МИНОБРНАУКИ РОССИИ
Федеральное государственное автономное образовательное учреждение
высшего образования «Санкт-Петербургский государственный
электротехнический университет
«ЛЭТИ» им. В.И. Ульянова (Ленина)»

Государственная корпорация по содействию разработке, производству
и экспорту высокотехнологичной промышленной продукции «Ростех»

Публичное акционерное общество «Информационные телекоммуникационные
технологии» (ПАО «Интелтех»)

Акционерное общество «Научно-производственное предприятие «Сигнал»
(АО «НПП «Сигнал»)

ОБРАЗОВАТЕЛЬНО-ПРОИЗВОДСТВЕННЫЙ КЛАСТЕР (НАВИГАЦИЯ, КОММУНИКАЦИИ, БЕЗОПАСНОСТЬ)

Сборник докладов Первой межведомственной
научно-технической конференции

г. Санкт-Петербург, 20–21 августа 2026 года

Санкт-Петербург
Издательство СПбГЭТУ «ЛЭТИ»
2026

УДК 621.39:004(082)
ББК 32я43
О-23

Члены программного комитета:
А. И. Яшин, д.т.н., профессор, заслуженный деятель науки Российской Федерации, ПАО «Интелтех»;
В. А. Сарычев, д.т.н., профессор, член Президиума Петропавловской Академии наук и искусств, АО «НПП «Радар ммс»;
П. А. Будко, д.т.н., профессор, почётный работник высшего профессионального образования Российской Федерации, ПАО «Интелтех»;
С. И. Макаренко, д.т.н., профессор, член специального экспертного совета ВАК при Минобрнауки Российской Федерации, СПбГЭТУ «ЛЭТИ» им. В. И. Ульянова (Ленина);
М. А. Ходаковский, советник генерального директора, АО «НПП «Сигнал»;
А. Д. Шульженко, к.т.н., СПбГЭТУ «ЛЭТИ» им. В. И. Ульянова (Ленина);
Е. С. Новикова, к.т.н., доцент, СПбГЭТУ «ЛЭТИ» им. В. И. Ульянова (Ленина)

Рецензенты:
С. И. Макаренко, д.т.н., профессор, член специального экспертного совета ВАК при Минобрнауки Российской Федерации, СПбГЭТУ «ЛЭТИ» им. В. И. Ульянова (Ленина);
П. А. Будко, д.т.н., профессор, почётный работник высшего профессионального образования Российской Федерации, ПАО «Интелтех»;
А. И. Яшин, д.т.н., профессор, заслуженный деятель науки Российской Федерации, ПАО «Интелтех»

О-23 Образовательно-производственный кластер (навигация, коммуникации, безопасность): сборник докладов Первой межведомственной научно-технической конференции; г. Санкт-Петербург, 20–21 августа 2026 года. – СПб.: Изд-во СПбГЭТУ «ЛЭТИ», 2026. – 436 с.

Сборник материалов Всероссийской научно-технической конференции «Образовательно-производственный кластер (навигация, коммуникации, безопасность)» (ОПК-2026) предназначен для преподавателей, аспирантов и студентов вузов, а также научных работников предприятий промышленности, включившихся в пилотный проект по внедрению производственной аспирантуры в систему государственной аттестации научных кадров высшей квалификации, реализуемый Минобрнауки России совместно с ГК «Ростех» с 2025/26 по 2028/29 учебные годы.

В издание вошли доклады аспирантов и соискателей учёных степеней как классической формы подготовки, так и участников пилотного проекта производственной аспирантуры — нового формата кооперации фундаментальной науки вузов и НИИ с прикладной наукой предприятий промышленности. Статьи представлены на площадке СПбГЭТУ «ЛЭТИ», ПАО «Интелтех» и АО «НПП «Сигнал» и объединены научной дискуссией по пяти секциям конференции:

Секция 1. Системы, сети и устройства телекоммуникаций;

Секция 2. Робототехника и искусственный интеллект;

Секция 3. Системы управления и навигации;

Секция 4. Безопасность сложных организационно-технических систем;

Секция 5. Подготовка кадров для IT-отрасли.

Материалы публикуются в авторской редакции. Авторы несут ответственность за подбор, точность приведённых цитат, статистических данных и иных сведений.

Информационные партнёры конференции ОПК-2026 — АНО «Корпоративная сетевая академия» (Техническая школа Академии Ростеха) и научно-технические журналы «Системы управления, связи и безопасности» и «Means of Communication Equipment» («Техника средств связи»).

ISBN 978-5-7629-3706-1
© СПбГЭТУ «ЛЭТИ», 2026

Уважаемые коллеги, участники и гости
Всероссийской межведомственной научно-технической конференции
«Образовательно-производственный кластер» (ОПК-2026)!

Искренне рад приветствовать всех в стенах Санкт-Петербургского государственного электротехнического университета «ЛЭТИ» им. В. И. Ульянова (Ленина), отмечающего в этом году 140-летие со дня своего основания и всегда находящегося в авангарде высших учебных заведений, занимающих ведущие позиции в деле подготовки передовых инженерных кадров и проведения научных разработок для технического лидерства страны. Сохранить лидерские позиции университету позволяет умение выступать в качестве интеграционной площадки и объединять академические компетенции и промышленные подходы в деле решения общих задач от обучения студентов до развития перспективных технологий.

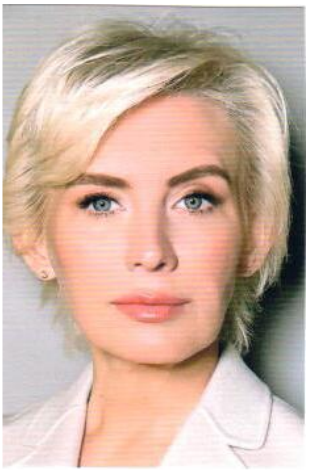
Одна из главных задач, которая стоит сегодня перед университетами и предприятиями реального сектора экономики, заключается в поиске форматов равноправного и долговременного партнерства, позволяющего решать задачи для достижения стратегических целей научно-технологического развития страны. Именно на стыке фундаментальной науки, академических подходов и практического опыта индустриальных партнеров рождаются решения, определяющие технологическое будущее страны, в первую очередь в области телекоммуникаций, робототехники, искусственного интеллекта, систем управления и информационной безопасности. Тематика конференции, посвященная поиску таких форм партнерства и созданию единого научно-образовательного пространства в формате образовательно-производственного кластера, является безусловно актуальной и своевременной.

Убежден, что такой формат отвечает интересам организаторов и участников конференции, станет действенным механизмом интеграции образования, науки и производства, а обмен опытом между преподавателями, учеными и инженерами-практикантами придаст новый импульс совместным исследованиям и подготовке специалистов, востребованных промышленностью сегодня.

Желаю участникам конференции плодотворной работы, интересных дискуссий, новых профессиональных контактов и научных результатов, которые найдут практическое применение в промышленности.

Уверен, что конференция ОПК станет доброй традицией и площадкой для долгосрочного сотрудничества ВУЗа и наших индустриальных партнеров.

Ректор СПбГЭТУ
«ЛЭТИ» В. Н. Шелудько



От имени Публичного акционерного общества «Информационные телекоммуникационные технологии», а также ведущих разработчиков телекоммуникационного оборудования России приветствую Вас и гостей данного научно-методического мероприятия, направленного на формирование творческой среды для симбиозного взаимодействия фундаментальной и прикладной науки в достижении инновационно значимых прикладных результатов. Мир стремительно меняется благодаря развитию и внедрению в повседневную жизнь высоких технологий. Цифровая трансформация общества и промышленности, многочисленные гаджеты, нейро-интерфейсы и все более интеллектуальные роботы, интерактивное обучение и smart-устройства не только активно внедряются, но и поднимают проблемы подготовки нового поколения IT-специалистов и IT-ученых по рациональному, безопасному использованию современных технологий.

Несомненно, задачи обеспечения конкурентных преимуществ и развития российской экономики должны решаться квалифицированными специалистами, в том числе, и в области информационных технологий совместно с ведущими производителями аппаратного и программного обеспечения. Популярность направления информационных технологий среди молодежи выглядит вполне естественно на фоне ее стремления к инженерным профессиям будущего.

Уверена, что конференция пройдет в конструктивном ключе, позволит вузовской науке и инженерно-конструкторскому составу предприятий промышленности обменяться накопленным опытом, будет способствовать деловому сотрудничеству и укреплению контактов молодых ученых образовательно-производственного кластера.

Надеюсь, что знаковое для вузовской и промышленной науки мероприятие перерастет в ежегодную тематическую площадку построения для нашей молодежи фундамента профессиональной карьеры!

Генеральный директор
ПАО «Интелтех» А. А. Лотонина

Приветствую вас от имени коллектива АО «НПП «Сигнал» — предприятия, для которого качественные разработка и производство технических средств напрямую зависят от притока молодых, хорошо подготовленных инженерных кадров. Конференция ОПК-2026 — это площадка, где вузовская наука встретится с реальными задачами промышленности. Вопросы подготовки кадров для нас не абстрактная тема, а повседневная необходимость: с каждым годом растут требования к защищенности и надежности разрабатываемых решений, и ответить на эти вызовы можно только совместными усилиями науки, образования и производства.

Уверен, что диалог между преподавателями кафедры информационной безопасности ЛЭТИ, специалистами других предприятий, принимающих участие в конференции, а также главными конструкторами нашего предприятия позволит найти решения проблемных вопросов, выработать практические подходы к подготовке специалистов, способных решать задачи отрасли уже с первых лет работы, и укрепит связи между кластерными партнерами.

Желаю участникам конференции содержательных докладов, живой дискуссии на круглом столе и уверен, что результаты этой встречи станут основой для новых совместных проектов.

Генеральный директор
АО «НПП «Сигнал» А. В. Балицкий

Предсекционные индивидуальные статьи членов организационного комитета

УДК 007.52

Технологии инфокоммуникаций, робототехники и искусственного интеллекта, как основа будущих этапов эволюции цифрового мира, создаваемого человечеством

Яшин А. И.

ПАО «Интелтех», г. Санкт-Петербург, Россия

Аннотация: *В статье исследуется эволюция цифрового мира и его трансформация в киберфизическую среду, где фундаментальную роль играют инфокоммуникационные технологии, робототехника и искусственный интеллект. Особое внимание уделяется революционному потенциалу сетей шестого поколения (6G), обеспечивающих взаимодействие технических систем на микроуровне и выступающих инфраструктурной основой для создания глобальной распределенной системы искусственного интеллекта. Подчеркивается критическая важность нативной интеграции искусственного интеллекта в радиосредства и необходимость перехода к архитектуре многостороннего доверия для гарантирования конфиденциальности и безопасности данных. Материалы статьи направлены на актуализацию перспективных научно-технических задач и привлечение молодых ученых к разработке инноваций в области киберфизических систем.*

Ключевые слова: *Инфокоммуникационные технологии, сети шестого поколения (6G), искусственный интеллект, робототехника, цифровые двойники, когнитивные интерфейсы, архитектура многостороннего доверия, конфиденциальность данных, микроуровень взаимодействия.*

Человеческое общество в современном мире движется с возрастающей скоростью по эволюционной спирали развития живой материи на планете Земля, пытаясь достичь все более сложных форм ее организации, требующих, как минимум, совершенных процессов инфокоммуникаций и интеллекта. Наблюдается процесс нарастания сложности как по массе – нарастание численности людей, так и по функциональным изменениям в обществе, которые имеют как планетарный, так и локальный характер.

Идут непрерывные процессы структурных и смысловых изменений в человеческом обществе, сопровождаемые многообразием эволюционирующих во времени коммуникационных отношений и связей, как между отдельными людьми, так и их группами, обусловленный перераспределением/агрегированием интеллектуальных и материальных ресурсов.

Динамика и качество этих процессов оказывает все более существенное влияние на скорость трансформации создаваемого человечеством искусственного мира технических систем – цифрового мира. Принципиальным необходимым условием существования такого процесса эволюции является симбиоз физического и цифрового миров. При этом непрерывная практическая

реализация процессов совершенствования цифрового мира является залогом выполнения достаточных условий такого симбиоза.

Цифровой мир по сложности и интеллектуальным возможностям становится все более адекватно похожим на мир физический и на данном этапе его развития определяется как киберфизический мир, который по своим возможностям закономерно отстает в своем развитии от мира физического.

Наблюдается определенная тенденция к созданию (сети пятого и шестого поколения, технологии виртуальной, дополненной реальности, робототехника, искусственный интеллект, биоинженерия и др.) и совершенствованию этого киберфизического мира, в котором человечество будет массово использовать цифровых двойников физического мира, включая человека, а также и человеческого общества.

Фактически человечество формирует технологическую и техническую основы для перехода на следующий этап развития цифрового мира, который условно можно определить как «мир желаний». Технические возможности «мира желаний», как цифрового мира, будут обеспечивать не только облегчение существования человека (настоящее время), а проникнут в саму суть его бытия и начнут существенно влиять на биологические процессы развития, как человека, так и человеческого общества. Данное влияние будет оказываться через всевозможные интеллектуальные интерфейсы «человек-техника», предоставляющие с помощью искусственного интеллекта когнитивно-выверенные сценарии развития процессов физической и психофизиологической деятельности как человека, так и его сообществ в виртуальном мире, создающих программируемое самим пользователем чувство максимального эффекта/комфорта.

Для движения в сторону «мира желаний» человечеству предстоит решать все более трудные технологические и технические задачи, требующие проникновения в основы построения и функционирования живой материи, ее симбиозных форм и способов существования природных сообществ, например, достижения предельных параметров инфокоммуникационных процессов как на макро-микроуровнях, а также широкого внедрения систем искусственного интеллекта, разнообразных робототехнических устройств, в том числе андроидного типа.

Развитие киберфизического мира и создание «мира желаний» требует революционных решений во многих областях науки и техники, например в технологиях искусственного интеллекта, создания перспективных материалов (многокомпонентные наноматериалы, термонестабильные полимеры), а также развития беспроводной связи как первоосновы для создания инфокоммуникационной инфраструктуры будущих цифровых миров.

Данная инфраструктура должна обеспечивать практическую реализацию инфокоммуникаций в n-мерных пространствах взаимодействия различных технических устройств по своим функциональным и массогабаритным параметрам, повторяющим (или превосходящим) физический мир.

Необходимо отметить, что в массовом проявлении человечеству данного эффекта до сих пор достичь не удалось несмотря на значительные успехи в различных предметных областях.

Впервые в сетях шестого поколения ставится революционная задача перехода к обеспечению инфокоммуникаций не только на макро, но и на микроуровне взаимодействия технических систем, обеспечивающих автоматический сбор, обработку, передачу, хранение и использование информации в человеческом мире в реальном масштабе времени. Причем технические решения реализуются в массогабаритных параметрах близких к природным, позволяющих создавать киберфизический мир очень похожим на физический мир.

Принципиальной особенностью робототехнических устройств и сетей шестого поколения, отличающей их от всех предыдущих поколений, является использование всеохватывающего искусственного интеллекта (ИИ) как связующего звена между физическим и цифровым мирами. Фактически делается попытка поэтапного создания беспроводной связной инфраструктурной основы для построения глобально распределенной системы искусственного интеллекта, насыщенной роботизированными платформами и роботами всех видов и функционирующей в интересах человеческого общества, которую могут попытаться функционально развить до уровня копирования функциональной деятельности головного мозга человека в локальных и/или глобальных постановках. Техническое решение данных задач, может являться одной из целей создания будущих технологий ИИ и сетей.

Несомненно, переход к сетям следующего поколения будет происходить постепенно под воздействием необходимости решать множество практических задач, требующих эффективных инфокоммуникационных ресурсов, например высокопроизводительные приложения предъявляют высокие требования к пропускной способности беспроводной сети с точки зрения детерминированной задержки и джиттера, требуют наличия гарантированного широкополосного доступа и надежности, высокая пропускная способность необходима для оперативного управления и контроля, а также для координации движений и совместной работы нескольких роботов. Такие варианты использования можно рассматривать как факторы развития экстремального быстродействия, которым должны обладать радиосети будущего.

Планируется, что ИИ станет движущей силой для всех видов повышения эффективности робототехнических устройств и радиосредств шестого поколения, потребует больших объемов данных для преобразования ситуационной осведомленности в реальном времени в принимаемые решения (также в режиме реального времени). Множество широкополосных датчиков будет задействовано для сбора огромного объема данных, необходимых для обучения и работы систем ИИ, а также принятия решения.

Таким образом, системы и средства искусственного интеллекта также должны будут претерпеть существенные эволюционные изменения.

Встроенная поддержка ИИ в перспективных радиосредствах и технологиях будет направлена на предоставление услуг ИИ в любом месте, в любое время, будет постоянно улучшать производительность системы и удобство работы пользователей за счет постоянной оптимизации (системы саморегулирования/самоподдержания состояния различных технических комплексов).

В дополнение к средствам безопасности, реализованным в сетях более ранних поколений, соблюдение конфиденциальности будет критически важным требованием и принципом проектирования сетей будущего. Обеспечение конфиденциальности во всех аспектах работы сети и использования данных будет иметь исключительное значение. В процессе функционирования средств радиосвязи следующего поколения гарантия конфиденциальности данных должна быть главным приоритетом, а не дополнительной функцией. Подобная система должна обеспечивать и гарантировать контроль и обработку данных.

При этом должна быть обеспечена нативная степень доверия процессу обеспечения конфиденциальности, соответствующая разнообразным вариантам осуществления коммуникаций. Важно иметь настраиваемую, поддающуюся проверке и измеряемую степень *доверия*. Владение и функционирование радиосредств, основанное на законах, характерных для текущего и предыдущих поколений сетей, будет перерастать в многостороннее доверие со стороны участников и действующих лиц. Это будет способствовать созданию новой архитектуры доверия, включающей в себя множество факторов. Инклюзивная модель многостороннего доверия будет более насущной, чем модель одиночного доверия. Помимо ориентации на будущее, архитектура многостороннего доверия должна включать защиту, конфиденциальность, отказоустойчивость, безопасность и надежность (системы аутентификации и идентификации). Для обеспечения вышеперечисленных свойств, ИИ должен образовывать экосистему, в которой гармонично взаимоувязаны данные, алгоритмы и вычисления.

Рассмотренные в данном докладе отдельные технологические направления развития инфокоммуникаций, искусственного интеллекта и робототехники
в приложении к созданию будущих цифровых миров, направлены на привлечение внимания молодых ученых к широте и перспективам научных поисков на пути достижения инновационно-значимых результатов, внедрение которых в практику жизни позволит каждому участнику осознавать себя творцом будущих научно-технических свершений человечества.

УДК 621.61

Производственная аспирантура как новая модель послевузовского образования, направленная на сращивание фундаментальной и прикладной науки

Будко П. А.

ПАО «Интелтех», г. Санкт-Петербург, Россия

Аннотация: *В работе рассмотрено продвижение пилотного проекта Минобрнауки и государственной корпорации «Ростех» по внедрению производственной аспирантуры в систему государственной аттестации научных кадров высшей квалификации в Российской Федерации. При этом производственная аспирантура рассматривается как самостоятельный институт ученых-практиков, представляющий собой апробации нового стратегического формата кооперации фундаментальной науки вузов и научно-исследовательских институтов с прикладной наукой отечественных предприятий промышленности. Рассмотрены уникальные цели и задачи производственной аспирантуры как новой модели послевузовского образования. Приведены сведения по мероприятиям прохождения Интенсива «Готовимся к поступлению в производственную аспирантуру» проводимого в рамках технической школы Академия Ростеха на базе интерактивной площадки Корпоративной сетевой академии.*

Ключевые слова: *Академия Ростеха, индустриальный наставник, кадры высшей квалификации, производственная аспирантура, портфолио абитуриента, базовый вуз.*

Введение

Начиная с 2025 года Министерством науки и высшего образования РФ (Минобрнауки) совместно с Государственной корпорацией по содействию разработке, производству и экспорту высокотехнологичной промышленной продукции «Ростех» (ГК «Ростех») в России запущен пилотный проект по внедрению в систему аттестации научных и научно-педагогических работников высшей квалификации *производственной аспирантуры*. Данную инициативу поддержал Президент РФ В.В. Путин [1].

В целях развития механизмов активной государственной политики по привлечению молодежи в сферу науки и технологий, вовлечения исследователей и разработчиков в решение важных задач для страны и общества в десятилетие науки и технологий, профессиональной адаптации, выявления и максимального использования творческого потенциала молодых интеллектуальных кадров, стимулирования научной деятельности и привлечения их к решению научно-технических задач, повышающих качество текущих научно-исследовательских и опытно-конструкторских работ (НИОКР), данный пилотный проект призван укрепить горизонтальные связи базовых высших учебных заведений страны с производственными предприятиями Российской Федерации.

Проект предполагает вести подготовку научных кадров высшей квалификации для реального сектора экономики с привязкой к конкретным

вызовам и задачам оборонно-промышленного комплекса. При этом модель производственной аспирантуры отличается двойным научным руководством: от базового вуза и от предприятия (индустриального партнера). Производственный аспирант большую часть времени по подготовке диссертации проводит на своем рабочем месте без отрыва от текущих на производстве НИОКР.

Развитию производственной аспирантуры и молодежной науке в ГК «Ростех» в настоящее время уделяется огромное внимание. Корпорация имеет в своем составе 120 научно-исследовательских организаций и конструкторских бюро, на предприятиях функционирует более 20 диссертационных советов. В последний год активно развиваются Советы молодых ученых и специалистов предприятий и холдинговых компаний. Развиваются передовые инженерные школы, призванные стать эффективным инструментом нового стратегического формата кооперации фундаментальной науки вузов и научно-исследовательских институтов с прикладной наукой отечественных предприятий промышленности. За 2026 год производственная аспирантура объединила более 30 университетов участников (базовых вузов), более 80 предприятий ГК «Ростех» (индустриальных партнеров) из 15 отраслей промышленности [2].

Производственная аспирантура как новая модель послевузовского образования

Пилотный проект производственной аспирантуры, казалось бы, созвучный с традиционной аспирантурой, а также имеющий общее целеполагание в системе подготовки научных кадров высшей квалификации, тем не менее, имеет существенные отличия в построении учебного процесса и несет в себе значительные преимущества в отношении соискателя ученой степени – производственного аспиранта. Рассмотрим эти отличия [2].

Во-первых, традиционная аспирантура вузов и научных организаций, как правило, направлена на продвижение фундаментальной науки. Это подтверждается тем, что большинство ученых степеней Высшей аттестационной комиссией (ВАК) Минобрнауки присуждаются за решение соискателями *научной задачи* и гораздо меньшая часть – за разработку *новых научно обоснованных технических, технологических или иных решений и разработок*… [3]. В тоже время, производственная аспирантура направлена на развитие прикладной науки, рассчитанной на применение в производстве. Соответственно, соотнесение традиционной аспирантуры от производственной аспирантуры можно просмотреть на соотнесении фундаментальной науки и прикладной науки.

Во-вторых, по своему предназначению производственная аспирантура направлена на развитие формы взаимодействия базового вуза с индустриальным партнером, направленной, с одной стороны на повышение эффективности научно-исследовательской работы, а с другой – на решение конкретных прикладных задач промышленного предприятия.

В-третьих, внедрение пилотного проекта производственной аспирантуры позволит молодым ученым и специалистам предприятий ГК «Ростех» повышать уровень своих компетенций, научного и карьерного роста без отрыва от производства, несмотря на представление формы обучения в очном формате.

Также, в отличие от другой формы подготовки научных кадров высшей квалификации в виде соискательства без освоения программы аспирантской подготовки [4], Минобрнауки к особенностям модели производственной аспирантуры относит следующие [2]:

− очная форма обучения, которая полностью интегрируется с производством, но при этом происходит сокращение числа аудиторных занятий в интересах увеличения времени, отводимых на исследовательскую работу (не менее чем на 30 % от общего объема образовательной программы должны состоять из прикладных исследований [5]);

− производственный аспирант помимо научного руководителя от базового вуза имеет индустриального наставника от предприятия-партнера, где проводятся прикладные исследования. Фактически план работы над диссертацией формируется данными руководителями в кооперации;

− проведение прикладных исследований осуществляется на базе предприятия-партнера с поэтапной верификацией и защитой получаемых научных и прикладных результатов, обязательной их публикацией;

− производственный аспирант совместно с научным руководителем и индустриальным наставником разрабатывает индивидуальный план работы над диссертацией, включающий наряду со сдачей кандидатских экзаменов, семестровые (годовые) отчеты, как правило, совмещаемые с этапами выполнения соискателем на производстве текущих НИОКР, находящихся в основе получаемых прикладных (научных) результатов;

− производственная аспирантура позволяет соискателю наряду с изучением теории глубоко вникнуть в производственные процессы, активно используя экспериментально-стендовую базу индустриального партнера;

− обучение в производственной аспирантуре завершается проведением итоговой аттестации в вузе, а также расширенного научно-технического семинара на предприятии, на котором дается оценка практической значимости полученных прикладных результатов. Возможно участие представителей предприятий – участников пилотного проекта в проведении итоговой аттестации и в защите диссертации, в том числе путем их включения в состав диссертационного совета (при наличии такой возможности) [5].

Реализация программы практико-ориентированной подготовки научных кадров для высокотехнологичных отраслей экономики

Программа практико-ориентированной подготовки научных кадров для высокотехнологичных отраслей экономики предполагает сроки проведения пилотного проекта производственной аспирантуры с 2025/26 по 2028/29 учебные годы [5], вплоть до подведения итогов реализации пилотного проекта и принятия решения о внедрении программы производственной аспирантуры в систему подготовки и аттестации научных кадров высшей квалификации.

Целевой установкой данного пилотного проекта является [5]:

- повышение эффективности аспирантуры (увеличение защит диссертаций за установленные сроки обучения в аспирантуре);
- получение научных и/или прикладных результатов, внедряемых на производственных предприятиях страны;
- подготовка научных кадров высшей квалификации для высокотехнологичных отраслей экономики;

В пилотном проекте на добровольной основе участвуют вузы, осуществляющие подготовку научных кадров по научным специальностям инженерно-технического профиля и других, значимых для высокотехнологичных отраслей экономики профилей, привлекающие на договорной основе организации, осуществляющие разработку и производство высокотехнологичной продукции. При этом договорная основа предполагает целевое обучение [6].

Реализация программы производственной аспирантуры может осуществляться с применением сетевой формы обучения [7], при которой вузы являются базовыми организациями, а предприятия промышленности (индустриальные партнеры) – организациями-участниками такой сетевой формы [5].

Договор о сетевой форме реализации программы производственной аспирантуры должен включать определение темы диссертации на основе прикладных задач предприятия-участника пилотного проекта [5]. При этом соискателю ученой степени назначается научный руководитель от базового вуза и научный консультант – от предприятия-участника пилотного проекта.

Образовательный процесс по освоению программы производственной аспирантуры должен быть интегрирован в выполнение научных исследований соискателем на предприятии-участнике пилотного проекта [5].

Реализация подготовки молодых ученых и специалистов предприятий ГК «Ростех» к поступлению в производственную аспирантуру в 2026 году

В настоящее время идет второй год реализации пилотного проекта по программе практико-ориентированной подготовки научных кадров для высокотехнологичных отраслей экономики (производственная аспирантура). Методическое сопровождение отбора молодых ученых

и специалистов предприятий промышленности из числа разработчиков и конструкторов осуществляет АНО «Корпоративная сетевая академия» (Академия Ростеха) – как центр обучения и развития для сотрудников организаций Корпорации.

С июля по сентябрь 2026 года проходят онлайн-встречи и онлайн-лекции с целью предоставления более полной информации для подготовки к поступлению в производственную аспирантуру и будущей научной деятельности молодых ученых ГК «Ростех». В качестве модераторов данных встреч на ВКС-площадке Научной школы Ростеха выступают сотрудники Академии Ростеха, представители производственной аспирантуры, эксперты ВАК и Федерального института промышленной собственности (Роспатента).

Примерный тематический план программы Интенсива «Готовимся к поступлению в производственную аспирантуру» включает четыре модуля, рис. 1.

Доступ к занятиям и материалам Интенсива происходит через обращение и регистрацию на ВКС-площадке Академии Ростех. Занятия проходят еженедельно по четвергам в 10.00 (Мск).

I	**Модуль 1. Введение в научную деятельность**
1.1	Развитие модели производственной аспирантуры в интересах высокотехнологичных предприятий
1.2	Устройство «научного мира» и Стратегия научно-технологического развития РФ
1.3	О Стратегии развития Государственной корпорации «Ростех» и ее реализации
1.4	Меры поддержки молодых учёных в Корпорации
1.5	Меры государственной поддержки молодых учёных
1.6	Карьерные траектории в науке: от инженера до генерального конструктора
II	**Модуль 2. Подготовка к аспирантуре (предаспирантура)**
2.1	Поступление в производственную аспирантуру и этапы освоения программы подготовки
2.2	Основы написания и защиты диссертации кандидата наук
2.3	Особенности подготовки и защиты диссертации по результатам разработки новых научно-обоснованных технических и технологических решений
2.4	Особенности определения темы, объекта, предмета и цели исследования
2.5	Формализованная постановка научной задачи. Декомпозиция на частные задачи. Определение пробела в имеющихся исследованиях
2.6	*Практическое занятие*: Разработка портфолио абитуриента при поступлении в производственную аспирантуру
III	**Модуль 3. Работа с научной информацией**
3.1	Патентные исследования и защита интеллектуальной собственности (РИД)
3.2	Порядок подготовки публикаций. Апробация и реализация научных результатов

3.3	*Практическое занятие*: Порядок подготовки публикаций по результатам диссертационного исследования
IV	**Модуль 4. Методология научного исследования**
4.1	Порядок проведения моделирования. Разработка основного научного результата диссертации в виде Модели
4.2	Разработка основного научного результата диссертации в виде Методики (Метода)
4.3	Разработка научно-технических предложений как прикладного результата исследования
4.4	Порядок проведения научно-технического эксперимента
4.5	*Практическое занятие*: Разработка развернутого плана диссертационного исследования

Выводы

Внедрение и расширение Министерством науки и высшего образования РФ совместно с ГК «Ростех» пилотного проекта по программе практико-ориентированной подготовки научных кадров для высокотехнологичных отраслей экономики рассматривается как самостоятельный институт ученых-практиков, представляющий собой апробации нового стратегического формата кооперации фундаментальной науки вузов и научно-исследовательских институтов с прикладной наукой отечественных предприятий промышленности.

Результат внедрения в систему подготовки научных кадров высшей квалификации такой новой модели послевузовского образования, как производственная аспирантура, призван существенно укрепить кадровый потенциал научных и инженерных школ предприятий не только ГК «Ростех», но и других наукоемких государственных корпораций «Росатом», «Роскосмос» и др. Это поможет объединить ведущие университеты и крупнейшие высокотехнологичные предприятия страны в единый образовательно-производственный кластер, способствуя деловому сотрудничеству и укреплению контактов вузовской науки и конструктората промышленности, создавая фундамент профессиональной карьеры молодых ученых и специалистов-практиков на производстве.

Список литературы

1. Выступление С.В. Чемезова на заседании Совета по науке и образованию (Москва, Кремль, 06 февраля 2025 года). – М.: 2025. – URL: http://www.kremlin.ru/events/president/news.76222 (дата обращения 16.08.2026).

2. Производственная аспирантура – новая модель подготовки кадров высшей квалификации для высокотехнологичных отраслей экономики. – URL: https://производственная-аспирантура.рф (дата обращения 16.08.2026).

3. Положение о присуждении ученых степеней (Пост. Правительства РФ от 24.09.2013 № 842 «О порядке присуждения ученых степеней». – URL: http://www.consultant.ru (дата обращения 16.08.2026).

4. Приказ Министерства образования и науки РФ от 28 марта 2014 г. № 248 «О порядке и сроке прикрепления лиц для подготовки диссертации на соискание ученой степени кандидата наук без освоения программ подготовки научно-педагогических кадров в аспирантуре (адъюнктуре)». – URL: http://www.garant.ru/products/ipo/prime/doc/70552360/ (дата обращения 16.08.2026).

5. Приказ Министерства науки и высшего образования РФ от 28 мая 2026 г. № 320 «О пилотном проекте по практико-ориентированной подготовке научных кадров для высокотехнологичных отраслей экономики». – URL: https://www.informio.ru/update/wuz/91539 (дата обращения 16.08.2026).

6. Постановление правительства РФ от 27.04.2024 г. № 555 «О целевом обучении по образовательным программам среднего профессионального и высшего образования». – URL: https://www.consultant.ru/document/cons_doc_LAN_475586/ (дата обращения 16.08.2026).

7. Приказ Министерства науки и высшего образования РФ от 05.08.2020 № 882/391 «Об организации и осуществлении образовательной деятельности при сетевой форме реализации образовательных программ». – URL: https://www.garant.ru/products/ipo/prime/doc/74526602/ (дата обращения 16.08.2026).

УДК 338.47:621.39

К вопросу о тенденциях технического и технологического развития телекоммуникационных систем

Кулешов И. А., Курносов В. И.

ПАО «Интелтех», г. Санкт-Петербург, Россия

Аннотация: *Темпы и особенности развития рынка телекоммуникационных услуг во многом определяют инфраструктуру современного бизнеса, отражают уровень развития информационных технологий и влияют на весь современный экономический и социальный уклад. В статье рассматриваются тенденции развития рынка телекоммуникационных услуг в нашей стране и их классификация по признакам зависимости от появления новых технологий (тенденции предложения), новых потребностей (тенденции спроса) либо новых условий рыночной среды. Сделаны выводы о замедлении темпов развития данного рынка, что обусловлено неблагоприятными макроэкономическими условиями, ограниченностью инвестиционных возможностей операторов мобильной связи стран СНГ.*

Ключевые слова: *телекоммуникации, рынок телекоммуникационных услуг, информационно-коммуникативные технологии, обеспеченность услугами связи.*

Введение

В современном мире информационный обмен различными видами информации приобрел лавинообразный характер и является одним из глобальных связующих факторов в экономике, геополитике и межкультурных связях. С ростом темпов индустриализации и милитаризации общества особую актуальность информационный обмен приобретает в сфере управления различными видами корпоративной и информационной деятельности [1].

Современные телекоммуникационные системы (стационарные и мобильные) являются сложными многокомпонентными организационно-техническими системами, транспортирующими разнообразную информацию в разнородных средах в виде сигналов различной физической природы [1, 2]. Сигналы передаются в условиях нестабильной внешней среды и деструктивных воздействий. Воздействия на сигналы и радиоэлектронное оборудование носят как случайный, так и организованный характер со стороны других противоборствующих систем [1].

Особенности развития современных систем связи

Отличительными особенностями современных систем связи являются следующие [1]:

− телекоммуникационные системы и системы управления телекоммуникациями создаются и развиваются одновременно;

− комплексная автоматизация управления информационным обменом;

− переход от коммутации каналов и сообщений к коммутации пакетов;

− широкое использование достижений в области цифровой связи и ЭВМ;

− интеллектуализация управления информационным обменом;

− исследования, направленные на индустриализацию умственного труда людей, занятых управлением сложными техническими системами, функционирующими в экстремальных условиях, в том числе в сфере управления телекоммуникационными системами.

Переход от коммутации каналов и сообщений к коммутации пакетов явился одним из важнейших шагов в развитии телекоммуникационных систем. Цифровые технологии открыли широкий спектр возможностей – максимальное использование дорогостоящих каналов связи, контроль передачи информации по информационному и логическому каналам, низкий уровень ошибки передачи сигналов ($P_{ош}=10^{-12}$), использование мини- и макро-ЭВМ в качестве коммутационных и интерфейсных машин, модульное построение аппаратных и программных средств, разграничение функциональных уровней в архитектуре систем обмена данными, регламентацию иерархий протоколов, реализацию основных протоколов транспортной станции в интерфейсных ЭВМ.

Другой отличительной чертой развития телекоммуникационных систем является интеллектуализация управления информационным обменом. В специальных системах связи (государственные, военные) из-за масштабности и сложности структуры, особой важности передаваемой информации, возможного противодействия со стороны противоборствующих систем, человек продолжает участвовать в управлении информационным обменом, системы остаются человеко-машинными. Психологические и интеллектуальные трудности, которые испытывает человек при решении задач управления, связаны с ограниченной емкостью его кратковременной памяти при выборе возможных вариантов решений, жесткие требования на время принятия решения – вступают в конфликт со скоростью человеческого мышления. Из-за тяжести возможных последствий резко возрастает роль человеческого фактора. Поэтому в высокоавтоматизированных телекоммуникационных системах должностные лица высших органов оперативного управления несут повышенные психофизические и интеллектуальные нагрузки. Наиболее остро проблема стоит в телекоммуникационных системах военного назначения, управления транспортом и ядерной энергетикой.

Ведущие научные центры мира проводят исследования, направленные на индустриализацию умственного труда людей, занятых управлением сложными техническими системами, функционирующими в экстремальных условиях, в том числе в сфере управления телекоммуникационными системами. Их главная цель – попытаться обобщить результаты, полученные в сфере исследований интеллектуального мышления человека, автоматизации физического и умственного труда, управления сложными техническими системами, создание систем искусственного интеллекта и построить компьютерные средства интеллектуальной поддержки управления телекоммуникационными системами.

Современное развитие в области телекоммуникаций, информатики привело к появлению большого числа взаимосвязанных научных направлений

и разнообразных их приложений в телекоммуникационной сфере. Несмотря на многообразие достижений, все полученные результаты имеют одну конечную цель – создание цифровых глобально интегрированных телекоммуникационных систем устойчивых к деструктивным воздействиям, с максимальной автоматизацией физического и умственного труда людей, занятых управлением информационным обменом.

Вектора развития телекоммуникационной и инфокоммуникационной системы

В последнее десятилетие специалисты отрасли электросвязи выделяли следующие тенденции, которые в настоящее время уже оказали влияние на деятельность операторов мобильной связи [3]:

− оптическая транспортная сеть (Optical Transport Network, OTN) — повышение пропускной способности оптической транспортной сети на несколько порядков, что связано с увеличением объема обмениваемой информации;

− глобальная информационная сеть (Global Gnoseology Graph, GGG) как качественное обновление существующей всемирной сети WWW — World Wide Web, предполагающее сортировку потоков информации и более упорядоченный обмен только качественной информацией, что позволяет сократить ее избыточность, объем, противоречивость и другие отрицательные явления бесконтрольного обмена информацией;

− «Интернет вещей» (Internet of Things, IoT) – управление через интернет различными устройствами, от бытовых до сложных медицинских, что меняет объем и характер трафика;

− «Большие данные» (Big Data) — рост потребности в обработке больших объемов плохо структурированных данных, что требует повышения пропускной способности системы, производительности маршрутизаторов в составе телекоммуникационной системы;

− облачные вычисления (Cloud Computing, CC) — услуги по обработке данных и их хранению в специальных «облаках» все более востребованы, что порождает дополнительные требования к телекоммуникационным системам.

Обобщив вышеперечисленные тенденции, в [4] предлагается систематизировать их по направлениям влияния на рынок телекоммуникационных услуг в зависимости от того какой аспект рынка они затрагивают.

Источники возникновения организационно-экономических проблем телекоммуникационной сферы

В результате анализа влияния информационно-телекоммуникационных технологий на экономическое развитие государства выявлены источники возникновения организационно-экономических проблем телекоммуникационной сферы, которые типичны для стран СНГ:

− особенности телекоммуникаций, как сферы, которая эксплуатирует средства связи и организует технологический процесс по передаче различной информации;

− возрастание социально-экономической роли телекоммуникаций в жизни общества;

− научно-технический прогресс, который вызывает стремительное развитие техники и технологий, принципов построения телекоммуникационных сетей, спектра услуг и т.п.

При этом проблемами телекоммуникационной сферы, обусловленными спецификой организации производственного процесса, являются:

− технико-технологические (обеспечение единства построения телекоммуникационной сети, обеспечение технико-технологического механизма использования объединенного оборудования, соблюдение единых правил технического обслуживания и т. п.);

− организационно-экономические (организация взаимных расчетов за выполненные работы, оплата услуг национального роуминга, пропуск трафика, взаимосоединение телекоммуникационных сетей и др).

Следует также отметить проблемы, вызывающие возрастанием роли телекоммуникаций в жизни общества:

− преодоление существующего «цифрового неравенства»;

− необходимость реализации проектов, реализующих конституционные права граждан – развитие телемедицины для спасения жизни людей, создание образовательных сетей, повышение уровня защищенности телекоммуникационных сетей;

− необходимость защиты от возможного использования информационных технологий для сбора информации о поведении и потребительскими предпочтениями людей спецслужбами, транснациональными и другими структурами.

В рассматриваемом аспекте, актуальными вопросами создания организационно-экономического механизма предоставления общедоступных телекоммуникационных услуг продолжают оставаться:

− разработка технико-экономических показателей обеспечения необходимого уровня доступа населения к социально значимым телекоммуникационным услугам;

− определение сроков достижения всеобщего обслуживания;

− определение размера средств, необходимых для компенсации потерь операторам, которые предоставляют убыточные услуги;

− определение порядка определения убыточности отдельных услуг и оператора, в целом, с целью предупреждения использования затратного механизма;

− определение порядка распределения средств между операторами, особенно в условия дефицита этих средств.

Итак, актуальными задачами поиска путей взаимодействия участников рынка, требующими своего совершенствования, являются:

− создание новых или совершенствование существующих систем ценообразования на телекоммуникационном рынке и взаиморасчетов между его участниками, в изменяющихся условиях;

− определение показателей качества новых услуг и методов их определения

− определение и обоснование конкурентных стратегий телекоммуникационных операторов в современных условиях;

− определение направлений и целесообразности распространения деятельности телекоммуникационных операторов на специализацию поставщиков контента.

Наступило время для исследования следующих вопросов в сфере экономических проблем телекоммуникаций:

− разработка методов определения уровня государственного регулирования и его влияния на эффективность хозяйственной деятельности;

− определение и обоснование оптимального для разных условий хозяйствования уровня государственного вмешательства в рыночные механизмы;

− создание методики определения интегрального показателя состояния и развития телекоммуникаций, его использования как одного из индикаторов при прогнозировании ВВП страны.

Заключение

В завершение можно сделать вывод о неоднозначности тенденций и перспектив развития рынка телекоммуникационных услуг. Сегодня главные тенденции развития телекоммуникационных систем включают внедрение сетей 5G и проектирование 6G, массовое использование искусственного интеллекта для автоматизации, переход на открытые архитектуры Open RAN, развитие спутникового интернета на низкой орбите, а также укрепление кибербезопасности и облачных платформ

Положительные тенденции развития формируются за счет роста спроса на новые виды услуг, связанные с передачей, обработкой, хранением информации, а также возможностями новых информационно-коммуникативных технологий, в развитие которых вкладываются значительные инвестиционные ресурсы.

Но для операторов связи не все эти возможности могут быть использованы ввиду специфики отечественного рынка телекоммуникационных услуг,

ограниченных возможностей инвестирования, неблагоприятных макроэкономических тенденций развития экономики страны.

Тем не менее анализ ключевых тенденций развития рынка телекоммуникационных услуг и их систематизация будут полезны при стратегическом планировании и управлении телекоммуникационными организациями.

Список литературы

1. Мирошников В. И., Кулешов И. А., Талагаев В. И. Тенденции и особенности развития современных телекоммуникационных систем // Техника средств связи. № 4 (160). – 2022. С. 8-16

2. Информационные технологии в системах управления силами ВМФ. Шпак В. Ф., Директоров Н. Ф., Мирошников В. И. и др. – СПб. «Элмор», 2005. – С. 832

3. Ефимов В. В., Соколов Н. А., Федоров А. В. Вероятные направления эволюции телекоммуникационной системы. // Труды ЦНИИС. Санкт-Петербугский филиал. Т 1, № 1 (2), 2016. С. 11-23.

4. Гапоненко Т. В., Жуковский Д. А. Тенденции развития российского рынка телекоммуникационных услуг // Вестник Бурятского государственного университетаа. Экономика и менеджмент. № 2, 2019. С. 8-16.

5. Инфокоммуникационные сети: энциклопедия. Кн. 4: Гетерогенные сети связи: принципы построения, методы синтеза, эффективность, цена, качество / П. А. Будко, И. А. Кулешов, В. И. Курносов, В. И. Мирошников; Под ред. проф. Мирошникова В. И. – М.: Наука, 2020. – 683 с.

УДК 004.056.53

Обеспечение безопасности автономных ИИ-агентов при их интеграции в телекоммуникационные системы

Ходаковский М. А.

АО «НПП «Сигнал», г. Санкт-Петербург, Россия

Аннотация: *Рассмотрены вопросы обеспечения безопасности автономных интеллектуальных агентов на базе больших языковых моделей (БЯМ), интегрируемых в телекоммуникационные системы специального назначения (ТКС СН) федеральных органов исполнительной власти (ФОИВ) для автоматизации задач управления, обработки данных и взаимодействия с внешними информационными ресурсами. Показано, что расширение автономности ИИ-агентов формирует разрыв между их функциональными возможностями и обеспечиваемым уровнем безопасности, что критично для систем, обрабатывающих данные ограниченного доступа в контуре единого информационно-управляющего пространства (ЕИУП) ФОИВ. Разработана шестидоменная модель угроз безопасности ИИ-агентов, систематизированная в соответствии с классификацией ФСТЭК России и банком данных угроз безопасности информации; для каждого домена риска определены соответствующие угрозы банка данных угроз и тактики их реализации, аналогичные тактикам MITRE ATT&CK. Обоснована целесообразность нивелирования выявленных тактик двумя взаимодополняющими моделями безопасности: AgentGuardian, реализующей контекстно-зависимое управление доступом на основе валидации графа потока управления и атрибутных политик, и архитектурой нулевого доверия Zero Trust, обеспечивающей изоляцию агента на уровне инфраструктуры. Показано, что практическая реализация указанных моделей в ТКС СН ФОИВ требует соблюдения требований Федеральных законов, применения сертифицированных средств криптографической защиты информации в соответствии с рекомендациями ФСБ России и построения частной модели угроз в соответствии с методикой ФСТЭК России. Обеспечение безопасности ИИ-агентов является необходимым условием их доверенной интеграции в ЕИУП ФОИВ наравне с обеспечением интероперабельности телекоммуникационных систем связи.*

Ключевые слова: *безопасность ИИ-агентов, инъекция промпта, контроль доступа, модель угроз, нулевое доверие.*

Введение

Стремительное развитие технологий больших языковых моделей обусловило переход интеллектуальных систем от пассивных инструментов формирования текста к автономным агентам, способным самостоятельно планировать и исполнять последовательности действий: обращаться к файловым системам, базам данных, сетевым сервисам и внешним API. Подобные ИИ-агенты все шире применяются в производственных средах, в том числе в контурах автоматизации управления сложными организационно-техническими системами, и в том числе высок интерес к их внедрению в телекоммуникационные системы специального назначения федеральных органов исполнительной власти для повышения оперативности исполнения рутинных задач. Внедрение ИИ-агентов в процессы обработки данных, поддержки принятия решений и взаимодействия с пользователями рассматривается как одно из направлений повышения уровня автоматизации

управления, наращивание которого предусмотрено в рамках концепции формирования единого информационно-управляющего пространства ФОИВ. Вместе с тем расширение автономности агентов формирует новый класс угроз безопасности, специфичных для систем на основе больших языковых моделей и качественно отличающихся от угроз традиционного программного обеспечения. Анализу этих угроз, их месту в системе классификации ФСТЭК России и способам их нивелирования средствами AgentGuardian и Zero Trust посвящен настоящий доклад.

Цель статьи – выявление угроз безопасности автономных ИИ-агентов, их систематизация в соответствии с классификацией ФСТЭК России, обоснование тактик нивелирования указанных угроз и способов их практической реализации в ТКС СН ФОИВ с соблюдением требований законодательства Российской Федерации и рекомендаций регуляторов.

Актуальность направления исследований

В современной практике ИИ-агенты перестали быть пассивными помощниками и превратились в автономные системы, способные самостоятельно планировать последовательности вызовов инструментов и принимать контекстно-зависимые решения. Однако интеграция агентов в сложные иерархические объекты управления выявила существенный разрыв между их функциональными возможностями и обеспечиваемым уровнем безопасности. Данный разрыв обусловлен тремя основными факторами.

Во-первых, существующие статические барьеры защиты (Llama Guard, Amazon Bedrock Guardrails и аналогичные решения) ориентированы на фильтрацию текстового содержания запросов и ответов, но не способны контролировать динамическую последовательность действий агента в процессе исполнения задачи [1].

Во-вторых, для больших языковых моделей инструкции и данные являются неразличимыми токенами в едином окне контекста, что делает атаки типа «инъекция промпта» структурной особенностью архитектуры агентов, а не устранимой программной ошибкой.

В-третьих, агенты подвержены генерации некорректных вызовов инструментов и зацикливанию действий даже в отсутствие внешнего вредоносного воздействия, что ведет к деградации функционирования системы управления.

Это придает задаче обеспечения безопасности ИИ-агентов не только техническое, но и нормативно-правовое значение, требующее последовательного анализа угроз, их систематизации в терминах, принятых регулятором, и обоснованного выбора мер защиты.

Угрозы безопасности ИИ-агентов и их место в классификации ФСТЭК России

Модель угроз описывает способы, которыми злоумышленник может превратить легитимные возможности агента в векторы атаки; основная цель

атакующего — скомпрометировать функциональность агента через манипуляцию его процессом принятия решений. К основным векторам атак относятся: манипуляция входными данными посредством прямых и косвенных инъекций промптов для изменения аргументов вызова инструментов (например, подмена адреса электронной почты для эксфильтрации данных); манипуляция последовательностью вызовов инструментов, побуждающая агента к выполнению вредоносной цепочки действий; компрометация учетных данных за счет использования доступа агента к секретам, хранящимся в конфигурационных файлах или переменных окружения; злоупотребление возможностями исполнения команд в оболочке, включая установку программных закладок и удаление файлов.

Обобщение перечисленных векторов атак позволило сформировать шестидоменную модель угроз, в которой учтены основные направления – учетные данные, исполнение, сетевой выход, целостность промптов, доступ к базам данных и дрейф конфигурации. Данная модель согласуется с подходом ФСТЭК России к оценке угроз безопасности информации, закрепленным методическим документом «Методика оценки угроз безопасности информации» (утв. ФСТЭК России 05.02.2021) [4], согласно которому модель угроз строится как совокупность сценариев — тактик и техник реализации угроз, аналогичных используемым в матрице MITRE ATT&CK, — с использованием банка данных угроз безопасности информации ФСТЭК России (БДУ, bdu.fstec.ru). В состав БДУ включен отдельный раздел угроз безопасности информации систем искусственного интеллекта, в котором в качестве самостоятельных объектов воздействия наряду с моделью и обучающими данными впервые выделены системные промпты и агенты [5], что подтверждает соответствие рассматриваемой модели угроз актуальным с точки зрения регулятора.

Сопоставление доменов риска с угрозами БДУ ФСТЭК, тактиками их реализации, аналогичными тактикам MITRE ATT&CK, и возможными последствиями представлено в табл. 1. Домены учетных данных, сетевого выхода и доступа к базам данных охватываются общими (не специфичными для систем искусственного интеллекта) угрозами БДУ и подлежат конкретизации в частной модели угроз ФОИВ с учетом состава нарушителей и объектов воздействия, определяемых в соответствии с методикой [4].

Таблица 1 – Угрозы безопасности ИИ-агентов в составе ТКС СН ФОИВ в классификации ФСТЭК России

Домен риска	**Возможные последствия**	**Угроза БДУ ФСТЭК**	**Тактика (аналог MITRE ATT&CK)**
Учетные данные	Несанкционированный доступ к облачным ресурсам и провайдерам БЯМ	Общие угрозы БДУ (доступ к учетным данным)	Доступ к учетным данным
Исполнение	Повышение привилегий, боковое перемещение по сети	УБИ.223, УБИ.225, УБИ.226	Повышение привилегий, закрепление
Сетевой выход	Утечка данных ограниченного доступа	УБИ.215	Эксфильтрация
Целостность промптов	Перехват управления агентом (agent corruption)	УБИ.220, УБИ.221	Обход средств защиты, воздействие
Доступ к базам данных	Массовая утечка данных ограниченного доступа	Общие угрозы БДУ (SQL-инъекции)	Сбор данных
Дрейф конфигурации	Создание условий для таргетированных атак	УБИ.217, УБИ.214	Закрепление, уклонение от обнаружения

Выявленные тактики — доступ к учетным данным, повышение привилегий и закрепление, эксфильтрация, обход средств защиты, сбор данных и уклонение от обнаружения — определяют состав мер, необходимых для их нивелирования. Указанные меры в обобщенном рассмотрении реализуются в рамках двух взаимодополняющих моделей безопасности: контекстно-зависимого управления доступом на уровне вызываемых инструментов, известной как AgentGuardian, и архитектуры нулевого доверия на уровне инфраструктуры, названной Zero Trust. Рассмотрим их далее.

Нивелирование атак с точки зрения моделей AgentGuardian и Zero Trust

Тактики повышения привилегий и закрепления реализуются за счет манипуляции последовательностью вызовов инструментов и нивелируются моделью AgentGuardian, реализующей три слоя контроля на уровне вызываемых инструментов [2]. Валидация потока управления заключается в построении графа допустимых траекторий исполнения агента в ходе контролируемой фазы подготовки и последующей проверке каждого выполняемого шага в процессе работы: если агент пытается вызвать инструмент в порядке, не предусмотренном графом, действие блокируется, что напрямую противодействует тактике закрепления. Политики управления доступом на основе атрибутов, ограничивающие каждый инструмент контекстными

атрибутами — идентификатором пользователя, временем выполнения, объемом затраченных токенов, — нивелируют тактики доступа к учетным данным и повышения привилегий за счет сужения области действия каждого вызова. Обобщение входных данных методом индукции регулярных выражений обеспечивает устойчивость политик к ранее не встречавшимся, но допустимым входным данным, снижая количество ложных срабатываний при сохранении полноты контроля.

Тактики обхода средств защиты, эксфильтрации и уклонения от обнаружения нивелируются архитектурой нулевого доверия, формирующей защищенный периметр исполнения агента на уровне инфраструктуры [3]. Изоляция рабочей нагрузки на уровне ядра операционной системы с использованием защищенного контейнерного рантайма в среде оркестрации Kubernetes противодействует тактике повышения привилегий даже в случае успешной инъекции промпта. Вынесение секретов в отдельный сопровождающий контейнер, исключающий прямой доступ агента к незащищенным учетным данным, нивелирует тактику доступа к учетным данным. Сетевые политики исходящего трафика, задающие разрешенные адреса назначения, противодействуют тактике эксфильтрации данных. Фреймворк целостности промптов, обеспечивающий криптографическую защиту метаданных о происхождении сообщений и явную маркировку недоверенного содержимого, нивелирует тактику обхода средств защиты, реализуемую через инъекцию промпта.

Таким образом, каждая из выявленных тактик атак имеет соответствующую меру нивелирования на уровне управления доступом или на уровне инфраструктуры. Практическую реализацию указанных мер в ТКС СН ФОИВ с соблюдением требований регуляторов рассмотрим далее.

Направления реализации в телекоммуникационных системах специального назначения федерального органа исполнительной власти

Практическая реализация рассмотренных моделей безопасности в ТКС СН ФОИВ должна осуществляться с соблюдением требований законодательства Российской Федерации и рекомендаций регуляторов. В соответствии с методикой ФСТЭК России [4] производится формирование частной модели угроз и осуществляются выбор мер защиты, в том числе определяется необходимость криптографической защиты данных в рамках фреймворка целостности промптов и проксирования учетных данных с применением сертифицированных средств криптографической защиты информации.

С учетом изложенного интеграция ИИ-агентов в контур ЕИУП ФОИВ требует решения следующих задач:

– приведение частной модели угроз ИИ-агентов в соответствие с методикой ФСТЭК России, в том числе построение сценариев, определение тактик и техник атак и ведение соответствия с банком данных угроз;

− построение эталонного графа потока управления для типовых сценариев использования агентов, обслуживающих задачи ТКС СН, и его верификация в процессе эксплуатации;

− разработка атрибутных политик доступа для каждого инструмента, используемого агентом при взаимодействии с элементами ЕИУП, с учетом требований к обработке данных ограниченного доступа;

− развертывание изолированной программно-аппаратной среды исполнения агентов с использованием защищенного рантайма и вынесением секретов в отдельный доверенный контур;

− регламентация сетевых политик исходящего трафика агентов в соответствии с перечнем разрешенных информационных ресурсов ТКС СН ФОИВ;

− применение сертифицированных средств криптографической защиты информации для защиты метаданных и секретов в соответствии с рекомендациями ФСБ России;

− внедрение процедур автоматизированного аудита безопасности парка агентов.

Практическая значимость рассмотренных мер подтверждается результатами их опытной эксплуатации в течение 90 суток промышленной эксплуатации. Речь идет о случае использования девяти автономных ИИ-агентов в организации, обрабатывающей данные ограниченного доступа, при этом автоматизированным агентом аудита безопасности были обнаружены и устранены четыре уязвимости высокой степени критичности, а достигнутый уровень защиты был сопоставлен со всеми известными паттернами атак на ИИ-агентов [3]. Аналогичный подход применим и к задачам ФОИВ: по мере автоматизации процессов обработки информации в рамках ЕИУП обеспечение доверенного и контролируемого поведения ИИ-агентов, соответствующего требованиям законодательства и рекомендациям ФСБ и ФСТЭК России, становится необходимым условием сохранения целостности и безопасности единого адресного пространства ФОИВ наравне с обеспечением интероперабельности ТКС СН.

Выводы

Показано, что расширение автономности ИИ-агентов, интегрируемых в ТКС СН ФОИВ, формирует новый класс угроз безопасности, специфичных для систем на основе больших языковых моделей. Разработана шестидоменная модель угроз, систематизированная в соответствии с классификацией ФСТЭК России и банком данных угроз безопасности информации, что позволило сопоставить каждый домен риска с конкретными угрозами БДУ и тактиками их реализации, аналогичными тактикам MITRE ATT&CK. Обоснована целесообразность нивелирования выявленных тактик двумя взаимодополняющими моделями безопасности — AgentGuardian, реализующей контекстно-зависимое управление доступом на уровне вызываемых

инструментов, и архитектурой нулевого доверия, обеспечивающей изоляцию агента на уровне инфраструктуры, — каждая из которых противодействует определенному набору тактик атак. Показано, что практическая реализация указанных моделей в ТКС СН ФОИВ требует соблюдения требований Федеральных законов, применения в случае необходимости сертифицированных средств криптографической защиты информации в соответствии с рекомендациями ФСБ России и построения частной модели угроз в соответствии с методикой ФСТЭК России. Научная новизна работы заключается в сквозной увязке угроз безопасности автономных ИИ-агентов, их систематизации в терминах официальной классификации ФСТЭК России, тактик нивелирования и технических моделей их практической реализации в единый непротиворечивый контур, применимый к условиям функционирования ЕИУП ФОИВ. Практическая значимость результатов заключается в возможности их использования при разработке регламентов безопасной эксплуатации ИИ-агентов в контуре ЕИУП ФОИВ. Направлениями дальнейших исследований являются разработка методики количественной оценки уровня доверия к ИИ-агентам и интеграция моделей AgentGuardian и Zero Trust с протоколами информационно-логического и технического сопряжения ТКС СН.

Список литературы

1. 1. Inan H., Upasani K., Chi J., Rungta R., Iyer K., Mao Y., Tontchev M., Hu Q., Fuller B., Testuggine D., Khabsa M. Llama Guard: LLM-based Input-Output Safeguard for Human-AI Conversations // arXiv:2312.06674 [cs.CL]. – 2023.
2. 2. Abaev N., Klimov D., Levinov G., Mimran D., Elovici Y., Shabtai A. AgentGuardian: Learning Access Control Policies to Govern AI Agent Behavior // arXiv:2601.10440 [cs.CR]. – 2026. – 14 p.
3. 3. Maiti S. Caging the Agents: A Zero Trust Security Architecture for Autonomous AI in Healthcare // arXiv:2603.17419 [cs.CR]. – 2026.
4. 4. Методический документ. Методика оценки угроз безопасности информации / утв. ФСТЭК России 05.02.2021.
5. 5. Банк данных угроз безопасности информации ФСТЭК России. Раздел «Угрозы безопасности информации систем искусственного интеллекта» [Электронный ресурс]. – URL: https://bdu.fstec.ru/threat/ai (дата обращения: 11.08.2026).
6. 6. ГОСТ Р 70569-2022. Информационные технологии. Интероперабельность. Термины и определения. – М.: Стандартинформ, 2022.
7. 7. Интероперабельность организационно-технических систем: Монография / С.И. Макаренко. – СПб.: Наукоемкие технологии, 2024. – 313 с.

Секция 1 – Системы, сети и устройства телекоммуникаций

УДК 550.388; 621.371; 621.396

Комплекс оценки пропускной способности канала спутниковой связи по данным ГНСС-зондирования ионосферы

Диптан П. А.

Северо-Кавказский Федеральный Университет, г. Ставрополь, Россия

Аннотация: *Разработана структура построения программно-аппаратного комплекса, позволяющего в автоматическом режиме оценивать пропускную способность канала спутниковой связи при возмущениях ионосферы с учетом возникновения общих и частотно-селективных замираний, межсимвольной интерференции. Комплекс включает совокупность специализированного двухчастотного приемника GPStation-6 глобальных навигационных спутниковых систем GPS/ГЛОНАСС и взаимосвязанных программных вычислительных модулей.*

Ключевые слова: *мелкомасштабные возмущения ионосферы, полное электронное содержание, пропускная способность, ионосферные мерцания, частотно-селективные замирания, межсимвольная интерференция, двухчастотный приемник, ГНСС-зондирование.*

Введение

Современные системы спутниковой связи (ССС) развиваются в направлении повышения надежности, качества обслуживания абонентов и эффективности использования частотного спектра [1, 2]. В настоящее время наметилась устойчивая тенденция к совмещению (интегрированию) систем спутниковой радиолокации, радионавигации (глобальных навигационных спутниковых систем (ГНСС)) и связи [3, 4].

Известно [5], что влияние частотно-селективных замираний (ЧСЗ) и межсимвольной интерференции (МСИ) на помехоустойчивость ССС заключается в изменении функциональной зависимости $P_{\text{ош}} = \psi\left(\overline{h^2}, \gamma^2\right)$ на более сложную $P_{\text{ош}} = \psi\left(\overline{h^2}, \gamma^2, \eta_{\text{ч}}, \eta_{\text{м}}\right)$, где коэффициенты $\eta_{\text{ч}} = \psi\left(F/F_{\text{к}}\right)$ и $\eta_{\text{м}} = \psi\left(1/T_s F_{\text{к}}\right)$ характеризуют проявление энергетических потерь при корреляционной обработке принимаемых сигналов, подверженных ЧСЗ и МСИ, h^2– отношение сигнал/шум на входе приемника ССС, γ^2–параметр Райса, характеризующий глубину замираний сигналов, T_s – длительность символа. При этом существенное увеличение уровней ЧСЗ ($F/F_{\text{к}}$) и МСИ ($1/T_s F_{\text{к}}$) принимаемых сигналов ССС *P*-диапазона (f_0=225…400 МГц) с заданными частотно-временными параметрами (f_0, F, T_s) будет наблюдаться в условиях сильных возмущений ионосферы, сопровождаемых возрастанием мелкомасштабных флуктуаций ($\sigma_{\Delta N_T}$) ПЭС ионосферы на несколько порядков и соответствующим сужением полосы когерентности замираний ($F_к \sim \frac{f_0^2}{\sigma_{\Delta N_T}}$) трансионосферного (спутникового) канала. Для устранения ЧСЗ и МСИ принимаемых сигналов

выбор ширины их спектра должен осуществляться на основе данных о текущих значениях ширины полосы когерентности $F_к$.

Для решения задачи прогнозирования помехоустойчивости ССС *P*-диапазона при ионосферных возмущениях разработан комплекс [6], который позволяет измерять мелкомасштабные флуктуации ПЭС ионосферы ($\sigma_{\Delta N_T}$) на основе метода ГНСС-зондирования в ГНСС и использовать эти результаты для прогнозирования вероятности ошибочного приема сигналов $P_{ош} = \psi\left(\overline{h^2}, \gamma^2(\alpha_С), \eta_ч(\alpha_С), \eta_м(\alpha_С)\right) = \psi\left(\overline{h^2}, f_0, F, T_S, \sigma_{\Delta N_T}(\alpha_н), \alpha_с\right)$, в ССС (где $\alpha_н$–угол наклона радиолинии ГНСС, $\alpha_с$–угол наклона радиолинии ССС).

Однако результаты прогнозирования $P_{ош}$ не выходят за пределы физического уровня (помехоустойчивости) и не рассматривают влияние общих, ЧСЗ и МСИ в каналах спутниковой связи на пропускную способность (на канальный уровень).

Вместе с тем, в работе [7] показано, что в условиях сильных ионосферных возмущений и выборе несущей частоты f_0=390 МГц, ширины спектра F=76,8 кГц сигналов, возникновении ЧСЗ и МСИ, пропускная способность канала спутниковой связи уменьшается на 65% (относительно случая отсутствия замираний в канале). Представляется необходимым расширить возможности программно-аппаратного комплекса с учетом оценки пропускной способности канала спутниковой связи.

Цель статьи: разработка структуры программно-аппаратного комплекса оценки пропускной способности канала спутниковой связи на основе результатов ГНСС-зондирования ионосферы.

Представленная работа является развитием исследований автора [6-18].

Возможности модификации приемника GPStation-6

В настоящее время для оценки ПЭС ионосферы (N_T) и его СКО ($\sigma_{\Delta N_T}$) применяются специализированные приемники ГНСС GPS/ГЛОНАСС класса GISTM (GNSS Ionospheric and TEC Monitor) [19].

В составе базового приемника GPStation-6 можно условно выделить две части:

1) аппаратную часть, включающую блок приема сигналов, осуществляющий аналого-цифровое преобразование, декодирование сигналов ГНСС и измерение их основных параметров: псевдодальностей (R_1', R_2') до космического аппарата (КА) ГНСС и псевдофаз (φ_1', φ_2') на двух несущих частотах (f_1, f_2);

2) программное обеспечение (ПО), реализующее обработку принятых навигационных сообщений ГНСС, вычисление значений радионавигационных параметров, координат приемника, ПЭС ионосферы и др., а также формирование сообщений содержащих результаты измерений.

Поскольку внесение изменений во встроенное ПО приемника невозможно, предложенная модификация состоит в разработке дополнительного ПО (программых блоков), которое на основе оценки помехоустойчивости приема

сигналов в трансионосферных каналах связи с различной глубиной общих замираний и степенью ЧСЗ и МСИ подробно рассмотренной в работе [6] последовательно реализует расчет пропускной способности канала спутниковой связи при возмущениях ионосферы.

Описанный подход позволяет расширить функциональность приемника путем разработки дополнительных программных модулей, функционирующих на отдельных вычислительных мощностях и потому не оказывающих влияния на работу встроенного ПО, непосредственная модификация которого недоступна.

Структура комплекса оценки пропускной способности канала спутниковой связи

С учетом известного [6] способа модификации GISTM-приемника GPStation-6 осуществить с его помощью оценку пропускной способности канала спутниковой связи при возмущениях ионосферы возможно путем разработки дополнительных блоков (программных модулей), позволяющих рассчитывать пропускную способность в соответствии с выражением

$$C(F) = F\left(1 + P_{\text{ош}}(F)\log_2 P_{\text{ош}}(F) + \left(1 - P_{\text{ош}}(F)\right)\log_2\left(1 - P_{\text{ош}}(F)\right)\right), \qquad (1)$$

где F – ширина полосы частот сигнала.

Для модификации GISTM-приемника GPStation-6 в состав его ПО необходимо ввести следующие блоки (программные модули):

1) блок расчета оптимальной ширины полосы частот F_{opt} (по критерию максимума пропускной способности) ($F=F_{opt}$);

2) блок расчета пропускной способности канала спутниковой связи в соответствии с выражением (1);

3) блок расчета максимальной пропускной способности канала спутниковой связи ($\max\limits_{F} C(\overline{h^2}, f_0, F, T_S, \sigma_{\Delta N_T}(\alpha_{\text{н}}), \alpha_{\text{с}})$).

На рис. 1 представлена структурная схема комплекса оценки пропускной способности канала спутниковой связи в условиях мелкомасштабных возмущений ионосферы на основе GPS-мониторинга мелкомасштабных флуктуаций ПЭС с помощью двухчастотного (ДЧ) приемника (ПРМ) GPStation-6. При этом радиолиния ГНСС на двух несущих частотах f_1 и f_2 проходит от космического аппарата (КА) ГНСС через мелкомасштабное ионосферное образование (МИО) под углом $\alpha_н < 90°$, а радиолиния ССС на отличной частоте $f_0 \neq (f_1, f_2)$ проходит от КА ССС до приемника (ПРМ) ССС через это же образование (то есть через одну и ту же подионосферную точку) под произвольным углом $\alpha_с \neq \alpha_н$.

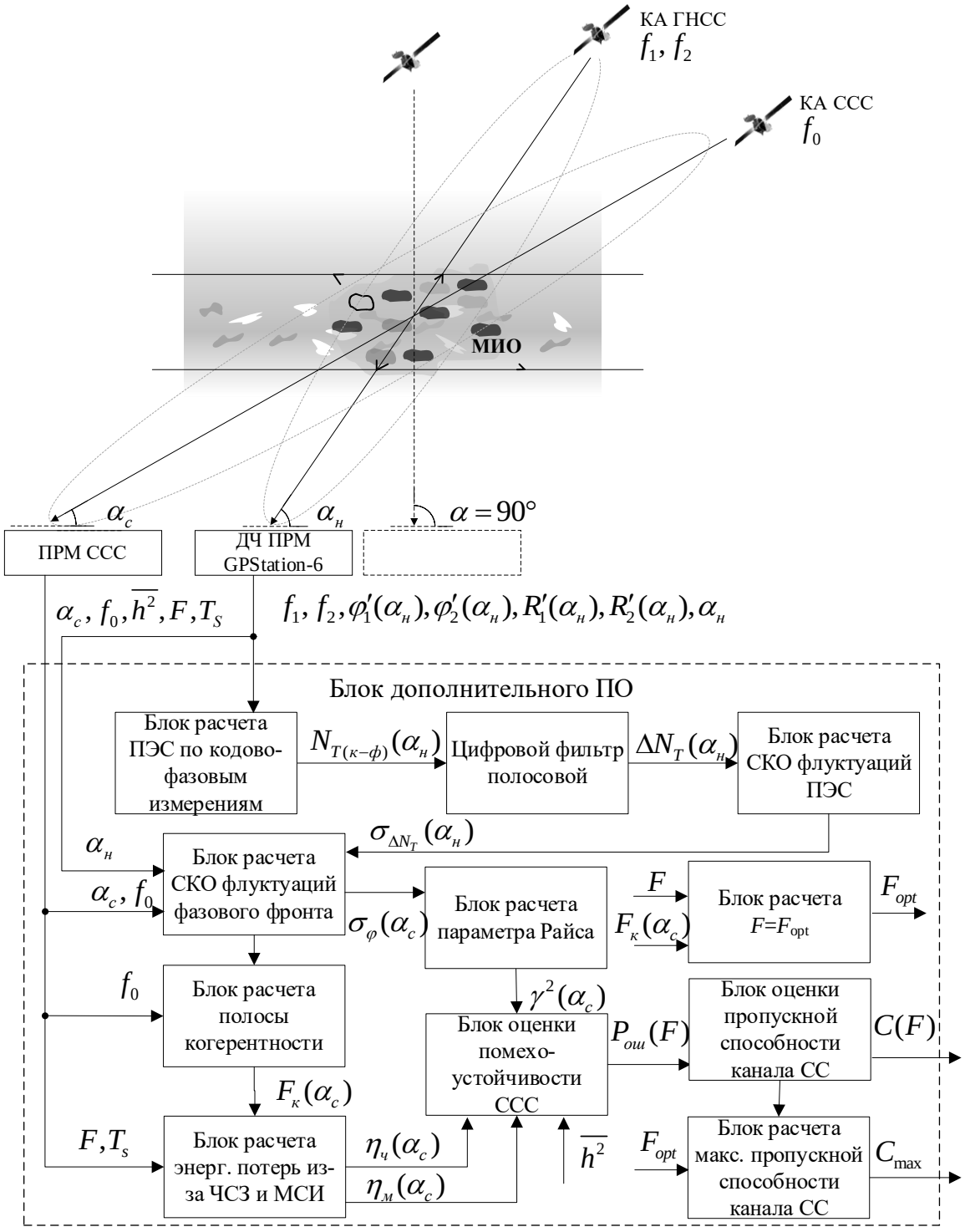


Рис. 1. Структурная схема комплекса оценки пропускной способности канала спутниковой связи по данным ГНСС-зондирования ионосферы

Таким образом, комплекс включает совокупность GISTM-приемника ГНСС GPS/ГЛОНАСС и взаимосвязанных программных модулей, реализующих функции вычисления ПЭС ионосферы, статистических характеристик его мелкомасштабных флуктуаций, полосы пропускания трансионосферного канала связи, помехоустойчивости и пропускной способности канала спутниковой

связи. Предложенный комплекс базируется на совокупности известных [6, 7] функциональных зависимостей, которые позволяют:

1) по сравнению со стандартным режимом работы приемника GPStation-6 оценить пропускную способность канала спутниковой связи при возмущениях ионосферы;

2) определить максимальную пропускную способность канала при возникновении частотно-селективных замираний и межсимвольной интерференции.

Заключение

Разработана структурная схема программно-аппаратного комплекса на базе специализированного двухчастотного приемника ГНСС GPS/ГЛОНАСС и взаимосвязанных дополнительных программных модулей.

Возможности входящего в состав комплекса приемника GPStation-6 существенно расширены за счет использования комбинации результатов кодовых и фазовых измерений, формируемых на входе приемника с увеличенной частотой дискретизации. Полученные результаты ГНСС-мониторинга ионосферы при ее возмущениях являются основой для оценки пропускной способности канала спутниковой связи, выбора ширины спектра частот передаваемого сигнала (F) в современных и перспективных системах спутниковой связи.

В дальнейшем планируется разработка методики определения оптимальной ширины спектра сигналов по критерию обеспечения максимальной пропускной способности многолучевых каналов связи на основе данных ГНСС-зондирования ионосферы.

Список литературы

1. Макаренко С. И. Системы спутниковой связи общего пользования и специального назначения. Монография. – СПб.: Наукоемкие технологии, 2025. – 222 с.

2. Воронин М. Ю., Бойченко И. А., Кривоклякин Т. К., Диптан П. А. Методический подход к обоснованию основных проектных параметров низкоорбитальной спутниковой системы связи с гибкой цифровой полезной нагрузкой с учетом влияния интерференции в абонентских лучах. // *Ural Radio Engineering Journal*. 2025. Т. 9. № 3. С. 299-315. DOI: 10.15826/urej.2025.9.3.004.

3. 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

4. Temiz M., Horne C., Peters N. J., Ritchie M. A., Masouros C. An experimental study of radar-centric transmission for integrated sensing and communications // IEEE Transactions on Microwave Theory and Techniques. 2023. Vol. 71. No. 7. P. 3203-3216. DOI: 10.1109/TMTT.2023.3234309

5. Пашинцев В. П. Модели трансионосферных радиоканалов и помехоустойчивость систем космической связи. Монография. – Москва; Вологда: Инфра-Инженерия, 2026. – 212 с.

6. Пашинцев В. П., Песков М. В., Михайлов Д. А., Диптан П. А. Прогнозирование помехоустойчивости системы спутниковой связи Р-диапазона при сильных возмущениях ионосферы // Журнал радиоэлектроники. – 2025. №. 12. https://doi.org/10.30898/16841719.2025.12.7

7. Пашинцев В. П., Диптан П. А., Белоконь Д. А. Методика прогнозирования пропускной способности канала спутниковой связи при мелкомасштабных возмущениях ионосферы, возникновении частотно-селективных замираний и межсимвольной интерференции // Системы управления, связи и безопасности. 2025. № 1. С. 156-186. DOI: 10.24412/2410-9916-2025-1-156-186.

8. Пашинцев В. П., Коваль С. А., Скорик А. Д., Диптан П. А. Комплекс оценки полосы пропускания трансионосферного канала связи на основе результатов GPS–мониторинга ионосферы. // В сборнике: Распространение радиоволн. Сборник докладов XXVIII Всероссийской открытой научной конференции. Йошкар-Ола, 2023. С. 164–167.

9. Пашинцев В. П., Скорик А. Д., Диптан П. А., Ткачев М. А. Оценка влияния дисперсионных и дифракционных свойств ионосферы на полосу пропускания трансионосферного канала связи. // В сборнике: Распространение радиоволн. Сборник докладов XXVIII Всероссийской открытой научной конференции. Редколлегия: Д.С. Лукин, Д.В. Иванов, Н.В. Рябова [и др.]. Йошкар-Ола, 2023. С. 168–171.

10. Диптан П. А. Алгоритм оценки пропускной способности спутникового канала связи с замираниями // Студенческая наука – для развития информационного общества: сборник научных трудов по материалам XIV Всероссийской научно-технической конференции (Ставрополь, 18 мая 2023 г.). Ставрополь: Северо-Кавказский федеральный университет, 2023. С. 124–127.

11. Диптан П. А., Гринев Е. М. Алгоритм оценки пропускной способности спутникового канала связи с частотно–селективными замираниями, межсимвольной интерференцией, дисперсионными искажениями. // Современные технологии обработки сигналов: сборник научных трудов по материалам четвертой Всероссийской конференции (Москва, 12 – 13 декабря 2023 г.). Москва. (СТОС–2023, РНТОРЭС им. А.С. Попова), 2023. С. 81-85.

12. Пашинцев В. П., Диптан П. А., Гринев Е. М., Киселев Н. В. Методика оценки пропускной способности спутникового канала связи с замираниями // Системы управления, связи и безопасности. 2023. № 4. С. 243-266. DOI: 10.24412/2410-9916-2023-4-243-266.

13. Пашинцев В. П., Диптан П. А., Гринев Е. М., Белоконь Д. А., Киселев Н. В. Пропускная способность спутникового канала связи с частотно-селективными замираниями и межсимвольной интерференцией. // В сборнике: Радиоэлектронные устройства и системы для инфокоммуникационных

технологий (РЭУС-ИТ 2024). Доклады всероссийской конференции, посвященной «Дню Радио». Москва, 2024. С. 208-213.

14. Пашинцев В. П., Диптан П. А., Белоконь Д. А., Назаренко Е. М. Влияние мелкомасштабных возмущений ионосферы на пропускную способность канала спутниковой связи *P*-диапазона частот. // Радиолокация, навигация, связь: сборник трудов XXXI Международной научно-технической конференции (г. Воронеж, 15–17 апреля 2025 г.): в 6 томах. / Воронежский государственный университет; АО «Концерн Созвездие». – Воронеж: Издательский дом ВГУ, 2025. т. 2. С 229-237.

15. Пашинцев В. П., Гринев Е. М., Диптан П. А., Белоконь Д. А. Оценка погрешности определения интенсивности неоднородностей при сильных возмущениях ионосферы // СВЧ-техника и телекоммуникационные технологии. 2025. № 7. С. 245-246

16. Пашинцев В. П., Гринев Е. М., Диптан П. А. Область применимости приближенной формулы оценки интенсивности мелкомасштабных неоднородностей в сильно возмущенной ионосфере // Известия института инженерной физики. 2025. № 4 (78). С. 16-19.

17. Пашинцев В. П., Гринев Е. М., Диптан П. А., Белоконь Д. А. Оценка интенсивности мелкомасштабных неоднородностей ионосферы при сильных ее возмущениях // доклады XLIV Всероссийской научно-технической конференции, филиал ВА РВСН (г. Серпухов). 2025. № 7. С. 198-201.

18. Пашинцев В. П., Диптан П. А., Гринев Е. М., Белоконь Д. А. Пропускная способность канала спутниковой связи с цифровыми видами модуляции при мелкомасштабных возмущениях ионосферы // Известия института инженерной физики. 2026. № 2 (80). С. 25-29.

19. Novatel Inc. GPStation-6. GNSS Ionospheric Scintillation and TEC Monitor (GISTM) Receiver User Manual. 2012. 89 p. [Электронный ресурс]. 21.06.2026 – URL: https://hexagondownloads.blob.core.windows.net/public/Novatel/assets/Documents/Manuals/om-20000132/om-20000132.pdf (дата обращения 21.06.2026).

УДК 550.388; 621.371; 621.396

Анализ методов оценки угла прихода сигнала в задачах локального позиционирования

Чижов А. С.

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

ПАО «Интелтех», г. Санкт-Петербург, Россия

***Аннотация**: Систематизированы методы оценки угла прихода радиосигнала, применяемые в системах локального позиционирования. Изложены физические основы фазовых и амплитудных измерений, приведены расчётные соотношения классических алгоритмов диаграммообразования и подпространственных алгоритмов сверхразрешения, а также современных подходов, основанных на разреженном представлении наблюдения, обучаемых моделях и перепрограммируемых отражающих поверхностях. Выполнено сопоставление методов по разрешающей способности, вычислительным затратам и устойчивости к когерентной многолучёвости, рассмотрены совмещённые измерительные схемы, сформулированы нерешённые задачи.*

***Ключевые слова:** угол прихода сигнала, антенная решётка, подпространственные методы, сверхразрешение, многолучёвость, локальное позиционирование.*

Введение

Локальным позиционированием называют определение координат подвижного объекта в пределах здания, производственного помещения или иного ограниченного пространства, где сигналы глобальных спутниковых систем недоступны либо существенно ослаблены. Построение таких систем опирается на измерение одного из четырёх первичных параметров принятого колебания: времени прихода (Time Of Arrival, ToA), разности времён прихода (Time Difference Of Arrival, TDoA), уровня принимаемого сигнала (Received Signal Strength, RSS) и угла прихода сигнала (Angle Of Arrival, AoA).

Угломерный подход не требует согласования шкал времени подвижного объекта и опорных точек, поскольку оценка направления формируется по разности фаз колебаний в пределах одной приёмной позиции. Для определения координат на плоскости достаточно двух опорных точек с известными координатами, а в совмещённых схемах — одной. Платой за это служат необходимость наличия антенной решётки, а также чувствительность к многолучевости. Сопоставление алгоритмов оценки направления составляет предмет обширного круга исследований [1–3] и существенно зависит от принятой модели наблюдения и от структуры решётки.

Практический интерес к угломерным методам возрос в связи с включением процедуры определения направления в спецификацию Bluetooth версии 5.1 и развитием беспроводных сенсорных сетей, систем «интернета вещей» и мобильной робототехники [4].

Цель статьи — систематизировать методы оценки угла прихода и выявить нерешённые задачи.

Физические принципы измерения угла прихода

Фазовый метод. Пусть на линейную эквидистантную решётку (рис. 1) из M приёмных элементов с шагом d падает плоская волна с длиной волны λ под углом θ, отсчитываемым от нормали к оси решётки. Разность хода между соседними элементами равна $d\sin\theta$, чему соответствует набег фазы

$$\Delta\varphi = \frac{2\pi d \sin\theta}{\lambda}. \quad (1)$$

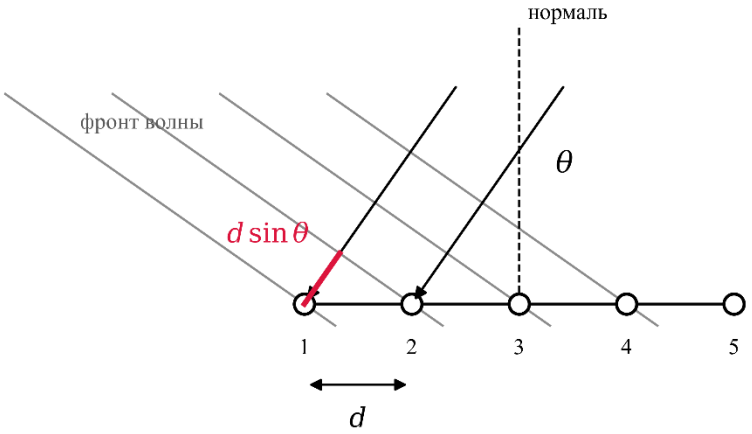


Рис. 1. Геометрия приёма плоской волны линейной эквидистантной антенной решёткой

Оценка угла производится согласно:

$$\hat{\theta} = \arcsin\left(\frac{\lambda\Delta\varphi}{2\pi d}\right). \quad (2)$$

Поскольку измерение фазы однозначно лишь в пределах интервала протяжённостью 2π, условие однозначности оценки во всём секторе обзора имеет вид

$$d \le \frac{\lambda}{2}. \quad (3)$$

Дифференцирование (2) даёт закон переноса погрешности: среднеквадратическое отклонение оценки угла связано с погрешностью измерения фазы соотношением

$$\sigma_\theta = \frac{\lambda\sigma_\varphi}{2\pi d\cos\theta}. \quad (4)$$

Точность падает при увеличении угла отклонения от нормали и повышается с ростом апертуры. Фазовый принцип применяется и в дальномерных задачах узкополосных систем, где измерения проводятся на наборе несущих частот [5].

Амплитудный метод. Здесь используется не фаза, а различие уровней сигнала, принятого антеннами с разными диаграммами направленности. Две антенны (либо два луча одной решётки) ориентируют так, чтобы их диаграммы $F_1(\theta)$ и $F_2(\theta)$ частично перекрывались и располагались симметрично относительно некоторого направления. В этом направлении обе антенны принимают одинаково, поэтому его называют равносигнальным; при отклонении источника в одну сторону уровень на первой антенне растёт, а на второй падает, при отклонении в другую — наоборот. Мерой отклонения служит нормированная разность откликов

$$u(\theta) = \frac{F_1(\theta) - F_2(\theta)}{F_1(\theta) + F_2(\theta)}. \quad (5)$$

Функция $u(\theta)$ монотонна в окрестности равносигнального направления, что даёт однозначную характеристику преобразования. Предельным упрощением этого подхода является измерение уровня сигнала при последовательном переключении между несколькими фиксированными лучами: приёмник поочерёдно подключается к антеннам, ориентированным в разные стороны, и направление определяется по тому, какой луч дал наибольший уровень, а также по соотношению уровней соседних лучей [6]. Решение требует минимума оборудования — одного приёмного тракта и коммутатора, — но даёт грубую оценку и сильно зависит от условий распространения, поскольку принятый уровень меняется не только от направления, но и от расстояния, и от препятствий.

Алгоритмы обработки информации в задачах оценки угла прихода сигнала

Наблюдение на выходах элементов решётки при воздействии K источников описывается моделью:

$$x(t) = A(\theta)s(t) + n(t), \qquad t = 1,\ldots,N, \quad (6)$$

где $x(t)$ — вектор комплексных огибающих размерности M; $s(t)$ — вектор сигналов источников; $n(t)$ — вектор шума; $A(\theta) = [a(\theta_1), \ldots, a(\theta_k)]$ — матрица направляющих векторов, элементы которой для линейной эквидистантной решётки имеют вид

$$a(\theta) = \left[1, e^{-j2\pi d \sin\theta/\lambda}, \ldots, e^{-j2\pi(M-1)d\sin\theta/\lambda}\right]^T. \quad (7)$$

Основой всех рассматриваемых алгоритмов служит корреляционная матрица наблюдения и её выборочная оценка:

$$R = \mathbb{E}\{x(t)x^H(t)\} = AR_sA^H + \sigma^2 I_M, \quad \hat{R} = \frac{1}{N}\sum_{t=1}^{N} x(t)x^H(t). \quad (8)$$

Диаграммообразование по Бартлетту соответствует согласованной пространственной фильтрации и даёт оценку углового распределения мощности:

$$P_B(\theta) = \frac{a^H(\theta)\hat{R}a(\theta)}{a^H(\theta)a(\theta)}. \quad (9)$$

Разрешающая способность (5) ограничена шириной главного лепестка, то есть величиной порядка $\lambda/(M_d)$, и не улучшается с ростом времени наблюдения.

Метод минимальной дисперсии без искажений (Кейпона) минимизирует выходную мощность при единичной передаче в направлении θ:

$$P_C(\theta) = \frac{1}{a^H(\theta)\hat{R}^{-1}a(\theta)}. \quad (10)$$

Подпространственные методы используют разложение корреляционной матрицы по собственным векторам с разделением на сигнальное и шумовое подпространства:

$$R = U_s \Lambda_s U_s^H + \sigma^2 U_n U_n^H. \quad (11)$$

Ортогональность направляющих векторов шумовому подпространству порождает алгоритм классификации множественных сигналов (алгоритм MUSIC):

$$P_{MUSIC}(\theta) = \frac{1}{a^H(\theta) U_n U_n^H a(\theta)}. \quad (12)$$

Направления θ определяются пиками псевдоспектра (7)

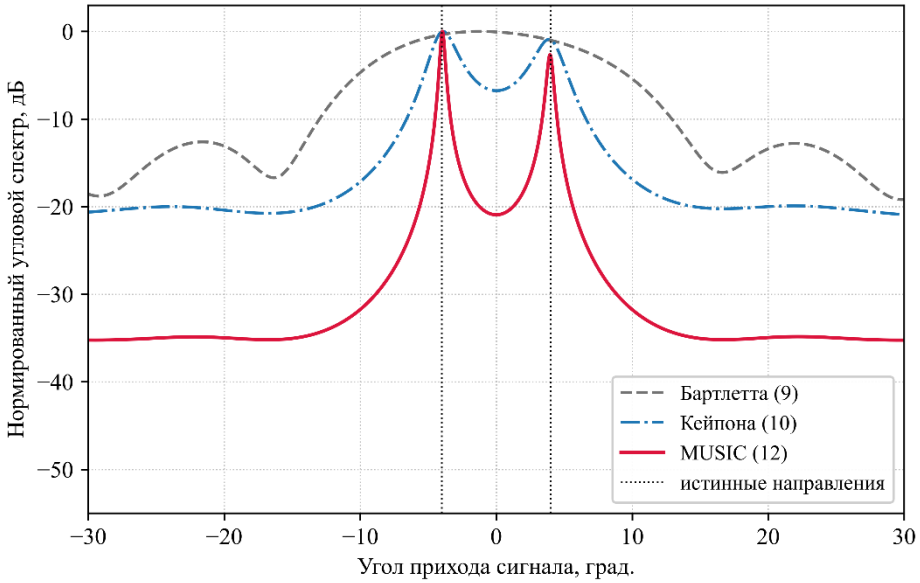


Рис. 2. Угловые спектры Бартлетта, Кейпона и MUSIC для двух некоррелированных источников с угловыми координатами −4° и +4°: M = 10, $d = \lambda/2$, отношение сигнал/шум 10 дБ, N = 200 выборок

Корневая модификация (Root-MUSIC) заменяет поиск максимумов (10) отысканием корней полинома, что устраняет погрешность дискретизации угловой сетки и снижает затраты на выполнение алгоритма:

$$p(z) = z^{M-1} a^T(z^{-1}) U_n U_n^H a(z). \quad (13)$$

Метод оценивания параметров по вращательной инвариантности (ESPRIT). Решётку мысленно разбивают на две одинаковые части — подрешётки, совпадающие по форме и сдвинутые одна относительно другой на вектор Δ. Для линейной эквидистантной решётки такими частями служат, например, первые $M - 1$ и последние $M - 1$ элементов, и тогда Δ равен шагу решётки. Обозначим через A_1 и A_2 те части матрицы направляющих векторов,

которые относятся к первой и второй подрешёткам, то есть составлены из соответствующих строк матрицы $A(\theta)$. Поскольку подрешётки одинаковы, а на вторую волна приходит с постоянным запаздыванием, эти части различаются только фазовым множителем, своим для каждого источника:

$$A_2 = A_1\Phi, \quad \Phi = diag\left(e^{j\mu_1},\ldots,e^{j\mu_K}\right), \quad \mu_k = \frac{2\pi\Delta\sin\theta_k}{\lambda}. \tag{14}$$

Оценка матрицы поворота по методу наименьших квадратов и последующий переход к углам дают

$$\Psi = \left(U_1^H U_1\right)^{-1} U_1^H U_2, \qquad \hat{\theta}_k = \arcsin\left(\frac{\lambda\arg(\gamma_k)}{2\pi\Delta}\right), \tag{15}$$

где γ_k — собственные числа матрицы Ψ. Модификация по полной невязке (TLS-ESPRIT) учитывает погрешности в обоих блоках и обеспечивает состоятельность оценки при конечном числе выборок. В отличие от (6), алгоритм не требует сканирования по углу, но нуждается в строгой геометрической инвариантности подрешёток. Принцип вращательной инвариантности переносится и на совместное оценивание нескольких параметров [7]. Разрешающая способность этих методов зависит и от геометрии решётки. Неэквидистантные структуры, в частности взаимно простые, при том же числе элементов увеличивают действующую апертуру и число разрешаемых источников [8].

Современные методы оценки угла прихода сигнала

Методы разреженного восстановления. Сектор обзора разбивается на плотную сетку из G направлений каждое такое значение далее называется узлом сетки. Это позволяет представить наблюдение в виде $x = \tilde{A}\,\gamma + n$, где $\tilde{A}$ — словарь направляющих векторов, а вектор γ содержит не более K ненулевых элементов. Оценка находится как решение задачи

$$\gamma = \arg\min_{\gamma} \| \gamma \|_1 \quad при \quad \| x - A\gamma \|_2 \le \varepsilon. \tag{16}$$

Данный метод не требует априорного знания числа источников, работоспособен при одной выборке и устойчив к когерентности сигналов, что делает его предпочтительным для разреженных сверхбольших апертур [9]. Ограничением служит несогласованность истинного направления с узлами сетки. Вычислительные затраты алгоритмов данного метода снижают понижением ранга и попеременной оптимизацией базиса [10].

Обучаемые модели. Оценка направления трактуется как задача восстановления зависимости $\theta = f(z)$, где z — признаковое описание наблюдения, выборочная корреляционная матрица, её собственные векторы либо квадратурные составляющие. Параметры модели определяются минимизацией эмпирического риска по обучающей выборке объёмом P:

$$W = \arg\min_W \frac{1}{P}\sum_{p=1}^{P} \mathrm{L}\left(f_W(z_p), \theta_p\right) \tag{17}$$

Достоинство подхода — перенос вычислительных затрат на этап обучения и неявный учёт отражений от известной обстановки; недостаток — зависимость качества от представительности выборки и слабая переносимость на изменённую обстановку.

Перепрограммируемые отражающие поверхности создают управляемый дополнительный путь распространения и тем самым формируют искусственную опорную позицию с известными координатами. Погрешности угловых оценок в таких системах, как правило, не подчиняются нормальному закону, вследствие чего обычный взвешенный метод наименьших квадратов даёт смещённую оценку координат. Здесь требуется раздельный учёт статистики угловых и временных измерений [11].

Проблемы практического применения

Многолучёвость. Отражения от строительных конструкций порождают дополнительные волновые фронты, коррелированные с прямым лучём. При полной когерентности матрица R_s вырождается, размерность сигнального подпространства становится меньше числа источников, и разложение (5) теряет смысл. Ранг восстанавливают пространственным сглаживанием по L перекрывающимся подрешёткам:

$$\overline{R} = \frac{1}{L}\sum_{l=1}^{L} R_l \,. \tag{18}$$

Данная процедура уменьшает действующую апертуру и, следовательно, разрешающую способность.

Модель (7) предполагает идентичность приёмных каналов и точное знание координат элементов. Различия коэффициентов передачи и фазовых сдвигов, а также взаимное влияние элементов смещают оценки, причём для подпространственных методов смещение возрастает быстрее, чем для диаграммообразующих.

Методы (12)–(15) предполагают известным число K. Информационные критерии асимптотичны и при малом числе выборок дают завышенные оценки. Байесовская постановка позволяет получить число источников по максимуму апостериорной вероятности и превосходит асимптотические критерии на малых выборках [13]. Отклонение шума от белого нормального требует обеления либо устойчивых оценок корреляционной матрицы.

Сравнительная характеристика методов оценки угла прихода сигнала

Предельно достижимая точность несмещённой оценки направления для одного источника при линейной эквидистантной решётке определяется границей Крамера — Рао (рис. 3). Она определяется выражением:

$$\mathrm{CRB}(\theta) = \frac{6}{N\,q\,M\,(M^2-1)}\left(\frac{\lambda}{2\pi d\cos\theta}\right)^2, \tag{19}$$

где q — отношение мощности сигнала к мощности шума на выходе элемента антенной решетки. Из данного выражение следует кубическая зависимость дисперсии от числа элементов, что объясняет целесообразность наращивания апертуры антенной решетки. Сводные характеристики методов приведены в таблице 1.

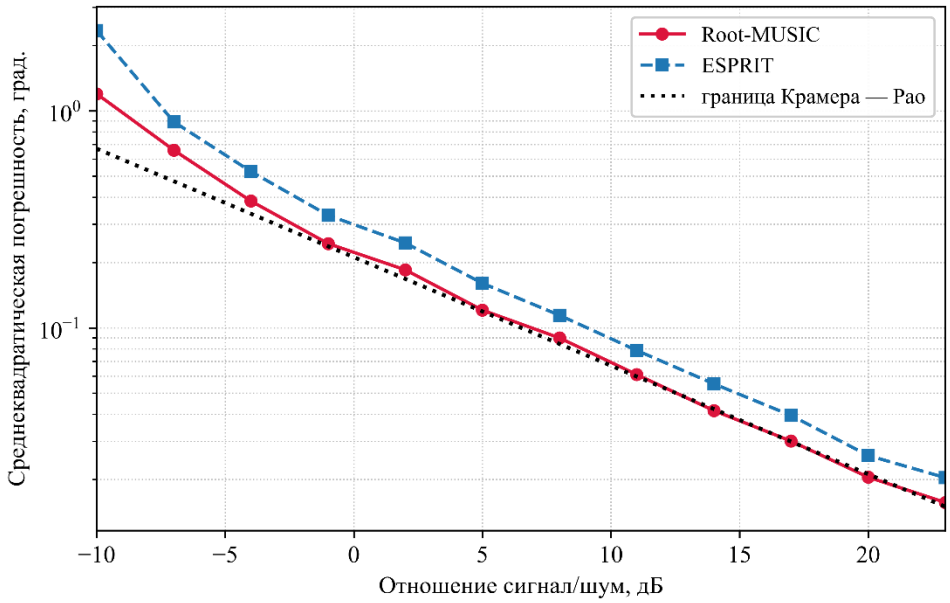


Рис. 3. Среднеквадратическая погрешность оценки угла корневым методом MUSIC и методом ESPRIT, в сопоставлении с границей Крамера — Рао $M = 8$, $d = \lambda/2$, $\theta = 20°$, $N = 100$ выборок, 500 повторений

Таблица 1 – Сравнительная характеристика методов оценки угла прихода сигнала

Метод	**Разрешающая способность**	**Вычислительная сложность**	**Устойчивость к когерентным сигналам**	**Априорное знание числа источников**
Бартлетта	ограничена шириной луча	$O(M^2G)$	высокая	не требуется
Кейпона (МДБО)	средняя	$O(M^3 + M^2G)$	низкая	не требуется
MUSIC	высокая	$O(M^3 + M(M - K)G)$	низкая без сглаживания	требуется
Root-MUSIC	высокая	$O(M^3)$	низкая без сглаживания	требуется
ESPRIT (по полной невязке)	высокая	$O(M^3)$	низкая без сглаживания	требуется

Метод	**Разрешающая способность**	**Вычислительная сложность**	**Устойчивость к когерентным сигналам**	**Априорное знание числа источников**
Разреженное восстановление	очень высокая	O(итер. × MG)	высокая	не требуется
Обучаемые модели	зависит от обучения	O(M^3) при обучении, малая при работе	высокая при представительной выборке	не требуется

Здесь M — число элементов решётки, K — число источников, G — число точек угловой сетки. Оценки вычислительно сложности приведены без учёта затрат на накопление корреляционной матрицы.

Совмещённые схемы позиционирования

Переход от оценок направления к координатам сводится к пересечению линий положения. При наличии I опорных пунктов с координатами $(x_i,\ y_i)$ и полученных для них оценок направлений θ_i искомая точка удовлетворяет системе

$$(x - x_i)\sin\theta_i - (y - y_i)\cos\theta_i = 0, \qquad i = 1, \ldots, I. \tag{20}$$

Каждое уравнение в 21 задаёт прямую, проходящую через соответствующую опорную точку под измеренным углом. При точных измерениях эти прямые пересекаются в одной точке, при наличии погрешностей система становится несовместной, и её приводят к виду $Hp = b$, решая взвешенным методом наименьших квадратов:

$$\hat{p} = (H^T W H)^{-1} H^T W b. \tag{21}$$

Матрица весов W строится по дисперсиям угловых оценок и тем самым понижает вклад направлений, полученных при малом отношении сигнал/шум либо при больших углах отклонения от нормали, — согласно (4) именно они наименее точны. Обусловленность системы определяется взаимным расположением опорных точек и объекта: при малом угле пересечения линий положения погрешность координат многократно превосходит погрешность углов, поэтому выбор состава опорных точек составляет самостоятельную задачу оптимизации [14]. Реализация такой схемы по двум и более приёмным позициям рассмотрена в [15].

Число необходимых опорных точек сокращается при совмещении угловых измерений с измерениями иной природы. Пара угол-дальность, полученная от одного и того же пункта, полностью определяет положение объекта на плоскости:

$$x = x_1 + r\cos\theta_1, \qquad y = y_1 + r\sin\theta_1.$$

Совмещение с разностно-дальномерными измерениями снижает геометрический фактор ухудшения точности: линии положения различной формы — прямые и гиперболы — пересекаются под большими углами, чем однотипные. Совмещение с измерениями уровня сигнала заметного выигрыша

в точности не даёт и оправдано лишь как средство грубого разрешения неоднозначности.

Выводы и нерешённые задачи

Диаграммообразующие методы сохраняют значение как вычислительно нетребовательные и устойчивые к когерентности процедуры, пригодные для встраиваемых устройств. Подпространственные методы обеспечивают сверхразрешение ценой знания числа источников и предварительной декорреляции. Разреженное восстановление и обучаемые модели снимают часть этих ограничений, но переносят трудность на выбор словаря и формирование обучающей выборки. К нерешённым задачам следует отнести:

− устойчивое оценивание числа источников при малом объёме выборки;

− автоматическую калибровку решётки в условиях эксплуатации;

− учёт негауссовской статистики угловых погрешностей при вычислении координат;

− согласование разреженного представления с непрерывной областью значений угла;

− перенос обучаемых моделей между помещениями без повторного обучения.

Отдельного исследования заслуживает совместная обработка угловых и частотно-временных измерений в системах с многочастотными сигналами.

Список литературы

1. Lavate T., Kokate V., Sapkal A. Performance analysis of MUSIC and ESPRIT DOA estimation algorithms for adaptive array smart antenna in mobile communication // Second International Conference on Computer and Network Technology (ICCNT). — IEEE, 2010. — URL: https://ieeexplore.ieee.org/document/5474488 (дата обращения: 06.08.2026).

2. Comparative performance analysis of MUSIC and ESPRIT on ULA // IEEE Conference Publication. — URL: https://ieeexplore.ieee.org/document/6450560/ (дата обращения: 06.08.2026).

3. Oumar O., Siyau M., Sattar T. Performance comparison of MUSIC and ESPRIT algorithms in presence of coherent signals for DoA estimation // IEEE. — URL: https://ieeexplore.ieee.org/abstract/document/8212844/ (дата обращения: 06.08.2026).

4. Angle-of-arrival estimation for localization and communication in wireless networks. — URL: https://www.researchgate.net/publication/255056341 (дата обращения: 06.08.2026).

5. Sheikh A., Romme J., Govers J., Farsaei A., Bachmann C. Phase-based ranging in narrowband systems with missing/interfered tones // IEEE Internet of Things Journal. — 2023. — Vol. 10, № 17. — P. 15171–15185.

6. Angle of arrival estimation algorithms using received signal strength indicator. — URL: https://www.researchgate.net/publication/298712266 (дата обращения: 06.08.2026).

7. Wu Y., Leshem A., Jensen J. R., Liao G. Joint pitch and DOA estimation using the ESPRIT method // IEEE/ACM Transactions on Audio, Speech, and Language Processing. — 2015. — Vol. 23, № 1. — P. 32–45.

8. Performance analysis of MUSIC and ESPRIT algorithms for direction-of-arrival estimation on coprime arrays. — URL: https://www.researchgate.net/publication/394754775 (дата обращения: 06.08.2026).

9. Hu Y., Xiao X., Jones S., Sun S. Single-snapshot localization using sparse extremely large aperture arrays. — 2025. — arXiv:2509.17511.

10. Cai Y., Qiu L., de Lamare R. C., Zhao M. Efficient reduced-rank DOA estimation algorithms using alternating low-rank decompositions. — 2016. — arXiv:1604.04321.

11. Wu T., Ren H., Pan C., Pan Y., Hong S., Elkashlan M., Shu F., Wang J. RIS-aided localization algorithm and analysis: tackling non-Gaussian angle estimation errors. — arXiv:2208.07606.

12. Wielandt S., De Strycker L. Indoor multipath assisted angle of arrival localization // Sensors. — 2017. — Vol. 17, № 11. — Art. 2522. — DOI: 10.3390/s17112522.

13. Tran V. H., Wang W. Bayesian inference for PCA and MUSIC algorithms with unknown number of sources. — 2018. — arXiv:1809.10168.

14. Van der Vorst T. [et al.] Anchor selection in angle-of-arrival estimation-based localization using polynomial chaos expansions. — 2020. — URL: https://www.researchgate.net/publication/342583050 (дата обращения: 06.08.2026).

15. Agrawal A. K. Localization using angle-of-arrival triangulation // International Workshop on Environmental Sensing Systems for Smart Cities (EnvSys ’25). — ACM, 2025. — arXiv:2508.16908.

УДК 621.39

Технология интеллектуального мониторинга состояния информационно-телекоммуникационных сетей и систем

Будко Н. П.

ПАО «Интелтех», г. Санкт-Петербург, Россия

Аннотация: *представлен подход к созданию технологии интеллектуального мониторинга состояния информационно-телекоммуникационных сетей и систем общего пользования, охватывающей технические (в виде патентов на изобретения и полезные модели, представленные схемной реализацией устройств и систем), технологические (в виде патентов на изобретения, представленные способами) и программные (в виде зарегистрированных программ для электронно-вычислительных машин и баз данных) решений.*

Ключевые слова: *диспетчерский уровень, информационно-телекоммуникационная сеть, сенсорный уровень, телекоммуникационный уровень, технология интеллектуального мониторинга.*

Введение

В исследовании предложен подход к формированию технологии интеллектуального мониторинга состояния информационно-телекоммуникационных сетей и систем (ИТКС) общего пользования (ОП) [1]. При этом под технологией понимается совокупность способов, правил, приемов, операций, средств, инструментов, ресурсов, режимов и этапов работы [2] с целью решения задач интеллектуального мониторинга состояния элементов ИТКС с использованием агентного подхода [3] сбора и обработки телеметрической информации в интересах идентификации вида состояния [4] и принятия управленческого решения по результатам мониторинга.

Технология интеллектуального мониторинга состояния ИТКС

В технологию вошли авторские технические и технологические решения, представленные на рис. 1, а также некоторые другие программные решения, позволяющие сформировать способ интеллектуального мониторинга состояния ИТКС ОП [5] и синтезировать систему, ее реализующую [6] на сенсорном, телекоммуникационном и диспетчерском уровнях сетевого мониторинга.

Сущность технологии состоит в сборе, накоплении и интеллектуальном анализе измерительной информации (ИИ) о состоянии сетевых элементов в виде устройств, узлов, каналов, маршрутов, подсетей, соответственно на аппаратном (сенсорном), канальном (телекоммуникационном) и структурном (диспетчерском) уровнях ИТКС. При этом происходит выявление их аномального состояния с передачей в систему поддержки принятия решения (СППР) ситуационного центра управления (СЦУ) расчетных значений достаточности используемых ресурсов каждого уровня для предотвращения аварийных режимов работы

путем регулировки параметров сетевых элементов либо их замены на резервные с наращиванием сетевой инфраструктуры при деградации ИТКС.

