного производства.

Результаты зависимости показателя информационного превосходства в информационном конфликте АСУ СН $P_{ИП}$ с позиции стороны 1 от отношения количества обнаруженных стороной 1 и стороной 2 УТ представлены на рис. 4.

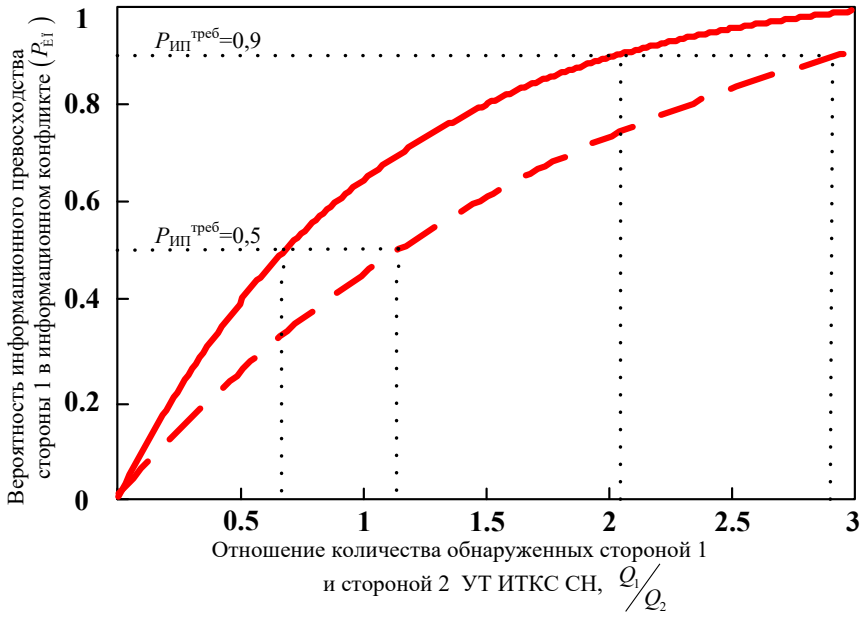

Рис. 4. Зависимость показателя информационного превосходства в информационном конфликте АСУ СН $P_{ИП}$ от отношения Q_1/Q_2

Значение показателя информационного превосходства в информационном конфликте АСУ СН $P_{ИП}$ до внедрения разработанных научно-технических предложений по реализации технологии динамической координации подсистем АСУ СН в прототип объекта исследования обозначено пунктиром.

Оценивание эффективности использования АСУ СН в условиях информационного конфликта осуществлялось по показателю $E(P_{ИП}^{треб})$:

$$E\left(P_{ИП}^{треб}\right)=\frac{\bar{Q}\left(P_{ИП}^{треб}\right)-\bar{Q}^{сов}\left(P_{ИП}^{треб}\right)}{\bar{Q}\left(P_{ИП}^{треб}\right)}\times 100\%,$$

где $\bar{Q}\left(P_{ИП}^{треб}\right)$ – отношение количества обнаруженных стороной 1 и стороной 2 УТ Q_1/Q_2 при выполнении критерия обеспечения информационного превосход-

ства в информационном конфликте АСУ СН без внедрения научно-технических предложений по реализации технологии динамической координации подсистем АСУ СН стороны 1; $\bar{Q}^{\text{сов}}\left(P_{\text{ИП}}{}^{\text{треб}}\right)$ – отношение количества обнаруженных стороной 1 и стороной 2 УТ Q_1/Q_2 при выполнении критерия обеспечения информационного превосходства в информационном конфликте АСУ СН после внедрения научно-технических предложений по реализации технологии динамической координации подсистем АСУ СН стороны 1.

Итоговые значения уровня повышения эффективности использования АСУ СН в условиях информационного конфликта представлены в таблице 2.

Таблица 2 – Результаты оценки повышения показателя эффективности

$P_{\text{ИП}}{}^{\text{треб}}$	0,5	0,6	0,7	0,8	0,9
$E(P_{\text{ИП}}{}^{\text{треб}})$	29%	37,5%	39%	34,8%	25%

Результаты проведенной оценки показали, что использование в прототипе АСУ СН научно-технических предложений по реализации технологии динамической координации подсистем АСУ СН в условиях информационного конфликта, позволяют повысить эффективность использования АСУ СН в условиях информационного конфликта по показателю эффективности динамической координации подсистем АСУ СН $E(P_{\text{ИП}}{}^{\text{треб}})$ в диапазоне 25…39% и обеспечить выполнение критериальных требований по обеспечению информационного превосходства в информационном конфликте АСУ СН для всех значений показателя вероятности информационного превосходства.

Выводы

По результатам проведенного исследования были сделаны следующие основные выводы.

1. Современные АСУ СН являются результатов конвергенции телекоммуникационных и информационных систем, при этом специальная сфера их деятельности подразумевает возникновение конфликтов различного рода, неотъемлемой частью которых является информационные конфликты АСУ СН на этапе сбора данных о состоянии, намерениях и действиях конфликтующей стороны в цикле управления основными (базовыми) силами и средствами.

2. Эффективность использования АСУ СН в условиях информационного конфликта определяется их способностью обеспечить информационное превосходство, т. е. способностью осуществлять непрерывный сбор сведений о конфликтующей стороне, их обработку, распределение потока достоверной информации в интересах применения основных (базовых) сил и средств, а также способностью обеспечить упреждение выполнения аналогичных действий конфликтующей стороной.

3. Учет вклада подсистем наблюдения и воздействия в процесс сбора данных о состоянии, намерениях и действиях конфликтующей стороны в интересах принятия решения о применении основных (базовых) сил и средств и затруднение (срыв) аналогичного процесса для конфликтующей стороны был

формализован и исследован в виде процесса двунаправленного динамического информационного конфликта АСУ СН.

4. Достижение информационного превосходства в информационном конфликте АСУ СН обеспечивается информационными контактами средств наблюдения и воздействия в составе соответствующих подсистем с УТ АСУ СН, которые, таким образом, выступают общим ресурсом подсистем наблюдения и воздействия, что актуализирует вопросы динамической координации этих подсистем посредством рационального динамического распределения средствам в их составе УТ АСУ СН для информационных контактов.

5. Разработанные модели, методы и комплекс методик динамической координации подсистем АСУ СН в условиях информационного конфликта, а также сформированные на их основе научно-технические предложения по реализации технологии динамической координации подсистем АСУ СН позволяют повысить эффективность использования АСУ СН в условиях информационного конфликта. Значение показателя эффективности, которое отражает синергетический эффект от динамической координации подсистем АСУ СН в условиях информационного конфликта, определяется снижением требуемого объема ресурсов (УТ АСУ СН) в процессе их перевода в целевой эффект от использования АСУ СН (выполнение критерия обеспечения информационного превосходства в информационном конфликте), в диапазоне 25…39% и обеспечить выполнение критериальных требований по обеспечению информационного превосходства в информационном конфликте АСУ СН для всех значений показателя вероятности информационного превосходства в диапазоне $[0{,}5; 0{,}9]$.

6. Результаты исследования подтвердили выдвинутую гипотезу исследования**,** которая состояла в том, что динамическая координация подсистем АСУ СН позволит повысить эффективность [30] использования в условиях информационного конфликта как подсистем наблюдения и воздействия, так и АСУ СН в целом, за счет получения синергетического эффекта, что обеспечит достижение информационного превосходства в информационном конфликте [31].

Литература

1. О связи. Федеральный закон РФ от 07.07.2003 № 126-ФЗ // Собрание законодательства Российской Федерации от 14 июля 2003 г. № 28 ст. 2895.

2. Антонович П. И., Макаренко С. И., Михайлов Р. Л., Ушанев К. В. Перспективные способы деструктивного воздействия на системы военного управления в едином информационном пространстве // Вестник Академии военных наук. 2014. № 3 (48). С. 93-101.

3. Михайлов Р. Л., Макаренко С. И. Оценка устойчивости сети связи в условиях воздействия на неё дестабилизирующих факторов // Радиотехнические и телекоммуникационные системы. 2013. № 4. С. 69-79.

4. Макаренко С. И., Рюмшин К. Ю., Михайлов Р. Л. Модель функционирования объекта сети связи в условиях ограниченной надежности каналов связи // Информационные системы и технологии. 2014. № 6 (86). С. 139-147.

5. Макаренко С. И., Михайлов Р. Л. Модель функционирования маршрутизатора в сети в условиях ограниченной надежности каналов связи // Инфокоммуникационные технологии. 2014. Том 12. № 2. С. 44-49.

6. Макаренко С. И., Михайлов Р. Л., Новиков Е. А. Исследование канальных и сетевых параметров канала связи в условиях динамически изменяющейся сигнально–помеховой обстановки // Журнал радиоэлектроники. 2014. № 10. – URL: http://jre.cplire.ru/jre/oct14/3/text.pdf (дата обращения 04.10.2021).

7. Макаренко С. И., Михайлов Р. Л. Информационные конфликты – анализ работ и методологии исследований // Системы управления, связи и безопасности. 2016. № 3. С. 95-178. DOI: 10.24411/2410-9916-2016-10304.

8. Михайлов Р. Л., Поляков С. Л. Состав и задачи перспективной автоматизированной системы управления средствами технической разведки и радиоэлектронной борьбы // I-methods. 2019. Том 11. № 2. С. 1-9.

9. Михайлов Р. Л. Помехозащищенность транспортных сетей связи специального назначения. Монография. – Череповец: ЧВВИУРЭ, 2016. – 128 с.

10. Михайлов Р. Л. Радиоэлектронная борьба в Вооруженных силах США. Монография. – СПб.: Наукоемкие технологии, 2018. – 131 с.

11. Михайлов Р. Л. Описательные модели систем спутниковой связи как космического эшелона телекоммуникационных систем специального назначения. Монография. – СПб.: Наукоемкие технологии, 2019. – 150 с.

12. Михайлов Р. Л. Анализ научно-методического аппарата теории координации и его использования в различных областях исследований // Системы управления, связи и безопасности. 2016. № 4. С. 1-29. – URL: http://sccs.intelgr.com/archive/2016-04/01-Mikhailov.pdf (дата обращения 04.10.2025).

13. Михайлов Р. Л. Анализ подходов к формализации показателя информационного превосходства на основе теории оценки и управления рисками // Системы управления, связи и безопасности. 2017. № 3. С. 98-118. – URL: http://sccs.intelgr.com/archive/2017-03/05-Mikhailov.pdf (дата обращения 04.10.2025).

14. Гнатуша А. А., Ефремов А. В. Михайлов Р. Л. К вопросу об актуальности определения показателя информационного превосходства // Межвузовская научно-практическая конференция «Проблемы технического обеспечения войск в современных условиях». (Санкт-Петербург, 17 февраля 2017 г.) – СПб.: ВАС, 2017. – С. 295-300.

15. Михайлов Р. Л. Динамическая модель информационного конфликта информационно-телекоммуникационных систем специального назначения // Системы управления, связи и безопасности. 2020. № 3. С. 238-251. DOI: 10.24411/2410-9916-2020-10309.

16. Михайлов Р. Л. Модель информационных контактов устройств телекоммуникаций информационно-телекоммуникационной системы специального назначения со средствами наблюдения и воздействия противостоящей стороны // Труды учебных заведений связи. 2020. Т. 6. № 3. С. 17-27.

17. Михайлов Р. Л. Новый базовый подход и методика оценивания информационного превосходства в информационном конфликте // Инфокоммуникационные технологии. 2021. Том 19. № 1. С. 7-20. DOI: 10.18469/ikt.2021.19.1.01.

18. Михайлов Р. Л. Базовая модель координации подсистем наблюдения и воздействия информационно-телекоммуникационной системы специального назначения в информационном конфликте // Системы управления, связи и безопасности. 2019. № 4. С. 437-450. DOI: 10.24411/2410-9916-2019-10418.

19. Михайлов Р. Л. Двухуровневая модель координации подсистем радиомониторинга и радиоэлектронной борьбы // Наукоемкие технологии в космических исследованиях Земли. 2018. Т. 10. № 2. С. 43-50. DOI: 10.24411/2409-5419-2018-10040.

20. Михайлов Р. Л., Шишков А. И. Принципы координации подсистем наблюдения и воздействия // Научная мысль. 2017. № 3 (25). Том. 1. С. 38-44.

21. Михайлов Р. Л., Поляков С. Л. Игровая модель координации подсистем наблюдения и воздействия // Межвузовская научно-практическая конференция «Проблемы технического обеспечения войск в современных условиях». (Санкт-Петербург, 17 февраля 2019 г.) – СПб.: ВАС, 2019. – С. 303-307.

22. Михайлов Р. Л. Модель динамической координации подсистем наблюдения и воздействия в информационном конфликте в виде иерархической дифференциальной игры трех лиц // Наукоемкие технологии. 2018. Т. 19. № 10. С. 44-51. DOI: 10.18127/j19998465-201810-08.

23. Михайлов Р. Л., Привалов А. А., Поляков С. Л. Модель телекоммуникационной сети при координации подсистем в составе инфокоммуникационной системы специального назначения // Информация и космос. 2021. № 1. С. 18-26.

24. Михайлов Р. Л. Задача распределения ресурса в информационном конфликте: формализация и пути решения // Наукоемкие технологии в космических исследованиях Земли. 2020. Т. 12. № 3. С. 77-83.

25. Михайлов Р. Л., Ларичев А. В., Смыслова А. Л., Леонов П. Г. Модель распределения ресурсов в информационном конфликте организационно-технических систем // Вестник Череповецкого государственного университета. 2016. № 6. С. 24-29.

26. Михайлов Р. Л., Поляков С. Л. Модель оптимального распределения ресурсов и исследование стратегий действий сторон в ходе информационного конфликта // Системы управления, связи и безопасности. 2018. № 4. С. 323-344. – URL: http://sccs.intelgr.com/archive/2018-04/17-Mikhailov.pdf (дата обращения 04.10.2025).

27. Михайлов Р. Л., Вещагин А. В., Ганиев А. Н., Кузнецов Н. П. Динамическая координация подсистем информационно-телекоммуникационной системы специального назначения в условиях информационного конфликта: метод развязывания взаимодействий // Системы управления, связи и безопасности. 2023. № 1. С. 244-275. DOI: 10.24412/2410-9916-2023-1-244-275.

28. Михайлов Р. Л., Николаев А. Е., Кузнецов Н. П. Динамическая координация подсистем информационно-телекоммуникационной системы специального назначения в условиях информационного конфликта: метод оценки взаимодействий // Системы управления, связи и безопасности. 2023. № 2. С. 228-257. DOI: 10.24412/2410-9916-2023-2-228-257.

29. Михайлов Р. Л., Данилов Д. Ю., Потапов А. А., Гречко П. В. Динамическая координация подсистем наблюдения и воздействия: метод прогнозирования взаимодействий // Системы управления, связи и безопасности. 2024. № 3. С. 49-77. DOI: 10.24412/2410-9916-2024-3-049-077.

30. Сазонов К. В., Михайлов Р. Л., Ратушин А. П. Методика управления эффективностью технических систем // Труды учебных заведений связи. 2024. Т. 10. № 2. С. 83-91.

31. Михайлов Р. Л., Ганиев А. Н., Ефремов А. В. Модели и методы динамической координации подсистем информационно-телекоммуникационной системы специального назначения в условиях информационного конфликта // Системы управления, связи и безопасности. 2021. № 5. С. 136-179. DOI: 10.24412/2410-9916-2021-5-136-179.

Информация об авторе

Михайлов Роман Леонидович – доктор технических наук, доцент. Научно-педагогический работник. Военный университет радиоэлектроники. Область научных интересов: информационные конфликты, координация подсистем наблюдения и воздействия, управление мониторингом. E-mail: cvviur6@mil.ru

Адрес: 162622, Вологодская обл., г. Череповец, Советский пр., д. 126.

УДК 621.396

Подход к восстановлению геоинформационных параметров сцены траекторного сигнала радиолокационной станции космического базирования

Мальгин И. Ю

В тезисе представлен подход к восстановлению геоинформационных параметров сцены траекторного сигнала радиолокационной станции космического базирования, предполагающий определение области в пространстве, в пределах которой при заданных частотно-временных параметрах не возникает явлений (помех) неоднозначности.

Ключевые слова: *радиолокационные станции космического базирования, положение сцены, частотно-временные параметры зондирующего сигнала, строб приема, кластеризация.*

Актуальность

Большинство радиолокационных станций космического базирования (РЛС КБ) с синтезированной апертурой формируют изображение поверхности Земли на основе когерентной обработки последовательности отражённых сигналов, регистрируемых при движении носителя вдоль траектории съёмки. При этом выбор частотно-временных параметров зондирующего сигнала и геометрии наблюдения осуществляется таким образом, чтобы формируемый режим съёмки (совокупность параметров съемки) обеспечивал требуемое пространственное разрешение на всей полосе съёмки при одновременном отсутствии неоднозначностей по дальности и азимуту.

Высокая степень взаимосвязи между параметрами зондирующего сигнала, орбитальной геометрией и возможным (допустимым) положением сцены делает задачу формирования режимов съёмки многопараметрической и трудоёмкой. Эффективным способом проверки корректности алгоритмов подбора параметров съёмки является решение обратной задачи: определение области в пространстве, в пределах которой при заданных частотно-временных параметрах не возникает явлений (помех) неоднозначности, и сопоставление ее с положением требуемого района съемки.

Опубликованные исследования по вопросу синтезирования апертуры РЛС КБ в целом формируют стройную картину принципов сигналообразования [1, 2] и формирования радиолокационных изображений [3, 4], а также содержат подробные наборы инженерных правил для выбора частотно-временных параметров и геометрии съёмки [5, 6]. Вместе с тем в указанных работах неоднозначности по дальности и азимуту, как правило, рассматриваются в прямой постановке – в виде ограничений и рекомендаций по выбору частоты повторения

Статья (тезис) опубликована в сборнике докладов конференции:
I семинар научной школы профессора С. И. Макаренко. Сборник тезисов докладов конференции. г. Санкт-Петербург, 20-21 декабря 2025 года. – СПб.: Наукоемкие технологии, 2026.

импульсов, строба приёма или геометрии, тогда как задача обратного восстановления области допустимого положения сцены по заданным частотно-временным параметрам специально не выделяется. Классические монографии [1, 7] и обзоры подробно излагают математическую модель траекторного сигнала, переход в систему координат «дальность – азимут», компрессию (сжатие) по дальности и азимуту, а также влияние орбитальных и антенных параметров на допустимую полосу доплеровских частот и разрешающую способность, но не раскрывают вопросы восстановления положения сцены по параметрам траекторного сигнала и не содержат в явном виде формализации данной задачи (построения области без неоднозначностей). Современные обзоры космических радиолокационных систем с синтезированной апертурой [8-12] описывают развитие технологий и режимов и показывают, как на практике достигается баланс между полосой обзора, разрешением и уровнем неоднозначностей при ограниченной пропускной способности, но не ориентированы на верификацию корректности выбора параметров съемки.