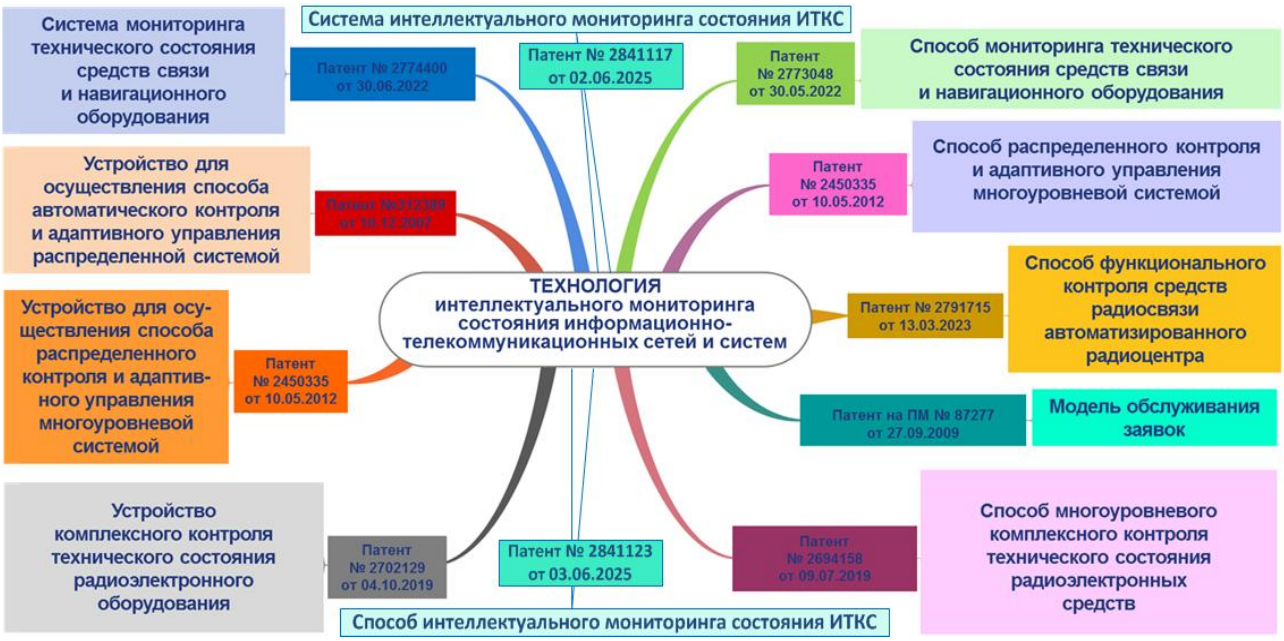


Рис. 1. Технология интеллектуального мониторинга состояния информационно-телекоммуникационных сетей и систем

Способ интеллектуального мониторинга состояния ИТКС и система, его реализующая

Технология интеллектуального мониторинга состояния ИТКС ОП по недопущению ее деградации сетевых элементов основана на применении способа интеллектуального мониторинга [5] и системы, его реализующей [6]. При этом названный способ состоит из нескольких этапов, рис. 2:

– предварительного этапа с заданием исходных данных мониторинга;

– первого этапа с формированием контура наблюдения и сбором ИИ от сетевых устройств, соединений и структур распределенной сети, а также передачу ее от серверов мониторинга сети к серверам СЦУ;

– второго этапа, на котором осуществляют оценку техническое состояние сетевых элементов в серверах СЦУ по оценке надежности, помехоустойчивости и живучести (связности) сети;

– третьего этапа, в ходе которого формируется контур управления сетевыми элементами путем перераспределения локальных параметрических (регулировка параметров сетевых устройств), телекоммуникационных (корректировка уровней передачи в трактах и каналах связи), а также структурных (изменение маршрутов передачи) ресурсов сети. При недостаточности локальных ресурсов задействуются дополнительные аппаратные (резерв устройств сети), канальных (резерв каналов связи) и

топологических (переход на другую топологию: звезда, шина, кольцо и пр.) ресурсов сети;

– завершающего этапа, на котором происходит актуализация базы состояния подсистемы мониторинга, прогноз состояния сетевых элементов с формированием всевозможных протоколов и отчетов, а также синтеза «витрины данных» по текущему циклу мониторинга.

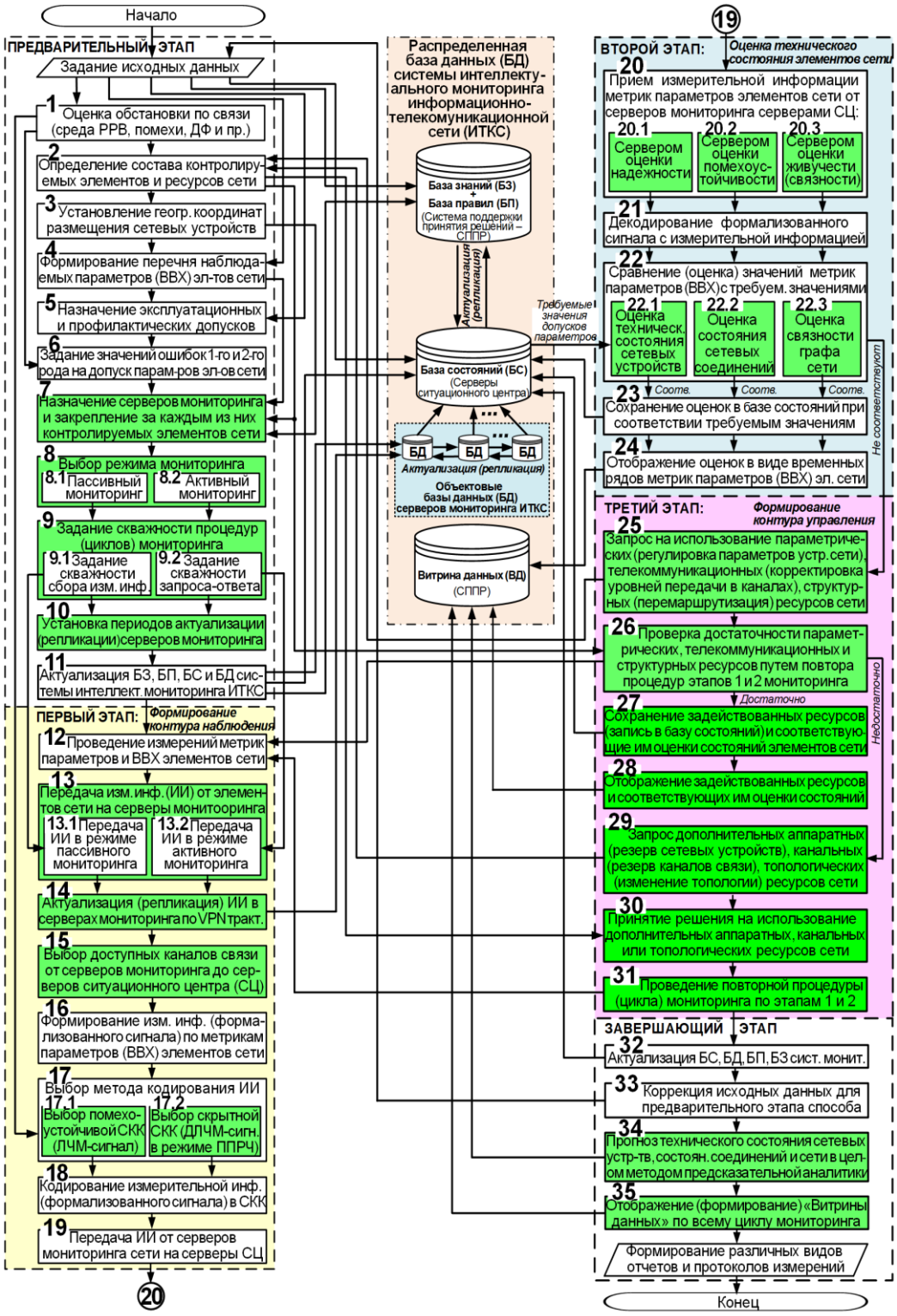


Рис. 2. Способ интеллектуального мониторинга состояния ИТКС ОП

Причем на рис. 2 зеленым цветом выделены новые блоки способа.

Предлагаемая технология интеллектуального мониторинга состояния ИТКС реализуется с помощью структуры системы интеллектуального мониторинга ИТКС [6], рис. 3 на основе мультиагентного подхода [3].

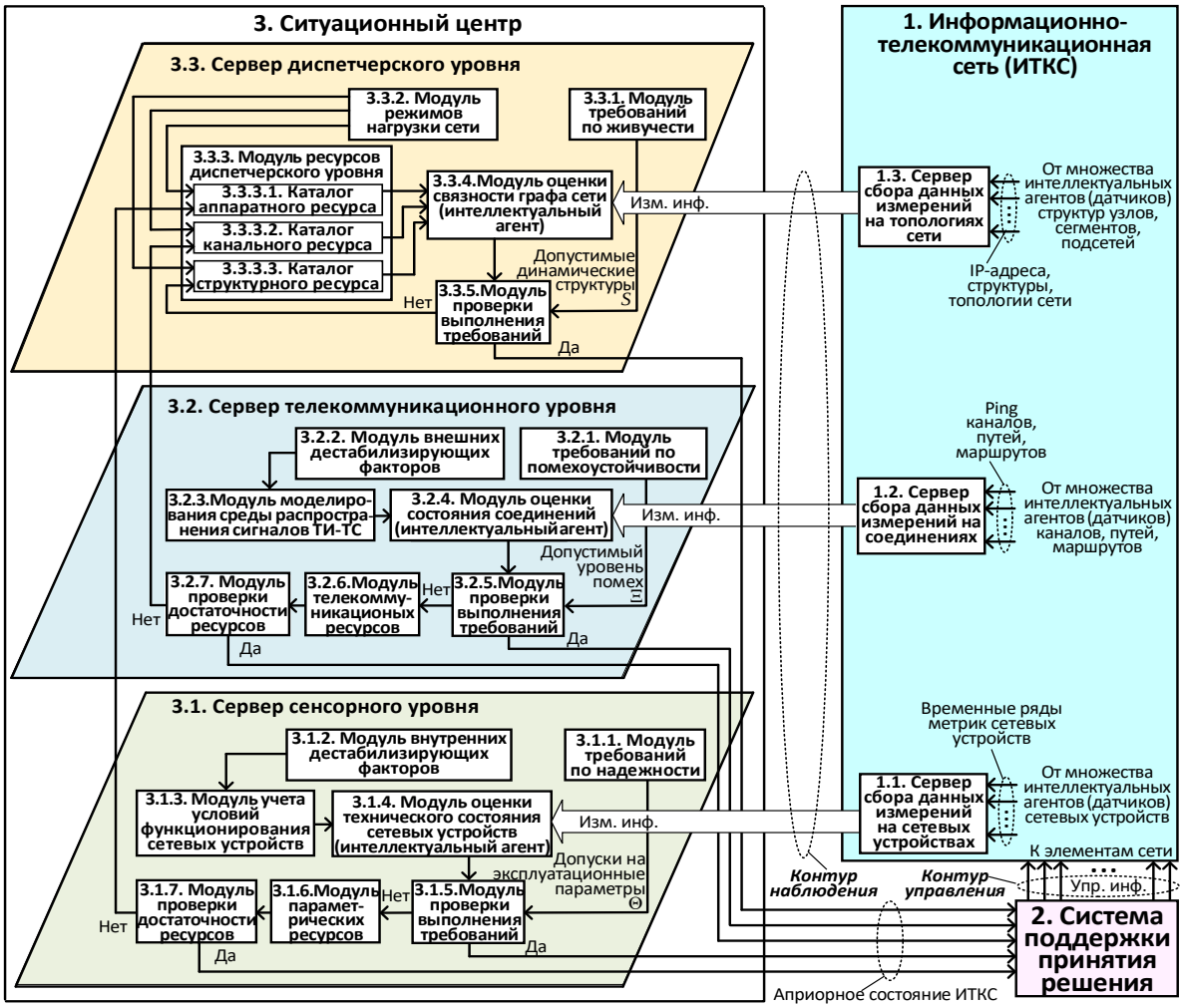


Рис. 3. Система интеллектуального мониторинга состояния ИТКС ОП

Сущность предлагаемой реализации состоит в обеспечении технологии опроса, сбора, накопления и интеллектуального анализа ИИ о техническом состоянии сетевых элементов и сети в целом, выполняемых для недопущения ее деградации и блокировки путем управления сетевыми ресурсами по результатам данного анализа. Как следствие, техническим результатом от заявленной технологии, является возможность сбора, накопления и интеллектуального анализа ИИ о состоянии сетевых элементов в виде устройств и узлов сети; каналов связи, путей и маршрутов; сегментов и подсетей, соответственно, на аппаратном, канальном и структурном уровнях ИТКС, идентификации предотказного и опасного состояния [4], а также предоставления в СППР расчетных значений достаточности ресурсов каждого уровня для устранения аварийных режимов работы и нагрузок путем регулировки эксплуатационных параметров элементов сети или включения резерва для восстановления/наращивания структуры ИТКС при ее деградации.

Выводы

Технология интеллектуального мониторинга состояния ИТКС ОП осуществляется на примере использования трех этапов функционирования:

− первый этап заключается в формировании *контура наблюдения*, который реализован непосредственно на ИТКС;

− второй этап предназначен для *идентификации вида технического состояния*, который реализован на СЦУ ведомственной ИТКС;

− третий этап посвящен формированию *контура управления,* который реализован в СППР, функционирующей как правило в составе СЦУ.

Список литературы

1. Инфокоммуникационные сети: энциклопедия. Кн. 4: Гетерогенные сети связи: принципы построения, методы синтеза, эффективность, цена, качество / П. А. Будко, И. А. Кулешов, В. И. Курносов, В. И. Мирошников; Под ред. проф. В. И. Мирошникова. – М.: Наука, 2020. – 683 с.

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

3. Пузанков Д. В., Мирошников В. И., Пантелеев М. Г., Серегин А. В. Интеллектуальные агенты, многоагентные системы и семантический Web: концепции, технологии, приложения. – СПб.: ООО «Технолит», 2008. – 292 с.

4. ГОСТ 27.002-2015 Надежность в технике. Термины и определения. – М.: Стандартинформ, 2016. – 23 с.

5. Будко Н. П., Васильев Н. В., Груздев А. А., Каретников В. В., Шаталов А. Е., Шмидт А. А. Способ интеллектуального мониторинга состояния информационно-телекоммуникационной сети / Патент на изобретение RU № 2841123 C1 от 02.06.2025. Заявка № 20241337867 от 12.11.2024. Бюл. № 16. – 41 с.

6. Будко Н. П., Виноградeнко А. М., Груздев А. А., Каретников В. В., Шаталов А. Е., Шмидт А. А. Система интеллектуального мониторинга состояния информационно-телекоммуникационной сети / Патент на изобретение RU № 2841117 C1 от 02.06.2025. Заявка № 2024114755 от 30.05.2024. Бюл. № 16. – 20 с.

УДК 621.391

Предиктивно-адаптивное управление модуляцией и кодированием в беспроводных системах передачи контент-зависимого трафика

Иванов В.А., Маркин А.В., Овсянкин С.В., Иванов И.В., Лапицкий В.Ф.

ПАО «Интелтех», г. Санкт-Петербург, Россия

Аннотация: *В докладе предлагается решение для повышения эффективности использования пропускной способности в каналах беспроводных сетей связи в условиях нестационарной помеховой обстановки и замираний. Предложен подход к предиктивно-адаптивному управлению модуляцией и кодированием (Р-АМС), основанный на анализе внутренней статистической структуры цифрового потока с использованием аппарата многосвязных цепей Маркова. Показано, что учёт энтропийных характеристик передаваемых данных позволяет осуществлять проактивный, а не реактивный выбор схемы модуляции и кода помехоустойчивого кодирования. Разработана функциональная схема модуля Р-АМС, описаны принципы его интеграции в телекоммуникационное оборудование. Ожидаемый эффект от внедрения – повышение эффективной пропускной способности спутниковых и радиоканалов на 15–25% в нестабильных условиях.*

Ключевые слова: *предиктивно-адаптивное управление, адаптивная модуляция и кодирование, цепи Маркова, цифровой поток, акселерация трафика, беспроводные сети, спутниковые каналы.*

Актуальность

Современные сети связи представляют собой гетерогенные мультисервисные инфраструктуры, интегрирующие трафик данных, голоса, видео и служебной информации. Ключевым ограничением для их развития выступают сегменты (направления) с ограниченной пропускной способностью, к которым относятся беспроводные сети, включающие спутниковые каналы, радиорелейные линии и сети доступа к удалённым абонентам [1]. В периоды пиковых нагрузок, связанных с чрезвычайными ситуациями или проведением специальных мероприятий, пропускная способность этих направлений перестаёт обеспечивать требуемые показатели качества обслуживания (QoS) [2].

Традиционные методы борьбы с перегрузками – буферизация, приоритизация, балансировка трафика – носят реактивный характер и направлены на перераспределение уже сформированного потока, но не на его проактивное преобразование [3]. Технологии акселерации трафика, предполагающие устранение избыточности на уровне контента и протокольной организации, предлагают принципиально иной подход [4]. Однако их эффективность на физическом уровне остаётся ограниченной из-за реактивного характера существующих систем адаптивной модуляции и кодирования (АМС).

Классические АМС-алгоритмы изменяют параметры передачи (тип модуляции, код коррекции ошибок) в ответ на измеренное текущее или недавнее состояние канала (отношение сигнал/шум, вероятность битовой ошибки). Это приводит к запаздыванию реакции и неоптимальному выбору режима

в условиях быстрых замираний, характерных для спутниковых и радиоканалов [5]. Кроме того, такие системы «не видят» передаваемый трафик, одинаково обрабатывая как критичный VoIP-поток, так и фоновую передачу файлов.

Преодоление таких негативных ситуаций требует перехода к предиктивной адаптивной модуляции и кодированию (P-AMC), основанной на проактивном анализе как состояния канала, так и внутренней статистической структуры цифрового потока [6]. В отличие от реактивных подходов, P-AMC прогнозирует ухудшение качества канала и заблаговременно переключает режим передачи, а также учитывает семантику передаваемых данных для выбора оптимальной стратегии помехоустойчивого кодирования.

Вербальная постановка задачи

В беспроводных системах передачи контент-зависимого трафика в условиях нестационарной помеховой обстановки и замираний требуется обеспечить максимальную эффективную пропускную способность канала при гарантированном соблюдении требований к вероятности битовой ошибки (BER) и задержке доставки. Существующие реактивные AMC-алгоритмы, переключающие схемы модуляции и кодирования на основе измерений текущего состояния канала, обладают инерционностью, что приводит к потерям пакетов и снижению спектральной эффективности в периоды быстрых изменений канальных условий.

Задача заключается в разработке метода предиктивно-адаптивного управления модуляцией и кодированием, который:

Прогнозирует краткосрочные изменения состояния канала (отношения сигнал/шум, уровень замираний) на основе анализа временных рядов и (или) марковских моделей.

Классифицирует передаваемый цифровой поток по его внутренней статистической структуре (распределению двоичных кодовых комбинаций, энтропии), определяя степень его предсказуемости и, следовательно, требуемый уровень помехоустойчивой защиты.

Проактивно выбирает пару «схема модуляции – код коррекции ошибок» (MCS), обеспечивающую оптимальный компромисс между скоростью передачи и помехоустойчивостью для конкретного типа трафика и прогнозируемого состояния канала.

Адаптируется к смене типа цифрового контента, изменяя стратегию кодирования в зависимости от статистических свойств потока.

Формализованная постановка задачи

Пусть цифровой поток на входе системы описывается последовательностью бит $a_k \in \{0,1\}$. Для анализа статистической структуры потока вводится скользящее окно длиной L бит, в котором формируются двоичные кодовые комбинации (ДКК) размерности n:

$$V_n=(a_{t-n+1},a_{t-n+2},...,a_t),\ \ V_n\in\{0,1\}. \quad (1)$$

Распределение ДКК характеризуется вектором вероятностей

$$\pi=[p(V_n^1),p(V_n^2),...p(V_n^{(2^n)}). \quad (2)$$

Ключевыми метриками, описывающими статистическую структуру потока, являются:

Энтропия Шеннона – мера неопределённости (информационной плотности) потока. Условная энтропия Шеннона потока на символ (бит) является мерой предсказуемости потока, а при известной модели порядка L характеризует среднюю неопределённость появления следующего бита [7]:

$$H_L=-\sum_{i=1}^{2^n}p(V_n^i)log_2p(V_n^i),0\le H\le 1. \quad (3)$$

Модифицированная метрика Минковского – интегральный показатель, характеризующий отклонение распределения ДКК от эталонного, например, равномерного:

$$M_N(P^{ref},P^{curt})=\sum_{k=1}^{N}\left[\sum_{s=1}^{2k}\left|P_{i,...}^{ref}(k,s)-P_{i,...}^{curt}(k,s)\right|\right]\times 2^{-(k+1)}, \quad (4)$$

где N – максимальная рассматриваемая размерность ДКК, [74,83], P^{ref},P^{curt} – векторы частостей ДКК для эталонного и текущего потоков; [7].

Состояние канала характеризуется отношением сигнал/шум $\gamma(t)$ и вероятностью битовой ошибки $BER(t)$. Множество доступных схем модуляции и кодирования образует конечное множество $MCS = \{m_1, m_2, ..., m_K\}$, где каждая схема m_i характеризуется спектральной эффективностью η_i (бит/с/Гц) и требуемым пороговым значением $SNR_{Yth,i}$ для обеспечения заданной BER_{target}.

Задача Р-АМС формализуется как задача оптимального управления:

$$\max_{m(t)\in MCS},\ \eta_{eff}=\eta_{m(t)}\times \mathrm{I}\{BER_{m(t)}\left(\gamma\left(t+\tau\right)\right)\le BER_{target}\}, \quad (5)$$

при ограничениях $T_{prog}\le T_{\max}$, $P_{out}\le P_{out}^{target}$, где $\gamma\left(t+\tau\right)$ - прогнозируемое значение SNR на горизонте упреждения τ; T_{prog} – время, затрачиваемое на прогнозирование и принятие решения; P_{out} – вероятность превышения BER порогового значения.

Выбор MCS осуществляется на основе композитного критерия, учитывающего как прогноз состояния канала, так и статистические свойства потока:

$$m_{opt}\left(t\right)=argmax_{m\in MCS}[\eta_m\times w_1\left(\gamma\left(t+\tau\right)\right)+w_2\left(H\left(t\right),M_N\left(t\right)\right)], \quad (6)$$

где w_1– вес, зависящий от прогнозируемого качества канала; w_2 – вес, определяемый энтропийными характеристиками потока, отражающий требуемый уровень помехоустойчивой защиты.

Автокорреляционная функция – используется для анализа автокорреляции, цикличности и стационарности цифрового потока, позволяет выявить скрытые периодичности и оценить длину памяти аппроксимирующей цепи Маркова. Оценка АКФ со сдвигом τ определяется как:

$$R(\tau) = \frac{1}{N-\tau}\sum_{k=1}^{N-\tau} x_k \times x_{k+\tau}, \quad (7)$$

где N – длина анализируемого участка потока.

Назначение АКФ в модели заключается в определении глубины τ, на которой $R(\tau)$ перестаёт превышать статистически значимый порог, что указывает на границу существенной корреляционной связи.

Порядок решения задачи

В каждый момент времени система перебирает все доступные схемы модуляции и кодирования. Для каждой схемы она смотрит, какой будет уровень сигнала через интервал времени τ. Если рассчитанный процент ошибок (*BER*) для этой схемы при таком будущем уровне сигнала окажется выше допустимого порога, схема отбрасывается (её вклад в результат равен нулю). Из оставшихся "разрешенных" схем выбирается та, у которой номинальная скорость (спектральная эффективность) максимальна. Эта максимальная скорость и становится итоговым значением.

Такая постановка задачи обеспечивает поиск решений по предиктивно-адаптивному управлению модуляцией и кодированием в беспроводных системах передачи контент-зависимого трафика, обеспечивающих повышение эффективной пропускной способности каналов на 15–25% в нестабильных условиях за счёт перехода от реактивного к проактивному выбору схемы модуляции и кода помехоустойчивого кодирования на основе анализа внутренней статистической структуры цифрового потока.

Ключевая гипотеза, лежащая в основе предлагаемого подхода, заключается в том, что статистические характеристики цифрового потока, в частности степень его предсказуемости, оцениваемая через энтропию Шеннона, а параметры аппроксимирующей цепи Маркова, коррелируют с оптимальной стратегией защиты от ошибок на физическом уровне [8].

Эмпирические исследования, проведённые на основе архивов реального трафика (*WIDE MAWI Working Group Traffic Archive*), показывают, что различные типы цифрового контента формируют потоки с характерными статистическими свойствами [9]:

Текстовые и служебные данные характеризуются низкой энтропией ($H \approx$ 0,3–0,6 бит/символ), наличием повторяющихся шаблонов и детерминированных переходов в матрице вероятностей. Такие потоки обладают высокой избыточностью, что позволяет использовать менее мощное (но более скоростное) помехоустойчивое кодирование без ущерба для достоверности, так как часть ошибок может быть исправлена на стороне приёмника за счёт знаний о статистической модели потока.

Голосовой трафик (кодеки *G*.711, *Opus*) характеризуется умеренной энтропией ($H \approx$ 0,5–0,8) и явной краткосрочной корреляцией, отражающей форму речевого сигнала. Требует сбалансированного подхода к помехоустойчивому кодированию.

Сжатое видео (*H*.264/*AVC*, *HEVC*) демонстрирует сложную иерархическую структуру с цикличностью, соответствующей группам кадров (*GOP*). Энтропия высокая ($H \approx 0{,}7–0{,}95$), что ограничивает возможности использования статистической избыточности для коррекции ошибок.

Зашифрованный или случайный трафик характеризуется энтропией, близкой к максимальной ($H \approx 1$), и псевдо-равномерным распределением ДКК. Для таких потоков требуется максимальная защита помехоустойчивым кодированием (*FEC*), так как статистическая избыточность отсутствует.

Таким образом, для потоков с низкой энтропией избыточность, вносимая помехоустойчивым кодированием, может быть уменьшена без ущерба для достоверности, и наоборот, для высокоэнтропийных (близких к случайным) потоков требуется максимальная защита *FEC*. Эта связь между энтропийными характеристиками цифрового потока и стратегией кодирования составляет основу концепции Р-АМС.

На основе проведённого анализа разработана функциональная схема модуля Р-АМС (рисунок 1), интегрируемого на границе между канальным и физическим уровнями телекоммуникационного оборудования.

Модуль Р-АМС включает следующие ключевые функциональные блоки:

Блок анализа цифрового потока выполняет сегментацию входящего битового потока на скользящие окна анализа и рассчитывает комплекс статистических метрик. Для каждого окна определяются:

− эмпирическое распределение частостей ДКК размерности n=1, 2, 3, 4;

− энтропия Шеннона H;

− модифицированная метрика Минковского M_N относительно эталонных распределений;

− параметры автокорреляционной функции (АКФ), позволяющие выявить периодичность и глубину памяти процесса.

Блок анализа состояния канала осуществляет непрерывный мониторинг параметров радиоканала: отношение сигнал/шум (*SNR*), вероятность битовой ошибки (*BER*), уровень замираний, доплеровский сдвиг частоты. Измерения выполняются как на основе пилот-сигналов, так и с использованием обратной связи от приёмной стороны.

Блок прогнозирования состояния канала на основе временных рядов измеренных параметров строит краткосрочный прогноз SNR на горизонте упреждения τ (от 10 до 100 мс). Для прогнозирования могут использоваться:

− классические методы анализа временных рядов (*ARIMA*, экспоненциальное сглаживание);

− Марковские модели, описывающие переходы между состояниями канала;

− методы машинного обучения (*LSTM*-сети, градиентный бустинг), обеспечивающие более высокую точность прогноза в условиях нестационарной помеховой обстановки [10].

Блок классификации и принятия решений является интеллектуальным ядром модуля Р-АМС. На основе вектора признаков, полученного от блока анализа потока, комитетный классификатор относит текущий сегмент трафика к одному из заранее определённых классов, каждый из которых характеризуется требуемым уровнем помехоустойчивой защиты. Классы формируются по двум осям: тип цифрового контента и статистический тип распределения ДКК [11].

Таблица соответствий «класс потока — требуемый уровень *FEC*-защиты» формируется на этапе калибровки системы и может динамически обновляться в процессе эксплуатации.

Решающее правило объединяет информацию о прогнозируемом состоянии канала и классе потока для выбора оптимальной пары «схема модуляции — код *FEC*»:

Для предсказуемого трафика (низкая энтропия, стабильное распределение ДКК) и прогнозируемого стабильного канала выбирается более скоростная, но менее помехоустойчивая схема.

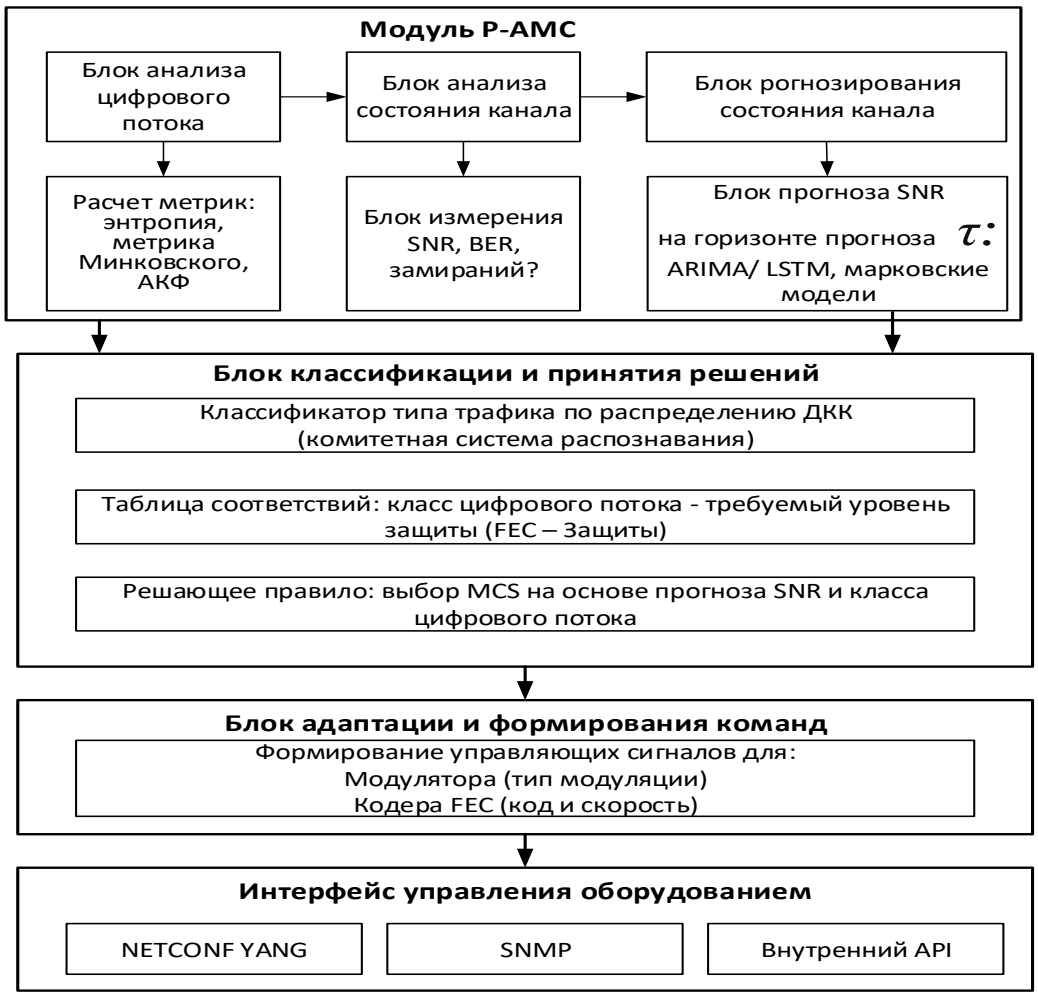


Рис. 1. Функциональная схема модуля предиктивно-адаптивного управления модуляцией и кодированием (Р-АМС)

Для непредсказуемого трафика (высокая энтропия, близкое к равномерному распределение) или ожидаемого ухудшения канала активируется более надёжная схема с мощным FEC.

Блок адаптации и формирования команд транслирует принятое решение в управляющие сигналы для модулятора (выбор типа модуляции: *QPSK*, 16-*QAM*, 64-*QAM* и др.) и кодера *FEC* (выбор кода и скорости кодирования). Информация о выбранном классе предсказуемости и применённой схеме кодирования может инкапсулироваться в служебные поля физического кадра для информирования приёмной стороны.

Интерфейс управления оборудованием обеспечивает интеграцию модуля P-AMC с телекоммуникационным оборудованием через стандартизированные протоколы (*NETCONF*/*YANG*, *SNMP*) или внутренний *API*.

Алгоритм функционирования модуля P-AMC реализует следующий циклический процесс:

Шаг 1. Инициализация. Задаются начальные параметры: множество доступных *MCS* $\{m_1, \ldots, m_K\}$, пороговые значения *SNR* для каждого MCS, размер окна анализа L, горизонт прогнозирования τ, коэффициенты весовой функции w_1, w_2.

Шаг 2. Анализ цифрового потока. Из входящего битового потока выделяется сегмент длиной L бит. Рассчитываются статистические метрики: энтропия H, модифицированная метрика Минковского M_N, параметры АКФ.

Шаг 3. Классификация потока. На основе вектора признаков комитетный классификатор относит сегмент к одному из классов, каждому из которых соответствует требуемый уровень *FEC*-защиты и скорость кодирования.

Шаг 4. Анализ состояния канала. Измеряются текущие значения *SNR*, *BER* и других параметров канала.

Шаг 5. Прогнозирование состояния канала. С использованием выбранной модели прогнозирования вычисляется оценка *SNR* на горизонте упреждения τ.

Шаг 6. Принятие решения. На основе прогноза *SNR* и требуемого уровня *FEC*-защиты выбирается оптимальная *MCS* – выражение 6.

Шаг 7. Формирование управляющих команд. Выбранная *MCS* транслируется в управляющие сигналы для модулятора и кодера FEC. Информация о применённой схеме кодирования добавляется в служебные поля кадра.

Шаг 8. Обратная связь и адаптация. На приёмной стороне измеряется фактическая BER. В случае превышения порогового значения формируется сигнал обратной связи, который используется для корректировки весовых коэффициентов и пороговых значений решающего правила.

Шаг 9. Цикл. Процесс повторяется для следующего сегмента потока.

Интеграция в телекоммуникационное оборудование

Модуль P-AMC может быть реализован в следующих вариантах исполнения:

Виртуальный модуль акселерации (VNF), развёртываемый на универсальной платформе (uCPE) на границе сети, взаимодействующий с программным обеспечением модема или радиомодуля через специализированный API.

Аппаратный ускоритель на базе ПЛИС (FPGA), интегрированный непосредственно в плату модема спутниковой или радиорелейной связи. Такой вариант критичен для минимизации задержки обработки и обеспечения работы на высоких скоростях передачи.

Программный модуль в составе прошивки программируемых радиомодулей (*SDR — Software-Defined Radio*).

Для обеспечения прозрачной интеграции в существующую инфраструктуру сетей связи предлагается использовать комбинацию протоколов *BGP* для динамического перенаправления трафика через модуль Р-АМС и *NETCONF*/*YANG* для централизованного управления его параметрами [12]. Модуль размещается до средств криптографической защиты (*VPN*-шлюзов, *IPsec*), так как шифрование маскирует статистические свойства потока, делая анализ неэффективным.

Оценка эффективности

Эффективность предложенного подхода оценивалась с использованием имитационной модели цифрового потока, построенной на основе аппарата управляемых многосвязных цепей Маркова [13]. Модель позволяет генерировать синтетические потоки с заданными статистическими свойствами и энтропийными характеристиками, а также эмулировать различные сценарии изменения состояния канала (замирания, помехи).

Результаты модельных экспериментов показывают:

Применение Р-АМС позволяет повысить среднюю спектральную эффективность (бит/с/Гц) на 15–25% по сравнению с классической реактивной *АМС* в условиях частых замираний.

Для потоков с низкой энтропией (текстовые данные, служебный трафик) выигрыш в эффективной пропускной способности достигает 20–30% за счёт использования менее избыточного помехоустойчивого кодирования.

Для высокоэнтропийных потоков (зашифрованный трафик) Р-АМС обеспечивает более стабильную работу за счёт проактивного переключения на более надёжные схемы *MCS* при прогнозируемом ухудшении канала.

Снижение числа ошибок декодирования и, как следствие, уменьшение количества повторных передач приводит к дополнительному повышению эффективной пропускной способности на 10–15%.

Выводы

1. *Научная новизна.* Впервые предложен и научно обоснован подход к предиктивно-адаптивному управлению модуляцией и кодированием (Р-АМС), основанный на комплексном анализе двух факторов: прогнозируемого состояния канала и внутренней статистической структуры передаваемого цифрового потока, описываемой через распределение двоичных кодовых комбинаций и энтропию Шеннона. В отличие от классических реактивных *АМС*-алгоритмов, предлагаемый подход осуществляет проактивный выбор схемы модуляции и кода помехоустойчивого кодирования, что позволяет минимизировать влияние инерционности системы в условиях быстрых замираний. Обоснована и формализована связь между энтропийными характеристиками цифрового потока и оптимальной стратегией помехоустойчивого кодирования, что является развитием теоретических основ адаптивной модуляции и кодирования.

2. *Теоретическая ценность.* Работа вносит вклад в развитие теории адаптивной модуляции и кодирования, расширяя её классическую парадигму, ориентированную исключительно на состояние канала, за счёт учёта семантических и статистических свойств, передаваемых данных. Предложенный подход синтезирует аппарат цепей Маркова для моделирования цифрового потока, методы теории информации для оценки его энтропийных характеристик и методы прогнозирования временных рядов для оценки состояния канала. Это создаёт теоретическую основу для нового класса систем — контент-зависимых адаптивных модуляционно-кодовых схем (*Content-Aware AMC*).

3. *Практическая значимость.* Разработана функциональная схема и описан алгоритм работы модуля Р-АМС, который может быть реализован как в виде виртуальной сетевой функции (*VNF*) на универсальных платформах, так и в виде аппаратного ускорителя на базе ПЛИС для работы на высоких скоростях. Предложены механизмы интеграции модуля Р-АМС в существующую инфраструктуру корпоративных сетей связи через стандартизированные протоколы (*BGP*, *NETCONF*/*YANG*). Оценён потенциальный эффект от внедрения: повышение эффективной пропускной способности спутниковых и радиоканалов на 15–25% в нестабильных условиях, что для дорогостоящих спутниковых каналов означает существенную экономию средств и повышение надёжности связи.

4. В отличие от существующих решений (классических АМС, статических схем модуляции и кодирования), предлагаемый подход является *проактивным и контекстно-осведомлённым*. Система не просто реагирует на изменения состояния канала, а прогнозирует их и адаптивно подстраивает параметры модуляции и кодирования под семантику и статистику проходящего трафика. Это позволяет достичь более высоких значений спектральной эффективности и устойчивости передачи в условиях нестационарной помеховой обстановки.

5. *Перспективы развития.* Дальнейшие исследования в данном направлении связаны с: интеграцией более сложных моделей машинного

обучения (глубокие нейронные сети, градиентный бустинг) для повышения точности прогнозирования состояния канала в условиях быстрых замираний; разработкой адаптивных алгоритмов совместной оптимизации параметров модуляции, кодирования и управления мощностью; созданием аппаратных прототипов модуля Р-АМС на базе *FPGA* и их тестированием на реальных трассах спутниковой и радиорелейной связи; расширением подхода на системы *MIMO* и массовые *MIMO*-системы 5*G*/6*G*.

Заключение

В работе предложен подход к предиктивно-адаптивному управлению модуляцией и кодированием в беспроводных системах передачи контент-зависимого трафика, основанный на синтезе методов прогнозирования состояния канала и анализа внутренней статистической структуры цифрового потока. Разработанный модуль Р-АМС обеспечивает переход от реактивной парадигмы адаптации к проактивной, что позволяет повысить эффективную пропускную способность спутниковых и радиоканалов на 15–25% в нестабильных условиях. Предложенные решения могут быть интегрированы в существующую инфраструктуру корпоративных сетей связи через стандартизированные протоколы управления и реализованы как в виртуальном, так и в аппаратном исполнении. Полученные результаты создают теоретический и практический фундамент для создания следующего поколения интеллектуальных систем адаптивной модуляции и кодирования, способных обеспечить гарантированное качество обслуживания в условиях динамически меняющейся помеховой обстановки и гетерогенного трафика.

Список литературы

1. Гавлиевский С. Л. Принципы построения мультисервисной сети ПАО «Ростелеком». – Москва: Горячая линия–Телеком, 2018. – 228 с.

2. Лихтциндер Б. Я. Трафик мультисервисных сетей доступа (интервальный анализ и проектирование). – Москва: Горячая линия–Телеком, 2018. – 290 с.

3. Дементьев А.Н., Захаркин С.В., Иванов В.А. Сигналы и каналы связи: учебное пособие для вузов. – Москва: Горячая линия–Телеком, 2024. – 327 с.

4. Шпунт Я. WAN-оптимизаторы. Удар по информационному бездорожью // Журнал сетевых решений LAN. – 2009. – № 17–18. – С. 32–39.

5. Иванов В.А., Маркин А.В., Овсянкин С.В., Иванов И.В., Соболев С.В. Виртуальный акселератор трафика физического уровня для спутникового сегмента связи. – Свидетельство о государственной регистрации программы для ЭВМ № 2025695696. – Москва: ФГУ ФИПС, 2026.

6. Маркин А.В., Иванов В.А., Овсянкин С.В. и др. Виртуальный модуль адаптивной акселерации трафика канального уровня для низкоскоростных линий связи и космического сегмента корпоративной сети связи. – Свидетельство о государственной регистрации программы для ЭВМ № 2025695698. – Москва: ФГУ ФИПС, 2026.

7. Овсянкин С.В., Маркин А.В., Иванов В.А., Аналитическая модель цифрового потока, поступающего с выхода источника сообщений на вход акселератора трафика // Техника средств связи. – 2024. № 2 (166). – С. 58-67.

8. Иванов И.В., Маркин А.В., Иванов В.А., Овсянкин С.В., Математическая модель нестационарного цифрового потока с памятью и контент-ориентированной калибровкой переходов // Техника средств связи. – 2026. – № 3 (171). – С. 86–97.

9. Репозитории трафика [Электронный ресурс]. – Режим доступа: ita.ee.ibi.gov; mawi.wide.ad.jp.

10. Experimental Validation of Decision Tree-Based Adaptive Modulation and Coding Prediction for Multiple Users in Dynamic Wireless Environment // IEEE Xplore, 2026.

11. Худайназарова Д.Р., Маркин А.В., Иванов В.А., Овсянкин С.В., Иванов И.В. Программа реализации алгоритма классификации и сжатия цифрового потока с адаптацией к цифровому контенту и распределению двоичных кодовых комбинаций. – Свидетельство о государственной регистрации программы для ЭВМ № 2026618063 от 24. 03. 2026. – Москва: ФГУ ФИПС.

12. Иванов В.А., Маркин А.В., Иванов И.В. Организация физического и сетевого взаимодействия оптимизаторов трафика с оборудованием связи / Материалы XIV Всероссийской межведомственная научная конференции «Актуальные направления развития систем обеспечения безопасности объектов государственной охраны и защиты охраняемых объектов, специальной связи для нужд органов государственной власти и специального информационного обеспечения государственных органов». – Орел: Академия ФСО России, 2025. – 147 с. – С. 126-129.

13. Добрышин М.М., Иванов В.А., Маркин А.В., Овсянкин С.В., Иванов И.В. Имитационная модель цифрового потока на основе применения многосвязных цепей Маркова с калибровкой памяти и переходов для цифрового контента. – Свидетельство о государственной регистрации программы для ЭВМ № 2026617974 от 23. 03. 2026. – Москва: ФГУ ФИПС

УДК 004.056

Оценка эффективности анализа защищённости морских систем управления движением судов с применением искусственного интеллекта

Позолотин С. И.

ЗАО «ИТ», г. Санкт-Петербург, Россия

Аннотация: *в тезисе затрагивается актуальность разработки научно-методического аппарата оценки эффективности анализа защищённости системы управления движением судов (СУДС) с применением технологий искусственного интеллекта. Показано, что развитие электронной навигации и безэкипажного судоходства расширяет поверхность компьютерных атак на СУДС как объект критической информационной инфраструктуры. Установлено, что действующая методика анализа защищённости одновременно требует выявления максимально возможного количества уязвимостей и недопущения нарушения функционирования эксплуатируемой системы, но не устанавливает правил выбора состава проверочных воздействий, а ограничения, сужающие границы проверки, не образуют репрезентативной выборки.*

Ключевые слова: *информационная безопасность, кибербезопасность, искусственный интеллект, тестирование на проникновение, е-навигация, СУДС.*

Морская транспортная инфраструктура составляет основу внешнеэкономической деятельности Российской Федерации: по итогам 2025 года грузооборот морских портов России составил 884,5 миллион тонн, из которых на экспортные грузы пришлось 696,6 миллион тонн (около 78,8 % перевалки) [1]. Устойчивость внешнеэкономической деятельности зависит от непрерывного функционирования обеспечивающих её информационных и управляющих систем. Согласно Федеральному закону от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» информационные системы, информационно-телекоммуникационные сети и автоматизированные системы управления субъектов в сфере транспорта относятся к объектам критической информационной инфраструктуры (КИИ) [2].

Система управления движением судов (СУДС) создаётся в целях повышения уровня безопасности мореплавания и эффективности судоходства и выполняет четыре функции: контроль за движением судов; передачу судам навигационной, оперативной и иной информации; организацию движения судов; оказание помощи в судовождении (п. 5.1 Положения о СУДС) [3]. Функции обеспечиваются техническими средствами: радиосвязью очень высокой частоты (ОВЧ), береговыми радиолокационными станциями (РЛС), автоматической информационной системой (АИС), системами телевизионного наблюдения [3, 4]. По функциональной роли и составу технических средств СУДС является объектом КИИ в сфере транспорта [2, 5].

Современное развитие судоходства определяется концепцией электронной навигации (e-Navigation), цель которой – создание единого информационного

пространства между судном и берегом [6, 26]. С ней связаны технологии безэкипажного судоходства: судно движется, маневрирует и выполняет задачи без человека на борту. С СУДС безэкипажное судно (БЭС) взаимодействует не на всём переходе, а в зоне её действия – на подходах к морскому порту, в его акватории и при выходе из него, где движение судов регламентировано и контролируется береговыми службами [3]. Именно в этой зоне СУДС выступает ключевым береговым элементом информационной инфраструктуры БЭС [7].

Обмен данными между судами и СУДС ведётся по нескольким радиоканалам: речевой связи ОВЧ, автоматической информационной системе (АИС), работающей в диапазоне ОВЧ, и данным береговых РЛС. Сообщения АИС передаются в открытом виде, без шифрования и подтверждения подлинности отправителя, поэтому они допускают подмену (spoofing) и подавление (jamming) [8]. По мере автоматизации этого обмена растут число сопрягаемых систем и объём передаваемых данных, а вместе с ними – количество точек, через которые нарушитель может воздействовать на СУДС. Эти каналы и подключённые к ним системы образуют поверхность компьютерных атак, которую и должен охватывать анализ защищённости СУДС как объекта КИИ.

Число киберинцидентов в морской отрасли в 2025 году возросло более чем вдвое [9], приоритет атак смещается к нарушению функционирования управляющих систем [10]. Современный уровень технологий искусственного интеллекта (ИИ) позволяет нарушителю автоматизировать значительную часть жизненного цикла атаки [11], что повышает требования к полноте и обоснованности анализа защищённости.

Порядок проведения анализа защищённости установлен Методикой анализа защищённости информационных систем (ИС), утверждённой ФСТЭК России 25 ноября 2025 г. [12]. Методика регламентирует выявление уязвимостей методами внешнего и внутреннего анализа уязвимостей (сканирования), в том числе активными методом – путём формирования специальных тестовых запросов (информационно-технических воздействий – ИТВ) (п. 2.12). Оценка устойчивости объекта к действиям нарушителя требует проверочных воздействий, воспроизводящих реальные атаки, – тестирования на проникновение, состав и последовательность процедур которого закреплены в ряде зарубежных стандартов и методик (OSSTMM, ISSAF, OWASP, PTES, NIST SP 800-115, BSI, PETA, PTF); их сравнительный разбор выполнен в обзоре С. И. Макаренко и Г. Е. Смирнова [13]. Именно такие воздействия создают риск нарушения работы проверяемого объекта. Для эксплуатируемой системы требования методики вступают в противоречие: п. 2.7 предписывает выявлять максимально возможное количество уязвимостей, п. 2.21 – не допустить нарушения функционирования. Правило оптимального выбора состава воздействий, обеспечивающее наибольшую полноту при непревышении допустимого риска методикой не установлено; не заданы в ней и показатели, по которым можно судить об эффективности – как

о полноте охвата уязвимостей, так и о способности полученных результатов адекватно отражать реальное состояние безопасности объекта для вынесения обоснованного заключения.

Ограничения заказчика – запреты на отдельные виды работ, исключение объектов из границ работ – фиксируются в отчёте (п. 4.2), тогда как заключение выдаётся в отношении всей информационной системы (п. 2.8). Такие исключения назначаются по эксплуатационным соображениям и не образуют репрезентативной выборки: из проверки выводятся прежде всего компоненты, нарушение работы которых недопустимо, то есть наиболее значимые для функционирования системы. Показатели, устанавливающие, в какой мере полученный при этом вывод характеризует защищённость объекта в целом, не предусмотрены.

Для снижения риска нарушения работы ИТВ проводят не на самой эксплуатируемой системе, а на её копии – испытательном стенде (киберполигоне), воспроизводящем инфраструктуру объекта [24]. Радиолокационную обстановку, сигналы автоматической информационной системы и радиочастотную среду современными средствами моделировать возможно, однако точность такого воспроизведения ограничена: ряд явлений (морские помехи, многолучёвое распространение, реальные задержки, совместная работа технических средств под реальным судопотоком) воспроизводится неполно, а количественное соответствие модели реальному оборудованию само требует проверки по натурным данным [25]. Поэтому обнаружение уязвимости на стенде с высокой вероятностью подтверждается на реальном объекте и характеризует достоверность найденного, но не полноту анализа: то, что стенд воспроизводит неточно, остаётся непроверенным. Мера, показывающая, насколько результаты, полученные на стенде, характеризуют защищённость реального объекта, не установлена.

Методика ФСТЭК [12] включает поиск уязвимостей программного обеспечения, в котором используются модели машинного обучения (МИИ.1–МИИ.2), то есть учитывает технологии ИИ в составе проверяемой системы. Случай, когда технологии ИИ применяются самим исполнителем и участвуют в формировании выводов и рекомендаций по результатам анализа, методикой не рассматривается.

Результаты, формируемые технологиями ИИ, включая большие языковые модели (LLM, Large Language Model), подвержены ошибкам: склонности к порождению недостоверных сведений (галлюцинациям), стремлению соответствовать ожиданиям оператора, нестабильности оценок [14]. Технологии объяснимого ИИ (XAI, Explainable Artificial Intelligence) позволяют сопроводить вывод модели объяснением, однако общепринятые показатели качества таких объяснений отсутствуют [15], а выдаваемое моделью объяснение не всегда отражает то, как результат был получен на самом деле [16]. Вследствие этого рекомендации, формируемые технологиями ИИ, не могут рассматриваться как достоверные без экспертной и методической проверки [17].

Научный аппарат анализа защищённости развивается по двум направлениям. Аналитическое направление опирается на графы атак и метрики защищённости. В частности, в работах И. В. Котенко, Е. В. Дойниковой, А. А. Чечулина [18, 19] состояние системы оценивается по её модели, без проведения практических воздействий на объект. При этом критичность отдельных уязвимостей выражается метриками CVSS (Common Vulnerability Scoring System), а защищённость системы в целом – интегральными показателями вероятности реализации атак, потенциального ущерба и уровня риска [18, 19]. В отличие от модельно-аналитического подхода, направление активного (инструментального) анализа опирается на тестирование устойчивости объекта через ИТВ (С. И. Макаренко, Г. Е. Смирнов), где состав тестовых ИТВ обосновывается по критерию «эффективность/стоимость» при заданном ограничении на ресурс аудитора [20–22]. Формализацию автоматизированного тестирования на проникновение развивают и зарубежные исследователи: C. Skandylas и M. Asplund предложили формальную постановку задачи и её программную реализацию [23]. Отдельно рассматривается тестирование технологических систем (OT, Operational technology) [24]. Воздействия на действующие объекты в данном случае ограничивают, поскольку они способны нарушить технологический процесс, но единой методики такого ограничения пока нет – это отмечается как открытая проблема в обзоре практики тестирования OT-систем [24].

Для СУДС эти ограничения являются определяющими: оценка эффективности анализа должна учитывать функциональную значимость технических средств для выполнения функций СУДС и допустимость воздействий на компоненты, нарушение работы которых затрагивает безопасность мореплавания. Возникает противоречие в практике – между необходимостью обеспечения требуемой эффективности анализа защищённости СУДС и невозможностью обеспечить её существующими процедурами, не устанавливающими правил выбора состава воздействий с учётом их допустимости и функциональной значимости компонентов. Целью исследования является повышение эффективности анализа защищённости СУДС, научной задачей – разработка научно-методического аппарата оценки эффективности анализа защищённости СУДС с применением технологий ИИ.

Объектом исследования являются процессы анализа защищённости системы управления движением судов. Предметом исследования является эффективность анализа защищённости СУДС. Противоречие в науке состоит в том, что достижение цели исследования на основе существующего научно-методического аппарата не обеспечивается в требуемой степени, поскольку: 1) известные методы обоснования состава тестовых ИТВ ориентированы на достижение наибольшей полноты проверки при заданном ограничении на ресурс аудитора. Допустимость воздействий на действующем объекте – а именно способность части из них нарушить его функционирование – в этих методах в качестве критерия отбора не рассматривается. Указанное свойственно как формализованным научным постановкам задачи обоснования

состава воздействий [20–22], так и методике ФСТЭК [12]: ни одна из них не устанавливает правила отбора воздействий с учётом их допустимости для функционирующего объекта. Не выработано такого правила и в практике тестирования на проникновение в целом [24]. 2) значимость проверяемого элемента в существующем аппарате определяют либо величиной ущерба от эксплуатации его уязвимости [20, 21], либо метриками CVSS [19]. Обе меры оценивают элемент по тяжести последствий нарушения его безопасности, но не по тому, какую из функций СУДС [3] он обеспечивает и насколько эта функция важна для безопасности мореплавания. Именно эта роль определяет, допустимо ли подвергать элемент разрушающим воздействиям, – и существующий аппарат её не выражает. 3) технологии ИИ не рассматриваются как средство формирования выводов и рекомендаций, обоснованность и достоверность которых подлежат оценке. Цель исследования состоит в повышении эффективности анализа защищённости СУДС. Для достижения поставленной цели необходимо провести анализ специфики СУДС как объекта КИИ, поверхности её компьютерных атак в контексте развития
е-навигации и существующих подходов к оценке защищённости. Выявить ограничения существующих методик тестирования на проникновение на эксплуатируемых объектах и риски, связанные с недостоверностью выводов, формируемых технологиями ИИ. Также необходимо обосновать систему критериев и показателей оценки эффективности анализа защищённости, учитывающую функциональную значимость компонентов СУДС при выполнении её основных функций, допустимость проверочных воздействий и достоверность решений ИИ. Проблемная ситуация обусловлена отсутствием средств, позволяющих совместно учитывать функциональную значимость проверяемых компонентов СУДС, допустимость проверочных воздействий на них и достоверность выводов, формируемых технологиями ИИ.

Список литературы

1. Грузооборот морских портов России за 2025 год // Ассоциация морских торговых портов [Электронный ресурс]. – URL: https://www.morport.com/rus/news/gruzooborot-morskih-portov-rossii-za-2025-god (дата обращения: 17.07.2026).

2. О безопасности критической информационной инфраструктуры Российской Федерации. Федеральный закон РФ от 26.07.2017 № 187-ФЗ // СПС «Контур.Норматив» [Электронный ресурс]. – URL: https://normativ.kontur.ru/document?moduleId=1&documentId=501334 (дата обращения: 17.07.2026).

3. Положение о системах управления движением судов (утв. Минтрансом России 29.07.2002). – М.: Минтранс России, 2002.

4. Об утверждении Требований к радиолокационным системам управления движением судов, объектам инфраструктуры морского порта, необходимым для функционирования Глобальной морской системы связи при бедствии и для обеспечения безопасности, объектам и средствам

автоматической информационной системы, службе контроля судоходства и управления судоходством. Приказ Минтранса России от 23.07.2015 № 226 // ФГУП «Росморпорт» [Электронный ресурс]. – URL: https://www.rosmorport.ru /media/File/News/requirements_VTS.pdf (дата обращения: 17.07.2026).

5. Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации. Приказ ФСТЭК России от 25.12.2017 № 239 // СПС «КонсультантПлюс» [Электронный ресурс]. – URL: https://www.consultant.ru /document/cons_doc_LAW_286438/ (дата обращения: 17.07.2026).

6. E-navigation // International Maritime Organization [Электронный ресурс]. – URL: https://www.imo.org/ru/ourwork/safety/pages/enavigation.aspx (дата обращения: 17.07.2026).

7. Пинский А. С. Е-навигация и безэкипажное судовождение // Транспорт Российской Федерации. Журнал о науке, практике, экономике. 2016. №4 (65) [Электронный ресурс]. – URL: https://cyberleninka.ru/article/n/e-navigatsiya-i-bezekipazhnoe-sudovozhdenie (дата обращения: 29.06.2026).

8. Caprolu M., Di Pietro R., Raponi S., Sciancalepore S., Tedeschi P. Vessels Cybersecurity: Issues, Challenges, and the Road Ahead // IEEE Communications Magazine. 2020. Vol. 58, № 6. P. 90–96. DOI: 10.1109/MCOM.001.1900632

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: 17.07.2026).

10. ENISA Threat Landscape 2025 // European Union Agency for Cybersecurity [Электронный ресурс]. 10.2025. – URL: https://www.enisa.europa.eu/sites/default/files/2025-11/ENISA%20Threat%20Landscape%202025.pdf (дата обращения: 17.07.2026).

11. 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: 17.07.2026).

12. Методика анализа защищённости информационных систем. Методический документ (утв. ФСТЭК России 25.11.2025) // ФСТЭК России [Электронный ресурс]. – URL: https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-25-noyabrya-2025-g (дата обращения: 17.07.2026).

13. 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.

14. Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile: NIST AI 600-1. Gaithersburg: NIST, 2024 [Электронный ресурс]. – URL: https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.600-1.pdf (дата обращения: 17.07.2026).

15. Explainable AI: enhancing decision-making in the detection of cyber threats // Frontiers in Computer Science [Электронный ресурс]. 2026. URL: –

https://www.frontiersin.org/journals/computer-science/articles/10.3389/fcomp.2026.1762332/full (дата обращения: 17.07.2026).

16. Beyond Explainable AI (XAI): An Overdue Paradigm Shift and Post-XAI Research Directions // arXiv [Электронный ресурс]. 2026. URL: – https://arxiv.org/html/2602.24176v5 (дата обращения: 17.07.2026).

17. G. Deng, Y. Liu, V. Mayoral-Vilches, P. Liu, Y. Li, Y. Xu, T. Zhang, Y. Liu, M. Pinzger, S. Rass. PentestGPT: Evaluating and Harnessing Large Language Models for Automated Penetration Testing // Proceedings of the 33rd USENIX Security Symposium. 2024. P. 847–864.

18. Котенко И. В., Степашкин М. В., Богданов В. С. Оценка безопасности компьютерных сетей на основе графов атак и качественных метрик защищённости // Труды СПИИРАН. 2006. Т. 2, № 3. С. 30–49. DOI: 10.15622/sp.3.2

19. Дойникова Е. В., Чечулин А. А., Котенко И. В. Оценка защищённости компьютерных сетей на основе метрик CVSS // Информационно-управляющие системы. 2017. № 6(91). С. 76–87. DOI: 10.15217/issn1684-8853.2017.6.76

20. Макаренко С. И., Смирнов Г. Е. Модель аудита защищённости объекта критической информационной инфраструктуры тестовыми информационно-техническими воздействиями // Труды учебных заведений связи. 2021. Т. 7, № 1. С. 94–104. DOI: 10.31854/1813-324X-2021-7-1-94-104

21. Макаренко С. И., Смирнов Г. Е. Методика обоснования тестовых информационно-технических воздействий, обеспечивающих рациональную полноту аудита защищённости объекта критической информационной инфраструктуры // Вопросы кибербезопасности. 2021. № 6(46). С. 12–25. DOI: 10.21681/2311-3456-2021-6-12-25

22. Смирнов Г. Е. Модель анализа защищённости объекта информатизации железнодорожного транспорта и методика обоснования набора тестовых информационно-технических воздействий для этого // Системы управления, связи и безопасности. 2022. № 4. С. 137–189.

23. Skandylas C., Asplund M. Automated penetration testing: formalization and realization // Computers & Security [Электронный ресурс]. – 2025. – Vol. 155. – Art. 104454. – URL: https://doi.org/10.1016/j.cose.2025.104454 (дата обращения: 17.07.2026).

24. Derbyshire R. The Challenges of Operational Technology Penetration Testing // Digital Threats: Research and Practice [Электронный ресурс]. – 2025. – URL: https://www.researchgate.net/publication/402600116_The_Challenges_of_Operational_Technology_Penetration_Testing (дата обращения: 17.07.2026).

25. Fiengo R., Adams A. Test and evaluation of radar systems operating in the modern electromagnetic spectrum // IET Radar, Sonar & Navigation. 2024. Vol. 18, № 11. P. 2189–2198. DOI: 10.1049/rsn2.12614

26. Позолотин С. И. Электронно-картографические информационно-навигационные системы. Перспективы современного судоходства. Определение е-навигации и её компоненты // Вестник науки и образования. 2022. № 7 (127) С. 53-57.

УДК 621.396

Результаты разработки средств и комплексов авиационной радиосвязи в НПП «ПРИМА»

Скрипник И. В.

ООО «НПП «Прима», г. Санкт-Петербург, Россия

Аннотация: *обсуждаются потребности и направления развития систем авиационной радиосвязи. Представлен опыт НПП «ПРИМА» и результаты разработки каналообразующей аппаратуры различных длин волн. Отдельные результаты связаны с новым направлением исследований и разработок средств радиосвязи для сетевого взаимодействия беспилотной и пилотируемой авиации.*

Ключевые слова: *авиационная радиосвязь, средство радиосвязи, бортовой комплекс средств связи.*

Введение

Эффективность применения пилотируемой и беспилотной авиации в гражданском секторе и особенно при решении специальных задач в составе современных разведывательно-ударных комплексов в значительной мере определяется возможностями информационного обеспечения.

Одним из определяющих условий для успешного ведения авиацией современных разведывательно-ударных действий, для которых характерны сложные и непрерывно изменяющиеся условия, является надежный высокоскоростной информационный обмен.

Несмотря на наличие множества бортовых комплексов авиационной радиосвязи, принятых на вооружение за последние десятилетия, имеется ряд ограничений, снижающих эффективность решения задач боевого управления в соответствии с современными требованиями. Отметим несколько важных потребностей [1], определяющих направления развития систем связи авиации военно-воздушных сил (ВВС):

− оперативная передача различных информационных потоков (речь, данные, видеоинформация и т.д.) в условиях возрастающей интенсивности трафика, формируемого и обрабатываемого средствами автоматизированного управления авиацией ВВС;

− повышение живучести, помехоустойчивости и надежности функционирования системы связи авиации ВВС с учетом интенсивного развития в ряде зарубежных стран средств разведки и радиоэлектронной борьбы;

− гарантированное обеспечение защищенности и безопасности систем связи как в мирное, так и в военное время;

− повышение уровня автоматизации управления связью;

− обеспечение «горизонтального» и «вертикального» взаимодействия функциональных подсистем всех уровней системы управления авиацией ВВС в реальном масштабе времени;

− информационное обеспечение групповых действий авиации на качественно новом уровне, способствующем эффективному решению многочисленных боевых задач;

− обеспечение межвидового взаимодействия при проведении операций с участием различных родов войск;

− разработка единых стандартов и протоколов авиационной радиосвязи для обеспечения совместимости комплексов связи, применяемых на летательных аппаратах (ЛА) разных моделей и различных производителей.

Опыт разработки радиосвязного оборудования

В НПП «ПРИМА» накоплен большой опыт разработки наземных и бортовых комплексов средств связи (БКС) [1, 2], включая:

− БКС для самолетов МиГ-29, МиГ-35 и Су-25СМ3, предназначенные для обеспечения речевой и телекодовой радиосвязи в режимах фиксированной радиочастоты (ФРЧ) и псевдослучайной перестройки радиочастоты (ППРЧ) в метровом и дециметровом (МВ-ДМВ) диапазонах и на ФРЧ в декаметровом (ДКМВ) диапазоне в открытом и закрытом режимах при взаимодействии с другими ЛА и с наземными пунктами управления ВВС;

− БКС для вертолетов Ми-28НМ и Ми-171А2, предназначенные для обеспечения открытой телефонной радиосвязи при взаимодействии с другими ЛА и с наземными пунктами управления ВВС и гражданской авиации.

Направления развития бортовых комплексов и систем радиосвязи

Основные перспективные направления развития бортовых комплексов и систем радиосвязи рассмотрены в [3]. По большинству из этих направлений, а также по связанным с ними проблемам на предприятии ведутся следующие разработки:

− обеспечение заданной надежности связи в условиях сложной помеховой обстановки на основе реализации многопараметрической адаптации радиолиний, применения технологии программно определяемой радиосистемы (SDR), позволяющей реконфигурировать радиотехнические параметры приемного и передающего трактов, а также внедрения элементов когнитивного радио;

− создание и реализация новых сетевых режимов в ДМВ диапазоне;

− серийное производство ДМВ радиостанций 6-го поколения («Прима-ПМА»);

− совершенствование и производство малогабаритных средств радиосвязи, предназначенных для применения на БпЛА среднего и легкого классов;

− совершенствование бортовых и наземных ДКМВ радиостанций, реализующих автоматическую адаптивную радиосвязь в режиме PR_ALE 3G;

− применение ППРЧ для повышения помехозащищенности ДКМВ радиосвязи;

− совершенствование бортовых комплексов средств связи ретранслятора;

− реализация процедур маршрутизации и многомаршрутной передачи;

− разработка перспективных терминалов для обеспечения межвидового взаимодействия;

− разработка новой каналообразующей аппаратуры СМВ диапазона с уменьшенными массогабаритными характеристиками и скоростями передачи данных до 100 Мбит/с;

− реализация методов пространственно-временной аналого-цифровой обработки сигналов;

− разработка протоколов для масштабируемой, динамической, многофункциональной, гетерогенной, самоорганизующейся широкополосной сети радиосвязи.

Совершенствование каналообразующей аппаратуры

Наряду с вышеперечисленными направлениями следует выделить ряд работ по совершенствованию авиационных БКС в части каналообразующей аппаратуры различных диапазонов длин волн.

Для совершенствования каналообразующей аппаратуры ДКМВ диапазона, состоящей из приемопередатчика ДКМВ диапазона и антенно-согласующего устройства, проводятся работы по повышению надежности антенно-согласующего устройства (АСУ) путем совершенствования конструкции и замены элементов, а также разработка нового поколения АСУ и ДКМВ радиостанции мощностью 1 кВт, оптимизация технических решений по стоимости и массогабаритным характеристикам, повышение вычислительных возможностей для внедрения новых алгоритмов обработки сигналов, полномасштабная реализация режима адаптивной ДКМВ радиосвязи PR_ALE3G (модернизированный режим ALE третьего поколения).

Наиболее многочисленным представителем парка каналообразующей аппаратуры МВ-ДМВ диапазона в настоящее время является радиостанция «Прима-ДМВ», которой оснащены многочисленные ЛА оперативно-тактической и армейской авиации. Эти радиостанции могут быть доработаны посредством обновления программного обеспечения, реализующего разработанный в НПП «ПРИМА» режим М1.2С сетевого взаимодействия абонентов с множественным доступом на основе частично децентрализованной (гибридной) топологии сети. Этот режим обеспечивает автоматическую связь в сети, включающей до 16 абонентов (ЛА), одновременный речевой обмен и защищенную передачу данных со скоростью 16,4 кбит/с на одном наборе частот в режиме ППРЧ.

В развитие режима М1.2С на предприятии разработан режим М4С, поддерживающий речевой обмен и защищенную передачу данных в режиме ППРЧ с максимальной скоростью 480 кбит/с для групп ЛА, включающих до 64 абонентов в одной подсети. Наряду с почти тридцатикратным увеличением скорости передачи режим М4С характеризуется значительно меньшим, чем в М1.2С временем работы на одной частоте в режиме ППРЧ.

Режим М4С реализуется в разработанных новых МВ-ДМВ радиостанциях шестого поколения семейства «Прима-ПМА». Эти радиостанции включают один базовый модуль и один или два радиомодуля. В одноканальном варианте исполнения «Прима-ПМА» включает один радиомодуль, а в двухканальном варианте – два радиомодуля соответственно. Базовый модуль обеспечивает информационное взаимодействие с внешней аппаратурой, а также выполнение задач управления радиостанцией и цифровой обработки сигналов. Радиомодуль выполняет усиление, фильтрацию и коммутацию радиочастотных сигналов.

В сантиметровом диапазоне (СМВ) длин волн представленная на рынке каналообразующая аппаратура позволяет формировать информационные и командные радиолинии для цифровой радиосвязи «точка – точка». Однако во многих вариантах использования авиации необходимо решение задач управления и информационного обмена между множеством абонентов, например, при групповых действиях, групповом самолетовождении и групповой радиоэлектронной борьбе, что определяет актуальность дальнейшего решения задачи создания авиационных сетей связи в СМВ диапазоне.

На предприятии создана новая аппаратуры радиосвязи СМВ диапазона, предназначенная для высокоскоростной передачи данных и видеоинформации. В частности, разработан приемопередающий модуль для организации сетевой архитектуры и обеспечения двусторонней радиосвязи в режиме полного дуплекса с временным разделением. При разработке применялись принципы и технология SDR, позволяющие гибко реконфигурировать радиотехнические параметры приемного и передающего трактов. Основу приемопередающего модуля составляют антенная система, модуль аналоговой обработки сигналов, приемопередающие устройства, модуль цифровой обработки сигналов, модулятор и демодулятор [4].

Приемопередающий модуль СМВ диапазона имеет два существенно различающихся варианта исполнения. Первый вариант имеет антенну с круговой диаграммой направленности в азимутальной плоскости. Он обеспечивает устойчивую связь в условиях прямой радиовидимости на дальностях до 200 км со скоростью передачи данных порядка 10 Мбит/с. Во втором варианте модуля применяются активные фазированные антенные решетки (АФАР), обеспечивающие электронное формирование диаграммы направленности. Применение направленных антенн позволяет получить значительный энергетический выигрыш и потенциально обеспечить скорость передачи информации до 100 Мбит/с [4]. Заданная надежность связи при ухудшении состояния радиоканала достигается с помощью адаптивного выбора сигнально-кодовых конструкций посредством соответствующего снижения скорости передачи информации. Кроме того, применение направленных антенн позволило реализовать пространственное разделение каналов, при котором несколько пар абонентов, находящихся на различных азимутальных направлениях, одновременно взаимодействуют на одной частоте, когда межканальные помехи находятся на допустимом уровне.

В результате при соответствующем усложнении алгоритмов множественного доступа и распределения канальных ресурсов, реализации оценивания направления прихода сигналов и слежения за положением абонентов достигается увеличение пропускной способности всей системы связи. Наконец, применение направленных антенн обеспечивает более высокую скрытность и, как следствие, помехозащищенность радиолиний. Вместе с этим для обеспечения устойчивой связи с применением направленных антенн необходимы управление лучом диаграммы направленности, оценка направления прихода сигналов и слежение за положением абонентов.

Моделирование новых сетевых режимов связи и разработка протоколов информационно-логического взаимодействия абонентов в совокупности со сформированными техническими решениями позволяют создавать широкополосные сети связи на основе авиационных терминалов, созданных в НПП «ПРИМА».

Разработка технического облика бортовых комплексов связи для взаимодействия БПЛА

Наряду с традиционными вариантами исполнения БКС для оперативно-тактической и армейской авиации за последние годы накоплен опыт по разработке БКС для беспилотных летательных аппаратов (БпЛА), которые находят все более широкое применение для решения разведывательных, ударных и других специальных задач. Эффективность решения этих задач в значительной мере определяется возможностями по созданию надежных и достаточно высокоскоростных информационных и командных радиолиний, а также организации сетевых режимов взаимодействия, необходимых для обеспечения групповых действий.

На сегодня связь с БпЛА зачастую базируется на применении широкополосных радиолиний с наземными пунктами управления (НПУ). Более перспективный вариант построения систем связи для БпЛА кроме взаимодействия с НПУ, предполагает реализацию сетевых режимов обмена данными в группах БпЛА, а также между БпЛА и пилотируемыми ЛА.

Основу для построения бортовых комплексов связи БпЛА могут составить технические решения и технологии построения БКС для пилотируемой авиации. Вместе с тем имеется ряд принципиальных различий в вариантах использования БКС БпЛА и пилотируемого ЛА, которые отражаются в тактико-технических требованиях к соответствующим комплексам и определяют состав решаемых задач [5]. С одной стороны, очевидно, что отсутствие пилота определяет некоторую аппаратурную и функциональную избыточность БКС самолета по отношению к БКС БпЛА (в частности, исключается необходимость в применении на борту пультов управления). С другой стороны средства связи БпЛА должны функционировать в полностью автономном режиме, что определяет необходимость создания новых организационно-распорядительных документов, регламентирующих информационный обмен и взаимодействие БпЛА с пилотируемыми ЛА, БпЛА между собой, а также с НПУ.

Для разработки новой концепции сетевого взаимодействия проведен анализ активно развивающейся за рубежом методологии самоорганизующихся сетей связи для ЛА [6, 7]. В таких сетях каждый абонент может являться как оконечной системой, формирующей и получающей потоки данных, так и ретранслятором потоков от других узлов, что образует многосвязную (ячеистую) топологию сети. Самоорганизующаяся сеть позволяет существенно улучшить возможности по доведению информационных потоков, повысить живучесть системы и расширить территорию выполнения операций за счет автоматической ретрансляции данных.

В условиях воздействия различных дестабилизирующих факторов, в том числе преднамеренных помех, самоорганизующаяся сеть способна обеспечивать высокие показатели надежности связи и устойчивости функционирования за счет применения новых методов управления сетью, автоматической реконфигурации сетевой топологии, а также многопутевой маршрутизации. Так, ухудшение сигнально-помеховой обстановки на некотором радионаправлении учитывается при определении маршрутов передачи блоков данных (пакетов) посредством динамической корректировки топологии самоорганизующейся сети.

Учитывая различный статус абонентов перспективной гетерогенной сети воздушной радиосвязи (различные типы пилотируемых ЛА, БпЛА, командных пунктов и НПУ), для обеспечения сетевого взаимодействия предлагается сочетание иерархического подхода с элементами самоорганизации.

В результате проведенных работ по разработке концепции и технического облика системы связи с БпЛА сформирована базовая структурная схема БКС перспективного БпЛА. В зависимости от класса БпЛА (тяжелый, средний, легкий) предполагается использование различного состава каналообразующей аппаратуры ДКМВ, МВ-ДМВ и СМВ диапазонов, а также терминалов спутниковой связи. Необходимость кардинального снижения массогабаритных характеристик аппаратуры для БпЛА среднего и легкого классов привела к созданию новых МВ-ДМВ радиостанций.

Заключение

Таким образом, научно-технический задел НПП «ПРИМА», включающий сформированные технические решения, серийно выпускаемые радиостанции и перспективные радиостанции, а также современные процессы и технологии разработки, достаточны для построения систем радиосвязи в интересах пилотируемой и беспилотной авиации.

Важнейшими задачами по обеспечению сетевого взаимодействия как пилотируемой, так и беспилотной авиации является создание новых унифицированных и взаимоувязанных стандартов связи на весь стек протоколов, определяющих, в частности, сигнально-кодовые конструкции, методы множественного доступа, процедуры ретрансляции и маршрутизации, способы назначения сетевых адресов и методы аккредитации абонентов в сети воздушной связи.

Список литературы

1. 1. Скрипник И.В. Опыт разработки и направления развития радиосвязного оборудования для пилотируемой и беспилотной авиации // Электросвязь, 2022. № 3. С. 24-29.

2. 2. Скрипник И.В. Опыт разработки и направления совершенствования бортовых комплексов связи для пилотируемой и беспилотной авиации // Труды XXII Российской межведомственной научно-технической конференции «Новые информационные технологии в системах связи и управления» (7-8 сентября 2023 г.). Калуга: Ноосфера. 2023. С. 192-196.

3. 3. Леньшин А.В., Тихомиров Н.М., Попов С.А. Бортовые радиоэлектронные системы. Основы построения: учебное пособие; под ред. А.В. Леньшина / Воронеж: Издательско-полиграфический центр «Научная книга», 2021. 486 с.

4. 4. Скрипник И.В. Подход к построению широкополосных авиационных сетей связи на основе приёмопередающих модулей НПП «ПРИМА» // Тезисы докладов VI Международной научно-технической конференции «Радиотехника, электроника и связь» (6–8 октября 2021 г.). Омск: ОНИИП. 2021. С. 92–94.

5. 5. Скрипник И.В. Задачи обеспечения сетевого взаимодействия БПЛА // Сборник научных статей по материалам VIII Международной научно-технической конференции, посвященной столетию образования войск связи «Современное состояние и перспективы развития систем связи и радиотехнического обеспечения в управлении авиацией» (23-24 октября 2019 г.). Воронеж: ВУНЦ ВВС «ВВА». 2019. С. 56-61.

6. 6. Скрипник И. В. Задачи разработки самоорганизующейся сети связи беспилотных летательных аппаратов // Материалы XXVI Международной научно-технической конференции «Информационные системы и технологии» (ИСТ – 2020). Н.Новгород: НГТУ. 2020. С. 179-183.

7. 7. Трушанин А.А., Скрипник И.В., Милов В.Р. Опыт разработки и пути совершенствования самоорганизующихся авиационных сетей связи // Электронный журнал: Наука, техника и образование. № СВ1(45). 2024. С.199-204.

УДК 004.7

Подход к технической реализации алгоритмов управления квазирезервированными устройствами комплексов аппаратно-программных средств

Лукин К. И., Сызранцев Г. В.

АО "Супертел", г. Санкт-Петербург, Россия

Аннотация: *в статье рассматривается подход к управлению квазирезервированными устройствами в составе комплексов аппаратно-программных средств для информационно-телекоммуникационных систем специального назначения и обосновывается необходимость совместного управления техническими и функциональными параметрами комплексов аппаратно-программных средств с учётом дестабилизирующих факторов и потока поступающих заявок. В качестве базового принципа конструирования предлагается функционально-модульный подход, а в основу управления техническим ресурсом – специальный критерий, нацеленный на максимизацию наработки на отказ, обеспечение требуемого качества обслуживания нагрузки и рациональное использование ресурсов (в том числе энергетических). Представлен вариант технической реализации и описана структурная схема устройства, включающая блоки уплотнения, модуляции, передачи и приёма, управления, измерения параметров среды, вычисления ошибок и др. Результаты показывают, что предложенные технические решения позволяют снизить потери производительности комплексов аппаратно-программных средств, повысить наработку на отказ и существенно сократить время восстановления при отказах. Кроме того, метод обеспечивает более быструю (по сравнению с известными подходами) оценку состояния каналов телеметрии и синхронизации, что повышает эксплуатационную надёжность и ремонтопригодность информационно-телекоммуникационных системах специального назначения.*

Ключевые слова: *информационно-телекоммуникационные системы, управление и алгоритмы, надёжность, диагностика, методы и математический аппарат, цифровая система передачи, дублированные системы с динамической задержкой, функционально-модульный принцип конструирования*

Исследования показывают, что в перспективных информационно-телекоммуникационных системах специального назначения (ИТКС СН), которые будут иметь мультисервисный, мультипротокольный характер функционирования, техническая реализуемость устройств комплексов аппаратно-программных средств (КАПС) должна предусматривать совместное управление их техническими и функциональными параметрами. При этом алгоритмы управления целесообразно формировать на основе оценки состояния дестабилизирующих факторов и потока заявок, поступающих на вход КАПС.

С учетом результатов, полученных в [1] в основу управления техническим ресурсом таких КАПС может быть положен критерий (1), а в качестве базового принципа конструирования выбран функционально-модульный:

$$\begin{cases} \max\limits_{\vec{t}\in T} T_0(\vec{t}) \quad \text{при} \quad K_{\sum тр} \le K_{\sum}(t),\ P_{энер.тр}(T) \le P_{\sum}(T); \\ \max\limits_{\vec{t}\in T} \overline{K}(\vec{t}) \quad \text{при} \quad K_{\sum тр} \ge K_{\sum}(t), P_{энер.тр} > P_{\sum}(t); \\ V \le V_{доп},\ W(t) \ge W_{тр}. \end{cases} \qquad (1)$$

Задача (1) формулируется следующим образом:

необходимо обеспечить такое распределение времени использования различного оборудования многофункциональных КАПС при эксплуатации их в ИТКС на заданном интервале времени Т: $\vec{t} = \left[t_1^*,\ t_2^*, ..., t_\xi^*\right]^T$, где ξ – количество непересекающихся множеств функциональных преобразований (НМФП) в структуре КАПС, которые максимизировали бы:

среднюю наработку на отказ $T_0(\vec{t})$ комплекса при $t_i^* \ge 0$ для всех $i = \overline{(1,\ \xi)}$;

обслуживание всей поступающей нагрузки Z(t) на различные виды услуг с требуемым качеством;

(при условии, что минимально необходимая производительность КАПС $K_{\sum ТР} \le K_{\sum}(T)$ меньше его возможностей, а энергетические возможности $P_{\sum} \ge P_{энерг.тр}(T)$ превышают их требуемое количество),

или:

достижение максимальной средней производительности на интервалах времени $Z(t)=Z_{max}$;

выполнение требований по своевременности и достоверности $W(T) \ge W_{ТР}$ передачи различных видов информации на заданном периоде эксплуатации оборудования;

(при условии, что энергетические возможности комплекса используются в полном объеме с задействованием всех ресурсов, в том числе в случаях воздействия дестабилизирующих факторов и ограничений на объем ресурсов: $V \le V_{доп}$).

Критерий (1) соответствует рассмотрению КАПС на уровне качества самоорганизации, отображает целевое предназначение КАПС в ИТКС СН и отвечает системе предпочтений ЛПР. Критерий показывает возможность обмена разнородным трафиком в сети с требуемым качеством и минимальным расходом различных ресурсов.

Возможный вариант технической реализации таких КАПС приведен на рис. 1.

Данное устройство содержит блок уплотнения 1, модулятор 2, передатчик 3, передающую антенну 4, приемную антенну, приемник 6, блок управления передатчиком 7, измеритель коэффициента состояния среды распространения электромагнитных сигналов 8, блок вычисления дисперсии 9, блок формирования сигналов телеметрии 10, блок вычисления среднего квадрата ошибки 11, блок управления включением канального оборудования 12,

задающий генератор 13, первый 14 и второй 21 делители с переменным коэффициентом деления, первый 15 и второй 17 демультиплексоры, блок определения числа включенных каналов16, дешифратор 18, приемник команд 19, блок выделения синхросигнала 20, блок разуплотнения 22, блок вычисления значения мощности 23, блоки задержек 24, 25, 26.

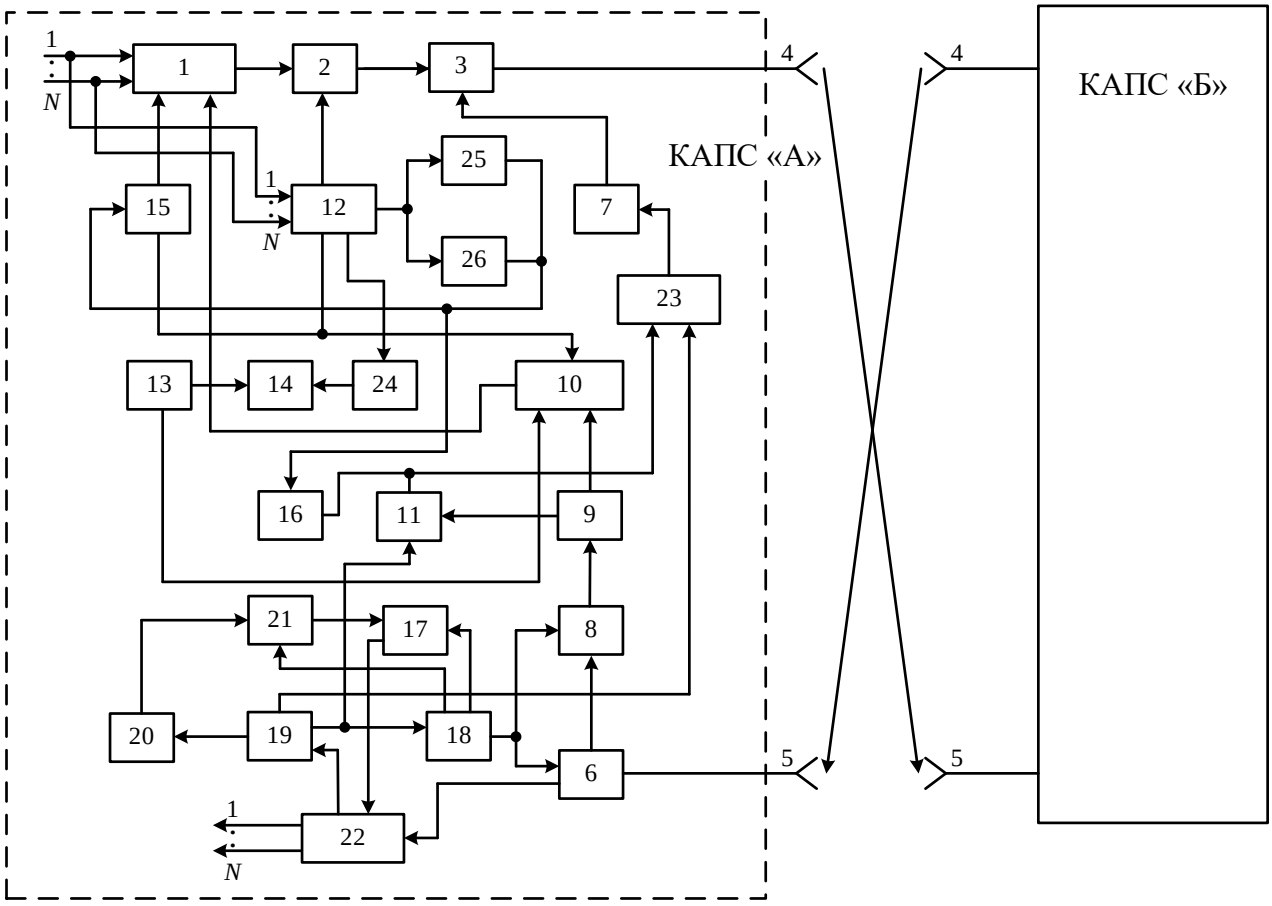


Рис. 1. Структурная схема построения квазирезервированных КАПС (вариант)

Данная структура КАПС, обеспечивает управление скоростью передачи станции путем включения и выключения аппаратуры канального оборудования на основе сигналов, поступающих по информационным соединительным линиям, а также изменением частоты следования тактовых импульсов. Одновременное повышение (уменьшение) выходной мощности осуществляется по командам вычислителя 23, который при их формировании учитывает состояние среды распространения электромагнитных сигналов, оцениваемое блоками 8, 9 и 11. Рациональное использование канального оборудования и модульного усилителя мощности (УМ) реализуется с помощью демультиплексоров 15, 17 и блока управления 7. Остальные элементы применяются для синхронизации работы элементов цифровой системы передачи (ЦСП) и управляющих устройств КАПС.

Приведенные на рис. 1 устройства обеспечивают реализацию правила (1) при одновременном перераспределении нагрузки между оборудованием КАПС,

т.е. осуществляется рациональный режим его эксплуатации во время функционирования ЦСП в составе мультисервисных ИТКС СН.

При этом необходимо отметить, что реализация блоков управления 7 и 12 на процессорах с изменяющимся программным обеспечением позволяет изменить алгоритм управления конфигурациями устройств, то есть в процессе эксплуатации в зависимости от температуры, давления, нагрузки адаптивно применять алгоритмы управления на основе рекуррентных последовательностей или по диагностическим параметрам.

Рассмотрим алгоритм и возможную техническую реализацию псевдослучайного управления конфигурациями ресурсосберегающих устройств в процессе эксплуатации КАПС в ИТКС СН.

Так как для многих устройств, используемых при реализации КАПС (рис. 1), априорно будут известны условия неравнопрочности узлов, образующих функциональные конфигурации КАПС, либо коэффициент их приведения, при котором целесообразно использовать методы скользящего ресурсосбережения для повышения их избыточности, то в этих условиях управление конфигурациями устройств целесообразно обеспечивать на основе рекуррентных последовательностей. К таким устройствам можно отнести: аппаратуру цифрового объединения и разъединения потоков, измеренных в ОЦК; устройство автоматической регулировки усиления, малошумящие усилители в приемных трактах; антенные системы на основе широкодиапазонных фазированных антенных решеток и др. Известны примеры использования данного подхода и для других устройств КАПС, например, коммутационного оборудования [2, 3, 4].

Известные из практики разработчиков КАПС устройства обеспечивают выравнивание эксплуатационного ресурса (ЭР) узлов функциональных элементов с целью увеличения их временной (запас времени на восстановление исправности при сохранении работоспособности), функциональной (за счет режима резервирования), структурной (посредством скользящего резервирования и равномерного расхода эксплуатационного ресурса) избыточности, а, следовательно, позволяют повысить эксплуатационную надежность ветвей ИНС мультисервисных ИТКС СН.

Однако в процессе эксплуатации КАПС в мультисервисных ИТКС СН чрезвычайно важное значение для повышения их эксплуатационного ресурса имеет управление резервируемыми устройствами по диагностическим параметрам.

Как показали проведенные исследования, неравнопрочность в смысле вероятности безотказной работы по причине разного количества элементов в узлах КАПС (неоднородности температурных полей, нагрузки, давления и др.), приводит к необходимости определения рациональных интервалов активной работы функциональных, имеющих одинаковое назначение в КАПС.

Оно осуществляется по известным алгоритмам, однако имеются способы решения этой задачи на основе оценки косвенных диагностических параметров, позволяющих при определении целесообразной конфигурации КАПС

при реконфигурациях без потери связи учитывать разную скорость старения оборудования для обеспечения максимальной наработки на отказ функциональных элементов КАПС. Прежде всего, к таким элементам относятся, например, мощные передатчики, источники вторичного электропитания, в которых бывает особо важным учет неоднородности температурных полей и др.

В данном аспекте проведем сравнительный анализ расхода ресурсов устройствами КАПС применительно к различным алгоритмам управления процессом их функционирования.

Например, для управления усилительными элементами (УЭ) без учета их неравнопрочности в соответствии с выводами, полученными в [1], интенсивность отказов определится как:

$$\lambda_1 = \sum_{i=1}^{N} \lambda(20^o)_{вкл} \cdot \exp[0{,}022(T_i-20^o)] \cdot P_i + \sum_{i=1}^{N} \lambda(20^o)_{откл} \cdot \exp[0{,}022(T_i-20^o)] \cdot (1-P_i),$$

где P_i - вероятность включения i-го УЭ; $\lambda(20^\circ)_{вкл}$ – интенсивность отказов включенных УЭ при $T^0=20^0C$; $\lambda(20^\circ)_{откл}$ – интенсивность отказов отключенных УЭ при $T^0=20^0C$; T_i - температура включенного УЭ.

С учетом неравнопрочности (т.е. учетом неравномерности температурных режимов УЭ) интенсивность отказов рассчитывается по формуле:

$$\lambda_2 = N_a \cdot \lambda(20^o)_{вкл} \cdot \exp[0{,}022(T_i-20^oN)] + (N-N_a) \sum_{i=1}^{N} \lambda(20^o)_{откл} \cdot \exp[0{,}022(T_i-20^o)],$$

где $N_a = N - N_{p.}$.

Пусть, например, N=5, $T_{ном}=60$, $T_i = 20^0 + 20^0(i-1)$, $P_i=0{,}2$; $\lambda(20^0)_{откл} = 10^{-5}\,1/ч$, $\lambda(20^0)_{вкл} = 10^{-4}\,1/ч$, $N_a=4$. Тогда, разделив второе выражение на первое, получим $G_\lambda \approx 1{,}25$, другими словами интенсивность отказов УЭ уменьшилась на 20%.

Таким образом, в рассмотренных условиях учет неравнопрочности узлов функциональных элементов КАПС позволяет существенно увеличить их наработку на отказ. Приведенное на рис. 1 техническое решение обладает всеми достоинствами данного подхода, в том числе связанных с организацией агрегатного ремонта КАПС, реализуемого в процессе их эксплуатации в ИТКС СН.

Другими важными устройствами, направленными на обеспечение устойчивого функционирования КАПС в составе ИТКС СН (рис.1), является канал телеметрии и канал синхронизации, образуемые блоком формирования сигналов телеметрии 10 и блоком выделения синхросигналов 20, соответственно. Для повышения их надежности установлена целесообразность применения дублированной системы с динамической задержкой [5].

Как следует из вышесказанного, для работы устройства (рис. 1) необходим будет блок анализа качества работы резервированных устройств (БАКРРУ), имеющий важное значение, поскольку на него предполагается возложить

функцию обеспечения требуемой достоверности принятия решения по реконфигурации дублированных систем КАПС.

В качестве БАКРРУ может быть использован сумматор по модулю 2. Однако, для каналов телеметрии и синхронизации, образуемых блоками 10 и 20 (рис. 1) соответственно, такое техническое решение может быть недостаточным, так как возможны сбои в системах из-за динамического изменения среды распространения сигналов. Диагностирование данных элементов КАПС ИТКС СН может быть основано на схеме независимых испытаний, базирующейся на усеченных биномиальных распределениях, функция распределения которых имеет вид [6]:

$$\begin{cases} 0, i < Y, \\ \sum\limits_{i=Y}^{]KZ[} \begin{pmatrix}]KZ[-Y \\ i-Y \end{pmatrix} \cdot p^{i-Y}(\omega) \cdot (1-p(\omega))^{]KZ[-1} = 1, \\ 0, i >]KZ[, \end{cases} \quad (2)$$

где $p(\omega)$ - вероятность появления единичных символов в любом разряде на выходе аппаратуры цифровых систем передачи; $\omega \subset \Omega$, Ω – пространство элементарных событий мощностью Z, представляющей разрядность выходной цифровой последовательности единичных и нулевых символов $(\omega_1, \omega_2, ..., \omega_z)$; K – коэффициент, характеризующий допустимую кратность единичных сигналов на выходе КАПС, образующих каналы телеметрии и синхронизации в Z-разрядных последовательностях при N испытаниях, причем $0 < K \le 1$; Y – минимально допустимое количество единичных символов на выходе аппаратуры в Z-разрядных последовательностях при N испытаниях; при этом $Y = (1, ...,]KZ[-1)$; $]*[$ - "антье", наибольшее целое.

Здесь, под усеченным биномиальным распределением понимается закон распределения вероятности появления случайной величины при ограничении на число появлений случайной величины ξ(ω), (например, запрет на появление длинных серий единичных и нулевых символов) в некотором количестве независимых испытаний. Частным случаем усеченного биномиального распределения при начальных параметрах усечения Y=0 и K=1 является биномиальное распределение [6].

Тогда при N-испытаниях дублированных КАПС на ее выходе возникают последовательности $(\omega_1, \omega_2, ..., \omega_z)$, содержащие различное количество единичных символов $Y \le \xi(\omega) \le]KZ[$ в каждом испытании. Для решения задачи идентификации состояния резервированных устройств необходимо определить числовые характеристики усеченного биномиального распределения, описывающего статистические характеристики сигналов на ее выходе. Поскольку случайная величина $\xi(\omega)$ является дискретной, имеет решетчатое распределение, то ее математическое ожидание и дисперсия, обозначаемые $M\xi$ и $D\xi$ соответственно, находятся с помощью формул [6, 7]:

$$\begin{aligned} M\xi &= (]KZ[-Y)\cdot p(\omega)+Y, \\ D\xi &= (]KZ[-Y)\cdot p(\omega)\cdot(1-p(\omega)). \end{aligned} \tag{3}$$

Тогда на основе решения данной системы уравнений относительно неизвестных параметров усечения K и Y методом подстановки получим следующие выражения:

$$\begin{cases} K=\left(M\xi+D\xi/p(\omega)\right)/Z, \\ Y=M\xi-D\xi/\left(1-p(\omega)\right). \end{cases} \tag{4}$$

где $M\xi=\left[\sum_{j=1}^{N}N(1)_{ij}\right]/N$,

$$D\xi=\sum_{j=1}^{N}\left[N(1)_{ij}-m(1)_i\right]^2/N, \tag{5}$$

а $p(\omega)=\left[\sum_{j=1}^{N}N(1)_{ij}\right]/NZ$.

Выбор Z определяется требуемой точностью оценки вероятности появления единичного символа $p(1)$ в каждой временной позиции. Проведенные исследования оценки показывают, что поскольку такая вероятность может быть вычислена в полной группе событий реализации различных векторов двоичных последовательностей, то данная величина может быть определена как отношение числа комбинаций, в котором участвуют сигнальные единицы данной временной позиции к общему числу возможных реализаций комбинаций [7]:

$$p_{\text{тр}ij}=p(\xi_j)=\frac{\sum_{j=1}^{]kn[}C_{n-1}^{j-1}}{\sum_{j=1}^{]kn[}C_n^j}. \tag{6}$$

Проведенные расчеты и построенные на их основе графики, приведенные на рис. 2, показывают, что для того, чтобы погрешность измерения вероятности появления единичного символа не превышала 10%, Z должно быть не менее 20 [6, 7, 8].

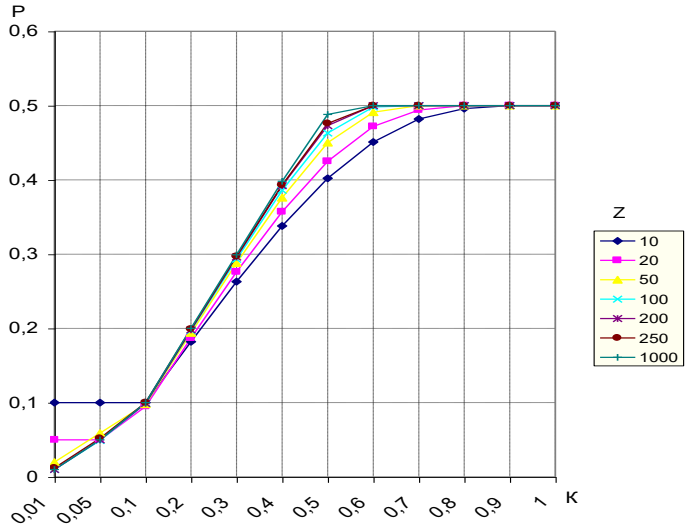


Рис.2. Зависимость точности оценки измеряемой величины от количества испытаний

Второй составляющей является выбор необходимого числа сегментов N. Значение N выбирается исходя из требований метрологической точности измерений математического ожидания и дисперсии числа единичных символов в Z-разрядных сегментах тестовой последовательности. Для обеспечения требуемой точности N должно быть не менее 10. Изменение вероятности появления единичных символов $p(1)$, параметров усечения K и Y говорит об изменении состояния резервированной аппаратуры цифровых систем передачи и характере его изменения, а именно:

– увеличение величины $p(1)$ относительно значения $p_0(1)$ говорит о преобладании отказов, проявляющихся в наличии единичных символов, а уменьшение – о преобладании отказов, проявляющихся в наличии нулевых символов;

– увеличение значения Y относительно значения Y_0 свидетельствует об уменьшении числа комбинаций снизу, то есть о появлении отказов или сбоев, проявляющихся в появлении фиксированного единичного символа;

– уменьшение значения K относительно значения K_0 показывает наличие в комбинациях фиксированных нулевых символов;

– одновременное изменение значений Y и K свидетельствует о кратном отказе или сбое.

При этом значения Y, Y_0, K и K_0 определяются по формулам:

$$\begin{cases} K_0 = \left(m_0(1) + d_0(1)/p_0(1)\right)/Z, \\ Y_0 = m_0(1) - d_0(1)/\left(1 - p_0(1)\right), \end{cases} \quad (7)$$

$$\begin{cases} K = \left(m(1) + d(1)/p_0(1)\right)/Z, \\ Y = m(1) - d(1)/\left(1 - p_0(1)\right), \end{cases} \quad (8)$$

где $m_0(1)$, $d_0(1)$, $p_0(1)$ K_0, Y_0 - значения математического ожидания, дисперсии и вероятности появления единичных символов, параметров усечения, соответственно, при работоспособном состоянии диагностируемой аппаратуры.

Для комплекса аппаратуры, реализующей полную группу векторов $(\omega_1, \omega_2, ..., \omega_z)$, кратность отказов (то есть число искаженных блоков сигналов) определяется по формуле [6]:

$$L = Y + (1 - K) \cdot Z \quad (9)$$

Для комплекса аппаратуры, у которой в рабочем режиме имеется запрет на определенные комбинации единичных и нулевых символов, кратность искажений блоков сигналов определяется по формуле:

$$L = \begin{cases} (Y_0 - Y + \left(1 - \left(K_0 - K\right)\right) \cdot Z)/2, \text{при} Y > Y_0, K < K_0; \\ \left(\left(Y_0 - Y\right) + \left(1 - \left(K_0 - K\right)\right) \cdot Z\right)/4, \text{при} Y < Y_{0,} K < K_0; \\ \left(\left(Y - Y_0\right) + \left(1 - \left(K - K_0\right)\right) \cdot Z\right)/4, \text{при} Y > Y_{0,} K > K_0. \end{cases} \quad (10)$$

Реализацию изложенного метода можно пояснить следующим образом.

На вход диагностируемой аппаратуры подаются N раз Z-разрядные сегменты информационной последовательности. При настройке ЦСП в качестве имитатора информационной последовательности применяют псевдослучайную последовательность, которая образуется специально сгенерированными сигналами на основе генератора псевдослучайных импульсов, построенного на рекуррентной линии задержки [1]. Примем, что число тактовых импульсов в одном сегменте Z=5, а число передаваемых сегментов информационной (ИП) или псевдослучайной последовательности (ПСП) N=32, что достаточно для получения достоверных оценок параметров усечения [6].

Сформированная ИП или ПСП подается на вход резервированных устройств, где происходит ее преобразование по установленному алгоритму (кодирование, модуляция, перенос в область высоких частот, усиление, передача, прием, демодуляция, декодирование. При работе КАПС по шлейфу ПСП ослабляется аттенюатором и смешивается с сигналом шума с целью "усиления" количества искаженных импульсов для имитации среды распространения сигналов. В этом случае имеется возможность проверки работоспособности КАПС в целом. Рассмотрим этот режим более подробно.

Сигналы ПСП выделяют после каждого преобразования в блоках преобразования сигналов передающего и приемного трактов для каждого из резервированных КАПС. Из каждой псевдослучайной последовательности $F_i(t)$ выделяют Z-разрядные сегменты. В каждом j-м Z-разрядном сегменте

каждой i-й псевдослучайной последовательности $F_i(t)$ вычисляют число единичных символов $N(1)_{ij}$. Затем для каждой i-й псевдослучайной последовательности $F_i(t)$ вычисляются, соответственно, значения математического ожидания числа единичных символов в одном сегменте псевдослучайной последовательности $m(1)_{io}$, дисперсии числа появления единичных символов $d(1)_{io}$ и вероятности появления единичного символа $p(1)_{io}$. Таким образом, получают $m(1)_{io}=2,5$, $d(1)_{io}=1$, $p(1)_{io}=0,5$.

Далее вычисляются значения параметров усечения Y_{io} и K_{io}, где $Y_{io}=0,5$ и $K_{io}=0,9$.

Таким образом, получаются R значений для каждой i-й псевдослучайной последовательности $F_i(t)$: $m(1)_{io}$, $d(1)_{io}$, $p(1)_{io}$, Y_{io} и K_{io}, которые соответствуют параметрам исправных контролируемых блоков диагностируемой аппаратуры, образующей каналы телеметрии и синхронизации.

Таким образом, увеличение $p(1)_i=0,6$ относительно значения $p(1)_{io}=0,5$ и значения $Y_i=1,38$ относительно значения $Y_{io}=0,5$, свидетельствует о том, что характер неисправности будет проявляться в появлении либо фиксированного единичного символа, либо перемежающегося отказа в виде скользящего единичного символа, либо периодического сбоя. Значение $L_i=1$ говорит о том, что отказ не является кратным.

Анализируя рассмотренные примеры, можно сделать вывод о том, что использование рассматриваемого способа позволяет идентифицировать сбои и перемежающиеся одиночные и кратные отказы диагностируемого по шлейфу комплекса аппаратуры (рис. 1). Это достигается вычислением параметров усечения псевдослучайной последовательности, подающейся в каналы телеметрии и синхронизации, изменение которых связано с изменением коэффициента ошибки, технического состояния диагностируемой аппаратуры, характером и кратностью отказов.

Описание работы устройства диагностики состояния аппаратуры, образующей каналы телеметрии и синхронизации, представлено в [1].

Эффективность оценки излагаемого подхода к техническому решению заключается в следующем. Сокращение сроков достоверной оценки состояния комплексов аппаратуры (рис. 1), образующих каналы телеметрии и синхронизации, позволяет существенным образом влиять на производительность ИНС ИТКС СН. Так, проверка их работоспособности известными методами требует при такой же точности оценки более 5 минут, что в несколько раз превышает временные затраты относительно предлагаемого метода. Это позволит существенно сократить время простоя ветвей ИНС ИТКС СН. Идентификация характера и кратности отказа (сбоя) также повышает их ремонтопригодность, что ведет к возрастанию их эксплуатационной надежности, что соответствует критерию (1). Важно отметить, что изложенное техническое решение позволяет оценивать коэффициент ошибок каналов телеметрии и синхронизации при эпизодическом контроле их состояния во время развертывания и вхождения в связь или при возникновении полных отказов КАПС (рис. 1) в ходе обеспечения связи. Для уменьшения вероятности

их возникновения в ходе боевой эксплуатации следует реализовать достоверный контроль состояния резервируемых устройств с целью уменьшения простоев КАПС, а значит увеличения их производительности по критерию (1).

Предлагаемая структурная схема БАКРРУ, обеспечивающая реализацию функции непрерывной идентификации состояния резервированных элементов 1 и 2 (каналов телеметрии или синхронизации ЦСП (рис. 1)), обеспечивает выявление сбоев и отказов одного из устройств 1 или 2, что позволяет передавать сигналы телеметрии и синхронизации на выход дублированной схемы с динамической задержкой. Причем с помощью блока анализа идентифицируются неработоспособные устройства путем сравнения с нормированными величинами коэффициента побитовой ошибки, и формируется сигнал на реконфигурацию системы. При отказе обоих устройств 1 и 2 система отключается, а блоком 5 обеспечивается включение генератора ПСП и алгоритма выявления отказавшего элемента КАПС. При отказе одного из устройств блок 5 показывает, в каком из устройств - 1 или 2 произошел сбой или отказ. Если причиной выключения КАПС (рис. 1) являлся внешний сбой (например, из-за питающих напряжений), то он возвращается в работу, а после реализации алгоритмов работы блоков - в режим восстановления путем поиска отказавших агрегатов с использованием внешних средств системы диагностирования.

Таким образом, предлагаемые способы технической реализации позволяют значительно понизить потери производительности КАПС более чем в 2 раза, повысить его наработку на отказ более чем в 2 раза и значительно уменьшить время восстановления при отказе в ходе их боевой эксплуатации в ИТКС СН. Это означает, что предложенные технические решения значительно повышают функциональную эффективность КАПС.

Список литературы

1. Курносов В. И. Методы и способы управления качеством функционирования телекоммуникационных систем специального назначения. – СПб.: ФГУП «НИИ «Рубин», 2007. – 337 с.

2. Лихачев А. М., Курносов В. И. Тенденции технического и технологического развития телекоммуникационных сетей. – СПб.: «Абрис», 1997. - 237 с.

3. Лукин К. И. Способы управления структурами многорежимных и многофунк-циональных комплексов аппаратно-программных средств связи на основе технологий квазирезервирования // Информация и Космос. Специальное приложение. – 2024. – Вып. 3. – С. 221-235. Инв. № Т-809с.

4. Лукин К. И. К вопросу о построении квазирезервированных комплексов аппаратно-программных средств специального назначения // Техника средств связи. 2024, №2 (166). - С. 12-30.

5. Гагарин С. П. Построение системы тактовой сетевой синхронизации в структуре транспортной цифровой сети связи специального назначения // Труды XI-й Всероссийской межведомственной научной конференции

"Актуальные направления развития систем охраны, специальной связи и информации для нужд органов государственной власти Российской Федерации". - Орел: Академия ФСО России, 2019.С. 159–163. Инв. 201/639.

6. Лихачев А. М. Математический аппарат для исследования многофункциональных технических систем на основе усеченных биномиальных распределений // Сборник трудов Всероссийской конференции «Проблемы создания и развития информационно - телекоммуникационных систем специального назначения». Часть 2. – Орел: ВИПС, 1997. – С. 78-92.

7. Вентцель Е. С. Теория вероятностей: учебник для вузов – М.: Высшая школа, 2002. – 367 с.

8. Калихман И. Л., Войтенко М. А. Динамическое программирование в примерах и задачах: учеб. пособие. - М.: Высшая школа, 1992. - 125 с.

УДК 004.05

Операторная модель управления информационно-телекоммуникационной системой специального назначения в условиях воздействий дестабилизирующих факторов

Лукин К. И., Сызранцев Г. В

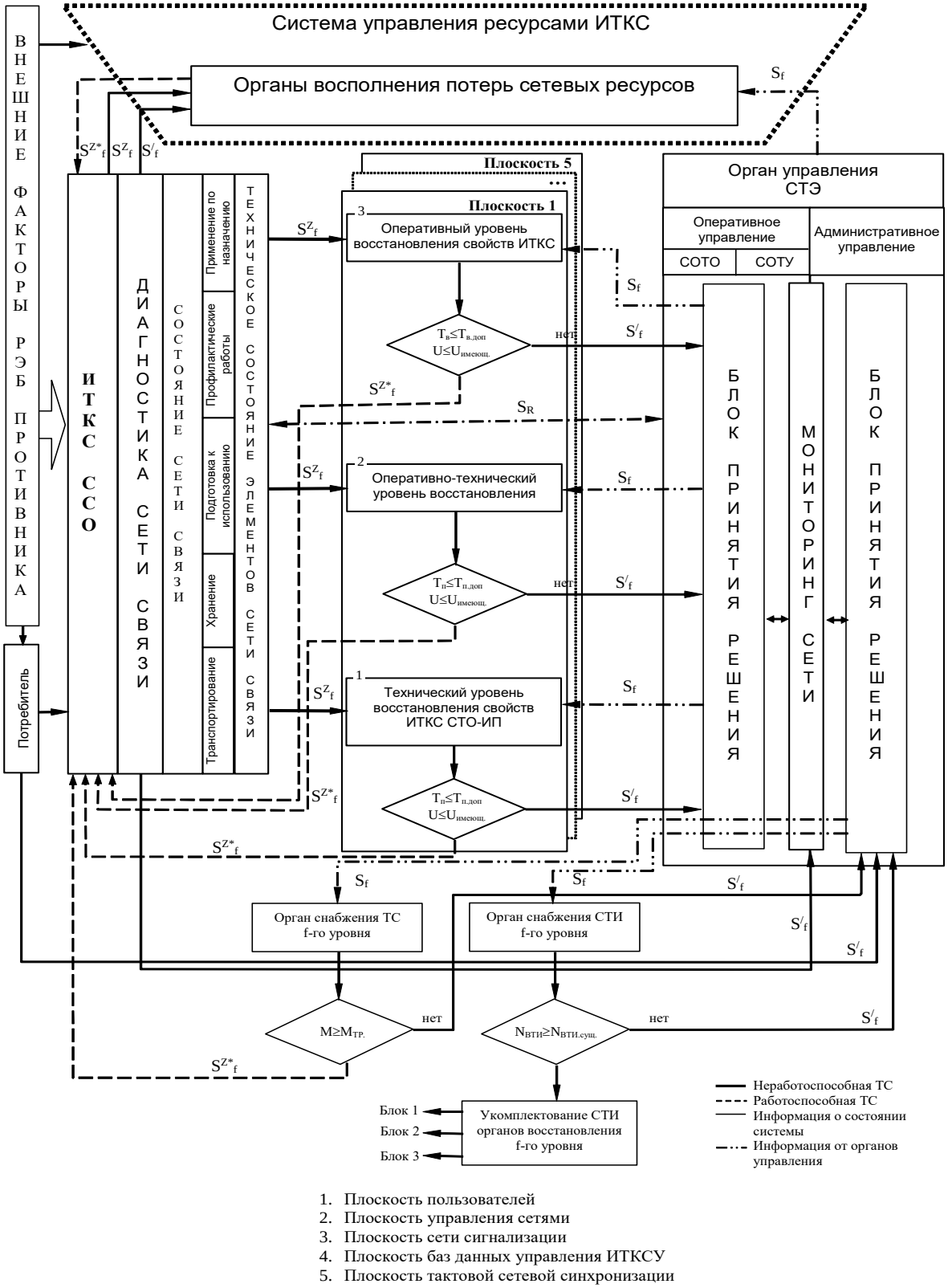
АО «Супертел», г. Санкт-Петербург, Россия

Аннотация: *в статье рассматривается проблема управления мультисервисной информационно-телекоммуникационной системой специального назначения в условиях радиоэлектронной борьбы и иных дестабилизирующих воздействий. Обоснована необходимость адаптивного управления сетевыми ресурсами с учётом динамичных и стохастических угроз, нарушающих функционирование узлов и линий связи, провоцирующих ошибки передачи данных и снижение эффективности управления. Предложена операторная модель описания процессов управления, базирующаяся на дискретном представлении эволюции системы, которая формализует последовательность изменений параметров системы. Для оценки эффективности эксплуатации предложен показатель, объединяющий вероятность успешного функционирования системы, а результаты исследования создают теоретическую основу для построения адаптивных систем управления в условиях комплексного противодействия.*

Ключевые слова*: информационно-телекоммуникационные системы, радиоэлектронная борьба (РЭБ), управление сетевыми ресурсами, модели угроз и воздействий, дискретная модель функционирования, операторная модель управления, маски воздействий, структурные и стохастические матрицы, полиструктура ИТКС, показатели качества и эффективности, векторная оптимизация, надёжность и отказоустойчивость*

Характерной особенностью функционирования мультисервисной информационно-телекоммуникационной системы специального назначения (ИТКС СН) является необходимость обеспечения информационного обмена между ее пользователями в условиях различного рода угроз. Данные угрозы в общем случае обусловливают изменение технического состояния техники связи, нарушают процесс функционирования узлов и линий мультисервисной ИТКС СН, приводят к возникновению ошибок в передаваемых сообщениях, блокированию оперативной и сигнально-управляющей информации и, как следствие, снижают эффективность управления. В этих условиях выполнение требований, предъявляемых к ИТКС СН по обеспечению информационного обмена между ее пользователями, во многом будет определяться характером управления сетевыми ресурсами ИТКС. В то же время сам характер формирования управляющих воздействий будет определяться целями, стоящими пред ИТКС СН в условиях радиоэлектронной борьбы. При этом, как показали исследования [1], данные цели в зависимости от выбранной стратегии радиоэлектронной борьбы могут существенно меняться, что в модельном плане обусловливает необходимость их учета.

Решение совокупности задач управления ИТКС СН (рис. 1) в условиях РЭБ возможно в том случае, когда система управления будет максимально адаптивна к внешним и внутренним возмущениям. Однако создание таких систем применительно к ИТКС СН в условиях РЭБ практически невозможно.



1. Плоскость пользователей
2. Плоскость управления сетями
3. Плоскость сети сигнализации
4. Плоскость баз данных управления ИТКСУ
5. Плоскость тактовой сетевой синхронизации

Рис.1. Модель процесса поддержания требуемых состояний ИТКС СН

Это связано с целым рядом причин, обусловленных стохастической природой дестабилизирующих факторов в условиях РЭБ; высокой динамичностью процессов, протекающих в ИТКС СН, при формировании ее комплексного ресурса; пространственным размахом, определяющим

инерционность исследуемых процессов. Данное обстоятельство характеризует особенности построения модели управления мультисервисной ИТКС СН в условиях информационного и радиоэлектронного противоборства с вероятным противником.

В анализируемых ситуациях применимы принципы, которым должны удовлетворять системы управления, инвариантные до некоторой альтернативы [2].

Для формального описания процессов управления мультисервисной ИТКС СН в радиоэлектронной борьбе за основу целесообразно взять дискретную модель функционирования ИТКС СН и системы радиоподавления (РЭП) противоборствующей стороны с учетом этапности и очередности выполнения задач данными системами в процессе функционирования. В этом случае формально модель управления будет описывать изменение фазового пространства состояний «ИТКС – РЭП» в некоторой последовательности моментов времени, характеризующих процесс изменения данных состояний [3].

Пусть фазовое пространство параметров состояния совокупности «ИТКС – РЭП» описывается вектором $H = \{S, R, S_R, R_S\}$, где S характеризует состояние ИТКС, R – состояние системы РЭП, S_R – воздействие системы РЭП на ИТКС, R_S – воздействие ИТКС на систему РЭБ противоборствующей стороны непосредственно или посредством ресурсов огневого и радиоэлектронного подавления.

В этом случае процесс функционирования системы можно выразить через некоторый оператор Θ. Тогда процесс эволюции системы H в фазовом пространстве состояний может быть представлен последовательностью отображений [2]:

$$\begin{aligned} &H(0), \Theta_1 : \{H(0)\} \to H(1), \Theta_2 : \{H(1), H(0)\} \to H(2), ..., \\ &\Theta_n : \{H(n-1), H(n-2), ..., H(n-k)\} \to H(n), \end{aligned} \quad (1)$$

где: n – номер шага процесса; k – число шагов, на которых проявляется последействие прошлых состояний системы.

Для систем без последействия (марковского типа) уравнение траектории H имеет вид

$$\begin{aligned} &H(0), \Theta_1 : \{H(0)\} \to H(1), \Theta_2 : \{H(1)\} \to H(2), ..., \\ &\Theta_n : \{H(n-1)\} \to H(n). \end{aligned} \quad (2)$$

Операторы преобразования $\Theta_1, \Theta_2, ..., \Theta_n$ в общем случае могут зависеть от номера шага. Однако если цели функционирования системы во времени не меняются, то можно считать $\Theta_1 = \Theta_2 = ... = \Theta_n$.

Характер функционирования системы и целенаправленность ее поведения при формальном представлении процесса эволюции системы (H) заключаются в том, что траектория $H(n)$ есть функция управления U(n), т. е.

$H(n) = H = \{U(n)\}$, где $U(n) = \{U_S(n), U_R(n)\}$ – вектор управляющих параметров ИТКС, $U_R(n)$ – вектор управляющих параметров системы РЭП.

Поскольку параметры состояния и управления системы S, R, S_R, R_S и U – взаимозависимые функции, то при дискретном описании процесса эволюции состояния системы «ИТКС – РЭП» необходимо учитывать последовательность изменения этих параметров.

При этом целесообразно исходить из того, что на каждом (n+1)-м шаге процесса взаимоотношения «ИТКС – РЭП» в соответствии с состоянием ИТКС, сложившемся на предыдущем шаге H(n) и управлении U(n), меняется состояние системы РЭП, т. е. формируется вектор R(n+1).

Изменение состояния системы РЭП определяет новое состояние ее воздействия на ИТКС $S_R(n+1)$. Это, в свою очередь, определяет изменение состояния ИТКС S(n+1) и соответствующее изменение ее воздействия на органы добывания информации РЭП – $R_S(n+1)$. В результате формируется общее состояние системы на (n+1)-м шаге H(n+1) и согласно ему, матрица управления системой U(n+1).

Таким образом, процесс изменения состояния системы $\Theta : \{H(n)\} \rightarrow H(n+1)$ и управления на (n+1)-м шаге можно представить рядом последовательных отображений:

$$\begin{aligned}
&\Theta_1 : \{R(n), S_R(n), R_S(n), S(n), U(n)\} \rightarrow R(n+1),\\
&\Theta_2 : \{R(n+1), S_R(n), R_S(n), S(n), U(n)\} \rightarrow S_R(n+1),\\
&\Theta_3 : \{R(n+1), S_R(n+1), R_S(n), S(n), U(n)\} \rightarrow R_S(n+1),\\
&\Theta_4 : \{R(n+1), S_R(n+1), R_S(n+1), S(n), U(n)\} \rightarrow S(n+1),\\
&\Theta_5 : \{R(n+1), S_R(n+1), R_S(n+1), S(n+1), U(n)\} \rightarrow U(n+1),
\end{aligned} \qquad (3)$$

т. е. оператор системы Θ, определяющий траекторию состояния системы «ИТКС - РЭП», может быть представлен совокупностью последовательно действующих операторов Θ_1, Θ_2, Θ_3, Θ_4, Θ_5, где Θ_1 – оператор, отображающий изменения параметров системы РЭП; Θ_2 – оператор, отображающий характер и степень воздействия системы РЭП на ИТКС (фактически наблюдаемая помеховая обстановка); Θ_3 – оператор, отображающий изменения в ИТКС (ее физической структуре, параметрах и режимах работы элементов) под воздействием системы РЭП; Θ_4 – оператор, описывающий функциональные преобразования состояния системы связи и ее наблюдения системой радиоразведки РЭП; Θ_5 – оператор, характеризующий управляющее воздействие, направленное на изменение состояния ИТКС с учетом текущего состояния и уровня дестабилизирующих факторов.

В то же время процесс формирования управляющих воздействий для ИТКС СН необходимо рассматривать относительно организации управления ее элементами.

В общем случае организация подсистемы управления ИТКС СН может быть представлена в виде многоуровневой иерархической структуры (рис. 2), состоящей из находящихся в определенных отношениях подсистем, элементы которых имеют право принимать решения [2].

При этом управляемый процесс для вышестоящего элемента представляется через взаимодействие связанных подсистем, каждая из которых преследует свои частные цели, имея соответствующий выбор средств для их достижения.

Формальная схема процессов управления ИТКС СН в условиях РЭБ относительно некоторого q-го уровня иерархии (рис. 2) в общем случае может быть представлена в виде рис. 3.

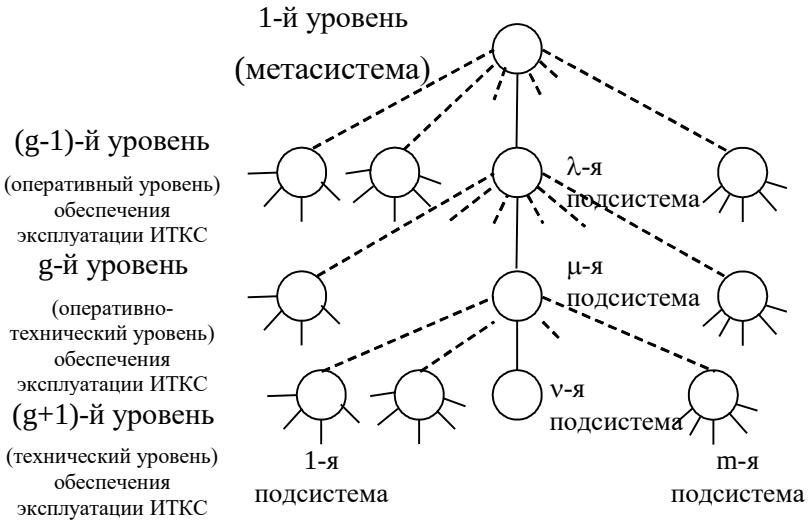


Рис. 2. Взаимоотношения формирования комплексного ресурса в мультисервисной ИТКС СН

Тогда цикл управления как временной интервал между состояниями системы q-го уровня иерархии на соседних шагах процесса

$$\Delta H_q : H_q(n) - H_q(n-1) \tag{4}$$

будет соответствовать разности моментов времени между данными состояниями системы $\tau_{ц_q} = \tau(n+1)_q - \tau(n)_q$.

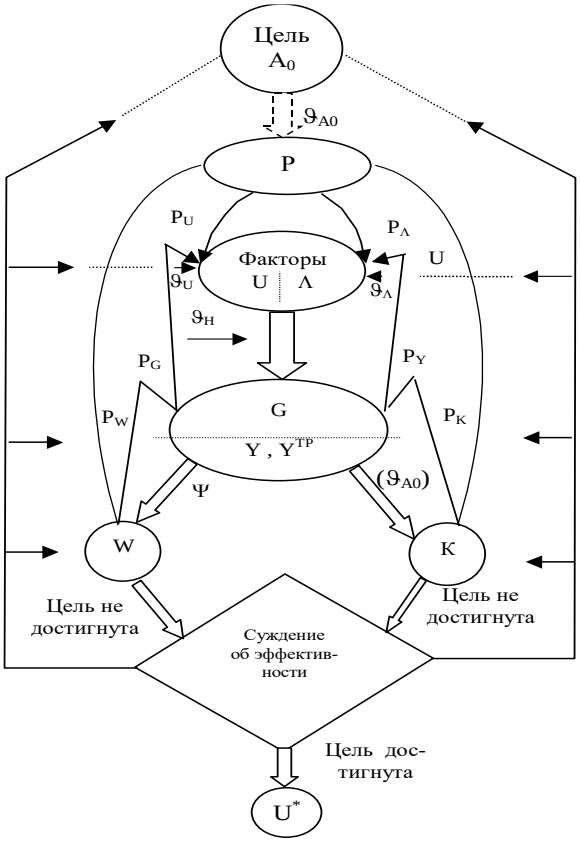


Рис. 3. Модель разрешения проблемной ситуации

Если следующие друг за другом изменения состояния будут проходить через промежутки времени $\Delta\tau\left[\left(n+1\right)_q - n_q\right] < \tau_{ц_q}$, то управляющая подсистема перестанет успевать реагировать на эти изменения, т. е. процесс станет неуправляемым.

Таким образом, необходимым условием управляемости иерархической системы является $\tau_{ц_q} \geq \Delta\tau\left[\left(n+1\right)_q - n_q\right]$. Тогда при противоборстве двух систем (ИТКС СН и РЭП противника) та система будет иметь преимущество, у которой время на принятие решений будет меньше или временные интервалы между целенаправленными воздействиями на элементы системы радиоподавления противника будут меньше цикла управления данными элементами в условиях противоборства.

Исследования [4] показывают, что характеристика взаимоотношения времени цикла управления и реакции системы противоборствующей стороны во многом будет определяться её стратегией радиоподавления противника. Основу системы РЭП вероятного противника составляют подсистемы комплексной радиоэлектронной разведки, целераспределения (управление ресурсами) и передатчики станций помех.

Рассмотренные способы целеподавления в совокупности с моделями угроз и радиоподавления элементов ИТКС СН позволяют сформировать маски воздействий. В общем случае данные маски могут быть представлены в виде

матриц $\|\Phi\| = \|\phi_{ij}\|$, включения которых отражают воздействия противоборствующей стороны (априорные или апостериорные) на элементы ИТКС СН. Наличие масок воздействий относительно каждого этапа формализации процесса управления состоянием ИТКС СН при использовании дискретного подхода позволяет для системы управления в условиях РЭБ сформировать вполне определенное множество целей и задать счетное количество возможных стратегий поведения системы. Это позволит органам управления добиться некоторой инвариантности в выборе тех или других управляющих решений.

В то же время процессы функционирования ИТКС СН в условиях РЭБ могут быть удовлетворительно описаны лишь многомерными моделями с большим числом измеряемых переменных [5]. При этом переменные имеют самую разную физическую природу, определяемую как особенностями формирования сетевого канального ресурса, так и методами предоставления его потребителям. В этих условиях управление мультисервисной ИТКС может быть интерпретировано как поиск оптимального показателя качества функционирования сети относительно различных стадий и этапов эволюционного развития ЕСУ для реализации поставленных целей перед ИТКС СН при комплексных воздействиях дестабилизирующих факторов с учетом использования части или всего имеющегося общесетевого ресурса. При этом управляющие воздействия формируются при возникновении невязок данных оперативной информации о состоянии элементов (рис. 1) с нормативными данными или прогнозными оценками, полученными на основе расчетов или моделирования внутренних и внешних процессов.

Изложенное показывает, что чем полнее и точнее комплексная информация о состоянии элементов ИТКС СН и противнике, предоставляемая системе управления системами диагностического обеспечения и мониторинга, тем более оперативным и эффективным будет управление.

Проанализированный ожидаемый характер функционирования ИТКС СН и ее системы управления в условиях информационного и радиоэлектронного противоборства может быть представлен моделью в операторном виде [6].

Данная модель, учитывающая результаты концептуального моделирования (рис. 1), включает следующую совокупность элементов (рис. 4):

I - ресурс сети, запрашиваемый службами связи для предоставления его сетям доступа. Данный ресурс характеризуется пропускной способностью, требуемого качества по своевременности, достоверности и безопасности (рис. 4) обмена информацией в ЕСУ, которую мультисервисная ИТКС должна предоставлять пользователям корреспондирующих пар узлов информационных направлений связи. Этот ресурс может быть определен, как $I = \sum_{j=1}^{m} \sum_{i=1}^{l} V_{ij}$, где V – ресурсы пропускной способности с учетом возможных протокольных потерь мультисервисной ИТКС СН, необходимые для обеспечения услуги связи с требуемым качеством; i =1,…,l – количество услуг связи, предоставляемых

службами связи сетям доступа; j=1,…,m – количество информационных направлений связи;

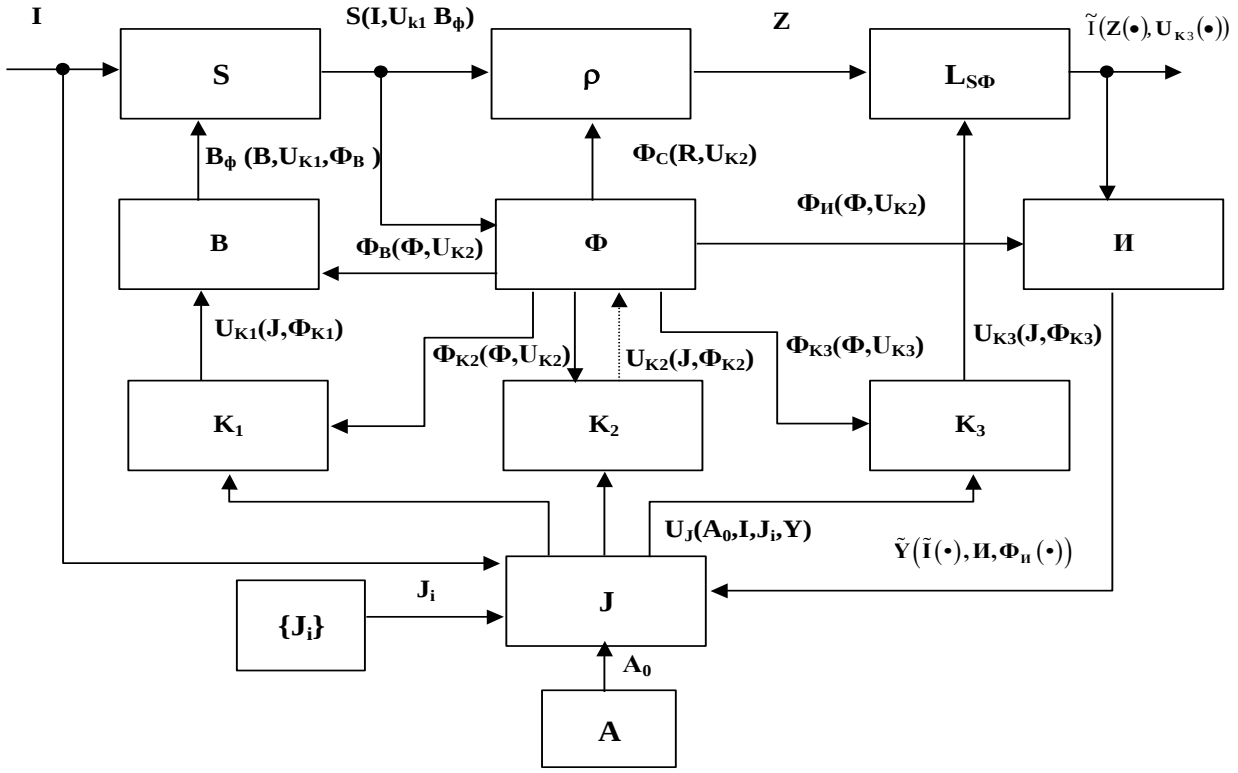


Рис. 4. Модель управления ИТКС СН в условиях радиоэлектронной борьбы

В – общий сетевой ресурс, формируемый мультисервисной ИТКС СН. В общем случае $B: B\left(G_T; G_П; G_Ф; G_Э\right)$ и формально данный ресурс может быть представлен совокупностью моделей: G_T - топологической, отражающей множество узлов сети и линий различных родов связи, их соединяющих, в их взаимном расположении; $G_П$ – потоковой, определяющей распределение ресурса сети по линиям различных родов связи и способность сети в динамическом предоставлении ее ресурса узлам связи ПУ; $G_Ф$ – физической, определяющей технологии и тип цифровых систем передачи, мультиплексирования и коммутации, образующих плезиохронные, синхронные цифровые иерархии на линиях различных родов связи и систему сетевой коммутации и мультиплексирования в транспортной сети связи; $G_Э$ – эксплуатационной, описывающей порядок эксплуатации ТСС на элементах ИТКС в условиях штатной эксплуатации и воздействия РЭБ вероятного противника, уточняющие комплекс формализованных моделей [9].

Топологическая модель:

$$G_T(A, P),$$

где $A = A_1 \cup A_2$, $A_1 = \left\{a_i\right\}, \left\{x_i^{(1)}, y_i^{(1)}\right\}, i = \overline{1, N1}$ – совокупность КЦ пунктов управления, из которых формируются корреспондирующие пары $Z = \left\{z_k\right\}, z_k = \left\{a_{p_k}; a_{g_k}\right\} : k = 1, ..., m$, соответствующих ИНС; $A_2 = \left\{a_j\right\}, \left\{x_j^{(2)}, y_j^{(2)}\right\}, j = \overline{1, N2}$ -

совокупность коммутационных центров сетевых узлов мультисервисной ИТКС СН; $P=\{b_{ij}\}$ – сетка ребер мультисервисной ИТКС, образуемая посредством наземного, воздушного и космического эшелонов между коммутационными центрами сетевых узлов.

Потоковая модель:

$$G_{П}\left(A,P,U,\vec{V},\vec{H},\vec{V}^{c},\vec{H}^{c},\vec{V}^{y},\vec{H}^{y},\vec{H}^{cc},J^{l}_{вх},k^{l}_{ош}\right),$$

в которой $U=\{u_{ij}\}$ – пропускная способность ребер мультисервисной ИТКС СН; $\vec{V}=[V_1;..,V_k,..,V_m]^T$ – вектор пропускных способностей ИНС, $V_k=\sum_{i=1}^{l}V_i$ – пропускная способность, измеренная в основных цифровых каналах (ОЦК) для каждого ИНС, выделяемая для различных видов услуг связи; $\vec{V}^{C}$ – вектор пропускных способностей, выделяемых для системы обмена сигнально-управляющей информацией при различных технологиях ее реализации; $\vec{V}^{y}$ – вектор пропускных способностей, выделяемых для системы управления связью в мультисервисной ИТКС СН, в том числе в интересах тактовой сетевой синхронизации; $\vec{H}=[H_1,...H_m]^T$ – вектор структурной надежности и отказоустойчивости ИНС; $k^{l}_{ош};J^{l}_{ош},l=1,...,L$ – требования к коэффициентам ошибки и фазовым дрожаниям сетевых цифровых ФЛК для различных родов и видов связи, обеспечивающих достижение заданных значений $P_{ош}$ для всех видов услуг и категорий пользователей; $\vec{H}^{cc}$ – вектор структурной надежности и отказоустойчивости системы тактовой сетевой синхронизации; $\vec{H}^{c}$ – вектор структурной надежности и отказоустойчивости системы сигнализации; $\vec{H}^{y}$ – вектор структурной надежности и отказоустойчивости системы управления связи.

Физическая модель:

$$G_{Ф}\left(A,P,R_{л},R_{y}\right),$$

где $R_{л},R_{y}$ - линейный и узловой ресурс, определяемый как совокупность цифровых систем передачи, образуемых с использованием плезиохронных и синхронных цифровых иерархий, который можно представить в следующем формализованном виде: $R_{л},R_{y}\left(\vec{n}^{\mu},\alpha_{\mu},\beta_{\mu},\gamma_{\mu},\vec{V}_{\mu},\vec{L}_{\mu},\vec{H}_{\mu},\vec{\Psi}_{\mu}\right),n=1,...Q;\mu=1,...M$,

где $\vec{n}^{\mu}$ – тип ТСС; $\alpha_{\mu},\beta_{\mu},\gamma_{\mu}$ – коэффициенты, отражающие приведенную стоимость ТСС и участков, образованных в мультисервисной ИТКС СН; $\vec{V}_{\mu}$ – вектор пропускных способностей, реализуемых ТСС в ФЛК мультисервисной ИТКС СН; $\vec{L}_{\mu}$ – вектор, определяющий структуру линии связи различных родов; $\vec{H}_{\mu}$ – вектор надежности и отказоустойчивости в мультисервисной ИТКС СН (рис. 1.10, 1.13), в том числе представляющих

КАПС; $\vec{\Psi}_{\mu}$ – вектор эксплутационных норм на параметры цифровых трактов и каналов.

Модель эксплуатации мультисервисной ИТКС в ЕСУ:

$$G_{Э}\left(A, P, \vec{K}_{у}, \vec{K}_{вти}, Л, C\right),$$

где $\vec{K}_{у} = \left[K_1, ..., K_i, ..., K_m\right]^T$, i=1,…,m – номенклатура АПСС, в том числе ТСС, задействованная для формирования сетевого ресурса на элементах ИТКС СН; $\vec{K}_{вти} = \left[K_{вти_1}, .., K_{вти_i}, .., K_{вти_m}\right]^T$, i=1,…,m – номенклатура ЗИП, обеспечивающая функционирование АПСС на элементах ИТКС СН; Л – личный состав эксплуатационно-технического персонала, имеющий соответствующую квалификацию, обеспечивающий функционирование АПСС; С – издержки системы технической эксплуатации, необходимые для обеспечения и поддержания требуемых укомплектованности, эксплуатационных ресурсов и отказоустойчивости ИТКС СН (рис. 1).

S – ресурс мультисервисной ИТКС СН, задействованный для передачи информационного трафика и сигнально-управляющей информации. В общем случае данный ресурс может быть представлен совокупностью матриц, каждая из которых отражает допустимое распределение потоков и сигналов по различным информационным направлениям связи в ЕСУ;

ρ - оператор взаимодействия сигналов и помех. Определяет качество сигналов в различных ИНС, образованных ИТКС СН. В зависимости от временной и энергетической доступности преднамеренных и непреднамеренных источников помех может иметь как аддитивный, так и мультипликативный характер;

Ф – множество воздействий, в которых функционирует мультисервисная ИТКС СН. Описывается комплексом обобщенных моделей угроз, согласно которым Ф($Ф_ф$, $Ф_с$) может быть представлена моделями двух видов: $Ф_ф$ – моделью физических воздействий; $Ф_с$ - моделями различных видов помех Здесь $Ф_ф$ определяет совокупность факторов, создаваемых в процессе ведения РЭБ вероятным противником против ИТКС и направленных на физическое уничтожение элементов ЕСУ, $Ф_с$ определяет энергетическую и временную доступность источников помех до формирующих и обрабатывающих сигнально-кодовые конструкции АПСС элементов мультисервисной ИТКС СН;

Z – наблюдения сигналов на входах приемных трактов аппаратно-программных средств различных родов связи, образующих ветви мультисервисной ИТКС СН. Определяется особенностями родов и видов связи (услуг) и может быть представлена матрицей наблюдений $Z = \left(S(\bullet), \Phi_c(\bullet)\right)^{\rho}$;

$L_{SФc}$ – множество допустимых алгоритмов обработки наблюдений Z. Алгоритмы обработки определяются множеством сигнально кодовых конструкций, применяемых для образования линий связи в ветвях ИТКС СН,

и видов помех, которые образованы в процессе формирования сетевого ресурса ИТКС или выработаны системой РЭБ противника;

K_n – регуляторы. Вырабатывают управляющие воздействия на элементы ИТКС СН в соответствии со сформированными алгоритмическими структурами принятия решений органами управления комплексными ресурсами ИТКС СН (рис. 1);

U_K – набор алгоритмов, управляющих воздействий, из допустимого множества возможных альтернатив, определяемых наличием канального сетевого ресурса и способами его распределения;

А – вышестоящая СУ на различных стадиях эволюционного развития;

$S(I, B_\phi)$ **– сетевой ресурс,** используемый в интересах элементов комплексной сети доступа;

$B_\phi(B, U_K, \Phi_B)$ **– избыточный управляемый сетевой ресурс,** создаваемый в мультисервисной ИТКС СН на заданной полиструктуре при РЭБ с вероятным противником и реализации управляющих воздействий системой управления;

$\Phi_B(\Phi, U_{K_2})$ **– ресурс системы РЭБ противника,** обеспечивающий физическую доступность ее элементов для изменения комплексного ресурса ИТКС СН;

$\Phi_C(\Phi, U_{K_2})$ **– ресурс системы РЭБ противника,** используемый им в интересах радиоподавления элементов ИТКС посредством различных видов помех;

$\Phi_{K_2}(\Phi, U_{K_2})$, $\Phi_{K_3}(\Phi, U_{K_2})$, $\Phi_И(\Phi, U_{K_2})$ **– ресурс РЭБ противника,** расходуемый на подавление элементов подсистем синхронизации, сигнализации и управления мультисервисной ИТКС СН;

$\tilde{I}(Z(\bullet), U_K(\bullet))$ **– сетевой ресурс,** предоставляемый мультисервисной ИТКС элементам сети доступа ЕСУ;

$Y(\tilde{I}, U_j, \Phi_и)$ **– сигналы контроля**, формируемые средствами диагностирования и мониторинга, о состоянии элементов сети и качестве формируемого комплексного ресурса ИТКС СН в условиях РЭБ с противником;

$U_J(A_0, I, J_i, Y)$ **– совокупность алгоритмов** (управляющих команд), формируемых системой, обеспечивающей принятие решения по управлению ИТКС и ее комплексными ресурсами посредством одной из технологий обмена данными;

A_0 – цель комплексного обеспечения эксплуатации ИТКС формируемая ЕСУ;

И – идентификатор. Формирует информацию о состоянии сети. Объективность оценок идентификатора определяется характером воздействий, описываемых возможными угрозами и противодействием, и поддерживается метрологическим сетевым ресурсом;

$\{J_i\}$ **– набор требований к качеству предоставляемых услуг** ЕСУ в различных информационных направлениях связи. Определяется видом услуги, классом пользователя, сетевой технологией, используемой для формирования комплексного ресурса. Например, набор требований при использовании в мультисервисной ИТКС СН технологии АТМ, как основной при ее построении, может быть представлен совокупностью следующих составляющих:

$Q_0S_i^I, Q_0S_i^{II}, Q_0S_i^{III}$ – качество соединений для I, II, III классов пользователей и i=(1,..,n) услуг связи;

$K_{or_i}^I, K_{or_i}^{II}, K_{or_i}^{III}$ – коэффициенты оперативной готовности ИНС для I, II, III классов пользователей и каждой i=(1,..,n) услуги связи;

$T_{OC_i}^I, T_{OC_i}^{II}, T_{OC_i}^{III}$ – наработка на сбой ИНС для I, II, III классов пользователей i=(1,..,n) и каждой услуги связи;

$T_{BC_i}^I, T_{BC_i}^{II}, T_{BC_i}^{III}$ – допустимое время восстановления ресурса ИНС после сбоя для I, II, III классов пользователей i=(1,..,n) услуги связи;

$T_{O_i}^I, T_{O_i}^{II}, T_{O_i}^{III}$ – наработка на отказ ИНС для I, II, III классов пользователей и каждой i=(1,..,n) услуги связи;

$T_{B_i}^I, T_{B_i}^{II}, T_{B_i}^{III}$ – восстановление ресурса ИНС после отказа для I, II, III классов пользователей и каждой i=(1,..,n) услуги связи.

J – система поддержки принятия решения ЛПР. Формирует обобщенный комплексный показателей качества на основе требований к качеству предоставляемых услуг, необходимого сетевого ресурса для их выполнения, запрашиваемого службами связи, реального состояния ИТКС и цели функционирования, определяемой вышестоящей ЕСУ.

Применительно к операторной модели (рис. 4) управление ИТКС СН в условиях РЭБ может быть интерпретировано как поиск рациональной системы показателя качества функционирования сети J в ситуациях, соответствующих различным угрозам, определяемым ресурсом противника Ф, целью A_0 , поставленной А (вышестоящей СУ), запрашиваемым I, используемым S, имеющимся B, формируемым $\tilde{I}$ комплексным ресурсом в операциональном комплексе, требованиями к ресурсу J_i для обеспечения качества обмена информацией в ЕСУ на основе данных системы диагностики и мониторинга (рис. 1) и совокупности управляющих воздействий - u из всего набора допустимых - U.

Если J выражается количественно (принимает значения на числовой оси) в метрической шкале измерений [4], то задача рационального управления ИТКС СН может быть представлена нахождением sup (inf) функционирования J в области, определяемой системой ограничений:

$$\sup J\left\{S(u), ф, \tilde{I}(u)\right\}, \qquad (5)$$

$$\begin{cases} S(u) \in S, \\ S \in B, \\ \hat{o} \in \hat{O}, \\ \tilde{I}(u) \in I, \\ u \in U. \end{cases} \quad (6)$$

Пространство фактических состояний ИТКС СН для допустимого множества вариантов ее полиструктуры (рис. 1) относительно имеющегося ресурса B может быть представлено посредством структурных матриц, соответствующих графу G сети. Под структурной матрицей в данном случае будем понимать квадратную матрицу порядка N, в которой каждому узлу $\{a_i\}$ соответствует i-я строка и j-й столбец:

$$G = \left\| a_{ij} \right\|, \text{ где } i, j = 1, \ldots N . \quad (7)$$

Если все ребра в графе ненаправлены, то матрица будет симметричной по отношению к главной диагонали, а если есть направленные ребра, то несимметричной. Если структурную матрицу последовательно возводить в q-ю степень, то будет получаться новая структурная матрица с вхождениями, содержащими b_{ij} от узла a_i к узлу a_j, ранга не более q , т.е.

$$M_q = B^q = \left\| m_{ij}^{r \le q} \right\| . \quad (8)$$

При этом имеется некоторое q_{max} , при котором матрица становится характеристической с отображением всех возможных путей между каждой парой узлов. В общем случае для полносвязной мультисервисной ИТКС СН, у которой ранг пути максимален и равен N-1, характеристическая матрица будет содержать все вхождения с рангом N-1:

$$B^{q_{max}} = B^{N-1} = M_{хар} \left\| m_{ij} \right\|. \quad (9)$$

По полученной характеристической матрице, используя в качестве вхождений различные виды ресурсов, можно оценить тот или другой вариант структуры ИТКС СН относительно ее матрицы смежности.

Если из имеющегося ресурса B, для организации информационного обмена в ЕСУ выделяется только часть ресурса S, то этим сужается допустимое количество структур, которое может быть образовано и использовано для достижения поставленной цели функционирования полиструктуры ИТКС СН (рис. 1). При этом может изменяться как базис структурных матриц, так и допустимо возможный ранг путей в полиструктурах ИНС ИТКС СН. В этом случае цель оптимизации в концепциях рационального поведения системы будет состоять в необходимости выбора при анализе из всего набора матриц $S_i \in M_q$ одной из матриц отношений между элементами $\left\| S_{ij} \right\|$, обеспечивающей наибольшую эффективность эксплуатации ИТКС СН по введенной системе показателей. В то же время, когда ИТКС СН функционируют в условиях угроз и РЭБ противника характер изменения состояний её элементов целесообразно рассматривать относительно масок взаимных воздействий. При этом маски

воздействий формируются и отображаются системой мониторинга посредством контроля состояния элементов мультисервисной ИТКС СН. В этом случае маска воздействий, соответствующая булевой матрице N×K, показывает возможность противника по подавлению К элементов $\|a_{ij}\|$ ИТКС СН:

$$\|\Phi\|_{N\times K} = \|\phi_{ij}\|. \quad (10)$$

Тогда множество стратегий системы РЭБ противника будет множеством всех допустимых матриц $\|\Phi\|$, определяемых ресурсом противника и противодействием ему со стороны ИТКС СН.

По маске воздействий и структурным матрицам формируются матрицы путей, отражающие возможность управления полиструктурой (рис. 1) в условиях РЭБ. При этом введенные ограничения (5) и (6) существенно сужают область альтернатив по выбору управляющих воздействий в подсистемах мультисервисной ИТКС СН.

Введение вероятностной меры относительно стратегий воздействия системы РЭБ противника на элементы ИТКС позволяет формировать маски воздействий на основе стохастических матриц [1]

$$\|\Phi\|_{N\times N} = \|p_{ij}\|, \quad (11)$$

где $\sum_{j\in N} p_{ij} \le 1$.

Тогда действия над структурной матрицей (8), с учетом (5), (6), (11), позволят спрогнозировать критические элементы в ИТКС СН и в дальнейшем эффективно управлять её полиструктурой (рис. 1) в условиях РЭБ.

С учетом вышесказанного показатель эффективности процесса обеспечения эксплуатации ИТКС СН на интервале τ_i, где $i \in [1,k]$ соответствует различным периодам эксплуатации, можно представить в виде

$$W^{ТКС} = \left(P^{УП};\ C_{\Sigma}^{Э}; \Phi; \tau_i\right). \quad (12)$$

В данном выражении $P^{УП}$ характеризует вероятность события, заключающегося в том, что на заданном периоде эксплуатации элементы ИТКС обеспечат успешное её функционирование.

Второй элемент в соотношении (12) $C_{\Sigma}^{Э}$ определяет суммарные затраты на обеспечение процесса эксплуатации ИТКС СН на различных периодах ее функционирования.

Таким образом, решение задачи (12) лежит в области решений задач векторной оптимизации и не является единственным. В этом случае, используя принцип Парето в качестве решения задачи, можно получить множество недоминируемых альтернативных стратегий для каждой допустимой конфигурации полиструктуры ИТКС СН в условиях РЭБ.

Разработанные формализованные модели, описывающие пространство возможных состояний полиструктуры ИТКС в условиях РЭБ, показывают необходимость создания математических моделей, характеризующих динамику

изменений взаимоотношений между элементами многофункциональных и многорежимных организационно-технических систем, которые лабильно изменяются в зависимости от внешних и внутренних воздействий. Теоретически данная проблема с учетом комплексной избыточности сложных систем (структурной, функциональной, временной, информационной и др.) исследована недостаточно. Поэтому она требует решения.

Список литературы

1. Макаренко С. И. Информационное противоборство и радиоэлектронная борьба в сетецентрических войнах начала XXI-го века: Монография. – СПб.: Наукоёмкие технологии, 2017. – 546 с.

2. Методология проектных исследований и управление качеством сложных технических систем электросвязи. С. П. Воробьёв, В. И. Курносов, К. И. Лукин и др. – СПб.: Изд. «Наука», 2022. – 340 с.

3. Сахнин А. А. Комплексная оценка развед- и помехозащищенности военных телекоммуникационных систем и ее практические приложения. – СПб.: ГП НИИ "Рубин", 2002. – 311 с.

4. Костарев С. В., Карганов В. В., Липатников В. А. Технологии защиты информации в условиях кибернетического противоборства: Науч. Монография / Под общ. ред. В. А. Липатникова. - СПб.: ВАС, 2020. – 716 с.

5. Курносов В. И., Лихачёв А. М. Модели процессов эксплуатации и восстановления технических систем электросвязи. – СПб.: «ТИРЕКС», 1998. – 81 с.

6. Новиков Д. А. Теория управления организационными системами. 2-е изд. – М.: Физматлит, 2007. – 584 с.

УДК 681.5

Тенденции развития автоматизированных систем управления оборудованием, сетями и системами связи общего и специального назначения

Курносов В. И., Сызранцев Г. В.

АО "Супертел", г. Санкт-Петербург, Россия

Аннотация: *в статье приводится анализ тенденций развития систем связи и систем управления системами связи. Рассматриваются концептуальные подходы, технические и технологические решения, технические стандарты и платформы, используемые в системах управления сетями связи и поддержки эксплуатационных процессов.*

Ключевые слова: *мультисервисные сети связи специального назначения, сети следующего поколения, глобальная информационная инфраструктура, автоматизированная система управления*

Современные системы и сети связи общего и специального назначения как объекты мониторинга и управления.

Перспективы создания и развития современных систем и сетей связи как общего пользования (ОП), так специального назначения (СН) (для нужд обороны, безопасности страны и обеспечения правопорядка) определяются возросшими потребностями различных ведомственных и корпоративных органов и систем управления (СУ) в качественном, своевременном, безопасном информационном обмене и должны соответствовать концепциям глобальной информационной инфраструктуры (Global Information Infrastructure, GII) и сетей следующего поколения (NGN-сетей) или мультисервисных сетей связи (МСС) [1–3].

В соответствии с этими концепциями современные телекоммуникационные сети (ТКС) ОП должны строиться как NGN-сети, которые обеспечивают предоставление неограниченного (наращиваемого) набора услуг связи с гибкими возможностями по их управлению, персонализации и созданию новых услуг за счёт унификации сетевых решений. При этом предполагается реализация универсальной многопротокольной транспортной сети (ТС) с распределённой коммутацией, обеспечивающей основную услугу переноса информации, вынесение функций предоставления услуг в оконечные сетевые узлы и интеграция с традиционными сетями связи (телефонной связи, передачи данных, обмена данными, документального обмена и т. д.).

Современные ТКС СН [4, 5] строятся как МСС СН, в основном в соответствии с концепцией сети связи следующего поколения, и обеспечивающие предоставление неограниченного (наращиваемого) набора санкционированных услуг спецпользователям (СП) (должностным лицам (ДЛ) органов управления (ОУ) федеральных органов исполнительной власти, комплексам средств информационных и управляющих систем, а также

комплексам средств автоматизации (КСА) этих ведомств) с обеспечением высоких требований по безопасности. Основой архитектурного построения МСС СН является защищенная многопротокольная ТС, защищенные сети доступа (СД), защищенные узлы служб и управления услугами, защищенная СУ – автоматизированная система управления (АСУ) МСС СН.

Транспортная сеть, входящая в состав и являющаяся ядром как NGN-сети ОП, так и МСС СН, должна являться мультипротокольной, так как должна обеспечивать эффективный перенос разных видов информации (разнородного трафика СП) с использованием различных протоколов передачи, т. е. должна реализовать универсальную услугу переноса, которая заключается в прозрачной передаче информации (пользователей (спецпользователей) между сетевыми окончаниями (сетями доступа) с минимальными задержками и без какого-либо анализа или обработки её содержания.

Как в NGN-сети ОП, так и в МСС СН должны быть реализованы решения, соответствующие концепции GII, предполагающей пользоваться всеми доступными услугами телекоммуникаций. Основой GII являются существующие и строящиеся ведомственные телекоммуникационные системы и сети. Для предоставления услуг телекоммуникаций в GII используются многочисленные программно-аппаратные средства, которые позволяют обмениваться любыми видами сообщений (речь, видео, данные) в любое время и с заданным качеством. Средства GII позволяют унифицировать процедуры предоставления доступа к услугам связи для пользователей (спецпользователей) различных федеральных округов, а также организовать межсетевое взаимодействие различных сетей. В такой трактовке единая сеть электросвязи (ЕСЭ) РФ должна являться частью GII.

Концептуально GII включает в себя четыре основных элемента:

– пользователи (спецпользователи), которые являются источниками и получателями сообщений и используют эту информацию;

– информационные устройства (information appliances), которые используются для хранения, обработки данных, и обеспечивают доступ к информации;

– коммуникационная инфраструктура, которая осуществляет передачу информации между географически удаленными информационными устройствами (она может быть представлена в виде ТС и СД);

– собственно, информация, которая включает в себя, прежде всего, видеоинформацию, речь, данные, а также прикладное программное обеспечение (пользовательские приложения), позволяющее конвертировать сообщения из оригинальной формы (речь, изображение, компьютерная графика, видео) в электронную форму, доступную для использования другими пользователями GII.

Взаимодействие перечисленных элементов показано на рис. 1.

В качестве платформы поддержки приложений могут использоваться вычислительные средства в совокупности с операционными системами,

микропрограммное обеспечение информационных устройств, прикладное программное обеспечение (ПО), специализированные процессоры и кодеки.

Платформы поддержки коммуникаций – это оконечное оборудование данных, модемы, устройства доступа различного назначения. Примеры средств доступа – абонентская линия связи до автоматической телефонной станции (АТС), линия DSL-доступа, сеть кабельного телевидения, оптическая линия доступа, канал радиосвязи, спутниковый канал, линия радиодоступа. Примеры ТКС – телефонная сеть связи ОП, первичная сеть связи (на основе технологий PDH, SDH.WDM, DWDM и др.), сети передачи данных различных стандартов (X.25, IP, Frame Relay, ATM, MPLS), сеть Интернет. Все перечисленные программные и аппаратные компоненты GII, а также услуги, оказываемые на их основе, являются объектами сетевого управления.

Структура GII связывает между собой в единое целое сетевые ресурсы ведомственных сетей, устройства хранения и обработки данных центров и пунктов управления (ЦУ и ПУ), а также ресурсы промежуточного ПО (middleware) для того, чтобы предложить спецпользователям стандартные услуги и поддержать их приложения.

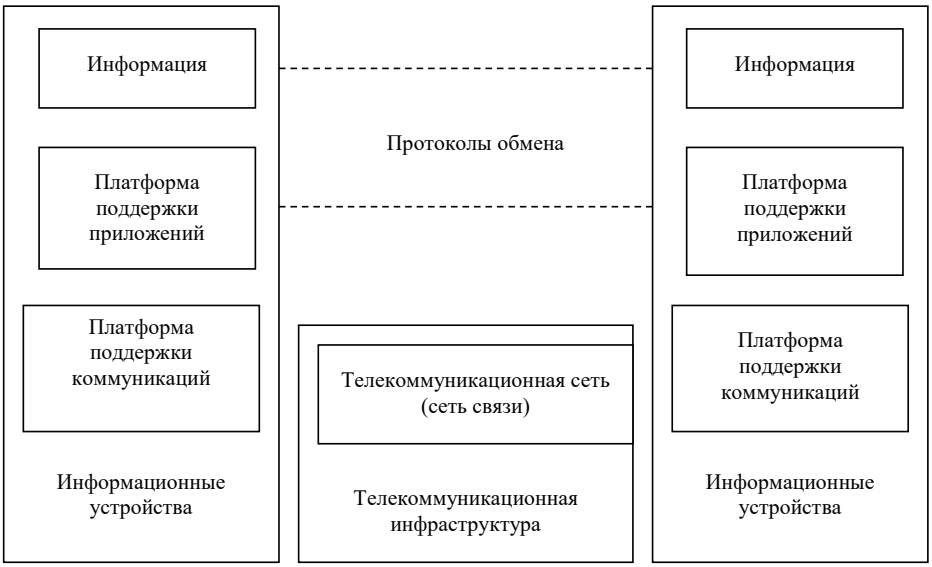


Рис. 1. Взаимодействие основных элементов GII

К средствам middleware в рамках GII можно отнести средства обеспечения информационной безопасности, биллинг, а также средства сетевого управления и администрирования. Средства middleware могут быть одновременно доступны не только индивидуальным СП, но и достаточно большим группам сторонних абонентов (например, населению при обращении к соответствующим ведомствам). Не участвуя непосредственно в преобразовании информации из одной формы в другую, средства middleware позволяют регулировать этот процесс, обеспечивая оптимальное распределение, защищённость и управляемость сетевых ресурсов.

В рамках GII услуги телекоммуникаций характеризуются транзакциями, которые осуществляет СП при запросе/активизации услуги. При этом их приложения позволяют получить полные права по использованию данной услуги. Например, установка программы почтового клиента на персональный компьютер ДЛ ПУ или сервер приложений позволяет СП воспользоваться услугами сетевой электронной почты (разумеется, если он имеет авторизацию и доступ к почтовой службе сети, что обеспечивается middleware). При этом данная программа имеет пользовательский интерфейс, который позволяет практически пользоваться данной услугой.

Общая структура услуг, предоставляемых современной NGN-сетью ОП или МСС СН в рамках GII представлена на рис. 2. При этом традиционные услуги телефонной связи, как правило, предлагают пользователям (для СС ОП) или СП (для МСС СН) технологии для доступа к новым услугам (за исключением базовых услуг связи), в то время как информационная технология предлагает пользовательские приложения для доступа/организации услуг.

В перспективе целесообразна конвергенция этих элементов, так как уже сегодня получить доступ к большинству новых услуг связи невозможно без пользовательских приложений (Интернет-браузеров, почтовых программ, приложений для кодирования и передачи речи по IP-сетям).

На сегодняшний день основное развитие инфокоммуникационных услуг ОП осуществляется в рамках компьютерной сети Интернет, доступ к услугам которой осуществляется через традиционные сети связи. В то же время в ряде случаев услуги Интернет, ввиду открытости сети, отсутствия требуемого уровня безопасности, ограниченных возможностей её транспортной инфраструктуры не отвечают требованиям специальных систем. В связи с этим развитие инфокоммуникационных услуг в рамках систем связи министерств, ведомств и корпораций требует решения задач эффективного управления информационными ресурсами с одновременным расширением функциональности сетей связи собственных систем связи.

Большинство инфокоммуникационных услуг являются “приложениями”. Обычно к инфокоммуникационным услугам предъявляются такие требования как:

– мобильность услуг;

– возможность гибкого и быстрого создания новых услуг;

– гарантированное качество услуг.

Большое влияние на требования к инфокоммуникационным услугам оказывает процесс конвергенции, приводящий к тому, что они становятся доступными пользователям (спецпользователям) вне зависимости от способов доступа.

Функциональная модель современных NGN-сетей и МСС СН, в общем случае, может быть представлена тремя уровнями:

− транспортный уровень;

− уровень управления коммутацией и передачей информации;

– уровень управления услугами.

Назначением ТС, как уже отмечалось, является предоставление услуг переноса, а реализация инфокоммуникационных услуг осуществляется на базе узлов служб (SN) с привлечением узлов управления услугами (SCP).

Узлы служб рассматриваются в качестве серверов приложений для инфокоммуникационных услуг, клиентская часть которых реализуется оконечным оборудованием пользователя, в то время как узлы управления услугами является элементом распределённой платформы, выполняющей функции управления логикой и атрибутами услуг.

Концепция NGN во многом опирается на технические решения, уже разработанные международными организациями по стандартизации. Так, взаимодействие серверов в процессе предоставления услуг предполагается осуществлять на базе протоколов, специфицированных IETF (MEGACO), ETSI (TIPHON), Форумом 3GPP2 и т. д. Для управления услугами в МСС СН с учетом наличия в их составе наследуемых сетей, целесообразно использовать протоколы H.323 (H.325), SIP и подходы, применяемые в интеллектуальных сетях связи.

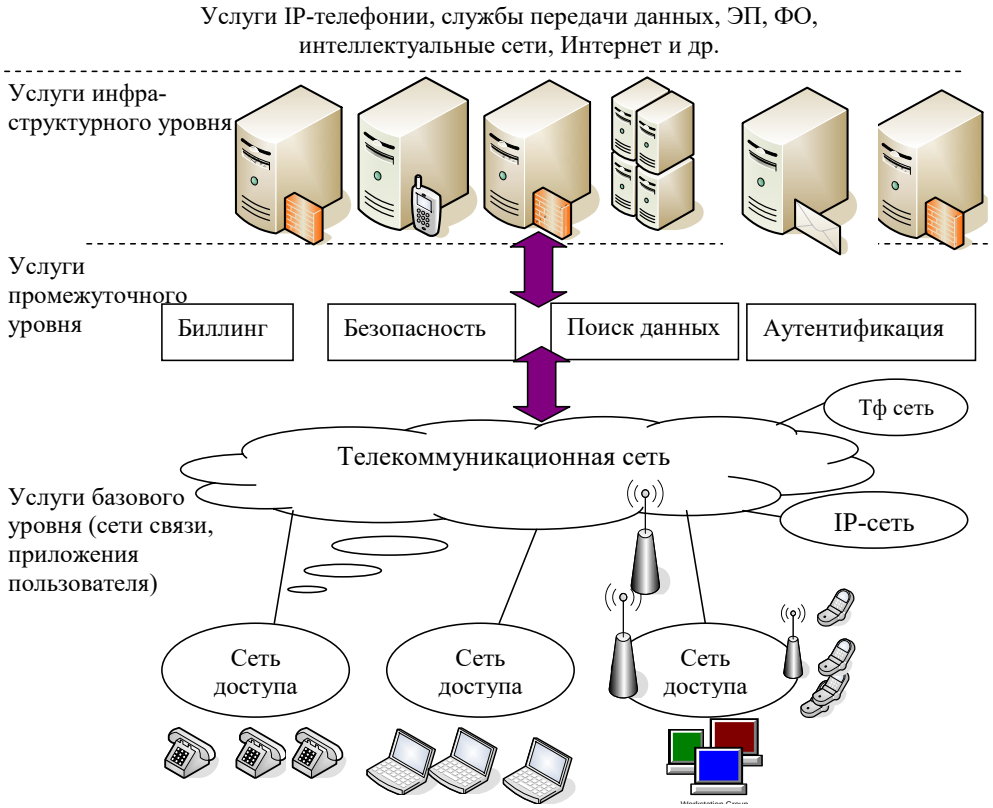


Рис. 2. Уровни услуг современной мультисервисной сети связи

В качестве технологической основы построения транспортного уровня МСС СН в настоящее время рассматриваются технологии IP-MPLS, ATM, FR, MPLS over ATM и редко IP поверх SDH (WDM и т.д.) в основном

для выделенных направлений и низкими требованиями по безопасности в силу уязвимости IP-сетей.

Рис. 3. Вариант структурного построения NGN-сети общего пользования и мультисервисной сети специального назначения

Для доступа СП к услугам используются:

– интегрированные СД, подключенные к оконечным узлам МСС СН и обеспечивающие подключение СП как к самой сети, так и к традиционным сетям (например, телефонной связи);

– традиционные сети (телефонные, сети передачи данных), абоненты которых получают доступ к услугам МСС СН через узлы, подключенные к шлюзам (Media Gateway).

На телефонных сетях для доступа часто используется абонентский участок, для увеличения пропускной способности которого может применяться технология xDSL, а на сетях подвижной связи – технологии 2G, 3G и 4G.

Автоматизированная система управления мультисервисной сети специального назначения

Особенностями как NGN ОП, так и МСС СН с точки зрения управления является то, что каждая из них состоит из большего числа разнотипных компонентов, а не из сравнительно небольшого количества менее разнообразных крупных коммутационных устройств, как моносервисные сети. Кроме того, в МСС СН будет поддерживаться большее число интерфейсов, чем в существующих сетях, разные системы сигнализации и более высокая

пропускная способность и безопасность. Всё это ведёт к необходимости пересмотра принципов и подходов к сетевому управлению для МСС СН по всему спектру задач управления.

Управление МСС СН рассматривается как широкое понятие, включающее техническую эксплуатацию как составную часть. При таком подходе техническую эксплуатацию следует понимать, как исполнительную составляющую СУ.

Функциональная область управления определяет, какие ресурсы в МСС СН являются управляемыми, т. е. указывает ресурсы, которые могут целенаправленно изменяться для достижения цели управления в процессе существования и функционирования сети.

Автоматизированная система управления МСС СН – это человеко-машинная СУ, в контуре которой совместно функционируют человек и средства вычислительной техники, другие информационные и технические средства, осуществляющие автоматизированный сбор и обработку информации с целью принятия целесообразных решений по управлению сложными организационно-техническими и динамическими объектами МСС СН и всей МСС СН в целом [4–6]. Другими словами, АСУ МСС СН – это совокупность административных, организационных, математических способов и средств вычислительной техники, взаимоувязанных в процессе своего функционирования в единую человеко-машинную систему для принятия управляющих решений по связи.

Автоматизация управления МСС СН представляет собой комплекс мероприятий, обеспечивающих управление организационно-техническими и динамическими объектами связи МСС СН с помощью средств автоматизации, вычислительной техники и различных технических устройств с соответствующим математическим и информационным обеспечением и человека – оператора и ДЛ ОУ связью.

Существующие АСУ отдельными сетями связи, ориентированные, в основном, на выборочный позадачный подход, реализуемый на разрозненных КСА, принципиально не могут удовлетворить современным требованиям к СУ МСС СН.

Автоматизированная система управления МСС должна строиться и развиваться как система, которая реализует преемственность, единство и технологическую взаимосвязь всех этапов реализации задач управления, связанных друг с другом общей идеологией, общностью исходных данных и сквозной последовательностью решения.

На верхних уровнях иерархии АСУ управление имеет преимущественно организационный характер, на нижних − технологический. На уровне организационного управления (ОргУ) осуществляется анализ состояния системы связи и выработка вариантов решения на этапах оперативного управления и планирования (в том числе по развертыванию, восстановлению, наращиванию системы связи, перераспределению каналов связи и потоков информации и т. п.). К задачам технологического управления (ТУ) относятся задачи сбора

и первичной обработки информации о задержанных сообщениях, состоянии линий, каналов и средств, и комплексов связи, доведения и реализации управляющих воздействий на средства связи (оборудование МСС СН).

Автоматизированная система управления МСС СН должна обеспечивать автоматизированное решение следующих классов задач:

– планирование и организация связи;
– управление прохождением информации;
– управление МСС СН и ее элементами;
– управление взаимодействием с внешними сетями и системами связи;
– управление услугами, предоставляемых сетями и службами МСС СН;
– управления всем спектром ТКС системы связи;
– технологическое управление оборудованием;
– сбор статистических данных о функционировании МСС СН.

Задачи автоматизированного управления АСУ разделены на уровни управления в соответствии с функциональной иерархией управления сетями в составе МСС СН. При этом необходимо также иметь разработки задач управления взаимодействием с соседними (внешними) сетями связи путем обеспечения оперативного и оперативно-технического взаимодействия с их СУ.

Автоматизированная система управления МСС СН должна отвечать всем основополагающим принципам построения любых АСУ. Структура АСУ в той или иной мере должна соответствовать как структуре МСС СН, так и системе органов и центров ведомственных или корпоративных АСУ, для которых собственно и создаются МСС СН. Автоматизированная система управления должна обеспечивать передачу управления с одних центров управления на другие. В случае необходимости средства АСУ МСС СН должны обеспечивать переход к неавтоматизированному (ручному) управлению связью.

Анализ международного опыта создания СУ сетями, отечественных разработок в области управления системами связи и опыта создания АСУС в ОАО «НИИ «Рубин» [5] можно утверждать, что при эволюционном развитии АСУ МСС СН проходят ряд этапов, граница между которыми часто не бывает достаточно четкой.

Как правило, *на первом этапе* создается и развертывается так называемая система сбора, обработки и отображения информации о состоянии МСС СН и всех ее элементов (автоматизированная информационная система или АИС), позволяющая автоматизировать основные процессы по сбору информации о состоянии оборудовании, комплексов и подсистем МСС СН, её своевременной обработки с использованием современной компьютерной техники, и отображением обработанной информации на мониторах и экранах операторов и ДЛ ПУ МСС СН. Это позволяет исключить рутинную работу операторов по сбору и ручной обработке исходной информации, снизить вероятность ошибок при оценке состояния, повысить достоверность данных, что в целом повысит достоверность данных и обоснованность принимаемых (на данном этапе вручную) решений.

На *втором этапе* автоматизации подлежат все задачи управления оборудованием МСС СН и всеми сетями, входящими в её состав. При этом упор делается на решение вопросов автоматизированного поддержания работоспособного состояния всего связного оборудования МСС СН и автоматизированного управления производительностью, структурой, безопасностью, сбоями в работе и ошибками сетей связи в составе МСС СН.

На *третьем этапе*, когда имеется полная оперативная информация о всей МСС СН, имеются механизмы автоматизированного изменения процессов и параметров функционирования оборудования и различных сетей в составе МСС СН, приступают к автоматизации основных процессов ОргУ, связанных с планированием и развитием МСС СН. Собственно, на третьем этапе появляется полноценная АСУ МСС СН, которую с полным основанием можно назвать именно автоматизированной системой управления.

В архитектурном плане, различные автоматизированные и информационные комплексы АСУ МСС СН строятся в виде открытых систем. При таком подходе каждая подсистема управления, входящая в АСУ, создается для выполнения прикладных процессов ЦУ, ДЛ и специальных прикладных процессов. Последние являются вспомогательными, они связаны с управлением и диагностикой работы самой АСУ МСС СН и обеспечением информационной безопасности. Любая АСУ состоит из ряда абонентских систем (в трактовке модели взаимосвязи открытых систем) в виде соответствующих ЦУАСУ МСС СН, включающих в себя собственно прикладные процессы управления и области взаимодействия, предназначенные для обеспечения связью прикладных процессов друг с другом, передачи информации во внешнюю для АСУ среду.

При организации взаимодействия различных ЦУ АСУ МСС СН решаются задачи инициации, поддержания требуемого качества, а также обработки ненормальных ситуаций (учитываются только те задачи управления, которые связаны с обменом различной информацией между удаленными объектами управления).

В ЦУ АСУ МСС СН в соответствии с моделью взаимодействия открытых систем выделяют три категории управления взаимодействием:

– управление прикладными процессами;

– управление системами;

– управление уровнями (в общем виде с первого по седьмой, но могут быть и специальные профили, и четырехуровневый профиль Интернет-ориентированных сетей).

Непременным условием создания высокоэффективной АСУ МСС СН является синтез её функциональной структуры, которая должна включать увязку отдельных задач управления друг с другом и включения их в единый процесс управления сетью. Функциональная структура АСУ МСС СН должна быть представлена в виде относительно независимых функциональных подсистем, взаимодействующих друг с другом в едином управляющем процессе.

В качестве коммуникационных служб, обеспечивающих информационное взаимодействие прикладных процессов и ДЛ по связи в АСУС, должны быть использованы службы, аналогичные тем, которые реализованы в системе связи, например, служба файлового обмена, служба электронной почты и др.

Спецификой объекта управления и среды функционирования АСУ МСС СН являются:

– территориальная распределённость МСС СН, наличие стационарной и мобильной компонент;

– необходимость формирования требований по объему и качеству услуг связи, предоставляемых МСС СН спецпользователям;

– сочетание наличия средств телекоммуникаций, имеющих в составе разного рода агентов управления, благодаря чему они могут быть включены непосредственно в контур управления АСУ, и средств, у которых такая возможность отсутствует;

– разнородность используемых средств телекоммуникаций;

наличие дестабилизирующих и деструктивных факторов и угроз различного характера – от прямого физического силового разрушающего воздействия до программно-аппаратных и кибератак.

Функциональность АСУ определяет, какие функции в функциональной области управления МСС СН и подразделениями связи автоматизируются (процессы) и каким образом в АСУ осуществлена данная автоматизация (средства, программы, алгоритмы).

Таким образом, на АСУ МСС СН возлагаются задачи ОргУ, оперативно-технического (ОТУ) и ТУ. Задачи ТУ и ОТУ решаются в подсистемах управления оборудованием, телекоммуникационными и информационными сетями МСС СН. Сопряжение подсистем ОргУ с этими подсистемами осуществляется на уровне ПУ (ЦУ) связью в рамках решения задач ОргУ. Технические решения по реализации сопряжения должны разрабатываться для каждой из подсистем отдельно, с учетом уровня их автоматизации и специфики решаемых в них задач.

Автоматизация управления связью ведется по двум функциональным ветвям. Первая ветвь связана непосредственно с оперативным управлением МСС СН. Вторая ветвь связана с управлением подразделениями связи, как в период их повседневной деятельности, так и на особый период (учет, снабжение, отчетность, планирование). Эти ветви общей АСУС должны быть связаны между собой.

Подсистему управления подразделениями связи, несмотря на то, что она является подсистемой АСУС, целесообразно интегрировать с системами автоматизированного управления федеральных органов исполнительной власти (ФОИВ) РФ.

Существенное влияние на создание АСУ оказывает мировая тенденция эволюции СУ, заключающаяся в переходе от систем, создаваемых только в рамках концепции и стандартов Telecommunication Management Network (TMN), к системам с функциональностью класса Operation Support System (OSS)

и далее – Business Support System (BSS), касающаяся функциональных аспектов ее построения. Однако, если построении АСУ в виде OSS имеет многие положительные моменты в трансформации функциональной структуры в сторону её более прозрачной и логичной архитектуры, то аспекты BSS, в которых во главу поставлены бизнес цели, подходят в основном для АСУ NGN ОП и в полной мере не приемлемы для АСУ СН к которым относится АСУ МСС СН.

Как известно [5], системы класса OSS – это системы, отличающиеся существенно большей функциональностью с точки зрения сферы решаемых прикладных задач управления и их соотнесения с различными аспектами и этапами жизненного цикла сетей связи. Применительно к АСУ МСС СН, рассматриваемой как система класса OSS, характерны (хотя в настоящее время общепринятая терминология в этой области практически отсутствует):

– объединение подсистем ОТУ и ТУ АСУ МСС СН в подсистему оперативного управления или в подсистему управления функционированием МСС СН;

– развитие подсистемы ОргУ в подсистему планирования связи или управления применением;

– выделение самостоятельных подсистем управления развитием (проектные, строительно-монтажные работы и т. д.), обслуживанием (взаимосвязи с поставщиками/потребителями услуг, задачи биллинга), технической эксплуатацией (ввод в эксплуатацию, ремонтные работы и т. д.), безопасностью (в самом широком смысле).

Применительно к АСУ МСС СН ориентация на создание объединения TMN с OSS реализуется как следующий подход:

– повышение роли наращиваемой подсистемы управления безопасностью;

– первоочередное создание подсистемы оперативного управления (управления функционированием) как функциональной подсистемы, во многом технически определяющей (ограничивающей) потенциальные возможности других подсистем;

– последовательное развитие подсистем АСУ МСС СН в части обеспечения планирования связи (ОргУ, биллинговые задачи и т. д.) до функционально полного набора взаимодействующих подсистем АСУС класса OSS.

Система управления МСС СН должна представлять собой набор решений, обеспечивающих управление сетями, реализованными на базе различных технологий (фиксированные и мобильные телефонные сети, сети передачи данных, сети сигнализации, сети обмена данными и документального обмена и т. д.), предоставляющих различные услуги и построенных на оборудовании различных производителей. Система управления будет строиться с использованием объектно-ориентированной распределённой структуры.

Одной из главных особенностей СУ МСС СН является открытая модульная архитектура, позволяющая разрабатывать и внедрять новые модули,

работать с существующими приложениями и модернизировать существующие модули.

Для реализации интегрированного управления сетями в составе МСС СН независимо от их производителя и технологии могут использоваться разнообразные стандарты и протоколы, такие как SNMP (Simple Network Management Protocol), SMIP (Simple Management Information Protocol), CORBA (Common Object Request Broker Architecture). Стандартом же управления в сетях в настоящее время де-факто является протокол SNMP. В модели TMN предполагалось использование протоколов OSI. Однако практическая реализация СУ на базе TMN оказалась сложной, медленной и дорогостоящей, в ней недостаточно проработаны вопросы управления услугами. В последнее время активно развиваются и реализуются решения по организации управления на базе архитектуры CORBA, которая является весьма перспективной, особенно на верхних уровнях управления [6].

В МСС СН СУ будет в первую очередь нацелена на решение конкретных задач, а уровневая архитектура TMN, хотя и сохранится, уже не будет иметь первостепенное значение для всей МСС СН, и отойдёт на второй план, так как TMN ориентирована на управление одной ТКС, а их в составе МСС СН несколько и разного рода с отличными функциональными задачами.

Поэтому архитектура АСУ МСС СН хоть и будет TMN-ориентированной, но более сложной и разнородной с различными межуровневыми взаимодействиями.

Интерфейсы СУ МСС СН должны быть открытыми. Отличительными чертами подобных интерфейсов являются: стандартизированные протоколы (например, CMIP, SNMP, FTP, SMTP, FTAM и др.), использование формальных языков для описания стандартизированных интерфейсов (например, CORBA, IDL, JAVA, GDMO, ASN1 и др.), стабильность, которая позволяет вносить только те изменения, которые будут обратно совместимы.

Так, например, для посылки аварийных сообщений могут использоваться протоколы CMIP, SNMP или CORBA с использованием объектной модели, определённой в X.733, а для организации услуг могут использоваться интерфейсы CORBA, для пересылки данных о рабочих характеристиках в части телекоммуникационной поддержки может применяться протокол FTP, а для обмена информацией между ДЛ ОУ – протоколы электронной почты SMTP, IMAP4, POP3 (рис. 4).

Основными требованиями, предъявляемыми к СУ МСС, являются:

– подготовленное решение по организации управления на практике должно реализовываться в кратчайшие сроки в связи с возможностью быстрого наращивания перечня услуг;

– структуры открытых систем должны обеспечивать гибкость реализации и совместимость с другими решениями, высокую надёжность и как результат – качество обслуживания;

– должностные лица ОУ МСС СН должен иметь возможность модифицировать ПО СУ для реализации специфических функций и вводить

новые услуги через изменение конфигурации, с учетом требований по информационной безопасности процессов управления;

– должны быть реализованы компонентные решения, которые упростят возможности оператора по введению новых пользователей и функций.

К основным технологическим тенденциям современных АСУ МСС СН следует отнести применение технологий масштабируемой адаптивной вычислительной среды (АВС) в соответствии со стандартами Advanced TCA (PICMG 3.X), который представляет собой первый открытый стандарт для создания оборудования на базе современных технологий высокоскоростной коммутации.

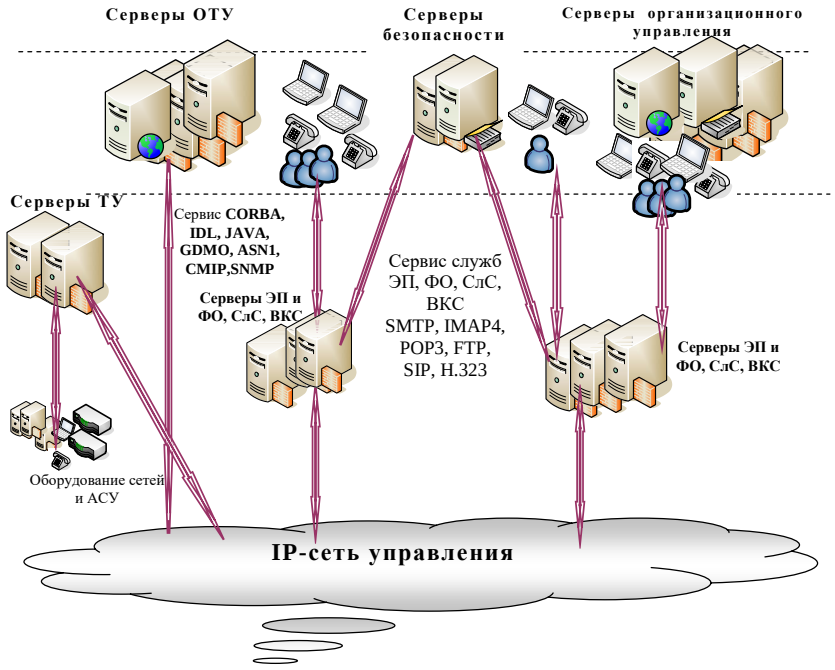


Рис. 4. Сервисы по обмену управляющей информацией в автоматизированной системе управления связью мультисервисной сети связи специального назначения

Одной их особенностей стандарта AdvancedTCA являются развитые и эффективные функции системного управления, базирующиеся на спецификации интеллектуального интерфейса IPMI с рядом расширений.

Интерфейс IPMI является на сегодняшний день одним из основных открытых стандартов для организации удаленного системного управления. Он позволяет осуществлять дистанционный контроль, диагностику, администрирование и восстановление системы через удаленную консоль. Будучи реализованным аппаратно, IPMI не зависит от используемой операционной системы, и потому с его помощью можно управлять питанием, вентиляторами, напряжениями и температурами вне зависимости от типа и состояние процессоров и ОС. Полная программная независимость IPMI позволяет производить диагностику и восстановление даже зависших и остановленных систем. Спецификация IPMI предусматривает как функции

автоматического мониторинга аппаратных средств, так и выведение уведомлений, благодаря которым оператор или ДЛ ОУ может следить за состоянием системы в реальном времени.

Список литературы

1. Рек. МСТ-Э Y.2001.Сети последующих поколений – Структура и функциональные модели архитектуры.
2. Рек. МСТ-Э Y.2091. Сети последующих поколений – Структура и функциональные модели архитектуры. Термины и определения для сетей последующих поколений.
3. Рек. МСЭ-Т Y.2261. Сети последующих поколений – Аспекты служб: взаимодействие служб и СПП. Эволюция сетей КТСОП/ЦСИС по направлению к СПП.
4. Буренин А. Н., Курносов В.И. Теоретические основы управления современными телекоммуникационными сетями / Под ред. д.т.н., проф. Курносова В.И. М.: Наука, 2011. 464 с.
5. Головкина В. Г, Кривов О.А., Лихачев А.М. Концептуальные основы совершенствования и развития АСУ ИТКС спецназначения // Вопросы радиоэлектроники. Сер СОИУ. 2012. Вып 2.

УДК 004.722

Обобщённая модель формирования структуры сети абонентского доступа специального назначения

Гагарин С. П., Сызранцев Г. В.

АО «Супертел», г. Санкт-Петербург, Россия

***Аннотация**: По своему характеру задача синтеза структуры сети абонентского доступа (САД) с интеграцией услуг связи для мобильного пункта управления (ПУ) органами государственной власти (ОГВ), представляющая разновидность задач системного проектирования, является оптимизационной и состоит в выборе такого набора внутренних первичных параметров (структурных и алгоритмических), при которых обеспечивается экстремум некоторого функционала полезности. На практике для большинства систем такого типа построить достаточно обоснованный функционал полезности весьма сложно. Ввиду этого находит применение так называемый маргинальный подход, суть которого состоит в оптимизации одного из внешних параметров системы при ограничениях на все остальные параметры [1]. Учитывая специфику функционирования сетей абонентского доступа, развёртываемых на мобильных ПУ, действующих в интересах системы управления ОГВ, в качестве основного критерия оптимальности предлагается использовать минимум суммарных затрат на построение и эксплуатацию САД [2].*

***Ключевые слова:** синтез структуры сети абонентского доступа, применение системных моделей, управление сетями доступа, управление оборудованием сетей доступа.*

Постановка задачи: задача синтеза структуры сети абонентского доступа с интеграцией услуг связи для мобильного пункта управления органами государственной власти, представляющая разновидность задач системного проектирования, является оптимизационной и состоит в выборе такого набора внутренних первичных параметров (структурных и алгоритмических), при которых обеспечивается экстремум некоторого функционала полезности. На практике для большинства систем такого типа построить достаточно обоснованный функционал полезности весьма сложно. **Целью работы** является использование различных упрощений, основная суть которых состоит в декомпозиции общей задачи на совокупность частных. Представленная задача относится к классу комбинаторных и может быть сформулирована в терминах дискретного математического программирования. Однако чрезмерно высокая размерность делает практически невозможным её прямое решение на базе существующих методов и средств. Предлагается применение так называемого маргинального подхода, суть которого состоит в оптимизации одного из внешних параметров системы при ограничениях на все остальные параметры.

Используемые методы: решение задачи синтеза сетевых структур и их дальнейшего развития с использованием системных моделей для решения задачи синтеза структуры сети абонентского доступа в классе иерархических сетевых структур. От обычных моделей системные модели отличаются большим числом учитываемых факторов, их взаимосвязью, широким набором критериев и ограничений, компактностью и простотой модификации.

Новизна: элементами новизны представленного решения являются применение системных моделей и, в частности, подхода, базирующегося на агрегативных системах, т.е. А – схемы, позволило получить аппарат решения структурно-сетевой задачи меньшей размерности и отличающийся от существующего, оригинальностью и простотой реализации. **Результат**: использование представленного решения позволяет снизить требования по вычислительной мощности центральных процессоров и объёму оперативной памяти к аппаратным средствам как системы управления телекоммуникационным оборудованием, так и агентов управления сетевых элементов.

Практическая значимость: представленное решение предлагается реализовать в виде математического и информационного обеспечения системы управления телекоммуникационным оборудованием сетей абонентского доступа. Реализация может позволить осуществлять реконфигурацию сетевых элементов в режиме времени, приближенного к реальному в соответствии с полученными выходными данными по результатам решения задач синтеза структуры сети абонентского доступа. Получение входных данных от телекоммуникационного оборудования сети доступа и его последующая реконфигурация могут осуществляться с применением протокола SNMP (v2c или v3).

Постановка задачи

Представленная задача относится к классу комбинаторных и может быть сформулирована в терминах дискретного математического программирования. Однако чрезмерно высокая размерность делает практически невозможным её прямое решение на базе существующих методов и средств [2]. В связи с этим используются различные упрощения, основная суть которых состоит в декомпозиции общей задачи на совокупность частных. Исходя из этого, предлагается один из подходов решения задачи синтеза рациональной структуры сети абонентского доступа (САД).

Эффективным инструментом решения задач синтеза сетевых структур и их дальнейшего развития являются системные модели (СМ) [3]. От обычных моделей СМ отличаются большим числом учитываемых факторов, их взаимосвязью, широким набором критериев и ограничений, компактностью и простотой модификации.

САД, развёртываемая на мобильном ПУ ОГВ занимает определённый уровень иерархии перспективной системы связи общего пользования (ССОП) системы связи ОГВ, к ресурсу которой она обеспечивает доступ, и, в свою очередь, имеет иерархическую структуру. Исходя из этого, предлагается использование СМ для решения задачи синтеза структуры САД в классе иерархических сетевых структур.

Обобщённая модель формирования структуры сети абонентского доступа

Если каждой операции, проводимой при синтезе и анализе САД, привести в соответствие некоторую частную (субмодель), то обобщённая модель

представляется совокупностью взаимоувязанных между собой субмоделей (рис.1). Каждая субмодель выполняет определённую задачу.

Таким образом, предлагаемая обобщённая модель формирования структуры САД, представляет собой модель, воедино увязывающую структурные параметры, показатели качества обслуживания абонентов (пользователей) (ВВХ процессов доставки информации), потоковые характеристики, технико-экономические показатели оборудования, технико-эксплуатационные характеристики САД, т.е. частные задачи, обеспечивающие решение поставленной научной задачи [4].

Предлагаемая обобщённая модель подобна «чёрному» ящику, преобразующему набор входов I, соответствующих исходным данным задачи синтеза рациональной структуры САД на мобильном ПУ ОГВ, в выходы, соответствующие заданным критериям и функциям – ограничениям задачи синтеза. Исходя из этого, выделяются следующие частные функциональные задачи и приведённые им в соответствие частные модели в составе обобщённой модели формирования распределённой структуры САД, представленной на рис. 1.

Обобщённая модель формирования структуры САД агрегируется из субмоделей путём объединения соответствующих входов и выходов. Подход при построении обобщённой модели, основанный на объединении графо-матричных процедур синтеза структуры САД и анализа полученных реализаций (распределение потоков, выбор пропускных способностей, оценка ВВХ и т.д.) в единую итерационно-циклическую схему, в данном случае является неконструктивным из-за большой размерности и обилия обратных связей. Эти связи вынуждают после решения очередной процедуры проводить корректировку всех предыдущих. Трудности, связанные с объединением в рамках одной обобщённой модели всего многообразия способов реализации будущей модели, растут экспоненциально с ростом размерности, т.е. описывающих САД параметров [5]. Учитывая это, задача синтеза рациональной структуры САД была декомпозирована на ряд частных задач синтеза и анализа, обеспечивающих получение искомой структуры САД с требуемыми характеристиками [1].

Таким образом применение СМ и, в частности, подхода, базирующегося на агрегативных системах, т.е. *А* – системы [6], позволило получить аппарат решения ССЗ меньшей размерности и отличающийся от существующего, оригинальностью и простотой реализации.

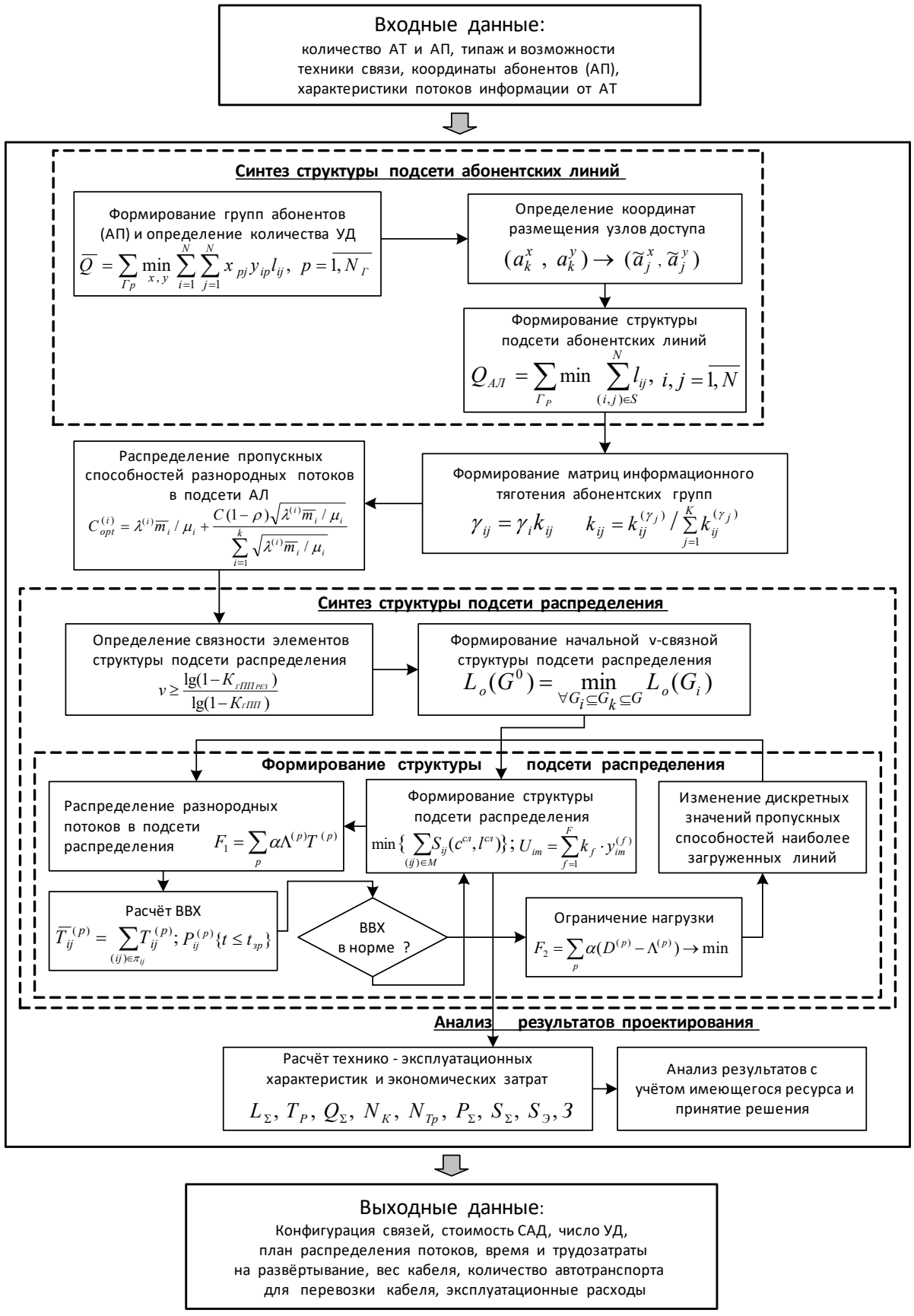


Рис. 1. Обобщённая модель формирования распределённой структуры САД

С учётом вышесказанного в основу обобщённой модели положены следующие основополагающих принципы [6]:

принцип иерархии, способствующий получению решений задачи синтеза в классе многоуровневых структур, являющихся наиболее экономичной структурной организацией сетей связи и учитывающий структурные составляющие САД (подсеть распределения и подсеть абонентских линий);

принцип функциональной полноты, предполагающий наличие частных моделей (задач) синтеза структуры САД и анализа полученных реализаций: распределения разнородных потоков, выбора пропускных способностей, оценки ВВХ, т.е. частных моделей, определяющих состав общей задачи синтеза структуры сети абонентского доступа полевого пункта управления объединения;

принцип упрощения, основанный на исключении несущественных факторов, объединении, линеаризации и регуляризации менее существенных переменных;

принцип многоцелевой ориентации, позволяющий использовать обобщённую модель для синтеза структуры САД в ситуациях, различающихся степенью детализации исходных данных, классами синтезируемых структур, целевыми функциями и составом ограничений, моделируемыми протоколами доступа, обмена и управления;

принцип композиции модели синтеза многоуровневой структуры САД из некоторого набора известных типовых структур;

принцип надёжности вычислений, обеспечивающий устойчивую работу алгоритма, как в допустимой, так и в недопустимой областях и отодвигающий на второй план задачу выбора начальной точки.

а) Компоненты обобщённой модели формирования распределённой структуры сети абонентского доступа

Приближённый характер исходных данных и пологость целевых функций в экстремальной области, свойственные задачам планирования связи, послужили основанием к использованию эвристических алгоритмов синтеза структур подсетей САД в составе обобщённой модели. Относительно потоков передаваемой информации приняты следующие допущения: пуассоновские входные потоки; неравномерный характер информационного тяготения между абонентами (пользователями).

Обобщённая модель формирования распределённой структуры САД представляется как многофункциональный преобразователь входных данных в выходные показатели. Этот многофункциональный преобразователь выполняет отдельные операции синтеза структуры САД и её анализа: расчёта структурных и потоковых параметров, оценки качества обслуживания абонентов (оценки ВВХ процесса доставки), стоимости, технико-эксплуатационных характеристик. Исходя из этого, предлагается рассмотреть функциональное назначение отдельных компонентов обобщённой модели формирования структуры сети абонентского доступа.

Формирование групп абонентов (абонентских пунктов - АП) представляет собой субмодель определения количества групп абонентов, территориальной тяготеющих друг – к другу и в соответствии с этим – требуемое количество УД.

Определение координат размещения узлов доступа (УД) в районах локализации абонентов (АП) позволяет выбрать такую точку, в которой обеспечивается минимум суммарных затрат на абонентские линии (АЛ) от подмножества абонентов (АП) данной группы.

Субмодель формирования структуры подсети АЛ представляет собой набор графо – матричных алгоритмических процедур. Она позволяет рассчитывать структурные параметры отдельных локальных подсетей АЛ каждого подмножества абонентов (АП) САД, зависящие от координат размещения абонентов (АП) и УД (узлов коммутации - УК) на местности, в целом составляющих параметры подсети АЛ. Строится на основе графовых субмоделей. Вершины графа, представляют собой узлы доступа (учитывая узел коммутации), размещаемые в группах абонентов (АП) [6].

Три перечисленные субмодели в целом составляют частную методику синтеза структуры подсети абонентских линий.

Субмодель формирования матриц взаимного информационного тяготения представляется функцией, определяющей степень взаимного информационного тяготения абонентов (АП) в группе, групп абонентов (АП) между собой, транспортной составляющей ССОП и обеспечивает прогнозирование разнородного трафика, генерируемого абонентами (АП) той или иной группы.

Субмодель распределения пропускных способностей в подсети АЛ представляет набор аналитических формул, позволяющих определить пропускные способности АЛ к УД, в зависимости от интенсивности входного информационного потока в АП, что обеспечивает минимизацию задержки пакетов (ячеек) в локальных подсетях АЛ.

Совокупность следующих субмоделей образует частную методику синтеза структуры подсети распределения.

Субмодель определения связности элементов структуры подсети распределения обеспечивает получение требуемых надёжностных характеристик САД.

Субмодель формирования начальной v – связной структуры подсети распределения обеспечивает получение стартовой структуры, с учётом ряда критериев.

Субмодель синтеза подсети распределения представляет собой набор графо – матричных алгоритмических процедур. Позволяет рассчитывать структурные параметры подсети распределения, зависящие от координат размещения УД и УК на местности. Строится на основе графовых субмоделей. На основе полученной начальной *v* – связной структуры позволяет синтезировать искомую структуру подсети распределения.

Субмодель расчёта ВВХ представляет набор аналитических субмоделей, позволяющих производить оценку качества обслуживания абонентов

(пользователей) – вычисление среднего времени и вероятности доставки пакета (ячейки).

Субмодель распределения приоритетных потоков предназначена для нахождения плана РП интенсивностей потоков в каналах связи подсети распределения, между УД – УД и УД – УК.

Субмодель расчёта параметров ОН является дополнением к предыдущей модели и предназначена для расчёта ограничений по внешнему трафику в тех случаях, когда не выполнены ограничения по ВВХ.

Последние составные части обобщённой модели позволяют провести анализ полученных результатов проектирования с использованием следующих субмоделей.

Субмодель расчёта технико-эксплуатационных характеристик и экономических затрат включает подзадачи расчёта общей длины линейно-кабельного оборудования САД, количества и веса катушек (барабанов) с кабелем, времени развёртывания САД, объёма трудозатрат необходимых для развёртывания САД, количества автомобильного транспорта, необходимого для перевозки линейно-кабельного оборудования и т. д. Позволяет рассчитывать общую стоимость САД и эксплуатационных расходы.

Важное место в обобщённой модели формирования распределённой структуры САД занимают субмодели анализа и, в частности, субмодели расчёта качества обслуживания пользователей (ВВХ процесса доставки). Использование данных субмоделей напрямую не представляется возможным, так как необходимо учитывать особенности, присущие широкополосным ЦСИС.

Главной особенностью источников нагрузки САД, построенной на принципах широкополосной цифровой сети с интеграцией служб (ЦСИС), является то, что они характеризуются различными скоростями передачи информации. Требуемая скорость передачи источника нагрузки может иметь случайный характер случайный характер как в момент возникновения заявки на обслуживание, так и в процессе передачи информации. Это обстоятельство требуется учитывать на этапе разработки САД на основе перспективных сетевых и информационных технологий. Нагрузка, создаваемая этими источниками, уже не является обычной пуассоновской нагрузкой, как это обычно предполагается при анализе телефонных сетей и не является также маркированной пуассоновской нагрузкой, как это принимается при анализе узкополосной ЦСИС.

Выводы

При описании моделей нагрузки, возникающей в САД, построенной на принципах широкополосной ЦСИС, обычно используется трёхуровневая модель источника нагрузки [5]. Первый уровень данной модели является уровнем вызовов и отбоев. Второй уровень – активной передачи информации. Третий уровень – передачи ячеек. Перечисленным уровням соответствуют три уровня управления: уровень вызова, уровень интервала активной передачи информации, уровень информационной ячейки.

Общая идеология исследования уровня передачи информационной ячейки, как правило базируется на предположении, что поток ячеек является непрерывным с заданной средней скоростью. Один из подходов к исследованию данной проблемы состоит в том, что предполагается [6]:

− малая ёмкость буферного накопителя и относительно малая скорость поступления информационных ячеек, при которых вероятность поступления двух ячеек на один путь была бы мала;

− вероятность перегрузки, с которой возникает большое число необслуженных ячеек в одно и то же время, пренебрежительно мала.

Эти предположения дают возможность моделировать уровень с помощью бернулиевского и пуассоновского случайных процессов с дискретным временем. Указанные допущения приводят к уже хорошо изученным моделям массового обслуживания с ограниченной ёмкостью буфера и детерминированным временем обслуживания [7].

Список литературы

1. Полак Э. Численные методы оптимизации. Пер. с англ. под ред. Вателя И. А. // М.: Изд-во «Мир». 1984. 376 с.

2. Бронштейн И. Н., Семендяев К. А. Справочник по математике для инженеров и учащихся ВТУЗов // М.: Наука. 1981. 720 с.

3. Волкова В. Н., Денисов А. А. Основы теории систем и системного анализа. 2-е изд. // СПб.: Изд-во СПбГПУ. 1999. 512 с.

4. Битнер В. И. Нормирование качества телекоммуникационных услуг: учебное пособие; под ред. профессора Шувалова В. П. // М.: Горячая линия – Телеком. 2004. 312 с.

5. Ершов В. А., Кузнецов Н. А. Мультисервисные телекоммуникационные сети // МГТУ им. Баумана. 2003. 432 с.

6. Бусленко Н. П. Моделирование сложных систем. 2-е изд. // М.: Наука. 1978. 400 с.

7. Хинчин А. Я. Работы по математической теории массового обслуживания под ред. Гнеденко Б. В. // М.: Физматлит. 1963. 235 с

УДК 621.396.24

Разработка и исследование цифрового радиоприёмного тракта в сложной помеховой обстановке реального КВ-канала

Михайлов В. А., Каримов Т. И., Росин С. Б.

ПАО «Интелтех», г. Санкт-Петербург, Россия

Аннотация: *Разработка устойчивых к помехам радиоприёмных трактов для коротковолнового диапазона остаётся актуальной задачей в связи с вероятностью существенных искажений сигнала и отсутствием средств контроля целостности данных в ряде систем связи, подлежащих модернизации. Для снижения вероятности битовой ошибки в работе предложено использовать фильтр на основе вейвлет-преобразования, и на базе данного подхода разработан цифровой радиоприёмный тракт для приёма F1B-сигналов.*

В рамках настоящего исследования проведён сравнительный анализ методов цифровой фильтрации при воздействии различных типов искажений, включая моделирование канала связи с использованием модели Ватерсона, что позволило учитывать характерные для КВ-диапазона эффекты распространения сигнала и обосновать выбор алгоритмов, используемых в разработанном радиоприёмном тракте.

Ключевые слова: *коротковолновый диапазон, модуляция F1B, цифровой радиоприёмный тракт, модель Ватерсона, КИХ-фильтр, вейвлет-фильтрация, вероятность битовой ошибки.*

Введение

Развитие систем радиосвязи, функционирующих в условиях сложной помеховой обстановки, остаётся актуальной задачей, несмотря на широкое распространение современных цифровых технологий передачи данных. Это связано с тем, что в ряде прикладных областей продолжают использоваться проверенные временем решения, в частности системы коротковолновой (КВ) радиосвязи, обладающие высокой дальностью и независимостью от инфраструктуры [1]. При этом особенности распространения радиоволн в КВ-диапазоне приводят к существенным искажениям сигнала, что затрудняет обеспечение устойчивого и достоверного приёма информации.

КВ-канал (коротковолновый канал) – это путь распространения радиоволн в коротковолновом диапазоне частот, который обеспечивает связь на большие расстояния за счёт отражения от ионосферы – слоя ионизированных газов в верхней атмосфере Земли. К коротким волнам относят частоты от 1,6 до 30 МГц (длина волны от 200 до 10 метров). К основным факторам, влияющим на качество приёма в КВ-канале, относятся многолучевость, замирания сигнала, а также доплеровские смещения частоты [2]. Кроме того, существенное влияние оказывают шумы различной природы, включая как аддитивные, так и импульсные помехи. В совокупности данные факторы приводят к росту

вероятности битовой ошибки и усложняют задачу построения эффективного радиоприёмного тракта.

Особый интерес представляет задача приёма телеграфных сообщений с частотной манипуляцией (F1B), поскольку подобные сигналы широко используются в существующих системах морской связи. При этом такие системы зачастую не предусматривают механизмов контроля целостности данных, что повышает требования к качеству обработки сигнала на стороне приёмника. В связи с этим возникает необходимость разработки алгоритмов цифровой обработки сигналов, обеспечивающих устойчивый приём в условиях значительных искажений.

В настоящее время на для рассматриваемых радиолиний уже реализован радиоприёмный тракт, предназначенный для решения аналогичной задачи. Однако точность приёма в условиях реального КВ-канала может быть повышена. Кроме того, существующее решение не в полной мере учитывает специфику КВ-диапазона, в частности влияние замираний и частотно-временных искажений, что ограничивает его эффективность. Это определяет необходимость проведения дополнительного исследования и разработки более адаптированных методов обработки сигнала.

Целью данной работы является разработка алгоритмов фильтрации, демодуляции и синхронизации, обеспечивающих устойчивый приём сообщений в условиях помех естественной среды.

Для достижения поставленной цели необходимо решить следующие задачи:

Обзор предметной области;

− Моделирование канала связи и проведение сравнительного анализа методов фильтрации;

− Реализация алгоритмов цифровой обработки в радиоприёмном тракте;

− Оценка качества и сопоставление результатов.

Объектом исследования является цифровой радиоприёмный тракт в комплексах связи КВ-диапазона.

Предметом исследования (рис. 1) являются алгоритмы цифровой обработки сигналов, включая фильтрацию, демодуляцию и синхронизацию, в условиях сложной помеховой обстановки.

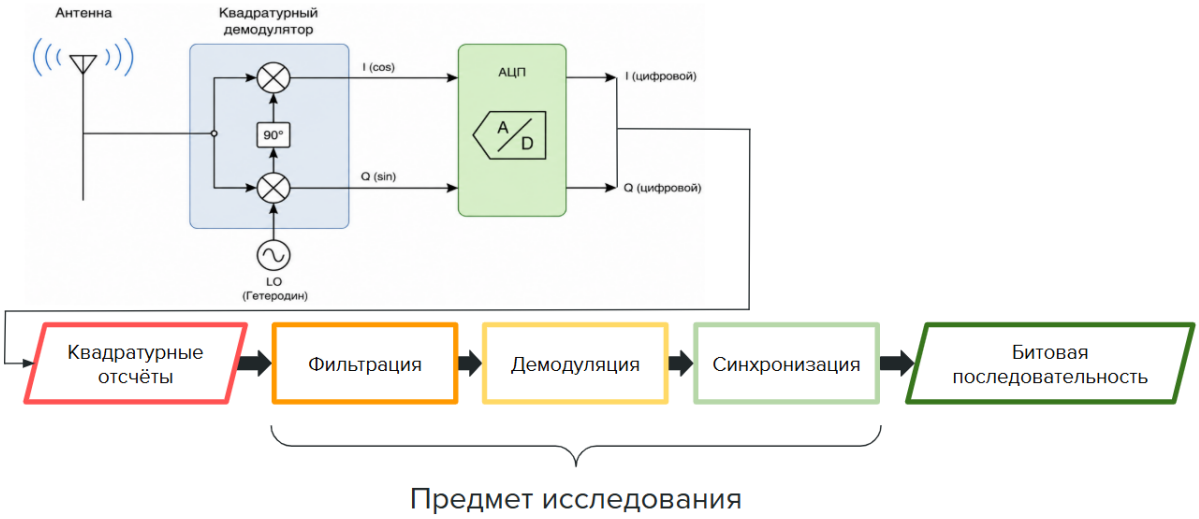


Рис. 1. Структурная схема радиоприёмного тракта

Практическая значимость работы заключается в возможности применения разработанных алгоритмов при модернизации существующих систем радиосвязи морских судов, а также при создании новых технических решений, ориентированных на работу в условиях КВ-канала.

Построение модели реальных шумов

В работе использовались данные, записанные из реального эфира, однако длина записанного сигнала было недостаточной для проведения полноценного исследования – всего 3 минуты записи, поэтому возникла идея получить статистическую модель шума, позволяющую генерировать реалистичные шумовые реализации для использования в экспериментах вместо АБГШ и других искажений.

Выделение шумовой составляющей.

Первым шагом являлось выделение шумовой составляющей из реальной записи. Для этого был расшифрован реальный сигнал из канала с использованием разработанного приёмного тракта. Корректность расшифровки была подтверждена следующим образом: в принятой битовой последовательности были обнаружены пять циклов по 38 повторений чередующихся «0» и «1», то есть пять последовательных меандров. Наличие меандров является стандартной процедурой проверки канала в системах RTTY и однозначно свидетельствует о том, что демодуляция выполнена корректно.

На основе расшифрованной битовой последовательности был синтезирован чистый F1B-сигнал со следующими параметрами:

Частота дискретизации приёмника: 24000 Гц;

Символьная скорость: 50 бод = 50 бит/с;

Индекс модуляции: 4 («0»: -100 Гц; «1»: +100 Гц);

Амплитуда сигнала: 6837,16.

Затем из реального записанного сигнала S был вычтен синтезированный чистый сигнал C:

$$\hat{n} = S - C.$$

Полученная разность $\hat{n}$ рассматривается как потенциальная реализация ансамбля шумов реального КВ-канала.

Статистический анализ шумовой реализации.

Из полученной шумовой реализации были удалены выбросы, определённые по межквартильному размаху (IQR): отсчёты, выходящие за пределы $[Q_1 - 1{,}5 \cdot IQR, Q_3 + 1{,}5 \cdot IQR]$, исключались из анализа. После удаления выбросов была построена гистограмма распределения амплитуд (рис. 2), которая по форме напоминает колоколообразную кривую с умеренно тяжёлыми хвостами.

Для аппроксимации эмпирического распределения были опробованы двенадцать теоретических распределений: обобщённое нормальное, Коши, Стьюдента, треугольное, бета, Лапласа, гауссовское гипергеометрическое, Рэлея, нормальное, гамма, логнормальное и Вейбулла. Близость каждой аппроксимации к эмпирическим данным оценивалась по двум критериям: статистике Колмогорова-Смирнова (KS) и информационному критерию Акаике (AIC). Критерий KS оценивает максимальное отклонение между эмпирической и теоретической функциями распределения, тогда как AIC учитывает как качество подгонки, так и число параметров модели, штрафуя за избыточную сложность [3].

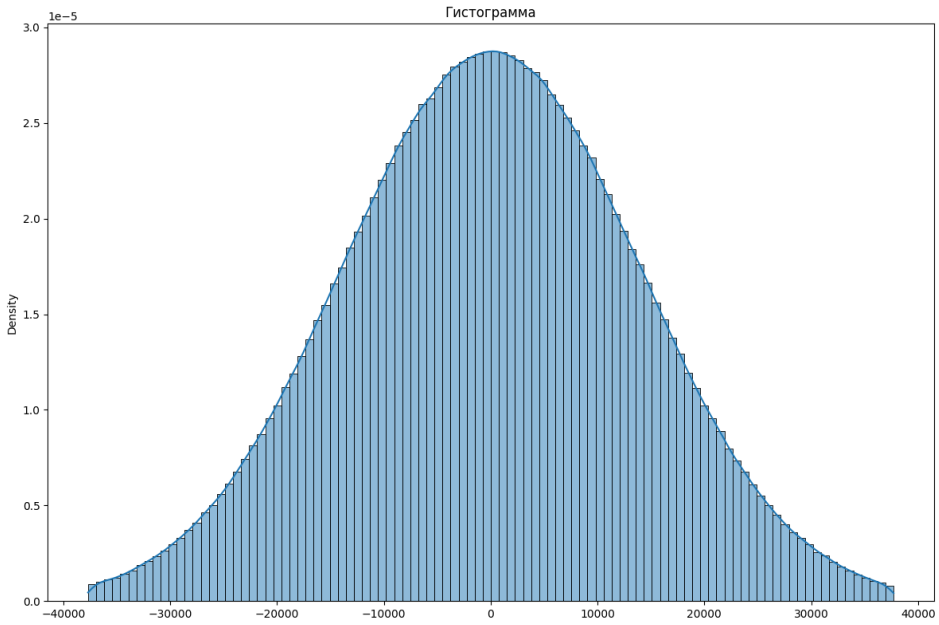


Рис. 2. Гистограмма распределения амплитуд шумовой реализации после удаления выбросов

По обоим критериям наилучший результат показало распределение Вейбулла со следующими параметрами: c=3,6, loc=-44043,36, scale=48872,5 (рис. 3).