Постановка задачи

Несмотря на значительное количество работ, посвящённых принципам формирования и обработки сигналов РЛС КБ, вопросы проверки корректности подбора параметров съёмки посредством решения обратной задачи остаются недостаточно изученными. Это определяет актуальность **научной задачи**: разработки пространственно-временной модели, позволяющей исследовать условия исключения неоднозначности при функционировании РЛС КБ и метода, позволяющего выявить зависимость положения сцены от траекторных характеристик и параметров зондирующего сигнала, путем статистического анализа допустимых диапазонов углов наблюдения и дальностей, при которых обеспечивается съёмка без возникновения паразитных отражений и спектральных перекрытий.

В рамках решения приведенной научной задачи планируется получить следующие научные результаты:

1) модель обработки параметров траекторного сигнала РЛС КБ, взаимоувязывающая множество возможных положений сцены и орбитальные (траекторные) характеристики и параметры зондирующего сигнала;
2) метод восстановления геоинформационных характеристик сцены по параметрам траекторного сигнала РЛС КБ, основанный на выявлении (оценивании) и использовании для определения положения сцены для каждого отдельного режима РЛС КБ зависимости наклонной дальности от некоторого параметра (аргумента) или их совокупности.

Модель обработки параметров траекторного сигнала РЛС КБ

Одной из особенностей, возникающих при функционировании РЛС КБ и обусловленных большой наклонной дальностью, является прием излученного радиолокационного импульса после передачи еще d импульсов, следующих с периодом повторения $T_{Иi}$ (рис. 1). При этом строб (окно приема) имеет продолжительность t_{in}, которая определяется разницей времени распространения

сигнала до ближайшей и до дальней точки сцены t_{img}, а также временной поправкой, вводимой для компенсации миграции по дальности сцены в процессе движения платформы $t_{\Delta R}$. Кроме того, учитывается время, необходимое для передачи стробов управления и перенастройки бортового оборудования с режима работы «передача» в режим «прием» $t_{\text{старт}}^{\text{тех}}$ и обратно $t_{\text{стоп}}^{\text{тех}}$.

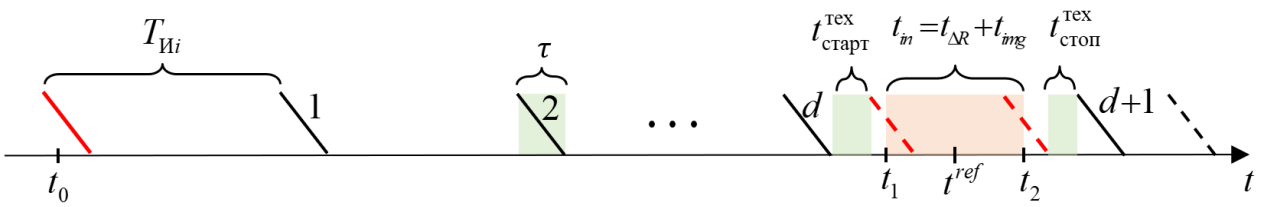

Рис. 1. Схема формирования строба приема в РЛС КБ

Учет данных особенностей позволит использовать в разрабатываемой модели в качестве координатно-информативного параметра начало $t_{di}^{\min}$ и конец строба приема $t_{di}^{\max}$:

$$t_{di}^{\min} = t_1 - t_0 = d \cdot T_{Ии} + \tau + t_{\text{старт}}^{\text{тех}},$$

$$t_{di}^{\max} = t_2 - t_0 = (d+1) \cdot T_{Ии} - \tau - t_{\text{стоп}}^{\text{тех}},$$

и на их основе получить соответствующие параметры положения – минимальное и максимальное расстояние до сцены.

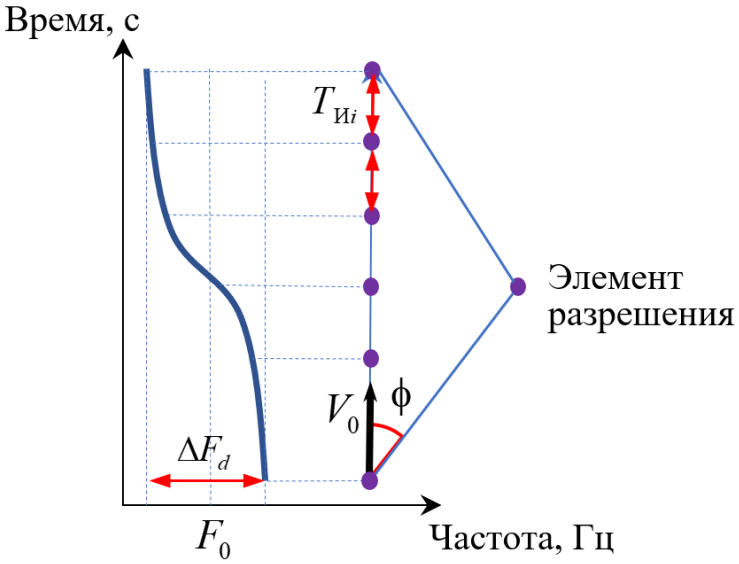

Рис. 2. Схема зависимости частотно-временных параметров и взаимного расположения РЛС КБ и элемента разрешения

Кроме того, планируется учесть особенность, заключающуюся в том, что при функционировании РЛС КБ, формируется последовательность откликов, соответствующих излученным импульсам и определенным дальностным ячейкам. Для определения отклика от каждого элемента разрешения (рис. 2) осуществляется цифровая обработка исходной последовательности – согласован-

ная фильтрация (свертка) по азимуту с опорным эталоном, описывающим предполагаемое доплеровское смещение частоты принимаемого отраженного сигнала. В связи с тем, что фазовая история (функция доплеровского смещения частоты) дискретизируется с частотой, соответствующей периоду повторения импульсов $T_{Иi}$, диапазон частот ΔF_d, который может быть однозначно интерпретирован в угол ϕ, определяющий положение элемента разрешения относительно положения платформы и ее вектора скорости, ограничен в соответствии с теоремой Котельникова $\Delta F_d < 2/T_{Иi}$.

Учет приведенной особенности позволит формализовать новый координатно-информативный параметр – допустимое доплеровское смещение частоты, и соответствующие ему параметр положения – предельные углы наблюдения сцены.

Метод восстановления геоинформационных характеристик сцены по параметрам траекторного сигнала РЛС КБ

Метод основан на выявлении (оценивании) и использовании для определения положения сцены для каждого отдельного режима РЛС КБ зависимости наклонной дальности от некоторого параметра (аргумента) или их совокупности. Для выявления указанной зависимости планируется включить в него следующие ранее не используемые операции: формирование множества возможных положений опорных точек сцены, их кластерный анализ и фильтрацию по количеству элементов в кластере, поиск и аппроксимацию зависимости наклонной дальности от аргумента, а также оценку его пригодности.

Кроме того, планируется разработать и включить в метод алгоритм, предполагающий представление поверхностей положения в виде множества окружностей в пространстве, что позволит учесть неравномерность поверхности Земли относительно эллипсоида (другими словами, учесть высоту над уровнем моря).

Прикладным результатом исследования будут являться научно-обоснованные технические рекомендации по определению области в пространстве, в пределах которой при заданных частотно-временных параметрах не возникает явлений (помех) неоднозначности. Сопоставление ее с положением требуемого района съемки позволит оценить корректность выбора частотно-временных параметров.

Литература

1. Curlander J. C., McDonough R. N. Synthetic Aperture Radar: Systems and Signal Processing. – New York: Wiley, 1991. – 647 p.

2. Cumming I. G., Wong F. H. Digital Processing of Synthetic Aperture Radar Data: Algorithms and Implementation. – Boston, MA: Artech House, 2005. – 636 p.

3. Franceschetti G., Lanari R. Synthetic Aperture Radar Processing. – Boca Raton: CRC Press, 1999. – 322 p.

4. Верба В. С., Неронский Л. Б., Осипов И. Г., Турук В. Э. Радиолокационные системы землеобзора космического базирования / под общ. ред. В. С. Вербы. – М.: Радиотехника, 2010. – 680 с.

5. Груздов В. В., Колковский Ю. В., Криштопов А. В., Кудря А. И. Новые технологии дистанционного зондирования Земли из космоса. – М.: Техносфера, 2018. – 483 с.

6. Raney R. K. The Delay/Doppler Radar Altimeter // IEEE Transactions on Geoscience and Remote Sensing. – 1998. – Vol. 36. – № 5. – P. 1578–1588.

7. Skolnik M. I. Radar Handbook. – 3rd ed. – New York: McGraw-Hill, 2008. – 1329 p.

8. Moreira A., Prats-Iraola P., Younis M., Krieger G., Hajnsek I., Papathanassiou K. P. A Tutorial on Synthetic Aperture Radar // IEEE Geoscience and Remote Sensing Magazine. – 2013. – Vol. 1. – № 1. – P. 6–43.

9. Song R., Liu Z., Zhang J., Yang J., Guo J. The Latest Developments in Spaceborne High-Resolution SAR Imaging and Technologies // Sensors [Электронный ресурс]. – 2024. – Vol. 24, № 18. – Art. 5978. – DOI: 10.3390/s24185978. – URL: https://www.mdpi.com/1424-8220/24/18/5978 (дата обращения: 23.10.2025).

10. Mapelli A., Lombardo P., Monti Guarnieri A., Gini F. Generalization of the Synthetic Aperture Radar Azimuth Multi-Aperture Processing Scheme // Remote Sensing [Электронный ресурс]. – 2024. – Vol. 16, № 17. – Art. 3170. – DOI: 10.3390/rs16173170. – URL: https://www.mdpi.com/2072-4292/16/17/3170 (дата обращения: 23.10.2025).

11. NASA Jet Propulsion Laboratory; ISRO. NISAR Mission Overview and Science Objectives [Электронный ресурс]. 2024. – URL: https://nisar.jpl.nasa.gov/mission/ overview/ (дата обращения: 23.10.2025).

12. European Space Agency. ROSE-L Mission Overview and Instrument Specification [Электронный ресурс]. 2023. – URL: https://www.esa.int/Applications/ Observing_the_Earth/Copernicus/ROSE-L (дата обращения: 23.10.2025).

Информация об авторе

Мальгин Игорь Юрьевич – соискатель ученой степени кандидата технических наук. Научный сотрудник. Военный университет радиоэлектроники. Область научных интересов: моделирование радиотехнических систем; прием и обработка сигналов. E-mail: igornemal@mail.ru

Адрес: 162622, Россия, Вологодская обл., г. Череповец, Советский проспект, д. 126.

УДК 004.75

Подход к автоматизированному управлению разноуровневой группировкой радиомониторинга

Павонский А. А.

В работе представлен подход к автоматизированному управлению разноуровневой группировкой радиомониторинга, предлагается оптимизировать распределение ограниченного ресурса сил и средств радиомониторинга в условиях динамически изменяющейся радиоэлектронной обстановки.

Ключевые слова: *автоматизированные системы управления, разноуровневая группировка, радиомониторинг.*

Вооруженные конфликты конца XX – начала XXI века доказывают, что результативное управление невозможно без использования информационных технологий в частности средств автоматизации. Современные автоматизированные системы управления радиомониторинга (АСУ РМ) стали ключевым элементом, определяющим эффективность армий XXI века [1, 2]. В современных условиях высокий уровень информационного обеспечения боевых действий группировок войск (сил) становится определяющим фактором достижения стратегического и оперативно-тактического превосходства над противником.

К основным критериям эффективности автоматизации процессов управления относятся: время, требуемое для выполнения тех или иных задач; объем затрачиваемых материальных и человеческих ресурсов; качество обрабатываемых данных, в том числе их актуальность, достоверность, полнота и доступность. Современные АСУ РМ должны обеспечивать сквозное управление силами и средствами от тактического до стратегического звена [1]. При этом управление силами и средствами должно быть устойчивым, непрерывным, оперативным и скрытным, а рациональное применение возможностей сил и средств влияет на успешное выполнение поставленных задач в различных условиях обстановки. Необходимо отметить, что на развитие и совершенствование системы управления войсками (силами) оказывает влияние требование обеспечения единства автоматизированного управления.

Так, в ходе вооруженного конфликта на разноуровневую группировку РМ возлагаются задачи по предоставлению достоверной, актуальной и полной информации о вероятном характере действий противника с целью информационного обеспечения войск (сил) [3]. Под разноуровневой группировкой РМ следует понимать соответствующие силы и средства тактического, оперативного и стратегического звеньев управления.

Статья (тезис) опубликована в сборнике докладов конференции:
I семинар научной школы профессора С. И. Макаренко. Сборник тезисов докладов конференции. г. Санкт-Петербург, 20-21 декабря 2025 года. – СПб.: Наукоемкие технологии, 2026.

Задействование противостоящей стороной различных телекоммуникационных систем привело экспоненциальному увеличению количества источников наблюдения, характеризующих деятельность объектов противника и возрастающим объемам разнородных данных. Соответствующие условия накладывают на подразделения РМ ряд трудностей, в первую очередь связанных с поиском источников, их селекцией по степени важности, информационной ценности и, соответственно, постановку на наблюдение. В связи с этим имеет место ресурсный конфликт – ситуация, когда доступных ресурсов сил и средств РМ недостаточно для выполнения всего спектра задач.

Кроме того, в условиях динамического изменения обстановки возникает необходимость оптимального распределения источников наблюдения между силами и средствами разноуровневой группировки РМ без потери полноты получаемой информации. В ряде известных работ [7, 8] рассматриваются вопросы оптимального распределения сил и средств РМ по объектам наблюдения, однаковопросы учета важности и информативности именно элементов телекоммуникационных сетей, функционирующих в интересах объектов наблюдения, не рассматриваются.

Анализ [4-8] существующих АСУ и реализованных в них технических решений по данной проблематике, показывает, что подсистемы АСУ функционально ограниченны и тем самым, не позволяют осуществлять указанное распределение сил и средств в автоматизированном режиме.

Вышеуказанные факторы позволили сформулировать проблемную ситуацию – между необходимостью повышения эффективности автоматизированного управления разноуровневой группировки радиомонтиторинга и невозможностью разработки соответствующего научно-обоснованного решения, на основе современного уровня развития научно-методического аппарата в составе теории оптимального распределения ресурсов.

Для разрешения данной проблемной ситуации может быть сформулирована актуальная цель исследования – повышение эффективности автоматизированного управления разноуровневой группировки РМ.

Для решения общей научной задачи в интересах достижения поставленной цели, она была декомпозирована на частные научные и прикладную задачи:

1) разработка модели подсистемы ситуационного управления разноуровневой группировкой РМ;
2) разработка метода распределения источников наблюдения между силами и средствами разноуровневой группировки РМ;
3) разработка методики ведения мониторинга обстановки разноуровневой группировкой РМ.

Решением этих задач будут научные и прикладной результаты, значимые для развития теории оптимального распределения ресурсов и обладающие практическим эффектом в части повышения эффективности автоматизированного управления разноуровневой группировкой РМ.

Литература

1. Юсупов И. Ж., Попов А. В., Пятов С. В. Время автоматизированного управления. Автоматизация деятельности должностных лиц автобронетанковой службы // Материально-техническое обеспечение Вооруженных Сил Российской Федерации. 2024. № 12. С. 13-25.

2. Выпасняк В. И., Гуральник А. М., Тиханычев О.В. Система поддержки принятия решений как «виртуальный штаб» // Военная мысль. 2015. № 2. С. 23-29.

3. Баранов А. Р. Разведывательная подготовка подразделений специального назначения: учебно-практическое пособие. – М.: Академический проект, 2020. – 467 с.

4. Никифоров А. В. Теоретические основы автоматизации управления в иерархических АСУ войсками // Sciences of europe. 2016. № 9 (9). С. 32-44. – URL: https://cyberleninka.ru/article/n/teoreticheskie-osnovy-avtomatizatsii-upravleniya-v-ierarhicheskih-asu-voyskami (дата обращения 20.02.2026)

5. Мосиенко Ю. И., Кругликов С. В. Адаптивные информационно-управляющие системы: сложившаяся необходимость и методология реализации // Информационно-измерительные и управляющие системы. 2016. № 4. Т. 14. С. 8-14.

6. Протасов А.А., Козичев В. Н., Каргин. В. Н. Автоматизированные системы управления войсками: определение и классификаци // Военная мысль. 2024. № 2. С. 60-70.

7. Островский Е. О., Сизов А.С. Концептуальные подходы к созданию автоматизированной системы прогнозирования состояния и деятельности объектов оперативной разведки // Военная мысль. 2013. № 6. С. 38-47.

8. Сумилов Е. А. Обоснование рационального способа распределения сил и средств разведки по направлениям деятельности войск // Военная мысль. 2017. № 9. С. 61-64.

Информация об авторе

Павонский Андрей Андреевич – соискатель ученой степени кандидата технических наук. Военный университет радиоэлектроники. Область научных интересов: мониторинг информационных ресурсов; сбор и обработка информации. E-mail: andreypavonskiy@yandex.ru

Адрес: 162622, Россия, г. Череповец, Советский проспект, д. 126.

УДК 355.469

Подходы к формированию маршрутов полетов БпЛА на основе алгоритмов поиска кратчайших путей

Цулун Д. В.

В статье проведен анализ алгоритмов поиска кратчайших путей и возможности их использования при формировании маршрутов беспилотных летательных аппаратов, что позволит повысить эффективность использования их целевой нагрузки при выполнении различного класса задач.

Ключевые слова: *беспилотный летательный аппарат, маршрутизация, мониторинг.*

Актуальность

В настоящее время беспилотные летательные аппараты (БпЛА) предназначены для решения широкого спектра задач [1-3]. По способу управления БпЛА разделяются на [1] дистанционно пилотируемые, автономные и аппараты с комбинированной системой управления.

Следует отметить, что в процессе организации управления БпЛА при реализации любого из приведенных выше способов, важную роль играет заблаговременное формирование маршрутов его полета, которое должно осуществляться с учетом различных факторов. К негативным факторам, влияющим на живучесть БпЛА, относятся противодействие со стороны систем противовоздушной обороны (ПВО) и радиоэлектронного подавления (РЭП) противоборствующей стороны, неблагоприятные погодные условия, опасные участки местности (линии электропередач, высотные здания) и т. п. Кроме того, важно учесть вероятность выполнения полезной нагрузкой БпЛА своей целевой функции (сбор информации, поражение противника, доставка груза и т. д.) с требуемой эффективностью, что сопряжено с необходимостью включения в маршрут полета БпЛА тех точек (участков местности), где собственно эта нагрузка и будет применяться.