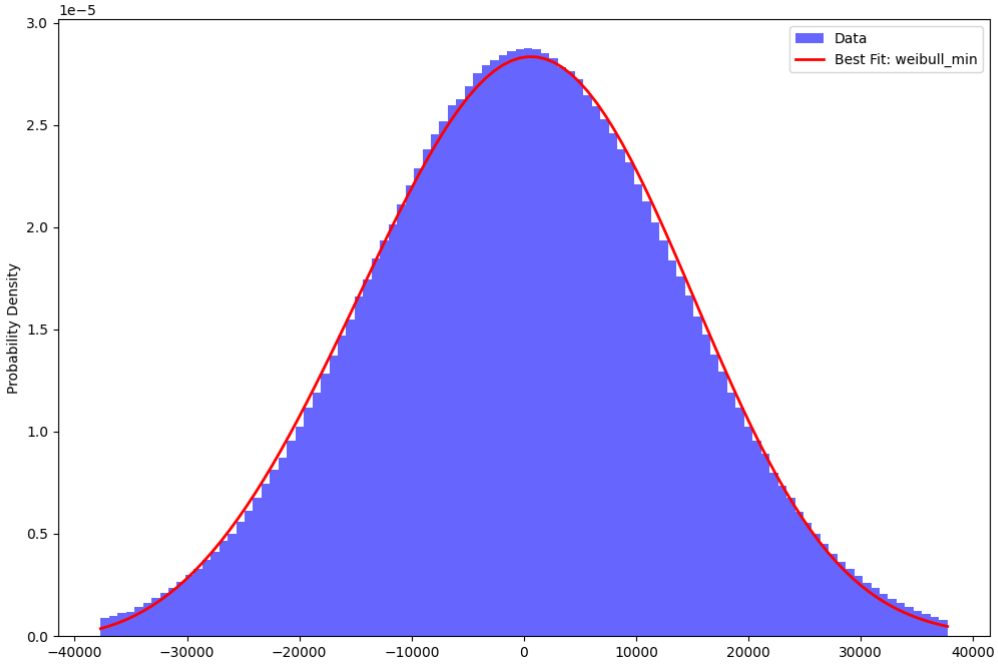


Рис. 3. Аппроксимация ансамбля шумов распределением Вейбулла

Верификация модели шума. На втором этапе была предпринята попытка подтвердить, что случайный процесс с найденным распределением действительно адекватно моделирует реальные шумы. Для этого формулировалась задача оптимизации: требовалось найти параметры распределения Вейбулла (c, loc, scale), при которых среднеквадратическое отклонение между реальным сигналом S и суммой синтезированного сигнала и шумовой выборки $C + a_i$ минимально:

$$RMSE(c, loc, scale) = \sqrt{\frac{1}{N}\sum_{n=1}^{N}(S[n] - (C[n] + a_i[n]))^2} \to \min,$$

где $a_i \sim Weibull(c, loc, scale)$. Задача решалась методом Симплексов (алгоритм Нелдера-Мида), в результате чего были получены оптимальные параметры: c=9,259, loc=8482,687, scale=109,568. Однако полученное значение RMSE оказалось достаточно большим, что поставило под сомнение применимость данной метрики для оценки близости сигналов.

Причина высокого RMSE состоит в следующем: реальный сигнал S и синтезированный сигнал C могут иметь фазовое рассогласование, при котором даже незначительный сдвиг по времени приводит к большому значению

поточечной разности. В этих условиях RMSE перестаёт быть адекватной мерой близости сигналов.

В связи с этим сигналы были проанализированы визуально. На рис. 4 представлены отфильтрованные записанный (красный) и синтезированный (синий) в сравнении с синтезированным сигналом без добавления шума (зелёный). Можно заметить, что график демонстрирует довольно близкое совпадение, но необходимо это проверить и количественно с помощью каких-то метрик, помимо RMSE. Были применены две альтернативные метрики. Первая – нормированный максимум взаимно-корреляционной функции, то есть оба сигнала нормируются на свои среднеквадратические отклонения, вычисляется полная ВКФ, которая затем нормируется на длину более короткого из двух сигналов, и берётся максимум модуля. Полученное значение составило 0,025, тогда как для двух идентичных сигналов, смещённых по фазе, данная метрика должна быть близка к 1. Столь низкое значение свидетельствует о том, что S и $C + a_i$ не являются близкими реализациями одного процесса.

Вторая метрика основана на сравнении статистики локальных экстремумов двух сигналов. Для каждого из сигналов – реального S и $C + a_i$ синтезированного – находились локальные максимумы и минимумы квадратурной компоненты с помощью функции scipy.signal.find_peaks. Затем для каждого набора экстремумов вычислялась матрица попарных евклидовых расстояний между ними в пространстве (t_k, A_k), где t_k – временна́я позиция экстремума, A_k – его амплитуда:

$$d_{ij} = \sqrt{(t_i - t_j)^2 + (A_i - A_j)^2}.$$

Метрика близости двух сигналов определялась как относительная разность средних попарных расстояний для максимумов и минимумов:

$$\Delta_{\max} = \frac{\left|\bar{d}^{(S)}_{\max} - \bar{d}^{(C)}_{\max}\right|}{\bar{d}^{(S)}_{\max}}, \quad \Delta_{\min} = \frac{\left|\bar{d}^{(S)}_{\min} - \bar{d}^{(C)}_{\min}\right|}{\bar{d}^{(S)}_{\min}},$$

где $\bar{d}^{(S)}_{\max}, \bar{d}^{(C)}_{\max}$ – средние попарные расстояния между максимумами реального и синтезированного сигналов соответственно, аналогично для минимумов. Итоговое значение метрики Δ=0,0043 формально является хорошим результатом и свидетельствует о схожести статистики экстремумов двух сигналов. Однако данная метрика чувствительна лишь к усреднённому разбросу экстремумов, но не к их конкретному расположению во времени и не к форме сигнала между ними, и поэтому не является достаточной для вывода о близости сигналов в целом.

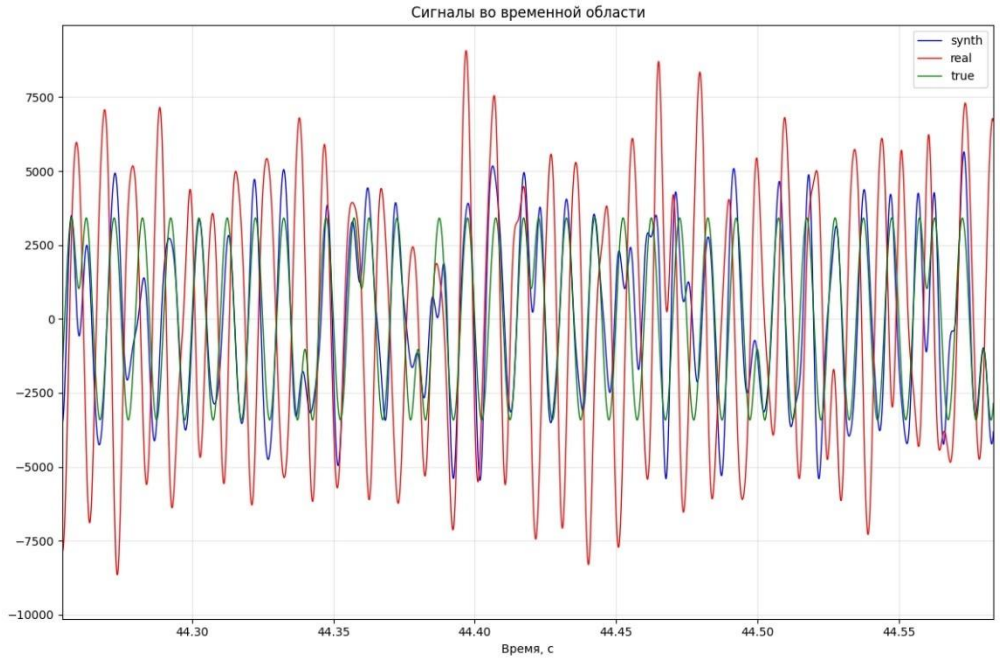


Рис. 4. Сравнение сигналов

Попытка построения модели реальных шумов на основе статистической аппроксимации распределением Вейбулла не привела к успеху: полученная модель не обеспечивает достаточно точного воспроизведения реального шумового процесса. Более перспективным подходом к решению данной задачи могло бы стать применение методов нелинейной идентификации систем – в частности, рядов Вольтерра, позволяющих моделировать нелинейные динамические системы с памятью [4], либо нейросетевых методов иденификации, способных аппроксимировать произвольно сложные зависимости между входом и выходом динамической системы. Реализация подобных подходов выходит за рамки настоящей работы, однако представляет собой перспективное направление для дальнейших исследований.

Моделирование и сравнительный анализ методов фильтрации Модель Ватерсона

Существуют модели, способные учитывать основные физические эффекты присущие непосредственно каналам КВ-диапазона (рис. 5). Одной из наиболее распространённых моделей такого типа является модель Ватерсона, разработанная на основе экспериментальных данных и рекомендованная Международным союзом электросвязи ITU-R F.1487 [5, 6, 7].

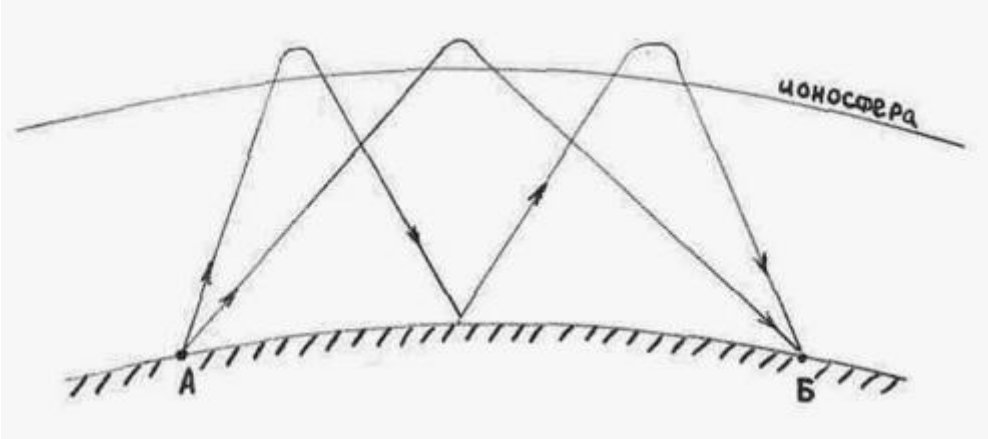


Рис. 5. Многолучевое распространение радиоволн в КВ-канале.

Эта модель аппроксимирует ионосферный канал с ограниченным числом дискретных лучей (обычно от 2 до 6), каждый из которых характеризуется:

1. Относительной задержкой τ_i (обычно от 0 до 5 мс);

2. Относительным коэффициентом усиления (мощности) G_i (в дБ);

3. Доплеровским расширением спектра $B_{d,i}$ (шириной доплеровского спектра, обычно от 0.1 до 2 Гц);

4. Формой доплеровского спектра (обычно гауссовой).

На основе этих характеристик каналы разделяются на три категории: «хороший», «средний» и «плохой», что отображено в таблице 1.

Таблица 1 – Характеристики ионосферных каналов

Профиль	Условия	Кол-во лучей	Задержки (мс)	Доплеровское расширение (Гц)
Плохой	Сильная многолучевость, полярные регионы	3-4	До 3-4 мс	0,1-1 Гц
Средний	Умеренные условия, средние широты	2-3	1-2 мс	0,5-2 Гц
Хороший	Спокойная ионосфера, ночью	2	0,5-1 мс	0,1-0,5 Гц

Модель Ватерсона относится к классу статистических моделей многолучевого ка-нала и описывает радиоканал как линейную нестационарную систему с распределёнными по времени задержками и случайными коэффициентами передачи. Основная идея модели заключается

в представлении канала в виде линии задержек (tapped delay line), где каждая ветвь соответствует отдельному пути распространения сигнала через ионосферу.

Коротковолновый канал моделируется линией задержки с отводами для каждой разделённой во времени моды. Этот задержанный сигнал модулирован по амплитуде и фазе случайной комплексной функцией времени, определяемой следующим образом:

$$G_i(t) = G_{ia}(t)\exp(j2\pi f_{ia}t) + G_{ib}(t)\exp(j2\pi f_{ib}t).$$

Здесь индексы a и b обозначают компоненты двух лучей магнитоионного расщепления для i-го элемента. В этом контексте $G_{ia}(t)$ и $G_{ib}(t)$ представляют два независимых комплексных гауссовых эргодических случайных процесса, каждый из которых имеет нулевое среднее и независимые действительную и мнимые части с равными среднеквадратическими значениями, которые вызывают рэлеевские замирания. Экспоненты обеспечивают частотный сдвиг f_{ia} и f_{ib} для магнитных компонент в спектре.

Структурная схема модели Ватерсона ионосферного коротковолнового канала для трёхлучевого случая представлена на рис. 6. Под шумом в этой модели следует понимать любой аддитивный шумовой процесс (внутренний тепловой шум приёмника, внешний атмосферный или индустриальный шум). Под помехой понимается внешняя станционная помеха.

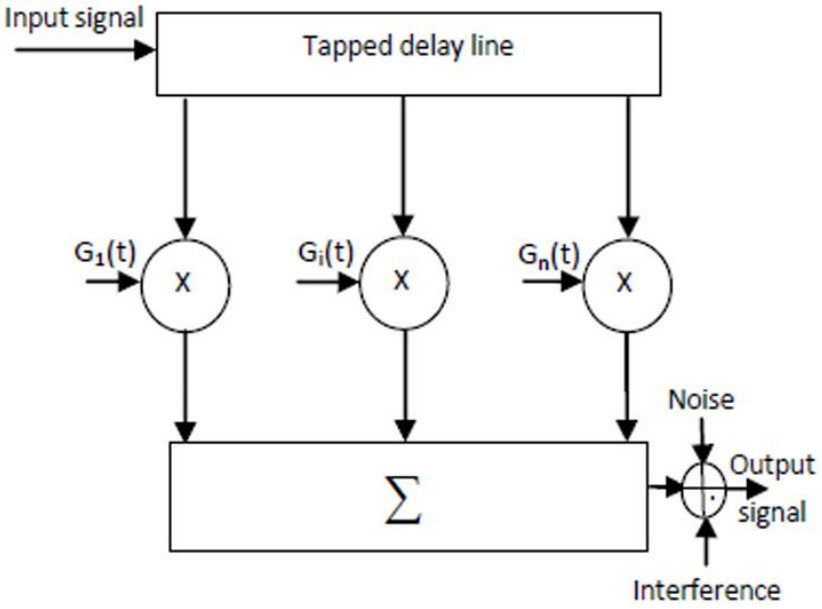


Рис. 6. Модель Ватерсона ионосферного коротковолнового канала

Принятый сигнал r(t) формируется как свёртка переданного сигнала s(t) с импульсной характеристикой канала плюс аддитивный белый гауссов шум n(t):

$$r(t) = \int h(t,\tau)s(t-\tau)d\tau + n(t) = \sum_{i=1}^{N} G_i(t)s(t-\tau_i) + n(t).$$

Комплексная функция рассеяния Ватерсона $G_i(t)$ состоит из двух независимых гауссовых случайных переменных, образующих вектор, который имеет двумерное гауссово распределение. Известно, что модуль комплексной переменной независимого двумерного гауссового случайного процесса имеет распределение Рэлея. Поэтому функция гауссового рассеяния формирует хорошо известные рэлеевские замирания, встречающиеся в распространении коротких радиоволн.

Использование модели Ватерсона в рамках настоящего исследования обусловлено необходимостью воспроизведения условий, близких к реальному КВ-каналу. Проведение экспериментов на реальных данных затруднено из-за ограниченного объёма записей и отсутствия эталонной информации о передаваемой последовательности.

В связи с этим применение статистической модели канала позволяет:

− воспроизводить различные сценарии искажений;

− варьировать параметры канала;

− проводить корректную оценку качества приёма, в частности по метрике BER.

Кроме того, использование данной модели обеспечивает сопоставимость результатов с другими исследованиями, поскольку модель Ватерсона является фактически стандартом при моделировании КВ-каналов. В рамках настоящей работы модель КВ-канала реализована на языке Python.

Сценарии экспериментов

Все эксперименты проводились на сигнале, параметры которого взяты на основе анализа записи реального КВ-приёмника. Эти параметры приведены в разделе 1.

Передаваемая битовая последовательность в каждом эксперименте формировалась случайно из дискретного равномерного распределения: b∼Uniform{0,1}^100. Амплитуда A=6837,16 получена как среднее значение амплитуды отфильтрованного реального сигнала и зафиксирована константой для всех экспериментов, чтобы исключить влияние амплитудного масштаба на результаты сравнения.

Каждый эксперимент повторялся n=1000 раз с независимой реализацией шума и замираний. В качестве итоговых метрик использовались значения BER и максимума ВКФ, усреднённые по всем 1000 прогонам, что обеспечивало статистическую устойчивость результатов.

Сценарии экспериментов. В работе рассматриваются одиннадцать экспериментальных сценариев, охватывающих как одиночные, так

и комбинированные искажения. В каждом сценарии к сгенерированному сигналу последовательно применяются искажения, после чего сигнал подаётся на вход каждого из пяти фильтров, и для каждого фильтра вычисляются BER и максимум ВКФ. Сценарии сведены в таблицу 2.

Ниже приводится подробное описание каждого сценария.

Сценарий №1. Только АБГШ. Базовый сценарий, в котором к чистому сигналу добавляется исключительно аддитивный белый гауссовский шум с SNR=-14 дБ. Данный сценарий является эталонным: он позволяет оценить поведение каждого фильтра в наиболее изученных и теоретически обоснованных условиях, а также верифицировать корректность реализации тракта путём сравнения с теоретическими кривыми BER.

Сценарий №2. Частотное искажение. К сигналу применяется асимметричное частотное искажение с подавлением на частоте f_0 = -100 Гц и с различными порядками фильтра: 651, 801, 821, 851. Дополнительно добавляется АБГШ с SNR=0 дБ или SNR=5 дБ. Сценарий моделирует избирательные замирания в узкой полосе спектра сигнала.

Сценарий №3. Фазовое искажение. К сигналу применяется полосовой фильтр Баттерворта с нелинейной ФЧХ. Дополнительно добавляется АБГШ с SNR=-12 дБ. Сценарий моделирует искажения групповой задержки, характерные для аналоговых трактов согласования и избирательных фильтров приёмника.

Таблица 2 – Сценарии экспериментов

Номер сценария	Тип искажения	Параметры АБГШ
1	Только АБГШ	-14
2	Частотное искажение с помощью КИХ-фильтра	0, 5
3	Фазовое искажение с помощью фильтра Баттерворта	-12
4	Компрессия с помощью гиперболического тангенса	20
5	Мультипликативное искажение	0, 5
6	Канал Ватерсона (с методом суммы синусоид)	20
7	Канал Ватерсона (с методом фильтрации шума)	20
8	Комбинация частотного и мультипликативного искажений	0, 10, 15
9	Комбинация частотного искажения и компрессии	20
10	Комбинация мультипликативного искажения и компрессии	20

Номер сценария	Тип искажения	Параметры АБГШ
11	Комбинация частотного, мультипликативного искажений и компрессии	20

Сценарий №4. Компрессия. К сигналу применяется компрессия огибающей с параметром нелинейности α=0,02. Дополнительно добавляется АБГШ с SNR=20 дБ. Сценарий моделирует работу усилительных каскадов приёмника в режиме насыщения при высоком уровне входного сигнала.

Сценарий №5. Мультипликативное искажение. К сигналу применяется синусоидальная амплитудная модуляция с частотой замираний f_m = 5 Гц, глубиной d=0,8 и случайной начальной фазой. Дополнительно добавляется АБГШ с SNR=0 дБ или SNR=5 дБ. Сценарий моделирует медленные периодические замирания, обусловленные интерференцией двух лучей с медленно меняющейся разностью хода.

Сценарии №6 и 7. Канал Ватерсона. К сигналу применяется модель канала Ватерсона с профилем moderate (три луча, задержки 0; 1,0; 2,5 мс) или poor (четыре луча, задержки 0; 1,0; 3,0; 5,0 мс) с разными методами генерации замираний: суммой синусов и фильтрации шума. АБГШ в данном сценарии добавляется с SNR=20 дБ. Сценарий является наиболее близким к реальным условиям КВ-канала из всех одиночных сценариев.

Сценарий №8. Частотное и мультипликативное искажения. Комбинированный сценарий: последовательно применяются мультипликативное искажение (f_m = 5 Гц, d=0,8) и асимметричное частотное искажение (порядок фильтра 801, f_0 = -100 Гц). Дополнительно добавляется АБГШ с SNR = 0, 10 или 15 дБ. Сценарий моделирует одновременное воздействие амплитудных замираний и частотно-избирательного затухания.

Сценарий №9. Частотное искажение и компрессия. Комбинированный сценарий: к сигналу последовательно применяются асимметричное частотное искажение (порядок фильтра 651, f_0 = -100 Гц) и компрессия огибающей (α=0,04). Дополнительно добавляется АБГШ с SNR=20 дБ. Данное сочетание моделирует ситуацию, при которой частотно-искажённый сигнал поступает на вход нелинейного усилителя.

Сценарий №10. Мультипликативное искажение и компрессия. Комбинированный сценарий: к сигналу последовательно применяются компрессия огибающей (α=0,07) и мультипликативное искажение (f_m = 5 Гц, d=0,8, случайная фаза). Дополнительно добавляется АБГШ с SNR=20 дБ. Порядок применения искажений соответствует типичной цепочке прохождения сигнала: замираниям в канале предшествуют нелинейности усилителя.

Сценарий №11. Частотное, мультипликативное искажения и компрессия. Наиболее сложный комбинированный сценарий, объединяющий три типа искажений: асимметричное частотное (порядок 801, f_0 = -100 Гц), компрессию огибающей (α=0,35) и мультипликативное искажение (f_m = 5 Гц, d=0,8, случайная фаза). Дополнительно добавляется АБГШ с SNR=20 дБ. Данный сценарий призван оценить устойчивость фильтров в условиях, максимально приближенных к реальной помеховой обстановке КВ-канала, когда одновременно присутствуют нелинейные, частотные и амплитудные искажения.

Методы фильтрации

Для борьбы с вышеперечисленными искажениями использовались фильтры из разных классов методов:

− Полосовой КИХ-фильтр [50;150] (Гц) с окном Кайзера порядка 513, это базовый фильтр, который уже реализован в действующем комплексе связи;

− Полосовой КИХ-фильтр [50;150] (Гц) с окном Хэмминга порядка 3961;

− Полосовой БИХ-фильтр Чебышева I типа 3-го порядка [50; 150] (Гц);

− Классический фильтр Калмана (адаптивный);

− Вейвлет-фильтр (Coiflet5, уровень разложения 6, универсальный порог);

− Медианный фильтр с окном 111 (нелинейный).

Параметры фильтров, которые приведены выше, подбирались на основе экспериментов по сценарию №1 путём перебора. Например, окно медианного фильтра выбрано путем перебора его размеров от 11 до 1001 с шагом 10.

Результаты экспериментов

По результатам проведённых экспериментов были получены значения BER для каждого из шести фильтров в каждом сценарии (таблица 3).

Можно заметить, что нет метода, который превосходил бы своих конкурентов во всех сценариях. При этом необходимо обратить внимание на основную модель – ионосферный канал Ватерсона. В этом сценарии лидером является вейвлет-фильтр. В других менее актуальных сценариях он также показывал низкие значения метрики BER, не сильно отставая от других фильтров. Интересно, что есть ряд сценариев, в которых безошибочным оказался медианный фильтр, тогда как в других сценариях он существенно деградировал.

Таблица 3 – Результаты экспериментов

Фильтр №	КИХ-фильтр		БИХ-фильтр	Фильтр Калмана	Вейвлет-фильтр	Медианный фильтр
	с окном Кайзера	с окном Хэмминга				
1	4,20e-4	2,40e-4	4,90e-4	9,46e-4	8,60e-4	4,62e-1
2	1,50e-5	5,04e-4	9,20e-4	5,18e-2	8,04e-4	0,0
3	1,70e-4	1,60e-4	4,80e-4	1,70e-2	1,16e-3	3,79e-1
4	1,50e-4	3,30e-4	6,60e-4	1,00e-2	7,90e-4	4,35e-1
5	3,00e-5	2,50e-5	6,00e-5	5,70e-4	9,5e-5	2,53e-3
6	8,10e-4	3,80e-3	3,60e-3	9,44e-3	3,33e-5	1,80e-3
7	2,20e-4	8,78e-3	3,67e-3	9,00e-5	1,00e-5	3,59e-2
8	8,20e-4	1,62e-3	4,21e-3	3,14e-3	1,56e-3	0,0
9	5,20e-4	8,00e-4	1,02e-3	8,43e-3	1,43e-3	3,06e-3
10	5,30e-4	7,80e-4	1,43e-3	6,97e-3	1,38e-3	1,03e-1
11	1,46e-3	1,71e-3	4,06e-3	3,09e-3	1,29e-3	0,0

Подробнее проанализируем поведение фильтров в канале Ватерсона. На рис. 7 представлена зависимость количества ошибок от отношения сигнал/шум. При низких значениях SNR базовый КИХ-фильтр был лучше вейвлет-фильтра, но при этом он проигрывал фильтру Калмана в этой области. А начиная с 10 дБ вейвлет-фильтр оказывается существенно предпочтительнее остальных методов. При этом уровень шума от 0 до 20 дБ можно считать наиболее реалистичным.

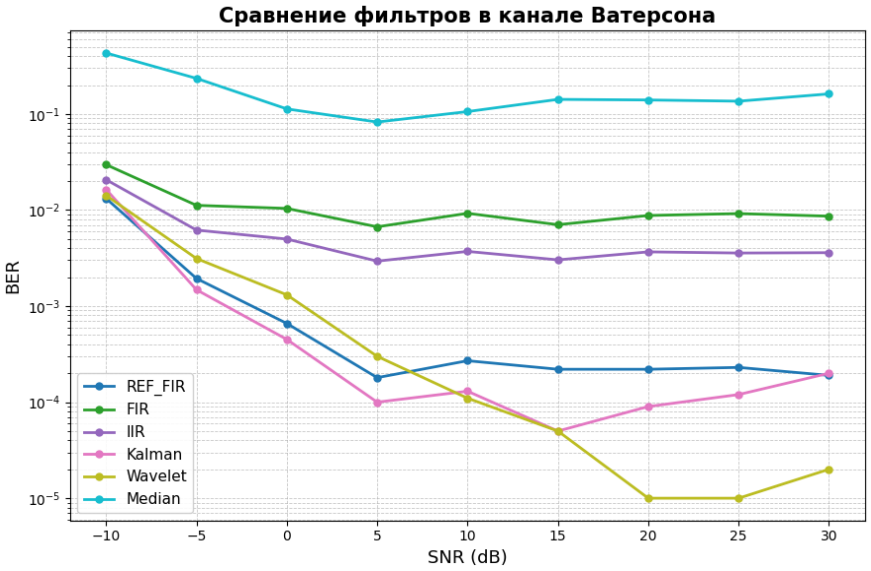


Рис. 7. Зависимость BER-SNR в канале Ватерсона для разных фильтров

Заключение

В настоящей работе решена задача разработки алгоритмов цифровой обработки сигналов для радиоприёмного тракта, обеспечивающего приём F1B-сигналов в коротковолновом диапазоне. Актуальность задачи обусловлена наличием в эксплуатации устаревших систем связи, не оснащённых современными средствами контроля целостности данных и работающих в условиях значительных искажений, характерных для КВ-канала, которые подлежат соответствующей модернизации.

Реализована программная модель КВ-канала на основе модели Ватерсона с двумя методами генерации замирающих коэффициентов – методом суммы синусоид Кларка-Джейкса и методом фильтрации белого шума – в соответствии с рекомендацией МСЭ-Р F.1487. Модель позволяет воспроизводить многолучевое распространение с произвольным числом лучей, нестационарные замирания и доплеровское расширение спектра, характерные для реальных КВ-каналов.

Проведён сравнительный анализ шести алгоритмов цифровой фильтрации. На синтетических данных подход с использованием вейвлет-преобразования превосходит существующее решение на порядок в рамках ионосферного канала Ватерсона.

Исследована модель реальных шумов на основе статистического анализа записи КВ-приёмника. Данная задача остаётся открытой. Перспективным направлением её решения является применение методов нелинейной идентификации – рядов Вольтерра или нейросетевых методов.

По метрике нормированного максимума ВКФ вейвлет-фильтр оказался предпочтительнее КИХ-фильтра в среднем на 2% на промежутках меандра реального сигнала, что в совокупности с результатами моделирования

обосновывает интерес к его внедрению в реальный тракт в качестве ближайшего направления развития. Вместе с тем для полноценного сравнения фильтров на реальных данных необходима представительная база записей с известными передаваемыми последовательностями, что является предметом дальнейших исследований.

Список литературы

1. Harris Corporation, RF Communications Division, Radio Communication In The Digital Age, Volume One: HF Technology, Edition 2, pp 16-38, 2005.

2. Eric E. Johnson, Erik Koski, William N. Furman, Third-generation and Wideband HF Radio Communications, Norwood, MA, Artech House, pp. 7-16, 2013.

3. Akaike H. A New Look at the Statistical Model Identification // IEEE Transactions on Automatic Control. 1974. Vol. 19, No. 6. P. 716–723.

4. Mathews V. J., Sicuranza G. L. Polynomial Signal Processing. John Wiley & Sons, 2000.

5. Watterson C., Juroshek J., Bensema W. // IEEE Trans. Commun. Techn. 1970. V. 18, No. 6. P. 792.

6. CCIR Recommendation 520-1 19821 “Use of High Frequency Ionospheric Channel Simulators”, Geneva: Int. Telecom. Union, 1995.

7. ITU-R Rec. F1487 “Testing of HF Modems with Bandwidth of up to about 12 kHz Using Ionospheric Channel Simulator”. Geneva: Int. Telecom. Union, 2000.

УДК 004.942

Методика информационного обеспечения потребителей о надводной обстановке при проведении поисково-спасательных операций

Тюстин М. М., Черевань Д. В., Зыков Д. Д.

Военно-космическая академия имени А.Ф. Можайского, г. Санкт-Петербург, Россия

Аннотация: *в работе представлена методика информационного обеспечения потребителей информации о надводной обстановке при проведении поисково-спасательных операций с использованием малогабаритного SDR-приемника и антенны петлевого типа, размещаемых на борту авиационного носителя, на основе приема и демодуляции сигналов автоматической идентификационной системы. Предложенная архитектура позволяет в реальном масштабе времени обеспечить одновременный доступ к данным о местоположении, идентификационных номерах и параметрах движения морских объектов для всех потребителей без увеличения числа приемных устройств, размещаемых на авиационном носителе.*

Ключевые слова: *поисково-спасательная операция, автоматическая идентификационная система, SDR-приемник, надводный объект, радиомониторинг.*

Введение

Поисково-спасательная операция (ПСО) представляет собой комплекс организационных и технических мероприятий, обеспечивающих обнаружение и установление координат местоположения кораблей (людей), которые терпят бедствие на море, и их последующее спасание.

Поисково-спасательные операции и их координация осуществляются национальными (государственными) организациями оповещения о бедствии, поиска и спасания, ведомственными службами наблюдения за флотом и аварийно-спасательными службами, службами безопасности мореплавания судовладельцев и другими подразделениями их систем управления безопасностью. В проведении ПСО участвуют береговые радиостанции, специализированные поисково-спасательные морские и воздушные суда, выделенные участниками взаимодействия, а также другие морские и воздушные суда, находящиеся в районе или вблизи района бедствия [1].

Наиболее информативным источником данных о местоположении судов, терпящих бедствие, является автоматическая идентификационная система (АИС), которая представляет из себя многофункциональную информационно-техническую систему, оборудование которой устанавливается на судах и в береговых службах в целях обеспечения безопасности мореплавания и автоматизации обмена навигационной информацией.

АИС обеспечивает:

– автоматическую и регулярную передачу судном другим судам и береговым службам информации, включающей сведения о судне, координаты, курс, скорость и другие данные;

− автоматический прием, обработку и отображение аналогичной информации от других судов и береговых служб;

− автоматическое сопровождение (прокладку движения) судов, оборудованных АИС, в целях предупреждения столкновений, а также контроля и регулирования судоходства;

− автоматизированный обмен сообщениями, связанными с безопасностью мореплавания, между судами и береговыми службами.

Авиационные средства поиска и спасения являются ключевым элементом морских ПСО. Их главные преимущества — это скорость и способность быстрого прибытия в удаленные районы, что критично для спасения жизней, так как вероятность выживания пострадавших резко падает в первые часы бедствия. Кроме того, возможность обширного охвата морских акваторий и высокая дальность действия позволяют наиболее эффективно оптимизировать маршруты полета [2].

Таким образом, в качестве наиболее эффективного средства проведения ПСО в морских акваториях и прибрежных зонах целесообразно рассматривать авиационные носители, оборудованные аппаратурой приёма и регистрации данных АИС.

При этом актуальной научно-прикладной задачей является разработка методики использования указанных данных для информационного обеспечения потребителей при оценке надводной обстановки.

Методика информационного обеспечения потребителей о надводной обстановке при проведении поисково-спасательных операций

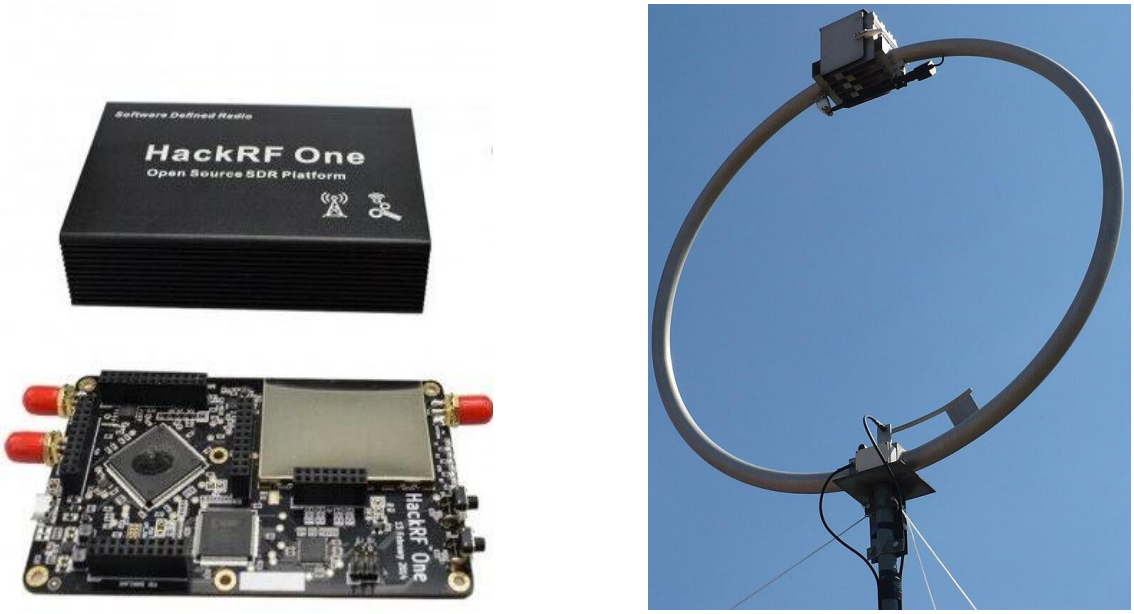
Под информационным обеспечением ПСО в контексте данной работы понимается своевременное предоставление потребителям сведений о типе надводного объекта, терпящего бедствие, его идентификационном номере морской подвижной службы (MMSI), последних зафиксированных координатах местоположения, путевой скорости и истинном курсе в момент бедствия [3]. Кроме того, специализированные персональные маяки АИС, которые крепятся к спасательному жилету, при активации начинают передавать сигнал с координатами человека. Точность такого позиционирования достигает 5 метров, что позволяет оперативно навести силы спасения на точку, где находится пострадавший.

Основой для получения перечисленных сведений является АИС, функционирующая в УКВ-диапазоне. В условиях отсутствия доступа к сети «Интернет» в ходе выполнения ПСО, единственным источником данных выступает непосредственный прием сигналов АИС на борту авиационного носителя.

Наличие в составе бортового оборудования воздушного носителя приемной аппаратуры и специализированного программного обеспечения для демодуляции сигналов позволяет существенно сократить временные затраты на поиск и идентификацию судов терпящих бедствие.

Корабельные станции АИС осуществляют передачу данных попеременно на двух фиксированных несущих частотах (161,975 МГц и 162,025 МГц) с шириной спектра сигнала 12,5 кГц (в территориальных водах) или 25 кГц (в открытом море) [4].

Прием сигналов обеспечивается пассивной антенной петлевого типа (Loop) с воздушным конденсатором, настроенной на центральную частоту 162 МГц. Антенна ориентирована в нижнюю полусферу для максимального охвата акватории (рисунок 1). Радиосигнал с антенны по высокочастотному фидеру (кабель РК-50) поступает на вход SDR-приемника HackRF, который выполняет функции оцифровки и переноса спектра в промежуточную частоту. Характеристики приемника (диапазон частот до 6 ГГц, полоса обзора до 20 МГц) позволяют производить захват всей необходимой полосы сигналов АИС [5].



а. б.

Рис 1. SDR-приемник HackRF с антенной типа Loop для регистрации сигналов АИС (а. – внешний вид приемника, б. – внешний вид антенны)

Структурная схема комплекса приема и регистрации сигналов АИС представлена на рисунке 2.

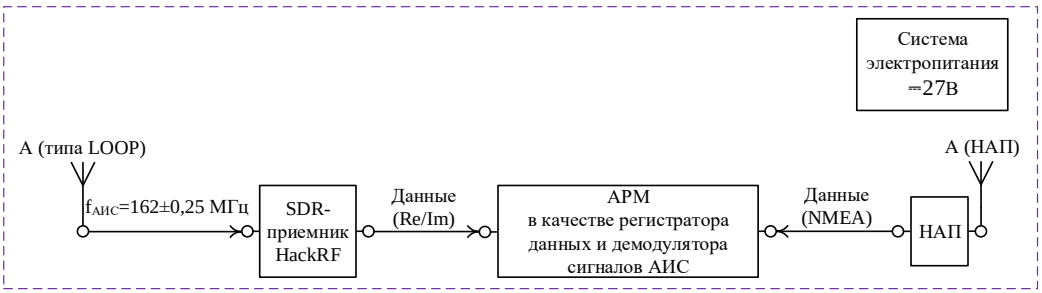


Рис. 2. Структурная схема комплекса приема и обработки сигналов АИС.

Технические характеристики применяемого SDR-приемника приведены

в таблице 1.

Таблица 1 – Характеристики SDR-приемника HackRF

№ п/п	Параметр	Значение
1.	Диапазон рабочих частот, МГц	50 - 6000
2.	Коэффициент усиления приемной антенны, дБ	8
3.	Пороговая чувствительность, дБВт/Гц	-173
4.	Коэффициент стоячей волны	1,6
5.	Полоса одновременного обзора, МГц	1 - 20
6.	Разрядность АЦП, бит	8
7.	Частота дискретизации АЦП, МГц	1 - 20
8.	Скорость обзора полосы шириной 1 ГГц, сек	5

Демодуляцию зарегистрированных сигналов (посылок) АИС возможно осуществлять с помощью свободно распространяемого программного комплекса SDRangel (рисунок 3) [6].

Отличительной особенностью программного комплекса SDRangel является возможность одновременной демодуляции сигналов АИС сразу на двух несущих частотах, при условии:

$$\Delta f_{\text{РПУ}} \geq f_{\text{нес}}^{(2)} - f_{\text{нес}}^{(1)} + \Delta f_{\text{АИС}}. \quad (1)$$

где $\Delta f_{\text{РПУ}}$ – ширина полосы пропускания радиоприемного устройства (HackRF);

$f_{\text{нес}}^{(1)}$, $f_{\text{нес}}^{(2)}$ – значения несущих частот приемных каналов АИС;

$\Delta f_{\text{АИС}}$ – ширина полосы частот, занимаемая сигналом АИС.

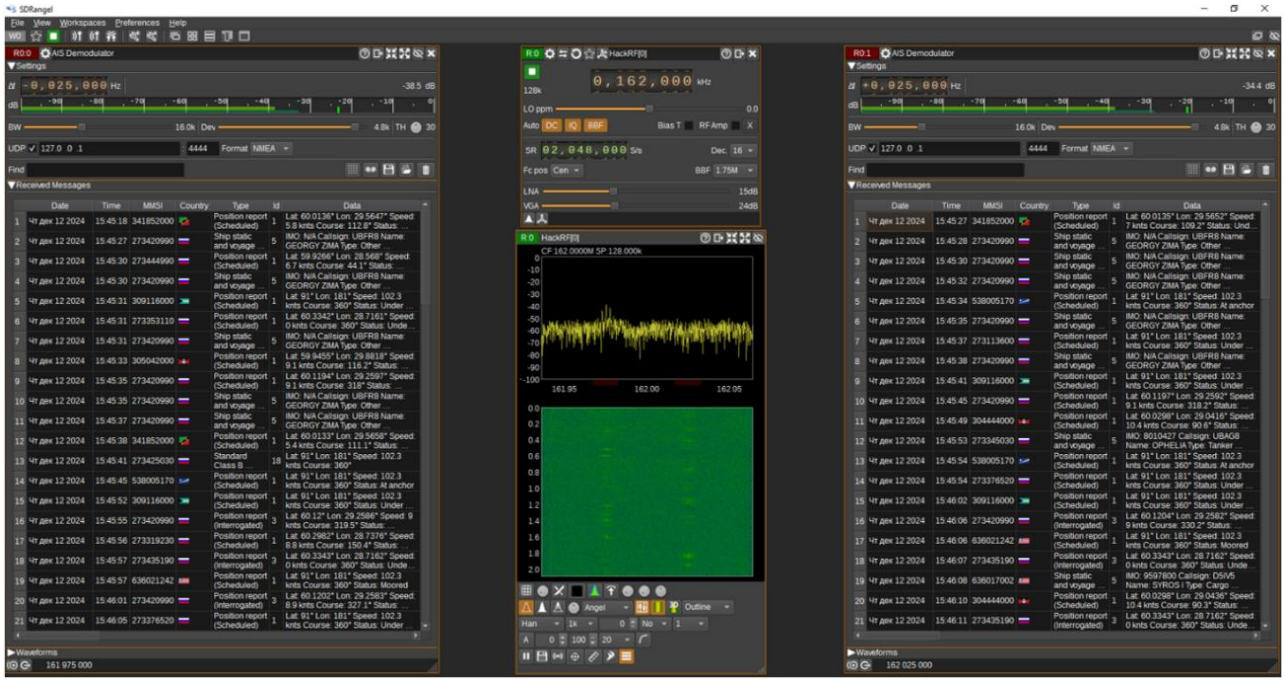


Рис. 2. Пример регистрации данных АИС

При включении в состав бортового оборудования дополнительного навигационного модуля GPS-ГЛОНАСС (рисунок 4) возможно отображение реального местоположения авиационного носителя относительно морских судов с целью контроля надводной обстановки в районе проведения ПСО, а также для построения оптимальных маршрутов при поиске и идентификации терпящих бедствие.

Предлагаемая методика включает в себя следующие этапы:

1. Обнаружение сигнала бедствия. При аварии судно активирует аварийный передатчик АИС-SART, который передаёт сигнал в УКВ-диапазоне, содержащий координаты места бедствия. Кроме того, предусмотрена возможность ручной отправки текстового сообщения о бедствии.

2. Приём и обработка сигналов АИС. Сигналы АИС принимаются береговыми станциями и судами-спасателями. Полученные данные автоматически декодируются и отображаются на электронных навигационных картах.

3. Анализ траектории и статуса судна. Операторы осуществляют мониторинг движения объекта. Резкое изменение курса, скорости или статуса (например, переход из режима «в движении» в режим «на якоре») может свидетельствовать о возникновении аварийной ситуации.

4. Оповещение и координация. При подтверждении аварийной ситуации данные о местоположении судна передаются в координационно-спасательные центры для планирования и организации поисково-спасательных мероприятий.

5. Подъем авиационного носителя. По команде из координационного центра выполняется подъём авиационного носителя, производится расчёт оптимального маршрута поиска и спасения, после чего осуществляется выдвижение в район проведения ПСО.

Рис. 4. Пример отображения данных АИС на карте местности

6. Поиск пострадавших. В районе бедствия поиск ведётся с использованием данных сигналов АИС, принимаемых бортовой аппаратурой авиационного носителя.

7. Визуальное подтверждение. Экипаж авиационного средства осуществляет визуальное обнаружение и подтверждение точного местоположения терпящих бедствие.

8. Проведение спасательных мероприятий. После подтверждения координат выполняется комплекс спасательных работ в соответствии с действующими регламентами.

Таким образом, применение комплекса приема и регистрации сигналов АИС на базе SDR-приемника HackRF с антенной типа Loop позволяет решить вопрос получения статической, динамической и рейсовой информации о надводных судах, терпящих бедствие, а также осуществлять поиск пострадавших, спасательные жилеты которых оборудованы персональными радиомаяками системы АИС.

Экспериментальная проверка комплекса приема и обработки сигналов АИС проводилась в условиях, приближенных к реальной эксплуатации. Измеренная дальность уверенного приема сигналов АИС от надводных объектов

при высоте полета 6000 метров составила до 180 километров, что подтверждает достаточную энергетику канала для решения задач обнаружения и координации береговых и надводных служб при проведении ПСО.

Заключение

Предложенная методика сокращает время между обнаружением аварийной ситуации и началом активных спасательных действий благодаря автоматизированной обработке сигналов на борту авиационного носителя, визуализации на электронных картах и оперативному информированию координационных центров.

Комплекс приема и обработки сигналов АИС, на базе SDR-приемника HackRF с антенной типа Loop, при размещении на борту авиационного носителя позволяет обеспечить информацией о надводной обстановке всех потребителей в ходе проведения ПСО, что критически важно в условиях жестких ограничений по времени реагирования спасательных служб на возникающие происшествия.

Результаты натурного эксперимента свидетельствуют о высокой эффективности использования низкобюджетных малогабаритных SDR-приемников для организации поиска пострадавших на основе приема и демодуляции сигналов АИС при проведении ПСО в морских акваториях.

Список литературы

1. Термины МЧС России - URL: https://www.mchs.gov.ru/ministerstvo/o-ministerstve/terminy-mchs-rossii/term/3262 (дата обращения: 01.09.2026).

2. Топольский, М.Г. Методика планирования поисково-спасательных работ в природной среде / М.Г. Топольский, Д.С. Береснев, А.А. Рыженко, А.В. Мокшанцев // Технологии техносферной безопасности: Интернет-журнал – 2016. – Вып. № 3 (67). – С. 165-169. http://www.agps-2006.narod.ru/ttb/2016-3/33-03-16.ttb.pdf.

3. Временное руководство по использованию автоматической информационной (идентификационной) системы на судах и в береговых службах / Государственная служба морского флота – М:. Министерство транспорта РФ, 2002. – 58 с.

4. Рекомендация МСЭ-R M.1371-4 (04/2010). Технические характеристики системы автоматической идентификации, использующей многостанционный доступ с временным уплотнением каналов в полосе ОВЧ морской подвижной службы – Женева: ITU, 2010. – 144 с.

5. HackRF initial review - URL: https://www.rtl-sdr.com/hackrf-initial-review (дата обращения: 07.03.2026).

6. SDRangel – Open-source TX & RX Software Defined Radio - URL: https://www.sdrangel.org (дата обращения: 07.08.2026).

УДК 621.39

Предложения по реализации алгоритмов сопряжения сетей передачи данных специального назначения

Спивак А. В.

ПАО «Интелтех», г. Санкт-Петербург, Россия

Аннотация: *рассмотрены научно-технические предложения по реализации алгоритмов сопряжения авиационных сетей передачи данных с сетями передачи данных наземных служб. В состав предложений вошли три обобщенных алгоритма, описывающих процесс передачи сообщений, соответственно с применением технологического модуля сопряжения, шлюза, моста. Приведены блок-схемы алгоритмов сопряжения, а также их достоинства и недостатки.*

Ключевые слова: *аппаратура передачи данных, блок сопряжения, преобразователь форматов, технологический модуль сопряжения, сеть передачи данных, шлюз.*

Известно, что технологический модуль сопряжения (ТМС) сетей передачи данных (СПД) должен обеспечить преобразование форматов передаваемых сообщений на представительном уровне. Согласование протоколов нижних уровней непосредственно выполняется в аппаратуре передачи данных (АПД) сопрягаемых СПД. В ТМС может быть реализовано преобразование адресов одной сети в адреса другой сети, обмен квитанциями и их преобразование, предотвращение перегрузок. Подключение модуля к АПД рассматриваемых сетей осуществляется по стыку И3. В каждой подсети ТМС должен иметь свой адрес, составленный по тем же правилам, что и адрес любого оконечного оборудования данных (ООД) этой подсети.

Функционирование такой взаимоувязанной СПД происходит следующим образом. Все абоненты одной сети обмениваются стандартными пакетами данных этой сети. Для передачи сообщения в другую сеть в заголовке сообщения должен указываться адрес ТМС сопряжения, который будет использоваться для дальнейшей передачи сообщения. Обобщенный алгоритм, описывающий процесс передачи сообщений из одной СПД в другую через ТМС показан на рис. 1.

Начало алгоритма соответствует вводу сообщения в АПД для передачи. Сообщение, вложенное в пакет своей подсети, отправляется к технологическому модулю сопряжения (блок 2). АПД (к которой подключен ТМС) принимает переданный пакет, извлекает сообщение из принятого пакета и производит его анализ на наличие ошибок (блок 3). При отсутствии ошибок, сообщение передается в ТМС (блок 6). В противном случае, осуществляется повторный прием сообщения. В блоке 7, описывающем ТМС, реализуются алгоритмы преобразования (формата сообщения, адреса, текста и т. д.). Далее, в блоке 8 преобразованное сообщение передается в АПД другой сети. С выхода АПД закодированное сообщение в составе пакета новой подсети пересылается АПД получателя (блок 9), в которой производится рассекречивание принятого

сообщения и анализ на наличие ошибок (блок 10). При отсутствии ошибок АПД передает квитанцию на полученное сообщение, если у него отсутствует признак циркуляра или списка, и сообщение выводится получателю (блоки 14,15). В противном случае, осуществляется повторный прием сообщения (блок 12). В соответствии с вышеизложенным алгоритмом работы ТМС может быть представлен следующим образом (рис.1).

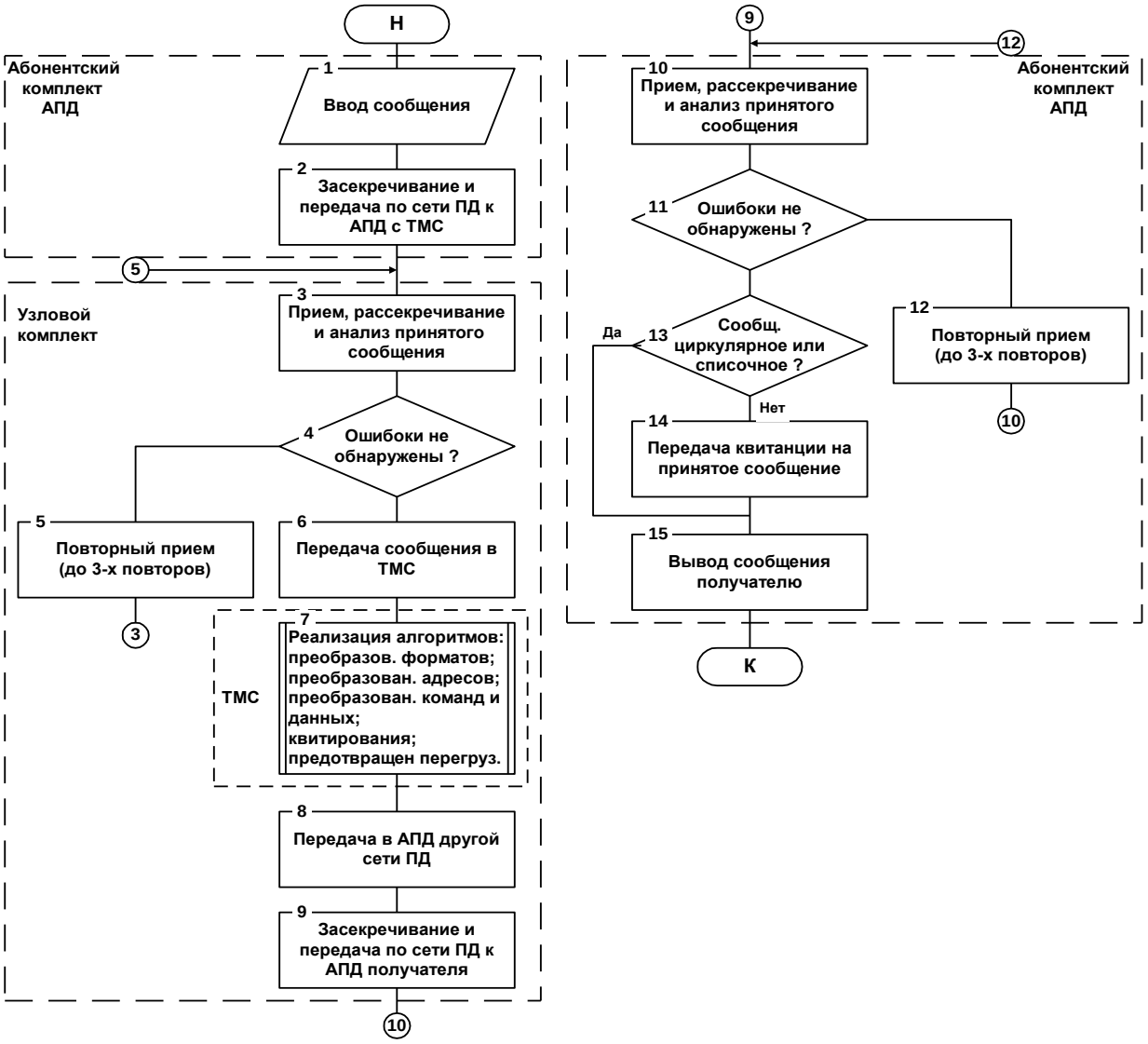


Рис. 1. Обобщенный алгоритм, описывающий процесс передачи сообщений из одной СПД в другую через ТМС

В составе ТМС можно выделить преобразователь форматов (ПФ), обеспечивающий: выполнение основных функций по преобразованию форматов сообщений; согласование способов распределения информации; приоритетное обслуживание сообщений в зависимости от их категории срочности.

Преобразователь форматов может быть выполнен на базе микропроцессора, включающего в себя: два блока сопряжения (БС1 и БС2), обеспечивающие сопряжение ТМС по стыку И3, соответственно; два специальных вычислителя (СВ1 и СВ2), управляющие работой БС1 и БС2; репрограммируемое запоминающее устройство (РПЗУ), служащее для хранения

изменяемой в процессе эксплуатации служебной информации; оперативное запоминающее устройство (ОЗУ), обеспечивающее хранение информации и промежуточных результатов обработки при совместной работе СВ1 и СВ2.

В состав ТМС также должен входить блок питания, предназначенный для преобразования напряжения 27В в напряжения различных номиналов, необходимых для питания микросхем и радиоэлементов.

Анализ показывает, что основным достоинством ТМС является простота реализации и минимум затрат. Недостатком использования ТМС является обязательное его применение только совместно с АПД (изделие А и изделие Б), что может привести к существенному увеличению временных затрат. Прогнозные оценки свидетельствуют, что суммарное время обработки сообщения в узловом комплекте ($t_{зад}^{ТМС} + t_{зад}^{изд.А} + t_{зад}^{изд.Б}$) намного превышает требуемые 2 секунды.

Шлюзы обычно применяются в тех случаях, когда требуется осуществить преобразование нескольких протоколов, используемых в одной сети, в протоколы другой сети путем замены сообщений, в которых сохраняются те же самые семантические конструкции протокола [1, 2]. Исходя из этого, можно констатировать, что для передачи сообщения из одной сети в другую сеть с применением шлюза в заголовок сообщения необходимо включить адрес межсетевого шлюза, который будет использоваться для дальнейшей передачи сообщения через СПД. Отправитель при этом должен посылать сообщение к этому шлюзу. Шлюз принимает переданный пакет, производит извлечение сообщения из принятого пакета, преобразует формат сообщения (адрес, текст и т. д.) в формат сообщения другой сети, и преобразовав полученное сообщение в пакет данных новой сети, производит пересылку получателю.

Алгоритм, описывающий процесс передачи сообщений из одной СПД в другую через шлюз, приведен на рис. 2.

Основным отличаем данного алгоритма является выполнение операций рассекречивания при приеме сообщения и засекречивания при передаче в самом шлюзе (устройстве сопряжения) (блоки 3, 7). Согласование протоколов нижних уровней выполняется не в АПД сопрягаемых сетей, как это реализовано в ТМС, а в самом шлюзе. Исследования показывают, что данное обстоятельство скажется на увеличении временных затрат при обработке сообщения в шлюзе (в отличие от ТМС) и усложнении самого устройства сопряжения. Однако, как показывает прогнозная оценка, общие временные затраты могут уменьшиться, т. к. вполне очевидно, что $t_{зад}^{шл}$ будет меньше ($t_{зад}^{ТМС} + t_{зад}^{изд.А} + t_{зад}^{изд.Б}$).

Учитывая перечень функций, возлагаемых на шлюз, в его составе необходимо иметь преобразователь форматов, полностью идентичный ПФ в ТМС. Преобразователь форматов должен обеспечивать: выполнение основных функций по преобразованию форматов сообщений; согласование способов распределения информации комплекса (изделие А и изделие Б); приоритетное обслуживание сообщений в зависимости от их категории срочности.

Преобразователь форматов необходимо выполнить на базе микропроцессора, включающего в себя: БС1 и БС2 (обеспечивающие

сопряжение ПФ с устройством защиты от ошибок – УЗО1 и УЗО2, соответственно); СВ1 и СВ2 (управляющие работой БС1 и БС2); репрограммируемое запоминающее устройство, служащее для хранения изменяемой в процессе эксплуатации служебной информации; ОЗУ, обеспечивающее хранение информации и промежуточных результатов обработки при совместной работе СВ1 и СВ2. Так же в состав шлюза предлагается включить: УЗО1 и УЗО2 (предназначенные для повышения достоверности принимаемых сообщений за счет использования помехоустойчивого кода, синхронного накопления и подтверждения правильного приема сообщения помехоустойчивой квитанцией); устройства преобразования сигналов УПС1 и УПС2 (служащие для преобразования двоичных сигналов, поступающих из УЗО, в сигналы, необходимые для передачи по каналу, и обратного преобразования, а также осуществляющие тактовую (поэлементную) синхронизацию и анализ качества дискретного канала).

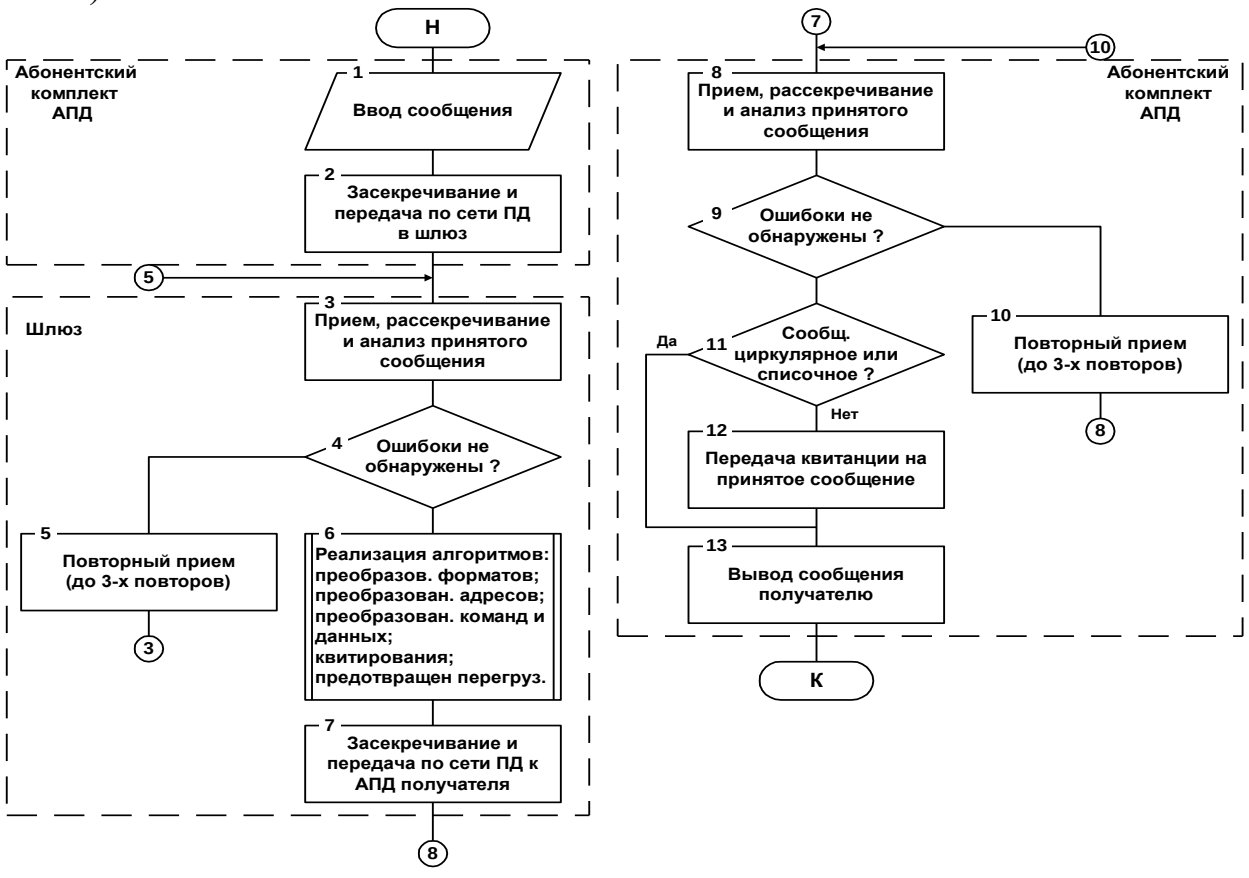


Рис. 2. Обобщенный алгоритм, описывающий процесс передачи сообщений из одной СПД в другую через шлюз

Анализ показывает, что алгоритмы работы данных устройств полностью соответствуют алгоритмам работы УЗО и УПС АПД (изделие А и изделие Б), соответственно, которые достаточно полно описаны в [3, 4].

Известно, что мосты находят применение при сопряжении сетей (сегментов сети), имеющих различные протоколы низкого уровня (физического и канального). Мосты должны обладать свойством быть прозрачными

для протоколов высокого уровня. При передаче данных между двумя СПД они могут не понимать проходящих через них данных, но при этом осуществлять маршрутизацию данных [5-7].

В случае использования межсетевого моста необходимо в составе ООД иметь специальное программное обеспечение (ПО), которое преобразует формат сообщения воздушной сети ПД в формат пакета данных для передачи по сети ПД наземных служб. Сформированный таким образом пакет данных передается через сеть ПД к межсетевому мосту. Мост осуществляет преобразование адресной части и заголовка межсетевой дейтограммы и укорачивает текстовую часть дейтаграммы. В результате этих действий на выходе моста формируется пакет данных формата авиационной СПД, который передается получателю.

Алгоритм, описывающий данный процесс передачи сообщений из СПД наземных служб в СПД авиации, представлен на рис. 3.

Основным отличаем данного алгоритма, от ранее рассмотренных, является реализация в мосту не всех алгоритмов преобразования сообщения, а только алгоритмов преобразования адресной части сообщения. Поэтому, время обработки сообщений в мосту, по сравнению со шлюзом, явно сокращается, из-за уменьшения числа алгоритмов, реализованных в нем. Но основным недостатком применения моста при сопряжении рассматриваемых СПД, является необходимость доработки специального ПО ООД СПД наземных служб.

Сравнительный анализ показывает, что в составе моста можно выделить устройства УПС1 и УПС2; УЗО1 и УЗО2 идентичные по своему назначению и выполняемым ими алгоритмам устройствам, реализованным в шлюзе. Однако преобразователь адресов моста отличается от преобразователя форматов шлюза уменьшенным количеством выполняемых им алгоритмов.

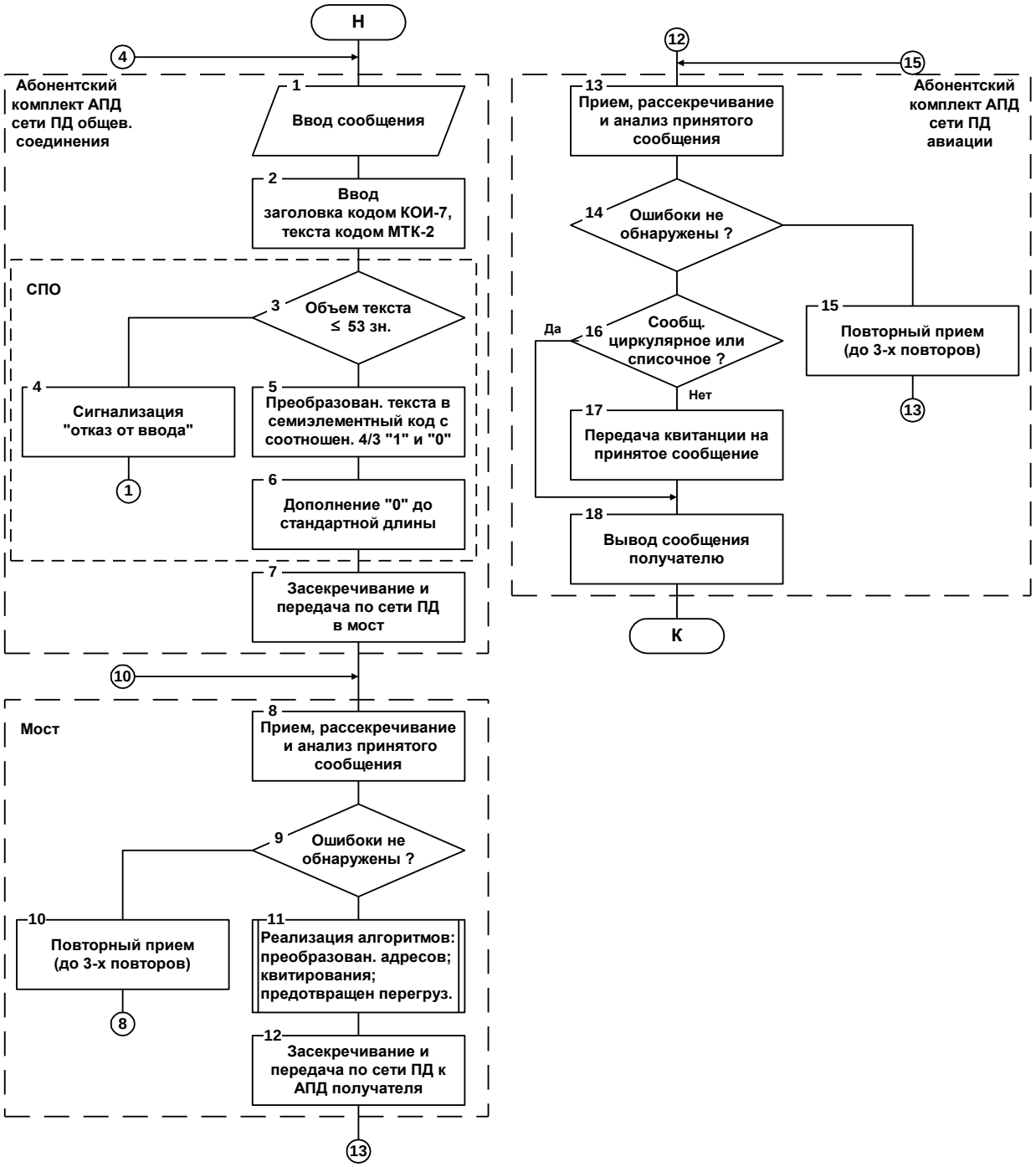


Рис. 3. Обобщенный алгоритм передачи сообщений из СПД наземной службы в сеть авиационную СПД через мост

Отправителем сообщения является абонент воздушной СПД, то в межсетевом мосту осуществляется обратный алгоритм преобразования заголовка и наращивание текстовой части (нулями) до величины необходимой для передачи по СПД. Сформированный таким образом пакет по СПД пересылается получателю, специальное ПО ООД, которого должно позволить правильно интерпретировать полученное сообщение.

Список литературы

1. Плотников Д. А. Разработка и исследование алгоритмов сопряжения сетей передачи данных: Дисс. ... канд. техн. наук. – Новочеркасск, 2022. – 150 с.
2. Кондратенко В. А., Новиков Ю. В. Теоретические основы сетевых протоколов. – СПб.: Реноме, 2005. – 232 с.
3. Кондратенко В. А. Структурированные кабельные системы и сети. – СПб.: Изд-во СПбГЭТУ «ЛЭТИ», 2006. – 158 с.
4. Спивак А. И. Защита информации техническими средствами (учебное пособие). СПб.: Национальный исследовательский университет информационных технологий, механики и оптики. 2021.
5. Спивак А. И. Методика проведения практических мероприятий по расследованию компьютерных инцидентов и анализу защищенности автоматизированных систем в информационно-телекоммуникационных сетях Министерства обороны Российской Федерации (дополнение, внесение изменений, практические рекомендации) Восьмое управление ГШ ВС РФ, г. Москва.
6. Спивак А. И. Модель информационно-телекоммуникационной сети военного назначения // Техника средств связи. 2025. Т. 2. № 2. С. 116-120. Инв. 6995с.
7. Спивак А. И. Методика оценки эксплуатационной надежности узлов связи // Техника средств связи. 2025. Т. 2. № 2. С. 121-127. Инв. 6995с.

УДК 621.39

Методы оценки процесса функционирования сетей передачи данных специального назначения

Спивак А. В.

ПАО «Интелтех», г. Санкт-Петербург, Россия

Аннотация: *в работе рассмотрены методы оценки функционирования сетей передачи данных специального назначения. Представленные исследования показали, что модели в виде уравнений регрессии для вероятности своевременной доставки сообщений могут быть построены с помощью метода наименьших квадратов, одной из предпосылок которого является стохастическая независимость результатов наблюдений. Рассмотрены основные этапы расчета.*

Ключевые слова: *вероятность своевременной доставки сообщений, методы оценки функционирования, сеть передачи данных, устройства сопряжения*.

Одним из ключевых этапов процесса сопряжения сетей передачи данных (СПД) специального назначения (СН) является оценка процесса функционирования сопрягаемых сетей ПД при различных значениях времени обработки сообщений в устройствах сопряжения ($t_{обр}$) и различной их канальности ($d_{шл}$).

Обработка полученных результатов позволила рассчитать зависимости вероятности своевременной доставки сообщений при использовании в СПД устройств сопряжения различной канальности и с разным временем обработки. Их величины в устройствах сопряжения для аппаратуры передачи данных (АПД) изделия А показывает, что требования по вероятности своевременной доставки сообщений выполняются при $T_{обр} \leq 0{,}1$ с и $d_{шл} \geq 4$. При увеличении количества устройств сопряжения в системе до 8 возможно уменьшение их канальности до 2. Зависимость вероятности своевременной доставки сообщений от времени обработки сообщений в устройствах сопряжения и их канальности для изделия Б показывает, что требования по вероятности своевременной доставки сообщений выполняются даже при $T_{обр} \leq 0{,}3$ с, но канальность устройств сопряжения при этом должна быть не менее 4. При увеличении количества устройств сопряжения в системе до 8 возможно выполнение требований по вероятности своевременной доставки сообщений для одноканальных устройств сопряжения, но время обработки сообщений в них не должно превышать 0,15 с.

Для обработки полученной статистики и определения степени влияния каждого из параметров на вероятность своевременной доставки сообщений в работе предложено использовать корреляционно-регрессионный анализ (КРА).

Данный анализ позволяет решать следующие группы задач [1-2]:

– нахождение вида связи между показателем Y и фактором X, т. е. нахождение детерминированной основы статистической связи, а также выбор наилучшего вида связи;

– оценка тесноты связи между показателем и факторами, определение степени влияния изменения фактора на значение показателя, т. е. нахождение случайной составляющей, характеризующей приближение статистической связи к функциональной.

Решением первой группы задач занимается регрессионный анализ. Он позволяет находить аналитическую зависимость на основе обработки полученных статистических данных. Второй группой задач занимается корреляционный анализ. Эти методы анализа весьма тесно связаны между собой, хорошо разработаны математически и достаточно широко освещены в литературе [1-2].

Анализ работ по исследованию СПД [3-5] показал, что наиболее распространенными формами регрессионных зависимостей вероятности своевременной доставки ($P_{\text{с.д.}}$) от параметров (x_i) СПД являются:

$$C(x) = a_0 + \sum_{i=1}^{m} a_i x_i , \qquad (1)$$

$$C(x) = a_0 \prod_{i=1}^{m} f_k(x_i), \quad f_k(x_i) = \left\{ x_i^{a_i},\ a_i^{x_i},\ e^{a_i x_i} \right\}, \qquad (2)$$

где a_0, a_1, ..., a_m – коэффициенты модели.

Параметры, включаемые в модель исследования результатов моделирования СПД, должны быть информативными и удовлетворять требованиям [5]: оказывать наиболее существенное, по сравнению с другими параметрами, влияние на вероятность своевременной доставки; быть независимыми друг от друга.

Проведенные исследования показали, что модели в виде уравнений регрессии для вероятности своевременной доставки могут быть построены с помощью метода наименьших квадратов (МНК), одной из предпосылок которого является стохастическая независимость результатов наблюдений. Характерным моментом при построении регрессионных зависимостей является оценка значимости статистических характеристик модели и проверка ее адекватности. Поэтому коротко остановимся только на предлагаемых этапах расчета [6].

1. Этап анализа значимости параметров для соответствующих выборок.

2. По извлеченным параметрам рассчитываются коэффициенты парной корреляции [7] при всевозможных сочетаниях

$$\hat{r}_{yx} = \frac{N \cdot \sum_{j=1}^{N} x_i y_j - \sum_{j=1}^{N} x_i \sum_{j=1}^{N} y_j}{\sqrt{\left[N \cdot \sum_{j=1}^{N} x_j^2 - \left(\sum_{j=1}^{N} x_j\right)^2\right]\left[N \cdot \sum_{j=1}^{N} y_j^2 - \left(\sum_{j=1}^{N} y_j\right)^2\right]}}, \quad (3)$$

и коэффициенты частной корреляции первого порядка

$$\hat{r}_{y1.2} = \frac{r_{y1} - r_{y2} r_{12}}{\sqrt{\left(1 - r_{y2}^2\right)\left(1 - r_{12}^2\right)}}, \quad (4)$$

второго порядка

$$\hat{r}_{y1.2.3} = \frac{r_{y1.3} - r_{y2.3} r_{12.3}}{\sqrt{\left(1 - r_{y2.3}^2\right)\left(1 - r_{12.3}^2\right)}}, \quad (5)$$

k-го порядка

$$\hat{r}_{y1.2..k} = \frac{r_{y1.3..k} - r_{y2.3..k} r_{12.3...k}}{\sqrt{\left(1 - r_{y2.3..k}^2\right)\left(1 - r_{12.3...k}^2\right)}}. \quad (6)$$

Индексом при $\hat{r}$ обозначены условные номера наблюдаемых параметров.

3. С помощью критерия Стьюдента производится оценка значимости выборочных коэффициентов парной и частной корреляции при числе степени свободы ν и соответствующем уровне значимости α по известным выражениям для коэффициента парной корреляции

$$t\left(\alpha, \nu = N - 2\right) = \left(0{,}5 \ln \frac{1 + \hat{r}_{xy}}{1 - \hat{r}_{xy}}\right) \cdot \sqrt{N - 3}, \quad (7)$$

для коэффициента частной корреляции

$$t\left(\alpha, \nu = N - k - 2\right) = \hat{r}_{y1.2..k} \sqrt{\left(N - k - 2\right) / \left(1 - \hat{r}_{y1.2..k}^2\right)}, \quad (8)$$

где *k*-число параметров, одновременное действие которых исключается.

4. Осуществляется проверка выполнения требования независимости параметров по величине выборочного значения коэффициента парной корреляции вида (6). С этой целью предложен алгоритм, в результате работы которого последовательно вычеркиваются строки и столбцы корреляционной матрицы, на пересечении которых находится элемент $\hat{r}_{xy} > 0{,}9$. В итоге получается матрица, содержащая взаимно независимые параметры.

Достоинством данного алгоритма является простота реализации. Недостатками метода являются его применимость только для задач с большими объемами выборок и неопределенность (субъективность) выбора порогового значения ($\hat{r}_{xy} = 0{,}9$) степени тесноты линейной связи между параметрами.

Например, в [8] пороговое значение выбирается равным $\hat{r}_{xy} = 0{,}8$, а в [7] – $\hat{r}_{xy} = 0{,}7$

В этих условиях для определения независимых параметров значительный интерес представляет применение асимптотики Колмогорова-Деева в сочетании с построением графа структуры зависимостей в виде дерева наибольшего веса. Суть данного подхода подробно изложена в [1-2].

5. По критерию Фишера проверяется адекватность сформированных моделей при n_1=N – 1 и n_2=N – m – 1 степенях свободы:

$$F = \frac{\frac{1}{N-1}\sum_{j=1}^{N}(y_i - \bar{y})^2}{\frac{1}{N-m-1}\sum_{j=1}^{N}(y_j - \hat{y}_j)^2}, \qquad (9)$$

где y_j – значение зависимой переменной, определенное по уравнению регрессии; m – число параметров модели.

Абсолютная ошибка модели $\left|P_j^{\phi} - P_j^{p}\right|$ применена для проверки методического подхода к оценке вероятности и выбора наилучшей модели по критерию:

$$\bar{\varepsilon} = \min_j \frac{1}{N}\sum_{j=1}^{N}\frac{\left|P_j^{\phi} - P_j^{p}\right|}{C_j^{™}} \cdot 100\% \ , \qquad (10)$$

где P_j^{ϕ}, P_j^{p} — фактическое и расчетное значение j-й вероятности своевременной доставки соответственно; N — количество параметров. При этом интерпретация точности моделей по величине абсолютной ошибки приведена в табл. 1.

Таблица 1 – Интерпретация точности моделей

Точность $\bar{\varepsilon}$, %	Интерпретация
10	Высокая точность
10 ÷ 20	Хорошая точность
20 ÷ 50	Удовлетворительная точность
50	Неудовлетворительная точность

С целью выбора оптимальной по критерию регрессионной модели вероятности своевременной доставки, построенной на основе описанных выше процедур, были проведены исследования различных моделей при различных объемах выборки с помощью пакета прикладных программ STATGRAPHICS *Plus* for Windows. Проведенные исследования позволил отдать предпочтение модели линейной регрессии, имеющей следующий вид

$$P_{сд} = 0{,}0592454 + 0{,}0133699d - 0{,}120512N_{цк} + 0{,}000132741R - 0{,}463274\lambda - 0{,}0122533S + \\ + 0{,}00442951N_{ла} - 0{,}439518P_{под} + 0{,}0374145d_{шл} - 0{,}712201t_{обр} + 0{,}401979\mu.$$

Регрессионная модель имеет хорошую точность (ε=10-20% по табл. 1) и отражает на 90,6 % изменчивость $P_{сд}$.

Исследование регрессионных моделей времени обработки в устройстве сопряжения ($t_{обр}$), при выполнении условия $P_{сд} \geq 0{,}95$ позволило отдать предпочтение модели линейной регрессии, имеющей следующий вид

$$t_{обр} = -0{,}140291 + 0{,}00810436d - 0{,}0250826N_{цк} + 0{,}00000575699R - 0{,}126249\lambda - \\ - 0{,}0173387S + 0{,}0000566729N_{ла} - 0{,}427865P_{под} + 0{,}0375219d_{шл} + 0{,}112466\mu.$$

при $P_{сд} \geq 0{,}95$.

Регрессионная модель также имеет хорошую точность (ε=10-20% по табл. 1) и отражает на 87,6% изменчивость $P_{сд}$.

Таким образом, проведенные исследования позволили разработать модели пригодные по своей точности для практического использования при сопряжении сетей ПД наземных служб и авиации. Использование полученных моделей позволило получить аналитическую зависимость количества устройств сопряжения от их канальности и времени обработки (табл. 2).

Таблица 2 – Требования к устройствам сопряжения

Тип АПД	Требуемое количество устройств сопряжения, шт (не менее)	Требуемая канальность устройств сопряжения, кан. (не менее)	Требуемые временные затраты на обработку сообщения 800 бит. млс. (не более)
Изделие А	4	4	100
	4	3	50
	8	2	100
	8	1	50
Изделие Б	4	1	100
	4	2	200
	4	3	250
	4	4	300

Тип АПД	Требуемое количество устройств сопряжения, шт (не менее)	Требуемая канальность устройств сопряжения, кан. (не менее)	Требуемые временные затраты на обработку сообщения 800 бит. млс. (не более)
	8	1	150
	8	2	250
	8	3	300

Полученные значения временных затрат, по предлагаемым моделям, являются исходными данными для разработки алгоритмов сопряжения.

Список литературы

1. Олифер В. Г., Олифер Н. А. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. – СПб.: Питер, 2021. – 816 с.

2. Таненбаум Э., Уэзеролл Д. Компьютерные сети. – СПб.: Питер, 2022. – 960 с.

3. Кондратенко В. А., Кучерявый Е. В. Технология SD-WAN: модели, алгоритмы и программное обеспечение для межсетевого взаимодействия. – СПб.: Изд-во СПбГЭТУ «ЛЭТИ», 2020. – 160 с.

4. Кондратенко В. А., Кучерявый Е. В. Интернет вещей: модели и алгоритмы. – СПб.: Изд-во СПбГЭТУ «ЛЭТИ», 2019. – 160 с.

5. Коваль А. В., Лыткин Ф. Ю. Предложения по методам сопряжения гетерогенных сетей связи специального назначения и их оценка // КиберЛенинка. 2022. № 4.

6. Аганесов А. В. Модель сети спутниковой связи на основе протокола случайного множественного доступа S-Aloha // Системы управления, связи и безопасности. 2015. № 2. С. 99–134.

7. Спивак А. И. Методика формирование структуры системы связи с центрами обработки данных. XXII Российская межведомственная научно-техническая конференция «Новые информационные технологии в системах связи и управления». Калуга. КНИИТМУ. 2023. С. 98-99.

8. Спивак А. И. Методика распределение потоков, расчет пропускных способностей элементов сети. XXII Российская межведомственная научно-техническая конференция «Новые информационные технологии в системах связи и управления». Калуга. КНИИТМУ. 2023. С. 125-129.

.

Секция 2 – Робототехника и искусственный интеллект

УДК 621.61

Наращивание оперативности доведения команд управления до беспилотного транспорта за счет формирования сигнально-кодовых конструкций по технологиям расширения спектра

Будко Д. Д.

Государственный университет морского и речного флота имени адмирала С.О. Макарова, г. Санкт-Петербург, Россия

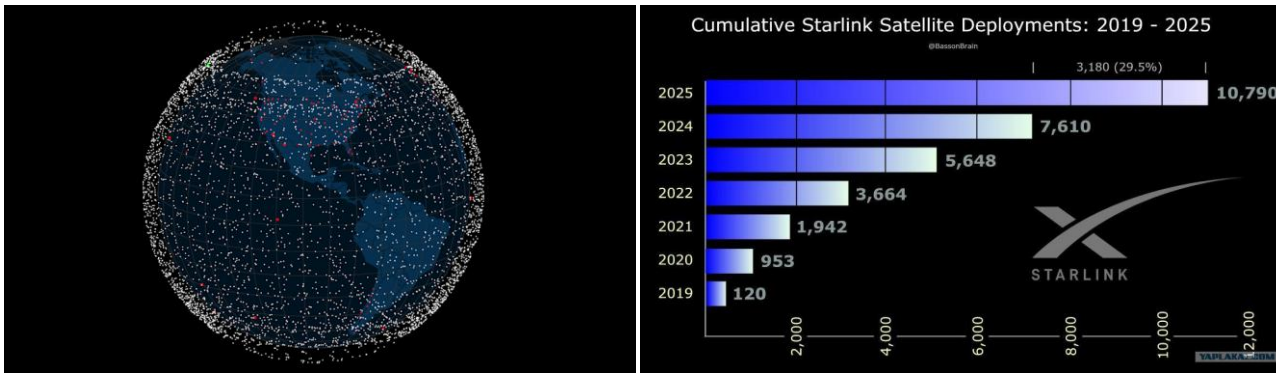
Аннотация: *В работе предложены варианты формирования сигнально-кодовых конструкций команд управления беспилотными транспортными системами с использованием различных технологий расширения спектра. Для перехода к управлению глобально перемещающимися объектами транспортной инфраструктуры в режиме реального времени применяются многочастотные сигналы с назначением рабочих частот по псевдослучайному закону. Повышение оперативности доведения команды управления до высокоскоростных транспортных систем достигается за счет параллельной их трансляции за время передачи одного информационного бита.*

Ключевые слова: *беспилотная транспортная система, многочастотный сигнал, режим реального времени, сигнально-кодовая конструкция, технология расширения спектра.*

Введение

Робототехнические комплексы (РТК) и беспилотные транспортные системы (БТС) наземного, морского, воздушного и космического базирования на сегодня все шире внедряются в повседневную жизнь человечества, рис. 1, 2. На автомагистрали России к 2035 планируется вывести более 57 тыс. беспилотных грузовиков. С 2026 года в Москве начата эксплуатация беспилотных метропоездов. В Дальневосточном федеральном округе полным ходом идет подготовка инфраструктуры под трансграничный переход «Приморье-2» для международных с Китаем беспилотных наземных и воздушных грузоперевозок [1, 2].

Рис. 1. Наземные, воздушные и морские беспилотные транспортные системы



а) *б*)

Рис. 2. Взрывной рост числа спутников связи (по данным компании Starlink)

Беспилотные технологии в совокупности с широким внедрением цифровых платформ и технологий искусственного интеллекта (ТИИ) позволяют уже сегодня получать синергетический эффект, востребованный для БТС и безэкипажных судов, при исследованиях агрессивных сред Арктики и глубин мирового океана, в овладении гиперзвуком для изучения Луны и дальнего Космоса.

Наиболее приемлемыми для связи с глобально перемещающимися БТС несомненно являются каналы спутниковой связи. Однако в приполярных районах, на которых в настоящее время самым активным образом идет освоение и развитие Северного морского пути, космической группировки ретрансляторов явно недостаточно, что видно из рис. 2 *а*). Это касается не только группировки Starlink, но и отечественной низкоорбитальной спутниковой системы «Гонец».

В данном случае универсальным выбором диапазона частот и применяемых беспроводных технологий является диапазон декаметровых волн (ДКМВ), способный обеспечить «прямую» связь с автономными БТС как в самых труднодоступных регионах России, так и на дальностях свыше 12 тыс. км в разных районах мирового океана. При этом средства ДКМВ-связи имеют достаточно низкую стоимость и малые массогабаритные показатели, что является их существенным преимуществом в обосновании применимости на борту БТС [3].

Между тем каналы ДКМВ-связи вполне обоснованно относят к каналам низкого качества из-за высокого коэффициента ошибок и быстрых изменений параметров среды распространения радиоволн – ионосферы, вызывающих эффект «многолучёвости» и мультипликативные «замирания» сигнала. Помимо этого, и что самое главное, ДКМВ диапазон отмечается достаточно высокой загрузкой радиочастотного спектра за счет функционирования многих других радиостанций, рассматриваемых сосредоточенными по спектру помехами, особенно вблизи области оптимальных рабочих частот (ОРЧ), рис. 3. Все это влияет на снижение вероятности приёма команд управления (КУ) бортовым комплексом связи БТС в автоматическом режиме и требует б*о*льших повторов, понижая оперативность.

Цель статьи: выбор вариантов построения сигнально-кодовых конструкций, обеспечивающих оперативность доведения команд управления до БТС вплоть до перехода к доведению одномоментно, в режиме реального времени.

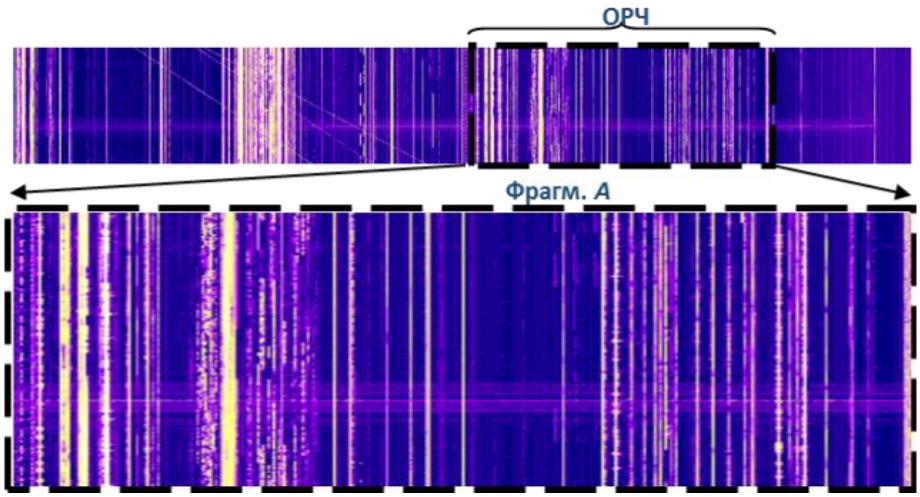


Рис. 3. Участок ОРЧ во фрагменте спектрограммы заданной ДКМВ радиотрассы

Переход от традиционных технологий доведения команд управления к сигнально-кодовым конструкциям на основе расширения спектра

Исторически, при появлении систем дистанционного управления мобильными объектами на глобальных расстояниях, использовались сигнально-кодовые конструкции (СКК) на основе азбуки Морзе [3]. Запатентованный в 1849 году и активно используемый с началом первой мировой войны данный способ широко применялся для связи с морскими и воздушными судами, при освоении Космоса и на поле боя. Однако СКК на базе кода Морзе обладает низкой оперативностью, поскольку ориентирована да «ручной» режим работы радиотелеграфиста. Радиосигнал доводится с помощью коротких («точек») и длинных («тире») бинарных посылок. За основу длительности знаков КУ в такой СКК принята длина «точки», $T_{\text{тчк}}$ = 70 мс. Соответственно длина одного «тире» в три раза больше, $T_{\text{тире}}$ = 210 мс. Межзнаковый интервал между тире и точками внутри передаваемых знаков сообщения (КУ) также равна $T_{\text{мз}}$ = 70 мс. Межгрупповой интервал между знаками внутри транслируемого слова равен одному «тире» (или трем «точкам»), $T_{\text{мг}}$ = 210 мс, [3]. Указанная величина оперативности
в передаче КУ относительна, в связи с тем, что в коде Морзе используется не фиксированное число элементов. Так, при передаче более часто употребляемой в русском языке буквы «Е» применяют всего одну «точку», а для «Й»: «точка–тире–тире–точка» и т. д. Но все-таки в большей степени на оперативность доведения КУ сигналами на базе кода Морзе влияет классность радиста.

Существенного увеличения оперативности доведения КУ до БТС возможно достичь путем перехода от «ручных» способов с традиционными СКК на базе кода Морзе к автоматической трансляции, использующей более перспективные СКК на основе применения технологий расширения спектра. К таким технологиям можно отнести линейные частотно-модулированные сигналы (ЛЧМ), CSS (Chirp Spread Spectrum) [4-7]. Причем ЛЧМ-сигналы информационной единицы «1» и информационного нуля «0» могут соответствовать «точке» и «тире» азбуки Морзе, из которых формируются бинарные посылки по процедурам линейного убывания и линейного возрастания закона изменения частоты, как показано на частотно-временной характеристике (ЧВХ) рис. 4 *а-г*)

$$S^{"0"}_{\text{ЛЧМ}}(t) = S_0\cos\{\varphi_0 + \varphi(t)\} = S_0\cos\{\varphi_0 + 2\pi[f_0 t + (b/2)t^2]\}, \quad (1)$$

$$S^{"1"}_{\text{ЛЧМ}}(t) = S_0\cos\{\varphi_0 - \varphi(t)\} = S_0\cos\{\varphi_0 - 2\pi[f_0 t + (b/2)t^2]\}, \quad (2)$$

где S_0 , φ_0 и f_0 – соответственно, амплитуда, начальная фаза и центральное значение несущей частоты транслируемого ЛЧМ-сигнала, рассчитываемое как среднее от суммы ее минимального $f_{\min}$ и максимального зйачения $f_{\max}$

$$f_0 = (f_{\max} + f_{\min})/2, \quad (3)$$

b – коэффициент учета скорости изменения частоты ЛЧМ-сигнала во времени t

$$T_c\, b = (f_{\max} - f_{\min})/T_c, \quad (4)$$

T_c – длительность бинарной посылки («0» или «1») ЛЧМ-сигнала, причем

$$T_c = T_c^{"0"} = T_c^{"1"} . \quad (5)$$

Таким образом, частоту бинарной посылки $f(t)$ меняют линейно по закону

$$f(t) = f_0 + b \cdot t, \quad (6)$$

$$-T_c/2 < t < T_c/2. \quad (7)$$

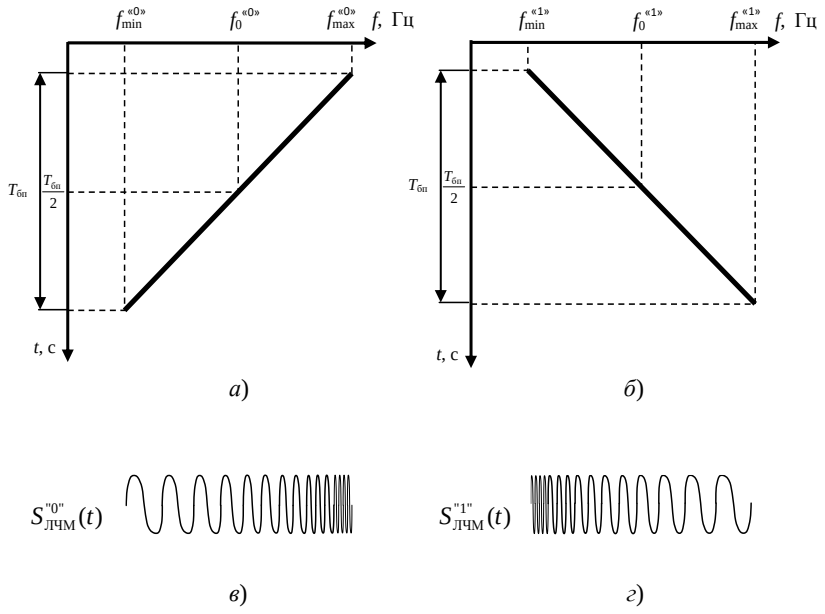


Рис. 4. ЧВХ ЛЧМ-сигналов с расширением спектра сформированных:
а) по технологии CSS с линейно возрастающим изменением частоты *в*);
б) по технологии CSS с линейно убывающим изменением частоты *г*)

Расчет оперативности доведения команд управления при переходе к перспективным СКК на основе технологии расширения спектра

На рис. 5 показан выигрыш в оперативности доведения КУ, представленных кодом Морзе и на базе применения технологии расширения спектра CSS.

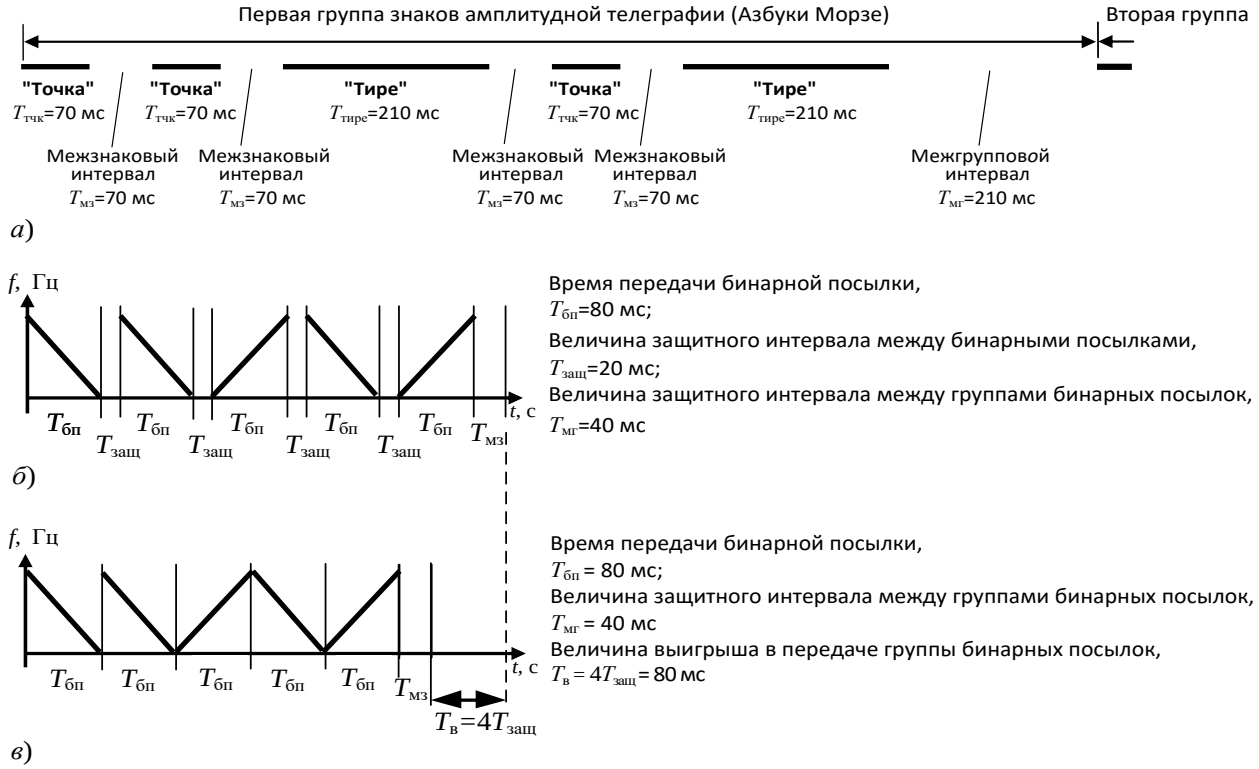
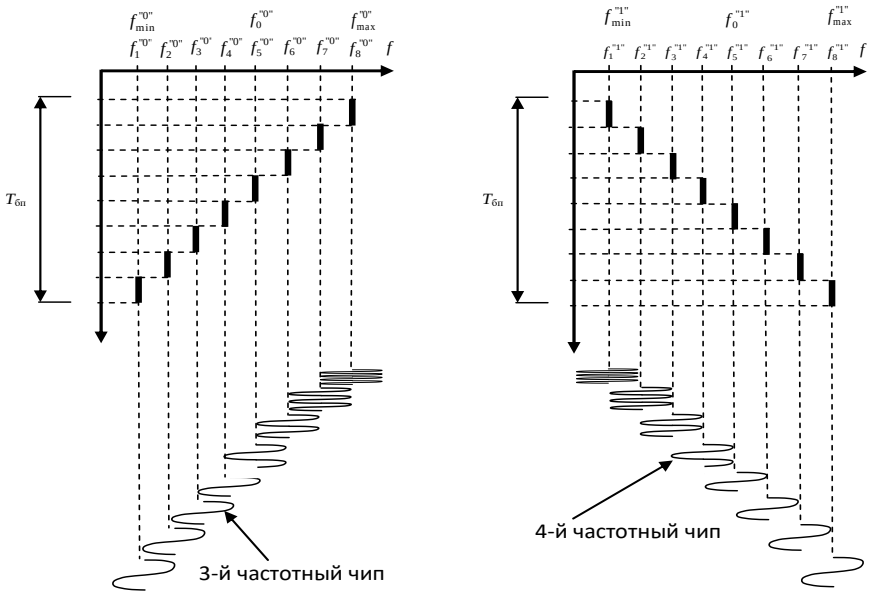


Рис. 5. Расчет выигрыша в оперативности СКК на основе: *а*) кода Морзе; *б*) ЛЧМ-сигналов с защитным интервалом бинарных посылок; *в*) и без него

Из рис. 5 *а*) видно, что для передачи пятиэлементной буквы в коде Морзе потребуется более 1 с (1040 мс). В тоже время, при замене «точек» и «тире» азбуки Морзе бинарными посылками одинаковой длины $T_{бп}$ = 80 мс на основе ЛЧМ-сигналов с защитным интервалом $T_{защ}$ = 20 мс, рис. 5 *б*) и *в*), наблюдается выигрыш в оперативности. Так, использование СКК на базе ЛЧМ-сигналов с длительностью бинарных посылок $T_{бп}$ и защитным интервалом уменьшится до 440 мс, рис. 5 *б*), т. е. более чем в два раза. При полном отказе от защитного интервала в СКК на базе CSS технологии, рис. 5 *в*), выигрыш составит 2,34 раза.

В работе автора [8] представленный выше способ доведения КУ до БТС усовершенствован, когда вместо технологии CSS используется технология DSSS (Direct Sequence Spread Spectrum) с расширением спектра прямой последовательностью (ПРС). При этом бинарные посылки КУ («1» или «0») разбиваются на n частотных чипов, каждый i-й из которых ($i = \overline{1,n}$) передается дискретно, рис. 6 *а*), *б*), в виде узкополосных сигналов. Причем передачу каждого i-го частотного чипа можно осуществлять на частотах некоторой

псевдослучайной последовательности (ПСП), известной только для заданного БТС.



а) *б*)

Рис. 6. Частотно-временные характеристики сигналов с расширением спектра: *а*) по технологии DSSS с дискретным возрастанием частот последующих чипов; *б*) по технологии DSSS с дискретным уменьшением частот последующих чипов

Существенным отличием СКК с технологией DSSS от СКК с режимом трансляции на рабочих частотах, изменяющихся по псевдослучайному закону (ППРЧ) FHSS (Frequency-Hopping Spread Spectrum) [9, 10] является факт, что DSSS-сигнал занимает ограниченную полосу частот $\Delta f = f_{max} - f_{min}$, а сигналы ППРЧ охватывают диапазон частот глобально. При этом СКК на базе DSSS-технологии, рис. 6, имеют такой же выигрыш в оперативности доведения КУ до БТС, как и в случае с ЛЧМ-сигналами, рис. 4. Однако обе эти технологии позволяют нарастить потенциальные возможности в оперативности доведения за счет параллельной трансляции бит в одном знаке КУ, вместо последовательной.

Наращивание оперативности доведения команд управления до БТС при параллельной передаче элементов сигнально-кодовых конструкций

Дальнейшее наращивание оперативности доведения КУ до БТС возможно путем передачи бинарных посылок их знаков в параллельном режиме, рис 7.

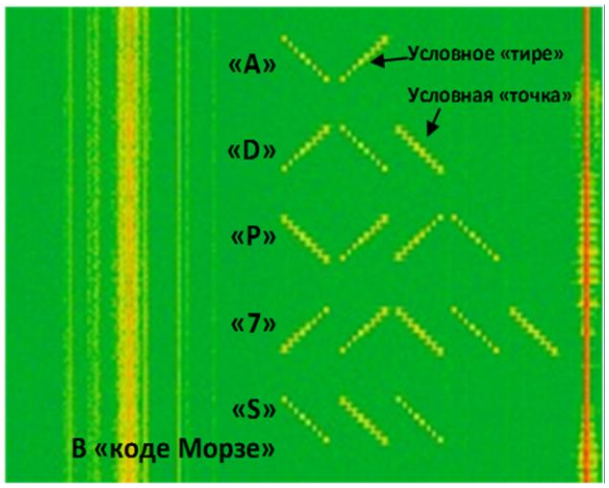


Рис. 7. Фрагмент спектрограммы варианта использования СКК, построенной по технологии DSSS (CSS) при ее параллельной передаче/приеме познаково

Такой режим передачи предпочтительнее в связи с наращиванием оперативности доведения. К примеру, знак КУ, состоящий из пяти бит (код МТК-2) при трансляции бит в параллельном режиме будет передан в пять раз быстрее, чем при последовательной передаче. Для кода МТК-2 выигрыш в оперативности доведения КУ до БТС составит пять раз, для кода KOI-8 – восемь раз.

Дальнейшее наращивание оперативности при доведении КУ до БТС возможно при использовании трансляции всех информационных бит (элементов КУ) в режиме ППРЧ (FHSS), но не с последовательной передачей, рис. 8, а параллельной их трансляции, рис. 9, с использованием многочастотного сигнала.

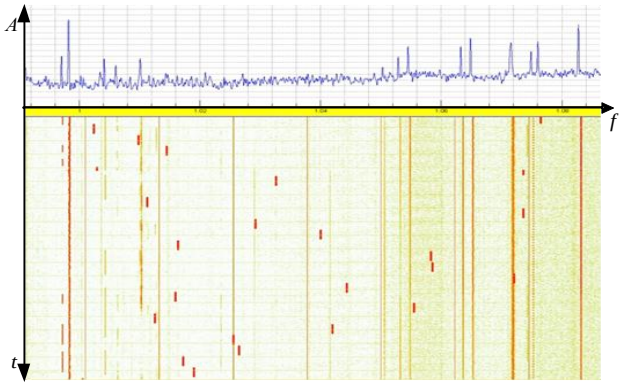


Рис. 8. Фрагмент спектрограммы последовательной трансляции многочастотной СКК в режиме ППРЧ

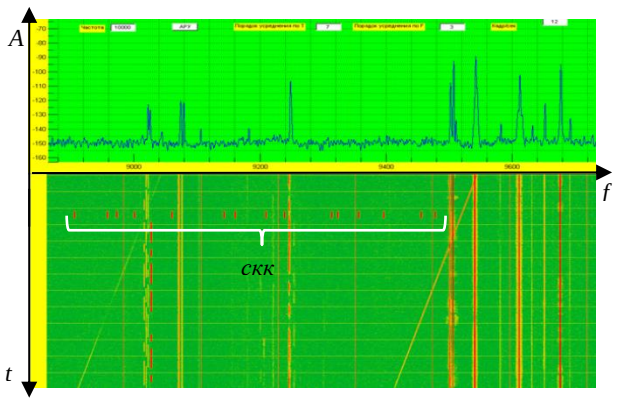


Рис. 9. Фрагмент спектрограммы параллельной трансляции многочастотной СКК в режиме ППРЧ

Величина выигрыша в оперативности доведения КУ до БТС при параллельной трансляции информационных бит будет кратна их числу, т. е. за время трансляции одного бита передается вся КУ (режим реального времени). Причем каждый элемент сообщения передается на своей частоте, определяемой в соответствии с ПСП и известной только абонентам командной радиолинии.

За повышение оперативности в данном случае приходится «платить» значительным увеличением задействованного частотного ресурса [11]. В сравнение с такими командными радиолиниями как С2/С3 (для беспилотных авиационных систем [12]), в предложенном способе необходимое число рабочих частот будет соответствовать числу информационных бит в фиксированной КУ.

Реализация данного способа управления БТС требует с одной стороны перехода от лицензионного использования РЧС к его задействованию на вторичной основе: свободные полосы частот занимают под передачу многочастотного сигнала в промежутки времени, когда они свободны от работы первичных пользователей – лицензиатов. Решение этой задачи приведено в [13] на основе технологий когнитивных радиосистем (CRS) и программируемого радио (SDR).

С другой стороны, необходима разработка формирователя таких многочастотных сигналов. Не вдаваясь в описание схемной реализации, на рис 10 предложен запатентованный автором [14] подход к построению формирователя многочастотных сигналов на основе сумматора кодов частот, процедур вторичного использования РЧС, а также современных успехов SDR и CRS технологий.

Выводы

Исходя из рассмотренных в ходе исследования способов формирования СКК КУ с различными режимами передачи, оценку кумуляции выигрыша в оперативности их доведения до БТС можно показать в виде таблицы 1.