Особенности реального управления и применения БпЛА, в том числе и в условиях боевых действий, а также противодействия ПВО и РЭП подробно рассмотрены в работах С. И. Макаренко [4, 5], М. К. Казамбаева, Б. Ж. Куатова [6], Б. И. Казарьяна [7], В. В. Ростопчина [8].

Разработке подходов к маршрутному управлению БпЛА с обходом опасных зон и препятствий посвящены работы И. А. Батраевой и Д. П. Тетерина [9], Н. П. Зубова [10], А. Н. Козуба и Д. П. Кучерова [11], Г. Н. Лебедева и А. В. Румакина [12], А. Н. Попова [13], К. С. Яковлева и соавторов [14], а также А. С. Васильченко и соавторов [15-16].

Статья (тезис) опубликована в сборнике докладов конференции:
I семинар научной школы профессора С. И. Макаренко. Сборник тезисов докладов конференции. г. Санкт-Петербург, 20-21 декабря 2025 года. – СПб.: Наукоемкие технологии, 2026.

В качестве общего недостатка указанных работ можно отметить отсутствие оценки при формировании маршрутов БпЛА полноты выполнения им поставленной задачи с требуемой эффективностью, что является критически важным в процессе реального применения БпЛА.

Разработка алгоритмов внесения корректировок в маршрут полета БпЛА с учетом изменения обстановки позволит перейти от формирования маршрута полета БпЛА к полноценной его маршрутизации. При этом в качестве перспективного направления исследований авторы рассматривают возможность использования при формировании маршрутов полета БпЛА алгоритмов поиска кратчайших путей, лежащих в основе протоколов маршрутизации информационных потоков в телекоммуникационных сетях (ТКС).

К протоколам маршрутизации в ТКС относят протоколы обмена служебной информацией, обеспечивающие построение сетевыми устройствами таблиц маршрутизации, которые в дальнейшем используются для поиска кратчайших путей передачи трафика между узлами сети.

В настоящее время в ТКС наиболее широко используются протоколы динамической маршрутизации [17], которые функционально разделяются на протоколы «внутреннего шлюза» (IGP, аббр. от англ. Interior Getaway Protocol) и «наружного» (EGP, аббр. от англ. Exterior Getaway Protocols).

При этом в качестве алгоритмов поиска кратчайших путей в большинстве протоколов используются:

– алгоритм Дейкстры [18];

– алгоритм Беллмана – Форда.

Ключевым отличием алгоритма Беллмана – Форда от алгоритма Дейкстры является возможность поиска кратчайших путей с циклами с отрицательным весом [19], что в практике определения маршрута полета БпЛА не имеет физического смысла. Таким образом, в качестве основы для маршрутизации БпЛА предлагается взять алгоритм поиска кратчайших путей Дейкстры.

Постановка задачи

Для формализации задачи маршрутизации БпЛА в первую очередь приведем топологическую модель зоны его полетов с учетом реальных условий применения целевой нагрузки по объектам (рис. 1).

Формализуем представленную топологическую модель зоны полетов БпЛА в виде графа (рис. 2), который будет включать в себя:

1) вершины графа:
   - совокупность районов местности, где возможно использование целевой нагрузки БпЛА для сбора информации о находящихся в этом районе объекте (объектах);
   - точка запуска и возможные точки посадки БпЛА;
2) ребра графа, представляющие собой возможные пути полета между вершинами графа.

Для формальной постановки и решения задачи в работе введены обозначения, представленные в таблице 1.

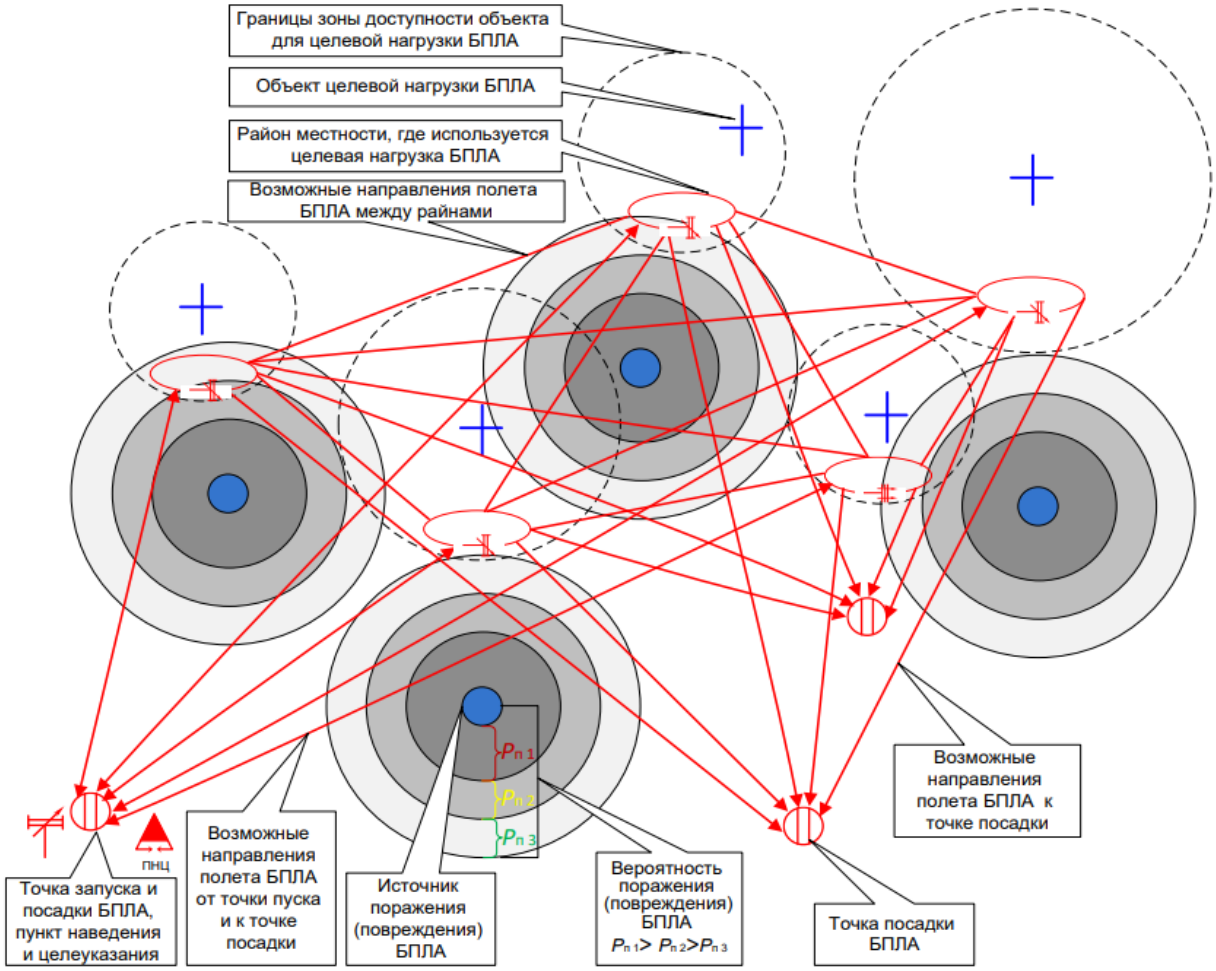

Рис. 1. Топологическая модель зоны полетов БпЛА

Таблица 1 – Обозначения

Обозначение	Физический смысл обозначения
$G(U, V)$	– ориентированный граф топологической модели зоны полетов БпЛА
$U=\{U_i\}$, $i = 1,\ldots, n$	– множество вершин графа G
U_1	– точка запуска БпЛА
U_{it}	– вершина графа U_i с указанием ее порядкового номера t в кратчайшем маршруте
M_i	– исходный вес вершины с позиции использования целевой нагрузкой БпЛА в i-м районе местности
$\{M_i\}$, $i = 1,\ldots, n$	– множество исходных весов вершин
M_{it}	– вес вершины U_{it} с позиции использования целевой нагрузкой БпЛА в i-м районе местности, заметим, что для графа, представленного на рис. 2, $M_{1t} = M_{2t} = M_{3t} = 0$, а также $M_{iT} = 0$
$\{M_{it}\}$, $i = 1,\ldots, n$, $t = 1,\ldots, T$	– множество весов вершин
t	– порядковый номер вершины в кратчайшем пути, $t = 1,\ldots, T$, $T \le n$
n	– общее количество вершин в графе $G(U, V)$
V_{ij}	– вес ребра, соединяющего i-ю и j-ю вершины

Обозначение	Физический смысл обозначения
V_{ijt}	– вес ребра, соединяющего i-ю вершину, имеющую (t-1) порядковый номер в кратчайшем маршруте, и j-ю вершину, имеющую t порядковый номер в кратчайшем маршруте
$i = 1,\ldots, n$, $j = 1,\ldots, n$	– переменные, счетчики вершин
$D = \{U_{it}\}$, $i = 1, \ldots, n$, $t = 1,\ldots, n$	– кортеж вершин кратчайшего маршрута
L	– вес кратчайшего маршрута, $L = \sum V_{ijt}$.
M	– сумма весов вершин, входящих в кратчайший маршрут, $M = \sum M_{ijt}$
$M_{тр}$	– требуемое значение результативности использования целевой нагрузки БпЛА

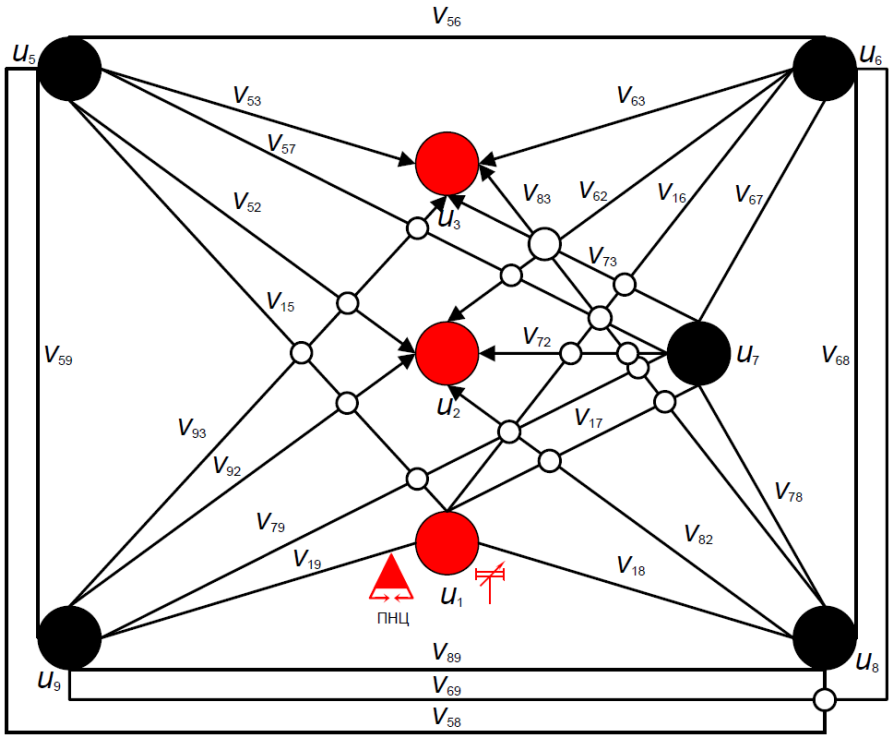

Рис. 2. Граф, формализующий топологическую модель зоны полетов БпЛА

Алгоритм маршрутизации БпЛА

Алгоритм маршрутизации БпЛА на основе алгоритма Дейкстры представлен на рис. 3.

В соответствии с подходами автора к маршрутизации БпЛА во главу угла может быть положена максимизация одной из функции результативности применения его целевой нагрузки.

1) Оперативность сбора информации – в этом случае вес кратчайшего маршрута определяется общим расстоянием, пройденным БпЛА при условии выполнения требований $M \geq M_{тр}$, но без учета необходимости обеспечения живучести БпЛА. Тогда значение веса ребра (V_{ij}), соединяющего i-ю и j-ю верши-

ны, определяется расстоянием между вершинами i и j, а суммарный вес кратчайшего маршрута (L) – суммой этих расстояний.

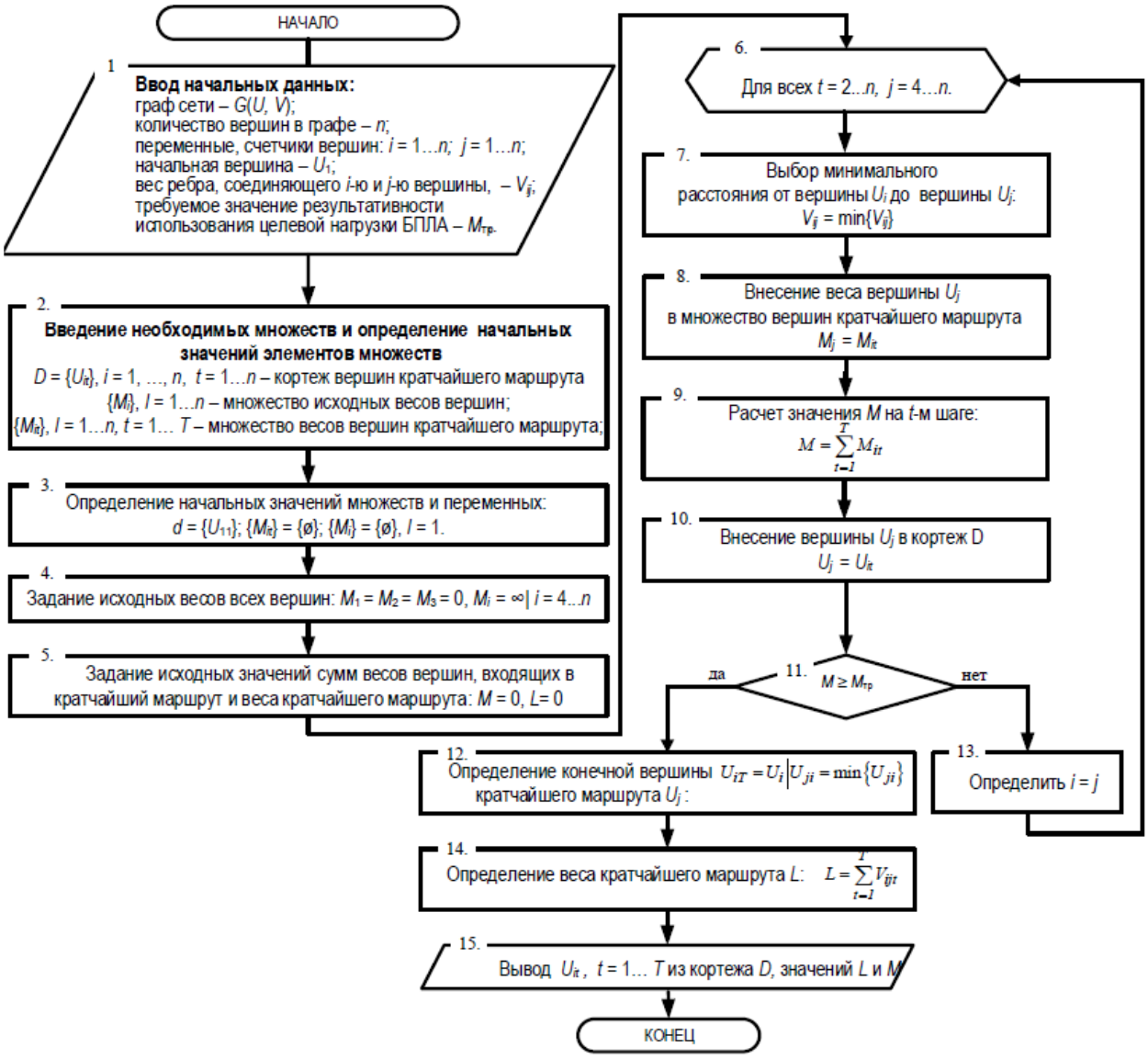

Рис. 3. Алгоритм маршрутизации БпЛА

2) Полнота сбора информации – в этом случае маршрут полета БпЛА также должен отвечать требованиям $M \geq M_{тр}$, однако значение общего расстояния, которое он должен преодолеть, не учитывается, а вес кратчайшего маршрута определяется минимальной вероятностью его поражения (повреждения). В этом случае значение веса ребра (V_{ij}), соединяющего i-ю и j-ю вершины, определяется вероятностью поражения (повреждения) БпЛА при полете между вершинами i и j, а – суммарный вес кратчайшего маршрута (L) – общей вероятностью поражения (повреждения) БпЛА от точки запуска до точки посадки.

3) Полнота охвата объектов целевой нагрузки БпЛА – в этом случае маршрут полета БпЛА должен проходить через все вершины графа, формализующие районы сбора информации об интересующих объектах ($U_{it} \in D$) при всех $i = 1, \ldots, n$ с учетом необходимости обеспечения минимизации как прой-

денного расстояния, так и вероятности его поражения (повреждения). Тогда значение веса ребра (V_{ij}), соединяющего *i*-ю и *j*-ю вершины, определяется произведением расстояния между вершинами *i* и *j* и вероятностью поражения (повреждения) БпЛА при полете между этими вершинами, а – суммарный вес кратчайшего маршрута (L) – общей суммой значений этих произведений для всех ребер, входящих в маршрут полета. При этом задача поиска кратчайшего маршрута сводится к известной задаче о коммивояжере [18].

Ранее соискателем было проведено исследование особенностей использования алгоритмов поиска кратчайших путей при формировании маршрута полета БпЛА [20]. В рамках направления дальнейших исследований планируется осуществить модификацию представленного алгоритма в направлении поиска резервных маршрутов из всех точек на ребрах графа.

Выводы

В работе проведен анализ алгоритмов поиска кратчайших путей в ТКС применительно к их использованию при формировании маршрута полета БпЛА и его корректировке при изменении исходных данных. Предложен алгоритм маршрутизации БпЛА, формализующий топологическую модель зоны полетов с учетом присущих им особенностей. Показаны направления дальнейших исследований в выбранной предметной области.

Литература

1. Макаренко С. И. Противодействие беспилотным летательным аппаратам. Монография. – СПб.: Наукоемкие технологии, 2020. – 204 с.

2. Аниськов Р. В., Архипова Е. В., Гордеев А. А., Пугачев А. Н. К вопросу борьбы с незаконным использованием беспилотных летательных аппаратов коммерческого типа // Вопросы обороной техники. Серия 16: Технические средства противодействия терроризму. 2017. № 9-10 (111-112). С. 71-75.

3. Еремин Г. В., Гаврилов А. Д., Назарчук И. И. Малоразмерные беспилотники – новая проблема для ПВО // Отвага [Электронный ресурс]. 29.01.2015. – URL: http://otvaga2004.ru/armia-i-vpk/armia-i-vpk-vzglyad/malorazmernye-bespilotniki/.html (дата обращения: 11.10.2025).