Таблица 1 – Оценка наращивания оперативности доведении команд управления до БТС при использовании СКК в различных режимах передачи

№ пп	Используемая СКК для доведения 5-элементной команды управления	Оценка оперативности	Достигаемый выигрыш
1.	СКК на основе кода азбуки Морзе для знака с 5 элементами (точки/тире)	1040 мс	рис. 5 *а*)
2.	СКК на основе ЛЧМ-сигналов, для МТК-2 с защитным интервалом	520 мс	в 2 раза, рис. 5 *б*)
3.	СКК на основе ЛЧМ-сигналов, для МТК-2 без защитного интервала	440 мс	в 2,34 раза, рис. 5 *в*)
4.	СКК на основе ЛЧМ-сигналов с параллельной передачей знаков управления в коде МТК-2	80 мс для одного знака (буквы) команды управления	в 13 раз, рис. 7
5.	СКК на основе технологии ПРС, для МТК-2 с защитным интервалом	520 мс	в 2 раза, аналогично рис. 2 *б*)
6.	СКК на основе технологии ПРС, для МТК-2 без защитного интервала	440 мс	в 2,34 раза, аналогично рис. 2 *в*)
7.	СКК на основе технологии ПРС, режим ППРЧ с параллельной побитной передачей одновременно всей команды управления	80 мс для всей команды управления, состоящей из *n* бит	кратно *n*, (обеспечение режима реального времени), рис. 9

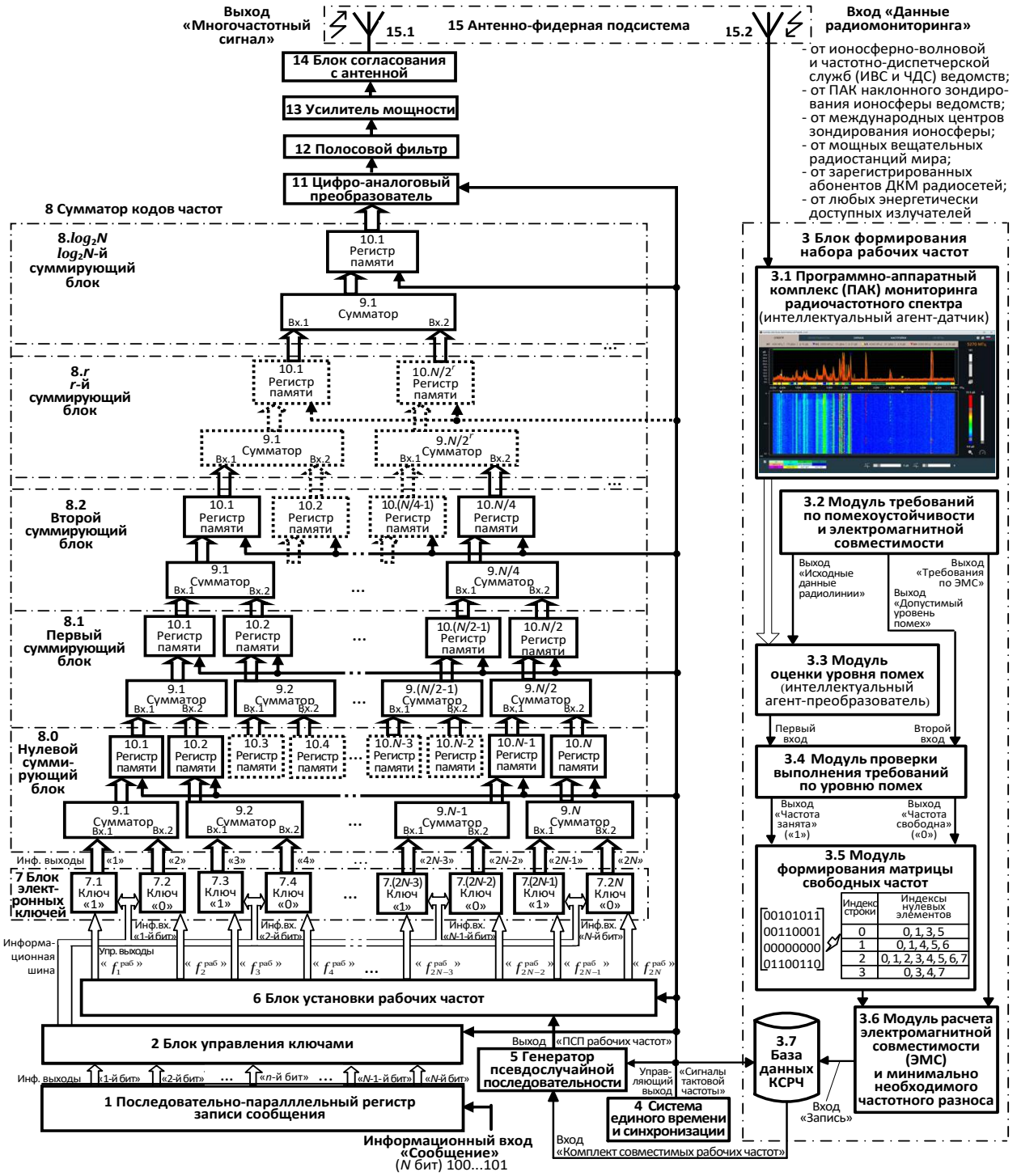


Рис. 10. Схемная реализация формирователя многочастотных сигналов

Таким образом, в работе представлен кумулятивный эффект повышения оперативности в доведении КУ до БТС за счет управления сигнальным ресурсом командной радиолинии [3, 5, 11] с переходом от традиционных СКК к технологиям расширения спектра на основе CSS, DSSS и FHSS.

Новизна предложенного способа повышения оперативности в доведении КУ до БТС состоит в применении псевдослучайного набора рабочих частот, транслируемого в многочастотном режиме, когда вся команда доводится до глобально перемещаемого транспортного средства за время излучения

информационного бита, фактически в режиме реального времени. Это крайне важно для оперативного предотвращения аварийных режимов их функционирования на маршрутах движения и обеспечения управляемости автономным транспортным средством.

Представленный в таблице 1 анализ оценки оперативности сформированных СКК позволяет сделать вывод, что заявленная цель статьи по переходу к режиму реального времени в доведении команд управления до БТС достигнута. При этом использование многочастотного сигнала позволяет транслировать всю команда управления одномоментно за время передачи одного информационного бита, что востребовано при работе с современными высокоскоростными БТС различных типов базирования.

Предложенный в исследовании и технически реализованный в [14] подход к синтезу многочастотных сигнально-кодовых конструкций стал возможным опираясь на современные успехи в развитии когнитивных радиосистем (CRS), технологий программируемых SDR-радиоустройств и цифровой обработки сигналов. Динамическое перераспределение информационных бит команд управления по свободным от первичных пользователей участкам радиочастотного спектра, рис. 3, обеспечивает интеграцию каналов управления БТС в уже распределенный диапазон частот на вторичной основе без создания взаимных помех, обеспечивая дополнительно электромагнитную совместимость бортовых комплексов связи при групповом выполнении миссии.

Представленная реализация процесса формирования СКК команд управления в командных радиолиниях БТС возможна к осуществлению как в режиме частотной телеграфии, так и в режиме амплитудной телеграфии.

Список литературы

1. 1. В России активно развиваются беспилотные технологии в сфере транспорта. [Электронный ресурс]. 2026. – URL: https://mintrans.gov.ru/press-center/news/12387 (дата обращения: 14.05.2026).

2. 2. Материалы совместного совещания В. В. Путина и Правительства РФ по вопросам развития автономных систем (Москва. Электродепо «Аминьевское», Московский метрополитен, 16.01.2026) [Электронный ресурс]. 2026. – URL: http://www.ktemlin.ru/events/president/transcripts/79016 (дата обращения: 14.05.2026).

3. 3. Инфокоммуникационные сети: энциклопедия. Кн. 4: Гетерогенные сети связи: принципы построения, методы синтеза, эффективность, цена, качество / П. А. Будко, И. А. Кулешов, В. И. Курносов, В. И. Мирошников; Под ред. профессора В. И Мирошникова. – М.: Наука, 2020. – 683 с.

4. 4. Борисов В. И., Зинчук В. М., Лимарев А. Е. Помехозащищенность систем радиосвязи с расширением спектра сигналов методом псевдослучайной перестройки рабочей частоты // под ред. В. И. Борисова. М.: РадиоСофт, 2008. – 512 с.

5. 5. Будко П. А., Федоренко В. В. Управление в сетях связи. Математические модели и методы оптимизации: Монография. – М.: Издательство физико-математической литературы, 2003. – 228 с.

6. 6. Макаренко С. И., Иванов М. С., Попов С. А. Помехозащищенность систем связи с псевдослучайной перестройкой рабочей частоты. Монография. – СПб. Свое издательство, 2013. – 166 с. ISBN 978-5-4386-0166-1.

7. 7. Будко Н. П., Будко П. А., Жолдасов Е. С., Жолдасова А. Е., Жуков Г. А., Кулешов И. А., Мальцев Д. С., Мирошников В. И., Николашин Ю. Л., Фатюхин И. Н. Способ передачи и приема бинарной информации по каналам радиосвязи в неавтоматическом режиме (Варианты) // Патент RU № 2605045 от 20.12.2016, бюл. № 35. 31 с.

8. 8. Будко Д. Д., Будко П. А., Зацепин Т. А., Клименко А. Д. Метод управления беспилотными транспортными системами на основе помехоустойчивых сигнально-кодовых конструкций в условиях сосредоточенных и шумовых помех // Системы управления, связи и безопасности. 2025. № 4. С. 143-178. DOI: 10.24412/2410-9916-2025-4-143-178.

9. 9. Борисов В. И., Зинчук В. М., Лимарев А. Е. Помехозащищенность систем радиосвязи с расширением спектра сигналов методом псевдослучайной перестройки рабочей частоты // под ред. В. И. Борисова. М.: РадиоСофт, 2008. – 512 с.

10. 10. Будко Д. Д. Обеспечение устойчивого доведения команд управления до беспилотных транспортных систем за счет комплексного использования радиочастотного спектра // Техника средств связи. 2026. № 1 (173). С. 95-99. DOI: 10.24412/2782-2141-2026-1-95-99.

11. 11. Будко П. А. Управление ресурсами информационно-телекоммуникационных систем. Методы оптимизации: Монография. – СПб.: ВАС, 2012. – 512 с.

12. 12. Руководство по дистанционно пилотируемым авиационным системам. [Электронный ресурс]. 2015. – URL: https://аэростандарт.рф/ru/icao/bundle/679 (дата обращения 17.07.2026).

13. 13. Будко Д. Д., Каретников В. В. Модель формирования многочастотных сигналов команд управления беспилотных транспортных систем в условиях помех // Системы управления, связи и безопасности. 2026. № 1. С. 182-218. DOI: 10.24412/2410-9916-2026-1-182-218.

14. 14. Будко Д. Д., Будко Н. П. Буцанец А. А., Груздев А. А., Каретников В. В., Клименко А. Д., Рыжкова Д. Н. Устройство формирования многочастотных сигналов // Патент на изобретение RU 2864855 C1, опубл. 30.06.2026, бюл. № 19. – URL: https://www1.fips.ru/registers-doc-view/fips_servlet?DB=Rupat&DocNumber=2864855 (дата обращения 18.07.2026).

УДК 004.93

Обзор методов компьютерного зрения

Голоскок Д. С.

ПАО «Интелтех», г. Санкт-Петербург, Россия

Аннотация: *В статье рассматривается компьютерное зрение, приводится его классификация по различным признакам. Анализируются современные подходы к решению задач компьютерного зрения — математические и основанные на нейронных сетях. Особое внимание уделяется нейронным сетям, работающим в реальном времени, а также специфике функционирования некоторых из них.*

Ключевые слова: *компьютерное зрение, нейронные сети, искусственный интеллект, детектирование, системы реального времени.*

Введение

Компьютерное зрение представляет собой научную область, предметом которой является исследование и разработка методов автоматической фиксации, обработки и анализа изображений с использованием вычислительных средств. Под обработкой понимаются такие задачи, как обнаружение, отслеживание и идентификация объектов. Иными словами, компьютерное зрение — это совокупность технологий, обеспечивающих распознавание устройством зрительных образов, благодаря чему технические системы способны не только выявлять объекты по их визуальному представлению, но и классифицировать данные объекты, оценивать расстояния до них и принимать решения на основе извлечённой информации.

Основная целевая установка компьютерного зрения заключается в получении полезной информации из одного или последовательности изображений. Спектр решаемых задач является исключительно широким и включает в частности:

– калибровка оптических систем, настройка и синхронизация параметров камер;

– определение движения объектов;

– распознавание объектов;

– реконструкция сцены;

– сравнение изображений и идентификация изменений.

Области применения компьютерного зрения охватывают практически все сферы человеческой деятельности — от бытовых устройств до промышленной автоматизации и высокотехнологичных научных изысканий. В мобильных устройствах компьютерное зрение используется для автоматической регулировки яркости экрана на основе данных датчиков освещённости, а также для распознавания лиц и биометрической аутентификации.

Существует несколько способов классификации технологий компьютерного зрения, каждый из которых акцентирует определённый аспект

функционирования данных систем. По объёму обрабатываемых данных оптические системы традиционно подразделяют на:

– одномерные;
– двумерные;
– объёмные;
– особые случаи (например, системы панорамной съёмки)

По типу используемых датчиков и «области видимости» можно выделить:

– системы отслеживания маркеров;
– технологию Одновременной локализации и построения карты (SLAM);
– систему Oculus Insight.

Важно отметить, что все перечисленные технологии могут использовать как классические библиотеки анализа изображений, так и современные подходы, основанные на методах искусственного интеллекта.

Особого внимания заслуживает компьютерное зрение, функционирующее на основе изображений, поступающих с обычной видеокамеры, поскольку именно этот случай является наиболее распространённым в практических приложениях. В рамках данной области традиционно выделяют два принципиально различных подхода: классический математический подход и подход, связанный с применением нейронных сетей.

Математические подходы

Математический подход опирается на строгие статистические и геометрические модели: изображение рассматривается как случайное поле, а задача обнаружения объекта сводится к проверке статистических гипотез, вычислению отношения правдоподобия и сравнению полученного отношения с пороговым значением. Данный подход является хорошо изученным, отличается прозрачностью и не требует значительных вычислительных ресурсов, однако его эффективность существенно зависит от того, насколько точно выбранная математическая модель соответствует реальному изображению.

Критерий Байеса и критерий Неймана-Пирса используются для обнаружения объектов на изображении. В основе критериев основе лежит отношение правдоподобия

$$L = \frac{\omega\left(\left\{z_{\bar{j}}\right\}|H_1\right)}{\omega\left(\left\{z_{\bar{j}}\right\}|H_0\right)},$$

где $\omega\left(\left\{z_{\bar{j}}\right\}|H_1\right)$ и $\omega\left(\left\{z_{\bar{j}}\right\}|H_0\right)$ условные Плотности распределения вероятностей (ПРВ) наблюдений при наличии и отсутствии сигнала, в условиях справедливости гипотезы H_1 и H_0 соответственно.

Недостатком критерия Байеса решающего правила является необходимость наличия априорной информации о вероятностях состояния объекта. Однако даже если известны вероятности ошибок первого и второго рода, этого недостаточно для определения ПРВ.

Поэтому в подобных ситуациях используется критерий Неймана–Пирсона, в котором пороговое значение находится из условия, что при выбранном допустимом максимальном уровне вероятности ошибки ложной тревоги, решающее правило должно минимизировать вероятность ошибки пропуска цели, а оценки ПРВ $\omega\left(\left\{z_{\bar{j}}\right\}|H_1\right)$ и $\omega\left(\left\{z_{\bar{j}}\right\}|H_0\right)$ получают с использованием параметрических и непараметрических методов.

Генетический алгоритм представляет собой поисковый алгоритм, основанный на природных механизмах селекции и генетики. Данные алгоритмы обеспечивают выживание наиболее приспособленных решений из множества сгенерированных, формируя и изменяя процесс поиска на основе моделирования эволюции исходной популяции решений. Генетические алгоритмы сконструированы таким образом, что при генерации каждой новой популяции используются фрагменты исходных решений, к которым добавляются новые элементы, обеспечивающие улучшение решений относительно сформулированного критерия отбора.

Идея применения генетических алгоритмов в задачах обработки изображений состоит в автоматизированном построении оптимальных процедур обнаружения и идентификации объекта на изображении по его эталонному изображению с использованием библиотеки изображений обучающей выборки. При этом параметры подстраиваются за несколько итерация, обеспечивая в рамках обучающей выборки оптимальные характеристики обработки, создавая мутации, вносящие случайные изменения в параметры для распознавания, и пытаясь подобратнаиболее подходящую структуру для распознавания эталонного изображения. Генетические алгоритмы имеют и ряд ограничений применения. В частности, корректный анализ эффективности генетических алгоритмов в настоящее время сталкивается с вычислительными сложностями, которые могут быть труднопреодолимыми для определённых классов задач.

Обнаружение по перепаду яркости заключается в поиске границы между объектом и фоном на основе резкого изменения значений яркости. В простейшей математической модели наблюдаемое изображение описывается как:

$$\theta(x,y) = u + \gamma_0 hI(x,y) + n(x,y),$$

где u – яркость фона, h – величина перепада яркости, $I(x,y)$ – индикаторная функция формы объекта, $n(x,y)$ – аддитивный гауссовский шум, а $\gamma_0 = 1$ при отсутствии объекта и $\gamma_0 = 1$ при его наличии. Таким образом, задача сводится к различению двух гипотез: H_0 – объект отсутствует и H_1 – объект присутствует.

Необходимо сразу отметить ряд принципиальных ограничений, которые накладывает данный подход. Предполагается, что объект и фон имеют примерно постоянные, но различные уровни яркости, а величина перепада яркости h должна превышать некоторый минимальный порог h_0, иначе граница становится неразличимой на фоне шума. Форма объекта заранее неизвестна,

однако задаются ограничения на минимальное r_1 и максимальное $r2$ расстояние от центра объекта до его границы, что позволяет сузить множество возможных конфигураций. Кроме того, метод чувствителен к шумам и к пространственной неоднородности фона. На реальных изображениях фон редко бывает идеально однородным, что существенно ограничивает применимость метода в неконтролируемых условиях.

Для поиска объекта на изображении используется двухэтапный алгоритм обнаружения объектов по перепаду яркости. На первом этапе определяется наличие границы объекта на сегменте изображения, а на втором производится процедура сбора соединения разрозненных границ на участках в единый контур объекта. Такой подход позволяет достаточно эффективно и быстро выделять объекты на изображениях при условии, что объект и фон имеют примерно постоянные, но различные уровни яркости, а фон является статистически однородным. Первый этап локального анализа обеспечивает надёжное нахождение кандидатов в граничные точки, а второй этап собирает их в целостный замкнутый контур с помощью статистически оптимальных решающих правил. Однако в реальных условиях эксплуатации этот метод сталкивается с серьёзными ограничениями. Чистые, статистически однородные фоны встречаются редко, поскольку фон чаще имеет сложную текстуру, градиенты освещения, тени или другие объекты. На таком неоднородном фоне перепады яркости, связанные с изменением текстуры или освещения, будут ложно приниматься за границы объектов, что приведёт к большому числу ошибок первого рода. Кроме того, если сам объект обладает неоднородной яркостью или слабым контрастом по отношению к фону, вероятность его пропуска также возрастает. Поэтому на практике данный метод наиболее применим либо в специально организованных условиях, либо в качестве первого этапа в более сложных гибридных системах, где затем подключаются методы машинного обучения для фильтрации ложных срабатываний.

Нейронные сети

Второй подход, являющийся более современным, основан на методах глубокого обучения и свёрточных нейронных сетях. Нейронная сеть — это вычислительная структура, которая моделирует работу биологических нейронов. Она состоит из большого числа взаимосвязанных искусственных нейронов, организованных в слои: входной, скрытые и выходной. В процессе обучения нейронная сеть автоматически подстраивает веса связей между нейронами. Это позволяет ей аппроксимировать сколь угодно сложные нелинейные зависимости без явного программирования правил принятия решений.

Нейронная сеть не нуждается в ручном конструировании признаков. Она самостоятельно извлекает иерархические представления — от простых линий до сложных текстур и целых объектов — непосредственно из сырых пиксельных данных. Это делает нейронные сети наиболее мощным инструментом для задач компьютерного зрения. В частности интересно современное поколение

нейронных сетей реального времени, которые способны обрабатывать изображение с камер и видео за доли секунды.

Faster R-CNN (Faster Region-based Convolutional Neural Network) представляет собой двухэтапный детектор объектов. Faster R-CNN впервые предложил выполнять эту операцию непосредственно на графическом процессоре с использованием глубоких свёрточных сетей.

Ключевая инновация Faster R-CNN — это модуль RPN (Region Proposal Network), представляющий собой небольшой полносвязный детектор, наложенный на карту признаков, полученную свёрточной сетью, которую называют опорной сетью. Принцип работы RPN заключается в том, что поверх карты признаков скользит окно размером, как правило, 3×3 пикселя. В каждой позиции этого окна модель оценивает фиксированный набор так называемых якорей — прямоугольных областей эталонного размера. В стандартной конфигурации используются три масштаба и три соотношения сторон, что даёт девять якорей на каждую позицию. Для каждого якоря RPN вычисляет два значения: объектность — вероятность наличия любого объекта внутри данной области, и четыре параметра регрессии для уточнения положения и размера ограничивающей рамки. Таким образом, сеть предложений регионов не требует отдельного алгоритма поиска, а учится предсказывать потенциальные области с объектами непосредственно из признаков изображения.

YOLO (You Only Look Once) представляет собой одноэтапный детектор объектов основный на принципе однопроходного обнаружения объектов, что и отражено в названии: алгоритм анализирует изображение только один раз. В отличие от двухэтапных методов, которые сначала генерируют регионы-кандидаты, а затем классифицируют их, YOLO формулирует задачу детектирования как единую задачу регрессии, непосредственно предсказывая ограничивающие рамки и вероятности классов из пикселей изображения.

Входное изображение разделяется на сетку размером $S \times S$ ячеек. Если центр какого-либо объекта попадает внутрь ячейки, то эта ячейка становится ответственной за обнаружение данного объекта. Каждая ячейка предсказывает B ограничивающих рамок и значение уверенности для каждой рамки, а также C условных вероятностей классов.

Каждая предсказанная ограничивающая рамка описывается пятью компонентами: координатами центра относительно границ ячейки, обозначаемыми как x и y, шириной и высотой рамки относительно всего изображения, обозначаемыми как w и h, а также значением уверенности. Значение уверенности для предсказанной рамки вычисляется как произведение вероятности наличия объекта в данной рамке и метрики пересечения с эталоном. Проанализировав рамки, удовлетворяющие минимальному уровню уверенности, затем слив воедино рамки, которые ссылаются на один и то же объект, можно получить рамки всех обнаруженных объектов и их классы.

SSD (Single Shot MultiBox Detector) состоит из двух основных компонентов: опорной сети и SSD-головы. Опорная сеть обычно представляет

собой предобученную сверточную нейронную сеть для классификации изображений, из которой удалён последний полносвязный классификационный слой. Такая сеть извлекает признаки, сохраняя пространственную структуру изображения. Опорная сеть формирует 256 карт признаков размером 7 × 7 для входного изображения. SSD-голова представляет собой один или несколько дополнительных сверточных слоёв, добавленных к опорной сети, выходы которых интерпретируются как ограничивающие рамки и классы объектов.

Ключевой особенностью SSD является использование многоячеечной сети: модель делает предсказания на нескольких уровнях иерархии карт признаков, начиная с более глубоких слоёв, что позволяет обрабатывать объекты различных масштабов. Вышележащие слои с более высоким разрешением лучше обнаруживают мелкие объекты, тогда как нижележащие слои с более низким разрешением отвечают за крупные объекты.

Входное изображение сначала обрабатывается опорной сетью для извлечения карт признаков. Затем SSD делит каждую карту признаков на сетку ячеек. В отличие от скользящего окна, каждая ячейка сетки отвечает за обнаружение объектов в соответствующей области изображения. Если объект отсутствует, ячейка относит его к фоновому классу, а информация о местоположении игнорируется.

Выводы

Обобщая полученную информацию, для компьютерного зрения на текущий момент применяются как математические методы, так и нейронные сети. Математические методы используют самые разные подходи и походят для решения чётко поставленной задачи, затрачивая небольшое количество ресурсов. Нейронные сети являются более гибким инструментом, способным решать несколько задач одновременно, при этом затрачивая значительные объёмы оперативной памяти компьютера на свою работу.

Список литературы

1. Андриянов Н. А., Дементьев В. Е., Ташлинский А. Г. Обнаружение объектов на изображении: от критериев Байеса и Неймана–Пирсона к детекторам на базе нейронных сетей efficientdet. *Компьютерная оптика*, 46(1):139–159, 2022.

2. Goldberg. D. E. *Genetic Algorithms in Search, Optimization and Machine Learning*. Addison-Wesley, Reading, MA, 1989.

3. Holland J. H. *Adaptation in Natural and Artificial Systems*. University of Michigan Press, Ann Arbor, 1975.

4. Huang C. L., Wang. C. J. A ga-based feature selection and parameters optimization for support vector machines. *Expert Systems with Applications*, 31(2):231–240, 2004.

5. Сирота А. А., Соломатин А. И., Воронова Е. В. Двухэтапный алгоритм обнаружения и оценивания границы объектов на изображениях в условиях аддитивных помех и деформирующих искажений. *Автометрия*, 46(5):109–120, 2010.

УДК 621.39

Эффективность применения робототехнических комплексов в интересах технического обеспечения связи

Клименко А. Д.

Военная орденов Жукова и Ленина Краснознаменная академия связи имени Маршала Советского Союза С.М. Буденного, г. Санкт-Петербург, Россия

Аннотация: *В статье затронуты вопросы интеграции робототехнических комплексов в систему технического обеспечения войск, описаны перспективные способы управления робототехническими комплексами, снижающие воздействие дестабилизирующих факторов на канал связи. Отдельное внимание уделено недостаткам, связанным с внедрением перспективных робототехнических средств и комплексов, а также возможные пути решения некоторых из них. Описаны направления дальнейших исследований в области мониторинга технического состояния робототехнических комплексов.*

Ключевые слова: *робототехнические комплексы военного назначения, беспилотные летательные аппараты, мониторинг технического состояния, техническое обеспечение, снабжение, частотная телеграфия.*

Введение

Современные вооруженные конфликты претерпели ряд изменений за последние десятилетия, они характеризуются сочетанием гибридных и высокоманевренных действий, а также взрывным ростом технологий. Традиционные крупномасштабные столкновения XX века, имеющие четкую линию фронта, глубокие эшелонированные тылы, а также последовательное проведение операций сменились рассредоточенными и мобильными воинскими формированиями. Гибридные противостояния XI века предъявляют принципиально новые требования к Вооруженным Силам Российской Федерации в целом, и к системе материально-технического обеспечения (МТО) в частности. Изменение характера ведения боевых действий оказывает существенное влияние на систему Технического обеспечения (ТОб) в целом, и на подсистему снабжения в частности.

Современные подходы к организации снабжения войск различными видами вооружения, военной и специальной техники, отличаются от традиционных (централизованных, опирающихся на наличие безопасных складов и плановое пополнение) отсутствием четкой линии фронта, безопасных логистических цепочек до подразделений, находящихся вблизи линии боевого соприкосновения (ЛБС) и должны учитывать совокупность факторов, воздействующих на систему технического обеспечения. Кроме того, традиционные пути снабжения войск, такие как железнодорожные узлы, автотранспортные колонны, склады и базы, стали приоритетной целью для высокоточного оружия и ударных беспилотных летательных аппаратов противника. В связи с возможностями современных средств ведения разведки во всех диапазонах (оптической, радио, радиотехнической, радиоэлектронной) и

избытком средств поражения, на расстоянии не более 10-15 км от ЛБС невозможно (нецелесообразно) применять штатные средства доставки военно-технического имущества (ВТИ), основанные на использовании автомобилей на базовом шасси.

Применение робототехнических комплексов специального назначения при организации снабжения

В настоящее время для организации снабжения подразделений вблизи ЛБС широкое применение нашли робототехнические комплексы (РТК) различных типов базирования, обладающие значительно большей защищенностью от видовой разведки противника за счет их низких массогабаритных показателей и существенно снижающие риски для личного состава подразделений, организующих доставку ВТИ. Однако успех выполнения задачи при помощи РТК зависит от ряда факторов, рис. 1.

Рис. 1. Факторы, влияющие на успешное выполнение задач с использованием РТК

Применение РТК в интересах снабжения войск ВТИ позволяет повысить эффективность выполнения задач, связанных с риском для жизни, а также снизить количество и загруженность личного состава, привлекаемого к решению этих задач. Однако применение РТК имеет ряд ограничений и угроз.

Одним из важнейших факторов выполнения задачи является наличие устойчивого канал связи (КС) между оператором и РТК. По нему передаются команды управления (КУ) в одну сторону (от пульта оператора или наземной станции до РТК), а также видеотрансляция и телеметрия в обратную сторону (от РТК до оператора). При высокой удаленности от наземного пункта управления применяются ретрансляторы. В большинстве случаев, КС организован с использованием радиосвязи (намного реже – с использованием оптоволокна) и подвержен воздействию средств радиоэлектронной борьбы (РЭБ). Кроме того, КС должен обладать высокой электромагнитной

совместимостью с другими средствами связи, применяемыми для управления войсками, а также работать на радиочастотах, не занятых ими (для исключения создания помех в радиоэфире). Для уменьшения влияния случайных и преднамеренных помех на КС используются ретрансляторы (по возможности), а также технологии расширения спектра.

Управление робототехническими комплексами при воздействии помех

Организации помехоустойчивого и эффективного канала управления РТК посвящены работы [1-3]. В них описаны этапы формирования и передачи сигнально-кодовых конструкций (СКК) КУ РТК с использованием линейных частотно-модулированных (ЛЧМ) сигналов, рис. 2.

Формирование опорных ЛЧМ-сигналов для бинарных посылок «0» и «1» КУ соответственно осуществляется по формулам (1) и (2), описывающим процедуру линейного возрастания или убывания закона изменения частот:

$$S^{"0"}_{\text{ЛЧМ}}(t) = S_0\cos\{\varphi_0 + \varphi(t)\} = S_0\cos\{\varphi_0 + 2\pi[f_0 t + (b/2)t^2]\}, \quad (1)$$

$$S^{"1"}_{\text{ЛЧМ}}(t) = S_0\cos\{\varphi_0 - \varphi(t)\} = S_0\cos\{\varphi_0 - 2\pi[f_0 t + (b/2)t^2]\}, \quad (2)$$

где S_0 – амплитуда сигнала, $f_0 = (f_{\max} + f_{\min})/2$ – центральное значение несущей частоты; $f_{\min}$ и $f_{\max}$ – минимальное и максимальное значения частоты сигнала, φ_0 – начальная фаза, $b = (f_{\max} - f_{\min})/T_c$ – параметр, соответствующий скорости изменения частоты во времени; T_c – длительность сигнала.

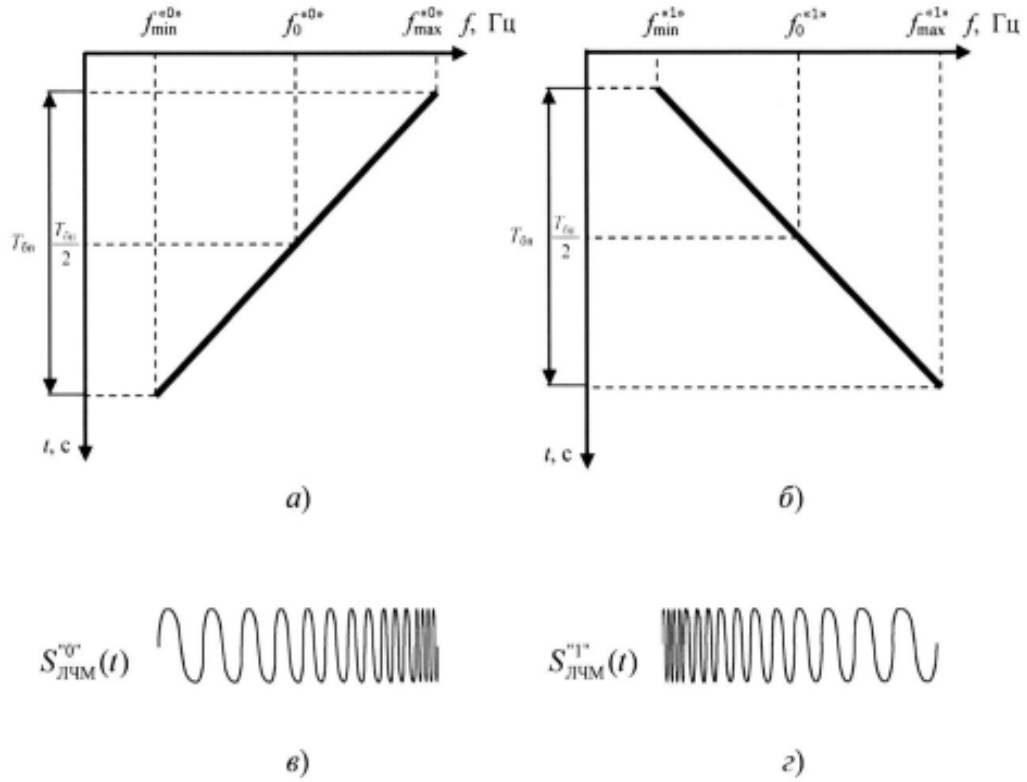


Рис. 2. Характеристики ЛЧМ-сигналов в частотно-временной области:
а) с законом линейно возрастающего изменения частоты *(в)*;
б) с законом линейно убывающего изменения частоты *(г)*

Организация КС с использованием СКК КУ на базе ЛЧМ-сигналов совместно с технологиями когнитивного радио и с устройством формирования многочастотных сигналов [4] позволит выполнять задачи с применением РТК в сложной помеховой обстановке, а также добиться оперативности и информационной скрытности доведения КУ до РТК.

Мониторинг технического состояния робототехнических комплексов

Критически важным аспектом применения РТК для решения задач ТОб, является техническое состояние (ТехС) РТК. Оно зависит от ряда факторов:

– своевременности и качества проведения технического обслуживания и ремонта (ТО и Р);

– наличия запасного инструмента и принадлежностей у техника (оператора) для проведения ТО и Р;

– ТехС каждого модуля РТК;

– полноты и достоверности данных, выявленных в ходе мониторинга ТехС РТК;

– наличия на техническом пункте источника переменного напряжения 220В или генератора для подзарядки аккумуляторных батарей (Акб);

– наличия сменных Акб на техническом пункте;

– наличия горючего (для РТК, использующих в качестве силового агрегата двигатель внутреннего сгорания) и т.д.

При этом следует отметить, что система мониторинга ТехС РТК недостаточно развита. Это связано с большой разновидностью РТК (всех видов базирования), с отсутствием единых стандартов при разработке модулей связи и управления РТК, а также с отсутствием выделенного ресурса для организации канала мониторинга ТехС РТК (с выводом информации либо на сервер мониторинга, либо непосредственно оператору) [5].

В большинстве случаев, информация, передаваемая от РТК до оператора по КС, представляет собой видеотрансляцию и телеметрию, а также показания немногочисленных датчиков (заряд Акб и процент потери пакетов в процессе управления). Техническое же состояние РТК определяется оператором (техником) при наличии физического доступа к нему (перед выполнением и после выполнения задачи).

Направления дальнейших исследований

Для обеспечения полноты и достоверности информации, полученной в процессе мониторинга ТехС РТК следует:

− провести анализ существующих датчиков, применяемых для идентификации ТехС наиболее важных модулей РТК;

− провести анализ возможностей оперативной памяти и процессоров современных РТК с целью выявления наивысшей частоты опроса датчиков, не влияющей не работу других модулей РТК;

− разработать модель мониторинга ТехС РТК, включающую в себя диспетчерский, телекоммуникационный и сенсорный уровни определения ТехС РТК;

– разработать методику мониторинга ТехС РТК в процессе выполнения задач технического обеспечения с применением перспективных технических и технологических решений.

Выводы

На данном этапе развития робототехники и степени интеграции РТК в оборонную сферу, их применение в интересах ТОб (особенно в части снабжения) позволят повысить эффективность выполнения задач, связанных с риском для жизни. Однако, внедрение РТК в систему ТОб на сегодняшний день может быть намного эффективнее при использовании описанных в статье способов доведения КУ в интересах РТК, а также при развитии системы мониторинга ТехС РТК.

Список литературы

1. Будко Н. П., Будко П. А., Клюшин М. А., Шаталов А. Е. Способ доведения управляющей и телеметрической информации в интересах робототехнических платформ различных типов базирования // Системы управления, связи и безопасности. 2025. № 3. С. 294-322. DOI: 10.24412/2410-9916-2025-3-294-322.

2. Будко Д. Д., Будко П. А., Зацепин Т. А., Клименко А. Д. Метод управления беспилотными транспортными системами на основе помехоустойчивых сигнально-кодовых конструкций в условиях сосредоточенных и шумовых помех // Системы управления, связи и безопасности. 2025. № 4. С. 134-178. DOI: 10.24412/2410-9916-2025-4-134-178.

3. Будко Д. Д., Будко П. А., Клименко А. Д., Рыжкова Д. Н. Модель выбора полосы частот в интересах формирования декаметровых радиолиний управления беспилотными транспортными системами // Техника средств связи. 2025. № 4 (172). С. 74-83. DOI: 10.24412/2782-2141-2025-4-74-83.

4. Будко Д. Д., Будко Н. П., Буцанец А. А., Груздев А. А., Каретников В. В., Клименко А. Д., Рыжкова Д. Н. Устройство формирования многочастотных сигналов // Патент на изобретение RU 2864855 C1, опубл. 30.06.2026, бюл. № 19.

5. Клименко А. Д., Решетов В. В. Применение роботизированных комплексов специального назначения при выполнении мероприятий технического обеспечения // Телекоммуникации и связь. 2026. № 2. С. 94-99. DOI: 10.21681/3034-2050-2026-2-94-99.

УДК 004.056.53

Раннее обнаружение DDoS-атак на стадии подготовки на основе машинного обучения и контроля остаточного трафика

Потапов Г. А., Гречишникова Т. А.

Федеральное государственное бюджетное образовательное учреждение высшего образования «МИРЭА – Российский технологический университет», г. Москва, Россия

Военная орденов Жукова и Ленина Краснознаменная академия связи имени Маршала Советского Союза С.М. Буденного, г. Санкт-Петербург, Россия

Аннотация: *Рассмотрена задача обнаружения распределённых атак типа «отказ в обслуживании» (DDoS) на стадии их подготовки, предшествующей достижению пиковой интенсивности воздействия. Предложена модель представления наблюдаемого сетевого трафика в виде суммы легитимной и нелегитимной составляющих, в которой легитимная составляющая выделяется классификатором, построенным методами машинного обучения, а признаком подготовки атаки служит скорость роста остаточной составляющей. Сформулировано правило упреждающего переключения нагрузки на резервный узел по прогнозу момента отказа защищаемого узла. Приведена схема раннего обнаружения и упреждающего переключения на резервный узел. Показано, что предлагаемый подход обеспечивает сокращение времени обнаружения атаки при фиксированной вероятности ложной тревоги.*

Ключевые слова: *DDoS-атака, классификация трафика, машинное обучение, остаточный трафик, последовательное обнаружение, раннее обнаружение, резервный узел, стадия подготовки атаки.*

Введение

Распределённые атаки типа «отказ в обслуживании» (Distributed Denial of Service, DDoS) остаются одним из наиболее массовых классов деструктивных воздействий на информационно-вычислительные сети [3]. Типовые способы защиты [1, 2] построены на выявлении уже состоявшегося несанкционированного воздействия: решение о наличии атаки принимается по факту совпадения идентификаторов потока с эталонными наборами либо по превышению интенсивностью трафика заданного порога. Как следствие, обнаружение происходит на стадии, когда интенсивность воздействия уже сопоставима с пропускной способностью защищаемого узла, а время, остающееся на реагирование, минимально.

Для повышения точности выделения атакующего трафика в современных решениях всё шире применяются методы машинного и глубокого обучения: предложены лёгкие свёрточные детекторы, ориентированные на минимизацию задержки принятия решения [7], обучаемые нейросетевые классификаторы сетевых потоков [8], решения с автоматическим дообучением модели в процессе эксплуатации [9] и гибридные архитектуры для выявления низкоинтенсивных атак [10], а также подходы операторского масштаба на основе цифровых двойников сети [11]. Вопросы оценки способности узла

связи функционировать в условиях DDoS-воздействий и мониторинга его защищённости рассматривались в работах [12, 13]. Развиваются и решения адаптивной фильтрации с самообучением [14, 15]. Вместе с тем большинство перечисленных подходов ориентировано на обнаружение уже развившейся атаки, тогда как выявление именно стадии подготовки, предшествующей достижению пиковой интенсивности, исследовано существенно слабее.

Вместе с тем жизненный цикл DDoS-атаки включает три последовательные стадии: инициацию (подготовку), эскалацию и исход. На стадии подготовки выполняются активация ботнета, разведка защищаемого объекта и пробные маломощные воздействия. Продолжительность этой стадии измеряется часами: так, по открытым данным о воздействиях на инфраструктуру Петербургского международного экономического форума в июне 2022 года массированные DDoS-атаки начались приблизительно за сутки до пиковой фазы, нарушившей работу систем аккредитации (по сообщению РБК от 17.06.2022, rbc.ru). Таким образом, стадия подготовки образует наблюдаемый интервал, на котором атака в принципе может быть обнаружена до достижения ею пиковой интенсивности.

Цель статьи: изложить модель наблюдаемого трафика и признак стадии подготовки DDoS-атаки, основанные на выделении легитимной составляющей трафика классификатором машинного обучения и контроле скорости роста остаточной составляющей, а также правило упреждающего переключения нагрузки на резервный узел.

Модель трафика и признак стадии подготовки атаки

Суммарный трафик, наблюдаемый на входе защищаемого узла, представим в виде суммы двух составляющих

$$T(t) = L(t) + U(t), \tag{1}$$

где $T(t)$ – суммарный наблюдаемый трафик; $L(t)$ – легитимная составляющая, порождаемая санкционированными абонентами; $U(t)$ – нелегитимная составляющая, порождаемая источниками атаки.

Составляющая $L(t)$ непосредственно не наблюдается. Для её выделения используется классификатор, построенный методами машинного обучения по признакам пакетов и потоков (аналогично признаковому описанию в [2]) и относящий каждый поток к легитимному либо нелегитимному классу. Обучение классификатора выполняется по методике самонастройки разметки: на пиковой стадии ранее состоявшейся атаки принадлежность потоков нелегитимному классу устанавливается практически достоверно, что позволяет обучить разделитель на данных пика и ретроспективно применить его к записям трафика, соответствующим стадии подготовки той же атаки. Такой приём частично компенсирует известное ограничение публичных наборов данных (в частности, CIC-DDoS2019 [4]), в которых стадия подготовки представлена слабо.

По результату классификации формируется остаточная составляющая трафика

$$R(t) = T(t) - \widehat{L}(t). \quad (2)$$

Здесь $\widehat{L}(t)$ — оценка легитимной составляющей, формируемая классификатором; в силу неидеальности классификатора остаток $R(t)$ служит оценкой нелегитимной составляющей $U(t)$, а не тождественно равен ей. В отсутствие атаки остаток $R(t)$ определяется ошибками классификации и фоновыми несанкционированными потоками и в среднем стационарен. Начало стадии подготовки проявляется как систематический рост остатка задолго до того, как суммарная интенсивность $L(t)$ превысит пороги, используемые в известных способах [1, 2]. Признаком стадии подготовки принимается выполнение условия

$$\frac{dR(t)}{dt} \geq \gamma, \quad (3)$$

где γ – порог скорости роста остаточной составляющей. При выполнении условия (3) формируется сигнал раннего предупреждения.

Контроль скорости роста остатка сводится к задаче скорейшего обнаружения разладки случайного процесса, для которой развиты последовательные процедуры [5, 6]. Порог γ выбирается из условия

$$M[\tau - \nu | \tau \geq \nu] \to min; F \leq F_{доп}, \quad (4)$$

где τ – момент обнаружения; ν – момент начала стадии подготовки; F – вероятность ложной тревоги за заданный период наблюдения; $Fдоп$ – её допустимое значение, задаваемое исходя из операционных требований владельца защищаемого объекта. Постановка (4) означает выбор порога γ, минимизирующего среднюю задержку обнаружения ($\tau - \nu$) при ограничении вероятности ложной тревоги сверху величиной $Fдоп$; тем самым при том же уровне ложных срабатываний обеспечивается в среднем более раннее обнаружение.

Принципиальное отличие постановки (4) от настройки порога в известных способах [1, 2] состоит в следующем. Изменение порога перемещает рабочую точку вдоль существующей характеристики обнаружения, обменивая задержку на ложные тревоги. Введение классификатора машинного обучения и переход к контролю остатка (2) смещают саму характеристику: при том же допустимом уровне ложных тревог $Fдоп$ достигается меньшее среднее время обнаружения за счёт информации о структуре трафика, извлекаемой классификатором.

Правило упреждающего переключения на резервный узел

Сигнал раннего предупреждения используется не только для оповещения, но и для упреждающего манёвра нагрузкой. По наблюдаемой траектории $R(t)$ экстраполяцией до критического уровня, соответствующего исчерпанию ресурса защищаемого узла, формируется прогноз момента отказа $t_{отк}$. Переключение нагрузки на резервный узел инициируется при выполнении условия

$$t_{\text{отк}} - t \le T_{\text{пер}} + \delta, \tag{5}$$

где t – текущий момент времени; $Tпер$ – длительность процедуры переключения на резервный узел; δ – гарантийный запас времени.

Содержательно правило (5) означает, что переключение начинается не позднее момента, когда прогнозируемое время до отказа сравняется с длительностью самого переключения с учётом запаса. Тем самым смена узла завершается до наступления отказа, а не после него, что исключает перерыв в обслуживании санкционированных абонентов.

Схема алгоритма

Последовательность операций раннего обнаружения и упреждающего переключения приведена на рис. 1. Схема выполнена с использованием символов по ГОСТ 19.701-90: приём трафика отображён символом данных, оценка легитимной составляющей классификатором – символом предопределённого процесса, проверка условий (3) и (5) – символами решения; прогноз момента отказа узла, используемый в условии (5), формируется экстраполяцией остаточной составляющей до уровня исчерпания ресурса. При невыполнении условий наблюдение продолжается.

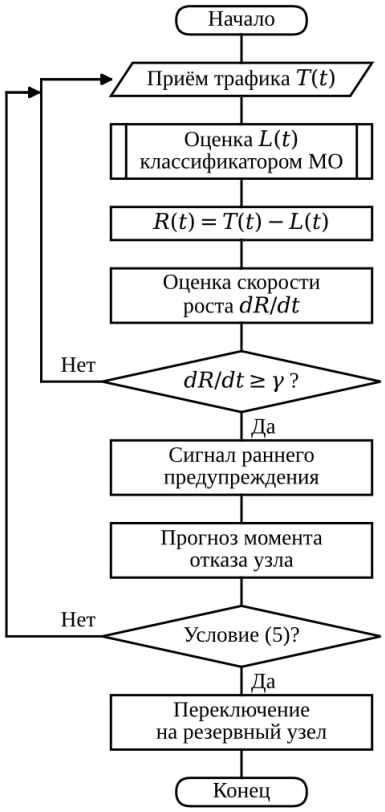


Рис. 1. Схема раннего обнаружения DDoS-атаки и упреждающего переключения на резервный узел

Заключение

Предложенная модель переносит момент обнаружения DDoS-атаки со стадии эскалации на стадию подготовки за счёт выделения легитимной составляющей трафика классификатором машинного обучения и контроля скорости роста остаточной составляющей. В отличие от настройки порога в известных способах защиты [1, 2], подход обеспечивает смещение характеристики обнаружения: сокращение среднего времени обнаружения при фиксированной вероятности ложной тревоги. Правило (5) связывает раннее предупреждение с упреждающим переключением нагрузки на резервный узел, сокращая время реагирования в целом.

Направлением дальнейших исследований является экспериментальная оценка вероятностно-временных характеристик обнаружения на композиции публичных наборов данных и записей изолированного стенда, воспроизводящего стадию подготовки атаки.

Список литературы

1. Пат. 2475836 Российская Федерация. Способ защиты вычислительных сетей / Баленко О. А., Бухарин В. В., Васинев Д. А., Кирьянов А. В., Стародубцев Ю. И., Стукалов И. В.; заявитель и патентообладатель Военная академия связи им. Маршала Советского Союза С. М. Буденного. – № 2012109258/08; заявл. 12.03.2012; опубл. 20.02.2013.

2. Пат. 2704741 Российская Федерация. Способ защиты от DDoS-атак на основе классификации трафика / Репин Д. С., Краснов А. Е., Надеждин Е. Н., Никольский Д. Н., Галяев В. С., Зыкова Е. А. – № 2018109398; заявл. 16.03.2018; опубл. 30.10.2019.

3. Mirkovic J., Reiher P. A taxonomy of DDoS attack and DDoS defense mechanisms // ACM SIGCOMM Computer Communication Review. 2004. Vol. 34, № 2. P. 39–53.

4. Sharafaldin I., Lashkari A. H., Hakak S., Ghorbani A. A. Developing Realistic Distributed Denial of Service (DDoS) Attack Dataset and Taxonomy // 2019 International Carnahan Conference on Security Technology (ICCST). Chennai, India, 2019. P. 1–8.

5. Ширяев А. Н. Об оптимальных методах в задачах скорейшего обнаружения // Теория вероятностей и её применения. 1963. Т. 8, вып. 1. С. 26–51.

6. Page E. S. Continuous inspection schemes // Biometrika. 1954. Vol. 41, № 1–2. P. 100–115.

7. Doriguzzi-Corin R., Millar S., Scott-Hayward S., Martinez-del-Rincon J., Siracusa D. LUCID: A Practical, Lightweight Deep Learning Solution for DDoS Attack Detection // IEEE Transactions on Network and Service Management. 2020. Vol. 17, № 2. P. 876–889. doi:10.1109/TNSM.2020.2977441.

8. Пат. 2683631 Российская Федерация. Способ обнаружения компьютерных атак / Алейник А. С., Лебедев М. А., Садовников В. В., Казаков Д. А. — Заявл. 14.02.2018; опубл. 29.03.2019.

9. Automatic retraining of machine learning models to detect DDoS attacks: пат. US 11665194 B2 / Cisco Systems. — Опубл. 30.05.2023.

10. Detection method and system for low-rate DDoS attack: пат. заявка CN 113206859 A. — Опубл. 2021.

11. Digital Twin-Enabled DDoS Attack Detection System and Method for Autonomous Core Networks: пат. заявка US 2025/0097259 A1. — Опубл. 20.03.2025.

12. Гречишников Е. В., Добрышин М. М. Оценка эффективности деструктивных программных воздействий на сети связи. — 2015.

13. Гречишников Е. В., Добрышин М. М. Модель узла доступа VPN как объекта сетевой и потоковой компьютерных разведок и DDoS-атак.

14. Adaptive machine learning-based DDoS traffic filtering: пат. EP 3609148 A1. — Опубл. 2020.

15. Methods for preventing DDoS attack based on adaptive self-learning of session and transport layers: пат. US 10834110 B2. — Опубл. 10.11.2020

УДК 621.39

Разработка волоконно-оптического датчика акселерометра для детектирования низкочастотных вибраций

Штеле Б. Э.

ПАО «Интелтех», г. Санкт-Петербург, Россия

Аннотация: *Современные приборы для проведения различных измерений нередко требуют не только высокой точности и скорости измерений. Всё чаще одним из пунктов технического задания при разработке прибора становится устойчивость к неблагоприятным факторам окружающей среды и электромагнитным помехам. Основным преимуществом оптических датчиков является точность и способность чувствительного элемента функционировать без питания. Также отсутствие электронных компонентов внутри чувствительного элемента может позволить работать в таких условиях, как например, высокая влажность. Цель исследования – разработать и описать математическую модель чувствительного элемента волоконно-оптического датчика акселерометра, разработать печатные платы для прибора. Научная новизна работы заключается в разработке конструкции волоконно-оптического акселерометра, в которой оптическое волокно используется в качестве консольной балки. Результаты моделирования позволяют сказать, что есть возможность проводить измерения в достаточно широкой полосе измерений вплоть до 450Гц, где разрешение по частоте будет зависеть от выборки отсчетов. Практическая значимость работы состоит в том, что прибор в отличии от емкостных и пьезоэлектрических аналогов может обладать большей устойчивостью к разрушающим электронику факторам. Также стоит отметить, что производство подобного датчика не будет требовать производства микро или нано фрагментов, что упрощает разработку и делает её доступней.*

Ключевые слова: *акселерометр, частота, полоса спектра, низкие частоты, консольная балка, длина, резонанс, мониторинг.*

Введение

Для решения задачи дефектоскопии оборудования, имеющего в своем составе крутящиеся подвижные части, нередко прибегают к анализу частотного спектра. На оборудование прикрепляется чувствительная головка датчика, которая может измерять низкочастотные вибрации. Получившийся спектр выводится в удобном для восприятия виде. Далее проводится анализ спектра и может выноситься решение о текущем состоянии оборудования. Такой подход помогает существенно снизить количество нештатных аварий. Акселерометр может применяться в этом случае для получения низкочастотного спектра с высоким разрешением по частоте. Однако такие типы как емкостные или пьезоэлектрические датчики, могут не справляться с такими задачами в неблагоприятных условиях окружающей среды, таких как, например, влажность, высокий уровень электромагнитных помех. В таких условиях хорошим решением может быть замена некоторых электронных компонентов на оптические. Это позволит повысить устойчивость прибора к условиям окружающей среды, а также может сделать полностью невосприимчивым к электромагнитным помехам.

Акселерометр – это прибор, позволяющий измерить ускорение или изменение проекции ускорения, что помогает определять изменение направления движения. Вибрация, как и другое механическое движение описывается ускорением, скоростью и перемещением. При гармонической вибрации перемещение объекта можно описать формулой.

$$x(t) = A\sin(2\pi ft).$$

где, $x(t)$ – смещение, A – амплитуда вибрации, f – частота, t – время

Первой производной этого выражения будет скорость, второй производной будет ускорение, а именно

$$a(t) = -(2\pi f)^2 x(t).$$

Из формулы видно, что ускорение пропорционально квадрату частоты.

Акселерометр измеряет именно $a(t)$, это переменный сигнал ускорения, который при воздействии вибрации тоже будет синусоидальным и с той же частотой.

В общем случае схема акселерометра выглядит следующим образом. Имеется корпус, внутри которого находится эталонная масса, подвешенная на пружинах. На рис. 1 представлен упрощенный вид акселерометра. При воздействии вибрации на корпус эталонная масса начинает колебаться с той же частотой. Вместе с этим изменяется растяжение пружины или пружин, что преобразуется в любой удобный для восприятия вид. Например, для механического акселерометра это может быть отклонение стрелки. Также можно закрепить на корпус одну обкладку конденсатора, а на эталонную массу другую, за счет изменения расстояния между обкладками, будет изменяться емкость.

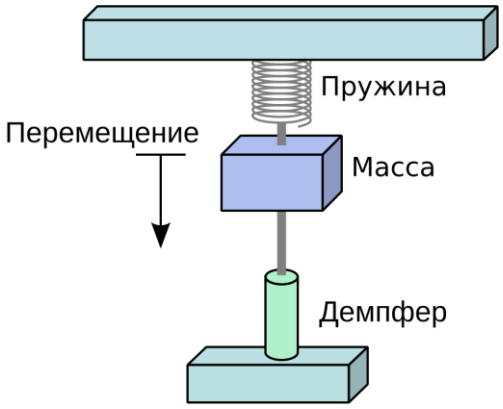


Рис. 1. Общая схема акселерометра

Благодаря этому возможно производить измерения, данный вид акселерометра называется емкостным.

$$C = \frac{\varepsilon_0 \varepsilon S}{d}$$

где, d – является изменяемым параметром в данной системе, а именно расстоянием между обкладками. На рис. 2 схематично представлен такой вид прибора.

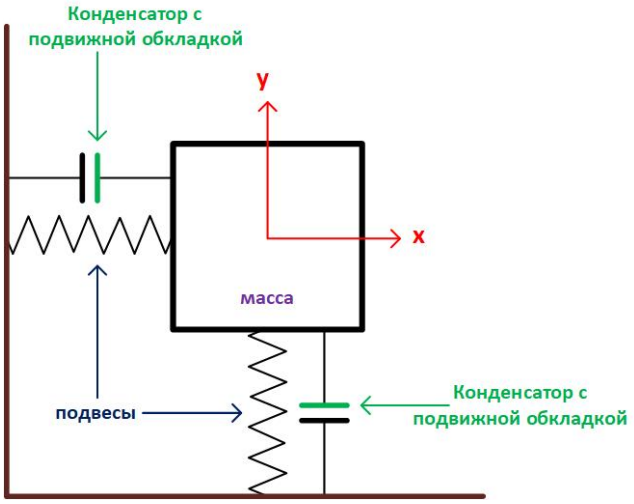


Рис. 2. Схема емкостного акселерометра

Описание устройства чувствительного элемента

На рис. 3 представлена консольная балка в виде некоторого структурного элемента, который жестко закреплен с одного конца, в то время как другой конец остается свободным.

Рис. 3. Консольная балка

В контексте применения такой конструкции для создания акселерометра, в качестве балки применяют оптоволокно. К основанию, корпусу, чувствительного элемента датчика прикладывают некоторую гармоническую вибрацию. Основание передает консольной балке гармоническую силу той же частоты. Амплитуда в таком случае будет меньше, чем амплитуда самой вибрации при условии, что свободный конец не находится в резонансе. В консольную балку заводят свет, например лазерное или светодиодное излучение. Свет собирается с помощью приемного оптоволокна и преобразуется в напряжение, при помощи сопряженных фотодиодов. На рис. 4 представлен пример такого фотодиода.

Рис. 4. Волокно с сопряженным фотодиодом

Также возможно использовать просто фотодиоды, без оптоволокна. Однако тогда чувствительный элемент потеряет невосприимчивость к электромагнитным помехам, необходимо будет подбирать фотодиод, чья чувствительная площадь будет достаточно маленькой (0.01мм^2-0.1мм^2). На рис. 5 представлен предполагаемый вид чувствительного элемента.

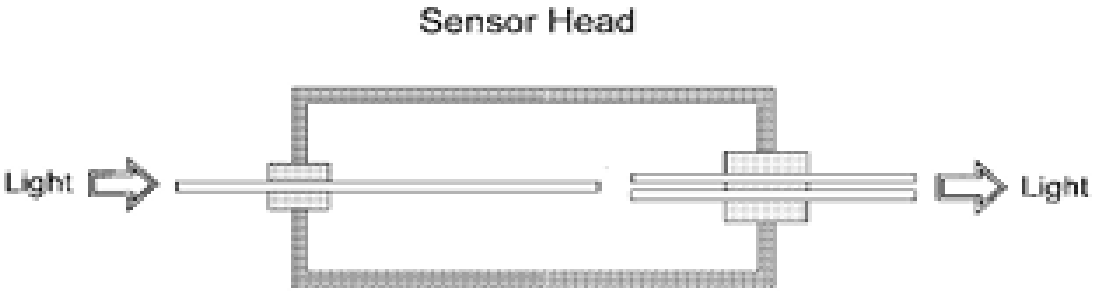


Рис. 5. Чувствительный элемент

Одним из самых важных параметров для такого датчика является длина свободного перемещающегося конца волокна. От него зависит какую максимальную частоту можно будет обнаружить. Ниже представлена формула для нахождения собственных частот консольной балки [1-3].

$$f_n = \frac{3.516}{2\pi}\sqrt{\frac{EI_z}{\rho L^4}},$$

где, константа 3.516 берется как коэффициент первой моды, возведенный в квадрат [2, 4] (этот коэффициент зависит от граничных условий) E – модуль Юнга или модуль упругости, I_z – момент инерции поперечного сечения, ρ – плотность материала, L – длина свободного конца.

Из формулы видно, что есть всего один параметр, который можно изменять, а именно длина. Параметр находится в знаменателе, тогда, при увеличении, первая собственная частота балки будет смещаться ближе к нулю. Это сокращает диапазон, в котором могут проводиться полезные измерения, так как резонанс искажает результат.

Однако, при уменьшении длины можно добиться плоской АЧХ вплоть до ~450Гц. Далее на рис. 6 представлена модель чувствительного элемента в среде моделирования Comsol.

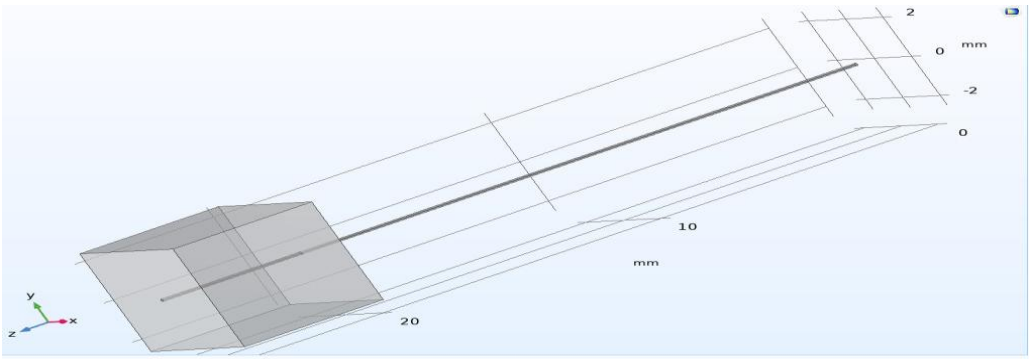


Рис. 6. Модель в Comsol

Модель состоит из вытянутого цилиндра с основными твердотельными параметрами, как у оптоволокна диаметром 125мкм (диаметр стандартного телекоммуникационного оптоволокна). Один конец жестко закреплен на платформе в виде куба. К одной из плоскостей которого будет прикладываться гармоническое воздействие. Ниже приведены результаты анализа на собственные частоты консольной балки.

На рис. 7 представлена АЧХ для разных длин волокна. По оси ординат измерение идет в мм, по оси абсцисс в Гц.

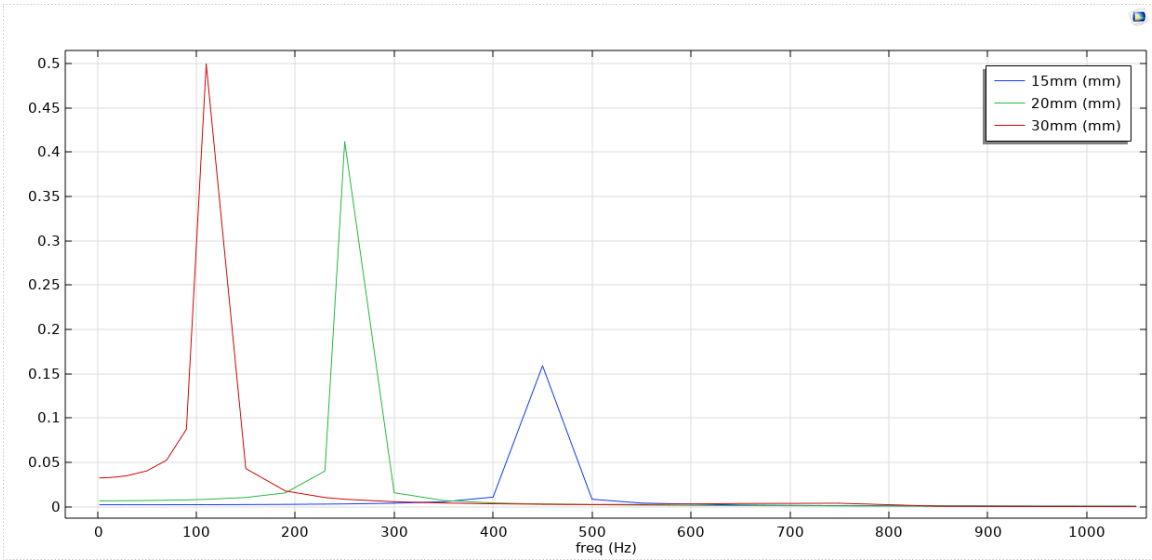


Рис. 7. Исследование в частотной области

Из графика становится понятно, что чем короче длина, тем меньше и амплитуда колебаний [4]. Это может стать проблемой для детектирования перемещения волокна. Наиболее широкодоступные SMD фотодиоды в различных корпусах обладают чувствительной площадью в порядке 4 мм^2 – 40 мм^2, чего недостаточно для детектирования смещения в единицы или десятки микрометров. Поэтому, для детектирования перемещения с такой малой амплитудой можно использовать схему, которая была приведена на рис. 5.

На рисунке передающее волокно направлено между двумя приемными волокнами, чей диаметр 125мкм. Расстояние от центра поперечного сечения одного приемного волокна до центра другого должно быть в пределах десятков микрометров. Это обеспечивает возможность обнаружения разницы между интенсивностью падающего света на каждое волокно, при амплитуде смещения волокна до 10 мкм. При таком расположении в покое, какое-то количество света будет попадать на оба волокна. Но при приеме с помощью волокна, необходимо учитывать его апертуру, которую желательно сделать как собирающую свет линзу. Приемное волокно можно заменить на малые фотодиоды со способом монтажа on die. Это может позволить расширить полосу для измерений, однако в таком случае нельзя будет говорить об устойчивости к неблагоприятным факторам окружающей среды. На рис. 8 приведен пример такого фотодиода.

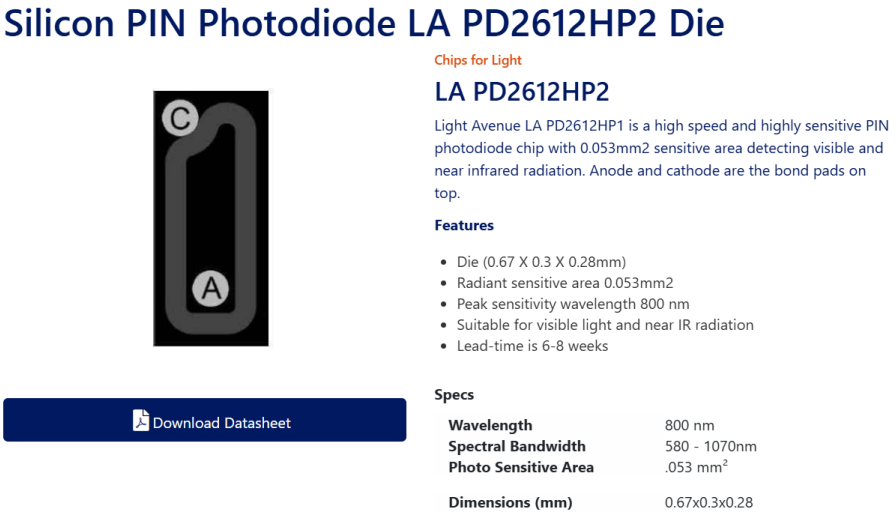


Рис. 8. Характеристики фотодиода

Передаточная функция датчика выглядит следующим образом [1]

$$H(w) = \frac{X(w)}{A(w)} = \frac{1}{w_0^2 - w^2},$$

где, X – это смещение конца балки, а A ускорение основания.

Функция показывает, что при малых частотах, когда ($\omega << \omega_0$) выход почти равен входу, при частотах близких к резонансу ($\omega \rightarrow \omega_0$) знаменатель стремится к нулю, следовательно амплитуда растет очень сильно. При частотах выше ($\omega >> \omega_0$), система перестает успевать за колебаниями снижая амплитуду.

Такой чувствительный элемент также обладает диаграммой направленности. Если оказать воздействие и его вектор будет направлен вдоль волокна, то детектировать смещение не получится. Датчик важно крепить таким образом, чтобы воздействие было перпендикулярно волокну.

В следующем разделе рассмотрена общая структура прибора: корпус чувствительного элемента, печатная плата чувствительного и вычислительного элементов.

Разработка прибора. Структурная схема прибора

На рис. 9 представлена структурная схема прибора, где:

− источник света – некоторый источник излучения, жёстких требований к нему не предъявляется. Однако, важно согласовать диапазон длин волн, на которых фотодиод может детектировать излучение и длину волны, с которой излучает источник света;

− чувствительный элемент – часть, где происходит прием и преобразование света в напряжение для дальнейшей обработки;

− вычислительный элемент – часть прибора, в которой происходит формирование спектра, фильтрация, дальнейшая передача данных на персональный компьютер.

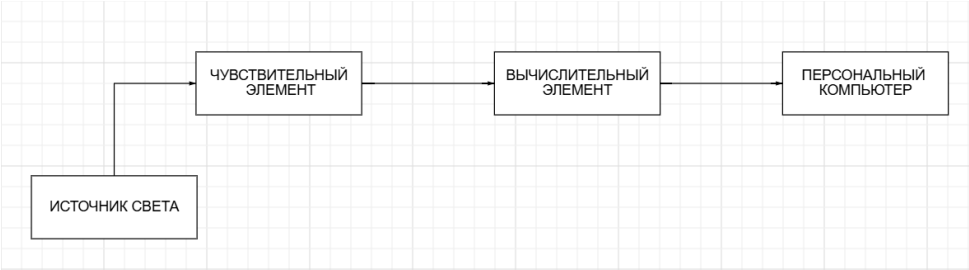


Рис. 9. Структурная схема прибора

Структурная схема позволяет понять основной принцип работы прибора, а также графически представить его.

Печатные платы и корпус

На плате чувствительного элемента обязательно необходимо расположить следующие элементы: фотодиоды, операционные усилители, аналогово-цифровой преобразователь. Первые два элемента участвуют в построении схемы трансимпедансного усилителя [5]. Усилитель позволяет преобразовать ток, возникающий при воздействии излучения на фотодиод, в напряжение. Далее это напряжение считывается 4-х канальным АЦП и передается по интерфейсу I2C на вычислительный элемент. На последнем происходит вычисление спектра, фильтрация и другая цифровая обработка, при необходимости. Также на плате вычислительного элемента расположена микросхема, позволяющая коммуницировать с COM-портом персонального компьютера. На плате находится лазерный диод, источник излучения, драйвер для управления диодом. Это позволяет сформировать обратную связь, с помощью которой можно регулировать мощность излучения. На рис. 10 представлен вид платы чувствительного элемента. На плате можно заметить два операционных усилителя и АЦП, а также микросхему стабилизатора для формирования устойчивого опорного напряжения. На рис. 11 представлена плата вычислительного элемента. В роли вычислителя выступает микроконтроллер STM32F100, также можно заметить коннекторы для чувствительного элемента, USB-Type C разъем, посадочное место

для лазерного диода и другие необходимые микросхемы, обвязочные элементы. На рис. 12 представлена распечатанная на 3D принтере модель корпуса для чувствительного элемента.

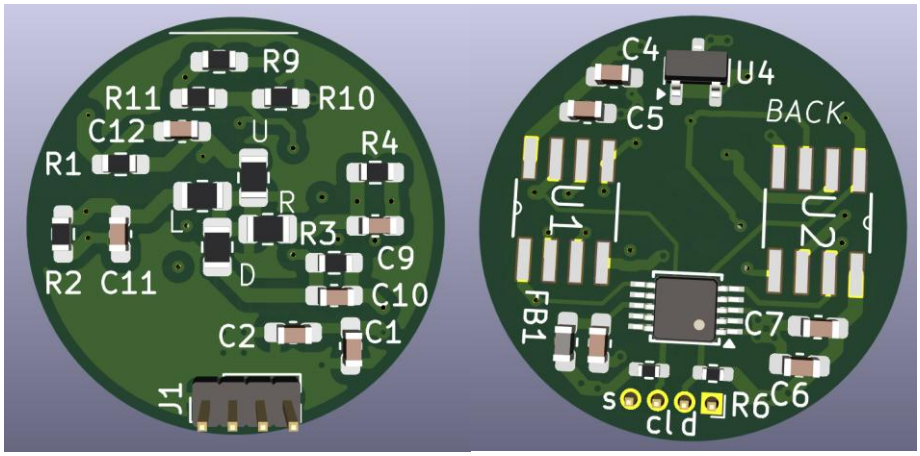


Рис. 10. Слева фронтальный вид платы, справа тыловой вид платы

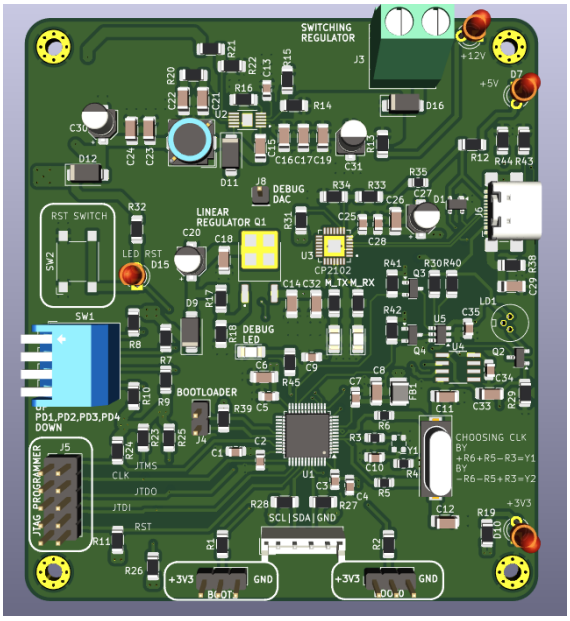


Рис. 11. Фронтальный вид платы вычислительного элемента

Рис. 12. 3D модель корпуса чувствительного элемента

Вывод

В статье приведен математический анализ принципа работы устройства. По рис. 7 можно сделать вывод, что самая плоская АЧХ достигается за счет меньшей длины свободного конца, а это позволяет проводить гораздо более точные измерения. При помощи нескольких чувствительных элементов, каждый из которых будет работать с разной длиной волокна, можно построить датчик, который способен очень точно детектировать определенные частоты (резонансные частоты). У такого варианта построения есть свои недостатки. К ним относятся: 1) при длительном высокоамплитудном колебании волокна, внутри могут образовываться трещины, что приведет к выходу из строя устройства, 2) нет возможности точно обнаруживать другие частоты.

Приведен обзор спроектированного корпуса чувствительного элемента, описаны его преимущества: возможность изменения длины волокна, закрытия фотодиода от лишнего излучения. Смоделирована и напечатана модель на 3D принтере. Представлен обзор результатов проектирования плат вычислительного и чувствительного элементов прибора, описание схемотехнических решений.

Реализация датчика позволит производить своевременное выявление элементов, которые могут выйти из строя, что поможет избежать негативные последствия, возникающие при несвоевременном выходе из строя оборудования.

Список литературы

1. Кобо А., Лопес Игуэра Х. М., Моранте М. А. Простой низкочастотный волоконно-оптический акселерометр для применения в системах мониторинга крупных вращающихся машин // J. Lightwave Technol. – 1997. – Т. 15, № 7. – С. 1120–1130.

2. Тимошенко С. П. Колебания в инженерном деле / С. П. Тимошенко, Д.Х. Янг, У. Уивер. – М.: машиностроение, 1985. – 472 с.

3. Регхупрасад А. Е., Коломберо К., Годио А. Волоконно-оптические акселерометры на основе последовательно соединенных консольных балок с волоконными брэгговскими решетками

4. Лэй Ю.-Ц., Ли Ж.-Ц., Чжан Л.-Ш., Ху П.-Х., Хуан Ц.-С. Optical accelerometers for detecting low-frequency micro-vibrations // Applied Sciences. — 2022. — Т. 12, № 8. — Ст. 3994. — DOI: 10.3390/app12083994.

5. Мамий А. Р., Тлячев В. Б. Операционные усилители. – Майкоп: АГУ, 2005. – 192 с. – ISBN 5-85108-142-2.

УДК 534.6; 004.942

Создание алгоритма обратной задачи для определения геометрии внутренних полостей в стене по данным акустического зондирования

Данченко И. Д., Ходаковский М. А., Косарев В. Р.

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

АО «НПП «Сигнал», г. Санкт-Петербург, Россия

Аннотация: *В работе рассматривается задача восстановления геометрии скрытых полостей в строительных конструкциях по акустическому отклику с целью выявления потенциальных каналов утечки речевой информации. Предложен подход на основе итерационного решения обратной задачи с регуляризацией Тихонова. Численное моделирование показало, что при уровне шума до ± 2 дБ погрешность восстановления толщины полости составляет от 5 до 10 %, а для дефектов, занимающих более 10 % объёма стены, – от 2 до 5 %. Разработанный алгоритм может быть использован для неразрушающего контроля акустической герметичности помещений и выявления скрытых полостей, создающих потенциальные каналы утечки речевой информации.*

Ключевые слова: *обратная задача, акустическое зондирование, регуляризация Тихонова, техническая защита информации, утечка акустической информации.*

Введение

Сегодня в свободном доступе (например, на торговых онлайн-площадках) оказались средства несанкционированного съёма информации и комплектующие, которые позволяют сделать их своими руками. Например, не составляет труда собрать в домашних условиях простые лазерные микрофоны, или приобрести виброакустические датчики и системы перехвата по боковым акустическим каналам, имеющие более высокие значения точности регистрации сигнала по сравнению с самодельными. Поэтому вопросы защиты речевой информации снова приобретают высокую значимость.

Как известно, акустический канал утечки формируется не только за счёт прямого распространения звуковых волн в воздушной среде, но и вследствие вибраций строительных конструкций, инженерных коммуникаций и предметов интерьера, возникающих при прохождении звуковой волны границы разделения сред. Особую опасность с точки зрения защиты акустической информации представляют помещения с низким качеством ограждающих конструкций, наличием скрытых полостей, вентиляционных каналов, кабельных шахт и неплотных стыков, которые создают зоны акустического усиления и могут использоваться для создания канала направленного распространения сигнала.

Как показывают современные исследования, даже незначительные дефекты в стенах – отверстия радиусом 10 мм при толщине конструкции 50 мм, технологические зазоры, трещины – способны резко снижать звукоизоляцию.

В области резонансных частот потери при передаче звука могут падать до отрицательных значений, что означает фактическое усиление акустической энергии на выходе дефекта [1]. Тонкостенные и полые конструкции, которые часто встречаются в современных зданиях, отличаются наличием неоднородностей. При этом надо понимать, что смещение резонаторов или микротрещины в мембранных метаматериалах приводят к падению звукоизоляции на 10–15 дБ [1]. Это служит фактическим доказательством актуальности такого канала утечки.

Традиционные методы контроля состояния стен – ультразвуковая дефектоскопия, визуальный осмотр и тепловизионный анализ – обладают существенными ограничениями. Ультразвуковой метод уверенно выявляет дефекты размером не менее 5–10 мм [2], однако микротрещины менее 1–2 мм часто остаются незамеченными из-за рассеяния волн в неоднородной структуре бетона; кроме того, армирование и сложная геометрия конструкций создают ложные отражения и зоны «акустической тени». Визуальный осмотр позволяет обнаружить лишь поверхностные повреждения, но скрытые полости под слоем штукатурки или отделки остаются незамеченными. Тепловизионный анализ даёт информацию о температурных аномалиях, однако вследствие особенностей физической основы анализатора дефекты диаметром менее 5 мм или расположенные на глубине более 100 мм остаются невидимыми [3]. Следовательно, существующие методы не обеспечивают надёжного выявления малых и сложных по форме полостей, которые могут служить каналами утечки речевой информации.

Цель настоящей работы – создание алгоритма определения геометрии внутренних полостей в стене на основе измеренных акустических сигналов, пригодного для практического использования в системах технической защиты информации. Для достижения цели решаются следующие задачи: построение математической модели распространения акустических волн в трёхслойной системе с дефектами, выбор и обоснование метода регуляризации, разработка итерационной схемы восстановления параметров, численное моделирование и оценка точности метода при различных уровнях шума.

Метод решения

Задача восстановления геометрии внутренних полостей в стене по данным акустического зондирования относится к классу обратных задач математической физики. Прямая задача состоит в моделировании распространения акустической волны через ограждающую конструкцию с известными параметрами. Рассматривается трёхслойная система: среда 1 – воздух помещения, среда 2 – строительная конструкция (стена), среда 3 – внешняя среда (соседнее помещение). Внутри среды 2 могут присутствовать дефекты – области с иными физическими характеристиками (воздушные полости, трещины).

Математическая модель распространения акустической волны описывается однородным волновым уравнением без внутренних источников:

$$\nabla \cdot \left(\frac{1}{\rho(x)} \nabla p(x,t) \right) - \frac{1}{K(x)} * \frac{\partial^2 p(x,t)}{\partial t^2} = 0, \quad (1)$$

где

- $p(x,t)$ – аккустическое давление;
- $\rho(x)$ – плотность среды;
- $\rho(x) = \begin{cases} \rho_1, \text{материал стены} \\ \rho_2, \text{воздушная полость} \end{cases}$;
- $K(x)$ – модуль объемной упругости;
- $K(x) = \begin{cases} K_1, \text{материал стены} \\ K_2, \text{воздушная полость} \end{cases}$.

Параметры среды связаны со скоростью звука соотношением

$$c(x) = \sqrt{\frac{K(x)}{\rho(x)}}. \quad (2)$$

Для бетона приняты значения [4] $\rho_1 = 2400$ кг/м^3, $c_1 = 3200$ м/с; для воздуха – $\rho_2 = 1{,}2$ кг/м^3, $c_2 = 343$ м/с. Таким образом, наличие дефекта проявляется в локальном изменении скорости звука при последовательном прохождении сред различной плотности.

На границе раздела двух сред выполняются условия непрерывности давления и нормальной скорости частиц:

$$p_1 = p_2, \quad (3)$$

$$\frac{1}{\rho_1} * \frac{\partial p_1}{\partial n} = \frac{1}{\rho_2} * \frac{\partial p_2}{\partial n}. \quad (4)$$

Для количественного описания отражения и прохождения волны используется понятие акустического сопротивления $Z = \rho c$. Коэффициент отражения по давлению на границе двух сред с сопротивлениями Z_1 и Z_2 определяется как

$$R = \frac{Z_2 - Z_1}{Z_2 + Z_1}, \quad (5)$$

а коэффициент прохождения – как

$$T = \frac{2Z_2}{Z_2 - Z_1}. \quad (6)$$

Для границы бетон–воздух $Z_1 \gg Z_2$, поэтому

$$R \approx 0.98 - 0.99, \quad (7)$$

$$T \approx 0.01 - 0.02. \quad (8)$$

Это означает, что воздушная полость внутри стены создаёт значительное отражение, что и используется для идентификации дефекта.

При наличии внутренней воздушной полости толщиной d формируются многократные отражения внутри этого слоя. Эффективный коэффициент передачи через полость вычисляется по формуле:

$$T = \frac{T_{12}T_{21}e^{-ik_2 d}}{1 - R_{12}^2 e^{-2ik_2 d}}, \quad (9)$$

где $k_2 = \frac{\omega}{c_2}$ – волновое число; d – толщина полости.

Численное решение прямой задачи выполняется методом конечных разностей на трёхмерной пространственной сетке с дискретизацией по времени, удовлетворяющей условию Куранта. Для каждого узла сетки вычисляется акустическое давление с учётом коэффициентов отражения и прохождения на всех границах раздела. На выходе получается модельный сигнал $p_{\text{мод}}(t;\theta)$, зависящий от искомых параметров дефекта θ (толщина, объём, положение полости).

Обратная задача заключается в восстановлении этих параметров по измеренному акустическому сигналу $p_{\text{изм}}(t)$. Она формулируется как задача минимизации функционала невязки между измеренными и модельными данными. Однако, поскольку задача относится к некорректным (не удовлетворяет условиям единственности и устойчивости по Адамару), малые погрешности измерений могут приводить к катастрофическим ошибкам в решении. Поэтому в функционал вводится регуляризующий член Тихонова:

$$J(\theta) = \sum_t \left| p_{\text{измер}}(t) - p_{\text{модел}}(t;\theta) \right|^2 + \lambda \|L\theta\|^2 \quad (10)$$

где $\lambda > 0$ – параметр регуляризации, а L – оператор сглаживания (обычно тождественный или дифференциальный). Первое слагаемое обеспечивает согласие с экспериментальными данными, второе – ограничивает сложность решения, подавляя нефизичные осцилляции и обеспечивая устойчивость к шумам. Выбор регуляризации Тихонова обоснован её эффективностью в волновых обратных задачах, подтверждённой в работах по ультразвуковой и акустической томографии, где показана возможность восстановления параметров среды при наличии шумов и ограниченном числе измерений.

Итерационный алгоритм решения обратной задачи строится следующим образом:

1. Задаётся начальное приближение θ_0 , соответствующее однородной стене без дефектов ($c = c_{\text{бетона}}, \rho = \rho_{\text{бетона}}$),

2. Для текущего приближения θ_n решается прямая задача и вычисляется модельный сигнал $p_{\text{мод}}(t; \theta_n)$,

3. Вычисляется значение функционала невязки $J(\theta_n)$,

4. Параметры уточняются градиентным методом:

   a. $\Theta_{n+1} = \theta_n - \beta * \left(\frac{\partial J}{\partial \theta}\right)$,

   b. где β – шаг градиентного спуска.

5. Итерации повторяются до выполнения условия сходимости:

   a. $|J(\theta_{n+1} - J(\theta_n)| < \varepsilon$,

   b. где ε – заданная малая величина.

Успешность алгоритма зависит от начального приближения: для сходимости отклонение параметров от истинных не должно превышать 10–30%, что обусловлено ограничением фазовой ошибки

$$\Delta\phi = k\Delta d < \frac{\pi}{2}. \quad (11)$$

Параметр регуляризации α подбирается эмпирически в диапазоне 0,01–0,1 в зависимости от уровня шума. Численное моделирование показало, что при шуме до ±2 дБ толщина полости восстанавливается с погрешностью 5–10% (для крупных дефектов – 2–5%), что подтверждает применимость метода.

Численное моделирование и результаты

Моделирование проводилось для бетонной стены с параметрами: плотность ρ = 2400 кг/м³, скорость звука c = 3200 м/с [1]; для воздуха – ρ = 1,2 кг/м³, c = 343 м/с [4]. Толщина стены варьировалась в диапазоне 0,2–0,5 м, частота зондирующего сигнала – в диапазоне 1–10 кГц. В конструкцию вводились воздушные полости различной толщины и положения. Для каждого набора параметров решалась прямая задача, после чего к полученному сигналу добавлялся аддитивный шум уровня ±2 дБ, и запускалась обратная задача с регуляризацией Тихонова.

В таблице 1 приведены обобщённые результаты восстановления параметров полостей.

Таблица 1 – Полученный результат

Параметр	**Значение**
Точность восстановления толщины и объёма полости (при уровне шума до ±2 дБ)	5–10 %
Для крупных дефектов (>10 % объёма стены)	2–5 %
Выявляемые дефекты	от 0,5 мм и более
Пространственное разрешение	до 0,5 мм
Критерий угрозы (провал звукоизоляции ниже 5–10 дБ в любой октавной полосе)	помещение не защищено

Для практической реализации метода были определены оптимальные параметры измерений, представленные в таблице 2.

Таблица 2 – Рекомендации по проведению измерений

Параметр	**Рекомендация**
Шаг сканирования	5–10 см
Шаг по частоте	10–20 Гц
Частота зондирования	1–10 кГц
Время одного измерения	2–3 секунды
SNR (отношение сигнал/шум)	≥ 40 дБ
Двухэтапный подход	1) Быстрое сканирование → 2) Полный итерационный алгоритм при отклонении >20–30 %

В таблице 3 показана зависимость вероятности пропуска дефекта от количества измерений (шага сканирования). Базовый режим (шаг 20 Гц, шаг 10 см, SNR 40 дБ) даёт вероятность пропуска ≈29 % (худший случай – узкий резонансный пик 50 Гц). Оптимизированный режим (шаг 10 Гц, шаг 5 см, SNR 50 дБ) снижает эту вероятность до 2 %.

Таблица 3 – Корреляция количества измерений и вероятности пропуска дефекта

Шаг (см)	**Пространственных точек**	**Частотных точек**	**Количество измерений**	**Вероятность пропуска**
5	400	900	360 000	2%
10	100	450	45 000	29%
15	49	200	9 800	≈49%
20	25	113	2 825	≈65%
25	16	72	1 152	≈77%
30	16	50	800	≈81%

Как видно из таблиц, соблюдение оптимизированных параметров (шаг 5 см, шаг по частоте 10 Гц, SNR ≥50 дБ) позволяет снизить вероятность пропуска дефекта до 2 %, что подтверждает эффективность предложенных рекомендаций. При этом алгоритм обеспечивает восстановление геометрии полостей

с погрешностью 5–10 % (для крупных дефектов – 2–5 %) и выявляет дефекты размером от 0,5 мм с пространственным разрешением до 0,5 мм. Полученные результаты подтверждают практическую применимость метода для выявления скрытых полостей, создающих потенциальные каналы акустической утечки.

Обсуждение

Полученные результаты демонстрируют, что предложенный алгоритм позволяет выявлять скрытые полости, критичные для акустической герметичности помещений. В отличие от традиционных методов строительного контроля (ультразвуковая дефектоскопия, визуальный осмотр, тепловизионный анализ), которые имеют ограничения по обнаружению малых и сложных по форме дефектов, особенно под слоем отделки, разработанный подход ориентирован на восстановление геометрии внутренних неоднородностей по акустическим данным.

Использование регуляризации Тихонова в итерационной схеме обеспечивает устойчивость решения при наличии шумов измерений, что подтверждено численными экспериментами с добавлением аддитивного шума до ±2 дБ. Применение данного подхода позволяет локализовать потенциальные пути утечки речевой информации и количественно оценивать эффективность звукоизоляции строительных конструкций, что соответствует задачам технической защиты информации, определённым современными требованиями.

Разработанный алгоритм может быть применён при экспертных обследованиях помещений перед проведением работ по обеспечению защиты информации, оценке акустической герметичности стен и перекрытий, а также для мониторинга состояния звукоизоляции в процессе эксплуатации зданий.

Заключение

В работе предложен алгоритм решения обратной задачи акустического зондирования для восстановления геометрии внутренних полостей в стенах. Метод основан на итерационной минимизации функционала невязки с регуляризацией Тихонова. Численное моделирование показало, что при уровне шума до ±2 дБ алгоритм позволяет определять толщину полости с погрешностью 5–10 % для дефектов, занимающих менее 10 % объёма стены, и 2–5 % для более крупных, что подтверждает возможность выявления скрытых неоднородностей.

Полученные результаты могут быть применены для оценки акустической герметичности помещений, выявления потенциальных каналов утечки речевой информации, экспертных обследований перед проведением работ по защите информации, а также для мониторинга состояния звукоизоляции в процессе эксплуатации зданий.

Список литературы

1. Yang C., Zhang X., Tao F. On the acoustic properties of a hole in a wall of finite thickness // Acoustics Australia. – 2016. – Vol. 44, № 1. – P. 1–10.

2. Ahmad N., Abdul Rahim R., Abdul Rahim H., Rahiman M. H. A Review of Ultrasonic Application on Non-Destructive Testing Method for Concrete Structure // Jurnal Teknologi (Sciences & Engineering). – 2014. – Т. 70, № 3. – С. 119–122.

3. Balaras C. A., Argiriou A. Infrared thermography in the built environment: A multi-scale review // Renewable and Sustainable Energy Reviews. – 2022. – Vol. 158. – Article 112167.

4. Sound, Noise, and Ultrasonics. In: McGraw-Hill Handbook of Acoustics. Table 10.6.1. New York: McGraw-Hill, 2015.

5. WiseGuy Reports. Global Counter Surveillance Equipment Market: Future Outlook and Trends to 2035 [Электронный ресурс]. — 2025. — URL: https://www.wiseguyreports.com/reports/counter-surveillance-equipment-market (дата обращения: 17.11.2025).

6. DataIntelo. Counter-Surveillance Sweeping Services Market Research Report 2033 [Электронный ресурс]. — 2024. — URL: https://dataintelo.com/report/counter-surveillance-sweeping-services-market (дата обращения: 17.11.2025).

7. DataIntelo. TSCM Services Market Research Report 2033 [Электронный ресурс]. — 2024. — URL: https://dataintelo.com/report/tscm-services-market (дата обращения: 17.11.2025).

8. Zhang Y., Zhang J., Li Y., Yao D., Zhao Y., Ai Y., Pan W., Li J. Research Progress on Thin-Walled Sound Insulation Metamaterial Structures // Acoustics. — 2024. — Т. 6, № 2. — С. 298–330. — DOI: 10.3390/acoustics6020016. — URL: https://www.mdpi.com/2624-599X/6/2/16 (дата обращения: 17.11.2025).

9. Visual Testing (VT). Основной метод неразрушающего контроля (NDT) [Электронный ресурс] // ASNT. — URL: https://www.asnt.org/what-is-nondestructive-testing/methods/visual-testing (дата обращения: 17.11.2025).

10. Романов В. Г. Ray Statement of the Acoustic Tomography Problem // Доклады Академии наук. Математика (Doklady Mathematics). — 2022. — Т. 106, № 1. — С. 254–258. — DOI: 10.1134/S1064562422040147. — URL: https://pmc.ncbi.nlm.nih.gov/articles/PMC9514200/ (дата обращения: 17.11.2025).

11. Базулин Е. Г., Гончарский А. В., Романов С. Ю., Серёжников С. Ю. Inverse Problems of Ultrasonic Tomography in Nondestructive Testing: Mathematical Methods and Experiment // Russian Journal of Nondestructive Testing. — 2019. — Т. 55, № 6. — С. 453–462. — DOI: 10.1134/S1061830919060020. — URL: https://www.researchgate.net/publication/335584628_Inverse_Problems_of_Ultrasonic_Tomography_in_Nondestructive_Testing_Mathematical_Methods_and_Experiment/ (дата обращения: 17.11.2025).

12. Lavrinovica I., Kalnina D., Zacepins A., Rudzitis N. A Comprehensive Review of Sensor-Based Smart Building Monitoring and Data Gathering Techniques // Sensors. — 2024. — Vol. 24, № 3. — P. 1123. — DOI: 10.3390/s24031123.

13. Aguilar E., Ng W., Orocu R. Designing an IoT-Based System for Monitoring Noise Levels in the Computer Science Faculty and Library of the Technological University of Panama // Sensors. — 2023. — Vol. 23, № 15. — P. 7089. — DOI: 10.3390/s23157089.

14. Суханов Д. Я., Кузова А. Е. High Resolution Acoustic Tomography Based on Backpropagation of Waves [Электронный ресурс]. — Томский государственный университет, 2021. — URL: https://www.researchgate.net/publication/369675697_High_resolution_acoustic_tomography_based_on_backpropagation_of_waves (дата обращения: 17.11.2025).

15. Cisco Systems. What Is a Smart Building [Электронный ресурс]. — URL: https://www.cisco.com/c/en/us/solutions/industries/smart-buildings.html (дата обращения: 17.11.2025).

16. Poudel J. et al. A Survey of Computational Frameworks for Solving the Acoustic Inverse Problem in Three-Dimensional Photoacoustic Computed Tomography // IEEE Reviews in Biomedical Engineering. — 2019.

17. Тихонов А. Н., Арсенин В. Я. Методы решения некорректных задач. — М.: Наука, 1977. — 288 с.

УДК 004.056.53

Оценка устойчивости защиты речевых аудиозаписей к нейросетевой очистке при атаках на голосовую биометрию транспортных систем

Вдовин Д. А., Фесько Н. В.

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

Аннотация: *В работе рассматривается задача оценки защищенности речевых аудиозаписей от восстановления индивидуальных признаков диктора с применением современных нейросетевых методов обработки сигнала. Актуальность исследования обусловлена развитием технологий Zero-Shot Voice Cloning, позволяющих создавать синтетическую копию голоса по короткому эталонному фрагменту. Для проверки устойчивости защищенных аудиозаписей реализован программный комплекс, включающий модуль нейроочистки MetricGAN+ и модуль извлечения биометрических эмбеддингов на основе архитектуры ECAPA-TDNN. В качестве критериев оценки использованы косинусное сходство между векторами признаков, косинусное расстояние и показатель разборчивости речи STOI. Проведены экспериментальные исследования влияния уровня шума, параметров сигнала и форматов аудио на возможность восстановления личности диктора. Полученные результаты позволяют оценивать не только факт искажения речевого сигнала, но и его устойчивость к обратному восстановлению с применением нейросетевых методов.*

Ключевые слова: *речевая биометрия, защита данных, клонирование голоса, нейроочистка, ECAPA-TDNN, MetricGAN+, STOI, косинусное сходство, косинусное расстояние.*

Введение

Развитие генеративных нейросетевых моделей привело к появлению доступных средств синтеза и клонирования речи. Современные системы Text-to-Speech и Voice Cloning способны воспроизводить индивидуальные особенности диктора по коротким аудиофрагментам, что создает угрозу компрометации голосовой биометрии. Особую опасность представляют модели Zero-Shot Voice Cloning, которым для формирования цифровой копии голоса может быть достаточно нескольких секунд эталонной записи.

Традиционные методы защиты речевых данных часто основаны на ухудшении качества сигнала: добавлении шума, снижении частоты дискретизации, компрессии или внесении иных искажений. Однако появление нейросетевых моделей улучшения речи снижает эффективность таких подходов. Модели Speech Enhancement способны подавлять шумы, восстанавливать разборчивость и частично возвращать спектральные признаки, необходимые для идентификации диктора. Поэтому при оценке защищенности речевого сигнала необходимо учитывать не только исходное искажение, но и возможность его последующего восстановления.

Целью работы является оценка устойчивости защищенных речевых аудиозаписей к нейросетевой очистке и восстановлению индивидуальных

признаков диктора. Для достижения цели реализован экспериментальный программный комплекс, позволяющий сравнивать эталонные и обработанные аудиофайлы по векторным биометрическим признакам и объективным метрикам качества речи.

Экспериментальная модель и методика оценки

Экспериментальная модель представляет собой пайплайн обработки речевого сигнала, включающий несколько последовательных этапов: стандартизацию аудио, применение искажений, нейросетевую очистку, извлечение биометрических признаков и расчет итоговых метрик защищенности.

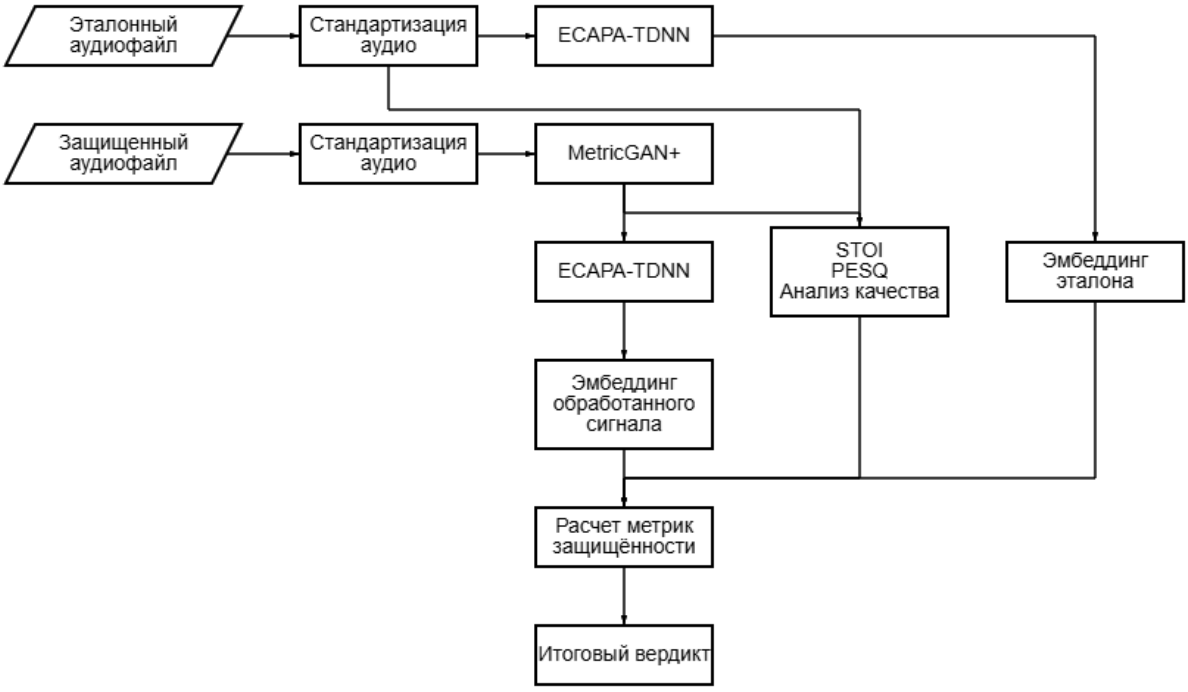


Рис. 1. Структурная схема программного комплекса оценки защищённости речевых биометрических данных

В качестве входных данных использовались речевые аудиозаписи, приведенные к единому формату: моно WAV, PCM 16 бит, частота дискретизации 16 кГц. Такой формат выбран как базовый для корректной работы моделей обработки речи и биометрической идентификации. Для исследования влияния помех были взяты группы аудиофайлов с различным отношением сигнал/шум: около 0 дБ, 10 дБ и 20 дБ.

Нейроочистка выполнялась с использованием модели MetricGAN+, предназначенной для улучшения качества речевого сигнала. Данная модель позволяет оценить сценарий, при котором потенциальный злоумышленник предварительно восстанавливает зашумленную запись перед попыткой извлечения биометрических признаков диктора.

Для извлечения индивидуальных признаков голоса использовалась архитектура ECAPA-TDNN. Она формирует speaker embedding - векторное

представление диктора, объединяющее спектральные, временные и просодические особенности речи. Сравнение эталонного и обработанного аудиосигнала выполнялось с помощью косинусного сходства и косинусного расстояния.

В качестве основного критерия биометрической защищенности использовалось косинусное сходство S_{cos} между эмбеддингами эталонного и обработанного сигналов. Дополнительно рассчитывалось косинусное расстояние $d_{cos}=1-S_{cos}$, позволяющее оценить степень различия между векторами признаков. В реализованном программном комплексе статус «ПРОБОЙ» или «Не защищено» фиксируется при $S_{cos}>0,7$, поскольку в этом случае обработанная запись сохраняет признаки, достаточные для сопоставления с эталоном. При $S_{cos}\leq 0,7$ выставляется статус «ЗАЩИЩЕНО», так как сходство между эмбеддингами считается недостаточным для надежной автоматической идентификации диктора.

Для контроля сохранения смысловой пригодности аудио применялась метрика STOI, отражающая объективную разборчивость речи. Такой подход позволяет учитывать противоречие между двумя требованиями: необходимо скрыть биометрические признаки диктора, но сохранить понятность речи для человека.

Таблица 1 – Основные критерии оценки защищенности речевого сигнала.

Показатель	Значение	Интерпретация
S_{cos}, d_{cos}	Оценка сходства и различия биометрических эмбеддингов	$S_{cos}>0,7$ или d_{cos} -3 - «ПРОБОЙ», $S_{cos}\leq 0,7$ или $d_{cos}\geq 3$ - «ЗАЩИЩЕНО»
STOI	Оценка разборчивости речи	Чем ближе к «1», тем выше разборчивость
SNR	Уровень шумового искажения	Чем ниже SNR, тем сильнее зашумление
ASR/Whisper	Проверка сохранения текста	Используется для анализа распознаваемости слов

Результаты и обсуждение

В базовом сценарии, при отсутствии внешних шумов и значительных искажений, система демонстрирует высокое косинусное сходство и малое косинусное расстояние между эталонным и тестовым аудиосигналом. Это соответствует статусу «ПРОБОЙ» или «Не защищено», поскольку индивидуальные признаки диктора сохраняются и успешно извлекаются моделью ECAPA-TDNN.

При высоком отношении сигнал/шум, превышающем 20 дБ, нейросетевая очистка фактически улучшает качество записи без разрушения биометрических признаков. В таком режиме MetricGAN+ удаляет незначительные помехи, но

сохраняет спектральную структуру голоса. В результате косинусное сходство между эталонной и очищенной записью превышает установленный порог 0,7, а защита оказывается недостаточной.

При среднем уровне шума, около 10-15 дБ, наблюдается переходная зона. С одной стороны, искажения уже влияют на положение биометрического вектора в пространстве признаков. С другой стороны, нейросетевая очистка частично восстанавливает сигнал и может снова приблизить эмбеддинг к эталону. В проведенном эксперименте при SNR = 10 дБ значение составило 0,537, что ниже порога 0,7 и соответствует статусу «ЗАЩИЩЕНО». Однако данный диапазон остается наиболее интересным для оценки эффективности защитных модификаций, поскольку при изменении параметров обработки возможно восстановление признаков диктора до уровня биометрического пробоя.

При низком SNR, менее 5 дБ, наблюдается снижение косинусного сходства и увеличение косинусного расстояния между эмбеддингами эталонного и обработанного сигналов. Такой сигнал может получить статус «ЗАЩИЩЕНО», поскольку восстановление личности диктора становится затруднительным. Однако одновременно ухудшается разборчивость речи, что снижает практическую ценность такого способа защиты. Таким образом, простое зашумление не является универсальным решением: оно может скрыть биометрию, но ценой потери полезной информации.

Таблица 2 – Значения метрик при различных уровнях SNR.

SNR, дБ	S_{cos}	d_{cos}	STOI	Статус
0	0,229	0,771	0,672	Защищено
10	0,537	0,463	0,832	Защищено
20	0,813	0,187	0,939	Не защищено

Из таблицы 2 видно, что при SNR = 0 дБ косинусное сходство составляет 0,229, что ниже установленного порога 0,7 и соответствует статусу «ЗАЩИЩЕНО». При SNR = 10 дБ значение S_{cos} возрастает до 0,537, однако также остается ниже порогового значения, поэтому биометрическая защита формально сохраняется. При SNR = 20 дБ значение S_{cos} достигает 0,813, что превышает установленный порог и соответствует статусу «Не защищено». Одновременно с ростом SNR увеличивается значение STOI, то есть повышается разборчивость речи, однако вместе с этим возрастает и риск восстановления биометрических признаков диктора.

Отдельно рассматривалось влияние формата аудио. Использование сжатых форматов, таких как MP3 и OGG, приводит к потере части высокочастотных гармоник и изменению спектральной структуры сигнала. Это может снижать косинусное сходство и увеличивать косинусное расстояние даже для одного и того же диктора. Следовательно, формат файла необходимо

учитывать при интерпретации результатов, иначе возможно ложное отнесение записи к защищенной.

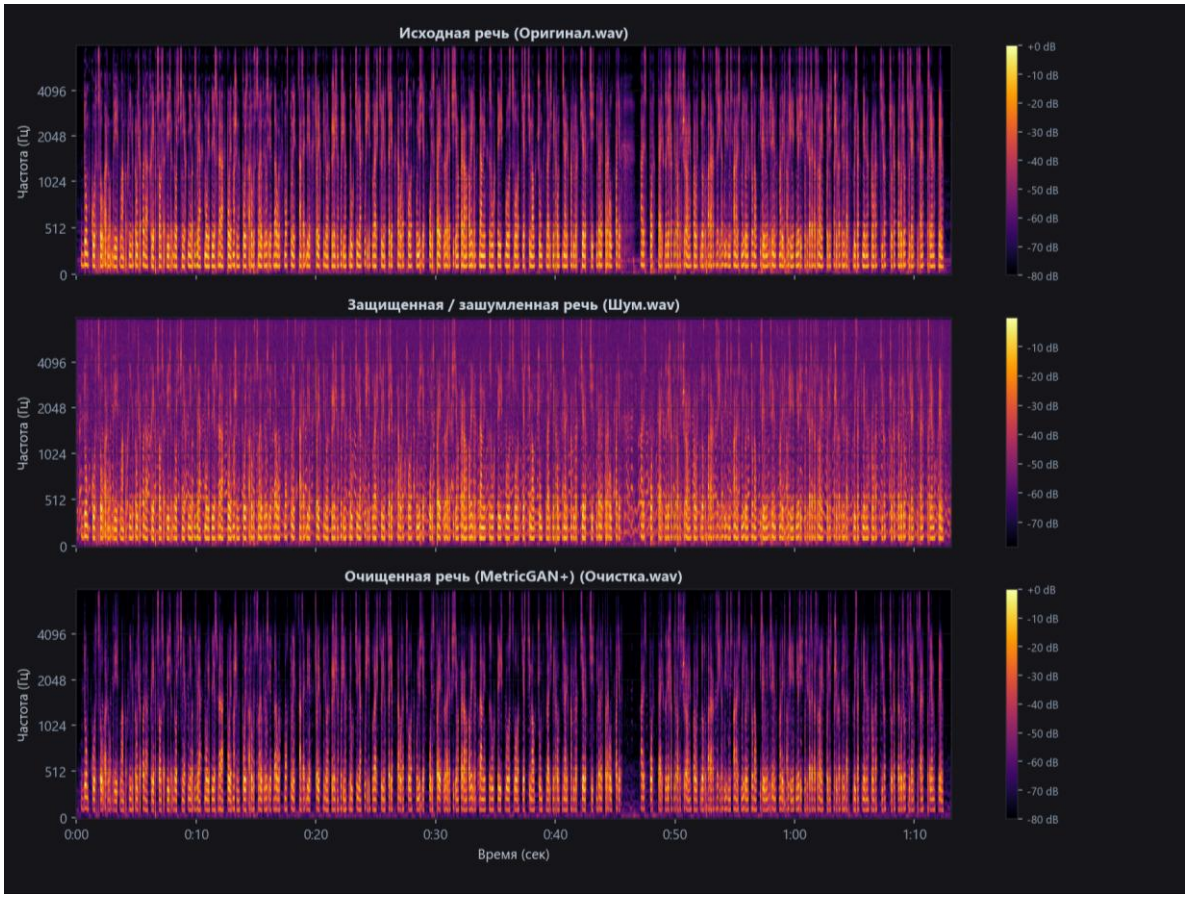


Рис. 2. Сравнение мел-спектрограмм исходного, защищённого и очищенного после нейроочистки MetricGAN+ речевых сигналов

Полученные результаты показывают, что оценка защищенности речевой биометрии должна проводиться после моделирования атакующего сценария. Недостаточно проверить, что исходная зашумленная запись плохо распознается биометрической системой. Необходимо дополнительно проверить, может ли нейросетевая очистка восстановить признаки диктора до уровня, достаточного для идентификации.