4. Макаренко С. И. Информационное противоборство и радиоэлектронная борьба в сетецентрических войнах начала XXI века. – СПб.: Наукоемкие технологии, 2017. – 546 с.

5. Макаренко С. И., Иванов М. С. Сетецентрическая война – принципы, технологии, примеры и перспективы. – СПб.: Наукоемкие технологии, 2018. – 898 с.

6. Казамбаев М. К., Куатов Б. Ж. Некоторые вопросы использования беспилотных летательных аппаратов // Надежность и качество сложных систем. 2017. № 4(20). С. 97-100. doi: 10.21685/2307-4205-2017-4-13.

7. Казарьян Б. И. Беспилотные аппараты. Способы применения в составе боевых систем // Военная мысль. 2012. № 3. С. 21-26.

8. Ростопчин В. В. Ударные беспилотные летательные аппараты и противовоздушная оборона – проблемы и перспективы противостояния // Беспилотная авиация. 2019. – URL: https://www.researchgate.net/publication/331772628_Udarnye_bespilotnye_letatelnye_apparaty_i_protivovozdusnaa_oborona_problemy_i_perspektivy_protivostoania (дата обращения: 20.09.2025).

9. Батраева И. А., Тетерин Д. П. Алгоритм планирования траектории движения беспилотного летательного аппарата при выполнении поисково-спасательных операций // Известия Самарского научного центра Российской академии наук. 2018. Т. 20. № 6. С. 210-214.

10. Зубов Н. П. Проблемные вопросы навигации и наведения роботизированных летательных аппаратов // Новости навигации. 2011. № 2. С. 29-33.

11. Козуб А. Н., Кучеров Д. П. Интеграционный подход к задаче выбора маршрута группы БпЛА // Системы и средства искусственного интеллекта. 2013. № 4. С. 333-343.

12. Лебедев Г. Н., Румакина А. В. Система логического управления обхода препятствий беспилотным летательным аппаратом при маршрутном полете // Труды МАИ. 2015. № 83. С. 5.

13. Попов А. Н., Тетерин Д. П. Методы планирования траектории движения беспилотного летательного аппарата с учетом противодействия противника // Известия Самарского научного центра Российской академии наук. 2017. Т. 19. № 1-2. С. 371-376.

14. Яковлев К. С., Баскин Е. С., Андрейчук А. А. Метод автоматического планирования совокупности траекторий для навигации беспилотных транспортных средств // Управление большими системами. 2015. № 58. С. 306-342.

15. Васильченко А. С., Иванов М. С., Колмыков Г. Н. Формирование маршрутов полета беспилотных летательных аппаратов с учетом местоположения средств противовоздушной обороны и радиоэлектронного подавления // Системы управления, связи и безопасности. 2019. № 4. С. 403-420.

16. Васильченко А. С., Иванов М. С., Малышев В. А. Формирование полетных зон беспилотных летательных аппаратов по степени устойчивости управления ими в условиях применения средств противовоздушной обороны и радиоэлектронного подавления // Системы управления, связи и безопасности. 2019. № 4. С. 262-279.

17. Олифер В. Г., Олифер Н. А. Компьютерные сети. Принципы, технологии, протоколы. – СПб.: Питер, 2010. – 945 с.

18. Свами М., Тхуласираман К. Графы, сети и алгоритмы. – М.: Мир, 1984. – 454 с.

19. Макаренко С. И., Квасов М. Н. Модифицированный алгоритм Беллмана–Форда с формированием кратчайших и резервных путей и его применение для повышения устойчивости телекоммуникационных систем // Инфокоммуникационные технологии. 2016. Т. 14. № 3. С. 264–274.

20. Михайлов Р. Л., Цулун Д. В. Применение алгоритмов поиска кратчайших путей при формировании маршрута полета беспилотного летательного аппарата // Информационные технологии и телекоммуникации. 2023. Том 11. № 1. С. 26-38. doi: 10.31854/2307-1303-2023-11-1-26-38.

Информация об авторе

Цулун Дмитрий Владимирович – научно-педагогический работник Военного университета радиоэлектроники. Область научных интересов: информационно-управляющие системы; маршрутизация БпЛА, мониторинг. E-mail: dmitrii_ts_80@mail.ru

Адрес: 162622, Россия, Вологодская обл., г. Череповец, Советский проспект, д. 126.

УДК 355:623

Исследование конфликта системы воздушно-космической обороны и средств воздушно-космического нападения

Афонин И. Е.

В статье кратко рассмотрены актуальность вопросов исследования устойчивости системы воздушно-космической обороны, сформулированы основные научные положения работы над диссертацией на соискание ученой степени доктора технических наук. Предложен комплекс мероприятий, направленных на повышение уровня устойчивости воздушно-космической обороны за счет адаптации к складывающейся оперативно-тактической обстановке. Приведена суть концептуальной модели динамического информационного конфликта «система ВКО – СВКН». А также представлен план разработки научных результатов в рамках диссертации, с указанием тех пунктов, которые уже выполнены автором и которые находятся в стадии дальнейшей разработки.

Ключевые слова: *конфликт, устойчивость, воздушно-космическая оборона, система управления, средства воздушно-космического нападения, огневое поражение, радиоэлектронное подавление, противовоздушная оборона.*

Актуальность вопросов исследования устойчивости системы воздушно-космической обороны (ВКО) в конфликте со средствами воздушно-космического нападения (СВКН) противника обусловлена все большим возрастанием военно-политической напряженности между Российской Федерацией и странами коллективного Запада. На случай перерастания напряженности в масштабный вооруженный конфликт в США разработана оперативно-стратегическая концепция «Быстрый глобальный удар» (БГУ), предполагающая одновременный удар большого количества средств поражения высокоточного оружия, прежде всего крылатыми ракетами морского (КРМБ) и воздушного базирования (КРВБ), по выбранным целям, административным и военным центрам, в том числе и по пусковым установкам межконтинентальных баллистических ракет (МБР). При этом в составе первого эшелона БГУ будут СВКН, ориентированные на поражение именно элементов системы ВКО с целью снижения ее эффективности при отражении удара СВКН последующих эшелонов БГУ. Последующие эшелоны БГУ составляют СВКН, предназначенные для поражения объектов системы государственного и военного управления, объектов критической инфраструктуры государства, в том числе и пусковых установок МБР, в условиях уже подавленной системы ВКО [1-9].

Таким образом, обеспечение устойчивости системы ВКО в целом, и ее системы управления (СУ), в частности, в условиях удара СВКН является важной военно-прикладной задачей, а разработка соответствующих моделей конфликта системы ВКО и СВКН – актуальным направлением исследований. Решение этой задачи осложняется высокими требованиями к готовности всех

Статья (тезис) опубликована в сборнике докладов конференции:
I семинар научной школы профессора С. И. Макаренко. Сборник тезисов докладов конференции. г. Санкт-Петербург, 20-21 декабря 2025 года. – СПб.: Наукоемкие технологии, 2026.

элементов системы ВКО, особенно в условиях функционирования их в неблагоприятной среде, а именно – в условиях физического поражения элементов системы ВКО ударными СВКН и функционального поражения средствами радиоэлектронного подавления (РЭП) противника [10].

Поскольку и система ВКО и СВКН – это множество взаимосвязанных технических средств и личного состава боевых расчетов различного уровня, обеспечивающего их функционирование и применение по назначению, можно ввести и в дальнейшем использовать в обоих случаях понятие *организационно-техническая система* (ОТС).

В связи с вышеизложенным имеет место **проблемная ситуация**, ***между*** развитием отдельных способов РЭП и применения противником различных видов воздействий на организационно-технические системы, входящие в состав многоэшелонированной системы ПВО страны, ***и*** недостаточным уровнем развития научно-методического аппарата оценивания динамики развития конфликтов организационно-технических систем (системы ВКО и СВКН) в рамках теории устойчивости динамических систем, применительно к многоэшелонированной системе ПВО. Таким образом, разработка моделей и методов оценивания динамических информационных конфликтов является актуальным направлением научных исследований.

Несмотря на большое количество работ, связанных с развитием эффективности различных аспектов ВКО, такое направление исследований, как обеспечение устойчивости системы ВКО в условиях массированного удара СВКН, не получило глубокого развития. В большинстве исследований совершенствование ВКО рассматривается через повышение частых показателей эффективности системы ПВО или повышение эффективности уже существующих образцов вооружения и военной техники: радиолокационных станций, автоматизированных систем управления (АСУ), комплексов средств автоматизации, зенитно-ракетных комплексов (ЗРК) и зенитно-ракетных систем (ЗРС) и других средств разведки и контроля воздушного пространства (РиКПВ).

В основу диссертационного исследования положено развитие научных направлений, сформулированных в работах Макаренко С. И., Михайлова Р. Л., Толстых Н. Н., Воронова Е. М. Однако отличительной особенностью работ этих авторов является то, что в них информационный конфликт рассматривался исключительно применительно к предметной области систем связи и АСУ.

Направлением же исследований автора является формирование моделей развития и прогнозирования результатов конфликта «СВКН – система ВКО», исследование устойчивости системы ВКО (СУ ВКО) при динамическом противоборстве со СВКН.

Развитие ударных средств, средств РЭП, системы разведки и целеуказания потенциального противника и совершенствование методологии их применения, с учетом необходимости противодействовать ему в ходе подготовки и реализации первого этапа развития полномасштабного военного конфликта, позволяет сформулировать актуальную ***прагматическую цель исследования*** – повышение устойчивости системы ВКО при динамическом конфликте с СВКН.

Объект исследования – динамический информационный конфликт организационно-технических систем – «система ВКО» и «СВКН».

Предмет исследования – устойчивость системы ВКО в условиях ее конфликтного взаимодействия с СВКН.

Проведенный анализ имеющихся научных работ в области конфликта «СВКН – система ВКО» позволил сформулировать **противоречие *между*** *необходимостью учета динамики развития информационного конфликта между такими организационно-техническими системами как «система ВКО» и «СВКН», а также повышения устойчивости системы ВКО при динамическом конфликте с СВКН* ***и*** *отсутствием элементов научно-методического аппарата оценивания динамических свойств информационных конфликтов, а также методов повышения устойчивости системы ВКО в условиях конфликта «СВКН – система ВКО».*

Для разрешения указанного противоречия предлагается решить ***научную проблему*** *развития теории информационного конфликта за счет разработки элементов научно-методического аппарата, учитывающего динамические свойства информационных конфликтов организационно-технических систем, а также повышения устойчивости системы ВКО, возникающих в условиях конфликта «СВКН – система ВКО».*

Решение научной проблемы предполагается вести через достижение ***цели исследования*** *– повышение устойчивости системы ВКО в условиях ее конфликтного взаимодействия с СВКН.*

Современное представление структуры конфликта «СВКН – система ВКО» практически не отражает возможности обеих ОТС по адаптации к складывающейся оперативно-тактической обстановке ведения боевых действий.

В частности, для повышения устойчивости ВКО предлагается выполнять следующий комплекс мероприятий:

1) оценивать состояние системы ВКО (в том числе СУ ВКО) в реальном (или близком к нему) масштабе времени;

2) в случае снижения устойчивости ниже требуемого (заданного) уровня производить восстановление ее работоспособного состояния, за счет выбора и реализации стратегий защиты (восстановления устойчивости):

- ввода в строй имеющихся «резервов» элементов системы ВКО (запасных и резервных командных пультов (КП), средств РиКВП, линий связи);
- реконфигурации системы связи, в том числе переход каналов связи на более развед- и помехозащищенные режимы работы, изменение путей передачи информации (ППИ) между взаимодействующими элементами системы ВКО и др.;
- восстановления состояния КП, вышедшего (выведенного) из строя, на одном из запасных (или резервных) КП за счет заблаговременного децентрализованного сохранения информации о его состоянии на других КП (например, в виде RAID-массивов);
- другие мероприятия;

3) предварительно закладывать в систему ВКО структурную, функциональную и информационную избыточность, в том числе за счет перехода от фиксированного иерархического принципа построения к адаптивно-сетевому;

4) применять средства противодействия СВКН (физического поражения (ФП) и РЭП), в том числе каналу разведки.

Процесс конфликтного взаимодействия ОТС S_1 и S_2 возможен в том случае, когда эти ОТС совместно функционируют в едином информационном пространстве. Такая область их совместного функционирования в информационном пространстве формируется принципиальной возможностью огневого и радиоэлектронного взаимодействия элементов каждой из ОТС и является ключевой с точки зрения начала и развития конфликта.

Суть конфликтного взаимодействия заключается с одной стороны, во-первых, в физическом (огневом) поражении элементов системы ВКО, а именно, КП, средств РиКВП, ударных средств ВКО, средств РЭП, а во-вторых, в радиоэлектронном подавлении линий связи между взаимодействующими КП, а также линий связи между КП и средствами РиКВП, и собственно радиоэлектронном подавлении самих средств РиКВП. С другой стороны, система ВКО, в свою очередь, применяет средства физического (огневого) поражения и средства радиоэлектронного подавления информационных средств СВКН с целью выполнения своего основного предназначения – обеспечения защиты (обороны) прикрываемого объекта от СВКН противника, а также обеспечения защиты (обороны) собственных элементов системы ВКО (в том числе СУ ВКО) (рис. 1) [2, 11].

Новизну проводимых автором исследований определяет учет двух основных факторов. Во-первых, сложное построение противоборствующих сторон, имеющих в своем составе подсистему управления, подсистему разведки и целеуказания, ударную подсистему и подсистему РЭП. Во-вторых, учет возможности адаптации обеих организационно-технических систем к складывающейся оперативно-тактической обстановке ведения боевых действий. Кроме того, опыт ведения специальной военной операции (СВО) Российской Федерацией и Ирано-Американо-Израильского военного конфликта наглядно демонстрирует существенное изменение спектра применяемых противоборствующими сторонами СВКН, а также низкую эффективность старых принципов построения систем ВКО.

На данный момент автором разработаны и опубликованы следующие научные результаты:

1. Анализ актуальности и постановка проблемы развития теории информационных конфликтов за счет разработки элементов научно-методического аппарата, учитывающего динамические свойства информационных конфликтов организационно-технических систем и возможности по адаптации обеих ОТС к складывающейся оперативно-тактической обстановке.

1.1. Анализ современного состояния и уровня развития системы воздушно-космической обороны [1, 11, 12].

1.2. Системный анализ развития средств воздушно-космического нападения вероятного противника и средств воздействия на многоэшелонированную систему ПВО, методов и способов их применения [1, 11, 13-18].

1.3. Анализ состояния научно-методического аппарата формализации и моделирования информационных конфликтов организационно-технических систем [11, 19-22].

1.4. Постановка проблемы, формулирование частных проблем и задач, рамок исследования [23, 24].

2. Общий подход к формализации динамических информационных конфликтов организационно-технических систем (выполнено частично).

2.1. Постановка частной научной задачи на разработку общего подхода к формализации динамических информационных конфликтов организационно-технических систем [25].

2.2. Концептуальная модель динамического информационного конфликта организационно-технических систем (рис. 1) [25].

2.3. Модель оценивания устойчивости системы управления воздушно-космической обороной в конфликте со средствами воздушно-космического нападения [26].

В настоящее время разрабатываются и планируются к разработке:

2.4. Влияние динамических свойств информационно-управляющих систем на интенсивность конфликтного взаимодействия.

2.5. Влияние информационных потерь на показатели оперативности и достоверности управления.

2.6. Общий подход к формализации и моделированию динамического информационного конфликта.

3. Модели, метод и комплекс методик оценивания динамических свойств информационных конфликтов организационно-технических систем.

3.1. Постановка частной научной задачи разработки моделей и метода оценивания динамических свойств информационных конфликтов организационно-технических систем.

3.2. Общий подход к моделированию динамического информационного конфликта методами теории популяционной динамики.

3.3. Обобщенная динамическая модель информационного конфликта.

3.4. Модели информационных конфликтов при различных исходных условиях.

3.5. Метод оценивания динамических свойств информационных конфликтов организационно-технических систем.

3.6. Комплекс методик оценивания структурных и временных параметров устойчивости систем управления в условиях динамического информационного конфликта.

4. Метод и комплекс частных методик достижения информационного превосходства в процессе динамического информационного конфликта организационно-технических систем.

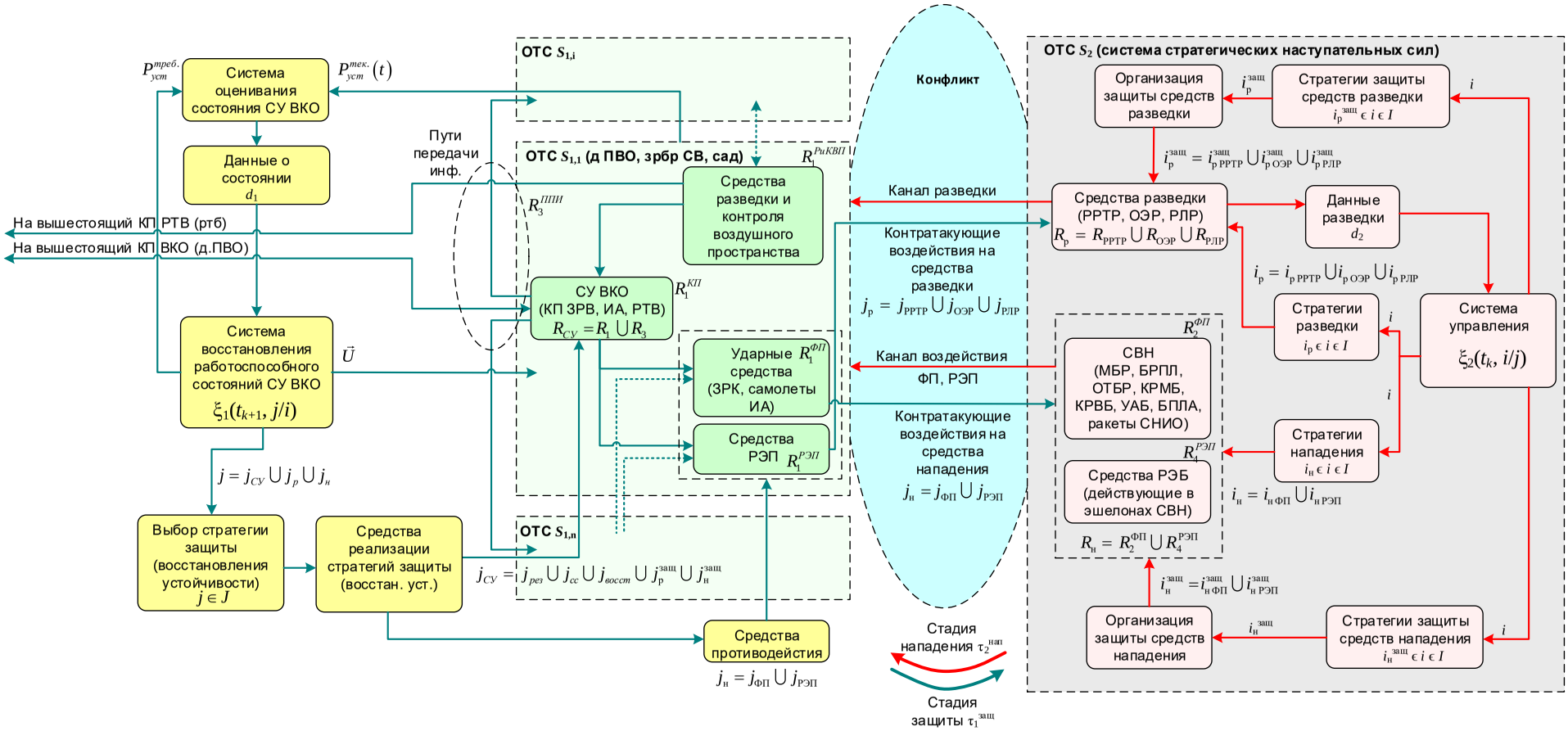

Рис. 1. Схема концептуальной модели конфликта ОТС S_1 и S_2

4.1. Постановка частной научной задачи разработки метода достижения информационного превосходства в процессе динамического информационного конфликта организационно-технических систем.

4.2. Метод достижения информационного превосходства в процессе динамического информационного конфликта организационно-технических систем.

4.3. Комплекс частных методик достижения информационного превосходства в процессе динамического информационного конфликта организационно-технических систем.

4.4. Оценка уровня повышения устойчивости системы управления при использовании метода достижения информационного превосходства в процессе динамического информационного конфликта организационно-технических систем.

5. Научно-технические предложения по совершенствованию информационного контура организационно-технических систем в условиях информационного конфликта.

5.1. Постановка частной прикладной задачи разработки научно-технических предложений по совершенствованию информационного контура организационно-технических систем в условиях информационного конфликта.

5.2. Научно-технические предложения по совершенствованию информационного контура системы предупреждения о ракетном нападении в условиях информационного конфликта.

5.3. Научно-технические предложения по совершенствованию информационного контура системы противовоздушной и противоракетной обороны в условиях информационного конфликта.

5.4. Научно-технические предложения по совершенствованию информационного контура радиотехнических войск в условиях информационного конфликта.

5.5. Научно-технические предложения по совершенствованию информационного контура системы радиоэлектронной разведки в условиях информационного конфликта.

5.6. Научно-технические предложения по совершенствованию информационного контура системы радиоэлектронной борьбы в условиях информационного конфликта.

Решением этих частных задач будут соответствующие научные и прикладные результаты значимые для развития теории информационного конфликта и обладающие практическим эффектом в части повышения устойчивости системы ВКО при динамическом конфликте с СВКН противника.

Таким образом, направлением исследований автора является формирование моделей развития и прогнозирования результатов конфликта «СВКН – система ВКО» и исследование устойчивости ВКО при нанесении противником удара СВКН.

Литература

1. Афонин И. Е., Макаренко С. И., Михайлов Р. Л. Быстрый глобальный удар: ретроспективный анализ концепции, вероятный сценарий нанесения, состав сил и средств, последствия и приоритетные мероприятия по противодействию. Монография. – СПб.: Наукоемкие технологии, 2022. – 174 с.

2. Ачасов О. Б., Буравлев А. И. Аналитическая модель оценки эффективности воздушно-космической обороны в условиях глобального удара высокоточным оружием // Вооружение и экономика. 2021. № 2 (27). С. 10-20.

3. Криницкий Ю. ВКО России: признаки будущей системы // Воздушно-космическая оборона. 2012. № 2. – URL: https://militaryarticle.vibrokatok.by/voenno-kosmicheskaya-oborona/2012/12688-vko-rossii-priznaki-budushhej-sistemy (дата обращения: 16.05.2025).

4. Чельцов Б. Система ВКО России есть ли у нее будущее // Воздушно-космическая оборона. 2003. № 6. – URL: https://militaryarticle.vibrokatok.by/voenno-kosmicheskaya-oborona/2003/12245-sistema-vko-rossii-est-li-u-nee-budushhee (дата обращения: 16.05.2025).

5. Чельцов Б. Воздушно-космической обороне – адекватное отражение в Военной доктрине России // Российское военное обозрение. 2007. № 4 (39). – URL: http://www.grinchevskiy.ru/rvo/042007/vozdushno-kosmicheskoy-oborone.php (дата обращения: 16.05.2025).

6. Михайлов А. Как строить ВКО в современных условиях // Воздушно-космическая оборона. 2010. № 5. – URL: https://militaryarticle.vibrokatok.by/voenno-kosmicheskaya-oborona/2010/12605-kak-stroit-vko-v-sovremennyh-uslovijah (дата обращения: 16.05.2025).

7. Ягольников С. В. Проблемы создания технической основы воздушно-космической обороны страны и пути их решения // Академия военных наук Российской Федерации [Электронный ресурс]. – URL: https://avnrf.ru/index.php/pravila-priema/proekty/72-novosti-sajta/629-problemy-sozdaniya-tekhnicheskoj-osnovy-vozdushno-kosmicheskoj-oborony-strany-i-puti-ikh-resheniya (дата обращения: 16.05.2025).

8. Палицын А. Б., Жиленко Д. Б. Анализ традиционных и перспективных задач системы воздушно-космической обороны России: проблемы и пути их решения // Военная мысль. 2020. № 9. С. 6-17.

9. Дронов С. В., Харин С. В. Проблемные вопросы обеспечения устойчивости функционирования системы управления истребительной авиации и пути их решения // Военная мысль. 2023. № 8. С. 71-78.

10. Афонин И. Е., Макаренко С. И., Петров С. В. Модель оценивания устойчивости системы управления воздушно-космической обороной в конфликте со средствами воздушно-космического нападения // Системы управления, связи и безопасности. 2023. № 3. С. 227-266.

11. Афонин И. Е., Макаренко С. И., Михайлов Р. Л. Описательная модель боевых потенциалов сторон в конфликте системы воздушно-космической обороны со средствами воздушно-космического нападения // Системы управления, связи и безопасности. 2022. № 3. С. 41-66.

12. Макаренко С. И., Ковальский А. А., Афонин И. Е. Обоснование перспективных направлений развития системы противокосмической обороны Российской Федерации в интересах своевременного вскрытия и отражения «Быстрого глобального удара» средств воздушно-космического нападения // Воздушно-космические силы. Теория и практика. 2020. № 16. С. 99-115.

13. Афонин И. Е., Макаренко С. И., Митрофанов Д. В. Анализ концепции «Быстрого глобального удара» средств воздушно-космического нападения и обоснование перспективных направлений развития системы воздушно-космической обороны в Арктике в интересах защиты от него // Воздушно-космические силы. Теория и практика. № 15. С. 75-87.

14. Афонин И. Е., Макаренко С. И., Петров С. В. Описательная модель комплексов разведки, используемых для вскрытия системы воздушно-космической обороны и целеуказания при нанесении удара средствами воздушно-космического нападения // Системы управления, связи и безопасности. 2021. № 1. С. 190-214.

15. Афонин И. Е., Макаренко С. И., Петров С. В. Описательная модель подсистемы радиоэлектронного подавления в составе средств воздушно-космического нападения, используемых для нарушения функционирования элементов системы воздушно-космической обороны // Системы управления, связи и безопасности. 2021. № 2. С. 76-95.

16. Афонин И. Е., Макаренко С. И., Михайлов Р. Л. Средства воздушно-космического нападения ведущих зарубежных стран. Часть 1. Межконтинентальные баллистические ракеты // Системы управления, связи и безопасности. 2024. № 1. С. 138-190.

17. Афонин И. Е., Макаренко С. И., Михайлов Р. Л., Куприянов Н. А., Потапов А. А. Средства воздушно-космического нападения ведущих зарубежных стран. Часть 2. Баллистические ракеты подводных лодок // Системы управления, связи и безопасности. 2024. № 4. С. 223-286.

18. Афонин И. Е., Дисенов А. А., Черепанов Д. А., Макаренко С. И., Михайлов Р. Л. Средства воздушно-космического нападения ведущих зарубежных стран. Часть 3. Баллистические ракеты большой дальности // Системы управления, связи и безопасности. 2025. № 3. С. 170-215.

19. Макаренко С. И., Афонин И. Е., Копичев О. С., Мамончикова А. С. Обобщенная модель Ланчестера, формализующая конфликт нескольких сторон // Автоматизация процессов управления. 2021. № 2. С. 66-76.

20. 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.

21. Модели военных, боевых и специальных действий / Под ред. Д. А. Новикова. – М.: ЛЕНАНД, 2025. – 528 с.

22. Афонин И. Е., Афонин Л. И. Модели, описывающие динамику численности наблюдаемых радиоэлектронных средств // Межвузовский сборник научных трудов. Вып. № 28. – Краснодар: КВВАУЛ, 2024. – С. 29-35.

23. Афонин И. Е., Петров С. В., Макаренко С. И. Переход к адаптивно-сетевой структуре системы управления воздушно-космической обороной, как один из основных путей повышения ее устойчивости // Воздушно-космические силы. Теория и практика. 2021. № 19. С. 159–178.

24. Афонин И. Е., Табырца Д. В. Перспективы использования новых информационных технологий в системе управления воздушно-космической обороной // Состояние и перспективы развития современной науки по направлению «Робототехника»: Сборник статей V Всероссийской научно-технической конференции, Анапа, 19-20 июля 2023 г. – Анапа: Федеральное государственное автономное учреждение «Военный инновационный технополис «ЭРА», 2023. – С. 421-431.

25. Афонин И. Е. Концептуальная модель конфликта системы управления воздушно-космической обороной и средств воздушно-космического нападения // Системы управления, связи и безопасности. 2025. № 3. С. 1-34.

26. Афонин И. Е., Макаренко С. И., Петров С. В. Модель оценивания устойчивости системы управления воздушно-космической обороной в конфликте со средствами воздушно-космического нападения // Системы управления, связи и безопасности. 2023. № 3. С. 227-266.

Информация об авторе

Афонин Илья Евгеньевич – кандидат технических наук, доцент. Доцент кафедры авиационного и радиоэлектронного оборудования. Краснодарское высшее военное авиационное училище летчиков. Область научных интересов: информационный конфликт средств воздушно-космического нападения и системы воздушно-космической обороны; радиолокационные системы обнаружения, распознавания и целеуказания; обработка радиолокационных сигналов. E-mail: ilyaafonin@yandex.ru

Адрес: Россия, 350090, г. Краснодар, ул. Дзержинского, д. 135.

УДК 623.01

Актуальные вопросы повышения устойчивости системы воздушно-космической обороны в конфликте со средствами воздушно-космического нападения

Петров С. В.

В статье производится анализ актуальности вопросов, связанных с повышением устойчивости системы воздушно-космической обороны в конфликте со средствами воздушно-космического нападения. Рассмотрен состав системы воздушно-космической обороны и средств воздушно-космического нападения, как сложных организационно-технических систем, взаимодействие которых может быть формализовано в виде конфликта. Представлены частные результаты, которые планируется использовать в качестве положений, выносимых на защиту диссертации на соискание ученой степени кандидата технических наук.

Ключевые слова: *средства воздушно-космического нападения, система воздушно-космической обороны, быстрый глобальный удар, организационно-техническая система, конфликт, устойчивость.*

Анализ военных конфликтов начала XXI века, проведённый в работе [1], показывает, что стратегия современных войн предусматривает нанесение массированного «обезоруживающего» удара средствами воздушно-космического нападения (СВКН) по военным и государственным объектам государства – противника в первые часы войны. В частности, в США разработана концепция «Быстрый глобальный удар» (БГУ), которая предусматривает одновременное массированное применение высокоточного оружия (ВТО) в обычном оснащении: крылатых ракет морского и воздушного базирования (КРМБ, КРВБ), межконтинентальных баллистических ракет (МБР), баллистических ракет подводных лодок (БРПЛ) по основным объектам военной и государственной инфраструктуры Российской Федерации (РФ). Анализ концепции БГУ, состава сил и средств ВТО, порядка применяя СВКН, представленный в работах [2-5] показывает, что при нанесении БГУ предусматривается применение двух ударных эшелонов СВКН. Первый эшелон СВКН ориентирован подавление системы воздушно-космической обороны (ВКО) РФ, второй – непосредственно на поражение объектов военной и государственной инфраструктуры РФ, в условиях уже подавленной ВКО. Таким образом, одной из основных задач противодействия БГУ со стороны системы ВКО является обеспечение ее устойчивости при нанесении удара первого эшелона БГУ в интересах недопущения поражения объектов военной и государственной инфраструктуры РФ вторым эшелоном БГУ.

Система ВКО представляет собой сложную иерархическую пространственно-распределенную организационно-техническую систему (ОТС), предна-

---

Статья (тезис) опубликована в сборнике докладов конференции:
I семинар научной школы профессора С. И. Макаренко. Сборник тезисов докладов конференции. г. Санкт-Петербург, 20-21 декабря 2025 года. – СПб.: Наукоемкие технологии, 2026.

значенную для защиты РФ от СВКН, в состав которой, в качестве ее составных частей входит [6-8]:

- система наблюдения – предназначенная для разведки и контроля за воздушно-космической обстановкой, вскрытия факта нанесения удара СВКН и их параметров, а также для выдачи целеуказаний средствам поражения ударной системы ВКО. Система наблюдения представляет собой пространственно-распределенную совокупность: радиолокационных станций (РЛС) контроля воздушного пространства наземного и воздушного базирования; наземных оптико-электронных средств (ОЭС) и РЛС контроля космического пространства; РЛС и ОЭС системы предупреждения о ракетном нападении (СПРН) наземного и космического базирования;
- ударная система – предназначенная для поражения СВКН, и представляющая собой пространственно-распределенную совокупность: зенитно-ракетных комплексов (ЗРК), организованных в многоэшелонированную систему противовоздушной обороны; самолёты и ударные беспилотные летательные аппараты (БПЛА) истребительной авиации; ударные средства противоракетной обороны (ПРО); ударные средства противокосмической обороны; средства радиоэлектронной борьбы, решающие задачи радиоэлектронного подавления (РЭП) каналов управления и РЛС СВКН в интересах обеспечения радиоэлектронной защиты своих сил и средств от средств РЭП противника;
- система управления – предназначенная для управления силами и средствами ВКО и представляющая собой иерархически-организованную, в соответствии со звеньями управления, совокупность автоматизированных систем управления (АСУ) и комплексов средств автоматизации (КСА) элементов системы наблюдения и ударной системы;
- система связи – предназначенная для передачи данных информационного обеспечения и команд управления между всеми элементами ВКО и представляющая собой пространственно-распределенную сеть узлов (каждый узел соответствует отдельному элементу системы ВКО) и каналов связи, построенную на основе проводных и радио- технологий.

При этом основной частью ОТС ВКО является система управления, использующая подсистему наблюдения и ударную подсистему в качестве собственных ресурсов для решения задачи отражения удара СВКН в первом эшелоне БГУ, которые могут быть интерпретированы как классические задачи органа управления – наблюдения и управления. При этом для доведения информации наблюдения и управления используется система связи. Таким образом, устойчивость системы ВКО, в целом, можно интерпретировать как устойчивость ее системы управления так как, фактически, каждый элемент системы наблюдения можно интерпретировать как источник информации для системы управления, а каждый элемент ударной системы – как объект управления, при этом все эти элементы замкнуты в единый цикл боевого управления в конфликте «система ВКО – система СВКН» посредством информационного обмена через систему связи.

Классически, под устойчивостью управления понимают способность органов управления выполнять свои функции в сложной, резко меняющейся обстановке в условиях помех и дестабилизирующих воздействиях [9]. С учетом сказанного, под понятием «*устойчивость системы управления ВКО*» будем понимать ее способность выполнять задачи по отражению ударов СВКН с требуемым качеством в условиях дестабилизирующих воздействий. При этом в качестве дестабилизирующих воздействий, в контексте данной работы, рассматриваются, прежде всего, негативное влияние СВКН первого эшелона БГУ.

При этом, первый эшелон БГУ, направленный на подавление системы ВКО, также может быть формализован в виде ОТС СВКН в состав которой, в качестве ее составных частей входит [3]:

- средства наблюдения – совокупность средств радио- и радиотехнической, оптико-электронной, радиолокационной и компьютерной разведки, наземного, воздушного и космического базирования, предназначенных для вскрытия местоположения элементов ВКО и их параметров, с последующей выдачей целеуказаний для ударных СВКН;
- средства физического поражения – совокупность: гиперзвуковых крылатых ракет; самолетов и БПЛА – носителей ВТО; подводных лодок и надводных кораблей – носителей ВТО; МБР; БРПЛ; КРВБ; КРМБ; самонаводящегося на излучение оружия, предназначенных для огневого физического поражения элементов ВКО;
- средства радиоэлектронного подавления (РЭП) – совокупность средств РЭП воздушного базирования, предназначенных для подавления РЛС системы наблюдения и каналов системы связи ВКО;
- средства функционального поражения электромагнитным излучением – совокупность КРМБ, КРВБ, МБР и БРПЛ в которых в качестве боевой части установлен генератор мощного СВЧ-излучения, предназначенных для поражения радиоэлектронных средств, находящихся в составе: РЛС системы наблюдения, ЗРК, комплексов РКО и ПРО, пунктов управления, оборудованных АСУ и КСА, узлов системы связи.

Взаимодействие ОТС ВКО и ОТС СПРН может быть формализовано в виде конфликта. При этом, под конфликтом, в контексте данной работы, будем понимать следующее.

Конфликт – процесс столкновения системы ВКО со СВКН на этапах формирования и сбора данных об обстановке, формировании команд управления ударными средствами и средствами наблюдения, передачи данных информационного обеспечения и команд управления, при этом СВКН стремятся нарушить процессы управления в системе ВКО за счет вскрытия местоположения и параметров ее элементов, их огневого физического и функционального поражения, а также радиоэлектронного подавления, с целью снизить эффективность системы ВКО.

Обобщая вышесказанное, можно сделать вывод об актуальности выполнения исследований с целью повышения устойчивости системы управления ВКО в конфликте со СВКН. При этом научной задачей исследования будет раз-

работка моделей и методики повышения устойчивости системы управления ВКО в конфликте со СВКН. А планируемыми частными результатами:

В свою очередь, частными научными результатами, которые планируется использовать в качестве положений, выносимых на защиту, являются:

1) описательная модель конфликта системы ВКО со СВКН;
2) модель оценивания устойчивости системы управления ВКО в конфликте со СВКН;
3) методика повышения устойчивости системы управления ВКО в конфликте со СВКН;
4) технические предложения по совершенствованию алгоритмического обеспечения системы управления ВКО в конфликте со СВКН.