Заключение

В работе проведена оценка устойчивости речевых аудиозаписей к восстановлению индивидуальных признаков диктора с применением нейросетевой очистки. Разработанный программный комплекс позволяет моделировать сценарий атаки, при котором защищенный или искаженный сигнал предварительно обрабатывается моделью MetricGAN+, после чего анализируется биометрическим экстрактором ECAPA-TDNN.

Установлено, что при слабых искажениях нейросетевая очистка может сохранять или восстанавливать признаки, необходимые для идентификации диктора. В таких условиях речевой сигнал получает статус «ПРОБОЙ» или «Не защищено», поскольку значение косинусного сходства превышает

установленный порог. При сильном зашумлении возможно снижение косинусного сходства и увеличение косинусного расстояния до уровня, соответствующего статусу «ЗАЩИЩЕНО», однако это сопровождается снижением разборчивости речи. Следовательно, эффективная защита голосовой биометрии должна быть направлена не на простое ухудшение качества аудио, а на целевое нарушение структуры биометрического эмбеддинга при сохранении понятности речи.

Практическая значимость работы заключается в возможности применения предложенного подхода для аудита систем голосовой биометрии и проверки устойчивости речевых данных к атакам с применением современных моделей нейросетевой обработки.

Список литературы

1. Fu S.-W., Liao C.-F., Tsao Y. MetricGAN+: An Improved Version of MetricGAN for Speech Enhancement // arXiv.org. 2021.

2. Desplanques B., Thienpondt J., Demuynck K. ECAPA-TDNN: Emphasized Channel Attention, Propagation and Aggregation in TDNN Based Speaker Verification // arXiv.org. 2020.

3. Wang Y., Chen S., Wu Y. et al. VALL-E X: Speak Foreign Languages with Your Own Voice // arXiv.org. 2023.

4. Casanova E., Weber J., Shulby C. et al. YourTTS: Towards Zero-Shot Multi-Speaker TTS and Zero-Shot Voice Conversion // arXiv.org. 2021.

5. Wan L., Wang Q., Papir A. et al. Generalized End-to-End Loss for Speaker Verification // arXiv.org. 2017.

6. Taal C. H., Hendriks R. C., Heusdens R. et al. A Short-Time Objective Intelligibility Measure for Time-Frequency Weighted Noisy Speech // IEEE ICASSP. 2010.

7. Radford A., Kim J. W., Hallacy C. et al. Robust Speech Recognition via Large-Scale Weak Supervision // arXiv.org. 2022.

УДК 004.934.2

Повышение точности детектирования артефактов AI-преобразования голоса на основе адаптивной модификации оконной функции спектрального анализа

Горбунова Д. А., Паленникова М. Д.

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

Аннотация: *В работе решается задача повышения точности обнаружения синтезированной речи, созданной с помощью технологий искусственного интеллекта. Проведен анализ современных методов AI-преобразования голоса (RVC, VITS, Diff-SVC) и классифицированы их характерные спектральные, временные и фазовые артефакты. Выявлено, что классический спектральный анализ с использованием окна Хэмминга приводит к маскировке слабых признаков синтеза из-за эффекта спектральной утечки. Предложена и математически обоснована модифицированная оконная функция с управляемым параметром α, адаптируемым под характеристики конкретного сигнала. Разработан итерационный алгоритм нахождения оптимального значения параметра на основе метода градиентного спуска. Экспериментальное исследование на эталонном наборе данных ASVspoof 2019 показало, что применение адаптивного окна позволяет снизить равный уровень ошибок (EER) на 1,47% по сравнению со стандартным методом. Интеграция предложенного метода с анализом остатка линейного предсказания обеспечила достижение рекордного значения EER = 13,18%, что подтверждает его эффективность для систем защиты голосовой биометрии.*

Ключевые слова: *голосовая биометрия, дипфейк, AI-преобразование голоса, артефакты синтеза, спектральный анализ, оконная функция Хэмминга, спектральная утечка, адаптивная обработка сигналов, детектирование спуфинг-атак, ASVspoof, LPC-остаток.*

Введение

В условиях глобальной цифровизации и перехода к многофакторным моделям аутентификации голосовая биометрия заняла позиции одного из наиболее перспективных методов верификации личности. В Российской Федерации развитие данных технологий приобрело статус государственного приоритета после вступления в силу Федерального закона № 572-ФЗ, закрепившего правовой статус Единой биометрической системы (ГИС ЕБС). Это сделало вопрос защищенности этих данных критически важным для национальной безопасности.

Однако стремительный рост популярности биометрических технологий сопровождается эскалацией угроз информационной безопасности. Согласно отчету Центрального Банка РФ за 2023 год количество атак с использованием методов социальной инженерии и технических подделок неуклонно растет.

Современный ландшафт киберугроз в РФ характеризуется переходом от примитивного воспроизведения записей (replay-атаки) к использованию

глубоких нейросетевых подделок в реальном времени. Зафиксированы массовые инциденты, такие как атаки «Fake Boss» в мессенджере Telegram и атаки на системы дистанционного банковского обслуживания (ДБО) с использованием клонированного голоса. Данные прецеденты, а также жесткие требования регуляторов (ФСБ, ФСТЭК) и стандартов (ГОСТ Р ИСО/МЭК 30107) обуславливают необходимость создания новых, более чувствительных методов обнаружения атак на биометрическое предъявление (Presentation Attack Detection, PAD).

Ключевая проблема заключается в том, что артефакты, вносимые AI-преобразованием, имеют малую мощность и часто маскируются при стандартном спектральном анализе из-за фундаментальных ограничений используемого инструментария. Основным источником погрешности является эффект «спектральной утечки» (spectral leakage) при применении классического кратковременного преобразования Фурье (STFT) со стандартными оконными функциями (в частности, окном Хэмминга). Это приводит к «замыливанию» спектральной картины и снижению вероятности правильного обнаружения подделок.

Таким образом, актуальность настоящей работы обусловлена необходимостью разработки методов прецизионного уточнения артефактов AI-преобразования. Переход от статических оконных функций к модифицированным адаптивным структурам позволит минимизировать спектральные утечки и повысить чувствительность биометрических систем к специфическим искажениям синтезированной речи, что является необходимым условием обеспечения информационной безопасности в условиях развития технологий искусственного интеллекта [SafeNet, 2024]. Для достижения поставленной цели необходимо классифицировать типичные артефакты синтеза, разработать математическую модель адаптивного окна, создать алгоритм его оптимизации и экспериментально подтвердить его эффективность на верифицированных наборах данных.

Теоретические основы исследования артефактов AI-преобразования голоса

Развитие систем искусственного интеллекта привело к качественному скачку в области цифровой обработки звука: произошёл переход от классических параметрических методов модификации сигнала (pitch-shifting, времяимпульсное растяжение) к методам глубокого генеративного синтеза. Современные технологии преобразования голоса направлены на решение задачи переноса голосовой идентичности (голоса диктора-источника) на лингвистическое содержание целевого сообщения при сохранении просодических особенностей речи.

С точки зрения архитектурного построения и характера формируемого сигнала, современные AI-технологии преобразования голоса можно классифицировать на три доминирующих группы:

1. Retrieval-based Voice Conversion (RVC). На текущий момент является наиболее распространенной технологией благодаря открытому исходному коду

и высокой производительности. Основной особенностью метода является механизм поиска в кодовой книге (Codebook) стилистических векторов целевого голоса, наиболее близких к извлеченным предобученным энкодерром признакам, характеризующим голос диктора.

2. Variational Inference Text-to-Speech/Voice Conversion (VITS). VITS объединяет этапы анализа текста (или речи) и генерации звука в единую стохастическую сеть. Такие системы обеспечивают высокую степень естественности, однако в процессе аппроксимации латентного пространства часто возникают микроаномалии в области высоких частот.

3. Диффузионные модели (Diff-SVC). Основаны на итерационном процессе удаления гауссова шума для восстановления мел-спектрограммы. Дают почти идеальный тембр, но требуют колоссальных ресурсов и часто ошибаются в фазе.

Ключевой проблемой AI-преобразования является спектральное сглаживание. При извлечении и восстановлении мел-кепстральных коэффициентов (MFCC) нейросети склонны к избыточной регуляризации, что приводит к потере тонкой структуры формант и размытию межформантных антирезонансов. Кроме того, дискретная природа вокодеров порождает ложные гармоники (aliasing) в области выше 4–6 кГц.

AI-модели обрабатывают сигнал фреймами фиксированной длины (10–25 мс), что на их границах приводит к разрывам амплитудной огибающей и аномалиям частоты пересечения нуля (ZCR). В вокализованных участках синтезаторы демонстрируют избыточную периодичность, лишенную естественных микрофлуктуаций частоты (джиттера) и амплитуды (шиммера), что служит важным классификационным признаком. Наиболее сложной задачей остается восстановление фазы: вокодеры минимизируют ошибку амплитудного спектра, игнорируя точную фазовую структуру. Возникающий фазовый диссонанс проявляется как «металлический» призвук и аномалии в остатке линейного предсказания (LPC-residual), содержащем высокочастотные компоненты, нехарактерные для естественной речи.

Современный аппарат противодействия атакам на системы голосовой биометрии (атаки типа «спуфинг») опирается на двухэтапную процедуру обработки: извлечение информативных признаков (feature extraction) и последующую классификацию полученных векторов. Для выявления вышеперечисленных артефактов AI-преобразований голоса существуют спектральные, временные и амплитудно-фазовые методы.

Спектральные методы фиксируют деградацию спектральной огибающей и аномалии в распределении энергии гармоник. Мел-частотные кепстральные коэффициенты (MFCC) имитируют слуховое восприятие, но мел-фильтрация сглаживает высокочастотные артефакты нейровокодеров. Линейно-частотные кепстральные коэффициенты (LFCC) используют линейную шкалу, что улучшает анализ высокочастотных аномалий. Метод кепстральных коэффициентов на основе постоянного Q-преобразования (CQCC), ставший

стандартом после ASVspoof 2019, обеспечивает переменное частотно-временное разрешение, эффективно локализуя формантные аномалии.

Временные методы анализируют динамику сигнала. ZCR выявляет аномальную гладкость или скачки на границах фреймов. Анализ огибающей энергии обнаруживает неестественную стабильность амплитуды, лишенную физиологического тремора. Однако временные методы чувствительны к шумам и качеству канала.

Фазовые методы исследуют тонкие аспекты генерации. LPC-остаток содержит следы фазового диссонанса; его статистические параметры (эксцесс, асимметрия) служат дескрипторами подделки. Анализ групповой задержки выявляет нарушения когерентности гармоник, неразличимые на амплитудных спектрограммах.

Однако даже современные классификаторы (GMM, RawNet2) показывают низкую точность на реальных данных. Причина — в низком отношении «сигнал-артефакт», обусловленном спектральными утечками классического окна Хэмминга при STFT: энергия доминирующих формант маскирует слабые аномалии синтеза.

Следовательно, для устранения имеющихся погрешностей в детектировании подделок необходимо перейти от анализа признаков к оптимизации самого процесса их извлечения. Уточнение артефактов возможно лишь через минимизацию спектрального растекания, что требует разработки и применения модифицированной оконной функции с адаптируемыми коэффициентами.

Теоретические исследования направлений модификации оконной функции

Классическое окно Хэмминга в дискретном виде описывается выражением:

$$w[n] = \alpha_0 - (1 - \alpha_0)cos\left(\frac{2\pi n}{N-1}\right), 0 \leq n \leq N-1 \qquad (1)$$

где N – длина последовательности отсчетов.

Окно Хэмминга имеет уровень боковых лепестков –43 дБ, что приводит к спектральным утечкам.

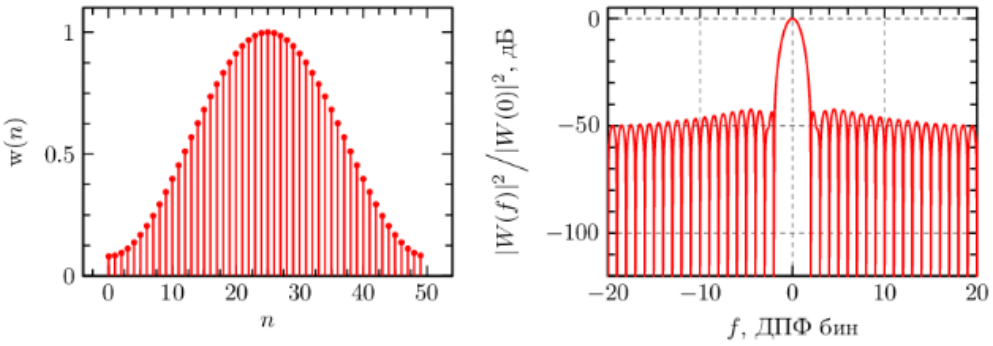


Рис. 1. Окно Хемминга

Для устранения выявленных ограничений статических оконных функций в работе синтезирована модифицированная весовая функция $w_{opt}[n]$ с управляемым параметром формы.

$$w_{opt}[n] = w_{hamming}[n] \cdot \left(1 + \alpha cos\left(\frac{2\pi n}{N-1}\right)\right), 0 \le n \le N-1, \quad (2)$$

где N – длина последовательности отсчетов.

Подстановка стандартного выражения для окна Хэмминга в (2.2) позволяет получить развернутую аналитическую форму:

$$w_{opt}[n] = \left[0{,}54 - 0{,}46cos\left(\frac{2\pi n}{N-1}\right)\right] \cdot \left[1 + \alpha co\, s\left(\frac{2\pi n}{N-1}\right)\right] \quad (3)$$

Введение коэффициента α позволяет динамически изменять весовую структуру окна, что приводит к следующим эффектам в частотной области:

При α>0 сужается главный лепесток, повышая частотную избирательность. Данный режим эффективен для сепарации близкорасположенных гармоник и анализа микроструктуры формант синтезированной речи.

При α<0 увеличивается крутизна спада боковых лепестков, подавляя спектральные утечки.

Это позволяет динамически адаптировать форму окна под характеристики анализируемого сигнала.

Для количественной оценки эффективности модификации введены три критерия:

1. Спектральный гребневый фактор (пик-фактор, PF). Характеризует контрастность резонансных пиков. Естественная речь обладает высокой добротностью формантных резонансов, нейросетевые вокодеры генерируют более «плоские» пики; максимизация PF через подбор α усиливает разделимость этих классов.
2. Ширина спектральной линии (BW). Определяет частотную разрешающую способность. Сужение линии за счет α позволяет локализовать узкополосные фазовые аномалии, скрытые при стандартном анализе.
3. Локальное отношение сигнал/шум (SNR_{leak}). Модификация окна направлена на рост SNR_{leak} за счет подавления уровня боковых лепестков в целевых частотных диапазонах.

На основе введенных критериев строится обобщенная целевая функция J(α) методом аддитивной свертки нормированных показателей:

$$J(\alpha) = w_1 \frac{PF(\alpha)}{PF_0} + w_2 \frac{BW_0}{BW(\alpha)} + w_3 \frac{SNR(\alpha)}{SNR_0}, \quad (4)$$

где:

− *PF(α), BW(α), SNR(α)* – значения критериев для текущего α;

− PF_0, BW_0, SNR_0 – эталонные значения для окна Хэмминга;

− w_1, w_2, w_3 – весовые коэффициенты, при условии $\sum_{i=1}^{3} w_i = 1$.

Выбор вектора весов $W=\{w_1, w_2, w_3\}$ напрямую зависит от специфики решаемой задачи защиты информации:

− приоритет частотного разрешения ($w_2 \rightarrow max$) — для локализации высококачественных подделок;

− приоритет подавления утечек ($w_3 \rightarrow max$) — для выявления слабых высокочастотных артефактов;

− приоритет контрастности ($w_1 \rightarrow max$) — для классификации «сглаженных» спектров.

Таким образом, задача оптимизации сводится к нахождению такого значения α^*, которое максимизирует функционал $J(\alpha)$ на заданном интервале допустимых значений:

$$\alpha^* = \arg \max_{\alpha \in [\alpha_{min}, \alpha_{max}]} J(\alpha). \quad (5)$$

Для нахождения α^* используется итерационный метод градиентного подъема:

$$\alpha_{t+1} = \alpha_t + \eta \cdot \nabla J(\alpha_t), \quad (6)$$

где:

α_t – значение параметра на текущем шаге;

η – адаптивный шаг, определяющий скорость сходимости;

$\nabla J(\alpha_t)$ – численный градиент целевой функции.

Поскольку функционал $J(\alpha)$ является скалярной функцией одного параметра, расчет градиента выполняется методом центральных разностей:

$$\nabla J(\alpha_t) \approx \frac{J(\alpha_t + \Delta\alpha) - J(\alpha_t - \Delta\alpha)}{2\Delta\alpha}, \quad (7)$$

где $\Delta\alpha$ – бесконечно малое приращение параметра.

Выбор метода градиентного спуска для систем антиспуфинга обусловлен:

− минимальным числом вычислений целевой функции (10–50 итераций);

− гладкостью поверхности отклика $J(\alpha)$;

− возможностью интеграции в конвейер извлечения признаков без задержек аутентификации.

Адаптивная настройка окна минимизирует спектральные утечки, повышая информативность LPC-остатка и стабильность MFCC-признаков, что создает условия для более точной классификации в системах антиспуфинга.

Экспериментальное исследование эффективности модифицированной оконной функции в задачах детекции синтезированной речи

Эксперимент проведен на эталонном наборе данных **ASVspoof 2019 (Logical Access)**, содержащем записи живой речи (Bonafide) и синтезированные подделки (Spoof), созданные 19 алгоритмами (от классических вокодеров на базе линейного предсказания до современных генеративно-состязательных сетей (GAN) и нейронных моделей преобразования голоса (Voice Conversion)).

Оценка проводилась для трех конфигураций предобработки:

− Статическое окно Хэмминга (Baseline).

− Статическое окно Ханна (промышленный эталон).

− Предложенное адаптивное окно $w_{opt}[n]$ с оптимизацией α.

Извлечение признаков: объединенный вектор из 20 мел-частотных кепстральных коэффициентов (MFCC) и 20 кепстральных коэффициентов на основе постоянного Q-преобразования (CQCC).

Классификатор: модель Гауссовых смесей (GMM) с 512 компонентами, обученная отдельно на подмножествах Bonafide и Spoof.

Для оценки качества систем защиты информации использовались следующие метрики:

− EER (Equal Error Rate) — основной показатель, точка равенства ложного принятия (FAR) и ложного отклонения (FRR).

− AUC (Area Under the Curve) — площадь под ROC-кривой, оценка разделимости классов.

В ходе итерационного подбора параметров (длина кадра, диапазон α, веса критериев) была определена оптимальная конфигурация: длина кадра 2048 отсчетов, диапазон $\alpha \in [-0.4; 0.4]$.

Сводные результаты представлены в таблице 1.

Таблица 1 – Сравнительная эффективность систем детекции

Конфигурация системы	**Оконная функция**	**EER (%)**	**AUC(%)**	**Прирост к Baseline (абс. %)**
Baseline (Static)	Хэмминг (статический)	15,21	92,7	—
Industry Standard	Ханн (статический)	13,91	93,8	+1,30
Proposed Method	Адаптивный Хэмминг	13,74	94,2	+1,47
Proposed Method+ LPC	Адаптивный Хэмминг	13,18	—	+2,03

Ключевые выводы по результатам:

1. Применение адаптивного окна $w_{opt}[n]$ снижает EER на 1,47% относительно классического окна Хэмминга и на 0,17% относительно промышленного эталона (окна Ханна).

2. Интеграция с анализом остатка линейного предсказания (LPC-residual) позволяет достичь рекордного значения EER = 13,18%, что подтверждает синергию прецизионного спектрального анализа и временных аномалий синтеза.

3. Наиболее значимый прирост точности зафиксирован для атак на основе RVC и нейровокодеров с высоким сглаживанием (oversmoothing). Адаптивное окно локализует фазовый диссонанс и аномалии в межформантных интервалах, ранее маскируемые спектральными утечками.

4. Вычислительная эффективность: среднее время поиска α составляет 0,28 с на 1 с аудиосигнала (при 4 ядрах CPU), что позволяет интегрировать метод в системы реального времени.

5. ROC-анализ покаал, что предложенный метод обеспечивает более высокую стабильность в области низких значений ложного принятия (FAR), что критично для биометрических систем.

Заключение

В работе решена задача повышения точности детектирования артефактов AI-преобразования голоса. Установлено, что классическое окно Хэмминга маскирует слабые признаки синтеза из-за спектральных утечек. Предложена модифицированная оконная функция $w_{opt}[n]$ с управляемым параметром α, адаптируемым под характеристики сигнала, и разработан алгоритм ее оптимизации на основе градиентного спуска.

Эксперимент на ASVspoof 2019 подтвердил эффективность метода: EER снижен с 15,21% до 13,74% (прирост 1,47%), AUC повышен с 92,7% до 94,2%. Интеграция с LPC-остатком обеспечила рекордное значение EER = 13,18%. Метод вычислительно эффективен (0,28 с на 1 с аудио) и рекомендуется для внедрения в системы защиты голосовой биометрии, включая ГИС ЕБС.

Список литературы

1. Müller N. M., Czempin P., Dieckmann F., Froghyar A., Böttinger K. "Does Audio Deepfake Detection Generalize?" // Proc. Interspeech 2022. - 2022. - P. 2783-2787.

2. Yoshioka D., Yasuda Y., Matsunaga N., Ohtani Y., Toda T. Spoken-Text-Style Transfer with Conditional Variational Autoencoder and Content Word Storage // Proc. INTERSPEECH. – 2022. – URL: https://www.isca-archive.org/interspeech_2022/yoshioka22_interspeech.html.

3. Sahidullah M., Kinnunen T., Hanilçi C. "A comparison of features for synthetic speech detection" // IEEE/ACM Transactions on Audio, Speech, and Language Processing. - 2015. - Vol. 23. - No. 12. - P. 2062-2075.

4. Harris F. J. "On the use of windows for harmonic analysis with the discrete Fourier transform" // Proceedings of the IEEE. - 1978. - Vol. 66, Issue 1. - P. 51-83.

5. Nuttall A. H. "Some windows with very good sidelobe behavior" // IEEE Transactions on Acoustics, Speech, and Signal Processing. - 1981. - Vol. 29, Issue 1. - P. 84-91.

6. Todisco M., Delgado H., Evans N. "Constant Q cepstral coefficients: A spoofing countermeasure for automatic speaker verification" // Computer Speech & Language. - 2017. - Vol. 45. - P. 516-535.

7. Wang X., Yamagishi J. "ASVspoof2019: A large-scale public database of synthesized, converted and replayed speech" // Computer Speech & Language. - 2020. - Vol. 64. - P. 101114.

8. Helmrich C. R. "On the use of sums of sines in the design of signal windows " // Proceedings of the 13th International Conference on Digital Audio Effects (DAFx-10). – Graz, Austria. - 2010. - P. 215-227.

9. Hemavathi R., Kumaraswamy R. "Voice conversion spoofing detection by exploring artifacts estimates" // Multimedia Tools and Applications. – 2021. – Vol. 80. – P. DAFX-1- DAFX-4.

10. Аршакян А. А., Ларкин Е. В. "Определение соотношения сигнал-шум в системах наблюдения" // Известия Тульского государственного университета. Технические науки. – 2012. – №. 3. – С. 168-174.

11. Chandrapalan K. "Deepfake Speech Detection: A Literature Review" // IEEE Access. - 2025. - Vol. 10. - P. 10123-10145.

12. Сергиенко А. Б. "Цифровая обработка сигналов: Учебник для вузов" // СПб.: Питер. –2003 –608 с.

13. Карпов А. А., Юсупов Р. М. "Многомодальные интерфейсы человеко-машинного взаимодействия" // Вестник российской академии наук. – 2018. – Т. 88. – № 2. – С. 146-155.

14. Лаврентьева Г. В., Новоселов С. А., Кудашев О. Ю. "Методы детектирования спуфинг-атак повторного воспроизведения на голосовые биометрические системы" // Научно-технический вестник информационных технологий, механики и оптики. – 2018. – Вып. 18 №3. – С. 428-436.

15. Минаев В. А., Бондарь И. В., Федорович В. Ю. "Биометрия защиты объектов: возможности и перспективы" // Информация и безопасность – 2025. – С. 47-56.

16. Шульженко А. Д., Горбунова Д. А., Новосельцева А. М., Давидчук А. Г. "Модифицированная оконная функция на базе окна Хемминга для повышения точности определения спектра голоса на аудиозаписи" // Моделирование, оптимизация и информационные технологии. – 2025. – Т. 13. – № 3. – DOI: 10.26102/2310-6018/2025.50.3.037.

УДК 004.934.2

Оценка информативности спектрально-статистических характеристик аудиосигнала до сжатия с потерями и после для обнаружения нейросгенерированной речи

Ишутин И. А., Сильвестрова Д. Д., Шульженко А. Д., Игнатьев А.А.

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

Аннотация: *В работе исследована возможность использования характеристик аудиосигналов до сжатия и после для обнаружения нейросгенерированной речи. Анализ основан на вычислении коэффициентов модифицированного дискретного косинусного преобразования (далее – МДКП) и оценке комплекса спектральных характеристик аудиосигнала. Выполнено экспериментальное сравнение человеческой и синтезированной речи, представленной в форматах wav, mp3, ogg и m4a. Установлено, что наиболее выраженные различия между человеческой и нейросгенерированной речью наблюдаются по признакам снижения энтропии, распределения коэффициентов и искажения энергии. Полученные результаты свидетельствуют о возможности использования спектрально-статистических признаков при разработке средств предварительного обнаружения голосовых дипфейков и защиты систем голосовой биометрии.*

Ключевые слова: *нейросгенерированная речь, голосовой дипфейк, аудиофорензика, модифицированное дискретное косинусное преобразование, информативность признаков, энтропия сигнала, спектральный анализ.*

Введение

Развитие технологий синтеза речи и голосового клонирования сделало нейросгенерированный голос доступным широкому кругу пользователей, что наряду с легитимным применением породило новый класс атак социальной инженерии – голосовой фишинг с использованием синтезированного голоса доверенного лица. Одновременно расширяется применение голосовой биометрии для аутентификации, для которой согласно приказу Минцифры России от 12.05.2023 № 453 вероятность ложного совпадения и ложноположительной идентификации не должна превышать 0,1, что при массовом использовании систем означает необходимость применения дополнительных, независимых от основного биометрического движка методов проверки подлинности голоса.

Существующие подходы к обнаружению синтезированной речи делятся на узкоспециализированные модели глубокого обучения, обладающие высокой точностью, но низкой интерпретируемостью решений, и методы, основанные на явных статистических и спектральных признаках сигнала, уступающие по точности, но допускающие содержательную интерпретацию результата. Ко второй группе относится ряд методов, разработанных в задачах цифровой аудиофорензики для решения иной задачи – установления факта и метода сжатия аудиофайла с потерями. Поскольку признаки, применяемые для решения этой задачи, отражают структурные свойства спектра и статистику коэффициентов

преобразования сигнала, представляет интерес оценить их применимость и информативность для разграничения человеческой и нейросгенерированной речи.

Цель работы – оценить информативность спектрально-статистических характеристик аудиосигнала для задачи обнаружения нейросгенерированной речи раздельно на двух этапах: до применения сжатия с потерями и после него.

Методика исследования

В основу исследования положен набор алгоритмов спектрального анализа, разработанных для выявления артефактов аудиосжатия. Анализ выполнялся в частотной области после вычисления коэффициентов МДКП. Сигнал разбивается на перекрывающиеся на 50% блоки длиной 576–2048 отсчётов в зависимости от целевого формата, к каждому блоку применяется оконная функция Ханна, после чего вычисляется МДКП блока.

На основе последовательности блоков МДКП вычислялись семь характеристик сигнала:

− снижение энтропии – нормированная энтропия Шеннона гистограммы амплитуд коэффициентов МДКП;

− искажение энергии – средняя относительная энергия разности спектров соседних блоков;

− распределение коэффициентов – доля коэффициентов МДКП, по модулю не превышающих заданный порог;

− фазовые сдвиги – дисперсия межблоковых приращений фазы, восстановленной преобразованием Гильберта;

− эффект преэхо, локальная вариативность и сила пика спектрального потока метрики, характеризующие резкость атак сигнала на границах блоков разной длины.

В задаче компрессионной форензики значения этих характеристик сравниваются с пороговыми коэффициентами, откалиброванными отдельно для каждого кодека, для принятия бинарного решения о факте и способе сжатия. В настоящей работе пороговые решающие правила не применялись – использовались непосредственно усреднённые по записи значения характеристик, что позволяет сравнивать их информативность напрямую, без потери данных при бинаризации. Для экспериментальной проверки была сформирована выборка из 122 записей человеческой речи. Для каждой записи была получена синтезированная нейросетью версия с сохранением исходного речевого содержания. Дополнительно каждая запись была представлена в форматах wav, mp3, ogg и m4a, что позволило оценить влияние алгоритмов сжатия на исследуемые характеристики.

Для каждого аудиофайла рассчитывались значения всех исследуемых признаков, после чего определялись средние значения по выборке и выполнялось сравнение человеческой и нейросгенерированной речи.

Результаты исследования

Полученные результаты показали, что несжатые нейросгенерированные аудиосигналы обладают спектральными характеристиками, отличающимися от характеристик естественной человеческой речи.

Экспериментальная выборка состояла из 122 записей человеческой речи и 122 синтезированных по ним нейросетевых записей того же речевого содержания. Каждая запись была представлена в четырёх форматах: несжатом wav и трёх форматах сжатия с потерями – mp3, ogg, m4a. Для каждого аудиофайла вычислялись усреднённые по всем блокам значения семи характеристик, после чего результаты усреднялись по классу (человек/ИИ) и формату.

Таблица 1 – Усреднённые значения характеристик для человеческой речи

Характеристика (размерность)	**wav**	**mp3**	**ogg**	**m4a**
Снижение энтропии	0,172	0,115	0,112	0,114
Фазовые сдвиги, Рад	6,796	6,116	5,988	6,787
Распределение коэффициентов	0,321	0,640	0,637	0,643
Эффект преэхо	0,426	0,379	0,284	0,538
Локальная вариативность	0,427	0,214	0,254	0,341
Сила спектрального потока	0,437	0,395	0,332	0,283
Искажение энергии (отн. ед.)	283	317	319	303

Таблица 2 – Усреднённые значения характеристик для ИИ-генерированной речи

Характеристика (размерность)	**wav**	**mp3**	**ogg**	**m4a**
Снижение энтропии	0,134	0,140	0,142	0,138
Фазовые сдвиги, Рад	6,652	6,651	6,600	6,795
Распределение коэффициентов	0,531	0,484	0,494	0,492
Эффект преэхо	0,442	0,424	0,417	0,417

Характеристика (размерность)	**wav**	**mp3**	**ogg**	**m4a**
Локальная вариативность	0,394	0,397	0,410	0,390
Сила спектрального потока	0,423	0,425	0,431	0,428
Искажение энергии (отн. ед.)	201	192	193	184

Из сравнения таблиц 1 и 2 видно, что для ИИ-сигнала значения характеристик «Снижение энтропии», «Распределение коэффициентов» и «Искажение энергии» в несжатом формате демонстрируют значения, более близкие к характерным для сжатых сигналов, чем к несжатой человеческой речи. Это объясняется тем, что нейросети генерируют более упорядоченный, сглаженный спектр с подавленными микрошумами дыхания и паузами, что имитирует эффект, достигаемый при компрессии с потерями.

Для количественной оценки разделяющей способности признаков была рассчитана относительная разница между классами на несжатых файлах (таблица 3), а также оценено изменение признаков при переходе от wav к сжатым форматам для ИИ-сигнала (таблица 4).

Таблица 3 – Разница характеристик между несжатыми человеческой и ИИ-речью

Характеристика	**Разница (человек – ИИ), %**
Снижение энтропии	38,7
Искажение энергии	36,1
Распределение коэффициентов	43,9
Локальная вариативность	8,4
Сила спектрального потока	3,3
Эффект преэхо	3,6
Фазовые сдвиги	2,2

Таблица 4 – Относительное изменение характеристик ИИ-сигнала при сжатии

Характеристика	**Разница (человек – ИИ), %**
Снижение энтропии	4,3
Искажение энергии	6,3
Распределение коэффициентов	8,4
Локальная вариативность	1,5
Сила спектрального потока	1,2
Эффект преэхо	5,5
Фазовые сдвиги	0,4

Заключение

Проведенное исследование показало, что спектрально-статистические характеристики аудиосигнала, первоначально разработанные для решения задач цифровой аудиофорензики и выявления следов сжатия с потерями, обладают информативностью при обнаружении нейросгенерированной речи. В отличие от традиционного применения, где указанные характеристики используются для определения факта и метода компрессии, в настоящей работе они рассматривались как количественные показатели структуры речевого сигнала, позволяющие сравнивать естественную и синтезированную речь без использования пороговых правил классификации.

Экспериментальное исследование на выборке из 122 пар записей показало, что в несжатом формате wav синтезированная речь отличается от естественной по ряду спектрально-статистических характеристик. Наибольшей информативностью обладают снижение энтропии коэффициентов МДКП, распределение коэффициентов преобразования и характеристика искажения энергии. Для этих показателей различия между человеческой и нейросгенерированной речью составили 38,7 %, 43,9 % и 36,1 % соответственно, что существенно превышает различия по остальным исследованным характеристикам. Полученные результаты свидетельствуют о том, что современные системы синтеза речи формируют более упорядоченную спектральную структуру сигнала с меньшей степенью случайности, характерной для естественной человеческой речи.

Дополнительный анализ показал, что последующее сжатие синтезированной речи кодеками mp3, ogg и m4a оказывает значительно меньшее влияние на значения наиболее информативных характеристик, чем можно ожидать для естественного речевого сигнала. Изменение их значений после компрессии не превышало 8,5 %, тогда как различия между человеческой и синтезированной речью достигали более 36 %. Это позволяет сделать вывод, что нейросгенерированный сигнал уже на этапе формирования обладает спектральными свойствами, близкими к тем, которые возникают после применения алгоритмов сжатия с потерями. Иными словами, часть статистических закономерностей, используемых кодеками для уменьшения избыточности аудиосигнала, воспроизводится современными моделями синтеза речи в процессе генерации.

Полученные результаты подтверждают возможность использования рассмотренных характеристик аудиосигнала в качестве интерпретируемых признаков предварительного обнаружения нейросгенерированной речи. Их применение не требует обучения специализированных моделей машинного обучения, обеспечивает физически объяснимую интерпретацию получаемых результатов и может использоваться как самостоятельный этап анализа либо в составе комплексных систем обнаружения голосовых дипфейков совместно с существующими методами автоматической классификации. Комплексное использование наиболее информативных характеристик позволяет повысить надежность выявления синтезированной речи и представляет практический интерес для построения средств защиты систем голосовой биометрии и предварительного обнаружения голосовых дипфейков.

Список литературы

1. В России появилась государственная единая биометрическая система // Правительство России. URL: http://government.ru/news/44280/ (дата обращения: 11.11.2025).

2. ICT – Voice Biometrics Market // Reports and data. URL: https://www.reportsanddata.com/report-detail/voice-biometrics-market (дата обращения: 15.11.2025).

3. Тренды фишинговых атак на организации // positive technologies. URL: https://www.ptsecurity.com/ru-ru/research/analytics/phishing-attacks-on-organizations-in-2022-2023/ (дата обращения: 20.11.2025).

4. Wu, Z. ASVspoof: the Automatic Speaker Verification Spoofing and Countermeasures Challenge / Z. Wu, J. Yamagishi, T. Kinnunen, C. Hanilc, M. Sahidullah, A. Sizov, N. Evans, M. Todisco // IEEE Journal of Selected Topics in Signal Processing. – 2017.

5. Abdullah, H. Practical Hidden Voice Attacks against Speech and Speaker Recognition Systems / H. Abdullah, W. Garcia, C. Peeters, P. Traynor, K. Butler, J. Wilson // The Network and Distributed System Security Symposium, NDSS 2019, 24–27 February 2019. – San Diego, USA, 2019.

6. Li, L. A study on replay attack and anti-spoofing for automatic speaker verification / L. Li, Y. Chen, D. Wang // 18th Annual Conference of the International Speech Communication Association (Interspeech 2017). – Stockholm, Sweden, 2018.

УДК 004.056.5

Экспериментальная оценка способа детекции ИИ-подделок голосовых аудиозаписей с использованием статистик LPC остатков

Мирошников Н. Ю., Нахапетян Ю. А., Шульженко А. Д., Игнатьев А. А.

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

Аннотация: *В работе рассматривается задача определения факта преобразования голоса с помощью интеллектуальных средств (AI-VC) на примере технологии RVC. Проанализированы акустические и статистические признаки речи, изменяющиеся при преобразовании: кепстральные коэффициенты, статистические свойства LPC-остатка, параметры основного тона (джиттер, шиммер), спектральный центроид и поток, скорость пересечения нуля. Построена формальная модель бинарной классификации аудиозаписей и разработано программное средство на языке Python, реализующее классификатор на основе смеси гауссовых распределений (GMM). Сформирован экспериментальный набор из 90 аудиозаписей (45 естественных и 45 преобразованных с помощью RVC), использованный для настройки классификатора перед дообучением на выборке ASVspoof2019. По результатам оценки получены значения AUC = 0,9378 и EER = 0,1391 для базовой модели признаков (MFCC, CQCC, ZCR) и AUC = 0,9389, EER = 0,1352 для модели, дополненной статистиками LPC-остатка, что подтверждает эффективность разработанного способа.*

Ключевые слова: *искусственный интеллект, преобразование голоса, RVC, спуфинг, акустические признаки, LPC-остаток, GMM, бинарная классификация, информационная безопасность, биометрия голоса.*

Введение

Атаки с использованием интеллектуальных средств преобразования голоса (AI-VC) представляют собой одну из новых угроз информационной безопасности, обусловленную растущей доступностью подобных технологий для широкого круга пользователей. Такие атаки объединяют приёмы социальной инженерии и технические возможности синтеза речи, что позволяет злоумышленнику убедительно имитировать голос доверенного лица. С каждым годом растёт количество фишинговых атак и ущерб от них [1], а всё чаще среди них встречаются случаи мошенничества с использованием подделанного голоса [2]. Известны случаи, когда злоумышленники, воспользовавшись синтезированным нейросетью голосом руководителя компании, вынуждали сотрудников совершать денежные переводы на сотни тысяч долларов [3]. Согласно докладу IBM за 2024 год, средняя глобальная стоимость утечки данных вследствие фишинга составляет 4,76 млн долларов [4], а применение средств преобразования голоса лишь повышает убедительность подобных атак, делая их более эффективными.

Целью работы является повышение эффективности защиты от атак с использованием интеллектуальных средств преобразования голоса за счёт

разработки способа и программного средства для определения факта преобразования речи.

Метод определения факта преобразования голоса

В качестве исследуемого средства преобразования голоса выбрана технология RVC (Retrieval-based Voice Conversion) — нейросетевая модель с открытым исходным кодом, использующая архитектуру Encoder–Decoder (HuBERT, Flow-Decoder VITS) совместно с вокодером HiFi-GAN и механизмом поиска ближайших стилистических представлений [5]. Выбор обусловлен доступностью, высокой реалистичностью преобразования, относительно низкой вычислительной сложностью и широким практическим применением данного средства.

Операции декодирования и вокодирования, применяемые в RVC, изменяют мел-спектрограмму и фазовую структуру сигнала, что проявляется в измеримых отклонениях акустических признаков [6]. Для выявления таких отклонений в работе рассмотрены: мел-частотные кепстральные коэффициенты (MFCC) и кепстральные коэффициенты на основе постоянного-Q (CQCC), статистические свойства LPC-остатка (среднее, дисперсия, асимметрия, острота), параметры основного тона — джиттер и шиммер, спектральный центроид и поток, а также скорость пересечения нуля (ZCR). Перечисленные признаки применяются в известных методах детекции спуфинга [7], тогда как статистики LPC-остатка остаются малоисследованными в задаче определения преобразования речи.

Задача определения факта преобразования голоса формализована как задача бинарной классификации: аудиофрагмент, представленный вектором акустических признаков, относится классификатором к классу «естественная речь» либо «преобразованная речь» на основании разности логарифмов правдоподобия, вычисленных для двух моделей смеси гауссовых распределений (GMM), обученных раздельно на естественной и на преобразованной речи. Для оценки вклада статистик LPC-остатка реализованы две модели классификатора: Baseline (признаки MFCC, CQCC, ZCR) и Baseline+LPC (дополнительно включает статистики LPC-остатка).

Экспериментальные исследования

Для настройки моделей был сформирован экспериментальный набор аудиоданных с участием 45 студентов первого курса, давших согласие на обработку обезличенных биометрических данных. Запись выполнялась на смартфон iPhone 12 в формате M4A; дикторы читали стандартизированный текст (отрывок из романа Л. Н. Толстого «Война и мир»), содержащий все фонемы русского языка. Полученные записи были преобразованы в формат WAV (16 бит PCM) и разбиты на сегменты по 3 секунды, после чего каждый сегмент обработан с помощью веб-интерфейса RVC. Итоговый набор данных составил 90 аудиофайлов (45 естественных и 45 преобразованных) общей длительностью 90 минут, обеспечив парную сбалансированную структуру

выборки, использованную для настройки классификатора перед дообучением на выборке ASVspoof2019.

Программное средство реализовано на языке Python 3.10 и состоит из пяти последовательно взаимодействующих модулей: подготовки метаданных, извлечения признаков, обучения GMM-моделей, вычисления метрик эффективности (EER, AUC) и визуализации результатов.

По результатам оценки на выборке ASVspoof2019 (этап Evaluation) получены следующие значения метрик: для Baseline-модели AUC = 0,9378, EER = 0,1391; для модели Baseline+LPC AUC = 0,9389, EER = 0,1352. График ROC-кривых AUC для обеих моделей представлен на рисунке 1.

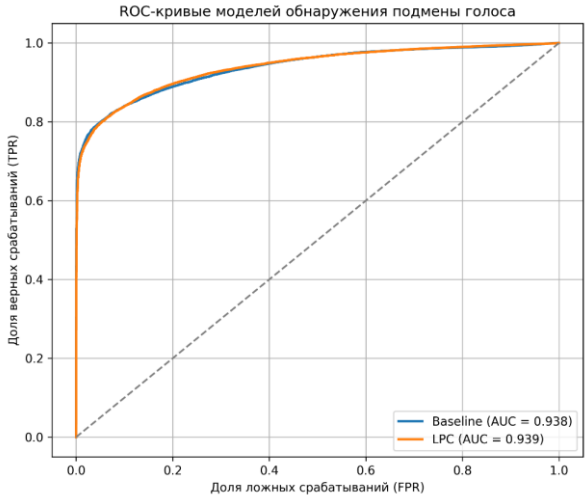


Рис. 1. График AUC для Baseline-модели и модели Baseline+LPC

Полученные значения свидетельствуют о высокой эффективности разработанного программного средства. Улучшение метрик при добавлении статистик LPC-остатка подтверждает, что данный признак способен предоставлять классификатору дополнительную комплементарную информацию, при этом степень его вклада зависит от алгоритма классификации и настроенных гиперпараметров модели.

Заключение

В работе предложен способ определения факта преобразования голоса с использованием интеллектуальных средств (на примере RVC), основанный на анализе акустических и статистических признаков речи. Разработано программное средство, реализующее классификатор на основе GMM, сформирован экспериментальный набор данных из 90 аудиозаписей и проведена оценка эффективности на выборке ASVspoof2019. Полученные значения AUC (до 0,939) и EER (до 0,135) подтверждают эффективность предложенного способа, а включение статистик LPC-остатка в состав признаков позволяет улучшить качество классификации. Разработанное программное средство может быть использовано в качестве дополнительного фактора аутентификации в системах голосовой биометрии, для защиты корпоративных и университетских

голосовых линий связи, а также в мессенджерах — для информирования пользователей о преобразованных голосовых сообщениях.

Список литературы

1. BI.ZONE Brand Protection: более чем в 1,5 раза увеличилось количество фишинга в 2024 году. URL: https://bi.zone/news/bi-zone-brand-protection-bolee-chem-v-1-5-raza-uvelichilos-kolichestvo-fishinga-v-2024-godu/ (дата обращения: 02.10.2024).

2. Новая схема атаки с помощью генерации голоса знакомых и коллег. URL: https://habr.com/ru/companies/startx/articles/800299/ (дата обращения: 03.10.2024).

3. Злоумышленники заставили сотрудника компании совершить трансфер размером 243 тысячи долларов с помощью голоса генерального директора компании, созданного нейросетью. URL: https://threatpost.com/deep-fake-of-ceos-voice-swindles-company-out-of-243k/147982/ (дата обращения: 07.10.2024).

4. IBM. Cost of a Data Breach Report 2024. URL: https://www.ibm.com/downloads/documents/us-en/107a02e94948f4ec (дата обращения: 22.10.2024).

5. Репозиторий программного обеспечения RVC с открытым исходным кодом. URL: https://github.com/RVC-Project/Retrieval-based-Voice-Conversion-WebUI (дата обращения: 05.02.2025).

6. Hemavathi R., Kumaraswamy R. Voice conversion spoofing detection by exploring artifacts estimates // Multimedia Tools and Applications. — 2021. — Vol. 15, № 23561–23580. DOI: 10.1007/s11042-020-10212-0.

7. Todisco M., Delgado H., Evans N., Yamagishi J. ASVspoof 2021: Automatic Speaker Verification Spoofing and Countermeasures Challenge Evaluation Plan, 2021. URL: https://www.asvspoof.org/asvspoof2021/asvspoof2021_evaluation_plan (дата обращения: 13.05.2025).

УДК 004.056.53

Влияние конструктивных особенностей измерительного стенда на погрешность идентификации дефектов в рефлектометрии проводных линий

Фесько Н. В., Рамзаев В. А., Зубов В. Г.

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

АО «НПП «Сигнал», г. Санкт-Петербург, Россия

Аннотация: *В данной работе проведён анализ влияния элементов конструкции тестового стенда (разъёмы, тумблеры, устройства защитного отключения, розетки) на погрешность измерений при рефлектометрии проводных линий. Установлено, что неидеальность контактов и наличие разветвлений вносят разброс амплитуды отражённого сигнала до* $\pm 2{,}5\%$ *, однако не изменяют угол наклона сигнала в месте дефекта. Экспериментально подтверждено, что угол наклона является конструктивно-независимым идентифицирующим параметром для определения обрыва (*5°*), короткого замыкания (*3°*) и конца линии (*9°*). Результаты могут быть использованы для создания автоматизированных систем диагностики, снижающих погрешность идентификации с* 50% *до значений, определяемых точностью измерения угла.*

Ключевые слова: *рефлектометрия, рефлектограмма, погрешность измерений, измерительный стенд, идентификация дефектов, угол наклона сигнала.*

Введение

Обеспечение целостности проводных линий связи и электропитания является важной задачей для всех видов информационных систем: государственных информационных систем, информационных систем персональных данных, автоматизированных систем управления технологическим процессом, критической информационной инфраструктуры и информационных систем общего пользования, особенно при работе с государственной тайной и конфиденциальной информацией. Одной из актуальных угроз является несанкционированное подключение аппаратных средств для перехвата информации, в том числе в цепи электропитания.

Наиболее распространённым методом диагностики в России является импульсная рефлектометрия, реализованная в приборах серии «РЕЙС» и «ИРК-ПРО Гамма Е». Однако, как показал анализ руководств по эксплуатации, в большинстве российских рефлектометров отсутствует автоматический механизм сравнения текущей рефлектограммы с эталонной базовой линией. Это вынуждает оператора полагаться на субъективную оценку, что приводит к погрешности измерений до 50 % [1], увеличению времени диагностики и пропуску реальных дефектов и подключений.

Цель работы – выявление параметров рефлектограммы, устойчивых к конструктивным особенностям измерительного стенда, для последующей автоматизации процесса индентификации дефектов и подключений.

Конструкция измерительного стенда и её влияние на погрешность

Для проведения экспериментов был сконструирован стенд, позволяющий имитировать следующие состояния линии: базовая линия (нормальное состояние), обрыв, короткое замыкание, отсутствие заземления и подключение устройств в розетки. На рисунке 1 представлен данный стенд.

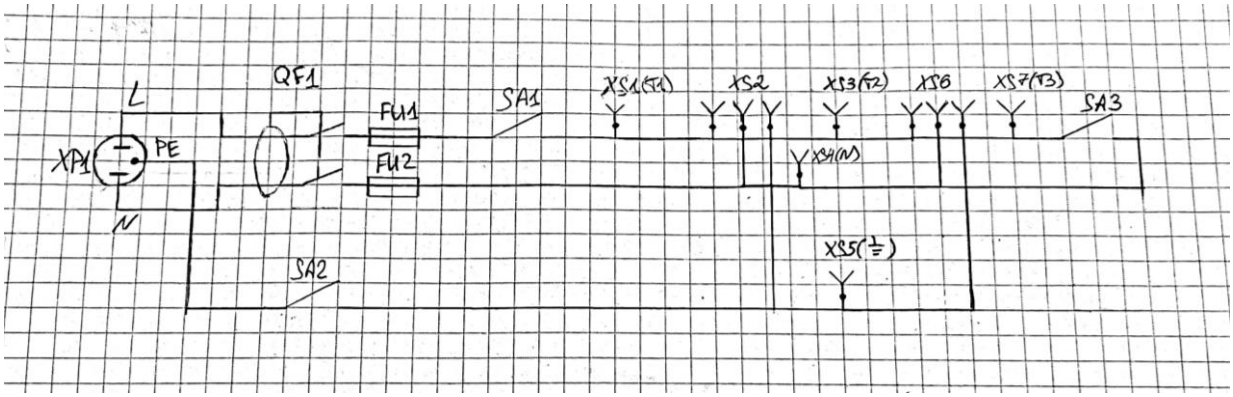


Рис. 1. Схема сконструированного стенда

В состав стенда входят следующие элементы, которые потенциально могут влиять на погрешность измерений:

− штепсель с заземляющим контактом (XP1);

− двухполюсное устройство защитного отключения (QF1);

− предохранители (FU1, FU2);

− тумблеры для имитации обрыва (SA1), отсутствия заземления (SA2) и короткого замыкания (SA3);

− две розетки двухполюсные с защитным контактом (XS2, XS6);

− разъём типа «банан» перед первой розеткой XS1 (T1);

− разъём типа «банан» между розетками XS3 (T2);

− разъём типа «банан» на нейтрали XS4 (N);

− разъём типа «банан» на заземлении XS5 (⏚);

− разъём типа «банан» после второй розетки XS7 (T3).

Каждый из этих элементов вносит дополнительные неоднородности импеданса и может создавать дополнительные отражения. Особенно критичны:

− механические контакты тумблеров, переходное сопротивление которых может варьироваться;

− разъёмы типа «банан», подверженные окислению и люфту;

− разветвлённая структура стенда, создающая переотражения.

Для измерения использовался программно-аппаратный комплекс «СИРИУС-МК» в режиме частотной рефлектометрии. Обработка данных выполнялась с помощью скрипта на Python.

Экспериментальные результаты

Было проведено три серии экспериментов (базовая линия, обрыв, короткое замыкание) по 20 измерений в каждой серии. На рисунке 2 представлены наложенные рефлектограммы всех опытов.

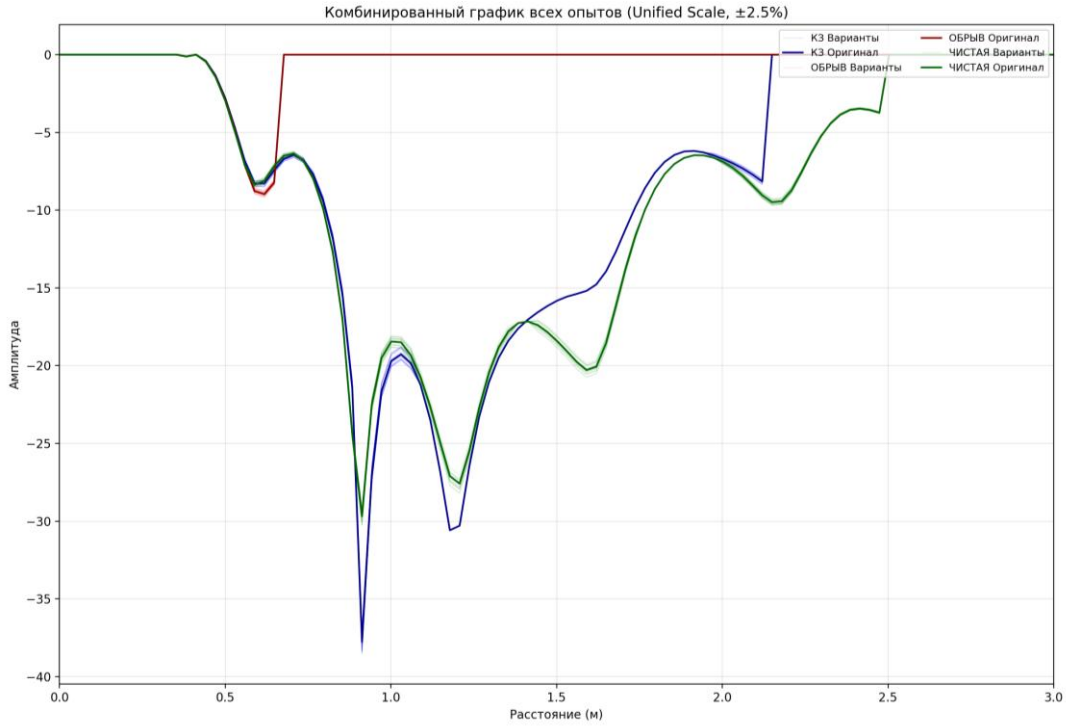


Рис. 2. Наложенные рефлектограммы всех опытов.

Анализ полученных данных показал следующее:

1. Разброс значений амплитуды отражённого сигнала между опытами не превысил $\pm 2{,}5\%$, что находится в пределах нормы для данного типа измерений. Это значение можно рассматривать как суммарную погрешность, вносимую конструктивными элементами стенда (неидеальные контакты, разъёмы, ветвление проводов).

2. Изначально была выдвинута гипотеза об эффективности вейвлетного анализа для идентификации дефектов и подключений. Однако огибающие сигнала при обрыве, коротком замыкании и конце линии оказались одинаковыми. Вместо этого был выявлен геометрический параметр – угол наклона сигнала в месте предполагаемого дефекта: обрыв характеризуется 5° наклона от вертикали вправо, короткое замыкание – 3° наклона от вертикали вправо, а норма (конец линии) – 9° наклона от вертикали вправо.

При двадцатикратном повторении эксперимента скорость возврата в нуль (угол наклона) оставалась стабильной, несмотря на разброс амплитуды $\pm 2{,}5\%$. Это позволяет использовать угол наклона как идентифицирующий параметр, устойчивый к конструктивным особенностям стенда.

Обсуждение влияния конструкции на погрешность

В ходе экспериментальной серии из 20 повторных измерений для каждого типа дефекта было установлено, что разброс амплитуды отражённого сигнала не превышает $\pm 2{,}5\%$. Данная величина может рассматриваться как интегральная оценка суммарного влияния всех конструктивных элементов стенда:

- неидеальность механических контактов тумблеров;
- переходные сопротивления разъёмов типа «банан»;
- наличие предохранителей и устройства защитного отключения;
- разветвлённая структура линии с двумя розетками.

При этом, несмотря на вариацию амплитуды в пределах $\pm 2{,}5\%$, угол наклона сигнала в месте дефекта оставался строго постоянным для каждого типа неоднородности. Это позволяет сделать вывод, что конструктивные особенности стенда влияют преимущественно на амплитуду сигнала, но не на его форму в области дефекта. Следовательно, угол наклона является конструктивно-независимым идентифицирующим параметром, что делает его пригодным для использования в автоматизированных системах диагностики.

Заключение

В ходе работы был сконструирован измерительный стенд для имитации дефектов проводных линий и проведены эксперименты по оценке влияния его конструктивных элементов на погрешность рефлектограмм. В результате установлено, что суммарный разброс амплитуды отражённого сигнала, обусловленный конструктивными элементами стенда, составил не более $\pm 2{,}5\%$, при этом гипотеза о применении вейвлетного анализа для идентификации дефектов не подтвердилась, так как огибающие сигнала для обрыва, короткого замыкания и конца линии оказались одинаковыми. В качестве устойчивого идентифицирующего параметра выявлен угол наклона сигнала в месте дефекта: для обрыва он составляет 5°, для короткого замыкания – 3°, для конца линии – 9°. Показано, что данный параметр не зависит от конструктивных особенностей стенда, поскольку остаётся стабильным при вариациях амплитуды в пределах $\pm 2{,}5\%$. Полученные результаты могут быть использованы для создания автоматизированных систем диагностики проводных линий, позволяющих снизить погрешность идентификации с 50% до значений, определяемых точностью измерения угла наклона.

Список литературы

1. 1. Авдеюк Д. Н. Информационно-измерительная система определения места повреждения магистральных линий электропередач: дис. канд. тех. наук: 2.2.11 / Шилин Александр Николаевич – Волгоград, 2023. – 121 с

УДК 004.056.5

Исследование влияния интенсивности и модуляции шумовой помехи на качество автоматического распознавания речи

Рамзаев В. А., Фесько Н. В., Шульженко А. Д.

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

Аннотация: *В работе исследовано влияние интенсивности и модуляции шумовой помехи на качество автоматического распознавания речи современными нейросетевыми системами. Проведено сравнение постоянной и модулированной помех при различных значениях отношения сигнал/шум с использованием систем Whisper, Faster-Whisper, Vosk и Google Speech Recognition. Установлено, что постоянная шумовая помеха значительно эффективнее снижает точность распознавания, тогда как модуляция создает временные интервалы, позволяющие алгоритмам частично восстанавливать речевой сигнал. Полученные результаты могут быть использованы при разработке средств акустической защиты речевой информации.*

Ключевые слова: *акустическая защита информации, автоматическое распознавание речи, нейросетевое распознавание речи, шумовая помеха, модуляция шума, отношение сигнал/шум, маскирование речи, помехоустойчивость.*

Введение

Современные системы автоматического распознавания речи демонстрируют высокую устойчивость к традиционным шумовым помехам, что снижает эффективность классических методов акустического маскирования. В связи с этим возрастает актуальность исследования факторов, позволяющих повысить эффективность шумовых помех и снизить вероятность корректного распознавания речевой информации. Одним из таких факторов является модуляция шумового сигнала. Изменение амплитуды помехи во времени способно влиять на процесс выделения речевых признаков и, как следствие, на качество распознавания речи нейросетевыми алгоритмами.

Цель статьи: исследование влияния интенсивности и модуляции шумовой помехи на точность автоматического распознавания речи. Для этого проведено экспериментальное сравнение постоянной и модулированной помех при различных значениях отношения сигнал/шум с использованием современных систем распознавания речи.

Методика исследования

Для оценки влияния интенсивности и модуляции шумовой помехи на качество автоматического распознавания речи проведено сравнение результатов распознавания при различных значениях отношения сигнал/шум.

В качестве исследуемых систем использовались современные модели автоматического распознавания речи: Whisper, Faster-Whisper, Vosk и Google Speech Recognition. В ходе эксперимента сравнивались два режима формирования

помехи: постоянный и модулированный белый шум. Исследования проводились при отношениях сигнал/шум 20, 10 и 0 дБ.

Эффективность оценивалась по точности автоматического распознавания речи и коэффициенту ошибок распознавания, что позволило определить влияние интенсивности и модуляции шумовой помехи на работу исследуемых систем.

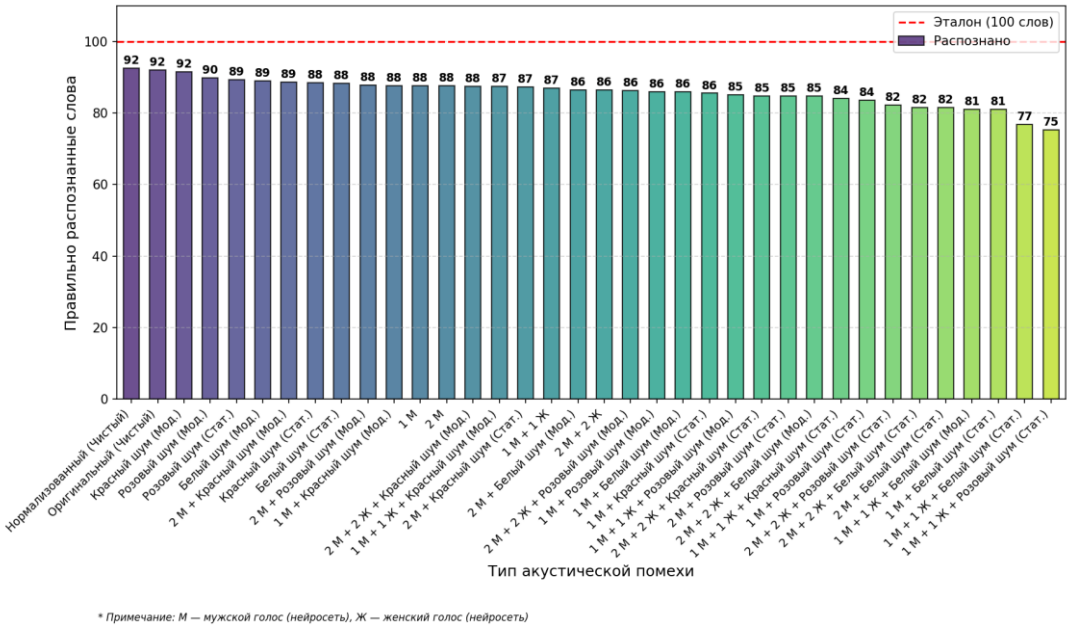


Рис. 1. Результаты эксперимента при отношении сигнал/шум 20 дБ

Результаты эксперимента показали, что при отношении сигнал/шум 20 дБ исследуемые модели сохраняют высокую точность распознавания на уровне 82–93% (рис. 1). В данных условиях шумовая помеха оказывает незначительное влияние на качество выделения речевых признаков.

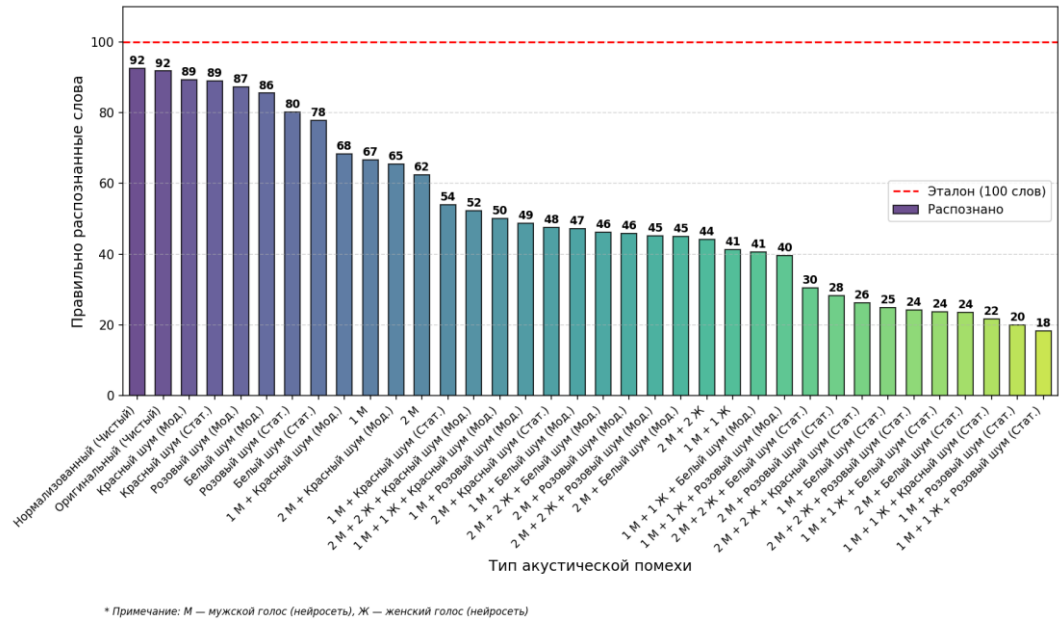
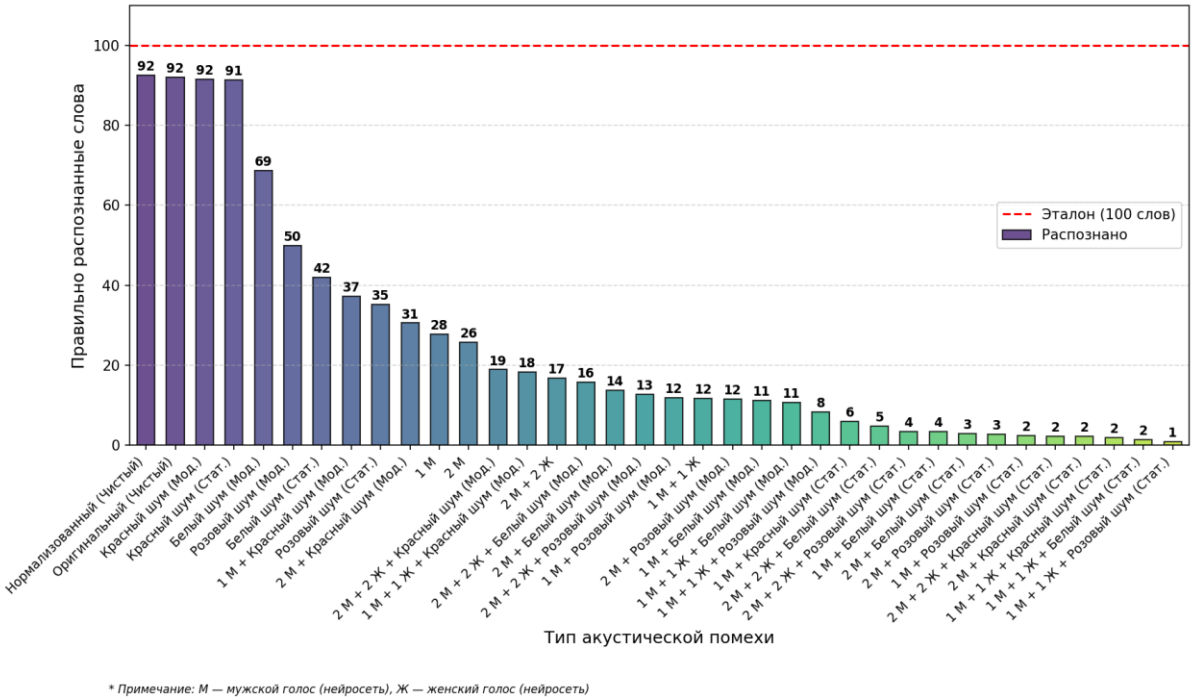


Рис. 2. Результаты эксперимента сигнал/шум 10 дБ

При уменьшении отношения сигнал/шум до 10 дБ точность распознавания снижается до 56–63% (рис. 2).



* Примечание: М — мужской голос (нейросеть), Ж — женский голос (нейросеть)

Рис. 3. Результаты эксперимента сигнал/шум 0 дБ

При отношении сигнал/шум 0 дБ, когда уровни полезного сигнала и помехи становятся одинаковыми, качество распознавания резко ухудшается. В условиях постоянной шумовой помехи точность идентификации речевых сигналов системой снижается до 15–40%, что свидетельствует о значительном ухудшении её работы (рис. 3).

Сравнение постоянной и модулированной шумовой помехи показало, что постоянный шум оказывает более выраженное влияние на качество распознавания. Так, при отношении сигнал/шум 0 дБ точность распознавания системой Google Speech Recognition составила 39% при использовании постоянной помехи и 75% при модулированной. Аналогичная закономерность наблюдалась и для других исследуемых систем.

Полученные результаты могут быть объяснены тем, что модуляция формирует кратковременные интервалы с пониженным уровнем помех, позволяющие алгоритмам распознавания восстанавливать часть речевой информации. Постоянная помеха обеспечивает непрерывное маскирование полезного сигнала и, как следствие, более эффективно снижает точность автоматического распознавания речи.

Заключение

В работе проведено исследование влияния интенсивности и модуляции шумовой помехи на качество автоматического распознавания речи современными нейросетевыми системами. Выполнено экспериментальное сравнение результатов распознавания при различных значениях отношения сигнал/шум с использованием постоянной и модулированной помех.

Результаты исследования показали, что уменьшение отношения сигнал/шум приводит к закономерному снижению точности распознавания речи всеми исследуемыми системами. При значении SNR = 20 дБ они сохраняют высокую точность распознавания, тогда как при снижении отношения сигнал/шум до 10 дБ наблюдается существенная деградация качества. Наиболее выраженное ухудшение достигается при SNR = 0 дБ, когда уровень шумовой помехи становится сопоставим с уровнем полезного сигнала.

Установлено, что постоянная шумовая помеха оказывает более эффективное воздействие на системы автоматического распознавания речи по сравнению с модулированной. Причиной этого является отсутствие временных интервалов со сниженным уровнем шума, которые позволяют алгоритмам распознавания частично восстанавливать речевой сигнал и использовать контекст для повышения точности распознавания.

Полученные результаты подтверждают, что выбор структуры шумовой помехи оказывает не меньшее влияние на эффективность акустического маскирования, чем её энергетические характеристики. Использование постоянной шумовой помехи позволяет создать более сложные условия для выделения информативных признаков речи и обеспечивает более значительное снижение качества автоматического распознавания.

Результаты исследования могут быть использованы при разработке средств акустической защиты речевой информации, проектировании систем тестирования помехоустойчивости алгоритмов распознавания речи, а также в дальнейших исследованиях методов противодействия современным нейросетевым системам обработки речевых сигналов.

Список литературы

1. Ахметшин А. Ф. Применение нейросетевых технологий для анализа речевой информации // CyberLeninka. – 2020. – URL: https://cyberleninka.ru/article/n/primenenie-neyrosetevyh-tehnologiy-dlya-analiza-rechevoy-informatsii/viewer (дата обращения: 13.05.2026).

УДК 004.056.5

Оценка репрезентативности методики испытаний систем автоматического распознавания речи при исследовании эффективности акустических помех

Рамзаев В. А., Фесько Н. В., Повеликин В.Я.

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

Аннотация: *В работе проведена статистическая оценка репрезентативности методики экспериментальных исследований с использованием современных систем автоматического распознавания речи. Выполнено 1600 независимых экспериментов с применением моделей Whisper, Faster-Whisper, Vosk и Google Speech Recognition. Для анализа воспроизводимости результатов использованы методы математической статистики, включающие расчет среднего значения, стандартного отклонения, коэффициента вариации, доверительных интервалов, критерий Граббса и критерий Шапиро—Уилка. Проведена оценка устойчивости исследуемых моделей, выявлены статистические выбросы и определена достаточность объема экспериментальной выборки. Полученные результаты подтверждают высокую воспроизводимость разработанной методики и ее пригодность для проведения исследований, основанных на применении систем автоматического распознавания речи.*

Ключевые слова: *автоматическое распознавание речи, математическая статистика, репрезентативность выборки, воспроизводимость эксперимента, доверительный интервал, критерий Граббса, критерий Шапиро—Уилка, коэффициент вариации, статистический анализ, нейросетевые модели.*

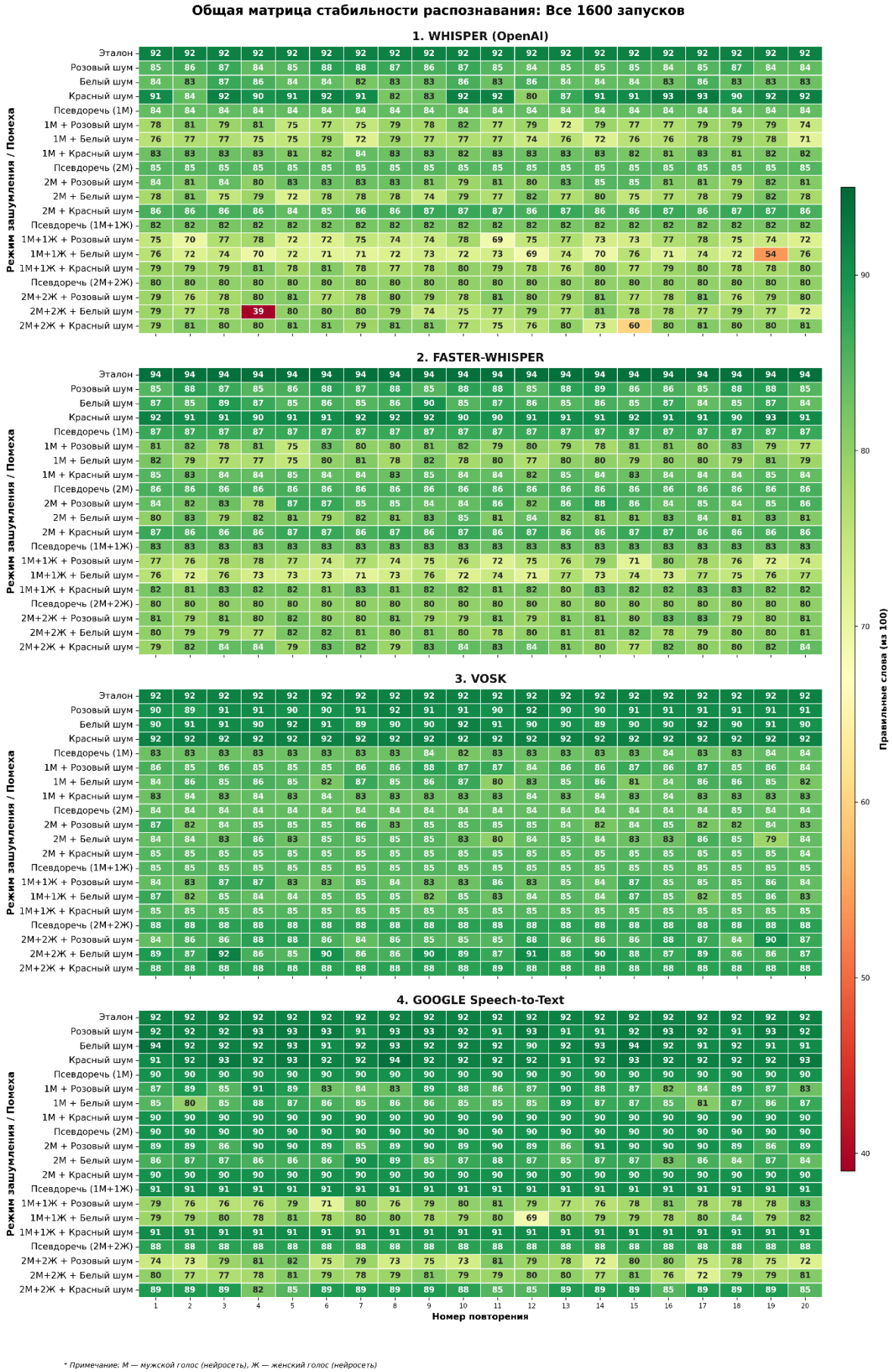
Введение

Современные системы автоматического распознавания речи основаны на вероятностных алгоритмах обработки аудиосигналов, что может приводить к вариациям результатов даже при повторной обработке одного и того же речевого сигнала. В связи с этим при проведении экспериментальных исследований возникает необходимость оценки воспроизводимости результатов и статистической достоверности используемой методики.

Целью работы является оценка репрезентативности методики экспериментальных исследований на основе современных систем автоматического распознавания речи. Для этого проведена серия многократных испытаний различных моделей распознавания в идентичных условиях с последующей статистической обработкой полученных результатов.

Экспериментальные исследования

Для оценки репрезентативности разработанной методики была проведена серия статистических испытаний современных систем автоматического распознавания речи. Целью исследования являлась проверка воспроизводимости результатов распознавания при многократной обработке одних и тех же аудиоданных в неизменных условиях.



* *Примечание: М — мужской голос (нейросеть), Ж — женский голос (нейросеть)*

Рис. 1 – Результаты экспериментов

В исследовании использовались четыре системы автоматического распознавания речи: Whisper, Faster-Whisper, Vosk и Google Speech Recognition. Для каждой модели исследовались двадцать вариантов акустических условий, включающих различные комбинации речеподобных и шумовых помех. Каждая комбинация модели и акустического условия обрабатывалась двадцать раз, вследствие чего общий объем экспериментальной выборки составил 1600 независимых испытаний (80 экспериментальных серий по 20 повторений).

Во всех экспериментах использовались одинаковые входные аудиофайлы, неизменные параметры распознавания и идентичная вычислительная среда. Это позволило исключить влияние внешних факторов и обеспечить сопоставимость результатов между всеми сериями испытаний.

Представленные на рисунке результаты позволяют визуально оценить воспроизводимость экспериментов. Для большинства исследованных условий значения точности распознавания изменяются незначительно, что свидетельствует о высокой повторяемости результатов. Вместе с тем отдельные модели демонстрируют повышенную чувствительность к сложным акустическим воздействиям, что проявляется увеличением разброса результатов.

Для количественной оценки воспроизводимости была выполнена статистическая обработка каждой экспериментальной серии. Среднее значение определялось по формуле

$$\overline{x} = \frac{1}{n}\sum_{i=1}^{n} x_i. \quad (1)$$

где (x_i) — результат отдельного эксперимента, (n=20) — количество повторений.

Разброс результатов оценивался с использованием несмещенного стандартного отклонения

$$s = \sqrt{\frac{1}{n-1}\sum_{i=1}^{n}(x_i - \overline{x})^2} \quad (2)$$

которое характеризует степень отклонения отдельных наблюдений от среднего значения.

Для сравнения стабильности различных моделей использовался коэффициент вариации

$$CV = \frac{s}{\overline{x}} \cdot 100\% \quad (3)$$

Данный показатель позволяет сравнивать устойчивость результатов независимо от абсолютных значений точности распознавания. Чем меньше значение коэффициента вариации, тем выше воспроизводимость результатов.

Точность оценки среднего значения определялась посредством построения 95 %-го доверительного интервала

$$CI = \overline{x} \pm t_{0.975} \cdot \frac{s}{\sqrt{n}}, \quad (4)$$

где ($t_{0.975}$=2.093) — коэффициент распределения Стьюдента при числе степеней свободы (n-1=19). Доверительный интервал определяет диапазон, в котором с вероятностью 95 % находится истинное среднее значение исследуемой величины.

Для выявления единичных аномальных наблюдений использовался критерий Граббса

$$G = \frac{|x_i - \overline{x}|}{s}. \quad (5)$$

При превышении критического значения ($G_{crit} = 2.711$) наблюдение классифицировалось как статистический выброс и дополнительно проверялось методом межквартильного размаха (IQR). Нормальность распределения экспериментальных данных оценивалась с использованием критерия Шапиро—Уилка при уровне значимости α=0.05).

Проведенный анализ показал существенные различия в устойчивости исследуемых моделей. Наиболее стабильные результаты продемонстрировала система Vosk, для которой среднее стандартное отклонение составило 0,795 слова, коэффициент вариации — 0,93 %, а средняя ширина доверительного интервала — 0,744 слова. Наибольший разброс результатов наблюдался у модели Whisper, для которой среднее стандартное отклонение достигло 2,071 слова, коэффициент вариации составил 2,65 %, а средняя ширина доверительного интервала — 1,938 слова. Модели Faster-Whisper и Google Speech Recognition заняли промежуточное положение, продемонстрировав коэффициенты вариации 1,40 % и 1,42 % соответственно.

Средняя ширина 95 %-го доверительного интервала по всем экспериментальным сериям составила 1,212 слова. Минимальное значение доверительного интервала наблюдалось у Faster-Whisper при распознавании режима «Псевдоречь (1М)», тогда как максимальная ширина доверительного интервала (8,359 слова) была зарегистрирована у модели Whisper при воздействии комбинированной помехи «2М+2Ж + Белый шум». Это свидетельствует о существенном увеличении неопределенности результатов в наиболее сложных акустических условиях.

Проверка экспериментальных данных критерием Шапиро—Уилка показала, что гипотеза о нормальном распределении не отвергается для 45 из 80 экспериментальных серий (56,25 %). Отклонения от нормального распределения наблюдались преимущественно при высокой точности распознавания, когда проявлялся эффект насыщения результатов, а также в сериях с интенсивными акустическими воздействиями, сопровождавшихся единичными резкими ошибками распознавания.

По критерию Граббса и методу межквартильного размаха было обнаружено 64 статистических выброса. При этом их влияние на итоговые оценки оказалось незначительным. Среднее смещение математического ожидания после исключения выбросов составило 0,1523 слова, что существенно меньше средней ширины доверительных интервалов и не оказывает заметного влияния на итоговые результаты исследования.

Дополнительно была выполнена оценка достаточности объема экспериментальной выборки. Расчеты показали, что при наблюдаемой дисперсии для оценки среднего значения с точностью ±2 слова при доверительной вероятности 95 % было бы достаточно 3,52 повторения каждого эксперимента. В настоящем исследовании использовалось 20 повторений, что превышает минимально необходимый объем выборки почти в 5,7 раза. Таким образом, объем экспериментальных данных является статистически достаточным, а полученные результаты можно считать репрезентативными
и пригодными для дальнейшего анализа.

Заключение

В работе проведена статистическая оценка репрезентативности методики экспериментальных исследований, основанной на использовании современных систем автоматического распознавания речи. Для этого выполнена серия из 1600 независимых экспериментов, включающая 80 экспериментальных серий по 20 повторных запусков каждая, что обеспечило достаточный объем данных для статистического анализа.

По результатам исследования рассчитаны основные статистические характеристики экспериментальных выборок, включая среднее значение, стандартное отклонение, коэффициент вариации, доверительные интервалы и показатели нормальности распределений. Для поиска аномальных результатов использовались критерий Граббса и метод межквартильного размаха, позволившие выявить единичные статистические выбросы и оценить степень их влияния на итоговые показатели.

Проведенный анализ показал, что исследуемые системы автоматического распознавания речи характеризуются высокой воспроизводимостью результатов при многократной обработке одинаковых аудиоданных. Наиболее устойчивой моделью оказалась Vosk, продемонстрировавшая минимальные значения стандартного отклонения и коэффициента вариации. Наибольший разброс результатов наблюдался у модели Whisper, однако даже в этом случае влияние случайных отклонений на итоговые оценки оказалось незначительным.

Проверка достаточности экспериментальной выборки показала, что использованный объем повторений более чем в пять раз превышает минимально необходимое количество наблюдений для достижения заданной точности при доверительной вероятности 95 %. Это подтверждает статистическую обоснованность выполненного исследования и позволяет считать полученные результаты репрезентативными.

Таким образом, разработанная методика обеспечивает высокую воспроизводимость результатов и может быть рекомендована для проведения экспериментальных исследований, основанных на использовании современных систем автоматического распознавания речи. Применение методов математической статистики позволяет объективно оценивать устойчивость работы нейросетевых моделей, своевременно выявлять аномальные результаты и повышать достоверность научных исследований, связанных с анализом алгоритмов автоматического распознавания речи.

Список литературы

1. Ахметшин А. Ф. Применение нейросетевых технологий для анализа речевой информации // CyberLeninka. – 2020. – URL: https://cyberleninka.ru/article/n/primenenie-neyrosetevyh-tehnologiy-dlya-analiza-rechevoy-informatsii/viewer (дата обращения: 13.05.2026).

Секция 3 – Системы управления и навигации

УДК 629.05

Сравнительный анализ современных систем наземной навигации специального назначения

Быстров Д. Е., Кириченко Р. Н.

АО "Супертел", г. Санкт-Петербург, Россия

***Аннотация**: В статье проведён сравнительный анализ современных систем наземной навигации специального назначения, применяемых для обеспечения действий сил специальных операций. Рассмотрены три основных типа навигационных систем: спутниковые (на примере ГЛОНАСС и GPS), наземные радионавигационные (на примере систем «Чайка» и «Лоран-С») и автономные средства навигации (инерциальные и одометрические системы). Приведены ключевые технические характеристики указанных систем, включая параметры орбит, рабочие частоты, дальность действия, среднеквадратическую погрешность определения местоположения и другие показатели.*

Проанализированы преимущества и недостатки каждого типа систем – в частности, вопросы помехозащищённости, точности, зоны действия и стоимости эксплуатации. Особое внимание уделено значимости исходных геодезических данных и требованиям к оперативности и достоверности навигационной информации в условиях манёвренных действий сил специальных операций. Результаты исследования позволяют обоснованно выбирать тип навигационной системы в зависимости от специфики решаемых задач и условий применения.

***Ключевые слова**: системы наземной навигации специального назначения, спутниковые навигационные системы, наземные радионавигационные системы, автономные средства навигации, ГЛОНАСС, GPS, инерциальные навигационные системы, безплатформенные инерциальные навигационные системы, сравнительный анализ навигационных систем*

Введение

Анализ путей развития специальной техники, а также возможные варианты действий систем специального назначения (СН) показывают, что требования к качеству и оперативности топогеодезической информации будут неуклонно возрастать. В специальных операциях современности существенно постоянно повышается значение маневра силами и средствами профильных служб, поэтому маневренные возможности объектов СН, в том числе и средств топогеодезической привязки, не должны снижать динамики действий сил специальных операций (ССО).

Необходимость обеспечения высокой эффективности применения специальных средств в условиях возросших маневренных возможностей ССО заставляет вести специальную операцию с развертыванием сил и средств в реальном масштабе времени и с полной готовностью к действию. Часто для повышения эффективности действий ССО предусматриваются рассредоточение и широкий маневр внутри позиционных районов, что приводит к необходимости заблаговременной подготовки позиционных районов в топогеодезическом отношении, существо которой будет определяться степенью оснащенности аппаратурой навигации и топопривязки, а также

наличием надлежащей топогеодезической основы. ***(Примечание:*** *здесь мы сталкиваемся с термином - навигация. Что это такое? Латинское navigation образовано от слова navigo, что значит плыву на судне. Решение задачи навигации предполагает определение координат подвижного объекта, а также его скорости и направления движения в реальном масштабе времени).*

С развитием средств и способов ведения специальных операций расширяется круг потребителей геодезических данных, возрастают требования к оперативности методов определения координат. Как показывает опыт специальных военных операций и вооруженную конфликтов, отсутствие геодезических данных часто делает самую совершенную специальную технику не только бесполезной с точки зрения её применения, но и губительной для своих специальных служб и мирного населения. А для подразделений ССО, действующих на местности автономно, наличие датчиков координат имеет жизненно важное значение.

В настоящее время в мире применяется три типа систем наземной навигации [1]:

− спутниковые навигационные системы (СНС);

− наземные радионавигационные системы (РНС);

− автономные средства навигации

Основные составляющие этих систем [2]:

1. Спутниковые радионавигационные системы (СРНС) представляют собой совокупность трех основных подсистем:

− подсистема космических аппаратов (ПКА);

− подсистема контроля и управления (ПКУ) (наземный командно-измерительный комплекс (КИК) или сегмент управления);

− аппаратура потребителей (АП) СРНС (приемоиндикаторы (ПИ)).

Причем подсистема потребителей (ПИ) входит составной частью и в остальные навигационные системы. Разнообразие видов АП обеспечивает потребности наземных, морских, авиационных и космических потребителей.

В настоящее время самое широкое применение нашли среднеорбитальные спутниковые навигационные системы (СНС) второго поколения GPS (США) и ГЛОНАСС (Россия) и европейская система GALILEO.

Предусмотрено их совместное использование на основе изготовления спутниковых навигационных приемников, которые позволяют принимать и обрабатывать сигналы обеих систем. Сравнительные параметры систем ГЛОНАСС и GPS представлены в таблице 1.

Таблица 1 – Сравнительные параметры систем ГЛОНАСС и GPS

Наименование параметра	**Значение параметра**	
	GPS	**ГЛОНАСС**
Орбиты НИСЗ: высота, км наклонение, град тип период обращения, ч	 20180 55 круговая 12	 19100 64,8 круговая 11,4
Структура сети: число НИСЗ число плоскостей орбит	 24 6	 24 3
Рабочие частоты: f_1, МГц f_2, МГц	 1575,4 1227,6	 1602,0 ... 1615,5 1246,0 ... 1256,5
Разделение навигационных сигналов НИСЗ	Кодовое	Частотное
Погрешности определения параметров (СКП) в плане по высоте по скорости по времени	 50 м 80 м 0,3 м/с 1 мкс	 30 м 45 м 0,05 м/с 0,3 мкс

2. Наземные радионавигационные системы.

Сравнительная характеристика этих систем представлена в таблице 2. Их условно (по дальности действия) можно разделить на следующие составляющие:

– фазовые;

– импульсно-фазовые системы.

Примером фазовой РСДН может служить система «Омега», работающая в диапазоне очень низких частот (10,2 – 13,6 кГц) и являющаяся практически глобальной разностно-дальномерной системой. Система предназначена для навигации воздушных и морских судов, подводных лодок и наземных объектов.

Наземные станции РСДН «Омега» не разделяются на ведущие и ведомые, а все работают независимо, синхронно с сигналами системы единого времени. Конструктивно эти станции представляют громоздкие и сложные сооружения с высотой антенных мачт до 365 м и с осью заземления диаметром 1000 м. Излучаемая мощность 10 кВт обеспечивает надежный прием сигналов РСДН «Омега» на расстояниях до 10000 км.

К импульсно-фазовым системам относятся развернутые в настоящее время 2 глобальные наземные навигационные системы «Лоран–С» (США) и «Чайка» (Россия), в которых функционирует 78 импульсно-фазовых радионавигационных станций (ИФРНС). Они размещены на территории различных государств: Канаде – 29 станций, в Европе – 8 станций, на побережье Средиземного моря – 4 станции, в Саудовской Аравии – 5 станций, в Индии – 6 станций, в Японии – 4 станции, в Корее – 2 станции, в Китае – 6 станций, на территории РФ и СНГ – 14 станций (354 РСДН г. Слоним, РБ).

Таблица 2 – Сравнительная характеристика наземных радионавигационных систем

Характеристика	**СИСТЕМЫ**	
	Чайка	**«Лоран–С»**
Центральная частота спектра сигнала, кГц	100	
Ширина спектра сигнала, кГц	23–25	20
Дальность действия, км суша море	1400–1800 2000–2500	
СКП определения места при отношении сигнал/шум =1/3, м	150–500	
СКП повторного выхода на заданную точку, м	20–70	10–45
Доступность	0,97	0,98
Коэффициент готовности одной станции	не менее 0,999	
Относительная суточная нестабильность опорных генераторов (стандартов частоты)	5×10^{-12}	3×10^{-13}

Эти системы для измерения радионавигационного параметра использует импульсно-фазовый метод – грубое измерение разности дальностей основано на измерении интервала времени между импульсами ведущей и ведомой станций, а точное – на фазовом методе. Использование низкочастотного диапазона (90 – 110 кГц) и когерентной обработки радионавигационных сигналов на борту потребителя позволило на земной волне увеличить дальность

действия системы до 1800 – 2000 км при работе над морем и до 1500 км над сушей.

Все передатчики системы «Лоран С», разнесенные относительно друг друга на расстояние 960 – 1300 км, излучают сигналы на фиксированной частоте 100кГц. Передатчик каждой станции генерирует импульсы мощностью 4 МВт, которые излучаются вертикальной антенной высотой до 400 м с зонтичным заземлением радиусом 300 м.

Аналогичная ИФРНС «Чайка» была разработаны по заказу военного ведомства. В настоящее время в эксплуатации находятся четыре цепи со стационарными опорными станциями (ОС). Система обеспечивает непрерывное определение плановых координат при неограченной пропускной способности с точностью (СКП) 150-500 м; общая площадь рабочих зон всех цепей составляет около 20 млн. км2, доступность системы – не менее 0,97.

3. Автономные средства навигации включают в себя:

– инерциальные системы;

– одометрические системы

Инерциальные навигационные системы (ИНС) на гиростабилизированных платформах способны обеспечить автономное определение пространственного положения и скорости перемещения объекта в любых погодных условиях, днем и ночью, при этом, не демаскируя себя, то есть, не излучая сигналов во внешнюю среду. Кроме этого, они полностью защищены от посторонних радиошумов и помех.

Однако, ИНС свойственны и недостатки. Прежде всего, это достаточно высокая стоимость, сложность настройки перед началом движения, необходимость частых остановок на опорных пунктах с известными координатами для проведения коррекции. Точность ИНС в большой степени зависит от плавности хода движущегося объекта и от наличия опорных пунктов на маршруте перемещения. Несмотря на это, ИНС на гиростабилизированных платформах широко используется для навигации движущихся объектов различных типов. Точность определения навигационной информации современными ИНС составляет 10-15 м в плане, при условии проведения коррекции через каждые 15-20 минут.

Для устранения недостатков ИНС в мировой практике появилась тенденция перехода от ИНС на гиростабилизированных платформах к безплатформенным инерциальным навигационным системам (БИНС), в основу которых положено использование лазерных гироскопов. Преимуществами БИНС над ИНС являются: нечувствительность к ускорениям и перегрузкам; высокая точность определения навигационной информации; короткое время приведения в готовность к применению; надежность и длительный срок службы; низкая стоимость в сравнении с механическими гироскопами, которые используются в ИНС.

Точность определения навигационной информации современными БИНС составляет 0.15-0.30% от пройденного пути.

Одометрические навигационные системы (ОНС) широко используются для определения местоположения наземных движущихся объектов, где скорость движения на каждом прямолинейном участке пути измеряется по числу оборотов колес транспортного средства. Курсовой угол на таком участке определяется с помощью гирокомпаса. Как правило, в состав ОНС входят гирокомпасы, гирокурсоуказатели, вычислительные блоки, одометрические датчики.

Современные ОНС имеют предельную ошибку определения координат – до 1.5% от пройденного пути. Для уменьшения ошибок определения местоположения, которые накапливаются со временем, осуществляется контрольное ориентирование. Его проводят на контрольных пунктах, координаты которых известны. Контрольное ориентирование требует затрат времени на его проведение и связано с необходимостью остановки транспортного средства непосредственно на контрольном пункте или вблизи от него, что требует дополнительных условий в выборе маршрута перемещения (наличие контрольных пунктов), или дополнительные определения контрольных пунктов на установленных маршрутах перемещения.

Основными недостатками характерными для навигационных систем являются:

а) для спутниковых систем:

– низкие показатели помехозащищенности и целостности;

– невозможность эффективного использования сигналов СРНС в условиях затрудненного приема (в больших городах, в лесных массивах, в горных ущельях и т.д.)

б) для наземных радионавигационных систем:

– низкая точность;

– ограниченная зона действия.

в) для наземных автономных навигационных систем:

– низкая точность при проведении измерений на больших расстояниях;

– высокая стоимость.

Следует отметить, что в рассматриваемом аспекте, эффективность применения ССО во многом зависит от точности определения исходных геодезических данных (ИГД), под которыми понимаются: геодезические координаты исходного пункта опорной геодезической сети, геодезический азимут направления на один из смежных пунктов, определенные астрономическим путем, а также высота геоида в этом пункте над поверхностью принятого земного эллипсоида. (Примечание: в Российской Федерации за исходный пункт принят центр круглого зала Пулковской астрономической обсерватории, здесь высота геоида над эллипсоидом считается равной нулю).

Особенно важно определение ИГД для случая, когда ССО представляют собой современные подвижные комплексы технических средств (ПКТС), для которых определение ИГД осуществляется по информации систем наземной навигации (СНН). В рассматриваемом случае ПКТС представляют собой подвижные железнодорожные и грунтовые объекты, причём, для первых

требования к точности определения координат выше, в силу большей средней скорости передвижения и длительности маршрута.

В свою очередь из заданных условий известно, что СНН являются *автономными,* т.е. реализующими *принцип счисления пути*, не требующий внешней информации для определения координат ПКТС, что полностью удовлетворяет предъявляемым к ним требованиям.

Список литературы

1. Августов, Л.И. Автономная навигация по контурам местности / Августов Л.И., Бабиченко А.В. // Оборонная техника, Москва, 2014, №3-4. - С.58 - 63.

2. Котов, Н.И. Физико-теоретические основы навигации: Учебное пособие. – Серпухов: МО РФ, 2008. – 310 с.

УДК 656.7

Управление объединенными запасами эксплуатантов с малым паркам воздушных судов на основе телекоммуникационных систем сбора эксплуатационных данных

Субботин В. С.

ФГБОУ ВО МГТУ "СТАНКИН", г. Москва, Россия

Аннотация: *в статье предложена цифровая среда интеллектуального администрирования объединённых запасов малых эксплуатантов, использующая телекоммуникационные системы связи. Система объединяет спрос, юридически независимых участников и обрабатывает передаваемые данные о наработке, отказах и техническом состоянии ВС. В модель непосредственно включены готовность связи и вероятность доставки агрегата. В расчётном сценарии запас сокращён до 26,9 %, его стоимость — до 36,1 % исходного уровня, а риск простоя из-за отсутствия агрегата — в 4,6 раза.*

Ключевые слова: *техническая эксплуатация воздушных судов (ТО ВС), телекоммуникационные системы связи, объединение данных и запасов (пуллинг), надёжность авиационной техники, малые эксплуатанты, поддержание лётной годности (ПЛГ).*

Актуальность

Указ Президента Российской Федерации от 7 мая 2024 г. № 309 [1] предусматривает повышение авиационной подвижности населения и расширение доли отечественных ВС, что требует устранения ограничений технической эксплуатации и снабжения.

Исследования по эффективности технической эксплуатации и экономики поддержания лётной годности, представленные в работах С. В. Далецкого и Д. В. Борисенко [6, 7] показывают особую уязвимость малых парков и эксплуатантов удалённых регионов. При одном-двух ВС редкие события делают индивидуальную оценку спроса статистически неустойчивой, а округление потребности до целой единицы создаёт одновременно дефицит у одних участников и неиспользуемый запас у других.

Ограниченность статистики малых парков отмечена EASA [3], а CASA AC 42-03 допускает объединение сопоставимых данных нескольких эксплуатантов одного типа [20]. Поэтому для улучшения условий эксплуатации удалённых парков принципиально важны одновременное объединение запасов (пуллинг) и данных, устойчивый телекоммуникационный обмен и логистическая достижимость агрегатов [2, 5].

Эффекты централизации и пуллинга запасных частей исследованы в работах [8,9, 13–16], а совместное обучение и адаптация запасов к состоянию снабжения — в [17, 18]. Однако эти подходы не связывают в одном расчёте наблюдаемость независимого участника, готовность канала связи и вероятность доставки агрегата в допустимое время.

В этих условиях одним из наиболее перспективных решений является внедрение системы интеллектуального администрирования объединенных запасов малых эксплуатантов и данных на основе систем телекоммуникационной связи. Система обеспечивает пуллинг юридически независимых эксплуатантов без передачи права собственности. Условное обозначение системы в работе «ИНВАЭРО». Предлагаемая система развивает подходы [6, 7] для распределённой цифровой среды. Готовность связи и доставка непосредственно изменяют состав доступного контура, расчётный запас и риск простоя.

Постановка задачи

Цель работы — снизить затраты малых эксплуатантов и повысить обеспеченность критичными компонентами посредством «ИНВАЭРО», объединяющей спрос на основе эксплуатационных данных, передаваемых телекоммуникационными системами. Объединяются данные и права доступа к части запаса; право собственности и юридическая самостоятельность участников сохраняются.

На рисунке 1 показано, что от малых операторов в систему передаются только данные, функционально связанные с расчётом: конфигурация борта, эксплуатационная наработка, события отказов, параметры логистики и экономические оценки дефицита. На выходе система выдаёт не «сырые данные», а расчётно-обоснованные решения для объединённого обеспечения: общую потребность по позиции, долю участия γ_i, рекомендации по перемещению $x_{ki,j}$ и приоритеты снабжения. Важно не только наличие связи как таковой, но и её коэффициент готовности, так как именно он определяет полноту наблюдения ρ_k и, следовательно, эффективное число участников объединения $n_{\text{эфф}}^{(i)}$. Идентификация P/N, S/N, ресурса и истории компонента рассматривается как условие прослеживаемости и допустимости обмена [11].

Таблица 1 – Перечень входных сигналов, математических переменных и выходных решений

Группа данных	**Обозначение**	**Что означает**	**На какую формулу влияет**	**Что система выдаёт**
Состав парка	$N_{вс}$, QPA_j	число ВС и число изделий на борту	μ_{ij}	базовая потребность по позиции
Эксплуатация	FH, n_{kj}, $H_{kj,}$ $MTBUR_{ij}$	годовой налёт, события съёма, наработка и оценка MTBUR	$\lambda_{дан,j}(i)$, μ_{ij}, σ_{ij}	оценка надёжности, скорректированный спрос и запас
Логистика	TAT_j, LT_j, tk_i, $T_{доп}$	время ремонта, поставки и допустимый простой	μ_{ij}, $n_{эфф}(i)$	окно покрытия и допустимые маршруты перемещения
Связь	ke, Rk	готовность каналов и маршрут передачи данных	ρk, qki,j, nэфф(i)	набор наблюдаемых участников
Экономика	$C_{u,j}$, $C_{o,j}$	потери от дефицита и стоимость хранения	p^*_j, z^*_j	целевой уровень и квантиль обеспеченности
Прослеживаемость	P/N, S/N, ресурс, история	идентичность и допустимость обмена агрегатом	Ограничения по допустимым заменам	разрешение/ запрет передачи
Доступность объединения	ρ_k, w_{ki}, $n_{эфф}(i)$	полнота наблюдения, доставка и фактический вклад участника	$\mu_{эфф,j}(i)$, $\sigma_{эфф,j}(i)$, $S_{общ,j}(i)$	доступный общий запас и маршруты передачи
Результат обеспечения	A_{ij}, $N_{AOG,ij}$, R_i	вероятность своевременного обеспечения, необеспеченные критичные заявки и ожидаемые простои	A_{ij}, R_i	контроль обеспеченности и риск простоя на одно ВС в год

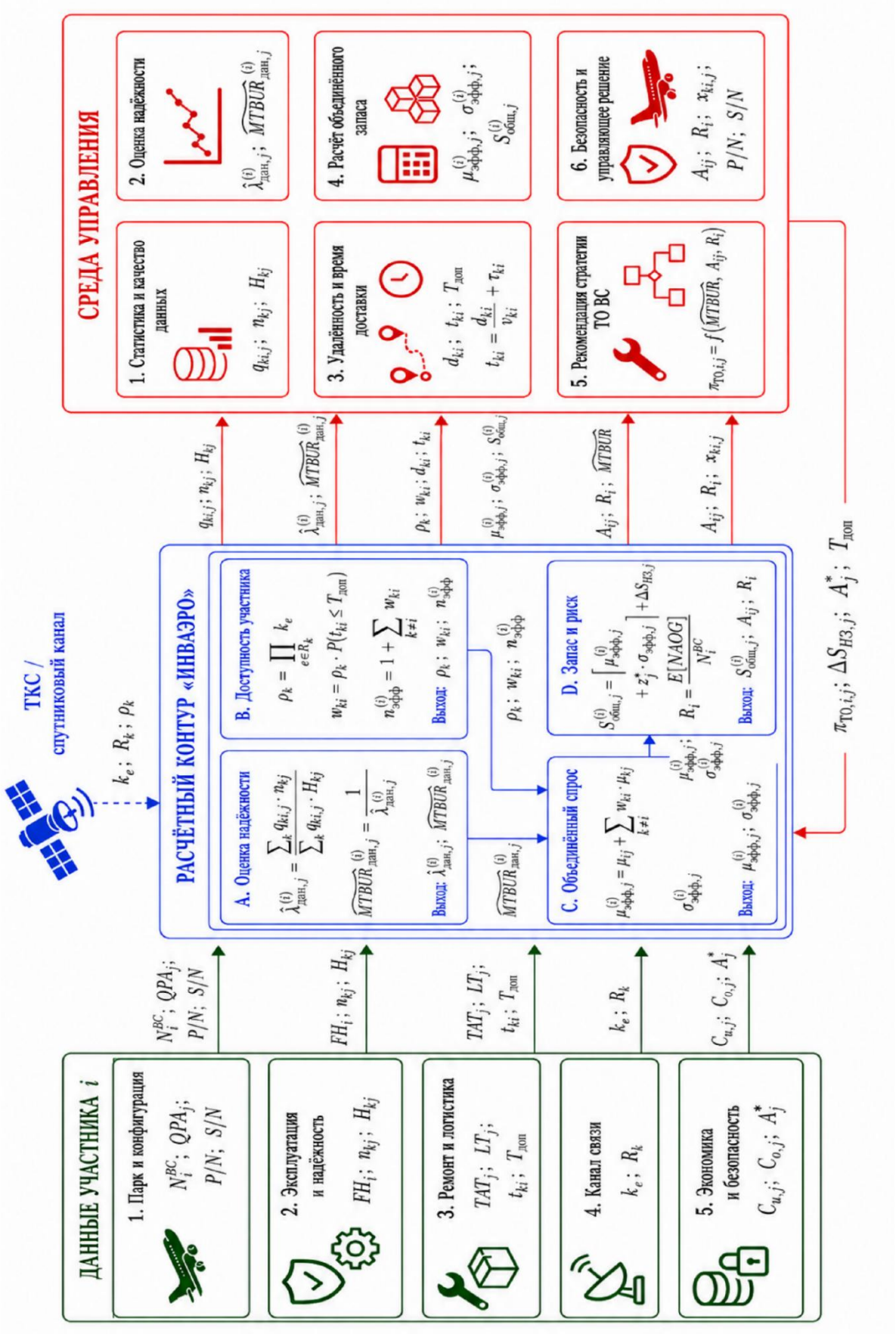


Рис. 1. Архитектура цифровой среды ПЛГ «ИНВАЭРО» с ТКС

Математическая модель

Чтобы объединение эксплуатационных данных влияло на расчёт, отдельно вводится информационный вес $q_{ki,j}$. Он учитывает наблюдаемость участника q_k и сопоставимость его данных $c_{ki,j}$ по типу и конфигурации ВС, режиму эксплуатации, среде и процедурам ТО:

$$q_{ki,j} = \rho_k \cdot c_{ki,j},\ 0 \le c_{ki,j} \le 1. \quad (1а)$$

Для базового расчётного сценария однотипных ВС при сопоставимых условиях принимается $C_{ki,j} = 1$. Условия сопоставимости соответствуют требованиям к объединению данных малых парков [20].

$$\hat{\lambda}^{(i)}_{\text{дан,j}} = \frac{(\sum_k q_{ki,j}\ n_{kj})}{(\sum_k q_{ki,j}\ H_{kj})}, \quad (1б)$$

где n_{kj} – число подтверждённых внеплановых съёмов позиции j у участника k за наблюдаемый период; H_{kj} – суммарная экспозиция (наработка) соответствующей совокупности изделий. Рабочая оценка средней наработки до внепланового съёма для объединённой информационной выборки определяется как $\widehat{\text{MTBUR}}^{(\iota)}_{\text{дан,j}} = 1/\hat{\lambda}^{(i)}_{\text{дан},j}$. При $q_{\text{ki,j}} = 0$ данные участника не входят в текущую оценку. Для ремонтопригодных систем при выявленном тренде отказов вместо постоянной интенсивности должна применяться модель непостоянного потока, например степенной процесс Crow–AMSAA [12]; статистический контроль показателей надёжности выполняется с учётом требований [4].

В режиме объединения данных величина $\text{MTBUR}_{\text{i},j}$ в выражении (1) заменяется на $\text{MTBUR}_{\text{дан},j}(i)$; при самостоятельном расчёте используется собственная статистика участника. Тем самым формируется замкнутая цепочка:

«наблюдаемые события и наработка → оценка надёжности → потребность → запас».

Средняя потребность i-го участника по позиции j за цикл пополнения определяется выражением (1); принятые индексы и математические обозначения используются в стандартной научно-технической трактовке [11].

$$\mu_{ij} = \frac{N_{BC,i}\ QPA_j\ FH_i\ (TAT_j + LT_j)}{\text{MTBUR}_{ij} \cdot 365}. \quad (1)$$

Здесь $N_{BC,i}$ – размер парка i-го участника; QPA_j – число изделий позиции j на одном воздушном судне; FH_i – годовой налёт; $\text{MTBUR}_{\text{i},j}$ – средняя наработка до внепланового съёма; TAT_j – время ремонта; LT_j– срок поставки.