В качестве теоретической основы для решения вышеуказанной научной задачи, предполагается использовать работы [9-23] по моделированию динамических информационных конфликтов. При этом новизной исследования является приложение известных подходов к исследованию динамических систем, методов системного анализа, моделей информационного конфликта к новой предметной области – процессу конфликтного взаимодействия системы ВКО со СВКН.

Литература

1. Макаренко С. И., Иванов М. С. Сетецентрическая война – принципы, технологии, примеры и перспективы. Монография. – СПб.: Наукоемкие технологии, 2018. – 898 с.

2. Михайлов Д. В. Война будущего: возможный порядок нанесения удара средствами воздушного нападения США в многосферной операции на рубеже 2025-2030 годов // Воздушно-космические силы. Теория и практика. 2019. № 12. С. 44-52.

3. Афонин И. Е., Макаренко С. И., Михайлов Р. Л. Быстрый глобальный удар: ретроспективный анализ концепции, вероятный сценарий нанесения, состав сил и средств, последствия и приоритетные мероприятия по противодействию. Монография. – СПб.: Наукоемкие технологии, 2022. – 174 с.

4. Афонин И. Е., Макаренко С. И., Митрофанов Д. В. Анализ концепции «быстрого глобального удара» средств воздушно-космического нападения и обоснование перспективных направлений развития системы воздушно-космической обороны в Арктике в интересах защиты от него // Воздушно-космические силы. Теория и практика. 2020. № 15. С. 75-87.

5. Макаренко С. И. Использование космического пространства в военных целях: современное состояние и перспективы развития систем информационно-космического обеспечения и средств вооружения // Системы управления, связи и безопасности. 2016. № 4. С. 161-213.

6. Справочник офицера воздушно-космической обороны / Под общей редакцией С.К. Бурмистрова. – Тверь: ВА ВКО, 2006. – 564 с.

7. Карпенко А. В. Противоракетная и противокосмическая оборона // Невский бастион. Приложение к военно-техническому сборнику. 1998. № 4. 49 с.

8. Диалектика технологий воздушно-космическое обороны / Под ред. В.Н. Минаева. – М.: Издательский дом «Столичная энциклопедия», 2011. – 367 с.

9. Макаренко С. И. Модели системы связи в условиях преднамеренных дестабилизирующих воздействий и ведения разведки. Монография. – СПб.: Наукоемкие технологии, 2020. – 337 с.

10. Макаренко С. И. Динамическая модель двунаправленного информационного конфликта с учетом возможностей сторон по наблюдению, захвату и блокировке ресурса // Системы управления, связи и безопасности. 2017. № 1. С. 60-97.

11. Макаренко С. И. Динамическая модель системы связи в условиях функционально-разноуровневого информационного конфликта наблюдения и подавления // Системы управления, связи и безопасности. 2015. № 3. С. 122-185.

12. Макаренко С. И. Информационный конфликт системы связи с системой дестабилизирующих воздействий. Часть I: Концептуальная модель конфликта с учетом ведения разведки, физического, радиоэлектронного и информационного поражения средств связи // Техника радиосвязи. 2020. № 2 (45). С. 104-117.

13. Макаренко С. И. Информационный конфликт системы связи с системой дестабилизирующих воздействий. Часть II: Формализация основных аспектов, определяющих выигрыш в конфликте // Техника радиосвязи. 2020. № 3 (46). С. 103-115.

14. Афонин И. Е. Концептуальная модель конфликта системы управления воздушно-космической обороной и средств воздушно-космического нападения // Системы управления, связи и безопасности. 2025. № 3. С. 1-34.

15. Афонин И. Е., Макаренко С. И., Петров С. В. Модель оценивания устойчивости системы управления воздушно-космической обороной в конфликте со средствами воздушно-космического нападения // Системы управления, связи и безопасности. 2023. № 3. С. 227-266.

16. Макаренко С. И., Афонин И. Е., Копичев О. С., Мамончикова А. С. Обобщенная модель Ланчестера, формализующая конфликт нескольких сторон // Автоматизация процессов управления. 2021. № 2. С. 66-76.

17. Афонин И. Е., Макаренко С. И., Петров С. В. Описательная модель комплексов разведки, используемых для вскрытия системы воздушно-космической обороны и целеуказания при нанесении удара средствами воздушно-космического нападения // Системы управления, связи и безопасности. 2021. № 1. С. 190-214.

18. Афонин И. Е., Макаренко С. И., Петров С. В. Описательная модель подсистемы радиоэлектронного подавления в составе средств воздушно-космического нападения, используемых для нарушения функционирования элементов системы воздушно-космической обороны // Системы управления, связи и безопасности. 2021. № 2. С. 76-95.

19. Афонин И. Е., Петров С. В., Макаренко С. И. Переход к адаптивно-сетевой структуре системы управления воздушно-космической обороной, как

один из основных путей повышения ее устойчивости // Воздушно-космические силы. Теория и практика. 2021. № 19. С. 159–178.

20. Афонин И. Е., Макаренко С. И., Михайлов Р. Л. Описательная модель боевых потенциалов сторон в конфликте системы воздушно-космической обороны со средствами воздушно-космического нападения // Системы управления, связи и безопасности. 2022. № 3. С. 41-66.

21. Афонин И. Е., Афонин Л. И. Модели, описывающие динамику численности наблюдаемых радиоэлектронных средств // Межвузовский сборник научных трудов. Вып. № 28. – Краснодар: КВВАУЛ, 2024. – С. 29-35.

22. 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.

23. Модели военных, боевых и специальных действий / Под ред. Д. А. Новикова. – М.: ЛЕНАНД, 2025. – 528 с.

Информация об авторе

Петров Сергей Валерьевич – соискатель ученой степени кандидата наук. Преподаватель кафедры авиационного и радиоэлектронного оборудования. Краснодарское высшее военное авиационное училище летчиков. Область научных интересов: устойчивость системы воздушно-космической обороны; радиоэлектронная борьба. E-mail: perskub@yandex.ru

Адрес: Россия, 350090, г. Краснодар, ул. Дзержинского, д. 135.

УДК 303.732.4

Апробация методологии С.И. Макаренко по формированию научно-методического аппарата диссертации по техническим наукам

Касаткин Ф. Ю.

В статье рассматривается практический пример формирования автором научно-методического аппарата своей диссертации по техническим наукам на базе методологии С.И. Макаренко и имеющегося неструктурированного научного материала – результатов исследования качества обработки вызовов в центрах обработки вызовов, методик оценки и оптимизации данного качества.

Ключевые слова: *формальные положения диссертации, частные научные задачи, частная прикладная задача, эффективность обработки информации, качество обработки информации, ординальная оценка качества, кардинальная оценка качества.*

Актуальность

В соответствии со статистикой, приведенной в работе [1], в год в России защищает кандидатские диссертации до 7000 человек. Выходящие на защиту соискатели ученой степени кандидата наук (в широком смысле; далее – соискатели) делятся на две группы – аспирантов (адъюнктов), обучающихся в высших учебных заведениях (около 1600 защит в год), и соискателей (в узком смысле), самостоятельно работающих над кандидатскими диссертациями (около 5400 защит в год). Как указано в работе [2] порядка 95% успешных защит подтверждается ВАК выдачей соответствующих дипломов, поэтому далее пренебрежем разницей между количеством выходящих на защиту и защитившихся соискателей.

Согласно данным из [1], из числа заканчивающих аспирантуру защищается только 11%. Количество соискателей, работавших над кандидатскими диссертациями, но по тем или иным причинам потерявших мотивацию и не вышедших на защиту, статистическими методами не определялось. Ввиду априорной неопределенности их доли, примем гипотезу, что она равна аналогичной доле для аспирантов, а именно 89%. Данная гипотеза включает в себя допущение, что основной причиной невыхода на защиту является именно утеря мотивации, а доля объективных причин непреодолимой для соискателя силы относительно невелика.

Исходя из указанной гипотезы, следует предположить, что ежегодно около 55000 человек отказываются от финализации и (или) защиты кандидатской

Статья (тезис) опубликована в сборнике докладов конференции:
I семинар научной школы профессора С. И. Макаренко. Сборник тезисов докладов конференции. г. Санкт-Петербург, 20-21 декабря 2025 года. – СПб.: Наукоемкие технологии, 2026.

диссертации ввиду субъективных причин. Данные причины для аспирантов проанализированы в работе [3]. Согласно данной работе, причиной отказа в выходе на защиту несмотря на окончание аспирантуры (подразумевающее за исключением частных случаев представление проекта диссертационной работы) в 44% случаев является «Трудности с написанием (подготовкой) текста диссертации». В рамках введенной выше гипотезы следует предположить, что более 24000 соискателей таким образом отказываются от доведения диссертации до защиты ввиду высокой степени формализации требований к составу диссертационной работы, акцентированной необходимости показывать мировую новизну достигаемых научных результатов, вклад в науку и пр. (см., например, работу [4]) независимо от объективного масштаба научных достижений соискателя (при фактическом наличии таковых и наличии в них элементов как научной, так и практической новизны). Данный вопрос в полемической форме раскрыт, например, в работе [5].

При этом в распоряжении каждого соискателя находится практически неограниченное количество литературы по методологии диссертационного исследования начиная от Положения о присуждении ученых степеней [6] – основного нормативно-правового акта, определяющего правоприменение законодательства РФ в области науки к предмету подготовки и защиты кандидатских диссертаций и по данной причине имеющего максимально возможную абстрактность, заканчивая работой [7] и аналогичными ей – передающими личный опыт автора от первого лица, относящихся к повествовательно-мотивирующим и применимым в качестве методического пособия исключительно для соискателей, работающих по тем же научным специальностям, что и авторы, и находящихся в хотя бы относительно аналогичной жизненной ситуации.

Вместе с тем, подавляющую часть данной литературы составляют вузовские учебники для аспирантов, по своей природе доводящие до читателя исключительно абстрактные основы научной работы и не преследующие в рамках соответствующих учебных курсов, которые они методологически обеспечивают, на помощь читателю в решении каких-либо прикладных задач в отношении его собственной работы.

Следует особо отметить литературу, которая не только формализует структуру и диалектическую связь элементов диссертационной работы, но и поясняет читателю раскрываемые положения, утверждения, выводы и связи. Наиболее яркими представителями такого класса литературы являются работы [4, 8, 9] и другие. Подробный анализ литературы по данной теме приведен в работе [10]. Несмотря на стройность и строгость раскрываемой методологии написания диссертационного исследования, указанные работы имеют общие особенности, крайне затрудняющие адекватное (в значении согласно работы [11] восприятие и практическое применение значительным числом соискателей теоретических положений указанных работ к собственному исходному материалу: высокую степень абстракции и бедность конкретных практических примеров. Также, существенным недостатком указанных работ является их сугубо теоретическая ориентация, не учитывающая и не отражающая фактической (субъективной) картины дел в предметных областях различных областей

наук и, соответственно, значительно идеализирующая реальные обстоятельства, важные (иногда – критически) для реальных защит.

Отдельно следует отметить работы [12, 13], которые представляют принципиально иной подход к построению и доведению до соискателя методологии диссертационного исследования. Работа [12] объективно сочетает достаточную строгость предлагаемой читателю методологии, простоту и доступность изложения и мотивирующие элементы. Однако, при указанном наборе преимуществ для соискателя, данная работа имеет принципиальный недостаток: она полностью лишена конкретных примеров, конкретизирующих теоретические положения автора. Причины этого автор вполне прозрачно и многократно доводит до читателя в работе. Не давая оценки выбранному автором указанной работы подходу, следует констатировать, что практическая ценность указанной работы (в отличие от теоретической) для среднего соискателя минимальна.

Работа [13], выдержав значительное количество переизданий, тем самым показала свою практическую значимость и востребованность для читателя. В ней приводится относительно сбалансированное сочетание методологии диссертационного исследования, существующих в научной среде диалектических связей и противоречий, а также последовательности действий от возникновения побуждения соискателя к научной работе до защиты кандидатской диссертации включительно. Однако, несмотря на выдающиеся достоинства работы [13], указанные выше, она вместе с тем имеет ряд принципиальных недостатков, значительно снижающих ее практическую ценность для соискателя. Основных недостатков два: относительно слабая адекватность сегодняшнему дню (работа в основном отражает реальность 1980-х годов) и практически полное отсутствие практических примеров в методологической части. По указанным причинам данную работу следует отнести к области скорее мотивирующей, чем помогающей формализовать научный багаж соискателя литературы.

Результатом описанных выше обстоятельств является проблемная ситуация, объединяющая как противоречие в науке (несмотря на исключительное изобилие работ по методологии подготовки и формирования диссертационного исследования, в них отсутствует необходимое и достаточное сочетание доводимых до соискателя формальных положений с понятными ему конкретными примерами, охватывающими имеющееся на практике тем и специфик диссертационных работ), так и противоречие в практике (несмотря на априорно значительное число соискателей, потенциально готовых не только заниматься ученой работой, но оформить полученные результаты в виде кандидатской диссертации, не менее 89 % · 44 % = 39 % из них не делают этого ввиду труднопонятности соответствующей методологии). Следовательно, построение методологии, свободной от указанных выше недостатков, является актуальной задачей, поскольку позволит в рамках принятой выше гипотезы увеличить долю защищающихся соискателей с нынешних 11 % до 11 % + + 39 % = 50 %, т.е. в 4,5 раза.

Разрешение проблемной ситуации

По мнению автора настоящей статьи, эффективным (в значении, раскрытом в работе [11]) вариантом разрешения указанной выше проблемной ситуа-

ции для соискателя, имеющего некий багаж научных наработок (в общем случае – неструктурированных и неформализованных) и достаточно мотивированного для их оформления в научно-квалификационную работу (кандидатскую диссертацию – см. [5]) с последующим выходом на защиту является детальное изучение и последовательное применение работы С.И. Макаренко [10]. Ключевые особенности данной работы, дающие автору основания для приведенного выше утверждения, следующие:

1) работа [10] принципиально отличается от описанных выше работ [4, 8, 9] и аналогичных им меньшей степенью абстракции и формализма изложения;

2) так как указанная работа в значительной части опирается на существующий пласт литературы в области методологии диссертационного исследования (в том числе указанные выше работы), она сохраняет присущую первоисточникам строгость изложения и диалектический подход к описанию взаимосвязи формальных положений исследования;

3) работа [10] диалектически сочетает теоретический характер и раскрытие фактически сложившихся (чаще всего – неформализованных) причинно-следственных связей, традиций и обычаев в научной среде, с которой должен познакомиться и – далее – влиться соискатель;

4) данная работа содержит значительное количество практических примеров, наглядно раскрывающих многообразие вариантов диссертационных работ как различной направленности (решение как научной, так и практической задачи), так и различных направлений исследований (теоретические и эмпирические исследования). Данное обстоятельство при наличии у соискателя когнитивных способностей, минимально необходимых для научной деятельности как таковой, позволяет использовать работу [10] фактически как пошаговое руководство по конвертации имеющегося (в общем случае – неструктурированного) багажа научных знаний соискателя в целостный и формально строгий научно-методический аппарат его кандидатской диссертации.

Практическая иллюстрация конверсии имеющихся научных результатов автора в формальные положения кандидатской диссертации

Ниже кратко приведена совокупность гипотез автора и результатов их рассмотрения, объединенная объектом исследования (услуги обработки вызовов абонентов операторами центров обработки вызовов) и предметом исследования (качество услуг обработки вызовов). Для наглядности материал приводится в хронологическом порядке появления (разработки), что позволит проиллюстрировать априорное отсутствие в нем причинно-следственных связей и «спуска» от общего к частному, требуемых для построения научного исследования путем формулирования и последующего описания (построения, обоснования, доказательства) системы формальных положений, далее в совокупности формирующих диссертационную работу.

1. Предложение и формализация интегрального критерия качества услуг центра обработки вызовов (далее – ЦОВ), построенного как сумма частных оценок качества услуг ЦОВ (далее – качества) с удельными весами, отражающими относительную значимость каждой из частных

оценок для заказчика услуг ЦОВ – см. работы автора [14, 15]. Предложение определенного эмпирическим путем набора частных оценок качества и правил их ранжирования.

2. Введение и обоснование гипотезы о некомпенсаторном характере предпочтений абонентов ЦОВ в отношении частных оценок качества и необходимости построения интегрального критерия качества некомпенсаторным методом. Введение гипотезы о целесообразности построения интегрального показателя качества методом некомпенсаторного порогового агрегирования – см. работу автора [16].
3. Анализ метода «Экономическая эффективность управления качеством» в отношениях заказчика и поставщика услуг ЦОВ. Построение модели взаимодействия заказчика и поставщика услуг в ходе оказания услуг для (для частного случая одномерной оценки (функции) качества. Введение понятий функций качества и ценности услуг. Обоснование построения функции ценности в виде степенной мультипликативной свертки. Доказательство максимальной эффективности для заказчика (в значении, определяемом работой [11]) линейной зависимости цены единицы услуги от значения функции качества – см. работы автора [17, 18].
4. Формализация выбора, определения границ, ранжирования частных оценок качества. Определение понятий необходимой, а также достаточной реальной цели заказчика. Построение интегрального критерия качества методом некомпенсаторного порогового агрегирования для адекватного (в значении, определяемом работой [11]) учета некомпенсаторных предпочтений как заказчика услуг (непосредственно), так и абонентов (опосредованно). Предложение и обоснование методики формирования интегрального критерия качества при неравных удельных весах частных оценок качества с помощью N-модели. Сравнительный анализ достижимости достаточной реальной цели заказчика при использовании интегрального критерия качества, построенного предлагаемым методом, а также традиционным методом взвешенной суммы критериев (частных оценок качества). Предложение и обоснование методики энтропийного анализа абсолютной, удельной и относительной потери информации при скаляризации вектора ранжированных частных оценок качества в интегральный критерий качества для обоих методов формирования интегрального критерия качества. Валидация теоретических результатов на эмпирических данных реального ЦОВ. Определение численных характеристик сравнения интегрального критерия качества, построенного различными методами. Обоснованный вывод о Парето-доминировании интегрального критерия качества, построенного методом некомпенсаторного порогового агрегирования над аналогичным критерием, построенным традиционным методом взвешенной суммы критериев – см. работу автора [19].

Из представленного выше кратного описания научного материала, разработанного автором самостоятельно, видно, что, несмотря на глубокую проработку отдельных элементов модели объекта исследования, диалектического пе-

рехода количества проделанной работы в новое качество ее оформления в функционально законченный научный труд не произошло. Для осуществления указанного диалектического перехода автором была проделана отдельная работа по анализу и последующему практическому применению методологии формирования научно-методического аппарата кандидатской диссертации, впервые в законченном виде сформулированной в работе С.И. Макаренко [10]. Ниже продемонстрированы полученные автором результаты в виде описания основных элементов своей диссертационной работы (с включением научных результатов, находящихся в разработке и еще не опубликованных на момент написания настоящей статьи).

Основные формальные положения диссертационной работы автора, сформированные по методологии С.И. Макаренко

Формирование противоречия в практике

Противоречие в практике - между необходимостью получения организацией, использующей ЦОВ, достоверной оценки оценки качества услуг ЦОВ с точки зрения клиентов ЦОВ и крайней ресурсозатратностью непосредственного получения такой оценки непосредственно от клиентов; между желательностью получения заказчиком как можно более качественных услуг и ростом их стоимости при росте качества.

Формирование противоречия в науке (или проблемной ситуации)

Существующий НМА анализа качества обслуживания вызовов ЦОВ не содержит моделей услуг ЦОВ, учитывающих взаимосвязь качества услуги, ее цены и прибыли поставщика, а также методик оценки и оптимизации качества услуг ЦОВ и их ценности для заказчика, учитывающих удовлетворенность звонящих обслуживанием, и некомпенсаторный характер предпочтений заказчика в отношении частных оценок качества ЦОВ.

Формулировка объекта, предмета и цели исследования

Объект исследования – услуги ЦОВ, предоставляемые поставщиком (оператором ЦОВ) заказчику.

Предмет исследования – эффективность информационного обмена абонентов и операторов ЦОВ.

Цель исследования – повышение эффективности информационного обмена абонентов и операторов ЦОВ за счет применения метода некомпенсаторного порогового агрегирования для формирования интегрального критерия качества информационного обмена.

Формулировка гипотезы исследования

Применение метода некомпенсаторного порогового агрегирования для формирования интегрального критерия качества информационного обмена абонентов и операторов ЦОВ в условиях взаимодействия заказчика и поставщика услуг ЦОВ методом «Экономическая эффективность управления качеством» позволяет повысить эффективность информационного обмена по сравнению со стандартной процедурой формирования указанного интегрального критерия методом взвешенной суммы критериев.

Обоснование ключевого показателя, который будет использоваться как критерий достижения цели исследования

Ключевой показатель - эффективность информационного обмена абонентов и операторов ЦОВ, определяемая заказчиком услуг ЦОВ как обобщающая функция, агрегирующая значения интегрального критерия качества информационного обмена, а также цены единицы услуг ЦОВ:

1) обоснование оценки эффективности информационного обмена (услуг) ЦОВ как обобщающей функции, агрегирующей значения интегрального критерия качества информационного обмена, а также цены единицы услуги;
2) обоснование функционального вида оценки эффективности услуг ЦОВ;
3) обоснование функциональной зависимости цены единицы услуг от значения интегрального критерия качества услуг;
4) формулировка необходимого и достаточного условия вида функции цены единицы услуги;
5) описание функции ценности в явном виде;
6) формирование критериев эффективности услуг для оптимального и квазиоптимального значения качества услуг.

Содержательная (вербальная) постановка научной задачи

Разработать элементы научно-методического аппарата (модель и методики) для достижения квазиоптимального значения эффективности информационного обмена абонентов и операторов ЦОВ в рамках взаимодействия заказчика и поставщика услуг ЦОВ методом «Экономическая эффективность управления качеством».

Декомпозиция научной задачи на взаимоувязанную совокупность частных научных и прикладных задач

Частная научная задача №1

Формализация и постановка задачи моделирования. Разработка и обоснование модели взаимодействия заказчика и поставщика услуг ЦОВ:

1) описание и обоснование применения метода «Экономическая эффективность управления качеством» для моделирования взаимоотношений заказчика и поставщика услуг ЦОВ;
2) построение модели жизненного цикла взаимодействия заказчика и поставщика услуг ЦОВ;
3) выделение формализуемого контура управления;
4) построение модели формализуемого контура управления;
5) описание и обоснование применения моделей поставщика услуг ЦОВ: абсолютно рациональный; ограниченно рациональный; нерациональный;
6) формирование сводки параметров модели формализуемого контура управления.

Частная научная задача № 2

Разработка методики формирования интегрального критерия ординального качества услуг ЦОВ как ординальной оценки качества методом некомпенсаторного порогового агрегирования:

1) обоснование применения метода некомпенсаторного порогового агрегирования для формирования интегрального критерия качества услуг;
2) описание методики формирования интегрального критерия качества услуг как ординальной оценки качества для случая равной значимости частных оценок качества услуг;
3) описание методики формирования интегрального критерия качества услуг как ординальной оценки качества с применением N-модели для случая неравной значимости частных оценок качества услуг;
4) выбор и обоснование критериев сравнения целевой и эталонной методики формирования интегрального критерия качества услуг ЦОВ как ординальной оценки качества;
5) разработка и обоснование метода энтропийного анализа потери информации при скаляризации вектора частных оценок качества услуг в интегральный критерий качества услуг и методики расчета абсолютной, удельной и относительной потери информации на основе разработанного метода;

Частная научная задача № 3

Разработка методики формирования интегрального критерия кардинального качества услуг ЦОВ методом некомпенсаторного порогового агрегирования как кардинальной оценки качества:

1) обоснование необходимости линеаризации маргинального качества для построения кардинальной оценки качества услуг ЦОВ в форме интегрального критерия качества услуг ЦОВ;
2) линеаризация маргинального качества интегрального критерия качества услуг ЦОВ, построенного методом некомпенсаторного порогового агрегирования, по методике реперных функций;

3) построение линеаризованного интегрального критерия качества как кардинальной оценки качества с учетом некомпенсаторных предпочтений заказчика
4) выбор и обоснование набора критериев сравнения целевой и эталонной методики формирования интегрального критерия качества услуг ЦОВ;

Частная прикладная задача № 1

Прикладные результаты исследования и проведение исследований ключевого показателя в интересах обоснования достижения цели работы:

1) выбор и обоснование состава и диапазонов значений частных оценок качества ЦОВ, методики ранжирования частных оценок качества и значений удельных весов частных оценок в рамках N-модели;
2) обоснование модельных условий, исходных данных для моделирования, исследуемых ситуаций.
3) валидация разработанной методики формирования интегрального критерия качества услуг ЦОВ как ординальной оценки качества по разработанному набору критериев;
4) исследование ключевого показателя без использования разработанных результатов исследования (с использованием известных решений);
5) исследование ключевого показателя с использованием разработанных научных и прикладных результатов исследования;
6) оценка достигаемого улучшения (выигрыша) по ключевому показателю. Вывод о достижении цели исследования;
7) оценка рамок применимости научных и прикладных результатов исследования.

Формирование рамок исследования

1. Все вызовы обрабатываются операторами ЦОВ без применения голосовых ассистентов;
2. Поток вызовов в ЦОВ квазистационарен;
3. Заказчик приобретает услуги ЦОВ у специализированной организации-поставщика;
4. Влияние внешних факторов на поставщика и (или) заказчика услуг ЦОВ не учитывается;
5. Срок действия договора на предоставление услуг ЦОВ квантуется на одинаковые отчетные периоды;
6. По окончании каждого отчетного периода производится оценка качества оказанных услуг и их оплата по цене, монотонно зависящей от качества услуг;
7. Предпочтения ЛПР зависимы по частным оценкам качества и носят некомпенсаторный характер;

8. Априорная информация о распределении частных оценок качества ЦОВ отсутствует.

Частные научные результаты

1. Методика формирования оценки эффективности информационного обмена абонентов и операторов ЦОВ и вида функции цены единицы услуги;
2. Модель формализуемого контура управления качеством услуг ЦОВ при взаимодействии заказчика услуг ЦОВ и поставщика услуг ЦОВ с различной степенью рациональности;
3. Методика формирования интегрального критерия ординального качества услуг ЦОВ методом некомпенсаторного порогового агрегирования, Парето–доминирующего над интегральным критерием качества, разработанным стандартным методом.
4. Методика формирования интегрального критерия кардинального качества услуг ЦОВ методом некомпенсаторного порогового агрегирования, обеспечивающая квазиоптимальное значение эффективности услуг ЦОВ.

Частный прикладной результат

5. Практические рекомендации по управлению услугами ЦОВ, а также иными услугами в рамках применяемого метода на базе разработанных методик.

Выводы

К основным выводам по итогам представленной работы автора относятся следующие:

1. Эффективная методология научной работы, подразумевающая конечным результатом защиту кандидатской диссертации, предполагает первоначальное формирование научно-методического аппарата диссертации как системы взаимоувязанных и связанных отношениями «причина – следствие»; «общее – частное» формальных положений исследования, и последующее раскрытие каждого из указанных положений в их диалектической взаимосвязи;

2. Обратный путь эмпирического научного поиска с последующей формализацией накопленного материала и результатов «задним числом» контрпродуктивен, так как требует значительно больших ресурсных затрат соискателя;

3. Публикация частных научных результатов в рецензируемых ВАК изданиях по мере их появления у соискателя с последующей попыткой компиляции текста диссертационной работы из совокупности публикаций контрпродуктивна, так как в соответствии с требованиями [5], публикации в рецензируемых ВАК изданиях подлежат основные научные результаты диссертации. В силу вышеуказанных пп. 1, 2 научные результаты должны первоначально формулироваться как ожидаемые и подтверждаться научными изысканиями соискателя. Обратный подход требует как минимум перекомпиляции фрагментов текста уже опубликованных статей в описание соответствующих разделов диссерта-

ции, а как максимум – недопуску к защите или отказу в присуждении ученой степени ввиду несоответствия научных результатов диссертации материалам опубликованных в рецензируемых ВАК изданиях статей соискателя;

4. Методическое пособие С.И. Макаренко [10] является эффективным инструментом методологической поддержки соискателя в работе по планированию и последующему самостоятельному творческому исполнению диссертационной работы, поскольку сочетает в себе как строгость и формальный стиль изложения, так и значительное количество практических примеров, иллюстрирующих доводимую до соискателя методологию. При этом безусловным достоинством как собственно работы [10], так и предлагаемой в ней методологии является отказ от превращения работы в пошаговое руководство для последовательного исполнения, что требует от соискателя определенных когнитивных способностей для постижения предлагаемой методологии, в целом необходимых и достаточных для занятия научной деятельностью как таковой.

Литература

1. Макаренко С. И. Научный ландшафт России – 2025 // Дзен [Электронный ресурс]. 12.12.2025. – URL: https://dzen.ru/a/aVuZkVifsUtYmBT7/ (дата обращения: 12.12.2025).
2. Макаренко С. И. Оформление и защита кандидатской диссертации по техническим наукам. Часть 2. – СПб.: Наукоемкие технологии, 2025. – 356 с.
3. Макаренко С. И. Почему аспиранты не защищаются? 5 основных причин // Дзен [Электронный ресурс]. 12.12.2025. – URL: https://dzen.ru/a/aGEua2uGpRcDn-6D. (дата обращения: 12.12.2025).
4. Бугаков И. А., Царьков А. Н. Диссертация на соискание ученой степени кандидата технических наук: система формальных признаков // Известия Института инженерной физики. 2016. № 3 (41). С. 84-95.
5. Винник Д. В. Объект-предметная казуистика и другие формы диссертационной схоластики // Философия науки. 2017. № 1 (72). С. 101-149. DOI: 10.15372/PS20170110.
6. Положение о порядке присуждения ученых степеней (в редакции от 25.01.2024). Постановление Правительства РФ от 24.09.2010 г. № 842. – М.: Правительство РФ, 2010.
7. Жданов И. Как написать диссертацию за 3 месяца [Электронный ресурс]. 12.12.2025. – URL: https://www.litres.ru/book/ivan-zhdanov-12782739/kak-napisat-dissertaciu-za-3-mesyaca-29829384/ (дата обращения: 12.12.2025).
8. Батько Б. М. Соискателю ученой степени. Практические рекомендации (от диссертации до аттестационного дела). – 4-е изд., переработанное, дополненное. – М.: СИП РИА, 2002. – 288 с.
9. Долгов А. И. Подготовка и написание диссертации. Методические указания. – Ростов-н/Д., 2002.
10. Макаренко С. И. Оформление и защита кандидатской диссертации по техническим наукам. Часть 1. – СПб.: Наукоемкие технологии, 2024. – 420 с.

11. Макаренко С. И. Справочник научных терминов и математических обозначений. – СПб.: Наукоемкие технологии, 2025. – 348 с.

12. Воронцова Н. С. Как написать диссертацию с «0» за 3 месяца. – М.: 1000 бестселлеров, 2023. – 226 с.

13. Райзберг Б. А. Диссертация и ученая степень: Пособие для соискателей. – 9-е изд., доп. и испр. – М.: ИНФРА-М, 2010. – 240 с.

14. Касаткин Ф. Ю. Актуальность интегральной оценки качества обслуживания входящих вызовов в контакт-центре // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VII Международная научно-техническая и научно-методическая конференция; сб. науч. ст. в 4 томах. Том 4. – СПб.: СПбГУТ, 2023. С. 81-87.

15. Касаткин Ф. Ю. Интегральный критерий качества обслуживания входящих вызовов в контакт-центре // Инновационные исследования: опыт, проблемы внедрения результатов и пути решения: сборник статей Международной научно–практической конференции, Тюмень, 17 февраля 2025 года. – Уфа: ООО "ОМЕГА САЙНС", 2025. – С. 22-27.

16. Касаткин Ф. Ю. Некомпенсаторное агрегирование для интегральной оценки качества обслуживания входящих вызовов в контакт-центре // Моделирование современных информационных систем в условиях цифровой трансформации: электронный сборник трудов II Международной научно-практической конференции, Санкт-Петербург, 12–13 декабря 2024 г. Под ред. Е. А. Благовещенской, Л. М. Божко, Ю. А. Дорофеевой, С. Г. Ермакова. – СПб.: ПГУПС, 2025. – С. 84–88.

17. Касаткин Ф. Ю. Об эффективном виде функции качества во взаимоотношениях заказчика и поставщика продукции военного назначения // Системы управления, связи и безопасности. 2025. № 3. С. 232–268. DOI: 10.24412/2410-9916-2025-3-232-268.

18. Касаткин Ф. Ю. Об эффективном виде функции качества услуг центра обработки вызовов // Современные научные исследования: теория, методология, практика. Сборник научных трудов по материалам X Международной научно-практической конференции (г.-к. Анапа, 16 сентября 2025 г.). – Анапа: НИЦ ЭСП в ЮФО, 2025. – 37 с.

19. Касаткин Ф. Ю. Некомпенсаторная интегральная оценка качества работы центров обработки вызовов // Системы управления, связи и безопасности. 2025. № 4. С. 200-243. DOI: 10.24412/2410-9916-2025-4 200-243.

Информация об авторе

Касаткин Феликс Юрьевич – соискатель ученой степени кандидата технических наук. Начальник ГБУЗ Запорожской области «Медицинский информационно-аналитический центр». Область научных интересов: теория принятия решений; теория важности критериев; теория управления качеством. E-mail: fkasatkin@yandex.ru

Адрес: 272304, Россия, Запорожская обл., г. Мелитополь, ул. Фрунзе, д. 69.

УДК 004.056

Актуальность разработки методического аппарата для оценки эффективности тестирования на проникновение с использованием искусственного интеллекта применительно к судовым компьютерным системам

Позолотин С. И.

В тезисе обоснована актуальность разработки методического аппарата оценки эффективности тестирования на проникновение с использованием искусственного интеллекта применительно к судовым компьютерным системам. На основе анализа современного состояния информационной безопасности, усложнения компьютерных, телекоммуникационных и судовых систем, а также роста числа и сложности компьютерных атак показано, что существующие подходы к оценке защищённости и тестированию на проникновение не обеспечивают формализованного и сопоставимого оценивания результатов тестирования и решений, принимаемых в ходе его проведения.

Ключевые слова: *информационная безопасность, кибербезопасность, тестирование на проникновение, искусственный интеллект, поддержка принятия решений, судовые системы управления.*

Современное состояние информационной безопасности (ИБ) в 2026 году характеризуется высокой степенью взаимосвязанности технических решений, управленческих практик и правового регулирования. В Российской Федерации нормативное закрепление категории критической информационной инфраструктуры (КИИ) и обязанностей по обеспечению её безопасности обусловило повышение ответственности субъектов КИИ, а также усилила потребность в аудите защищённости [1]. В контексте данной работы, защищённость компьютерной системы — состояние системы, при котором обеспечивается требуемый уровень противодействия компьютерным атакам и сохраняются её значимые свойства безопасности. В Европейском союзе аналогичная тенденция выражена в принятии Директивы (ЕС) 2022/2555 (NIS2 — Директива о мерах по обеспечению высокого общего уровня кибербезопасности на территории Союза) [2], действие которой распространено, в том числе, на транспорт, цифровую инфраструктуру и электронные коммуникации [2]. В этих условиях оценка фактического уровня защищённости становится обязательным элементом обеспечения безопасности значимых объектов КИИ.

В указанных условиях тестирование на проникновение сохраняет значение одного из основных инструментов экспериментальной проверки защищённости, поскольку позволяет моделировать действия нарушителя и выявлять уязвимости, ошибки конфигурации и иные недостатки, не выявляемые в рамках формальных процедур контроля соответствия [3]. Вместе с тем ключевой науч-

Статья (тезис) опубликована в сборнике докладов конференции:
I семинар научной школы профессора С. И. Макаренко. Сборник тезисов докладов конференции. г. Санкт-Петербург, 20-21 декабря 2025 года. – СПб.: Наукоемкие технологии, 2026.

ный дефицит связан не с отсутствием самой практики тестирования на проникновение, а с недостаточной проработанностью методического аппарата оценки эффективности[7] тестирования и обоснованности принимаемых решений, особенно при переходе к сценариям с использованием искусственного интеллекта (ИИ) и их применении в судовых компьютерных системах.

Следовательно, актуальность рассматриваемого направления определяется не только ростом угроз и усложнением инфраструктур, но и наличием научно-методического разрыва: практическая потребность в регулярной экспериментальной проверке защищённости возрастает, тогда как научно обоснованные и формализованные[8] критерии оценки эффективности тестирования на проникновение, включая показатели полноты, точности, достоверности, воспроизводимости и сопоставимости результатов, а также учёт ошибок первого и второго рода, остаются фрагментарными и недостаточно разработанными для различных объектов и условий применения [4].

Актуальность исследования определяется также ростом структурной и организационной сложности компьютерных систем, вследствие чего классические периметры защиты утрачивают определяющее значение, а множество компонентов, интерфейсов, сервисов и межсистемных связей, уязвимости которых могут быть использованы при реализации атак, увеличивается за счёт цепочек поставок, многооблачных сред и взаимосвязанных информационных и технологических систем. В отчёте «Cost of a Data Breach Report 2025» [5], подготовленном компанией IBM, отмечается, что инциденты в средах, где данные распределены между публичными и частными облаками, а также локальной инфраструктурой, характеризуются более высокой стоимостью и большей длительностью выявления инцидента и предотвращения ущерба, что свидетельствует о прямой связи архитектурной сложности с усложнением процессов защиты и реагирования [5].