В базовом сценарии, TAT и LT суммируются, поскольку являются последовательными интервалами одного цикла покрытия. Если ремонт и

поставка выполняются параллельно, продолжительность цикла принимается равной max(TAT, LT).

Разброс потребности задаётся дисперсией σ_{ij}^2. Для базового сценария редких независимых съёмов принимается пуассоновская модель $\sigma_{ij}^2 = \mu_{ij}$. Если эмпирическая дисперсия превышает среднее, используется коэффициент сверхдисперсии $\varphi_j \geq 1$: $\sigma_{ij}^2 = \varphi_j \, \mu_{ij}$, который оценивается по историческому окну. При объединении потоков спроса суммарная дисперсия определяется выражением (2).

$$\sigma_{\sum,j}^2 = \sum_{i \in K} \sigma_{ij}^2 + 2 \sum_{\substack{i,k \in K \\ i<k}} r_{ik,j} \sigma_{i,j} \sigma_{kj}, \quad (2)$$

где $r_{ik,j} = Corr(D_{ij}, D_{kj})$ – коэффициент корреляции потоков спроса i-го и k-го участников по позиции j. В базовом сценарии для выражения (2) принимается независимость потоков, $r_{ik,j} = 0$; ненулевая корреляция рассматривается как ограничение, уменьшающее эффект объединения. При полной доступности участников ($w_{ik,j} = 1$) и $r_{ik,j} = 0$ выражение (7) сводится к обычному суммированию дисперсий, представленному частным случаем выражения (2).

Полнота наблюдения k-го участника определяется готовностью телекоммуникационного маршрута R_k по выражению (3).

$$\rho_k = \prod_{e \in R_k} k_e, \quad (3)$$

где k_e — коэффициент готовности канала e. Произведение в (3) соответствует последовательному телекоммуникационному маршруту и предполагает независимость отказов его звеньев. При общей причине отказов или резервировании каналов ρ_k должна определяться по модели надёжности соответствующей структуры. Значение ρ_k, а не просто число подключённых операторов, характеризует наблюдаемость участника в общей системе.

Связь телекоммуникационной и логистической доступности с запасом задаётся коэффициентом фактического участия k-го оператора в контуре обеспечения i-го участника, определяемым выражением (4).

$$w_{ki} = \rho_k \, P(t_{ki} \leq T_{\text{доп}}), \quad (4)$$

где $0 \leq w_{ki} \leq 1$; согласно (4), значение $w_{ki} = 1$ соответствует полностью наблюдаемому участнику, запас которого достижим в допустимое время, а $w_{ki} = 0$ исключает его вклад из объединённого контура. t_{ki} – время доставки агрегата от участника k к участнику i; $T_{\text{доп}}$ – предельно допустимое время обеспечения заявки участника i.

Эффективное число участников для i-го эксплуатанта определяется выражением (5).

$$n_{\text{эфф}}^{(i)} = 1 + \sum_{\substack{k \in K \\ k \neq i}} w_{ki}, \quad (5)$$

где w_{ki} — коэффициент фактического участия k-го оператора в обеспечении i-го участника, определяемый по выражению (4); $k \neq i$. Величина $n_{\text{эфф}}^{(i)}$ представляет собой эквивалентное число полностью наблюдаемых и логистически доступных участников для контура обеспечения эксплуатанта i. Она является безразмерной и может принимать нецелые значения. Следовательно, $n_{\text{эфф}}^{(i)}$ (5) характеризует не номинальное число зарегистрированных участников, а сумму их фактических вкладов с учётом готовности связи и вероятности доставки агрегата в допустимый срок.

Для участника i средняя потребность, статистически доступная для совместного обеспечения по позиции j, определяется выражением (6).

$$\mu_{\text{эфф},j}^{(i)} = \mu_{ij} + \sum_{\substack{k \in K \\ k \neq i}} w_{ki}\mu_{kj}. \quad (6)$$

При независимости потоков спроса и событий доступности соответствующая дисперсия определяется выражением (7).

$$\sigma_{\text{эфф},j}^{2(i)} = \sigma_{ij}^2 + \sum_{\substack{k \in K \\ k \neq i}} [w_{ki,j}\sigma_{kj}^2 + w_{ki,j}(1 - w_{ki,j})\mu_{kj}^2]. \quad (7)$$

Дополнительное слагаемое $w_{ki,j}(1 - w_{ki,j})\mu_{kj}^2$ в (7) учитывает неопределённость самого факта участия k-го оператора. При $w_{ki} = 1$ выражение (7) сводится к обычному суммированию дисперсий; при $w_{ki} = 0$ вклад участника исчезает. Тем самым готовность связи ρ_k по (3) и возможность доставки через (4) непосредственно входят в параметры конечного расчёта запаса.

После расчёта $n_{\text{эфф},j}^{(i)}$ и $\sigma_{\text{эфф},j}^{(i)}$ по (6)–(7), а также $n_{\text{эфф}}^{(i)}$ по (5), система сначала определяет экономически обоснованный критический уровень по выражению (8).

$$\rho_j^* = \frac{C_{u,j}}{C_{u,j} + C_{o,j}}, \quad (8)$$

где $C_{u,j}$ — ожидаемые потери от дефицита и простоя, а $C_{o,j}$ — стоимость хранения. Обе величины должны быть приведены к одной расчётной базе и одному временному горизонту. По критическому уровню ρ_j^*, найденному из (8), определяется квантиль стандартного нормального распределения по выражению (9).

$$\rho_j^* = \Phi^{-1}(\rho_j^*), \quad (9)$$

где $\Phi(\cdot)$ — функция распределения стандартной нормальной случайной величины, а $\Phi^{-1}(\cdot)$ — её обратная функция. Общая потребность в пуле затем рассчитывается по выражению (10). Для критичных позиций полученный экономический уровень дополнительно проверяется по ограничению безопасности (12).

$$S_{\text{общ},j}^{(i)} = \lceil \mu_{\text{эфф},j}^{(i)} + z_j^* \sigma_{\text{эфф},j}^{(i)} \rceil + \Delta S_{\text{НЗ},j}. \quad (10)$$

Здесь $\Delta S_{\text{НЗ},j}$ – дополнительный неделимый резерв по позиции j, задаваемый требованиями критичности, эксплуатационными ограничениями или принятой политикой аварийного запаса. В базовом сравнительном сценарии $\Delta S_{\text{НЗ},j}$ одинаков для сопоставляемых вариантов; при отсутствии отдельного обязательного резерва принимается $\Delta S_{\text{НЗ},j} = 0$.

Риск простоя определяется выражением (11) как ожидаемое число случаев, когда критичная заявка не обеспечена агрегатом в течение допустимого времени $T_{\text{доп}}$, в расчёте на одно воздушное судно за год.

$$R_i = \frac{1}{N_{BC,i}} \sum_{j \in J_{kp}} E\left[N_{AOG,ij}\right], \quad (11)$$

где $N_{AOG,ij}$ – число за год критичных заявок по позиции j, не обеспеченных в течение $T_{\text{доп}}$; R_i в (11) измеряется в ожидаемых простоях на одно ВС в год. Такая трактовка отделяет риск дефицита запаса от технической вероятности отказа самого компонента.

Для воспроизводимого расчёта математическое ожидание числа необеспеченных заявок связывается с годовой интенсивностью критичных запросов Λ_{ij} и вероятностью превышения допустимого времени обеспечения:

$$E\left[N_{AOG,ij}\right] = \Lambda_{ij} \cdot P\left(T_{\text{обесп},ij} > T_{\text{доп},ij} | S_{\text{общ},j}^{(i)}\right), \quad (11a)$$

где $T_{\text{обесп},ij}$ включает наличие агрегата в доступном контуре и фактическое время его перемещения. При моделировании эта вероятность определяется по тем же ограничениям наблюдаемости и логистической достижимости, что и коэффициент w_{ki} , поэтому показатель Ri непосредственно связан с рассчитанным запасом и состоянием распределённой сети.

Безопасность и управляемая обеспеченность критичных компонентов

Для критичных компонентов (No-Go) сокращение запаса допустимо только при сохранении заданного уровня своевременного обеспечения [2, 3]. Значения 98,5–99,5 % используются как эксплуатационный ориентир, сопоставимый с открытыми данными ATR и Airbus [20, 21], а не как универсальная норма регулятора.

В модели «ИНВАЭРО» требование безопасности переводится в управляемое ограничение по вероятности своевременного обеспечения критичной заявки. Для позиции j вводится минимально допустимый уровень A_j^*, а рассчитанный по (8)–(10) запас принимается только при выполнении условия (12).

$$\text{A}_{ij} = P\left(T_{\text{обесп},i,j} \le T_{\text{доп},i,j} | S_{\text{общ},j}^{(i)}, \rho, W\right) \ge A_j^*, \quad (12)$$

где $W = \{w_{ki}\}$ матрица коэффициентов фактического участия операторов.

Тем самым объединение позволяет управлять целевым уровнем обеспеченности: при высоком A_j^* система повышает расчётный запас или резервирует доступные агрегаты, а при росте числа наблюдаемых и логистически достижимых участников тот же уровень может поддерживаться

меньшим суммарным запасом. Малый эксплуатант получает возможность повысить обеспеченность за счёт общей статистики и распределённого доступа к компонентам без объединения собственности.

Важно, что речь не идёт о снижении требований к допуску воздушного судна к полёту. При отказе No-Go-компонента воздушное судно остаётся неготовым до выполнения всех установленных процедур. Эффект цифровой среды состоит в повышении вероятности того, что исправный, допустимый к установке и документально прослеживаемый агрегат будет найден и доставлен в пределах $T_{доп}$. При ухудшении связи или невозможности доставки участник автоматически теряет часть веса w_{ki} , а расчёт переходит к более консервативному уровню запаса; поэтому деградация телекоммуникационного контура не маскируется моделью.

Непрерывная история P/N и S/N, наработки, установок, съёмов, отказов и ремонтов позволяет выявлять повторные и групповые отказы и сохранять прослеживаемость компонентов [3, 10].

Результаты расчёта

Модельный сценарий охватывает 977 позиций и десять независимых владельцев единичных ВС одного типа при налёте 2250 ч на борт в год. При неизменных исходных параметрах менялся только способ формирования запаса. Пуллинг сократил число единиц до 26,9 %, стоимость — до 36,1 % исходного уровня, а ожидаемые простои — с 0,467 до 0,102 на одно ВС в год.

Таблица 2 – Зависимость эффекта объединения от полноты наблюдения участников.

Полнота наблюдения	Участники	Единиц запаса	Стоимость запаса, млн руб.	Простоев на 1 ВС в год	Экономия стоимости
0 (канала нет)	0	14 010	9 112	0,467	0 %
0,3	3	11 977	7 964	0,390	12,6 %
0,5	5	9 706	6 703	0,306	26,4 %
0,7	7	7 396	5 348	0,229	41,3 %
0,9	9	4 977	3 949	0,150	56,7 %
1,0 (полное)	10	3 769	3 287	0,102	63,9 %

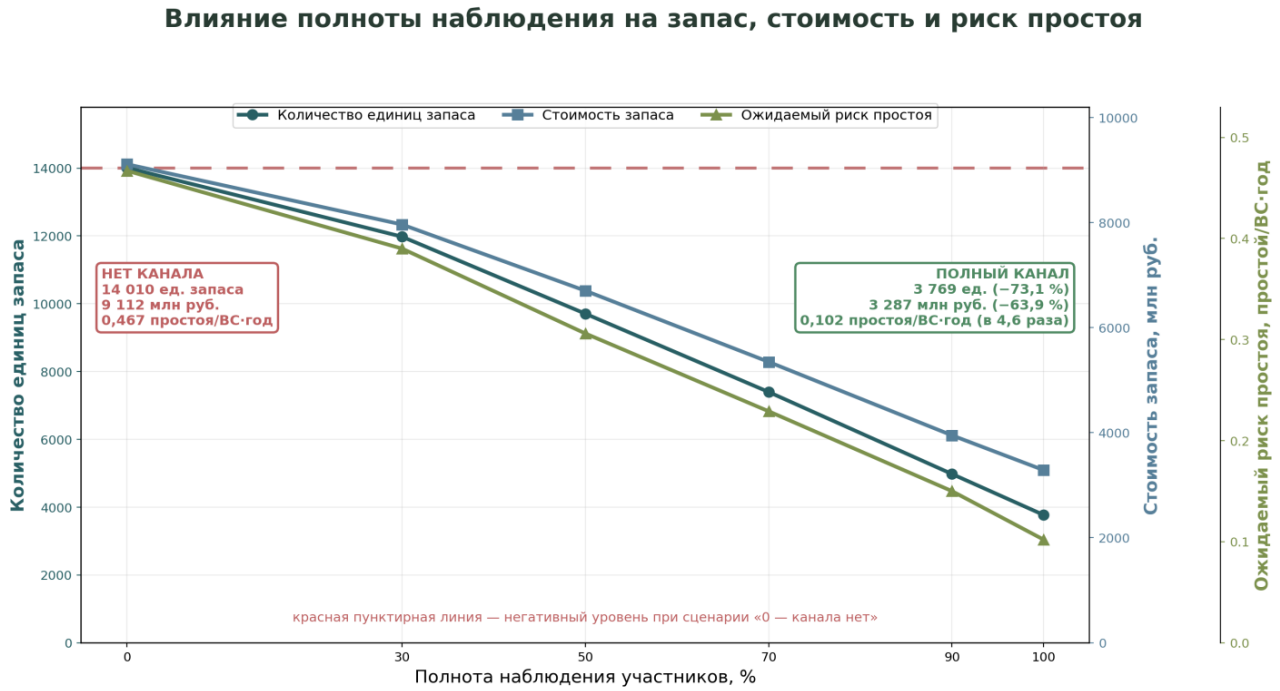


Рис. 3. Сравнение показателей при отсутствии канала и при полной наблюдаемости участников

Таблица 2 подтверждает постепенное усиление эффекта с ростом наблюдаемости: при пяти доступных участниках стоимость составляет 6 703 млн руб. и 0,306 простоя на ВС в год; при десяти — 3 287 млн руб. и 0,102 соответственно.

Существенно также, что ограничивающим фактором является не столько пропускная способность канала, сколько его готовность и стоимость устойчивого доступа. Поэтому снижение σ_k по (3) уменьшает w_{ki} по (4) и $n_{\text{эфф}}$ по (5), а через (6)–(7) – достижимый эффект объединения и расчётный запас (10). Для парков без наземного покрытия спутниковый канал является не сервисной, а несущей подсистемой предлагаемого решения.

Выводы

1. Для малого парка индивидуальный расчёт ограничен редкостью событий и дискретностью запаса. Объединение данных повышает обоснованность оценки надёжности, а пуллинг снижает многократное резервирование.

2. Показано, какие параметры поступают от малых операторов: N_{BC}, QPA, FH, события съёма n_{kj}, накопленная наработка H_{kj}, TAT, LT, k_e, t_{ki}, Cu, Co и данные прослеживаемости. По ним формируются оценка надёжности (1a), параметры потребности и разброса (1)–(2), наблюдаемость и достижимость (3)–(7), целевой уровень обеспеченности (8)–(9), запас (10) и риск простоя (11), (11a).

3. В модельном сценарии запас сокращён до 26,9 %, его стоимость — до 36,1 % исходного уровня, а ожидаемые простои — с 0,467 до 0,102 на одно ВС в год.

4. Для удалённых регионов решающим фактором является готовность телекоммуникационного тракта: при ухудшении связи уменьшается полнота наблюдения и достигаемый эффект объединения.

Список литературы

1. О национальных целях развития Российской Федерации на период до 2030 года и на перспективу до 2036 года: Указ Президента Российской Федерации от 7 мая 2024 г. № 309 // Официальный интернет-портал правовой информации [Электронный ресурс]. – URL: http://www.kremlin.ru/acts/bank/50542?ysclid=msmwzwo1oe373966935 (дата обращения: 08.08.2026).

2. Reliability Program Methods – Standards for Determining Time Limitations: Advisory Circular AC 120-17B. – Washington: Federal Aviation Administration, 2018. – 68 p.

3. Appendix I to AMC M.A.302 and AMC M.B.301(b) – Content of the maintenance programme: ED Decision 2023/013/R // Easy Access Rules for Continuing Airworthiness. – Cologne: EASA, 2023.

4. ГОСТ 27.410-87. Надёжность в технике. Методы контроля показателей надёжности и планы контрольных испытаний на надёжность. – М.: Изд-во стандартов, 2002. – 108 с.

5. Doc 10039. Manual on System Wide Information Management (SWIM) Concept. – Montreal: ICAO, 2015.

6. Далецкий С. В., Деркач О. Я., Петров А. Н. Эффективность технической эксплуатации самолётов гражданской авиации. – М.: Воздушный транспорт, 2002. – 216 с.

7. Борисенко Д. В. Оптимизация издержек на техническое обслуживание и ремонт магистральных воздушных судов иностранного производства: дис. ... канд. экон. наук. – М.: МГТУ ГА, 2007. – 195 с.

8. Sherbrooke C. C. Optimal Inventory Modeling of Systems: Multi-Echelon Techniques. 2nd ed. – Boston: Kluwer Academic Publishers, 2004.

9. van Houtum G.-J., Kranenburg B. Spare Parts Inventory Control under System Availability Constraints. – New York: Springer, 2015.

10. Guidance Material and Best Practices for Life Limited Parts Traceability. 1st ed. – Montreal: IATA, 2020. – 64 p.

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

12. Crow L. H. Reliability Analysis for Complex Repairable Systems // Reliability and Biometry: Statistical Analysis of Lifelength / ed. by F. Proschan, R. J. Serfling. – Philadelphia: SIAM, 1974. – P. 379–410.

13. Eppen G. D. Effects of centralization on expected costs in a multi-location newsboy problem // Management Science. – 1979. – Vol. 25. – No. 5. – P. 498–501.

14. Kranenburg A. A., van Houtum G. J. Effect of commonality on spare parts provisioning costs for capital goods // International Journal of Production Economics. – 2007. – Vol. 108. – P. 221–227.

15. Kilpi J., Vepsäläinen A. P. J. Pooling of spare components between airlines // Journal of Air Transport Management. – 2004. – Vol. 10. – No. 2. – P. 137–146. – doi: 10.1016/j.jairtraman.2003.09.001.

16. Wang R., Qin Y., Sun H. Research on Location Selection Strategy for Airlines Spare Parts Central Warehouse Based on METRIC // Computational Intelligence and Neuroscience. – 2021. – Vol. 2021. – Article 4737700. – doi: 10.1155/2021/4737700.

17. Drent C., Drent M., van Houtum G.-J. J. A. N. Optimal data pooling for shared learning in maintenance operations // Operations Research Letters. – 2024. – Vol. 52. – Article 107056. – doi: 10.1016/j.orl.2023.11.009.

18. Song J.-S., Zipkin P. H. Inventory Control with Information About Supply Conditions // Management Science. – 1996. – Vol. 42. – No. 10. – P. 1409–1419. – doi: 10.1287/mnsc.42.10.1409.

19. Civil Aviation Safety Authority. AC 42-03 Reliability Programs. Version 1.1. – Australia, November 2022. – Sec. 3.13 “Pooling of data”. – URL: https://www.casa.gov.au/reliability-programs (дата обращения: 09.08.2026).

20. ATR. Previous Generations: Proven reliability — over 99.5% dispatch reliability [Электронный ресурс]. – URL: https://www.atr-aircraft.com/regional-mobility/regional-aircraft/previous-generations/ (дата обращения: 09.08.2026).

21. Airbus. A330neo: advanced to future proof your widebody fleet [Электронный ресурс]. – 11.09.2024. – Operational reliability 99.5 %. – URL: https://www.aircraft.airbus.com/en/newsroom/case-study/2024-09-a330neo-advanced-to-future-proof-your-widebody-fleet (дата обращения: 09.08.2026).

УДК 621.396.96:623.62

Способ построения ортогональных и квазиортогональных базисов Франка при реализации разделения каналов в спутниковых системах связи

Ерунов А. А., Черкашин А. П.

Военно-космическая академия имени А.Ф. Можайского, г. Санкт-Петербург, Россия

Аннотация: *Рассмотрена проблемная ситуация функционирования отечественной низкоорбитальной системы спутниковой связи в условиях ограниченного числа космических аппаратов связи. Для повышения помехоустойчивости радиоканалов предлагается переходить на многостанционный доступ с кодовым и квазикодовым разделением каналов. Такой подход позволяет компенсировать снижение пропускной способности радиоканалов, вызванное увеличением базы используемых при передаче сигналов. Так как сигналы Франка помимо ортогональности обладают хорошими автокорреляционными свойствами, именно базис Франка выбран основным для кодового разделения каналов. С целью увеличения структурной сложности сигналов, а также дополнительного увеличения пропускной способности радиоканалов с квазикодовым разделением в статье представлен новый способ построения ортогональных и квазиортогональных базисов Франка.*

Ключевые слова: *ортогональные базисы, сигналы Франка.*

Введение

В настоящее время активно развиваются низкоорбитальные системы спутниковой связи (НССС), обеспечивающие широкую зону обслуживания пользователей. Такие системы предоставляют широкий спектр услуг связи, при этом количество абонентов непрерывно возрастает. Повышение качества обслуживания достигается главным образом за счет увеличения численности спутников-ретрансляторов и повышения надежности сети.

Вместе с тем отечественные перспективные низкоорбитальные широкополосные системы спутниковой связи, находящаяся на этапе развертывания, характеризуется ограниченным количеством космических аппаратов связи (КАС). На текущем этапе это не позволяет в полном объеме удовлетворить потребности наземных абонентов.

Поскольку в зоне радиовидимости КАС одновременно функционируют аналогичные системы связи, а также могут действовать источники организованных помех, особую актуальность приобретает задача повышения помехоустойчивости радиоканалов. Одновременно ограниченность частотно-орбитального ресурса приводит к дефициту пропускной способности системы связи.

Таким образом, возникает классическое противоречие между пропускной способностью радиоканала и его помехоустойчивостью. В условиях недостаточного количества резервных линий связи решение данной задачи сводится к выбору такого метода многостанционного доступа, который

обеспечивал бы максимально возможному числу абонентов требуемое качество обслуживания при сохранении высокой устойчивости к помехам.

Методы многостанционного доступа

Организация многостанционного доступа основана на использовании технологий коммутации (сетевой уровень эталонной модели взаимодействия открытых систем — ЭМВОС) и разделения каналов (физический уровень ЭМВОС). Поскольку отечественная НССС в настоящее время характеризуется относительно невысокой структурной сложностью сети, на этапе развертывания орбитальной группировки многостанционный доступ целесообразно реализовывать преимущественно на основе методов разделения каналов.

В современных системах спутниковой связи применяются следующие основные методы разделения каналов:

- частотное (Inmarsat, WGS);
- временное (Iridium, AEHF, Milstar, OneWeb);
- кодовое (Globalstar);
- пространственное (Starlink, OneWeb, WGS, AEHF);
- комбинированное (частотно-временное, частотно-кодовое, пространственно-кодовое и др.) — Starlink, OneWeb.

Пространственное разделение основано на формировании нескольких независимых либо взаимосвязанных радиоканалов за счет пространственного разнесения передающих и приемных устройств (технология MIMO) или использования различных поляризаций сигнала. Как правило, данный метод применяется совместно с другими способами разделения каналов и позволяет многократно увеличить пропускную способность системы, а также уменьшить влияние интерференции при многолучевом распространении радиоволн.

Следует отметить, что при пространственном разделении в каждом сформированном радиоканале может использоваться любой тип сигнала независимо от выбранного способа разделения каналов. Поэтому далее рассмотрим их аналитическое представление.

Аналитическое представление сигналов при множественном доступе

При основных методах разделения в групповом радиоканале формируется сложный сигнал, который можно представить в обобщенном комплексном виде [1]:

$$S(t) = \sum_{i=0}^{N-1} S_i = \sum_{i=0}^{N-1} e^{j2\pi f_{нес} t} a_i e^{(j2\pi f_i (t-\Delta T_i)+\phi_i)} \mathrm{rect}_{T_i}, \qquad (1)$$

где $e^{j2\pi f_{нес}(t)}$ -высокочастотное опорное гармоническое колебание с несущей частотой $f_{\text{нес}}$, для удобства заменим $2\pi f_{нес}$ на радиальную частоту ω;

a_i – амплитуда i-ого сигнала;

f_i – частота i-ого сигнала

φ_i– начальная фаза i-ого сигнала

ΔT_i – задержка i-ого сигнала

T_i – длительность i-ого сигнала

Как видно из выражения 1, каждый из N сигналов S_i, отличается набором параметров модуляции (a_i, f_i, φ_i, $\mathrm{D}T_i$, T_i) гармонического колебания $e^{j2\pi f_{нес}(t)}$. Выбор этих параметров определяется таким образом, чтобы взаимная корреляция $R_{i,j}$ сигналов S_i и S_j равнялась либо была близка к 0. Физически это сводится к поиску сигналов S_i с низким уровнем взаимных помех.

Самый простой способ построения таких сигналов используется при частотном и временном разделении каналов [1-3].

Простота реализации таких сигналов приводит к тому, что доступ абонентов к групповому каналу ограничен либо временем T, либо шириной полосы пропускания DF, либо всем сразу.

По этой причине формируемые сигналы подвержены узкополосным, а также импульсным помехам. Для борьбы с такими помехами может использоваться псевдослучайная перестройка рабочей частоты (ППРЧ), однако такой подход приводит к невысокой эффективности использования частотно-временного ресурса радиоканала и плохо реализуем при многостанционном доступе более 10 абонентов одновременно.

По этой причине большее распространение получило частотное мультиплексирование с ортогональным разделением каналов (OFDM-модуляция), при котором формируется множество низкоскоростных каналов с сигналами большей длительности. Тем не менее, в условиях заградительных помех даже при OFDM-модуляции требуется переход на резервные частоты, реализация ППРЧ, либо увеличение базы сигнала.

Все это ведет к снижению эффективности использования ЧОР, и как следствие к снижению пропускной способности радиоканала. Компромиссом в данной ситуации является реализация кодового разделения каналов. В зависимости от выбранной базы сигнала B достигается выигрыш до $10\log_{10}(B)$ дБ отношения сигнал шум на приеме. При этом пропускная способность снижается только в $\sqrt{B}$, а не в B раз по сравнению с прямым расширением спектра.

Несмотря на то, что кодовое разделение каналов в коммерческих сетях связи (CDMA-2000) столкнулось с проблемами масштабирования в рамках рассмотрения систем связи двойного назначения, особенно, применения на ограниченных участках местности более чем оправдано.

Аналитическое представление группового сигнала при кодовом разделении и частотном мультиплексировании с ортогональным разделением схожи и могут быть представлены выражением 2 [4-7]

$$S(t) = \sum_{i=0}^{N-1} \sum_{k=0}^{K-1} c_k e^{j\omega(t-\Delta T_i)} \mathrm{rect}_{\Delta T_i}, \qquad (2)$$

где c_k является коэффициентом в последовательности из K $\{c_k\}$, которое соответствует начальной фазе колебания $e^{j\omega t}$.

Применительно к последовательности $\{c_k\}$ используется термин кодовая манипулирующая последовательность (КМП) [5,7-9], а ее коэффициенты c_k

задают порядок манипуляции гармонического колебания $e^{j\omega t}$

В качестве $\{c_k\}$ можно использовать ортогональные функции произвольного базиса *C*, дискретный вид которого задается матрицей $C_{K\times K}$. Каждая строка данной матрицы соответствует отдельной ортогональной функции.

Ортогональность базисных функций лучше всего продемонстрировать в виде корреляционной матрицы *R*, вычисляемой по формуле:

$$R = C \times C', \tag{3}$$

где C' - матрица комплексно-сопряженная *C*

Элементы $R_{i,j}$ соответствуют значению автокорреляционной функции при $i=j$ и взаимной корреляционной функции при $i\neq j$ последовательностей $\{c_k\}$. Для ортогонального базиса матрица *R* будет равна.

$$R = \begin{vmatrix} K & 0 & . & 0 \\ 0 & K & . & 0 \\ . & . & . & . \\ 0 & 0 & . & K \end{vmatrix} = K \begin{vmatrix} 1 & 0 & . & 0 \\ 0 & 1 & . & 0 \\ . & . & . & . \\ 0 & 0 & . & 1 \end{vmatrix}. \tag{4}$$

Фактически умножение вектора на матрицу $C_{K\times K}$ соответствует прямому преобразованию в выбранном базисе, а на $C'_{K\times K}$ обратному. Поэтому для проведения данных операций необходимо используется нормированный коэффициент $\frac{1}{\sqrt{K}}$ для всех элементов $c_{i,j}$.

Таким образом задачу множественного доступа с кодовым и квазикодового разделением каналов можно свести к поиску подходящего ортогонального базиса и выбора в нем ортогональных функций.

Разработка способа построения ортогональных и квазиортогональных сигналов в расширенном базисе Франка

Применительно к задачам кодового разделения каналов на основе фазоманипулированных расширяющих последовательностей универсальным является обобщенный базис дискретно-экспоненциальных функций (ДЭФ) [8]. При этом большинство известных последовательностей (Уолша, m-последовательности, последовательности Голда и т.д.) фактически являются частным случаем ДЭФ. Данные последовательности либо требуют реализации синхронного кодирования для кодового разделения (Уолша), либо имеют малый набор базисных функций (m-последовательности, последовательности Голда), что приводит к снижению пропускной способности радиоканала с кодовым и квазикодовым разделением.

Из обобщенного базиса ДЭФ особый интерес вызывают последовательности Франка. Помимо ортогональности они обладают хорошими автокорреляционными свойствами и изначально нашли применение в радиолокации. В то же время, поиск новых сигналов в обобщенном базисе Франка, дополнительно расширяет область его применения для задач кодового разделения каналов. Дополнительно в работе [10] установлено, что базис Франка

обладает большей вариативностью построения и является квазиортогональным дискретному базису Фурье (ДПФ) [11], реализуемого в OFDM-модуляции.

Данное обстоятельство является закономерным, так как изначально сигналы Франка были получены из базиса ДПФ [8]:

$$f_0 = \bigcap [e_i,..,e_k], i,k \in [0....K-1], \quad (5)$$

где f_0 – векторная запись дискретного сигнала Франка с периодом $M=m^2$;
$e_{\text{i и}}\, e_{\text{k}}$ – базисные функции ДПФ с периодом m;
$\bigcap$ – порядок следования e_{i} в сигнале Франка, который включает все возможные варианты перестановок $P = m!$

В работе [8] описан метод построения базиса Франка, который основан на проведении операции m-ичного сдвига [9] применительно к исходному сигналу f_0. Поскольку сигнал f_0 является векторной формой представления ДПФ обозначим проводимую операцию m-ичного сдвига в виде логической функции *frank*, совершаемой над выбранным базисом E

$F=frank(E)$. (6)

Принцип операции m-ичного сдвига удобнее рассмотреть над базисом E с малыми основанием m=2 и m=3.

$$E_2 = \begin{vmatrix} 1 & 1 \\ 1 & -1 \end{vmatrix}, \qquad E_3 = \begin{vmatrix} 1 & 1 & 1 \\ 1 & e^{-\frac{\pi}{3}i} & e^{-\frac{2\pi}{3}i} \\ 1 & e^{-\frac{2\pi}{3}i} & e^{-\frac{2\pi}{3}i} \end{vmatrix},$$

Сперва получим первую ортогональную функцию базиса Франка f_0

$$f_0 = |1 \quad 1 \quad 1 \quad -1| \qquad f_0 = \left|1 \quad 1 \quad 1 \quad 1 \quad e^{-\frac{\pi}{3}i} \quad e^{-\frac{2\pi}{3}i} \quad 1 \quad e^{-\frac{2\pi}{3}i} \quad e^{-\frac{\pi}{3}i}\right|.$$

Элементы f_0 нумеруются в соответствии с m-ичной системой счисления

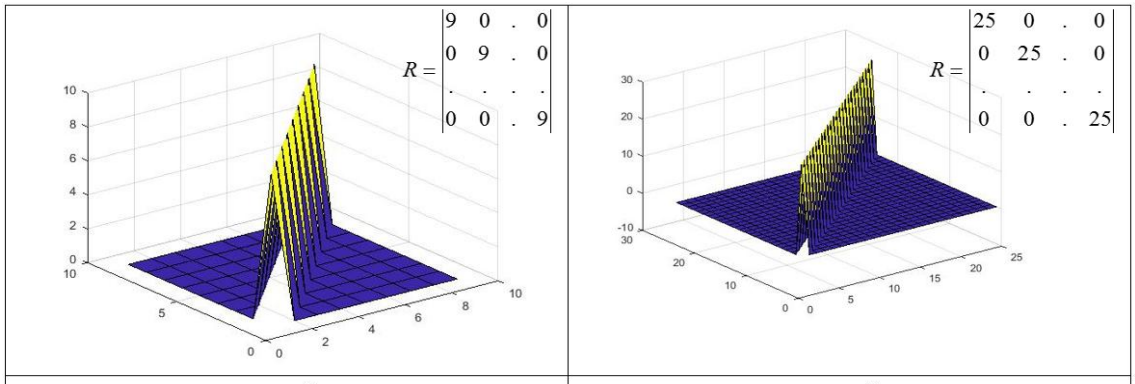
$$f_0 = |1^{00} \quad 1^{01} \quad 1^{10} \quad -1^{11}| \qquad f_0 = \left|1^{00} \quad 1^{01} \quad 1^{02} \quad 1^{10} \quad e^{-\frac{\pi}{3}i_{11}} \quad e^{-\frac{2\pi}{3}i_{12}} \quad 1^{20} \quad e^{-\frac{2\pi}{3}i_{21}} \quad e^{-\frac{\pi}{3}i_{22}}\right|$$

Последующие ортогональные функции базиса Франка f_l, $l=1...m^2-1$, получаются из $f_{0,}$ путем перестановки ее элементов согласно правилу:

$$f_l = f_0|00+l, \quad 01+l, \quad 10+l, \quad 11+l| \qquad f_l = f\,|00+l \quad 01+l \quad 02+l \quad 10+l \quad 11+l \quad 12+l \quad 20+l \quad 21+l \quad 22+l|$$

$$f_1 = |1 \quad 1 \quad -1 \quad 1| \qquad f_1 = \left|1 \quad 1 \quad 1 \quad e^{-\frac{\pi}{3}i} \quad e^{-\frac{2\pi}{3}i} \quad 1 \quad e^{-\frac{2\pi}{3}i} \quad e^{-\frac{\pi}{3}i} \quad 1\right|$$

На рисунке 1 показана проверка ортогональности базисов Франка с основаниями m =3 и 5 в виде трехмерного графика. Горизонтальная плоскость соответствует координатам матрицы корреляции, а в вертикальной плоскости показаны ее значения. На горизонтали приведены значения автокорреляционной функции сформированных последовательностей, а на остальных областях взаимной корреляции.



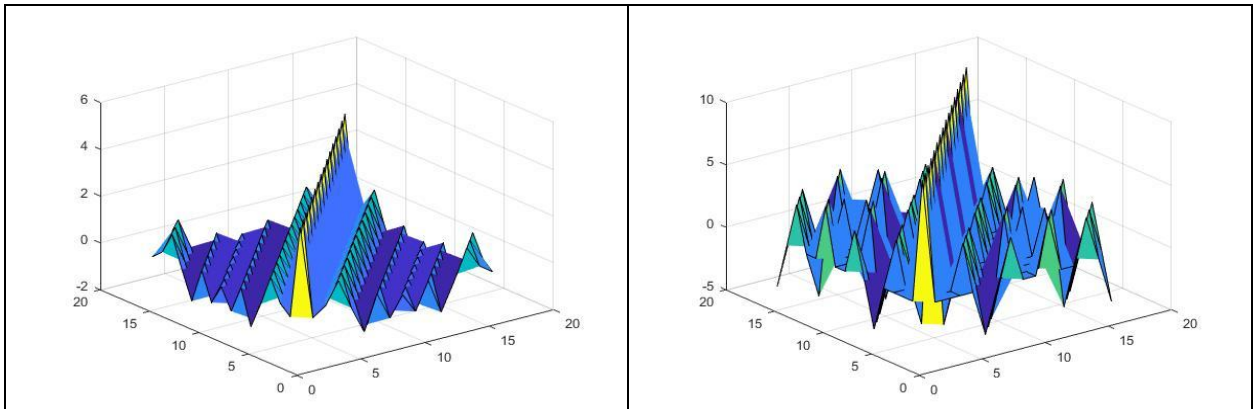
m=3	m=5
$F_9 = frank(E_3)$	$F_{25} = frank(E_5)$

Рис. 1. Проверка ортогональности базиса

В работе [12] было предложено совершенствование данного подхода за счет проведения m-ичного сдвига, применительно к произвольным базисам. Установлено, что базисы дискретного косинусного и синусного преобразований (ДКП и ДСП) не позволяют построить новый ортогональный базис за счет *m*-ичного сдвига (рис. 2).

Системы гармонических колебаний {cos(*kω*)} и {sin(*kω*)}, используемые при ДКП и ДСП имеют только односторонний интервал ортогональности [0, π) [2-3], который меньше области определения (-π, π), опорного колебания $e^{j2\pi f_{нес}(t)}$. В этой связи новые базисы необходимо выбирать из базиса ДЭФ.

В работах [7-8,10] были получены последовательности Франка-Уолша. Одним из способов задания базиса Уолша являются использование матриц Адамара, которые строятся при помощи кронекерова произведения (обозначим данную операцию в виде *kron*) матриц меньшей размерности.



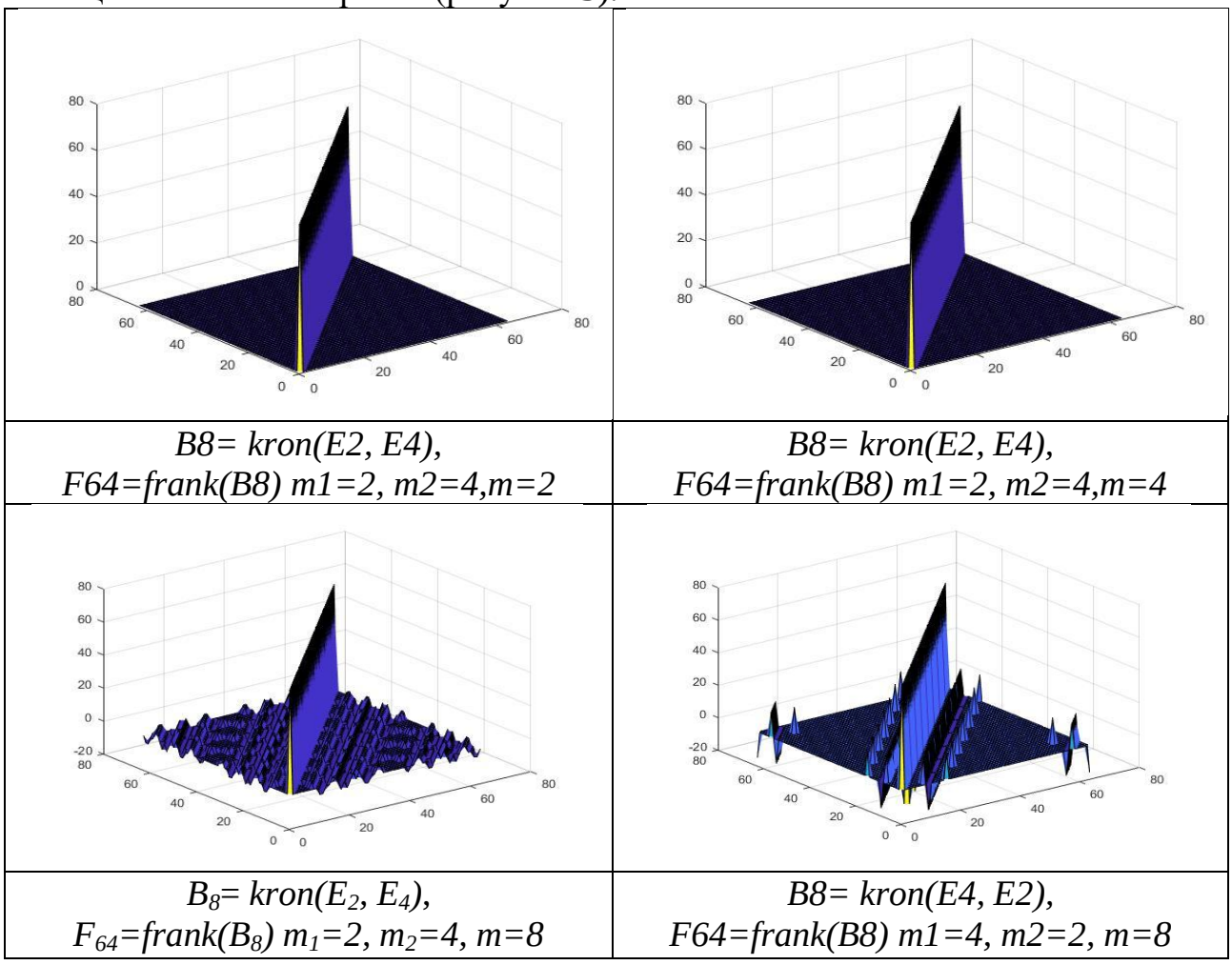
F_{16}=*frank*(Co_4), *m*=4 Франк-ДКП	F_{16}=*frank*(S_4), *m*=4 Франк-ДСП

Рис. 2. Проверка ортогональности последовательностей Франка-ДКП и Франка-ДСП

По аналогии с матрицами Адамара в работе [12] были представлены ортогональные базисы B, полученные при помощи кронекерова произведения матриц ДЭФ

$$B = kron(E, E). \quad (7)$$

В случае проведения операций *m*-ичного сдвига над указанным базисом *B* были получены новые ортогональные последовательности, являющиеся обобщением базиса Франка (рисунок 3).

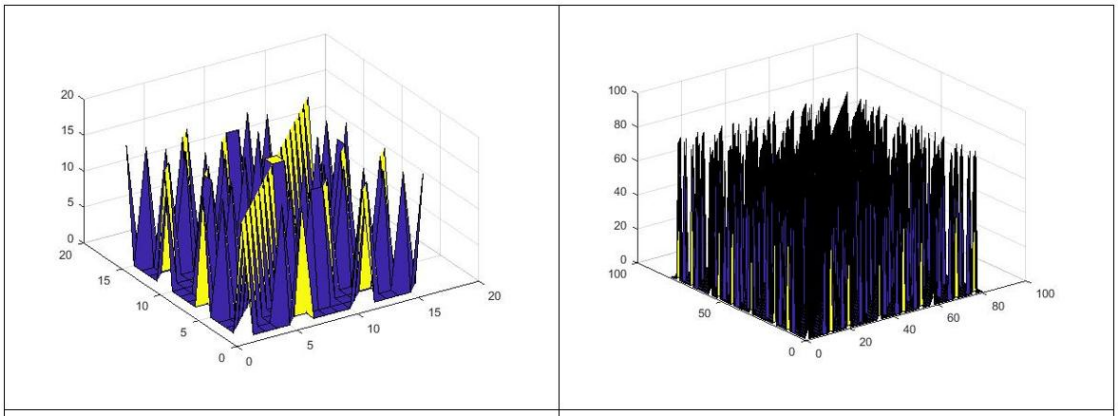


B8= kron(E2, E4), F64=frank(B8) m1=2, m2=4,m=2	*B8= kron(E2, E4), F64=frank(B8) m1=2, m2=4,m=4*
$B_8 = kron(E_2, E_4)$, $F_{64}=frank(B_8)$ $m_1=2$, $m_2=4$, $m=8$	*B8= kron(E4, E2), F64=frank(B8) m1=4, m2=2, m=8*

Рис. 3. Проверка ортогональности обобщенных последовательностей Франка

При этом ортогональность нового базиса достигается только при согласовании операции *m*-ичного сдвига с основаниями равным m_1 или m_2. В случае, когда размер *m* выбирался как $m_1 * m_2$ появлялись участки со взаимной корреляцией, не превышающей $1/m^2_1$ либо $1/m^2_2$. По мере увеличения значений m_1 и m_2, полученные последовательности можно использовать для квазикодового разделения каналов.

Дальнейший поиск новых последовательностей в базисе Франка свелся к проверке рекурсии операции *frank*, которая приводит к повторению кодовых последовательностей и не позволяет построить ортогональный базис. (рисунок 4)



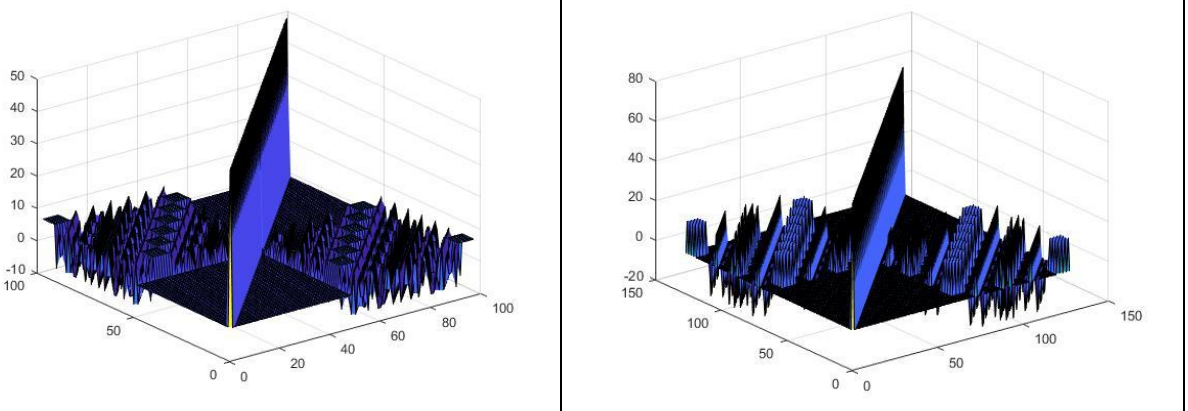
m=2	m=3
$F_{16} = frank(F_4)$	$F_{81} = frank(F_9)$

Рис. 4. Проверка ортогональности рекурсивных последовательностей Франка.

Помимо выбора исходного базиса, размера и рекурсии *m*-ичного сдвига важным является проверка вариантов перестановок $\bigcap e_i$ в исходном сигнале Франка f_0. Отдельно каждый вариант порождает ортогональный базис на периоде $N=n^2$. Однако, если корректно подобрать возможные варианты перестановок на этом же периоде можно увеличивать число используемых последовательностей Франка за счет реализации квазиортогонального разделения.

Установлено, что в зависимости от выбранного основания *n* уровень взаимных помех не превышает 1/n для нечетных и 2/n для четных значений n.

На рисунке 5 представлены результаты проверки ортогональности квазиортогональных последовательностей Франка.



$F_{49}=frank(E_7)$, m=7 133 пары из 5040 вариантов	$F_{64}=frank(E_8)$, m=8 16912 из 40320

Рис. 5. Проверка ортогональности квазиортогональных последовательностей Франка.

Так для основания m=7 условию квазиортогональности соответствует 133 пары дискретных базисов Франка из возможных 5040 вариантов перестановок. Для четного основания m=8 в относительном выражении число возможных пар выше, однако уровень взаимных помех практически в 2 раза выше. Данное обстоятельство обуславливает выбор в качестве квазиортогональных систем использовать последовательности Франка с нечетным основанием.

Заключение

Предложен новый способ построения ортогональных и квазиортогональных сигналов в расширенном базисе Франка, основанный на увеличении числа возможных вариантов формирования последовательностей при сохранении их периода. Выбор базиса Франка обусловлен его высокими корреляционными характеристиками, обеспечивающими эффективное применение как в радиолокационных системах, так и в системах связи с кодовым разделением каналов.

Разработанный способ позволяет существенно расширить пространство сигналов базиса Франка и многократно увеличить число возможных вариантов их построения. Так, для периода N=8^2 число возможных вариантов возрастает в восемь раз и достигает 8*8!=322560. Увеличение структурной сложности сигналов способствует повышению их устойчивости к имитационным помехам и расширяет возможности выделения полезного сигнала на фоне помех.

Кроме того, в базисе Франка выявлены семейства базисных функций, обладающие внутренней ортогональностью и одновременно квазиортогональные по отношению друг к другу. Наиболее благоприятные характеристики демонстрируют последовательности Франка с нечетным основанием. Для основания m=7 на периоде N=72 получено 133 пары дискретных базисов из 5040 возможных вариантов перестановок, удовлетворяющих условию попарной квазиортогональности. Из указанного множества могут быть сформированы шесть базисных систем, одновременно обладающих взаимной квазиортогональностью.

Использование предложенного подхода при реализации квазикодового разделения каналов позволяет существенно увеличить пропускную способность радиоканала при сохранении низкого уровня взаимных помех. В частности, для периода N = 1024 уровень взаимных помех составляет около 0,06 (приблизительно −14 дБ), тогда как пропускная способность радиоканала возрастает более чем в 30 раз по сравнению с традиционным кодовым разделением каналов.

Список литературы

1. Макаренко С. И. Системы спутниковой связи общего пользования и специального назначения. Монография. - СПб.: Наукоемкие технологии, 2025. - 222 с.

2. Фано Р. Передача информации. Статистическая теория связи: пер. с англ. – М.: Мир, 1965. – 438 с.

3. Финк Л. М. Теория передачи дискретных сообщений. – М.: Сов. радио, 1970. – 728 с.4. Клейнрок Л. Теория массового обслуживания / Л. Клейнрок; пер. с англ. — М.: Машиностроение, 1979. — 432 с.

4. Цветков К. Ю. Спектральный анализ сигналов в дискретных ортогональных базисах Франка // Изв. вузов. Приборостроение. – 2002. – Т.45. – № 5. – С.3-10.

5. Айзенберг Н. Н., Трофимлюк И. О. Сдвиг, свёртка и корреляционная функция дискретных сигналов в произвольном базисе // Доклады АН СССР. Сер. Кибернетика и теория регулирования. – 1980. – Т.250. – № 1. – С. 47 – 50.

6. Цветков К. Ю., Малозёмов В. Н., Машарский С. М. Сигнал Франка и его обобщения // Проблемы передачи информации. – 2001. – Т.37. – Вып.2. – С. 18 – 26.

7. Ерунов А. А., Кадуков Е. П., Черкашин А. П. Аналитическая модель сигнала с модифицированной ofdm-модуляцией для реализации квазикодового разделения каналов // Труды Военно-космической академии имени А.Ф.Можайского – 2025 № 598. С. 52-29.

8. Ерунов А. А. Методы построения ортогональных базисов для цифровой обработки сигналов // Известия института инженерной физики – 2024 – № 4 (74). С. 24-34.

УДК 004.942

Оценивание энергетической доступности источников радиоизлучений при проведении спасательных операций

Тюстин М. М., Черевань Д. В., Сивохина Н. В.

Военно-космическая академия имени А.Ф. Можайского, г. Санкт-Петербург, Россия

Аннотация: *В работе обосновывается возможность применения программно-определяемого радиоприемника (SDR) HackRF, размещенного на борту авиационного носителя, для решения задач поисково-спасательных работ (ПСР) в условиях труднодоступной местности. Предложен подход к оцениванию энергетической доступности типовых абонентских терминалов (АТ) стандартов GSM-900/1800 и автоматического радиомаяка «КОМАР-2М – КОСПАС». В рамках предложенного подхода выполнен расчет энергетического потенциала линий связи «Земля–борт» с учетом затухания сигнала в атмосфере и поляризационных потерь. Результаты моделирования подтверждают принципиальную возможность обнаружения и параметрической оценки сигналов указанных ИРИ с использованием бортового SDR-приемника.*

Ключевые слова: *SDR-приемник, поисково-спасательные работы, энергетическая доступность, абонентский терминал, «КОМАР-2М – КОСПАС».*

Введение

Ключевая задача спасательных операций – локализация и эвакуация пострадавших, оказание им первой помощи [1]. В структуре поисково-спасательных работ (ПСР) значимая роль отводится применению специализированной техники, средств связи и наблюдения, авиационных носителей различного типа для поиска объектов в зоне бедствия.

Современная практика ПСР при морских и авиационных происшествиях, лесных пожарах и горноспасательных работах активно использует наземные, авиационные и космические средства мониторинга. В состав поисковых комплексов входят оптико-электронные, радиолокационные и радиоэлектронные системы (системы радиомониторинга). Наиболее информативным источником данных о местоположении пострадавших служат источники радиоизлучений (ИРИ), к которым относятся:

− абонентские терминалы (АТ) сотовой связи, характеризующиеся высокой плотностью распределения в зонах техногенной активности;

− штатные авиационные радиостанции и радиомаяки аварийных комплектов, функционирующие в диапазонах международной спутниковой системы «КОСПАС-САРСАТ».

Анализ опыта эксплуатации авиационных средств радиомониторинга выявляет их преимущества [2]:

1. Относительно наземных средств:

− обеспечение ПСР в географически труднодоступных районах;

− повышение оперативности охвата обширных акваторий и территорий за счет высокой крейсерской скорости носителя;

− увеличение дальности радиогоризонта и, как следствие, дальности приема сигналов за счет подъема приемной аппаратуры на высоты до 10 км.

2. Относительно космических средств:

− прием более слабых сигналов за счет существенно меньшего расстояния до ИРИ и отсутствия ионосферных потерь, характерных для трассы «Земля–космос»;

− возможность оперативной обработки данных радиомониторинга в реальном масштабе времени без задержек на ретрансляцию;

− относительная простота и экономическая целесообразность.

Таким образом, для проведения ПСР на обширных и труднодоступных территориях наиболее эффективны средства воздушного радиомониторинга. Кроме того, методика планирования маршрутов поиска в природной среде позволяет оптимизировать зоны облета [2] и производить учет факторов, влияющих на эффективность ПСР.

К преимуществам использования авиационного носителя также относятся:

- относительно невысокая стоимость полетного времени;
- высокая маневренность и значительный радиус действия.
- возможность многоканального приема (установка нескольких радиоприемных устройств) для мониторинга различных частотных диапазонов;
- возможность комплексирования с оптическими средствами наблюдения для уточнения визуальной обстановки и оценки состояния пострадавших.

Критическим условием обнаружения сигналов и определения координат ИРИ является нахождение бортового оборудования радиомониторинга в пределах зоны радиовидимости, т.е. необходимость обеспечения энергетической доступности ИРИ.

Оценивание энергетической доступности источников радиоизлучений различных типов

Под оцениванием энергетической доступности ИРИ понимается расчетная процедура, определяющая возможность обработки сигнала ИРИ бортовой аппаратурой с заданными характеристиками. Для решения задачи использована методика, учитывающая коэффициенты поглощения энергии электромагнитной волны (ЭМВ) на трассе распространения.

Исходные данные:

1. высота полета носителя:

H = 6000 м;

2. приемная аппаратура:

SDR-приемник HackRF (диапазон 50–6000 МГц) с антенной круговой поляризации (LOOP с воздушным конденсатором) [3];

3. исследуемые ИРИ:

- АТ стандартов GSM-900/1800;
- радиомаяк «Комар-2М – КОСПАС».

Процедура оценивания энергетической доступности источников

радиоизлучений включает этапы:

1. анализ технических характеристик ИРИ и РПУ с целью определения параметров, необходимых для расчета мощности сигнала на входе радиоприемного устройства;
2. расчет максимальной дальности прямой видимости;
3. оценка затухания ЭМВ в атмосфере;
4. расчет мощности сигнала на входе радиоприемного устройства (РПУ);
5. расчет отношения сигнал/шум (h) для наихудших и наилучших условий;
6. формулировка вывода по правилу [4, 5]:

− 10 дБ ≤ h < 15 дБ – только обнаружение сигнала;

− h ≥ 15 дБ – обнаружение и оценивание параметров.

Структурная схема комплекса приема и регистрации радиосигналов АТ и радиомаяков индивидуальных аварийных комплектов представлена на рисунке 1.

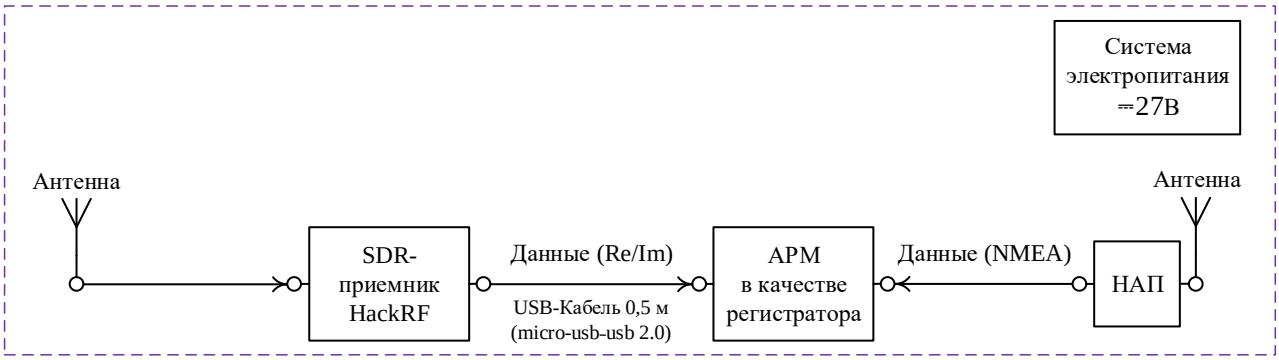


Рис. 1. Структурная схема комплекса приема и регистрации радиосигналов ИРИ

Характеристики радиоприемного устройства на базе SDR-приемника HackRF приведены в таблице 1.

Таблица 1 – Характеристики РПУ

№ п/п	Параметр	Значение
1.	Диапазон рабочих частот	50 - 6000 МГц
2.	Коэффициент усиления приемной антенны	8 дБ
3.	Пороговая чувствительность	-173 дБВт/Гц
4.	Коэффициент стоячей волны	1,6

Анализ, проведенный на основе сведений, представленный в [6-8], позволил сформулировать исходные данные для оценки доступности перечисленных ИРИ (таблица 2). В ходе расчета было принято допущение, что в качестве антенных систем для указанных радиосредств применяются

ненаправленные (изотропные) антенны.

Расчет минимальной и максимальной дальности приема выполнен на основе тригонометрических преобразований, суть которых поясняет рисунок 2.

Таблица 2 – Технические характеристики рассматриваемых ИРИ

№ п/п	Наименование ИРИ	Наименование параметра		
		Частота, МГц	Мощность передатчика, Вт	Ширина спектра сигнала, кГц
1.	АТ стандарта GSM-900	890 - 915	2	200
2.	АТ стандарта GSM-1800	1710 - 1785	1	200
3.	Радиомаяк «Комар-2М – КОСПАС» (в режиме «ближний привод – радиостанция»)	121,5	0,1	3
4.	Радиомаяк «Комар-2М – КОСПАС» (в режиме «спутниковый канал»)	406,037	5	0,4
5.	Радиомаяк «Комар-2М – КОСПАС» (в режиме «ближний привод – маяк»)	121,5	0,05	3

Минимальной дальности приема (d_{MIN}) соответствует высота полета авиационного носителя. Максимальной дальности приема (d_{MAX}) соответствует дальности прямой видимости, которая рассчитывается по формуле:

$$d_{MAX} = 4{,}12 * \left(\sqrt{d_{MIN}} + \sqrt{H_{\text{ИРИ}}}\right), \quad (1)$$

где $H_{\text{ИРИ}}$ – высота антенной системы ИРИ.

Приняв высоту антенны $H_{\text{ИРИ}}$ равной 1 м, с учетом заданной высоты полета d_{MIN} = 6 км, получаем $d_{MAX} \approx 323$ км.

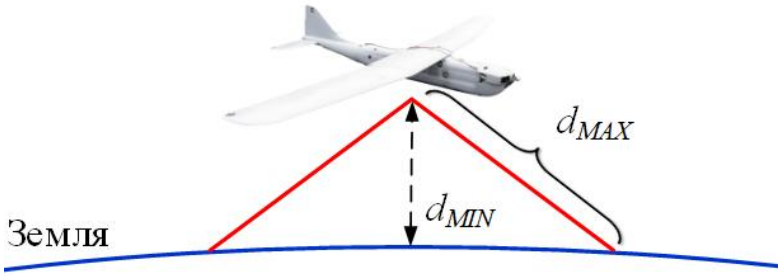


Рис. 2. Графическая модель расчета радиовидимости при проведении ПСР

Затухание в атмосфере и поляризационные потери (3 дБ) учтены согласно [9, 10]. Результаты представлены в таблице 3. Влиянием атмосферы на минимальной дальности можно пренебречь.

Таблица 3 – Значения коэффициентов поглощения энергии ЭМВ

№ п.п.	Вид ослабления		Значение (диапазон значений), дБ			
			АТ стандарта GSM-900	АТ стандарта GSM-1800	Радиомаяк «Комар-2М – КОСПАС» (в режиме «спутниковый канал»)	Радиомаяк «Комар-2М – КОСПАС» (в режиме «ближний привод»)
1.	Влияние атмосферы	при d_{MIN}	0,031	0,040	0,014	0,002
		при d_{MAX}	1,671	2,166	0,763	0,097
2.	Поляризационные потери		3			

Основа для расчета мощности сигнала на входе РПУ представлена классической формулой для расчета линий радиосвязи [11]:

$$P_{\text{ВХ}} = \frac{P_{\text{ИЗЛ}} G_{\text{ПРМ}} G_{\text{ПРМ}} \lambda^2}{(4\pi)^2 d^2} F(f), \quad (2)$$

где P_{BX} – мощность излучения на входе приемного устройства;

$P_{\text{ИЗЛ}}$ – мощность, излучаемая радиоэлектронным средством;

$G_{\text{ПРД}}$ – коэффициент усиления антенной системы ИРИ (при расчетах принят равным 1, вследствие допущения об использовании ненаправленных антенн);

$G_{\text{ПРМ}}$ – коэффициент усиления антенной системы РПУ;

d – дальность приема;

$F(f)$ – функция ослабления, характеризуемая следующим произведением:

$$F(f) = F_{\text{А}}(f) F_{\text{П}}(f) S \quad (3)$$

где $F_{\text{А}}(f)$, $F_{\text{П}}(f)$ – функции ослабления, характеризующие энергетические потери ЭМВ при распространении через атмосферу и вследствие поляризационного рассогласования;

S – коэффициент стоячей волны.

Расчет выполнен для наихудших условий приема. Под наихудшими условиями понимается прием на максимальной частоте, при минимальной мощности излучения и максимальной дальности приема. Под наилучшими условиями понимается прием на минимальной частоте, при максимальной мощности излучения и минимальной дальности приема. Результаты расчета, представлены в таблице 4.

Полученные данные подтверждают теоретическую возможность обнаружения и обработки сигналов ИРИ с использованием SDR-приемника HackRF на борту авиационного носителя.

В наилучших условиях обеспечивается обнаружение и оценивание параметров АТ GSM-900 и всех режимов работы радиомаяка «Комар-2М – КОСПАС». Для АТ GSM-1800 возможно только обнаружение (h = 10,238 дБ).

Таблица 4 – Значения коэффициентов поглощения энергии ЭМВ

№ п/п	Наименование ИРИ	Название параметра		
		Функция ослабления $F(f)$, дБ	Мощность излучения на входе РПУ, Вт	Отношение сигнал шум на входе РПУ, дБ
Наилучшие условия				
1.	АТ стандарта GSM-900	3,031	$7{,}833*10^{-12}$	**18.929**
2.	АТ стандарта GSM-1800	3,040	$1{,}059*10^{-11}$	**10,238**
3.	Радиомаяк «Комар-2М – КОСПАС» (в режиме «спутниковый канал»)	3,014	$9{,}446*10^{-10}$	**56,732**
4.	Радиомаяк «Комар-2М – КОСПАС» (в режиме «ближний привод – маяк»)	3,002	$1{,}058*10^{-10}$	**38,473**
5.	Радиомаяк «Комар-2М – КОСПАС» (в режиме «ближний привод – радиостанция»)	3,002	$2{,}116*10^{-10}$	**41,483**
Наихудшие условия				
6.	АТ стандарта GSM-900	4,671	$1{,}753*10^{-14}$	-17,572
7.	АТ стандарта GSM-1800	5,166	$2{,}055*10^{-15}$	-26,882
8.	Радиомаяк «Комар-2М – КОСПАС» (в режиме «спутниковый канал»)	3,763	$2{,}743*10^{-13}$	**21,362**
9.	Радиомаяк «Комар-2М – КОСПАС» (в режиме «ближний привод – маяк»)	3,097	$3{,}571*10^{-14}$	3,757
10.	Радиомаяк «Комар-2М – КОСПАС» (в режиме «ближний привод – радиостанция»)	3,097	$7{,}142*10^{-14}$	6,767

В наихудших условиях уверенный прием гарантирован только для радиомаяка «Комар-2М – КОСПАС» в режиме «спутниковый канал». Прием сигналов АТ стандартов GSM на предельной дальности (323 км) без дополнительных антенных систем маловероятен из-за отрицательного отношения сигнал/шум.

Заключение

Проведенное исследование подтверждает целесообразность применения SDR-приемника HackRF, установленного на авиационном носителе, для проведения поисково-спасательных работ. Предложенный подход к оценке энергетической доступности позволяет оценить возможность обнаружения

и параметрического анализа сигналов типовых источников радиоизлучений (абонентских терминалов сотовой связи и радиомаяков) в зависимости от высоты полета, дальности до объекта и условий распространения радиоволн. Результаты моделирования свидетельствуют о высокой эффективности использования низкобюджетных малогабаритных SDR-приемников для организации радиомониторинга при проведении поисково-спасательных работ
в труднодоступных районах.

Список литературы

1. Термины МЧС России - URL: https://www.mchs.gov.ru/ministerstvo/ o-ministerstve/terminy-mchs-rossii/term/3262 (дата обращения: 01.09.2026).

2. Топольский М. Г. Методика планирования поисково-спасательных работ в природной среде / Топольский М. Г., Береснев Д. С., Рыженко А. А., Мокшанцев А. В. // Технологии техносферной безопасности: Интернет-журнал – 2016. – Вып. № 3 (67). – С. 165-169. http://www.agps-2006.narod.ru/ttb/2016-3/33-03-16.ttb.pdf.

3. HackRF initial review - URL: https://www.rtl-sdr.com/hackrf-initial-review (дата обращения: 01.09.2026).

4. Калмычков, И. Е. Метод расчета порога обнаружения при параллельном обзоре полосы частот / И. Е. Калмычков, О. А. Нохрин // Наукоемкие технологии. – 2010. – Т. 11, № 9. – С. 14 – 19.

5. Чемаров, А. О. Совместное обнаружение и фазовое пеленгование источников радиоизлучения при одновременном обзоре в широкой полосе частот в условиях априорной неопределенности сигнально-помеховой обстановки: автореферат дис…канд. техн. наук: 05.12.04 / Чемаров А. О. – Санкт-Петербург, 2009. – 18 с.

6. Стандарт сотовой связи GSM-900/1800 - URL: https://www.radioscanner.ru/info/article105 (дата обращения: 01.09.2026).

7. Связь и бортовая аппаратура АО «РТИ» - URL: https://www.aorti.ru/upload/catalog/sba.pdf (дата обращения: 01.09.2026).

8. Анализ принципов построения комплексов приема, обработки и ретрансляции информации международной системы КОСПАС–САРСАТ и перспективы их развития / А.А. Романов [и др.] // Ракетно-космическое приборостроение и информационные системы – М.: Физматлит, 2017. – Т. 4, № 3. – С. 58-68.

9. Рекомендации МСЭ-R P. 676-10 (09/2013). Затухание в атмосферных газах – Женева: ITU, 2013. – 24 с.

10. Ротхаммель, К. Антенны. Том 1/ К. Ротхаммель, А. Кришке. – Пер. с нем. – М.: ЛАЙТ Лтд, 2000. – 416 с.:ил. – ISBN 5-85648-715 X.

11. Долуханов, М. П. Распространение радиоволн. Учебник для вузов / М. П. Долуханов. – М.: Связь, 1972. – 336 с.: ил.

УДК 004.942

Моделирование ракурсных изображений типовых участков местности в инфракрасном диапазоне длин волн

Ширямов О. А., Захарчук А. В.

Военно-космическая академия имени А.Ф. Можайского, г. Санкт-Петербург, Россия

Аннотация: *В работе представлена компьютерная реализация алгоритма моделирования ракурсных изображений районов местности в инфракрасном диапазоне длин волн. Представлен процесс формирования полигональной модели сцены района местности. Приведены подходы к решению вопросов расчета освещенности и затененности объектов сцены. Предложена структурная схема модели базы данных для хранения спектральных коэффициентов излучения объектов сцены. Приведены расчетные выражения для определения значений индикатрисы изучения граней объектов сцены. Предложено проводить расчет температурных полей объектов сцены с использованием библиотеки с открытым исходным кодом Partial Differential Equations в пакете прикладных программ MatLab. Представлен пример компьютерного моделирования ракурсного изображения района местности в инфракрасном диапазоне длин волн.*

Ключевые слова: *ракурсное изображение, инфракрасный диапазон длин волн, полигональная модель, сцена района местности, температурные поля, эталонное изображение.*

Введение

Эффективность применения современных образцов вооружения и военной техники (ВВТ), работающих в инфракрасном диапазоне длин волн (ИКД), существенно зависит от качества информационного обеспечения фоноцелевой обстановки, содержанием которого является эталонное изображение (ЭИ) района местности, включающий в себя подстилающую поверхность и сюжетноважные объекты инфраструктуры [1].

Формирование ЭИ в ИКД района местности, является одним из наиболее трудоемких этапов подготовки исходных данных для применения образцов ВВТ. Решение данной задачи основано на рациональном сочетании экспериментальных измерений и математического моделирования районов местности. Математические модели ЭИ в ИКД позволяют создавать аппаратно-программные комплексы имитационного цифрового моделирования, в первую очередь к ним относится пакет прикладных программ с открытым исходным кодом MatLab. Основное требование, предъявляемое к таким комплексам, – это адекватное воспроизведение в вычислительном эксперименте физических закономерностей отраженного и собственного излучения энергии подстилающей поверхности и сюжетноважных объектов инфраструктуры (рисунок 1) [2].

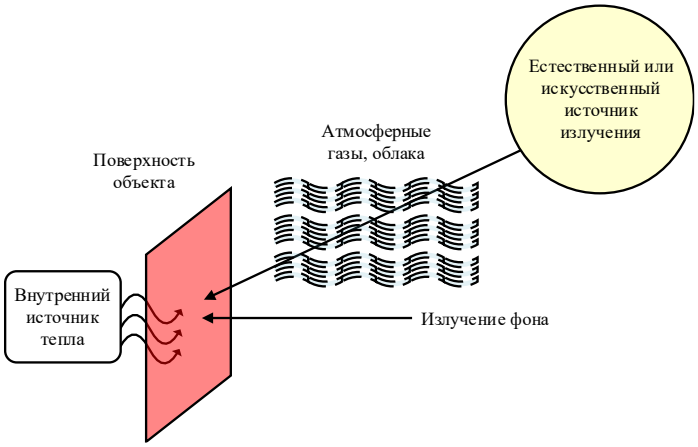


Рис. 1. Источники энергии, влияющие на объекты ЭИ в ИКД

Алгоритм моделирования ракурсных эталонных изображений районов местности в инфракрасном диапазоне

Моделирование ракурсных ЭИ в ИКД является актуальной задачей, что подтверждается многочисленными опубликованными работами данной тематики, в частности [3-6]. Однако в них не до конца раскрыты вопросы реализации моделирования на ЭВМ.

В данной работе предлагается следующий алгоритм моделирования ракурсных ЭИ районов местности в ИКД (рис. 2).

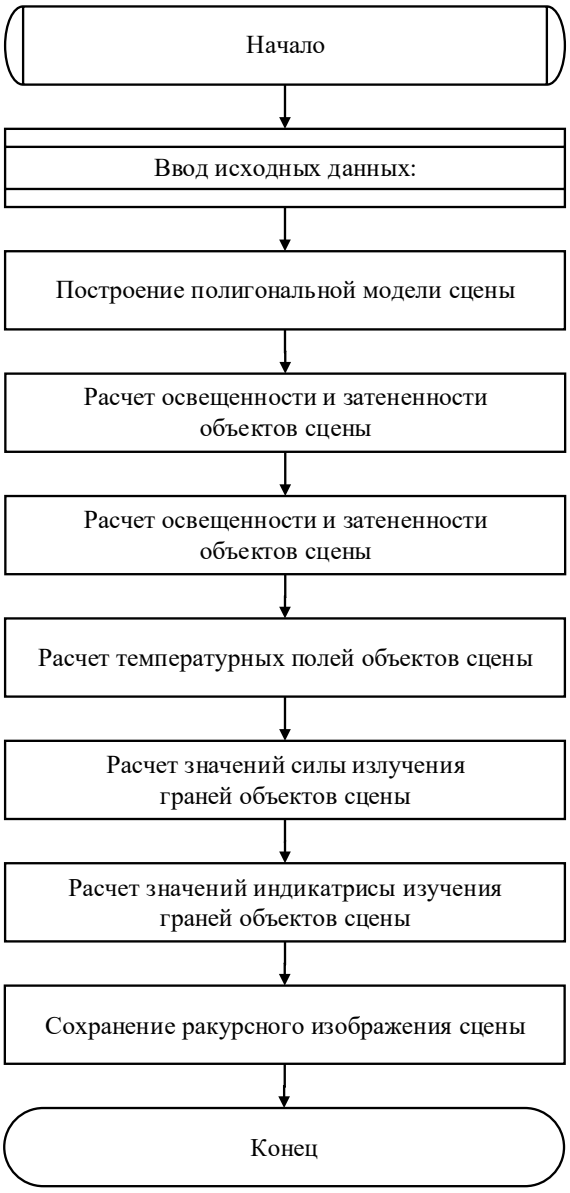


Рис. 2. Алгоритм моделирования ракурсных ЭИ районов местности в ИКД

Последовательность выполнения алгоритма следующая:

1. Начало.

2. **Блок 1.** Ввод исходных данных.

На данном этапе вводятся необходимые данные для моделирования ЭИ в ИКД:

− географические координаты моделируемой сцены *{lat, lon}*;

− дата и время моделирования сцены *D*;

− массив метеорологических параметров на дату моделирования сцены *Meteo*.

– топология подстилающей поверхности и сюжетно-важных объектов инфраструктуры, включающая массив координат точек вершин объекта и массива последовательности соединения этих вершин

{P, listPoint}, а также данные о материалах граней *M*;

– координаты точки наблюдения сцены оптико-электронной системой (ОЭС).

3. **Блок 2.** Построение полигональной модели сцены.

По значениям *{P, listPoint}* производится триангуляция граней и строится полигональная модель сцены (рисунок 3).

При этом рассчитываются значения вектора нормали *n(x,y,z)* каждой грани объектов сцены, определяющие их ориентацию в пространстве.

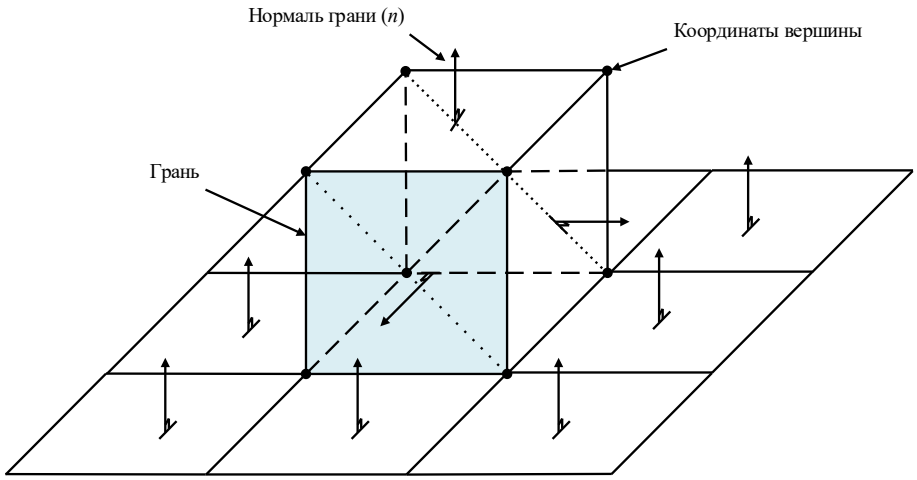


Рис. 3. Полигональная модель сцены

4. **Блок 3.** Расчет освещенности и затененности объектов сцены.

Используя исходные значения {*lat*, *lon*} и D производится расчет положения Солнца по алгоритму, предложенному в работе [7]. Результатом работы данного алгоритма являются значения азимута α_c и угла места α_l Солнца относительно моделируемой сцены. При этом абсолютная погрешность значений с астрономическим альманахом составляет не более ± 1'.

Далее производится определение угла освещенности граней объектов (рисунок 4) сцены k_{rad} в соответствии с условием:

$$\begin{cases} при\ 0 < \alpha_{rad} < 180, k_{rad} = \sin(\alpha_{rad}) \\ при\ 180 \le \alpha_{rad} \le 360\ (0), k_{rad} = 0 \end{cases}, \quad (1)$$

где α_{rad} – угол, образованный ориентацией грани объекта сцены α и значением азимута Солнца: $\alpha_{rad}=\alpha-\alpha_c$, при этом если $\alpha_{rad}<0$, то производить нормирование значения угла $\alpha_{rad}=\alpha_{rad}+360$.

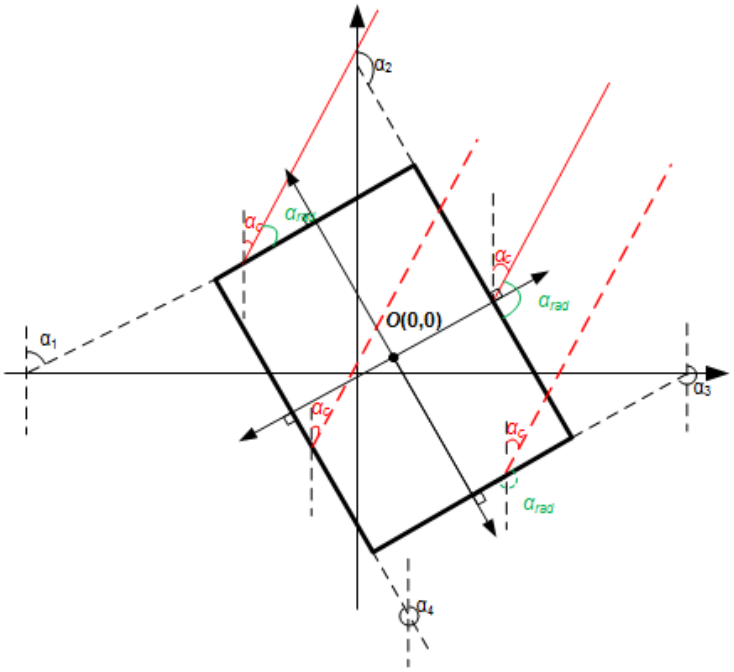


Рис. 4. Определение угла освещенности граней объектов сцены

На следующем шаге происходит расчет областей теней, образованных объектами сцены. В современном компьютерном моделировании теней используются два основных подхода [8-11] – метод теневых карт и алгоритм трассировки лучей. Однако указанные подходы не позволяют учитывать влияния областей теней на температурные поля при их попадании на грани объекта.

Предлагается использовать полигональный алгоритм построения областей теней, позволяющий учесть влияние их температурных полей на грани объектов. Алгоритм заключается в построении полигонов теней (рисунок 5) по следующим выражениям:

$$x' = \frac{x - h \cdot \sin(\alpha_c)}{tg(\alpha_l)} \tag{2}$$

$$y' = \frac{y - h \cdot \sin(\alpha_c)}{tg(\alpha_l)}, \tag{3}$$

где x, y – координаты точек вершин грани объекта;

x', y' – координаты точек вершин области тени;

h – высота объекта моделируемой сцены.

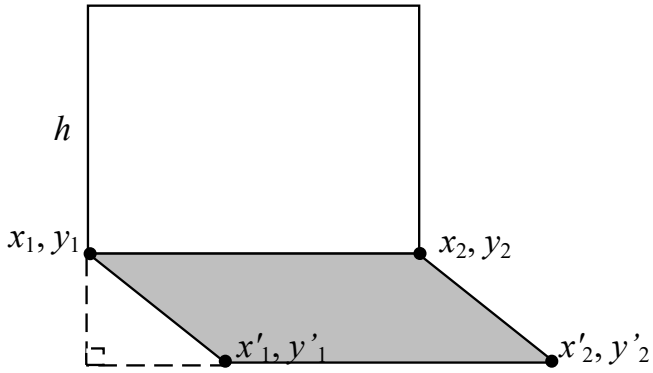


Рис. 5. Построение полигона тени

5. **Блок 4.** Расчет коэффициента ослабления излучения атмосферой.

В данном блоке на основе массива *Meteo* производится расчет коэффициентов поглощения и рассеивания инфракрасного излучения атмосферой на основе методов, предложенных в работах [12, 13].

6. **Блок 5.** Расчет температурных полей объектов сцены.

Моделирование задач, связанных с нахождением температурного поля, осуществляется на основе решения дифференциального уравнения Фурье-Кирхгофа для нестационарного переноса теплоты теплопроводностью, когда устанавливается связь между временным и пространственным изменением температуры в любой точке тела [14]:

$$\rho \cdot c \cdot \frac{\partial t}{\partial \tau} = \frac{\partial}{\partial x}\left(\lambda \cdot \frac{\partial t}{\partial x}\right) + \frac{\partial}{\partial y}\left(\lambda \cdot \frac{\partial t}{\partial y}\right) + \frac{\partial}{\partial z}\left(\lambda \cdot \frac{\partial t}{\partial z}\right) + Q_w\left(x, y, z, \tau, t\right), \qquad (4)$$

где t – температура, °С;

ρ – плотность, кг/м^3;

c – удельная теплоемкость, Дж/(кг·К);

λ – коэффициент теплопроводности, Вт/(м·К);

τ – время, с;

Q_w – мощность внутренних источников тепловыделения, Вт/м^3.

Уравнение (1) вместе с условиями однозначности дает полную математическую формулировку краевой задачи теплопередачи объектов сцены [15]. Его аналитическое решение в виду сложности геометрии реальных объектов, нелинейность уравнений, разнообразие и неустойчивость гидродинамических полей и т.п. является затруднительным. Численное моделирование уравнения может быть решено с использованием библиотеки с открытым исходным кодом *Partial Differential Equations* в пакете прикладных программ *MatLab* [16].

Результатом вытолнения текущего блока является массив температурных полей *T* граней объектов сцены.

7. **Блок 6.** Расчет значений силы излучения граней объектов сцены.

Производится расчет энергетической силы излучения граней объектов по формуле Стефана-Больцмана:

$$I = \frac{\varepsilon_\lambda \sigma T^4 S}{\omega}, \quad (5)$$

где ε_λ – спектральный коэффициент излучения материала *M* грани;

σ – постоянная Стефана-Больцмана $5{,}67 \cdot 10^8$ Вт/(м^2·К^4);

S – площадь грани, м^2;

ω – телесный угол, ср;

T – температура граней объекта, К.

При этом основным проблемным вопросом данного блока является получение значений спектрального коэффициент излучения ε_λ, так как он зависит от материала грани объекта, его состояния и степени ее окисления. Также необходимо учитывать спектральный диапазон $\lambda_1 \ldots \lambda_2$ для которого моделируется сцена.

В качестве источника значений спектрального коэффициента излучения ε_λ предлагается использовать базу данных (БД). Структурная схема модели БД представлена на рисунке 6.

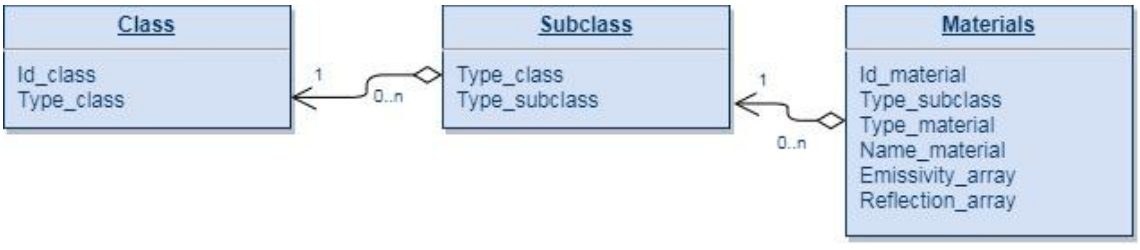


Рис. 6. Структурная схема модели БД

Модель содержит три таблицы – *Class*, *Subclass*, *Materials*. В первой и во второй таблице содержатся унифицированные классы и подклассы возможных материалов граней. В третьей – характеристики этих материалов, в том числе массив значений коэффициента излучения материала от длины волны. Такой подход позволяет с помощью SQL-запросов к БД получать данный массив, проводить его интерполяцию и дальнейшее интегрирование для получения значения спектрального коэффициента излучения выбранного диапазона длин волн.

На рисунке 7 представлен графический интерфейс работы с БД.

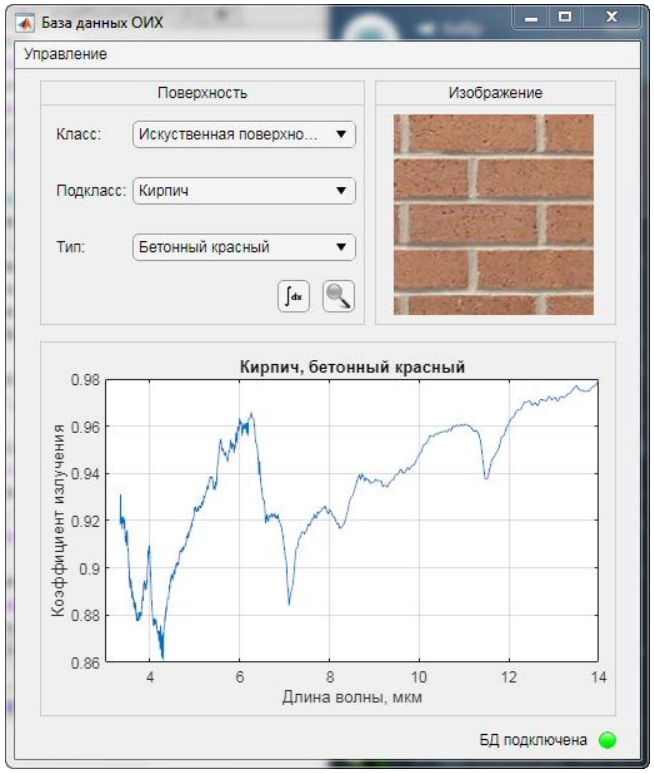


Рис. 7. Графический интерфейс работы с БД

8. **Блок 7.** Расчет значений индикатрисы изучения граней объектов сцены.

Для реальных объектов трудно построить точную индикатрису излучения в связи с многообразием форм и ориентацией излучающих поверхностей. Поэтому предлагается использовать упрощенную схематизацию грани объекта как излучателя. При этом исключаются из рассмотрения те грани, вклад которых в суммарное излучение объекта незначителен. Каждую из граней рассматривают как излучатель, подчиняющийся закону Ламберта, тогда значение энергетической силы излучения можно определить:

$$I = I_0 \cos a_v , \tag{6}$$

где I – значение энергетической силы излучения грани с учетом индикатрисы, Вт/ср;

I_0 – исходное значение энергетической силы излучения грани, Вт/ср;

α_v – угол наклона излучающей грани относительно плоскости наблюдения, град.

Для расчета значений энергетической силы излучения граней объектов сцены с учетом индикатрисы излучения предлагается использовать следующее выражение:

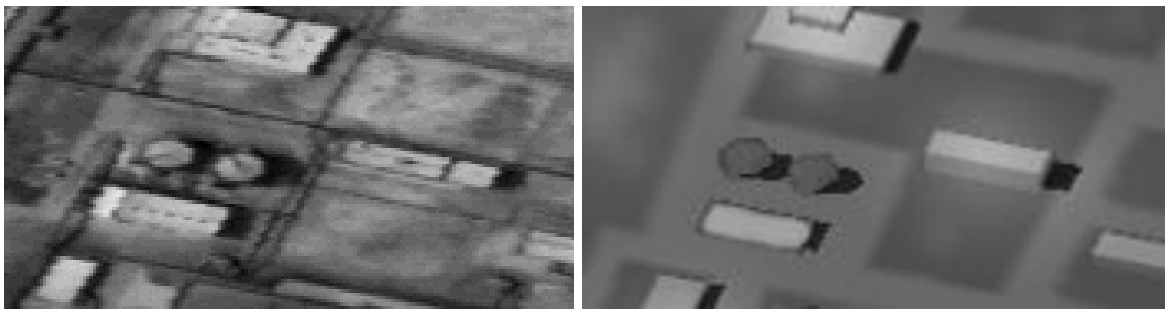
$$I = I_0 \cos\left(\arcsin\left(-\frac{\left|a_x \cdot n_x + a_y \cdot n_y + a_z \cdot n_z\right|}{\sqrt{a_x^2 + a_y^2 + a_z^2} \cdot \sqrt{n_x^2 + n_y^2 + n_z^2}}\right)\right) = I_0 \sqrt{1 - \left(-\frac{\left|a_x \cdot n_x + a_y \cdot n_y + a_z \cdot n_z\right|}{\sqrt{a_x^2 + a_y^2 + a_z^2} \cdot \sqrt{n_x^2 + n_y^2 + n_z^2}}\right)^2}, \tag{7}$$

где a – вектор направления плоскости наблюдения ОЭС к грани объекта.

9. **Блок 8.** Сохранение ракурсного изображения сцены.

На данном этапе производится сохранение сцены с учетом технических характеристик ОЭС, для которого проводится моделирование ЭИ.

На рисунке 8 представлен результат компьютерного моделирования ракурсного изображения района местности с применением алгоритма, описанного в работе.



а. б.

Рис. 8. Пример результата работы алгоритма (а. – изображение, полученное ОЭС, б – смоделированное изображение).

Заключение

Таким образом применение предложенного алгоритма позволяет выполнить компьютерное моделирование ракурсных изображений районов местности в ИКД с использованием спектральных коэффициентов излучения, хранимых в БД, значений индикатрисы изучения граней объектов сцены, а также топологии подстилающей поверхности и сюжетно-важных объектов инфраструктуры сцены.

Дальнейшим развитием моделирования ракурсных изображений является разработка алгоритма использования цифровой матрицы рельефа и космических снимков моделируемых районов местности для реализации автоматического формирования полигонной модели сцены.

Список литературы

1. Ширямов О. А., Шубин Д. А. Подход к расчету излучательных характеристик объектов инфраструктуры в дальнем инфракрасном диапазоне // Сборник трудов XXXI Всероссийского симпозиума «Радиолокационное исследование природных сред». – 2020. – С. 78-84.

2. Лабунец Л. В., Попов А. В. Математическое моделирование тепловизионного изображения 3D-объекта в ИК-координаторе цели // Вестник МГТУ им. Н. Э. Баумана. Сер. “Приборостроение”. – 2015. – №3. – С. 13-25.

3. Pavlov V., Ruser H., Horn M. Model-based object characterization with active infrared sensor array // ICSENS. – 2017. – Vol. 121. – P. 360-363.

4. Han J. Exploration of Establishing Near-Infrared Model of DDGS Feed without Grinding // Hans Journal of Food and Nutrition Science. – 2020. – Vol. 9. – P. 187-192.

5. Gabdrakhmanov I., Teryaev O., Khandramai V. L. Infrared models for the Bjorken sum rule in the APT approach // Journal of Physics: Conference Series. – 2017. – Vol. 938. – P. 122-131.

6. Хисматов И. Ф. Метод воспроизведения полей яркости наземной фоноцелевой обстановки при имитационном моделировании авиационных оптико-электронных систем // Сборник статей II всероссийской научно-технической конференции «Состояние и перспективы развития науки и техники по направлению «Информатика и вычислительная техника»». – 2020. – Ч. 1. – Т. 4. – С. 100-108.

7. Schlyter P. Computing planetary positions - a tutorial with worked examples [Электронный ресурс]. – 2018. URL: http://stjarnhimlen.se/comp/ tutorial.html (дата обращения: 22.09.2020).

8. Taygur M., Eibert T. A Ray-Tracing Algorithm Based on the Computation of (Exact) Ray Paths With Bidirectional Ray-Tracing // IEEE Transactions on Antennas and Propagation. – 2020. – Vol. 69. – P. 1-23.

9. Salvi M., Vidimce K., Lauritzen A., Lefohn A., Pharr M. Adaptive Volumetric Shadow Maps // Computer Graphics Forum (Proceedings of EGSR). – 2018. Vol. 29(4). P. 1289-1296.

10. Jia N., Luo D., Zhang Y. Distorted shadow mapping // Proceedings of the ACM Symposium on Virtual Reality Software and Technology VRST. – 2018. – Vol. 38. – P. 209-214.

11. Kolivand H. Shadow Mapping or Shadow // International Journal of New Computer Architectures and their Applications (IJNCAA). – 2017. – Vol. 2. – P. 275-281.

12. Тарасов В. В., Якушенков Ю. Г. Инфракрасные системы «смотрящего» типа. – М.: Логос, 2004. – 444 с.

13. Апорович В. А, Минов А. И. Методика оценки пропускания инфракрасного излучения атмосферой при наблюдении воздушного объекта из космоса // Доклады БГУИР. – Минск: БГУИР, 2011. – № 2(56). – с. 109-114.

14. Журмилова И. А. Совершенствование систем тепло- и холодоснабжения зданий с применением грунтовых теплообменников. – Владивосток: ФГАОУ ВО «Дальневосточный федеральный университет», 2016. – Автореферат диссертации ... канд. тех. наук. – 176 с.

15. Тонкошкур А. Г., Моделирование процесса кондуктивного теплопереноса в грунтовом воздухоохладителе // Математическое моделирование. – 2018. – Т 30. – № 1. – С 103-112.

16. Солодов А. П. Курс тепломассообмена // Открытое образование. – 2013. – №1(96). – С. 8-16.

УДК 004.052.3

Коэффициент готовности элемента распределённой системы управления и подходы к автоматизированному восстановлению его функции на резервном узле

Бесчастнов А. А.

Санкт-Петербургский государственный электротехнический университет "ЛЭТИ" им. В. И. Ульянова (Ленина), г. Санкт-Петербург, Россия

Аннотация: *рассматриваются подходы к обеспечению коэффициента готовности элемента распределённой системы управления в условиях, когда при отказе его функция восстанавливается на резервном узле. Показано, что время восстановления функции является ключевым фактором, влияющим на коэффициент готовности, а его сокращение упирается в трудоёмкость и слабую воспроизводимость ручного восстановления конфигурации резервного узла. Проанализированы существующие подходы к восстановлению функции на резервном узле и обоснована связь между автоматизированным воспроизводимым восстановлением конфигурации и коэффициентом готовности через декомпозицию времени восстановления. Показано, что вблизи высоких значений коэффициента готовности эффект автоматизированного восстановления функции целесообразно оценивать по относительному сокращению ожидаемого годового простоя, а не по абсолютному приращению коэффициента готовности. Сформулированы задачи дальнейшего исследования.*

Ключевые слова: *распределённая система управления, коэффициент готовности, доступность, время восстановления, резервный узел, автоматизация конфигурации, отказоустойчивость.*

Введение

Современные технологические и информационные комплексы всё чаще строятся как распределённые системы управления, отдельные элементы которых выполняют управляющие функции на территориально или логически разнесённых узлах. Отказ такого элемента приводит к утрате соответствующей функции управления, а в критически важных инфраструктурах к нарушению непрерывности технологического процесса. Требования к устойчивости подобных систем закреплены на нормативном уровне, в том числе для объектов критической информационной инфраструктуры [1]. Одним из базовых способов сохранения работоспособности является резервирование, при котором функция отказавшего элемента восстанавливается на резервном узле.

Ключевым показателем, характеризующим долю времени, в течение которого элемент способен выполнять свою функцию, служит коэффициент готовности. Его значение напрямую зависит от того, насколько быстро функция отказавшего элемента может быть восстановлена на резервном узле. Однако восстановление функции требует не только переключения нагрузки, но и приведения резервного узла в требуемое конфигурационное состояние, обеспечивающее воспроизведение конфигурации отказавшего элемента. При ручном выполнении эта операция трудоёмка, слабо воспроизводима и

зависит от квалификации оператора, что увеличивает и делает нестабильным время восстановления. Таким образом, возникает задача сокращения времени восстановления функции на резервном узле за счёт автоматизации и повышения воспроизводимости восстановления конфигурации. Настоящая работа носит обзорно-аналитический характер. Её цель – проанализировать существующие подходы к автоматизированному восстановлению функции элемента распределённой системы управления на резервном узле, обосновать их связь с коэффициентом готовности через сокращение времени восстановления и сформулировать направления дальнейшего исследования.

Актуальность

Актуальность исследования определяется как ростом требований к доступности систем, так и разрывом между ожидаемыми и фактически достигаемыми показателями восстановления. В контексте обеспечения информационной безопасности сокращение времени восстановления функции связано также с повышением доступности объекта информатизации в составе информационно-телекоммуникационной системы (ИТКС), поскольку уменьшается продолжительность периода недоступности соответствующей функции объекта. Согласно обзору ландшафта киберугроз Агентства Европейского союза по кибербезопасности, значительная часть инцидентов связана именно с нарушением доступности сервисов и данных [2]. При этом отраслевая аналитика фиксирует устойчивый разрыв между планируемым и реальным временем восстановления. По данным отчёта о состоянии резервного копирования и восстановления, более 60 % организаций рассчитывают восстановить работу менее чем за сутки, однако на практике это удаётся лишь примерно трети из них [3]. Одной из причин такого разрыва является высокая трудоёмкость ручного сопровождения и зависимость результата
от человеческого фактора.

Нормативно-методическая база связывает устойчивость организации с достижением целевых показателей восстановления. Стандарты в области менеджмента непрерывности деятельности и готовности информационно-коммуникационных технологий вводят такие показатели, как целевое время восстановления и целевая точка восстановления, задающие допустимые границы простоя и потери данных [4, 5]. Для элемента распределённой системы управления это означает, что время восстановления его функции на резервном узле должно укладываться в заданные пределы, а сам процесс восстановления должен быть предсказуемым и повторяемым.

Особую значимость обеспечение требуемого времени восстановления приобретает в инфраструктурах ограниченного доступа, к которым относятся объекты критической информационной инфраструктуры и изолированные корпоративные сети. В таких условиях внешние облачные механизмы восстановления, как правило, неприменимы, и все процедуры восстановления реализуются внутри доверенного периметра организации. Это повышает

нагрузку на персонал и делает воспроизводимость восстановления конфигурации критическим фактором достижения приемлемого времени восстановления.

Существующие подходы к восстановлению функции на резервном узле

Задача восстановления функции на резервном узле исследуется в нескольких смежных направлениях. В работах по реконфигурируемым системам и восстановлению крупномасштабных систем с резервными компонентами процесс восстановления формализуется как задача выбора конфигурации резервов в зависимости от текущего состояния системы, причём ручной перебор вариантов признаётся непрактичным по мере роста масштаба [6, 7]. Тем самым подчёркивается необходимость автоматизированного, формализованного управления составом и конфигурацией резервов.

Отдельное направление связано с оркестраторными средами. Для кластеров Kubernetes [8] предложены архитектуры автоматизированного аварийного восстановления, включающие обнаружение отказов и автоматическое развёртывание сервисов в целевом окружении, в том числе с переносом приложения на резервный кластер; такие подходы позволяют существенно сократить время восстановления и снизить влияние человеческого фактора [9]. Следует, однако, различать понятия: оркестраторная платформа выступает здесь механизмом, обеспечивающим развёртывание функции на резервном узле, но сама по себе не тождественна распределённой системе управления в прикладном смысле. В контексте настоящей работы оркестратор рассматривается именно как средство воспроизводимого развёртывания состояния элемента.

Третье направление – автоматизированное управление конфигурациями вычислительной среды. Сравнительные обзоры средств управления конфигурациями показывают, что переход от ручной настройки узлов к декларативному, воспроизводимому применению конфигураций повышает управляемость и надёжность настройки и сокращает время конфигурирования, причём эффект усиливается с ростом числа однотипных узлов [10]. Именно воспроизводимость и детерминированность конфигурационного состояния являются условием того, чтобы резервный узел мог быть приведён в состояние, эквивалентное отказавшему элементу, за предсказуемое время.

В русле этого направления автором ранее предложен подход «резервное копирование как код», при котором описание эксплуатационных параметров сервиса размещается рядом с самим сервисом в декларативной форме, а приведение централизованной подсистемы в соответствие с фактическим составом сервисов выполняется автоматически и идемпотентно [11]. При апробации подхода зафиксировано сокращение числа ручных операций инженера и трудозатрат на сопровождении конфигураций, а также устранение характерного для ручного режима класса ошибок. Необходимо подчеркнуть, что эти результаты характеризуют трудозатраты инженера на жизненном цикле сервиса, а не время восстановления функции элемента: это разные показатели, и

прямое отождествление их недопустимо. Вместе с тем полученные результаты служат качественным свидетельством того, что автоматизация и воспроизводимость конфигурации сокращают длительность и разброс операций по приведению узла в требуемое состояние, что создаёт предпосылку для сокращения соответствующей составляющей времени восстановления.

Коэффициент готовности и декомпозиция времени восстановления

Коэффициент готовности элемента как объекта надёжности определяется в соответствии с [12] и в стационарном приближении может быть записан в виде отношения средней наработки на отказ к сумме наработки и среднего времени восстановления:

$$K_{Г} = \frac{T}{\left(T + T_{В}\right)}, \tag{1}$$

где T – средняя наработка на отказ элемента; $T_в$ – среднее время восстановления функции.

Из формулы (1) следует, что при фиксированной наработке T сокращение времени восстановления $T_в$ монотонно увеличивает коэффициент готовности и, соответственно, уменьшает суммарный простой. Это позволяет рассматривать время восстановления функции на резервном узле как основной управляемый фактор повышения готовности.

Время восстановления функции на резервном узле неоднородно и может быть представлено как сумма последовательных составляющих:

$$T_{в} = t_{обн} + t_{перекл} + t_{разв} + t_{пров}, \tag{2}$$

где $t_{обн}$ – время обнаружения отказа; $t_{перекл}$ – время переключения на резервный узел; $t_{разв}$ – время приведения резервного узла в требуемое состояние развёртывания и воспроизведения конфигурации элемента; $t_{пров}$ – время проверки корректности восстановленной функции.

Из декомпозиции времени восстановления, представленной формулой (2), следует, что из перечисленных составляющих именно $t_{разв}$ в наибольшей степени поддаётся автоматизации: воспроизводимое декларативное восстановление конфигурации сокращает как среднее значение, так и разброс этой составляющей, снижая зависимость результата от квалификации оператора. Обнаружение отказа и переключение определяются преимущественно свойствами инфраструктуры мониторинга и резервирования, а проверка может быть частично автоматизирована средствами тестирования восстановления. Чтобы оценить влияние времени восстановления на готовность элемента, следует учитывать, что сокращение времени неработоспособного состояния приводит к уменьшению ожидаемой продолжительности простоя. В практически значимом случае, когда среднее время восстановления существенно меньше средней наработки между отказами, продолжительность простоя в течение периода эксплуатации определяется главным образом временем восстановления функции. Поэтому эффект от автоматизированного восстановления функции корректно оценивать не по абсолютному приращению

коэффициента готовности, а по относительному сокращению ожидаемого простоя, к которому этот эффект наиболее чувствителен.

Направления дальнейшего исследования

Проведённый анализ позволяет сформулировать задачи дальнейшего исследования. Во-первых, необходимо построить модель элемента распределённой системы управления с резервным узлом, отражающую отказ, переключение и восстановление функции, и выбрать адекватную модель коэффициента готовности – от стационарного приближения по формуле (1) до марковской модели состояний. Во-вторых, требуется экспериментально определить параметры надёжности – среднюю наработку на отказ и составляющие времени восстановления, – которые в настоящей работе не измерялись. В-третьих, следует получить количественную оценку составляющей $t_{разв}$ для автоматизированного и ручного восстановления конфигурации на резервном узле и провести анализ чувствительности коэффициента готовности к её изменению. Наконец, полученную модель целесообразно проверить на данных апробации в реальной инфраструктуре ограниченного доступа.

Заключение

В работе проанализированы подходы к автоматизированному восстановлению функции элемента распределённой системы управления на резервном узле с позиции их влияния на коэффициент готовности. Показано, что при фиксированной средней наработке на отказ сокращение времени восстановления функции приводит к повышению коэффициента готовности, а возможность сокращения этой составляющей существенно зависит от трудоёмкости и воспроизводимости восстановления конфигурации резервного узла. На основе анализа смежных направлений – реконфигурации систем с резервными компонентами, автоматизированного восстановления в оркестраторных средах и автоматизированного управления конфигурациями – обоснована связь между автоматизированным воспроизводимым восстановлением конфигурации и коэффициентом готовности, реализуемая через сокращение составляющей времени развёртывания в общем времени восстановления. Полученные результаты определяют направление дальнейшего исследования, в рамках которого предполагается построение модели готовности, экспериментальная оценка её параметров и количественный анализ эффекта автоматизации восстановления функции на резервном узле.

Список литературы

1. О безопасности критической информационной инфраструктуры Российской Федерации. Федеральный закон РФ от 26.07.2017 № 187-ФЗ // Федеральная служба по техническому и экспортному контролю [Электронный ресурс]. – URL: https://fstec.ru/dokumenty/vse-dokumenty/zakony/federalnyj-zakon-ot-26-iyulya-2017-g-n-187-fz (дата обращения: 15.12.2025).

2. ENISA Threat Landscape 2025 // European Union Agency for Cybersecurity [Электронный ресурс]. 2025. – URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025 (дата обращения: 20.10.2025).

3. State of Backup and Recovery Report 2025 // Unitrends [Электронный ресурс]. 2025. – URL: https://www.unitrends.com/media/downloads/resources/The-State-of-Backup-and-Recovery-Report-2025.pdf (дата обращения: 05.12.2025).

4. ГОСТ Р ИСО 22301-2021. Безопасность и устойчивость. Системы менеджмента непрерывности деятельности. Требования. М.: Российский институт стандартизации, 2021.

5. ГОСТ Р ИСО/МЭК 27031-2012. Информационная технология. Методы и средства обеспечения безопасности. Руководство по готовности информационно-коммуникационных технологий к обеспечению непрерывности бизнеса // Электронный фонд правовых и нормативно-технических документов [Электронный ресурс]. – URL: https://docs.cntd.ru/document/1200105651 (дата обращения: 16.11.2025).

6. Trapiello C., Puig V., Cembraño G. Reconfiguration of large-scale systems using back-up components // Computers & Chemical Engineering. 2021. Vol. 149. Art. 107288. DOI: 10.1016/j.compchemeng.2021.107288.

7. Vavrík V., Fusko M., Bučková M., Gašo M., Furmannová B., Štaffenová K. Designing of Machine Backups in Reconfigurable Manufacturing Systems // Applied Sciences. 2022. Vol. 12, № 5. Art. 2338. DOI: 10.3390/app12052338.

8. Kubernetes // The Linux Foundation [Электронный ресурс]. – URL: https://kubernetes.io/ (дата обращения: 14.01.2026).

9. Kim J., Choi J., Jung E. Design and Implementation of an Automated Disaster-Recovery System for a Kubernetes Cluster Using LSTM // Applied Sciences. 2024. Vol. 14, № 9. Art. 3914. DOI: 10.3390/app14093914.

10. Костромин Р. О. Сравнительный обзор средств управления конфигурациями ресурсов вычислительной среды функционирования цифровых двойников // Информационные и математические технологии в науке и управлении. 2021. № 1 (21). С. 131–145. DOI: 10.38028/ESI.2021.21.1.011.

11. Бесчастнов А. А. Подход backup-as-code для автоматизированного управления конфигурациями резервного копирования в изолированных on-premise инфраструктурах // 64-я Международная научная студенческая конференция (МНСК-2026): материалы конференции. Новосибирск: Новосибирский государственный университет, 2026. С. 206.

12. ГОСТ 27.002-2015. Надежность в технике. Термины и определения. М.: Стандартинформ, 2016

УДК 004.052.3

Способ геопривязки инфракрасных изображений, получаемых в ходе плановой аэросъёмки с воздушного носителя

Галайчук К. В., Захарчук А. В., Черевань Д. В.