Особую значимость рассматриваемая задача приобретает применительно к судовым компьютерным системам, в которых ИБ непосредственно связана с безопасностью эксплуатации, экологическими рисками и непрерывностью технологических процессов. Резолюция MSC.428(98) Международной морской организации [7] закрепила необходимость учитывать риски компьютерных атак в системах управления безопасностью судоходных компаний и при обеспечении безопасности мореплавания [7]. Одновременно отраслевые рекомендации по кибербезопасности на борту судов фиксируют увеличение степени цифровой

---

[7] В рамках настоящего тезиса эффективность тестирования на проникновение понимается как свойство целенаправленного процесса, характеризующее степень соответствия полученных результатов цели тестирования при заданных ограничениях по времени, ресурсам и допустимому уровню ошибок.

[8] Формализованная оценка — это оценка, выполняемая на основе явно заданных показателей, критериев, правил расчёта и правил интерпретации результата.

интеграции судовых систем и расширение их сетевого взаимодействия, что сопровождается ростом уязвимости к компьютерным атакам, включая воздействие на оборудование, процессы и подготовку персонала [8]. Дополнительным эмпирическим подтверждением служат материалы международной классификационной и сертификационной компании DNV (Det Norske Veritas) [9], в которых отмечен существенный рост доли организаций морской отрасли, сообщивших о кибератаках за последний год, что указывает на практическую значимость рассматриваемой тематики для судовых компьютерных систем [9].

Рост сложности атак проявляется в ускорении эксплуатации уязвимостей, профессионализации преступных сообществ и расширении воздействия на цепочки поставок и зависимые инфраструктуры. В отчёте ENISA Threat Landscape 2025 [10], охватывающем период с июля 2024 года по июнь 2025 года, отмечаются высокая интенсивность угроз, быстрое превращение выявленных уязвимостей в средства реализации атак и усложнение установления источника и исполнителей атак (атрибуции нарушителя); при этом атаки с использованием программ-вымогателей по-прежнему сохраняют существенную роль [10]. Кроме того, фиксируются объединение различных сценариев атак, автоматизация и индустриализация их реализации, а также усиление роли ИИ как средства ускорения подготовки и реализации компьютерных атак, что повышает значимость методик и процедур оценки результатов защитных проверок в условиях действующей атаки [10].

Динамика угроз подтверждается и исследованиями, посвящёнными реагированию на вторжения. Данные M-Trends 2025 [11] дополнительно подтверждают сокращение временного интервала между проникновением нарушителя в систему и нанесением ущерба, что повышает значимость предварительных проверок защищённости [11].

Обобщая вышеизложенное, можно сделать вывод, что рост темпа атак и их индустриализация усиливают потребность в методически строгой оценке эффективности тестирования на проникновение. При отсутствии формализованных критериев невозможно надёжно сопоставлять результаты различных проверок во времени, оценивать влияние изменений архитектуры и средств защиты на уровень защищённости системы, а также обосновывать управленческие решения по приоритизации мер обеспечения безопасности в КИИ [10, 11].

Дополнительным фактором, усложняющим решение указанной научно-методической задачи, является развитие ИИ, включая большие языковые модели (LLM, Large Language Model), и переход к частично автономным сценариям их применения в кибербезопасности. В докладе [12] отмечается, что ИИ существенно изменяет способы реализации компьютерных атак и организации защиты в цифровой среде[9]; при этом большинство опрошенных руководителей

[9] В рамках настоящего тезиса термины «киберсреда» и «цифровая среда» используются как близкие по смыслу и обозначают совокупность информационных систем, сетей, программно-аппаратных средств и цифровых сервисов, в

рассматривает его как один из ключевых факторов изменения уровня рисков, связанных с компьютерными атаками, в ближайшей перспективе. В том же источнике зафиксирован рост распространённости процедур оценки безопасности инструментов ИИ перед внедрением, однако одновременно сохраняется значительная доля организаций, не имеющих таких процедур, а среди барьеров внедрения называются необходимость человеческой проверки и неопределённость рисков. Это позволяет сделать вывод о том, что качество решений, формируемых системами ИИ, должно быть измеримым и управляемым, иначе автономизация будет увеличивать вероятность ошибок, затрагивающих функционирование системы в целом [12].

Государственные оценки угроз также подтверждают практическую значимость рассматриваемой темы. В докладе Национального центра кибербезопасности Великобритании об ожидаемом влиянии ИИ на киберугрозы до 2027 года [13] отмечается, что нарушители уже используют ИИ для повышения эффективности существующих тактик, включая разведку целей, исследование уязвимостей, разработку средств эксплуатации уязвимостей, социальную инженерию и обработку похищенных данных [13]. Одновременно подчёркивается, что широкое внедрение систем ИИ в технологическую базу, в том числе на объектах критической инфраструктуры, приводит к увеличению числа компонентов, интерфейсов и сервисов, уязвимости которых могут быть использованы при реализации атак [13].

В этих условиях ИИ начинает использоваться непосредственно в тестировании на проникновение, преобразуя его из практики, основанной преимущественно на деятельности специалиста, в гибридный процесс, в котором отдельные решения формируются моделью и реализуются программным агентом. Научные результаты по применению LLM в тестировании на проникновение показывают двойственный эффект. В работе [14] показано, что LLM способны эффективно решать отдельные подзадачи, в частности интерпретировать вывод инструментов и предлагать последующие шаги, однако при усложнении цели и сценария эксплуатации качество получаемых результатов становится неоднозначным [14]. В более поздних исследованиях вводятся показатели покрытия уязвимостей и числа успешно выполненных подзадач, однако использование несопоставимых показателей и различных испытательных сред указывает на отсутствие общепринятой научно обоснованной системы оценки эффективности тестирования на проникновение с использованием ИИ [15].

Ключевая причина актуальности рассматриваемой научной задачи состоит в том, что для программных агентов, использующих ИИ, существенен не только полученный результат, но и способ его достижения: с какой точностью, скоростью и устойчивостью к искажению исходных данных и условий функционирования, а также с каким уровнем управляемости рисков ошибок. В доку-

---

пределах которых осуществляются обработка, хранение и передача информации, а также реализуются компьютерные атаки и меры защиты.

ментах Национального института стандартов и технологий США по управлению рисками ИИ [16] указано, что доверенные системы ИИ должны быть корректными, надёжными, безопасными, устойчивыми, подотчётными и прозрачными, а выбор показателей и пороговых значений требует содержательного экспертного суждения с учётом условий применения [16]. Для генеративных моделей отдельно выделяются риски ошибочных выводов, смещений и негативных последствий автоматизированных решений, что в критических условиях делает задачу оценки качества решений обязательным элементом обеспечения безопасности [17].

Анализ существующих подходов к тестированию на проникновение и оценке защищённости показывает, что международные методологии исторически ориентированы преимущественно на стандартизацию этапов работ и повышение повторяемости процедур. В документе NIST SP 800-115 [3] представлены рекомендации по планированию и проведению технических проверок, а также описаны достоинства и ограничения отдельных техник; вместе с тем данный документ прямо позиционируется как обзор ключевых элементов, а не как исчерпывающая программа тестирования [3]. В результате он задаёт общую последовательность процедур, но не формирует строгой системы количественных критериев эффективности тестирования на проникновение, пригодной для сопоставления результатов между организациями, типами систем и уровнями критичности [3]. Дополнительным ограничением является то, что указанный документ опубликован в 2008 году и, следовательно, не учитывает специфику современных сценариев применения ИИ [3,6].

Сходную процессную направленность демонстрируют и иные широко применяемые стандарты и руководства: PTES фиксирует фазы и типовую структуру работ [18], а OSSTMM ориентирует оценивание на анализ каналов взаимодействия и множества элементов системы, потенциально доступных для реализации атак [19]. Однако ориентация преимущественно на порядок выполнения работ при отсутствии общепринятой системы показателей, учитывающей свойства сложных распределённых систем и специфику критических областей применения, приводит к тому, что эффективность тестирования на проникновение нередко оценивается по косвенным признакам, таким как количество выявленных уязвимостей, субъективная оценка глубины проверки или степень соответствия отчёта ожиданиям заказчика. Подобный подход недостаточен для научно обоснованного управления риском [18–20].

Указанная научная задача дополнительно усложняется при переходе к автоматизированному тестированию на проникновение с использованием ИИ. В работе [21] показано, что само понятие автоматизированного тестирования на проникновение трактуется неоднозначно, а значительная часть исследований ограничивается этапом планирования атаки, не охватывая изменение состояния системы и процессы принятия решений [21]. Тем самым фиксируется методический разрыв между практической потребностью в полномасштабной автоматизации и современным состоянием научного аппарата.

В отечественной науке задача оценки защищённости и контроля состояния ИБ рассматривается в контексте аудита, моделирования атак, мониторинга и построения государственных и корпоративных систем реагирования. В работах Петренко С. А. и Ступина Д. Д. [22] показано, что раннее предупреждение о компьютерном нападении представляет собой комплексную научно-техническую задачу, непосредственно связанную с развитием государственной системы реагирования и повышением требований к устойчивому функционированию объектов КИИ [22]. В работах Котенко И. В. и Саенко И. Б. показаны возможности применения систем управления информацией и событиями безопасности, а также средств моделирования сетевых атак для защиты критически важных инфраструктур. Одновременно обоснована необходимость формализованного анализа событий безопасности [23].

При всей значимости указанного множества работ для развития отечественной школы ИБ их основной акцент сделан на организационно-техническом построении систем мониторинга, классификации мероприятий аудита и архитектурных решениях для инфраструктур реагирования. В работе Макаренко С. И. [4] отмечены противоречивость терминологии, неоднозначность существующих классификаций и недостаточное внимание к системной классификации мероприятий и экспериментальным исследованиям реальных систем, что свидетельствует о недостаточной разработанности методического аппарата контроля и проверки защищённости даже на уровне классического аудита [4]. В работе Макаренко С. И. и Смирнова Г. Е. [24] показано, что развитие идей экспериментального аудита через тестовые информационно-технические воздействия выводит на новый уровень задачу оценки качества тестирования, особенно при переходе к системам ИИ - изменяется сама природа принятия решений, вследствие чего возникает необходимость оценивать не только конечные результаты, но и качество логических выводов и действий, особенно в условиях неполноты информации о состоянии исследуемой системы и повышенного риска воздействия на её критические элементы [24].

Объектом исследования являются процессы тестирования на проникновение компьютерных систем с использованием ИИ при экспериментальной оценке защищённости судовых компьютерных систем. Предметом исследования является эффективность указанных процессов, рассматриваемая через показатели полноты, достоверности, воспроизводимости, сопоставимости и ресурсоёмкости результатов, а также через показатели обоснованности решений, принимаемых в ходе тестирования. Научное противоречие заключается в том, что при возрастающей практической потребности в формализованной, воспроизводимой и сопоставимой оценке эффективности тестирования на проникновение с использованием ИИ современный научно-методический аппарат не обеспечивает достаточного обоснования таких оценок. Цель исследования состоит в повышении эффективности тестирования на проникновение с использованием ИИ применительно к судовым компьютерным системам путём разработки соответствующего методического аппарата. Для достижения поставлен-

ной цели необходимо решить задачи анализа современного состояния угроз и существующих подходов к оценке защищённости; выявления ограничений классических и интеллектуализированных методик тестирования на проникновение; обоснования системы критериев и показателей оценки эффективности тестирования и обоснованности принимаемых решений ИИ; определения особенностей применения указанных положений применительно к компьютерным системам.

Литература

1. О безопасности критической информационной инфраструктуры Российской Федерации. Федеральный закон РФ от 26.07.2017 № 187-ФЗ // Официальный интернет-портал правовой информации [Электронный ресурс]. – URL: https://normativ.kontur.ru/document?moduleId=1&documentId=501334 (дата обращения: 29.03.2026).

2. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) // EUR-Lex. Official Journal of the European Union [Электронный ресурс]. 27.12.2022. – URL: https://digital-strategy.ec.europa.eu/en/policies/nis2-directive (дата обращения: 29.03.2026).

3. Scarfone K. A., Souppaya M. P., Cody A., Orebaugh A. Technical Guide to Information Security Testing and Assessment. NIST Special Publication 800-115 // Gaithersburg: National Institute of Standards and Technology [Электронный ресурс]. 2008. – URL: https://csrc.nist.gov/pubs/sp/800/115/final (дата обращения: 29.03.2026).

4. Макаренко С. И. Аудит информационной безопасности: основные этапы, концептуальные основы, классификация мероприятий // Системы управления, связи и безопасности. 2018. № 1. С. 1–29. URL: http://sccs.intelgr.com/archive/2018-01/01-Makarenko.pdf (дата обращения: 29.03.2026).

5. Cost of a Data Breach Report 2025 [Электронный ресурс]. – Armonk: IBM Corporation, 2025. – URL: https://www.ibm.com/reports/data-breach (дата обращения: 29.03.2026).

6. Assessing Security and Privacy Controls in Information Systems and Organizations. NIST Special Publication 800-53A Rev. 5 – Gaithersburg: National Institute of Standards and Technology [Электронный ресурс]. 2022. – URL: https://csrc.nist.gov/pubs/sp/800/53/a/r5/final (дата обращения: 29.03.2026).

7. Resolution MSC.428(98): Maritime Cyber Risk Management in Safety Management Systems // London: International Maritime Organization [Электронный ресурс]. 2017. – URL: https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/Resolution%20MSC.428%2898%29.pdf (дата обращения: 29.03.2026).

8. The Guidelines on Cyber Security On Board Ships. Version 5 // The International Association of Dry Cargo Shipowners [Электронный ресурс]. 2024. – URL: https://www.intercargo.org/guidelines-cyber-security-onboard-ships/ (дата обращения: 29.03.2026).

9. Tackling a growing cybersecurity threat in an increasingly connected industry // DNV [Электронный ресурс]. 12.12.2024. – URL: https://www.dnv.com/expert-story/maritime-impact/tackling-a-growing-cybersecurity-threat-in-an-increasingly-connected-industry/ (дата обращения: 29.03.2026).

10. ENISA Threat Landscape 2025 // The European Union Agency for Cybersecurity [Электронный ресурс]. 2025. – URL: https://www.enisa.europa.eu/sites/default/files/2025-11/ENISA%20Threat%20Landscape%202025.pdf (дата обращения: 29.03.2026).

11. M-Trends 2025: Data, Insights, and Recommendations From the Frontlines // Google Cloud Blog [Электронный ресурс]. 23.04.2025. – URL: https://services.google.com/fh/files/misc/m-trends-2025-en.pdf (дата обращения: 29.03.2026).

12. Global Cybersecurity Outlook 2026 – Geneva: World Economic Forum [Электронный ресурс]. 2026. – URL: https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2026.pdf (дата обращения: 29.03.2026).

13. Impact of AI on cyber threat from now to 2027 // National Cyber Security Centre [Электронный ресурс]. 07.05.2025. – URL: https://www.ncsc.gov.uk/report/impact-ai-cyber-threat-now-2027 (дата обращения: 29.03.2026).

14. Deng G., Liu Y., Mayoral-Vilches V., Liu P., Li Y., Xu Y., Zhang T., Liu Y., Pinzger M., Rass S. PentestGPT: Evaluating and Harnessing Large Language Models for Automated Penetration Testing // Proceedings of the 33rd USENIX Security Symposium. 2024. P. 847-864. – URL: https://www.usenix.org/system/files/usenixsecurity24-deng.pdf (дата обращения: 29.03.2026).

15. Ginige Y., Niroshan A., Jain S., Seneviratne S. AutoPentester: An LLM Agent-based Framework for Automated Pentesting // arXiv [Электронный ресурс]. 2025. – URL: https://arxiv.org/html/2510.05605v1 (дата обращения: 29.03.2026).

16. Tabassi E. Artificial Intelligence Risk Management Framework (AI RMF 1.0). NIST AI 100-1 // Gaithersburg: National Institute of Standards and Technology [Электронный ресурс]. 2023. – URL: https://nvlpubs.nist.gov/nistpubs/ai/nist.ai.100-1.pdf (дата обращения: 29.03.2026).

17. Autio C., Schwartz R., Dunietz J., Jain S., Stanley M., Tabassi E., Hall P., Roberts K. Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile. NIST AI 600-1 – Gaithersburg: National Institute of Standards and Technology [Электронный ресурс]. 2024. – URL:

https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.600-1.pdf (дата обращения: 29.03.2026).

18. The Penetration Testing Execution Standard // PTES Technical Guidelines [Электронный ресурс]. – URL: http://www.pentest-standard.org/index.php/Main_Page (дата обращения: 29.03.2026).

19. Herzog P. Open Source Security Testing Methodology Manual. OSSTMM 3.0 // ISECOM [Электронный ресурс]. 2010. – URL: https://www.isecom.org/OSSTMM.3.pdf (дата обращения: 29.03.2026).

20. OWASP Web Security Testing Guide. Version 4.2 // OWASP Foundation [Электронный ресурс]. 2020. – URL: https://owasp.org/www-project-web-security-testing-guide/stable/3-The_OWASP_Testing_Framework/1-Penetration_Testing_Methodologies (дата обращения: 29.03.2026).

21. Skandylas C., Asplund M. Automated penetration testing: Formalization and realization // Computers & Security. 2025. Vol. 155. Art. 104454. DOI: 10.1016/j.cose.2025.104454.

22. Петренко С. А., Ступин Д. Д. Национальная система раннего предупреждения о компьютерном нападении. Монография. – СПб.: Афина, 2017. – 439 с.

23. Котенко И. В., Саенко И. Б., Полубелова О. В., Чечулин А. А. Применение технологии управления информацией и событиями безопасности для защиты информации в критически важных инфраструктурах // Труды СПИИРАН. 2012. № 1 (20). С. 27-56. DOI: 10.15622/sp.20.2

24. Макаренко С. И., Смирнов Г. Е. Методика обоснования тестовых информационно-технических воздействий, обеспечивающих рациональную полноту аудита защищенности объекта критической информационной инфраструктуры // Вопросы кибербезопасности. 2021. № 6 (46). С. 12-25. DOI: 10.21681/2311-3456-2021-6-12-25

Информация об авторе

Позолотин Святослав Игоревич – соискатель ученой степени кандидата технических наук. Государственный университет морского и речного флота имени адмирала С. О. Макарова. Область научных интересов: кибербезопасность критической информационной инфраструктуры, аудит защищенности морских систем управления и е-навигации, автоматизированное тестирование на проникновение с использованием ИИ. E-mail: pozolotin-cvat@yandex.ru

Адрес: 195272, Санкт-Петербург, Богословская улица, 6. корп. 2.