Военно-космическая академия имени А.Ф.Можайского, г. Санкт-Петербург, Россия

Аннотация: *в работе представлен метод геопривязки аэросъемочных данных инфракрасного диапазона, получаемых в ходе проведения плановой аэросьемки с воздушного носителя. Моделирование и реализация решения представлена в среде Matlab, результатом первичной обработки являются изображения участков местности в формате *.jpg с известными геоданными.*

Ключевые слова: *глобальная навигационная спутниковая система, геоданные, геопривязка, разноспектральная съемка, инфракрасные изображения.*

1. Введение

Разносторонняя и качественная информация о состоянии земной поверхности и расположенных на ней объектах, необходимая для изучения окружающей среды, археологии, видового мониторинга, а также при определении границ территорий, может быть получена по материалам аэрофотосъемок. Аэрофотографирование – фотографирование земной поверхности с использованием фотоаппаратуры, установленной на воздушном судне с целью получения, изучения и представления объективных пространственных данных на участках проведенной съемки.

В ходе проведения плановой аэросьеки регистрируется большой объем разноспектральной аэросъемочной информации. Для получения инфракрасных изображений как правило используется несколько типов аппаратуры для перекрытия всего интересующего диапазона: инфракрасные камеры диапазона 3-5 и 8-14 мкм.

Для повышения качества, оперативности обработки и последующей каталогизации полученных аэросъемочных данных по регионам съемок возникает необходимость разработки метода привязки геопространственной информации к получаемым изображениям.

Возможным вариантом решения данной задачи является создание полигонов по имеющимся изображениям, которые возможно наложить на земную поверхность с использованием геоинформационных систем. Необходимую информацию возможно использовать из файла KML (от англ. Keyhole Markup Language – язык разметки на основе XML для представления трехмерных геопространственных данных).

2. Построение полигонов по имеющимся аэросъемочным данным

Описывая общий подход к определению координат изображений, рассмотрим этапы построения полигонов по имеющимся аэросъёмочным данным.

Этап № 1. Получение координат начала и окончания съемки по известному времени включения и отключения аппаратуры

В качестве источника геопространственной информации, по которой возможно построение полигонов изображений, можно использовать файлы треков полета воздушного носителя (далее – ВН), которые регистрируются в полете отдельным автоматизированным рабочим местом (далее – АРМ) с присоединенной глобальной навигационной спутниковой системой (ГНСС-приемник) (рис. 1).

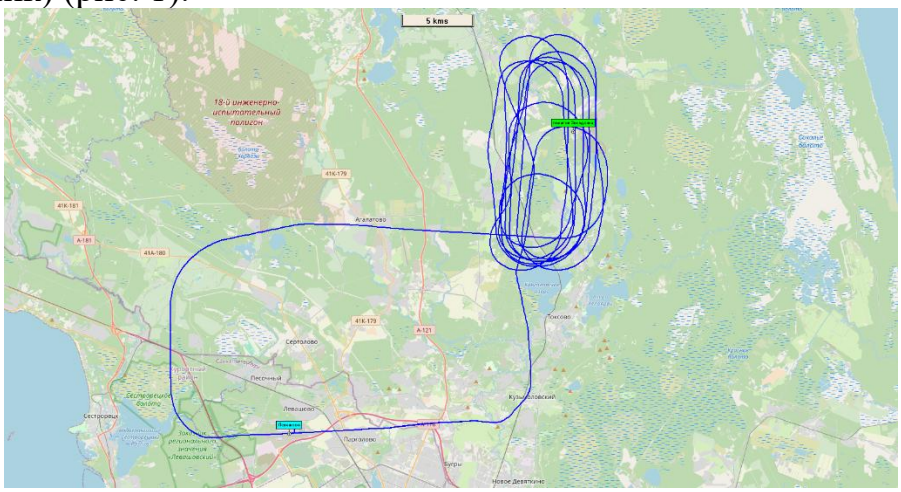


Рис. 1. Пример маршрута полета ВН при проведении аэросъёмочных работ

Необходимо загрузить файл с геоданными, представленными в формате NMEA с расширением *.plt. Данный файл имеет табличную структуру, где каждая ячейка строки соответствует определенному географическому параметру, такому как широта, долгота, высота, дата и время полета. Следует учитывать различие между временем регистрации в часовом поясе района съемки (Московское время или местное время) и временем в треке, который использует координированное всемирное время (UTC) согласно Гринвичу.

Из файла трека полета воздушного судна (рис. 2) можно получить координаты начала и окончания съемки, зная время начала и окончания съемки на маршруте (время включения и отключения аппаратуры регистрации).

```
0,2,16711680,Track Tail Copy 20.08.2024 9:42:00 ,0,0,2,8421376,-1,0
1355
  56.740809,  60.821562,1,  807.0,45524.2096181, 20-ртч-24, 5:01:51
  56.740651,  60.820810,0,  804.0,45524.2097338, 20-ртч-24, 5:02:01
  56.741248,  60.805643,0,  780.0,45524.2103935, 20-ртч-24, 5:02:58
  56.741400,  60.801685,0,  791.0,45524.2104398, 20-ртч-24, 5:03:02
  56.741574,  60.797508,0,  828.0,45524.2104861, 20-ртч-24, 5:03:06
  56.731871,  60.684009,0, 2590.0,45524.2115509, 20-ртч-24, 5:04:38
  56.729103,  60.680121,0, 2668.0,45524.2115972, 20-ртч-24, 5:04:42
  56.727004,  60.677200,0, 2728.0,45524.2116319, 20-ртч-24, 5:04:45
  56.724883,  60.674280,0, 2789.0,45524.2116667, 20-ртч-24, 5:04:48
  56.722748,  60.671373,0, 2861.0,45524.2117014, 20-ртч-24, 5:04:51
  56.720606,  60.668490,0, 2943.0,45524.2117361, 20-ртч-24, 5:04:54
  56.718462,  60.665645,0, 3034.0,45524.2117708, 20-ртч-24, 5:04:57
```

Рис. 2. Пример трека полета воздушного носителя

Для преобразования геодезических систем координат к единому виду, а именно перевод из формата «градусы и десятичные минуты»

(ГГ ММ.ММММ) в формат «десятичные градусы» (ГГ.ГГГГ) необходимо использовать выражение:

ГГ.ГГГГ = «Градусы» + «Десятичные минуты» / 60 (1)

Соответственно, при обратном преобразовании:

ГГ ММ.ММММ = «Градусы» . «Десятичные минуты» * 0.6 (2)

Например, дано 50,23 (ГГ. ГГГГГ), с помощью выражения (1) получаем: ГГ ММММ СС.СССС = 50 + 23/60 = 50.13,8

Этап № 2. Вычисление азимута полета ВС на маршруте съемки (по координатам начала и окончания съемки)

Для корректного построения полигонов на земной поверхности, отражающих реальную площадь съемки на маршруте съемки, расчет координат углов полигона должен учитывать азимут полета ВС при проведении съемки.

Азимут полета на маршруте съемки можно вычислить путем решения тригонометрических задач, для чего необходимо географические координаты перевести в плоскость, в связи с малыми длинами маршрутов съемки, ошибками из-за кривизны Земли можно пренебречь (пример кода MATLAB):

```
latStart = 44.69702;                % координаты начала и конца съемки
lonStart = 33.59392;
latStop = 44.68707;
lonStop = 33.55409;
latStart = deg2rad(latStart);       % перевод в радианы
lonStart = deg2rad(lonStart);
latStop = deg2rad(latStop);
lonStop = deg2rad(lonStop);
deltalon = lonStop - lonStart;      % разница долгот
x = sin(deltalon) *cos(latStop);    % вычисление азимута
y = cos(latStart) * sin(latStop) - sin(latStart) * cos(latStop) * cos(deltalon);
azimuth_rad = atan2(x, y);
azimuth = rad2deg(azimuth_rad);     % перевод в градусы и приведение к диапазону 0-360
azimuth = mod(azimuth +360, 360);
```

Результатом выполнения приведенного кода является азимут в градусах относительно направления на север.

Этап № 3. Получение точного пространственного разрешения изображения по известной высоте воздушного носителя на маршруте съемки и коэффициента пересчета для конкретной аппаратуры регистрации

Получаемые с помощью инфракрасной аппаратуры изображения земной поверхности, помимо динамического диапазона, определяемого возможностью аппаратуры, характеризуются разрешающей способностью на местности, которая, в случае авиационного базирования аппаратуры, определяется разрешением фоточувствительного элемента (фотоматрицы), применяемой

оптической системой (фокусным расстоянием объектива), а также высотой полета носителя на маршруте съемки.

Этап № 4. Поиск координат углов полигона по размеру изображения и координатам начала съемки

Для нахождения координат углов полигона сначала вычисляется размер изображения с весовым коэффициентом каждого пикселя (при этом считаем, что «вес» пикселя по ширине и по длине одинаков), затем вычисляем координаты углов по известным величинам расстояний относительно точки начальных координат:

```
[height, width, ~] = size(img);        % вычисление размера изображения в пикселях
    % вычисление угловых координат
pixel_size = (pixel) / 111320;         % размер пикселя, преобразование метров в градусы
Width_1 = width * pixel_size;
Height_1 = height / 2 * pixel_size; % расстояние от центра начальных координат
latUL = latStart + Height_1;           % ↑ правый угол по широте
latUR = latUL;                         % ↑ левый угол по широте
latLR = latStart - Height_1;           % ↓ правый угол по широте
latLL = latLR;                         % ↓ левый угол широта
lonUR = lonStart;                      % ↑ правый угол по долготе
lonUL = lonStart + Width_1;            % ↑ левый угол по долготе
lonLR = lonStart;                      % ↓ правый угол по долготе
lonLL = lonStart + Width_1;            % ↓  левый угол долгота
    % формируем матрицу координат полигона
coords = [lonUR, latUR; lonUL, latUL; lonLL, latLL; lonLR, latLR;];
```

Этап № 5. Построение матрицы поворота полигона в зависимости от вычисленного азимута полета

По вычисленному азимуту полета ВС на маршруте съемки рассчитаем матрицу поворота:

```
    % Углы в радианах для курса съемки
azimuth_rad = -(deg2rad(azimuth-270));  % необходимо для корректного счета относительно направления на север
    % Формирование матрицы поворота
rotation_matrix = [cos(azimuth_rad), -sin(azimuth_rad); sin(azimuth_rad), cos(azimuth_rad)];
```

Этап № 6. Поворот полигона и сохранение в соответствии с разметкой KML

На основании рассчитанной матрицы поворота пересчитаем новые координаты:

```
% Применение матрицы поворота для разворота полигона
new_coords = zeros(size(coords));
for i = 1:size(coords, 1)
    offset = coords(i, :) - [lonStart, latStart];        % Смещение относительно центра
    rotated_offset = (rotation_matrix * offset')';   % Поворот
    new_coords(i, :) = rotated_offset + [lonStart, latStart];              % Новые координаты
end
```

Код для сохранения геопространственной информации с помощью языка разметки KML:

```
RFN=[path_ch file_ch '.kml'];        % открываем (создаем) файл для записи
    fileID = fopen(RFN, 'w');
    fprintf(fileID, '<?xml version="1.0" encoding="UTF-8"?>\n');          % заголовок KML
    fprintf(fileID, '<kml xmlns="http://www.opengis.net/kml/2.2">\n');
    fprintf(fileID, '<Placemark>\n');
    fprintf(fileID, ' <name>"ИК-изображение"</name>\n');
    fprintf(fileID, ' <Polygon>\n');
    fprintf(fileID, ' <outerBoundaryIs>\n');
    fprintf(fileID, ' <LinearRing>\n');
    fprintf(fileID, ' <coordinates>\n');
    for i = 1:size(new_coords, 1)  % Запись новых координат в KML
        fprintf(fileID, ' %.6f,%.6f,0\n', new_coords(i, 1), new_coords(i, 2));
    end
    fprintf(fileID, ' %.6f,%.6f,0\n', new_coords(1, 1), new_coords(1, 2));% Замыкание полигона
    fprintf(fileID, ' </coordinates>\n');
    fprintf(fileID, ' </LinearRing>\n');
    fprintf(fileID, ' </outerBoundaryIs>\n');
    fprintf(fileID, ' </Polygon>\n');
    fprintf(fileID, '</Placemark>\n');
    fprintf(fileID, '</kml>\n');
   fclose(fileID);
```

где path_ch - путь к создаваемому файлу; file_ch - имя создаваемого файла.

В результате исполнения кода будет создан файл вида «XXX.kml», где «XXX» название файла, в котором будет содержаться геопространственная информация (рис. 3).

```
<?xml version="1.0" encoding="UTF-8"?>
<kml xmlns="http://www.opengis.net/kml/2.2">
<Placemark>
 <name>"ИК-изображение"</name>
 <Polygon>
 <outerBoundaryIs>
 <LinearRing>
 <coordinates>
 30.195783,60.110294,0
 30.188919,60.071369,0
 30.216269,60.066546,0
 30.223133,60.105471,0
 30.195783,60.110294,0
 </coordinates>
 </LinearRing>
 </outerBoundaryIs>
 </Polygon>
</Placemark>
</kml>
```

Рис. 3. Пример *.kml файла с геопространственной информацией

После загрузки *.kml файла в геоинформационную систему (на примере QGIS 3.38.3), получаем по привязанным к земной поверхности изображениям – полигон, отражающий участок земной поверхности, по которому имеются аэросъемочные данные (рис. 4).

Рис. 4. Пример наложения полигона из *.kml файла в геоинформационной системе на географическую карту

3. Заключение

Разработанный метод первичной обработки и геопривязки аэросъемочных данных ИК-диапазона, позволяет строить полигоны по имеющимся аэросъемочным данным, которые возможно «наложить» на земную поверхность с использованием геоинформационных систем. Метод позволяет повысить качество, оперативность обработки и последующей каталогизации полученных аэросъемочных данных.

Список литературы

1. Блиновская Я. Ю. Задорья Д. С. Введение в геоинформационные системы: учеб. пособие. – М.: Форум, 2019. – 112 с.

2. Коберниченко В. Г., Иванов О. Ю., Зраенко С. М., Сосновский А. В., Тренихин В. А. Обработка данных дистанционного зондирования Земли: практические аспекты // Екатеринбург: Издательство Урал. Ун-та, 2013. – 168 с.

3. Ковин Р. В. Н.Г.Марков. Геоинформационные системы и технологии: учеб. пособие. – Томск: ТПУ, 2015. – 267 с.

4. Коковин П. А. Фотограмметрия и дистанционное зондирование Земли – Екатеринбург, 2019. – 53 с.

5. Корниенко В. П. Методы оптимизации. – М.: Высш. Шк., 2007. – 664 с.

6. Сеньченков В. И. Статистические методы обработки экспериментальных данных – СПб.: ГУАП, 2006. – 207 с.

УДК 621.396.96

Реализация цифрового фильтра при обработке широкополосных сигналов

Глубоких В.В., Зыков Д.Д., Сивохина Н.В.

Военно-космическая академия имени А.Ф.Можайского, г. Санкт-Петербург, Россия

Аннотация*: в статье представлена реализация цифрового фильтра в процессе обработки радиолокационных изображений. Рассмотрен способ выделения паразитных сигналов от наземных станций в спектре принятого сигнала и их фильтрация методом коррекции опорной функции. Приводятся результаты моделирования влияния паразитных сигналов на характеристики радиолокационных изображений, а также результаты их фильтрация в среде Matlab.*

Ключевые слова: *радиолокатор с синтезированной апертурой; широкополосный сигнал, радиолокационные изображения.*

1. Введение

Современное направление развития радиолокационных станций (РЛС) радиовидения космического базирования заключается в использовании широкополосных радиолокационных сигналов, применение которых обеспечивает повышение разрешающей способности, высокую электромагнитную совместимость, скрытность работы и помехоустойчивость станции [1]. Одним из ключевых факторов, снижающих качество радиолокационных изображений (РЛИ), являются паразитные сигналы наземных систем, структура которых согласована или частично согласована со структурой зондирующих импульсов. Прохождение таких сигналов через систему обработки приводит к появлению шумовых эффектов на всем РЛИ. Фильтрация таких сигналов в процессе приема затруднительна. При этом возможно применение цифровых фильтров в процессе обработки РЛИ.

2. Принцип реализации цифрового фильтра

Для фильтрации паразитных сигналов в процессе обработки РЛИ на первом этапе проводится их обнаружение и выделение из полезного сигнала. Ввиду того что уровень помехового сигнала, как правило сопоставим с уровнем сигнала отраженного от наблюдаемого участка поверхности Земли, обнаружение необходимо проводить в спектральной области после ее осреднения по каналам дальности.

Излучаемый сигнал представляет собой последовательность ЛЧМ-импульсов, каждый из которых характеризуется выражением [1]:

$$\dot{s}(t) = rect\left[\frac{t_R - \tau_u / 2}{\tau_u}\right]\exp\left[j\frac{\pi\Delta F}{\tau_u}\left(t_R - \frac{\tau_u}{2}\right)^2 + j2\pi f_0 t_R\right]. \qquad (1)$$

где t_R – быстрое время

$\tau_и$ – длительность зондирующего импульса;

ΔF – ширина спектра зондирующего сигнала;

f_0 – несущая частота;

Спектр зондирующего сигнала представлен на рис. 1.

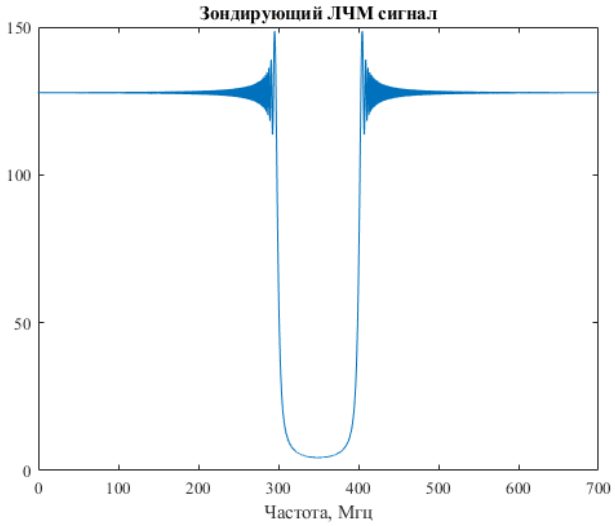


Рис. 1. Аналитический зондирующий сигнал РСА

Сигнал, отраженный от отдельного элемента разрешения (ЭР) описывается в форме [1]:

$$\dot{s}(t_R,t_x)=\dot{A}_\phi rect\left[\frac{t_R-\tau_u/2-\tau_з}{\tau_u}\right]\exp\left[j\frac{\pi\Delta F}{\tau_u}\left(t_R-\frac{\tau_u}{2}-\tau_з\right)^2+j2\pi f_0\left(t_R-\tau_з\right)\right], \quad (2)$$

где $\dot{A}_\phi=A_\phi\exp\left[-j\psi_\phi\right]$ – комплексный коэффициент отражения ЭР.

Спектр принятого сигнала в канале дальности и осредненный спектр по азимутальным каналам представлены на рисунке 2 (а) и (б) соответственно. Моделирование сигнала проводилось в среде Matlab. Был сформирован линейно-частоно модулированный сигнал X – диапазона с шириной спектра 600 МГц и длительностью 20 мкс. Частота дискретизации при оцифровке – 700 МГц.

Рис. 2. Спектр принятого сигнала в 1 канале дальности (а) и спектр принятого сигнала (б) без воздействия помех.

В условиях сложной природной и антропогенной электромагнитной обстановки на вход приемного устройства приходит совокупность полезного s_c и паразитного $s_{\text{п}}$ сигналов.

$$s_{\text{с+п}} = s_{c+}s_{\text{п}}$$

Паразитные сигналы приводят к искажениям РЛИ. На изображениях проявляются шумовые эффекты, снижающие информативные свойства РЛИ, при этом проявляемый эффекты зависят от степени согласованности паразитных сигналов с передаточной функцией цифровой системы обработки РСА по частоте и времени воздействия, а также от длительности и мощности паразитного импульсного сигнала.

Для реализации цифрового фильтра было смоделировано воздействие паразитного сигнала шириной 500 МГц. Спектр принятого сигнала, представляющего аддитивную смесь полезного и паразитного сигналов, представлен на рисунке 4. На интервале от 0 до 400 МГц (выделено контуром), видны характерные биения, что позволяет выделить полосу частот паразитного сигнала.

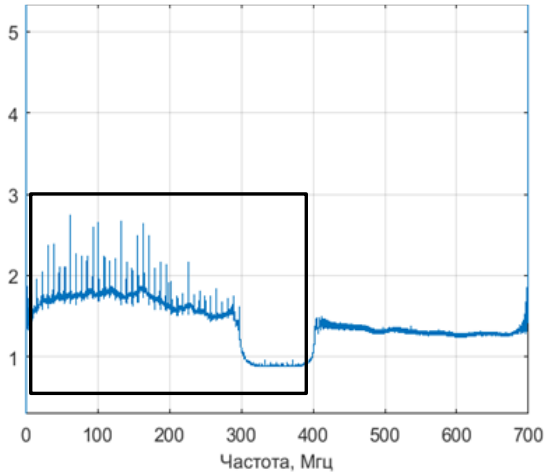


Рис. 4. Осредненный спектр принятого сигнала при наличии паразитных сигналов

Обнаружение в спектре зарегистрированного сигнала составляющих паразитных импульсов позволяет провести их фильтрацию в процессе первичной обработки радиолокационных данных.

Комплексное поле РЛИ $\dot{\text{U}}_{\text{и}}(\text{r},\text{x})$ является результатом двумерной свёртки зарегистрированной РЛГ $\dot{\text{S}}_{\text{г}}(\text{r},\text{x})$ с передаточными функциями процессора РСА по дальности $\dot{\text{h}}_{\text{r}}^{*}$ и азимуту $\dot{\text{h}}_{\text{x}}^{*}$, которые комплексно сопряжены с соответствующими функциями отражённого сигнала [2]:

$$\dot{U}_{\text{и}}(r,x) = \iint_{-\infty}^{\infty} \dot{S_{\text{с+п}}}(r,x) \cdot \dot{h_r}^{*}(r) \cdot \dot{h_x}^{*}(x) dr dx\,. \qquad (3)$$

где r, x – координаты в дальностной и азимутальной плоскостях.

В интересах оценки реализуемости изложенного подхода к цифровой фильтрации широкополосных паразитных сигналов было получено модельное радиолокационное изображение участка фона с линейкой уголковых отражателей (рис. 5).

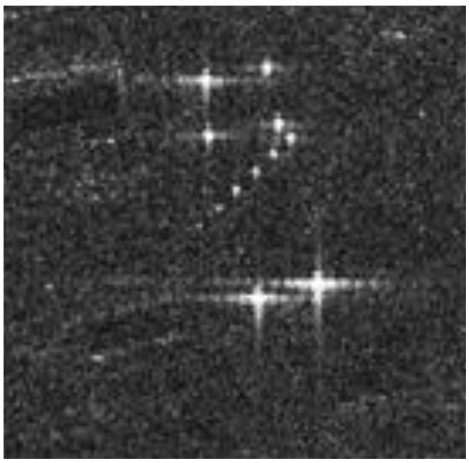


Рис. 5. Модельное РЛИ участка фона с уголковыми отражателями

Далее в модельную радиоголограмму была введена аддитивная добавка паразитного широкополосного сигнала с характеристиками, представленными ранее, что привело к снижению контрастности РЛИ (рис. 6).

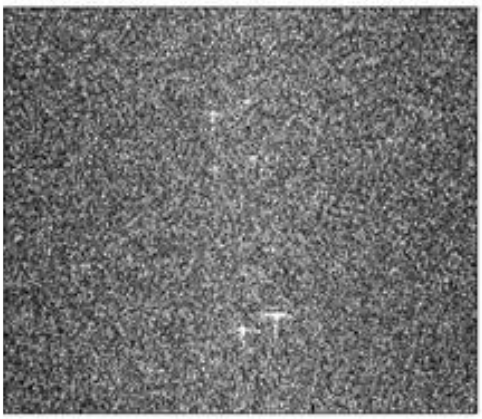


Рис. 6. Модельное РЛИ с аддитивной добавкой широкополосного паразитного сигнала

Одним из самых легко реализуемых и низкоресурсоемких методов является преобразование опорной функии с обнулением диапазона частот. Спектр преобразованной опорной функции по дальности представлен на рисунке 7.

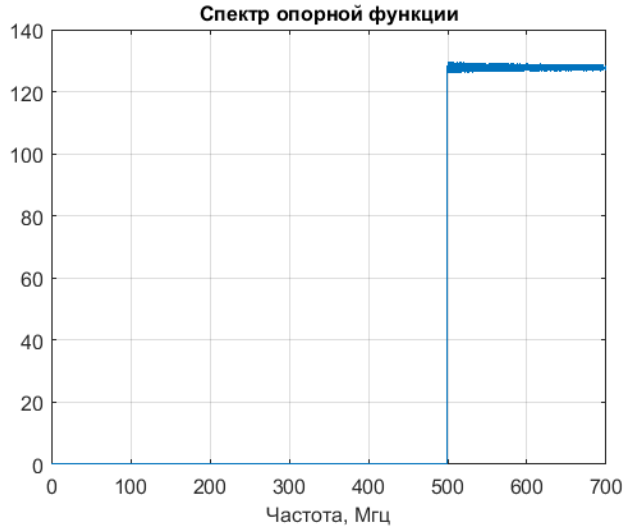


Рис. 7. Спектр преобразованной опорной функции по дальности

Результат свертки, полученной в ходе моделирования радиоголограммы с преобразованной опорной функцией показан на рисунке 8.

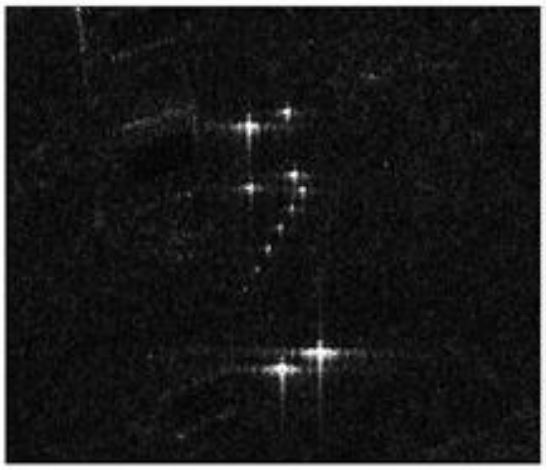


Рис. 8. Модельное РЛИ после фильтрации.

Как видно из рисунка 8 обнуление составляющих спектра с паразитными сигналами (в диапазоне от 0 до 500 МГц) позволило устранить шумовой эффект на РЛИ. Однако обнуление спектра шириной 500 МГц привело к ухудшению потенциального разрешения в 3 раза с 0,25 м до 0,75 м и снижению общей интенсивности РЛИ.

3. Вывод

Таким образом, в работе рассмотрена реализация цифрового фильтра в процессе обработки радиолокационных изображений, методом коррекции опорной функции с удалением полосы частот соответствующей ширине спектра паразитного сигнала. Обнуление диапазона спектра позволяет устранить шумы на РЛИ, однако при этом ухудшается пространственное разрешение. Преимуществом данного способа является простота, быстродействие и низкая ресурсоемкость.

Список литературы

1. Верба В. С. Радиолокационные системы землеобзора космического базирования / Верба В. С., Неронский Л. Б., Осипов И. Г. – М.: Радиотехника, 2010. – 526 с.

2. Купряшкин И. Ф., Лихачев В. П. Космическая радиолокационная съемка земной поверхности в условиях помех: монография. – Воронеж: Научная книга, 2014. – 458 с.

Секция 4 – Безопасность сложных организационно-технических систем

УДК 004.056

MITM-атака привилегированным сетевым узлом посредством перехвата ACME-подтверждения

Смирнов Я. В.

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

Аннотация: *Широкое распространение протоколов автоматизированной выдачи TLS-сертификатов, таких как ACME, создает потребность в анализе устойчивости механизмов подтверждения владения доменом к атакам со стороны привилегированных сетевых узлов. Протокол ACME подразумевает, что узел является легитимным владельцем домена, если он способен ответить на HTTP-01 запрос центра сертификации. Однако транзитный сетевой узел способен пройти проверку и получить доверенный сертификат без участия владельца домена, что создаёт поверхность для скрытой MITM-атаки. В работе описан механизм реализации атаки MITM, основанной на перехвате ACME HTTP-01 подтверждения. Выполнено моделирование с использованием классических инструментов для обработки сетевого трафика, таких как Nginx. Исследованы условия и ограничения, при которых привилегированный сетевой узел может выполнить несанкционированный выпуск TLS-сертификата без участия владельца домена. Подтверждена техническая возможность получения доверенного TLS-сертификата на транзитном узле сети без нарушения доступности сервиса и аномалий для пользователя. Проведённое моделирование рассматривает частный случай атаки на выпуск сертификатов. Данная угроза не закрывается существующими механизмами удостоверяющих центров и требует от владельцев доменов установки дополнительных средств защиты. Анализ ограничений и условий выполнения атаки формирует направление дальнейших исследований, направленных на обнаружение и предотвращение атак подобного типа.*

Ключевые слова: *MITM, Web-PKI, ACME, HTTP-01 подтверждение, Certificate Transparency, TLS-сертификат, сетевая безопасность.*

Введение

В связи с широким распространением защищённых протоколов обмена данными и ростом автоматизации в области управления сертификатами в сетевых сервисах актуализируются вопросы обеспечения безопасности инфраструктуры TLS и устойчивости механизмов подтверждения владения доменными именами к злонамеренным действиям со стороны нарушителя. Большую роль в архитектуре WEB-PKI играет Automatic Certificate Management Environment, предназначенный для автоматизированного выпуска сертификата удостоверяющим центром. Использование ACME позволило упростить эксплуатацию TLS-инфраструктуры, однако привело к расширению поверхности атак, связанной с автоматизацией подтверждения владения доменом. [1] Доля крупнейшего ACME-провайдера – Let’s Encrypt составляет 60.3 % [2].

В настоящее время существует ряд подходов к снижению риска несанкционированного выпуска TLS-сертификатов. К числу таких решений относится механизм Certificate Transparency. В его основе лежит своевременная

публикация сведений о выданных сертификатах в открытых криптографически проверяемых логах. Данный подход предоставляет возможность аудита действий удостоверяющих центров. [3] Однако само по себе наличие CT-логов не устраняет проблему обнаружения подозрительного выпуска сертификатов, поскольку эффективность мониторинга зависит от полноты охвата внешними средствами наблюдения и от задержек обработки соответствующих событий. [4].

В работе H. Birge-Lee и соавторов продемонстрирована возможность несанкционированного получения TLS-сертификатов сетевым злоумышленником посредством реализации атаки на процедуру подтверждения владения доменом с использованием BGP-манипуляций. В работе предложены контрмеры, такие как: подтверждение из нескольких сетевых точек и мониторинг маршрутизации в реальном времени. Действительно, часть атак, основанных на кратковременном BGP-перехвате трафика, становится существенно затруднена. [5] Однако эти контрмеры не устраняют угрозы со стороны привилегированного транзитного узла, способного с использованием существующих программных средств (например, с использованием типового HTTP/TLS-прокси) перехватывать ACME HTTP-01-подтверждение и реализовывать скрытую MITM-атаку без вмешательства в глобальную систему маршрутизации.

Анализ других работ показал, что методы противодействия несанкционированному выпуску сертификатов в основном ориентированы либо на постфактум-выявление события выпуска через CT-логи, либо на усиление процедур проверки со стороны удостоверяющего центра. При этом инфраструктура привилегированного транзитного узла не рассматривается как поверхность атаки. [6,7].

Таким образом, сохраняется угроза безопасности, связанная с несвоевременным обнаружением несанкционированного выпуска и применения TLS-сертификата на контролируемый домен. Для разрешения данного противоречия требуется исследование условий и ограничений атак на перевыпуск сертификата и его практического применения в канале связи. Перспективным направлением дальнейших исследований является разработка методов обнаружения данного класса атак. [8]

Актуальной научно-технической задачей является моделирование MITM-атаки, реализованной посредством перехвата ACME HTTP-01-валидации привилегированным сетевым узлом. Решение данной задачи представляет практический интерес для защиты веб-ресурсов организаций, операторов связи, информационных систем массового обслуживания, а также иных объектов, для которых критичны конфиденциальность и целостность передаваемой информации с помощью протоколов, основанных на TLS.

Модель угроз

Модель нарушителя. Нарушитель занимает позицию привилегированного сетевого узла (EvilProxy на рис. 1), через который транзитом проходит трафик, предназначенный для атакуемого домена. В рамках данной модели нарушитель обладает следующими возможностями:

− перехват и проксирование трафика на портах 80 и 443 для целевого домена без нарушения доступности сервиса для конечных пользователей (Client 1 – Client n на рис. 1);

− селективная обработка HTTP-запросов: перехват запросов центра сертификации (Certificate Authority на рис. 1) к пути /.well-known/acme-challenge/ и подмена ответа собственным токеном при сохранении прозрачного проксирования всего остального трафика;

− инициирование ACME-процедуры: самостоятельный выпуск сертификата на подконтрольном узле с HTTP-01 подтверждением, перехваченным у защищаемого сервера (Origin на рис. 1);

− переключение в режим TLS-терминации: после получения сертификата – выполнение полного TLS-рукопожатия с клиентом от имени легитимного домена, расшифровка трафика и повторное шифрование перед пересылкой на защищаемый сервер;

− скрытность операции: на всём протяжении атаки пользователь наблюдает валидный HTTPS без предупреждений браузера;

Нарушитель не может компрометировать непосредственно защищаемый сервер, не может получить доступ к его приватному ключу и не может нарушить работу прикладного уровня. Он контролирует транзитный сетевой узел и маршрутизацию трафика целевого домена (на рис. 1).

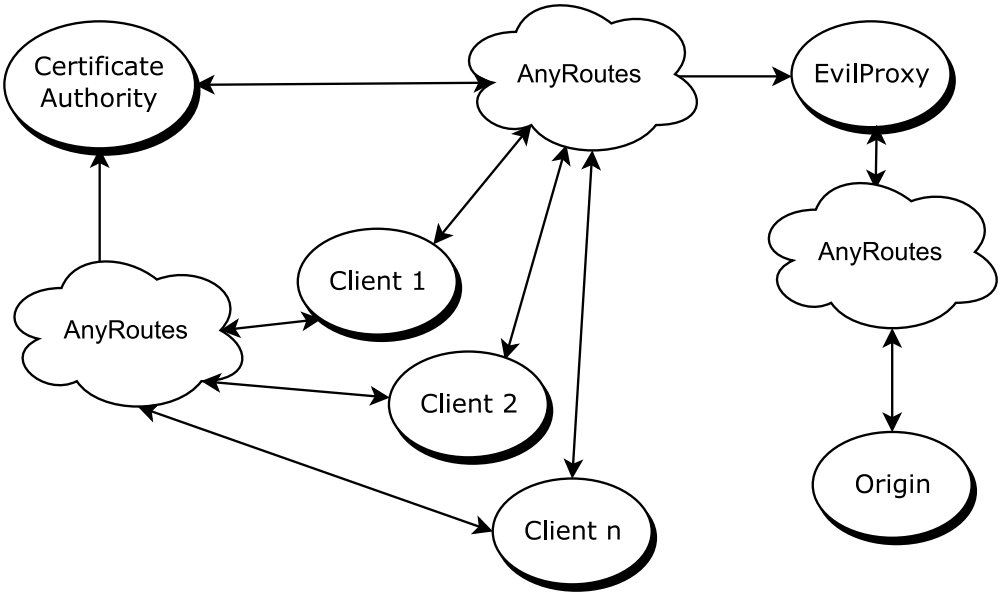


Рис. 1. Сетевая схема модели нарушителя

Для скрытной реализации этих возможностей с целью проведения атаки MITM нарушитель должен учитывать следующие ограничения:

− фильтрация по SNI (Server Name Indication) до TLS-терминации. Поскольку TLS-терминация на стороне нарушителя выполняется только для атакуемого домена, необходимо читать имя сервера из ClientHello без расшифровки. Трафик остальных доменов маршрутизируется на соответствующие им узлы без обработки, не затрагивая их работу.

− предварительная фильтрация трафика на уровне сети. Трафик, не предназначенный для атакуемого IP-адреса, должен идти в обход прокси. Это реализуется посредством перенаправления на уровне маршрутизатора или статической маршрутизации внутри автономной системы. Без этого условия прокси будет получать трафик множества несвязанных узлов, усложнится управление этим узлом и повысится вероятность обнаружения.

− изоляция программного обеспечения для съема дешифрованного трафика. Компонент, слушающий атакуемый домен, должен работать на локальном интерфейсе.

− переадресация на целевой сервер по IP, а не по DNS-имени. Использование IP-адреса исключает зависимость от DNS-разрешения внутри узла нарушителя и устраняет риск рекурсивного перенаправления при изменении DNS-записей.

− корректная обработка порта 80. Перехват HTTP-трафика ограничивается исключительно путём `/.well-known/acme-challenge/`; весь остальной HTTP-трафик проксируется без изменений, что минимизирует видимые аномалии для администратора сервера.

Моделирование атаки ACME HTTP-01 через привилегированный узел

В качестве reverse-proxy для эксперимента выберем наиболее популярный и мощный инструмент – Nginx. [9] В данной статье специально приводится минимальная конфигурация, необходимая для демонстрации возможности атаки, а не подробный алгоритм совершения скрытой атаки, устойчивой к обнаружению.

Подготовка нарушителя к атаке. На подготовительном этапе узел нарушителя функционирует как прозрачный L4-прокси с SNI-фильтрацией уровня L7: в Nginx директива ssl_preread_on позволяет читать поле server_name из ClientHello без TLS-терминации, и только трафик, предназначенный для атакуемого домена, принимается к обработке. Остальные домены при этом не затрагиваются (рис. 2).

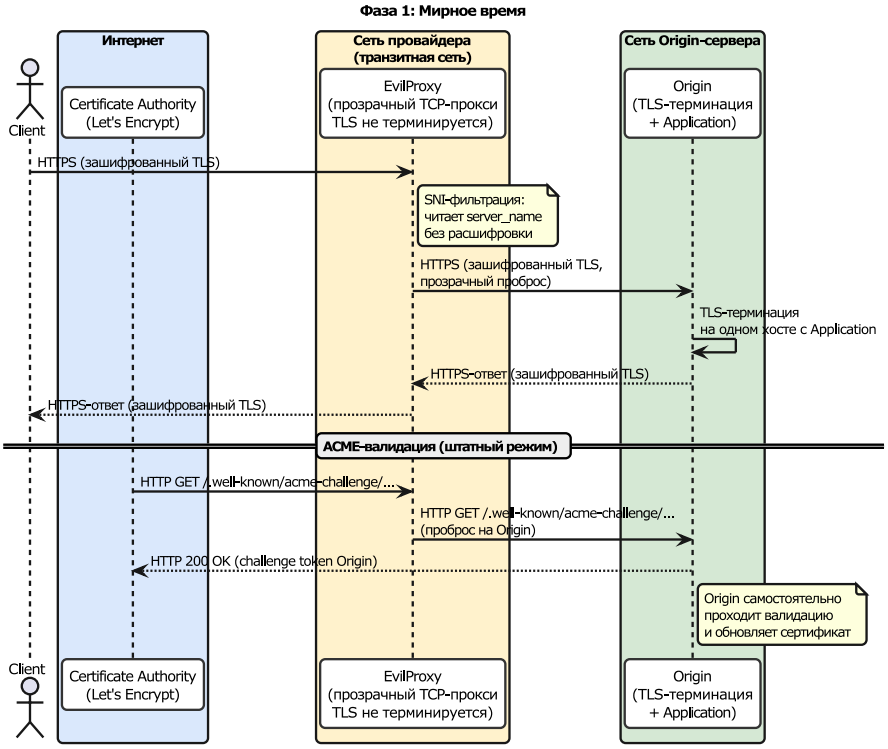


Рис. 2. Диаграмма последовательности на подготовительном этапе

Несанкционированное получение сертификата. На этапе ACME-подтверждения конфигурация stream-блока остаётся неизменной: HTTPS-трафик продолжает прозрачно передаваться на сервер без TLS-терминации. В HTTP-контексте вводится селективная обработка: запросы к /.well-known/acme-challenge/ обслуживаются локально из собственной директории нарушителя, весь остальной HTTP-трафик передается на сервер без изменений. Трафик по порту 80 крайне редко затрагивает сторонние домены, поэтому перехват challenge-запросов не нарушает работу других узлов. Сразу после применения этих настроек, нарушитель запрашивает выпуск нового доверенного сертификата на атакуемый домен, проходит подтверждение и получает корректный сертификат и сохраняет приватный ключ. На это может уйти от нескольких секунд до нескольких минут. Сразу после этого конфигурация возвращается к исходной: трафик на порту 80 прозрачно пропускается на сервер (рис. 3).

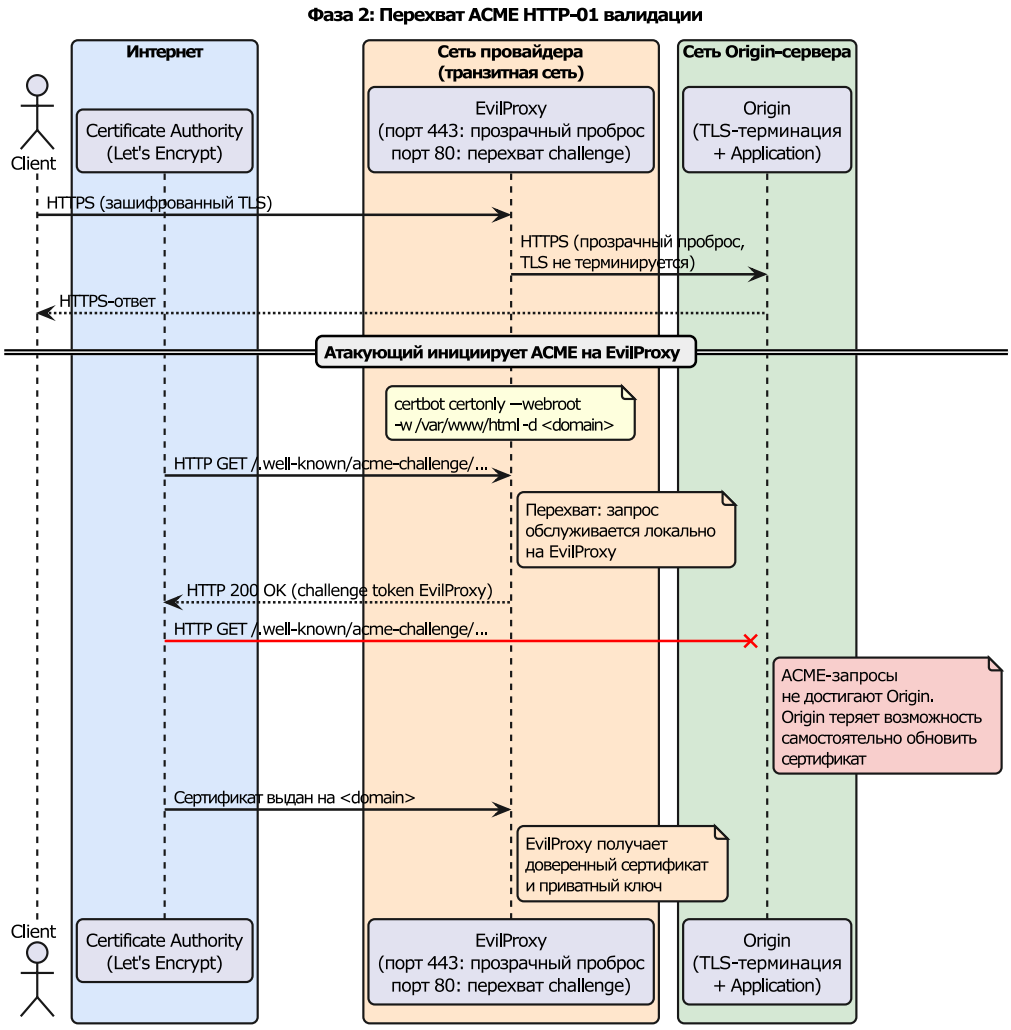


Рис. 3. Диаграмма последовательности на этапе несанкционированного выпуска сертификата

Активная MITM-атака на сервер. После получения сертификата нарушитель начинает выполнять терминацию TLS на своём узле и передавать расшифрованный трафик на локальный анализатор, слушающий на localhost. Трафик остальных доменов продолжает маршрутизироваться на сервер без изменений, что исключает нарушение работы сторонних узлов. Нарушитель выполняет TLS-терминацию только для атакуемого домена, после чего анализатор устанавливает отдельные TLS-соединения с сервером и отправляет запросы как клиент (рис. 4).

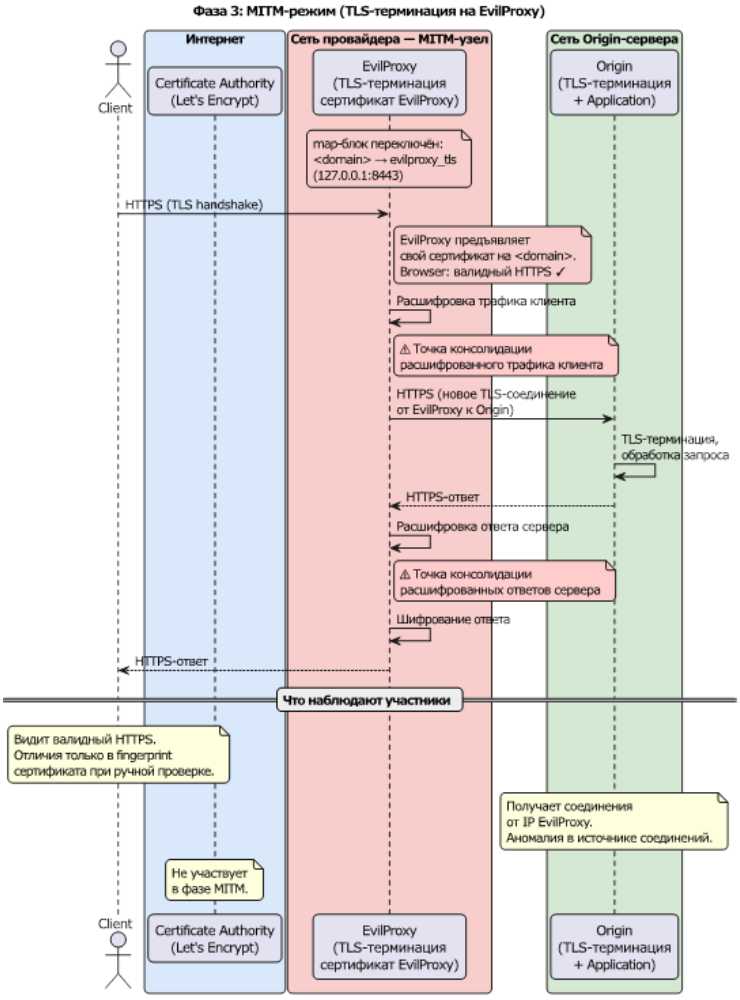


Рис. 4. Диаграмма последовательности на этапе активной MITM-атаки

Нарушитель получил точку консолидации дешифрованного трафика и может читать, анализировать, модифицировать или блокировать его.

Эксперимент по проведению атаки ACME HTTP-01 через привилегированный узел

В состав стенда входят два узла: Origin (легитимный веб-сервер) и EvilProxy (узел, моделирующий привилегированный транзитный элемент сети). Маршрутизация трафика была настроена таким образом, что весь входящий трафик на адрес Origin по портам 80 и 443 проходил через EvilProxy.

Конфигурация Origin. Для эксперимента на Origin установлена операционная система Linux. В качестве полезной нагрузки сервера выступил простой HTML-сайт из одной страницы index.html. Специально для эксперимента был арендован отдельный домен (имя домена обезличено, далее domain.com). В A-записи домена указан внешний IP-адрес Origin. Через ACME у Let's Encrypt получен сертификат на тестовый домен. На Origin запущен Nginx с базовой https конфигурацией с отдачей одного файла из /var/www/domain.com/index.html.

В браузере стал открываться адрес https://domain.com/index.html. Зафиксирована ключевая информация о сертификате домена: fingerprint, JA3/JA3S. [10]

Развертывание EvilProxy. Для эксперимента на EvilProxy установлена операционная система Linux и Nginx.

Подготовительный этап. Настроена первая конфигурация Nginx.

```
stream {
    upstream origin {
        server <IP_Origin>:443;
    }
    map $ssl_preread_server_name $upstream {
        <domain>    origin;
        default      origin;
    }
    server {
        listen 443;
        proxy_pass $upstream;
        ssl_preread on;
    }
}
http {
    server {
        listen 80;

        location / {
            proxy_pass http://<IP_Origin>;
        }
    }
}
```

При корректном обновлении файла конфигурации через nginx -s reload, время недоступности этого Nginx либо отсутствует, либо составляет доли секунды, а активные соединения не разрываются. Поэтому временем подмены файлов конфигурации Nginx при корректном файле конфигурации можно пренебречь.

Первый файл конфигурации настроен на прозрачное проксирование трафика, поэтому для клиента ничего не изменилось. Ключевая информация о сертификате домена осталась неизменной.

Несанкционированное получение сертификата

Подготовлен файл конфигурации 2.

```
stream {
    upstream origin {
        server <IP_Origin>:443;
    }
    map $ssl_preread_server_name $upstream {
        <domain>    origin;
        default      origin;
    }
    server {
        listen 443;
        proxy_pass $upstream;
        ssl_preread on;
    }
}
http {
    server {
        listen 80;
        location /.well-known/acme-challenge/ {
            root /var/www/html;
        }
        location / {
            proxy_pass http://<IP_Origin>;
        }
    }
}
```

Для минимального времени перехвата http-пути `/.well-known/acme-challenge/` на 80 порту и снижения вероятности обнаружения, команды были выполнены подряд через скрипт:

```
cp /opt/configs/config2 /etc/nginx/conf.d/domain.com
start_ts=$(date +%s%N)
nginx -s reload
certbot certonly --noninteractive --agree-tos -m
origin_owner@mail.com --webroot -w /var/www/certbot -d
domain.com
cp /opt/configs/config1 /etc/nginx/conf.d/domain.com
nginx -s reload
end_ts=$(date +%s%N)
echo "Время перехвата http: $(( end_ts - start_ts )) ns"
```

В результате мы осуществили несанкционированный выпуск сертификата, и временное окно перехвата пути http://domain.com/.well-known/acme-challenge/ составило всего $T = 10034073308$ нс $\pm$ 1 нс.

В исследованиях в области мониторинга доступности фигурируют

интервалы опроса от десятков секунд до нескольких минут, что связано с компромиссом между скоростью обнаружения отказов, нагрузкой на инфраструктуру и устойчивостью к ложным срабатываниям. [11-13] Таким образом, обнаружение подмены пути с продолжительностью порядка 10 секунд может быть воспринято как ложное срабатывание, т.к. однократная недоступность встречается достаточно часто. На практике такой подход к обнаружению атаки использовать сложно.

Активный MITM. Для скрытного перехода на MITM, установка файла конфигурации также была сделана через `nginx -s reload`. Файл конфигурации 3.

```
stream {
    upstream evilproxy_tls {
        server 127.0.0.1:8443;
    }
    upstream origin {
        server <IP_Origin>:443;
    }
    map $ssl_preread_server_name $upstream {
        <domain>    evilproxy_tls;
        default      origin;
    }
    server {
        listen 443;
        proxy_pass $upstream;
        ssl_preread on;
    }
}
http {
    server {
        listen 80;
        location / {
            proxy_pass http://<IP_Origin>;
        }
    }
    server {
        listen 8443 ssl http2;
        server_name <domain>;
        ssl_certificate
/etc/letsencrypt/live/<domain>/fullchain.pem;
        ssl_certificate_key
/etc/letsencrypt/live/<domain>/privkey.pem;
        ssl_protocols TLSv1.2 TLSv1.3;
        ssl_ciphers HIGH:!aNULL:!MD5;
        ssl_prefer_server_ciphers on;
```

```
        location / {
            proxy_pass https://<IP_Origin>;
            proxy_ssl_server_name on;
            proxy_ssl_name <domain>;
        }
    }
}
```

Для клиента сервис не теряет доступности, так как действующие сессии не завершаются при такой перезагрузке. После перехода к активному MITM клиент все ещё может получать доступ к ресурсу на Origin, и браузер считает данный сертификат доверенным. Повторно зафиксирована ключевая информация о сертификате домена: fingerprint, JA3/JA3S. Сертификат теперь не соответствует эталонному, полученному при конфигурации Origin. На стороне EvilProxy мы получили точку консолидации дешифрованного трафика. EvilProxy не может скрыть от мониторинга факт выпуска нового сертификата, о котором не знает владелец домена, но на выявление этой атаки через Certificate Transparency требуются автоматизированные средства. Даже при обнаружении несанкционированного выпуска сертификата, требуются механизмы предотвращения активной фазы атаки. Реакционной мерой противодействия может быть смена A-записи домена на другой IP-адрес, но за время обновления DNS-записей нарушитель может выполнить атаки на полезную нагрузку сервиса. А после завершения смены адреса, сервис будет недоступен для клиентов до завершения работы над инцидентом информационной безопасности. [14-15]

Обсуждение

Проведённое моделирование подтвердило актуальность угрозы информационной безопасности со стороны привилегированного транзитного сетевого узла. В проведённом эксперименте в условиях контролируемого тестового окружения успешно выполнена MITM-атака. Существующие средства предотвращения атак со стороны удостоверяющего центра не могут обнаружить атаку подобного класса. Описаны условия, необходимые для успешного перехвата HTTP-01-подтверждения. Экспериментально получено временное окно перехвата трафика на 80 порту в 10 с, необходимое для несанкционированного получения сертификата. Для проведения атаки не требуется разработка специальных программных средств или вмешательство в глобальную маршрутизацию.

Полученные результаты подтверждают необходимость рассмотрения привилегированных транзитных узлов как самостоятельной поверхности атаки.

Заключение

В работе представлена модель реализации атаки на инфраструктуру WEB-PKI, основанная на перехвате ACME HTTP-01-подтверждения привилегированным транзитным сетевым узлом. В контролируемом тестовом

окружении экспериментально проведен полный цикл атаки: встраивание в канал, несанкционированный выпуск сертификата, MITM-атака на TLS-соединения сервиса. Эксперимент подтвердил, что атака может быть выполнена с использованием типовых средств (в эксперименте использовался Nginx). При этом не происходит заметного изменения доступности сервиса для клиентов. Зафиксировано временное окно перехвата HTTP порядка 10 секунд, что затрудняет современное обнаружение атаки штатными средствами мониторинга доступности. Показано, что существующие усиленные процедуры децентрализованной проверки владения доменом со стороны удостоверяющего центра не предотвращают несанкционированный выпуск сертификата транзитным узлом. Полученные результаты формируют дальнейшее направление исследования в части методов обнаружения, предотвращения и ликвидации последствий подобного класса атак.

Список литературы

1. Barnes R., Hoffman-Andrews J., McCarney D., Kasten J. Automatic Certificate Management Environment (ACME) // RFC 8555. IETF, 2019. URL: https://datatracker.ietf.org/doc/html/rfc8555 (дата обращения: 09.03.2026).

2. W3Techs. Usage statistics and market share of Let’s Encrypt as SSL certificate authority on websites. – URL: https://w3techs.com/technologies/details/sc-letsencrypt (дата обращения: 09.03.2026).

3. Laurie B., Langley A., Kasper E. Certificate Transparency // RFC 6962. IETF, 2013. URL: https://www.rfc-editor.org/rfc/rfc6962.html (дата обращения: 09.03.2026).

4. Szalachowski P. Towards More Robust Certificate Transparency // IEEE European Symposium on Security and Privacy (EuroS&P), 2018.

5. Birge-Lee H., Owens G., Rexford J., Mittal P. Bamboozling Certificate Authorities with BGP // Proceedings of the 27th USENIX Security Symposium. 2018. P. 833–849. – URL: https://www.usenix.org/system/files/conference/usenixsecurity18/sec18-birge-lee.pdf (дата обращения: 09.03.2026).

6. Sun A., Lin J., Wang W., Liu Z., Li B., Wen S. Certificate Transparency Revisited: The Public Inspections on Third-Party Monitors // NDSS Symposium 2024. – URL: https://www.ndss-symposium.org/wp-content/uploads/2024-834-paper.pdf (дата обращения: 09.03.2026).

7. Li B., Li F., Ma Z., Wu Q. Exploring the Security of Certificate Transparency in the Wild // ACNS Workshops, 2020. P. 453–470.

8. Birge-Lee H., Owens G., Rexford J., Mittal P. Using BGP to Acquire Bogus TLS Certificates // Proceedings on Privacy Enhancing Technologies Sym-posium, HotPETs. 2017. – URL: https://petsymposium.org/2017/papers/hotpets/bgp-bogus-tls.pdf (дата обращения: 09.03.2026).

9. W3Techs. Usage statistics and market share of Nginx [Электронный ресурс]. URL: https://w3techs.com/technologies/details/ws-nginx (дата обращения: 09.03.2026).

10. Ишкуватов С. М., Бегаев А. Н., Комаров И. И. Метод автоматической классификации цифровых отпечатков TLS-протокола // Вопросы кибербезопасности. 2024. № 1. С. 67–74.

11. Pandya M. Y. Uptime Monitoring and Reporting Strategies: A Case Study // International Journal for Research in Applied Science and Engineering Technology. 2024. Vol. 12, Issue IV. P. 766–771. DOI: 10.22214/ijraset.2024.59855. URL: https://www.ijraset.com/research-paper/uptime-monitoring-and-reporting-strategies-a-case-study (дата обращения: 09.03.2026)

12. Menpara R. Micro-Downtime Indexing: Tracking Sub-Second Failures Before Users Notice // Improwised Blog. 2025. 14 May. URL: https://www.improwised.com/blog/micro-downtime-indexing/ (дата обращения: 09.03.2026).

13. Sebring S. Micro-Outages Uncovered: Exploring the Real Cost of Downtime for Your Business // SolarWinds Orange Matter. 2023. 11 July. URL: https://www.solarwinds.com/blog/true-cost-of-downtime (дата обращения: 09.03.2026).

14. Benton K., Bross T. Timing Analysis of SSL/TLS Man in the Middle Attacks // arXiv preprint arXiv:1308.3559. 2013. 9 p.

15. Effectiveness of Information Security Incident Management Systems: Identifying Practices, Challenges and Development Perspectives // Economic and Social Development. 2025. No. 1. P. 576–592.

УДК 621.39

Способы обеспечения информационной безопасности в каналах управления беспилотными транспортными системами

Будко Д. Д.

Государственный университет морского и речного флота имени адмирала С.О. Макарова, г. Санкт-Петербург, Россия

Аннотация: *В статье затронуты вопросы обеспечения информационной безопасности на каналах и трактах управления беспилотными транспортными системами. При этом такие глобально перемещающиеся автономные объекты рассматриваются Минтрансом России и его федеральными агентствами Росморречфлот, Росавиация, Росжелдор и Росавтодор как объекты критической информационной инфраструктуры, требующие защиты и принятия мер по предотвращению несанкционированного доступа к их управлению, а также к данным, которые они передают и получают. Рассмотрены некоторые известные виды сигнально-кодовых конструкций, которые наряду с применением современных технологий когнитивных радиосистем и программно-конфигурируемого радио позволяют добиться информационной скрытности сигналов управления беспилотными транспортными системами на сети автомобильных и железных дорог, внутренних водных путях России и в морских акваториях.*

Ключевые слова: *амплитудная телеграфия, беспилотная транспортная система, информационная скрытность, когнитивные радиосистемы, однополосная модуляция, программно-конфигурируемое радио, сигнально-кодовая конструкция, частотная телеграфия.*

Введение

В последние годы в России, как и в мировом сообществе, наблюдается всплеск научных разработок и практических реализаций по внедрению робототехнических систем (РТС) широкого применения во все сферы деятельность: от медицины до грузоперевозок, от охраны границ до подводных исследований. Сложности по внедрению робототехнических РТС сопряжены, прежде всего, с тем, что они являются открытыми, распределенными, динамическими, вероятностными и сложными эргатическими системами. При этом:

– *сложность* системы обусловлена наличием большого числа взаимодействующих элементов – технических устройств и ситуационных центров управления (СЦУ), т. е. обслуживающего и управляющего персонала, составляющих единое целое и обладающих существенными свойствами, отсутствующими у отдельных элементов. Только полностью развернутая и обслуживаемая РТС позволяет эффективно функционировать в то время, как ни один из элементов этой системы сам по себе такой возможности не обеспечивает;

– *распределенность* системы связана с тем, что ее элементы не локализованы, а рассредоточены на большой площади (территории страны);

– *открытой* система является по причине, что она постоянно взаимодействует с окружающей средой, являющейся агрессивной в части влияния шумов и помех различной физической природы, а также иных дестабилизирующих факторов (ДФ) случайного и преднамеренного характера;

– *динамической* система считается в связи непрерывным изменением ее состояния под воздействием факторов внешней среды и различных внутренних отказов ее элементов;

– все перечисленные события по отношению к РТС носят случайный характер, следовательно, такую систему следует считать *вероятностной*.

Исходя из указанных выше особенностей современных РТС, в работе рассмотрены вопросы безопасного внедрения такой их разновидности как беспилотные транспортные системы (БТС). В целом беспилотные технологии наряду с искусственным интеллектом и цифровыми платформами на современном этапе развития определяют будущее человечества. Широкое внедрение их в наш обход – это не дань моде, а непреложный факт времени, открывающий путь к обеспечению конкурентоспособности в мире, решению проблем социально-экономического развития на фоне демографический провалов и дефицита на рынке труда, укреплению безопасности и суверенитета России.

С активным внедрением в транспортную отрасль и повседневную жизнь человечества БТС различного назначения одним из актуальных направлений научных исследований являются вопросы обеспечения информационной безопасности их каналов управления [1]. Это связано с тем, что такие глобально перемещающиеся автономные объекты, как уже отмечалось выше, считаются открытыми эргатическими системами критический инфраструктуры с точки зрения обеспечения безопасности и предотвращения несанкционированного доступа к управлению ими и к данным, которые они передают или получают.

Цель статьи: рассмотреть различные виды сигнально-кодовых конструкций в диапазоне декаметровых волн (ДКМВ), позволяющие добиться информационной безопасности сигналов управления глобально перемещающихся БТС.

Существующий научно-методический аппарат синтеза сигнально-кодовых конструкций команд управления в интересах БТС

Существенный прирост эффективности и безопасности применения каналов управления как между СЦУ и БТС, так и в группе БТС возможно получить посредством применения в них формализованных сообщений (ФС). В данном случае в работе под каналами управления будем понимать как каналы информационного взаимодействия, включающие фиксированные поля набора данных: адресная часть, информационное поле (содержащее корректирующие команды или командную информацию), так и каналы траекторного наведения:

– *по направлению и скорости движения*: «вперед» – «назад», «ускорение» – «торможение», «пуск» – «стоп»;

– *по азимуту*: «вправо» – «влево»;

– *по углу места* (или тангажу): «погружение» – «всплытие», «вверх» – «вниз», «взлет» – «посадка», «спуск» – «подъем».

К этому также можно отнести и часть ФС, формируемой системой кодирования (защиты информации) для обеспечения на составных трактах передачи (в гетерогенных средах и на разных диапазонах частот, например от радио- до гидроакустических), заданных показателей помехоустойчивости.

В данном случае ФС используются, прежде всего, для уменьшения периода энергетического контакта, а также повышения оперативности обмена данными в направлениях СЦУ – БТС, или БТС – БТС, обеспечивая их информационное взаимодействие. Уменьшение энергетического контакта можно добиваться не только путем снижения мощности излучения сигнала, но и за счет варьирования его полосой или радиочастотным спектром (РЧС), обеспечивая устойчивую работу «под шумами», либо имитацию звуковых сигналов крупных морских животных в звукоподводной связи для морских БТС, например, [2].

Осуществленные исследования [3-6] научно-методического аппарата (НМА), используемого при формировании радио- и гидроакустических трактов и каналов связи показал, что значительный прогресс в синтезе алгоритмов дистанционного управления автономными системами, РТС и БТС в автоматическом и автоматизированном режимах был достигнут с развитием дистанционных систем автоматического регулирования.

В данной же работе больше внимания уделяется построению сигнально-кодовых конструкций (СКК) для каналов доведения команд управления (КУ) до БТС с применением бинарных посылок «1» и «0». Так исторически сложилось, что базовым аналогом, представляемым в работе алгоритмов построения СКК в интересах каналов управления БТС, является известный более века способ ведения радиообмена с использованием азбуки Морзе [6], запатентованный в 1849 году Сэмюэлем Морзе и широко внедряемый еще со времен первой мировой войны. Способ предусматривает формирование так называемых «точек» и «тире» в виде бинарных посылок с использованием длинных и коротких сигналов. Причем основой единицы времени в данной СКК при формировании букв, цифр, и знаков принимается длина одной «точки». Длина «тире» равняется трём «точкам». Пауза между знаками в буквах (цифрах) соответствует одной «точке», пауза между буквами внутри одного слова – трем «точкам», пауза между словами в предложении – семь «точек». Режимом трансляции сигналов азбуки Морзе является режим амплитудной телеграфии (АТ) на фиксированных частотах. А принимают сигналы на слух с применением головных телефонов.

Несмотря на простоту данного метода формирования каналов управления, к основным его недостаткам относят критически низкую скорость передачи, ориентированную на слуховой прием, что делает неприемлемым такой «ручной режим» в автоматических системах и для высокоскоростных БТС, управляемых в режиме реального времени. К этому добавляется низкая помехоустойчивость

метода в связи с большой загрузкой диапазона ДКМВ помехами и замираниями в ионосфере, как в среде распространения радиоволн (РРВ).

В последние годы активно внедряются способы автоматического приема азбуки Морзе различными трансиверами. На рис. 1 приведены варианты спектрограмм приема сигналов АТ в условиях сосредоточенных и шумовых помех: *а*) спектрограмма сигнала АТ и его амплитудно-частотная характеристика (АЧХ); *б*) сигнал АТ под сосредоточенной помехой; *в*) сигнал АТ под мощными сосредоточенной и шумовой помехами; *г*) сигнал АТ под шумовой помехой.

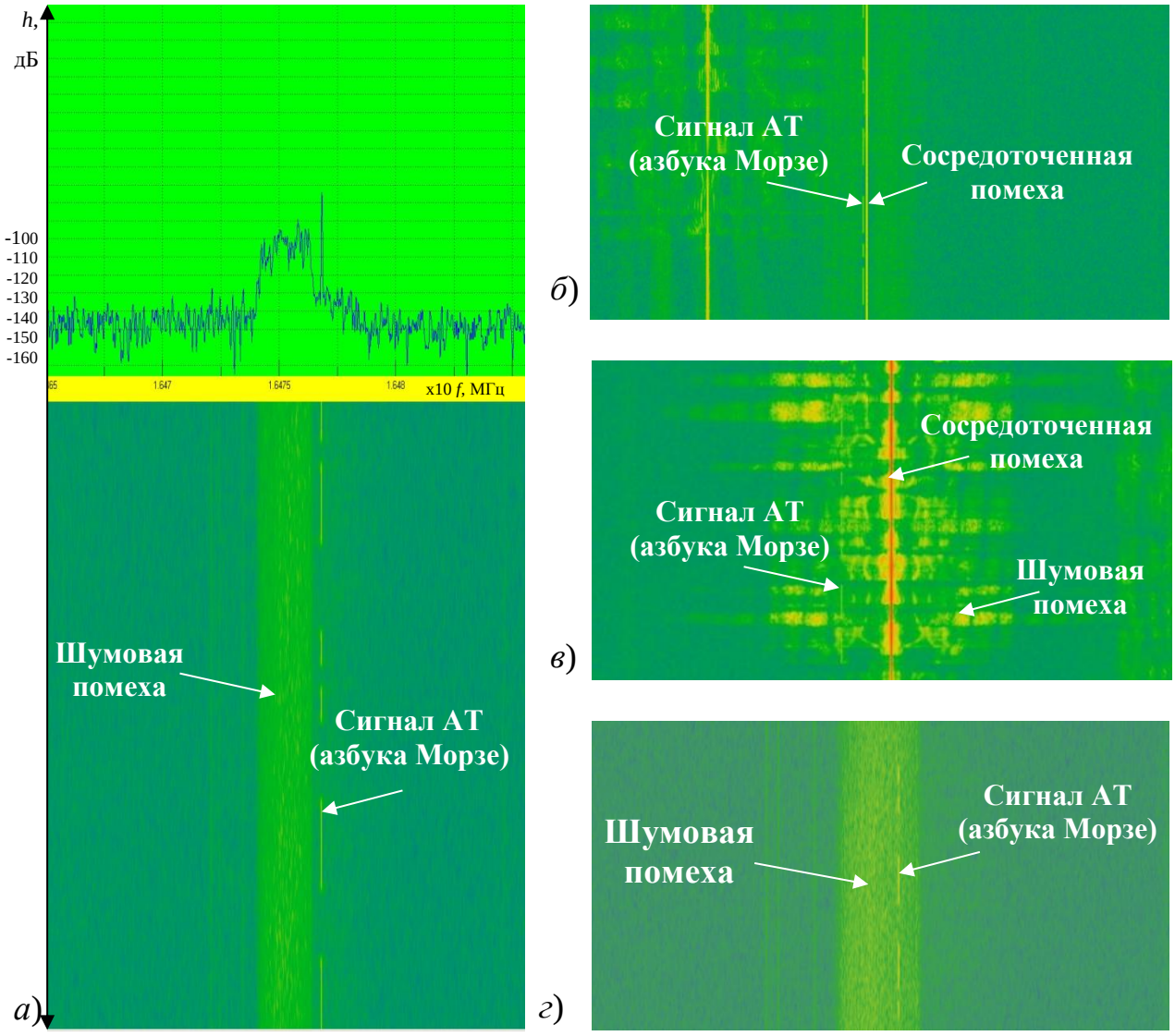


Рис. 1. Фрагменты спектрограмм сигналов АТ (азбуки Морзе) при воздействии шумовых и сосредоточенных по спектру помех

Как видно из рис. 1, сигналы АТ (азбуки Морзе) не обладают какой-либо информационной скрытностью и обычный энергетический обнаружитель [7] легко справляется с автоматическим перехватом команд управления БТС.

Поэтому при широком внедрении БТС необходим поиск новых подходов к построению СКК их КУ, обладающих экономической целесообразностью и технической реализуемостью как при передаче от СЦУ и пунктов дистанционного пилотирования (ПДП) [8], так и при приеме бортовым комплексом связи.

Другим общеизвестным, но более безопасным в части скрытности, способом передачи КУ по беспроводным каналам связи можно отметить сигналы частотной телеграфии (ЧТ), когда информационные биты «1» и «0» передаются на разных частотах $f^{«1»}$ и $f^{«0»}$, и на приемной стороне командной радиолинии должны быть известны с их закреплением за единичными и нулевыми битами.

Также передача КУ возможна путем использования режима однополосной модуляции (ОМ), в радиолюбительской среде называемой SSB (single-sideband modulation), или однополосной модуляцией с подавленной несущей (SSB-SC) рис. 2. В данном случае, например, за битами в виде информационной единицы «1» или информационного нуля «0» (или наоборот) закрепляется верхняя боковая (ВБП) либо нижняя боковая полоса (НБП), относительно несущей частоты. На рис. 2 *а*) и б) приведен процесс формирования сигналов с двухполосной амплитудной модуляцией (DSB), соответственно, с несущей частотой f_0 и с подавленной несущей. На рис. 2 *в*) и *г*) показаны, соответственно, режимы SSB – ОМ по НБП и ОМ по ВБП. Однако, даже в случае работы на передачу с подавленной несущей частотой, а также отсутствия сведений у противоборствующей стороны о частотном разносе НБП и ВБП ($F_н$, $F_в$), данный алгоритм доведения КУ также не будет обладать информационной скрытностью.

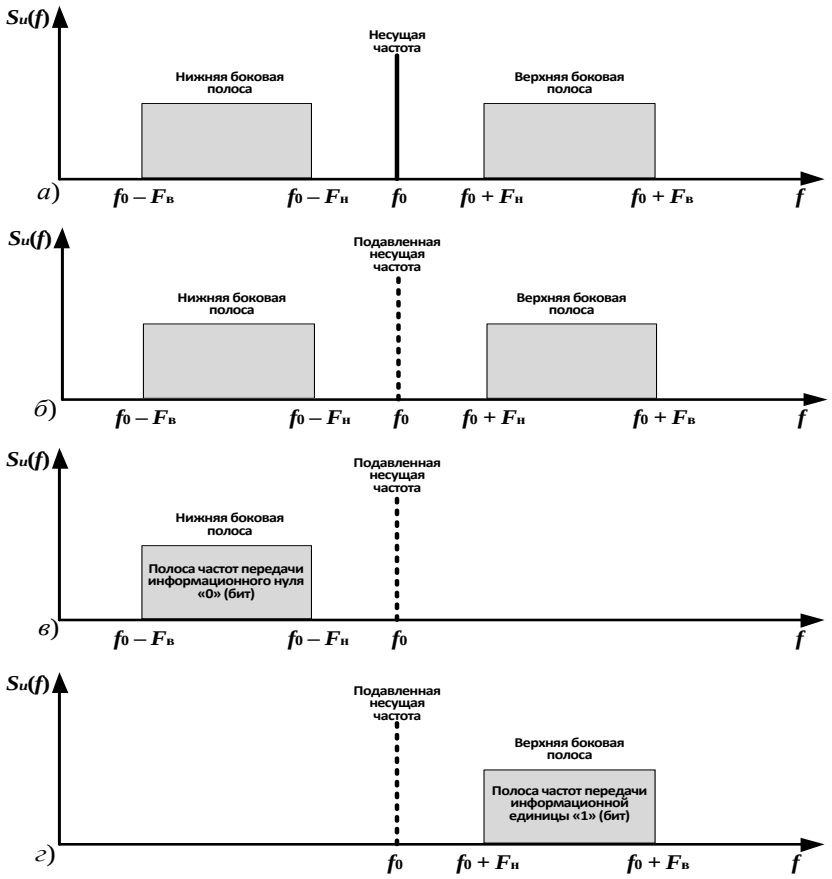


Рис. 2. Процесс формирования сигнала однополосной модуляции

Предложения по формированию сигнально-кодовых конструкций команд управления, обладающих информационной скрытностью

В работе предложен алгоритм формирования СКК, с использованием многочастотного сигнала, передаваемого по параллельным каналам в режимах ЧТ и АТ, рис. 3. Процесс синтеза кода многочастотного сигнала с представлением схемной реализации сумматора кода частот [9] и устройства формирования многочастотных сигналов команд управления БТС в условиях помех подробно представлен в [8], где описаны два основных этапа алгоритма:

– этап формирования Комплекта совместимых рабочих частот (КСРЧ), осуществляемый заблаговременно в результате интеллектуального мониторинга состояния среды РРВ и выбора свободных частотных полос РЧС с помощью технологий когнитивных радиосистем;

– этап формирования многочастотного сигнала на основе КСРЧ, транслируемого в параллельном режиме, таким образом, что за время передачи одного бита до БТС осуществляется доведение всей команды управления в режиме реального времени.

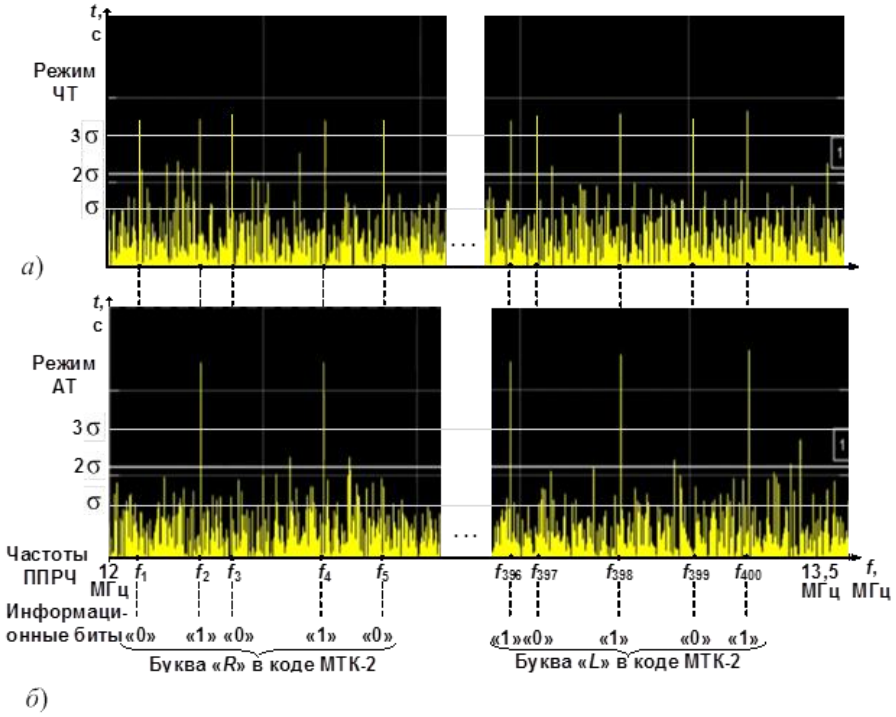


Рис. 3. Вариант формирования сигналов команды управления в режимах: *а*) ЧТ; *б*) АТ

На рис 3 *а*) представлены фрагменты спектрограммы формирования многочастотного сигнала команды управления длиной в 400 бит в режиме ЧТ, когда информационная единица «1» передается по ВБП, а информационный нуль «0» – по НБП. В данном случае постороннему наблюдателю (злоумышленнику) без истинного знания значения несущей частоты каждой из 400 частотных позиций невозможно определить информационный смысл переданной КУ. На спектрограмме все переданные информационные биты рассматриваются как активные частоты (как ложные «информационные единицы»). Несмотря на то, что на частоте f_1, f_3, f_5, …, f_{397} и f_{399} передаются информационные нули «0». Т. е., факт передачи команды управления может быть зафиксирован, однако семантика сообщения (01010….10101) не будет расшифрована.

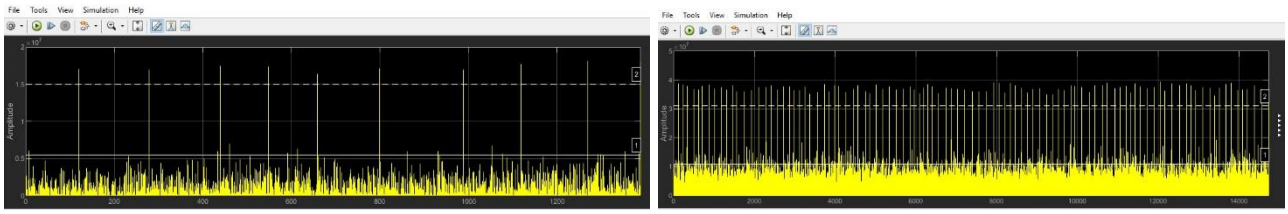
На рис 3 *б*) показаны фрагменты спектрограммы формирования многочастотного сигнала команды управления длиной в 400 бит в режиме АТ, когда информационная единица «1» передается на активной частоте, а информационный нуль «0» – на пассивной (частота не активируется), как показано на рисунке при передаче информационной последовательности 01010….10101 КУ в виде букв «*R*» … «*L*» в коде МТК-2. В данном случае также факт передачи команды управления злоумышленником фиксируется, а смысл сообщения нет, поскольку в радиоэфире регистрируются только активные частоты (информационные единицы). Без знания актуальной для радиолинии псевдослучайной последовательности (ПСП) задействованных в сообщении рабочих частот определить на каких частотах передаются

информационные нули не представляется возможности. Следовательно команда управления не будет распознана.

Таким образом, может быть обеспечена полная информационная скрытность доведения КУ до БТС в условиях попыток несанкционированного доступа к ней на маршруте движения, или в ходе выполнения миссии.

Заключение

Пример работы предложенной модели формирования многочастотных сигналов команд управления БТС представлен на рис. 4, где приведена имитационная модель (в пакете прикладных программ MATLAB) спектрограммы варианта реализации режима передачи команды управления на 10 и на 100 рабочих частотах, выбранных по псевдослучайному закону (ППРЧ).



а) *б*)

Рис. 4. Вариант формирования многочастотного сигнала команды управления БТС при параллельной трансляции информационных бит в режиме ППРЧ:

а) на 10 рабочих частотах; *б*) на 100 рабочих частотах

Режим ППРЧ относят к технологиям расширения спектра (FHSS) и традиционно осуществляется путем периодической смены рабочей частоты в соответствие с некоторой ПСП, известной только для передающей и приемной сторон. Однако, в предложенном алгоритме смена рабочих частот не осуществляется последовательно. Изначально происходит подбор Комплекта совместимых рабочих частот на доступных от сосредоточенных помех участках РЧС и далее вся команда управления транслируется в параллельном формате одномоментно. Такой режим ППРЧ с параллельной трансляцией элементов (информационных бит) сигнала, как показано на рис. 4, существенно повышает оперативность доведения команд управления до глобально перемещающегося БТС, доводя этот процесс до условий реального времени, что важно в аварийной ситуации.

Данный подход стал возможным благодаря современным достижениям в развитии когнитивных радиосистем (CRS) и технологий перепрограммируемых передающих и приемных SDR-радиоустройств. При этом выделение информационных бит команд управления и их динамическое распределение в свободных от первичных пользователей участках радиочастотного спектра позволяет интегрировать каналы управления БТС в уже распределенный диапазон частот без создания взаимных помех.

Список литературы

1. Материалы совместного совещания В. В. Путина и Правительства РФ по вопросам развития автономных систем (Москва. Электродепо «Аминьевское», Московский метрополитен, 16.01.2026) [Электронный ресурс]. 2026. – URL: http://www.ktemlin.ru/events/president/transcripts/79016 (дата обращения 01.02.2026).

2. Будко Н. П., Будко П. А., Клюшин М. А., Шаталов А. Е. Способ доведения управляющей и телеметрической информации в интересах робототехнических платформ различных типов базирования // Системы управления, связи и безопасности. 2025. № 3. С. 294-322. DOI: 10.24412/2410-9916-2025-3-294-322.

3. Будко Д. Д., Будко П. А., Зацепин Т. А., Клименко А. Д. Метод управления беспилотными транспортными системами на основе помехоустойчивых сигнально-кодовых конструкций в условиях сосредоточенных и шумовых помех // Системы управления, связи и безопасности. 2025. № 4. С. 134-178. DOI: 10.24412/2410-9916-2025-4-134-178.

4. Будко Д. Д., Будко П. А., Клименко А. Д., Рыжкова Д. Н. Модель выбора полосы частот в интересах формирования декаметровых радиолиний управления беспилотными транспортными системами // Техника средств связи. 2025. № 4 (172). С. 74-83. DOI: 10.24412/2782-2141-2025-4-74-83.

5. Тузов Г. И., Сивов В. А., Прытков В. И. и др. Помехозащищенность радиосистем со сложными сигналами. Под ред. Г.И. Тузова. – М.: Радио и связь, 1985. – 264 с.

6. История отечественных средств связи / Под ред. А. С. Якунина. – М.: ЗАО «Издательский дом «Столичная энциклопедия», 2013. – 576 с.

7. Куприянов А. И. Радиоэлектронная борьба. М.: Вузовская книга, 2013. 360 с.

8. Будко Д. Д., Каретников В. В. Модель формирования многочастотных сигналов команд управления беспилотных транспортных систем в условиях помех // Системы управления, связи и безопасности. 2026. № 1. С. 182-218. DOI: 10.24412/2410-9916-2026-1-182-218.

УДК 621.39

Архитектура потоковой передачи телеметрических данных для систем интеллектуального мониторинга объектов водного транспорта

Груздев А. А.

Государственный университет морского и речного флота имени адмирала С.О. Макарова, г. Санкт-Петербург, Россия

Аннотация: *В статье рассматривается задача построения отказоустойчивой архитектуры сбора и передачи телеметрической информации от объектов водного транспорта в режиме, приближенном к реальному времени. Предложено решение на основе распределённой платформы обмена сообщениями Apache Kafka, обеспечивающей гарантированную доставку данных, горизонтальное масштабирование и низкую задержку при высокой интенсивности потоков информации. Показана интеграция предложенной архитектуры с инструментами экосистемы Big Data (HDFS, Apache Pig) для последующего применения методов предиктивной аналитики и машинного обучения при оценке технического состояния судов и портовой инфраструктуры. Отдельное внимание уделено сравнению пассивного и активного режимов мониторинга применительно к задачам контроля судоходства.*

Ключевые слова: *телеметрия, водный транспорт, Apache Kafka, брокер сообщений, потоковая обработка данных, Big Data, предиктивная аналитика, интеллектуальный мониторинг, мониторинг инфраструктуры, режим реального времени.*

Введение

Цифровая трансформация транспортной отрасли затрагивает практически все виды перевозок, и водный транспорт не является исключением. Развитие автоматизированных систем управления судоходством, рост числа судов, оснащённых бортовыми датчиками, а также расширение сети автоматических идентификационных систем (АИС) и гидрологических постов приводят к экспоненциальному увеличению объёма данных, которые необходимо собирать, передавать и анализировать практически непрерывно. При этом задача структуризации, обработки, выделения закономерностей и внедрения в производственные процессы *Big Data* становится наиболее актуальной [1].

Традиционные подходы к организации мониторинга, основанные на периодическом опросе объектов и централизованной пакетной обработке данных, всё чаще оказываются неспособны обеспечить требуемую оперативность реагирования на нештатные ситуации — будь то отказ судового оборудования, отклонение от маршрута, изменение гидрометеорологической обстановки или инцидент в порту. В условиях, когда счёт при принятии решений может идти на секунды, критически важной становится возможность передачи и обработки телеметрической информации в режиме реального времени, а также применения методов интеллектуального анализа данных для прогнозирования и предупреждения аварийных ситуаций.

Одновременно с этим возрастает и объём генерируемых данных — сегодня речь идёт уже не о десятках, а о тысячах и десятках тысяч параметров, снимаемых одновременно с судовых механизмов, навигационного оборудования и элементов береговой инфраструктуры. Это ставит перед разработчиками систем мониторинга задачу выбора такой архитектуры передачи данных, которая способна одновременно обеспечивать:

− высокую пропускную способность при значительном числе источников телеметрии;

− надёжность доставки сообщений даже при временной недоступности отдельных компонентов системы;

− возможность горизонтального масштабирования по мере роста флота и расширения зоны мониторинга;

− гибкую интеграцию с аналитическими платформами для последующей обработки накопленных данных методами Big Data и машинного обучения.

Цель статьи — рассмотреть архитектурное решение для построения системы передачи телеметрической информации объектов водного транспорта на основе распределённой платформы обмена сообщениями Apache Kafka, а также описать принципы её интеграции с инструментами хранения и анализа больших данных для решения задач предиктивного мониторинга.

Принципы построения архитектуры передачи телеметрических данных

Задача организации потокового обмена данными между разнородными источниками телеметрии и системами хранения/анализа традиционно решается двумя основными способами: посредством прямого взаимодействия «точка-точка» между источником и получателем данных либо через промежуточный слой — брокер сообщений, обеспечивающий буферизацию, маршрутизацию и гарантированную доставку сообщений.

Для условий мониторинга водного транспорта, характеризующихся большим числом рассредоточенных и мобильных источников данных (суда, портовые сооружения, гидрологические посты), прямое взаимодействие оказывается малопригодным: оно плохо масштабируется, чувствительно к временной недоступности отдельных узлов сети и не позволяет эффективно балансировать нагрузку между несколькими потребителями данных.

В связи с этим в качестве базового архитектурного решения выбрана централизованная модель обмена сообщениями, ядром которой выступает распределённая платформа Apache Kafka. Она изначально проектировалась для обработки потоков событий с высокой частотой поступления и способна обеспечивать пропускную способность, достаточную для одновременного обслуживания тысяч источников телеметрии без деградации производительности при пиковых нагрузках.

Общая структура системы представлена на рис. 1, где показаны основные элементы: producers, передающие метрики в кластер брокеров Kafka; consumers и stream processors, обрабатывающие данные в режиме реального времени;

а также connectors, обеспечивающие интеграцию с внешними хранилищами и базами данных.

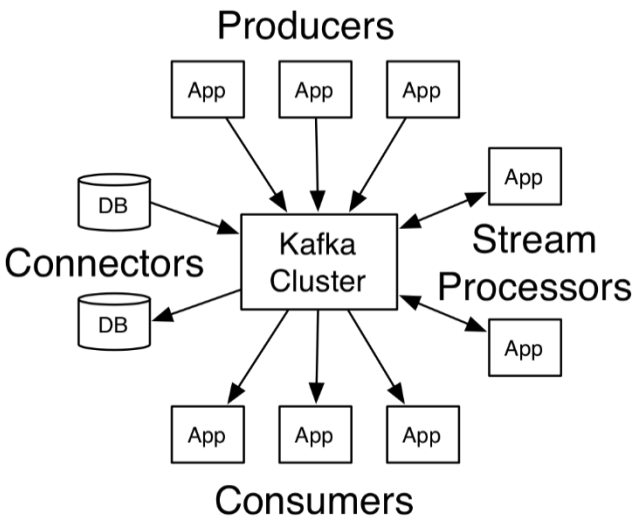


Рис. 1. Архитектура системы передачи данных с использованием брокера сообщений Kafka

Брокер сообщений Apache Kafka как ядро системы потоковой передачи

Выбор Apache Kafka в качестве центрального компонента архитектуры обусловлен рядом преимуществ, которые данная платформа демонстрирует по сравнению с альтернативными решениями для организации очередей сообщений [2]:

– гарантированная доставка сообщений — при возникновении сбоя на стороне потребителя данные не теряются, а сохраняются в очереди до момента восстановления его работоспособности, что критически важно при мониторинге удалённых и труднодоступных объектов;

– горизонтальная масштабируемость — по мере увеличения числа отслеживаемых судов и объектов инфраструктуры кластер Kafka может расширяться добавлением новых брокеров без остановки системы и без изменения логики работы уже подключённых источников и потребителей;

– низкая задержка доставки сообщений — что особенно важно при необходимости оперативного реагирования на внештатные ситуации, например, при отклонении судна от маршрута или резком изменении гидрометеорологических условий;

– разделение (декаплинг) компонентов системы — производители и потребители данных функционируют независимо друг от друга, что повышает общую отказоустойчивость архитектуры.

Телеметрические данные — координаты и курс судна, скорость, расход топлива, параметры работы судовых механизмов, гидрометеорологические характеристики — поступают в систему мониторинга через агентов, взаимодействующих с продюсерами Kafka. Далее сообщения помещаются

в очередь, где обрабатываются потребителями и направляются как в системы долговременного хранения, так и на модули оперативного анализа.

Важной особенностью такой схемы является независимость её компонентов друг от друга: отказ или временная перегрузка одного из элементов (например, модуля визуализации или аналитического сервиса) не приводит к остановке всей системы в целом, поскольку Kafka обеспечивает временное хранение поступивших сообщений с последующей их доставкой, как только соответствующий потребитель восстановит работоспособность. Это принципиально отличает предложенное решение от систем с жёсткой связью между источником и получателем данных, где отказ одного узла способен нарушить работу всей цепочки мониторинга.

Интеграция с инфраструктурой хранения и анализа больших данных

Отдельного внимания заслуживает вопрос интеграции архитектуры потоковой передачи с системами долговременного хранения и аналитической обработки данных [3], представленной на рис. 2.

После поступления в кластер Kafka телеметрические сообщения направляются в распределённую файловую систему HDFS (Hadoop Distributed File System), обеспечивающую надёжное хранение больших объёмов данных с возможностью их репликации между узлами кластера. Для предварительной обработки и подготовки «сырых» данных к последующему анализу применяется инструмент Apache Pig, позволяющий описывать сложные преобразования данных в виде относительно простых скриптов на языке Pig Latin, что существенно упрощает трансформацию разнородной телеметрической информации в единый формат, пригодный для аналитической обработки.

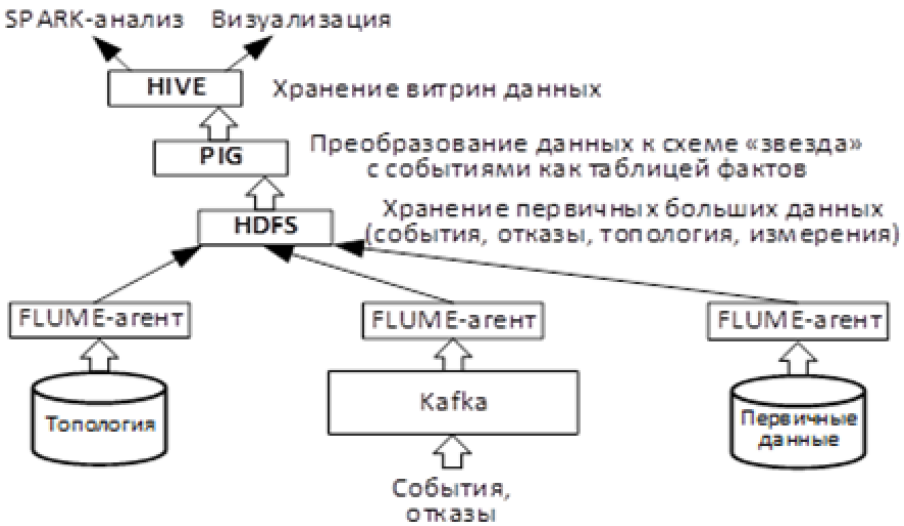


Рис. 2. Интеграция Kafka в систему мониторинга состояния ИТКС с использованием технологий Big Data

Такая двухуровневая схема — потоковая передача через Kafka с последующим накоплением и структурированием данных средствами Hadoop-экосистемы — создаёт основу для применения методов интеллектуального

анализа и машинного обучения. В частности, накопленные и структурированные данные могут использоваться для решения следующих прикладных задач:

− предиктивной оценки времени прибытия судов с учётом текущей навигационной и гидрометеорологической обстановки;

− оптимизации расхода топлива на основе анализа исторических данных о режимах работы судовых механизмов;

− прогнозирования неисправностей судового оборудования по отклонениям контролируемых параметров от нормальных значений;

− выявления аномалий в поведении судов, потенциально свидетельствующих о навигационных нарушениях или технических инцидентах.

Режимы мониторинга: пассивный и активный подходы

Предложенная архитектура поддерживает два принципиально различных режима получения телеметрической информации — пассивный и активный, — выбор между которыми определяется спецификой контролируемого объекта и требованиями к оперативности данных [4].

Пассивный мониторинг предполагает получение событий по мере их естественного возникновения в контролируемой системе: датчик формирует сообщение при достижении определённого условия либо через равные интервалы времени, задаваемые самим источником данных. Такой подход минимизирует избыточную нагрузку на канал связи и кластер обработки, поскольку данные передаются только тогда, когда в этом действительно есть необходимость.

Активный мониторинг, напротив, реализуется путём периодического опроса контролируемых объектов с заданной внешней системой частотой, независимо от того, произошли ли в состоянии объекта какие-либо изменения. Такой режим особенно востребован при необходимости непрерывного отслеживания ключевых судов, а также при точной диагностике состояния критически важных элементов инфраструктуры — шлюзов, портовых кранов, главных двигателей, — когда важно получать данные с гарантированной периодичностью независимо от наличия изменений в контролируемых параметрах.

Использование Kafka-инфраструктуры обеспечивает необходимую гибкость для реализации обоих механизмов в рамках единой архитектуры без необходимости разработки принципиально различных технических решений для каждого из режимов.

Заключение

Рассмотренная архитектура передачи телеметрической информации на основе распределённой платформы Apache Kafka демонстрирует ряд существенных преимуществ по сравнению с традиционными подходами к организации мониторинга объектов водного транспорта. Гарантированная

доставка сообщений, горизонтальная масштабируемость и низкая задержка передачи данных делают предложенное решение пригодным для эксплуатации в условиях постоянно растущей интенсивности судоходства и увеличивающегося числа отслеживаемых объектов.

Интеграция архитектуры с инструментами экосистемы Big Data — распределённой файловой системой HDFS и средствами предварительной обработки данных Apache Pig — создаёт технологическую основу для перехода от простого сбора телеметрии к полноценной предиктивной аналитике состояния судов и портовой инфраструктуры. Поддержка как пассивного, так и активного режимов мониторинга обеспечивает гибкость применения системы для решения широкого круга практических задач — от непрерывного отслеживания ключевых судов до точной диагностики критически важных элементов береговой инфраструктуры.

Таким образом, применение подхода на базе Apache Kafka подтверждает свою эффективность для построения отказоустойчивой, масштабируемой и интеллектуальной системы мониторинга инфраструктуры водного транспорта, способной служить основой для дальнейшего внедрения методов машинного обучения и автоматизированного принятия решений в данной предметной области.

Список литературы

1. Мошак Н. М., Рудинская С. Р., Груздев А. А. Третья платформа информатизации и Big Data // Наукоемкие технологии в космических исследованиях Земли. 2023. Т. 15. № 4. С. 47-59.

2. И чем же она хороша: ТОП-10 достоинств Apache Kafka для Big Data систем [Электронный ресурс] // Школа больших данных. 2019. URL: https://bigdataschool.ru/blog/kafka-big-data-advantages/ (дата обращения: 17.05.2025).

3. Будко Н. П., Васильев Н. В., Груздев А. А. Сбор и обработка больших данных в системах мониторинга информационно-телекоммуникационных сетей средствами технологии Hadoop // Техника средств связи. 2023. № 1(161). С. 78-88. DOI: 10.24412/2782-2141-2023-1-78-88.

4. Груздев А. А., Курносов В. И. Синтез системы мониторинга информационно-телекоммуникационной сети на основе технологии обработки больших данных // Подготовка профессиональных кадров в магистратуре в эпоху цифровой трансформации (ПКМ-2024): сборник трудов Международной научно-практической конференции. 2024. С. 679–683.

УДК 004.722

Методика многофакторного мониторинга и адаптивного восстановления критических сервисов распределенных программно-аппаратных комплексов связи

Прохоркин Д. А.

Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» имени В. И. Ульянова (Ленина), г. Санкт-Петербург, Россия

ПАО «ИНТЕЛТЕХ», г. Санкт-Петербург, Россия

Аннотация: *современные программно-аппаратные комплексы связи характеризуются высокой степенью распределенности, ростом числа взаимодействующих сервисов и жесткими требованиями к непрерывности функционирования. Переход к микросервисной архитектуре повышает масштабируемость, но увеличивает вероятность отказов, связанных с логическим зависанием компонентов, нарушением межсервисного взаимодействия и деградацией производительности. Анализ существующих решений показал, что большинство из них контролирует отдельные параметры (существование процесса, загрузку ресурсов, аварийные сообщения) и не обеспечивает комплексной оценки фактического функционального состояния сервиса. В работе предложена методика многофакторного мониторинга и адаптивного восстановления, объединяющая пять независимых источников диагностической информации (контроль процессов, Heartbeat, журналы событий, межсервисное взаимодействие, вычислительные ресурсы) в интегральный показатель состояния сервиса. Для повышения устойчивости к повторяющимся отказам применен алгоритм адаптивного восстановления на основе экспоненциальной задержки (Exponential Backoff) со стохастическим джиттером, предотвращающим синхронные массовые перезапуски. Представлена математическая модель оценки состояния, методика экспериментальной проверки и подход к организации замкнутого контура обеспечения надежности, объединяющего мониторинг, тестирование, эксплуатацию и сопровождение программного обеспечения.*

Ключевые слова: *программно-аппаратный комплекс связи, распределенная система, микросервисная архитектура, надежность, отказоустойчивость, мониторинг, наблюдаемость, диагностические сообщения (Heartbeat), адаптивное восстановление, эксплуатационная телеметрия, DevOps, SRE.*

Введение

Современные программно-аппаратные комплексы связи представляют собой сложные распределенные системы, включающие множество вычислительных узлов, сетевую инфраструктуру и взаимодействующие программные сервисы. Переход от монолитной архитектуры к сервисным решениям обеспечивает масштабируемость и независимость разработки компонентов, однако усложняет обеспечение надежности: отказ отдельного сервиса способен вызвать каскадное распространение неисправностей и снижение доступности всего комплекса. Особую опасность представляют скрытые отказы, при которых процесс продолжает существовать в операционной системе, но перестает выполнять свои функции

вследствие логического зависания, блокировки потоков или деградации производительности.

На практике надежность распределенных комплексов чаще всего обеспечивается локальными механизмами контроля процессов, сторожевыми таймерами (Watchdog), централизованным журналированием и средствами инфраструктурного мониторинга. Эти решения контролируют отдельные аспекты функционирования и не дают комплексной оценки состояния сервисов. Кроме того, результаты эксплуатационного мониторинга редко используются для совершенствования процессов разработки и тестирования, вследствие чего выявленные дефекты повторяются в последующих версиях продукта — несмотря на то, что современные концепции DevOps и Site Reliability Engineering (SRE) предполагают интеграцию разработки, тестирования, развертывания и эксплуатации в единый жизненный цикл.

Целью исследования является разработка методики многофакторного мониторинга и адаптивного восстановления критических сервисов распределенных программно-аппаратных комплексов связи, повышающей надежность за счет интеграции мониторинга, автоматизированного восстановления и процессов обеспечения качества программного обеспечения. Объект исследования — распределенные программно-аппаратные комплексы связи, функционирующие под управлением специализированных операционных систем; предмет — методы и алгоритмы обеспечения надежности распределенных сервисов на этапах разработки, эксплуатации и сопровождения.

Для достижения цели решаются задачи: анализ современных подходов к обеспечению надежности; разработка архитектуры многоуровневого мониторинга; построение математической модели оценки состояния сервисов; разработка алгоритма адаптивного восстановления; интеграция эксплуатационного мониторинга с процессами обеспечения качества. Научная новизна заключается в объединении многофакторной диагностики, адаптивного восстановления с экспоненциальной задержкой повторных запусков и анализа эксплуатационной телеметрии в единую систему обеспечения надежности.

Анализ современных подходов к обеспечению надежности

В отличие от монолитных приложений, отказ распределенной системы не всегда сопровождается завершением процессов или потерей сетевой доступности узла: широко распространены состояния, при которых процесс существует, но фактически не выполняет функций. Дополнительную сложность создают каскадные отказы, затрудняющие определение первопричины инцидента.

Традиционные методы контроля работоспособности включают: контроль существования процессов (простой и малозатратный, но не обнаруживающий логических зависаний); аппаратные и программные сторожевые таймеры Watchdog (эффективны при полном прекращении функционирования, но не дают информации о причинах отказа и взаимосвязях компонентов); централизованное журналирование (облегчает поиск неисправностей, однако

анализ обычно выполняется постфактум и не предотвращает развитие аварийной ситуации).

Современным направлением является концепция наблюдаемости (Observability), предусматривающая совместный анализ метрик, журналов событий и распределенной трассировки запросов. Де-факто отраслевым стандартом сбора и передачи телеметрии стал открытый фреймворк OpenTelemetry, унифицирующий форматы метрик, журналов и трасс; для низкоуровневого мониторинга без модификации приложений все шире применяются технологии на основе eBPF. Развитием направления служит концепция SRE, предполагающая автоматизацию эксплуатационных процедур и использование объективных показателей надежности при принятии решений о развитии продукта. Вместе с тем большинство существующих систем наблюдаемости ориентировано на облачные среды; их непосредственное применение в специализированных комплексах связи под управлением ОС реального времени (Защищенная операционная система реального времени «Нейтрино») или защищенных ОС (операционная система специального назначения «Astra Linux Special Edition») затруднено из-за ограниченности ресурсов, требований детерминированности и политик безопасности.

Анализ публикаций показывает, что исследования ведутся по направлениям обнаружения отказов, автоматического восстановления, наблюдаемости, интеллектуального анализа журналов и прогнозирования отказов методами машинного обучения, однако рассматривают эти направления преимущественно изолированно. Недостаточно исследованы вопросы комплексной интеграции диагностических механизмов в единую систему принятия решений и использования эксплуатационных данных для совершенствования тестирования. Результаты сравнительного анализа приведены в таблице 1.

Таблица 1 – Сравнительный анализ методов обеспечения надежности

Критерий	**Контроль процессов**	**Watchdog**	**Централизованный. мониторинг**	**Observability**	**Предлагаемая методика**
Контроль существования процесса	+	+	+	+	+
Обнаружение логического зависания	–	±	±	+	+
Анализ журналов	–	–	+	+	+
Контроль Heartbeat	–	±	±	±	+

Критерий	Контроль процессов	Watchdog	Централизованный. мониторинг	Observability	Предлагаемая методика
Контроль межсервисного взаимодействия	–	–	±	+	+
Интегральная оценка состояния	–	–	–	±	+
Автоматическое восстановление	+	+	±	±	+
Обратная связь с тестированием	–	–	–	–	+

Таким образом, научной задачей является разработка методики, обеспечивающей многофакторную диагностику состояния критических сервисов, обнаружение скрытых отказов, адаптивное автоматическое восстановление, накопление эксплуатационной телеметрии и ее интеграцию с процессами обеспечения качества программного обеспечения.

Предлагаемая методика
Концепция и архитектура

Методика основана на совместном анализе нескольких независимых диагностических признаков с последующим вычислением интегральной оценки состояния сервиса и реализуется в виде непрерывного цикла из пяти этапов: сбор диагностической информации; вычисление интегральной оценки; принятие решения о наличии отказа; адаптивное восстановление; накопление эксплуатационной статистики.

Архитектура включает три логических уровня — мониторинга, анализа и восстановления (рисунок 1). На каждом вычислительном узле функционирует локальный агент, осуществляющий непрерывный контроль сервисов и передающий данные центральному модулю анализа, который рассчитывает интегральную оценку и принимает решение о восстановительных мероприятиях. В отличие от централизованных систем, локальное восстановление допускается и при временной недоступности центрального сервера, что исключает единую точку отказа.

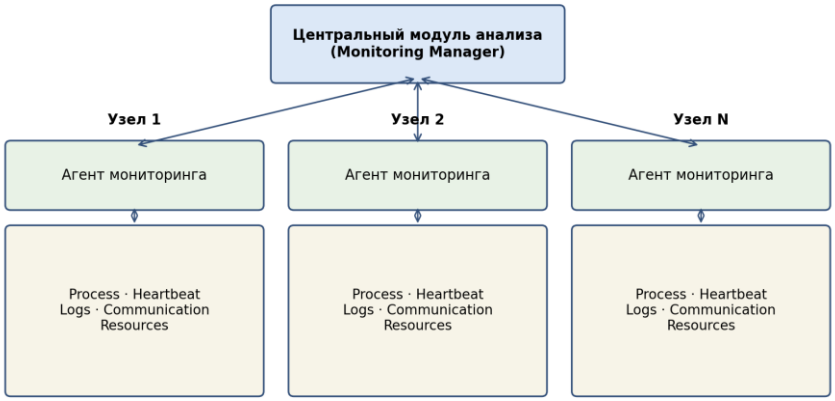


Рис. 1. Архитектура системы мониторинга и восстановления

Многофакторная модель диагностики

Для каждого сервиса контролируются пять групп признаков:

– **Process Status (P)** — существование и состояние процесса, PID, время непрерывной работы;

– **Heartbeat (H)** — периодические диагностические сообщения (идентификатор сервиса, временная метка, версия, внутренний статус, контрольная сумма); отсутствие Heartbeat — признак возможного отказа;

– **Log Status (L)** — критические ошибки, аварийные сообщения, повторяющиеся предупреждения, переполнение очередей; частота ошибок учитывается механизмом скользящего окна;

– **Communication Status (C)** — успешность обмена, время ответа, потери соединений, тайм-ауты, нарушение последовательности обмена;

– **Resource Status (R)** — загрузка процессора, память, файловая система, сетевые очереди, число потоков.

Интегральная оценка состояния сервиса

Вместо бинарной оценки работоспособности вводится интегральный показатель:

$$Q = \sum_{i=1}^{5} w_i d_i, \qquad \sum_{i=1}^{5} w_i = 1, \qquad 0 \le d_i \le 1, \tag{1}$$

где d_i — нормированное значение i-го диагностического признака; w_i — весовой коэффициент. Для критически важных комплексов связи предложены веса: Heartbeat — 0,30; Process — 0,25; Log — 0,20; Communication — 0,15; Resources — 0,10 (отсутствие Heartbeat наиболее достоверно отражает нарушение фактического функционирования). Итоговые значения (уточняемые экспериментально для конкретного комплекса) интерпретируются по непрерывной шкале (таблица 2), что позволяет обнаруживать деградацию до полного отказа. Такая модель устойчивее к единичным диагностическим ошибкам, чем жесткая логическая схема P ∧ H ∧ L ∧ C ∧ R.

Таблица 2 – Классификация состояния сервиса

Значение Q	**Состояние**
$Q \geq 0{,}90$	Нормальная работа
$0{,}75 \leq Q < 0{,}90$	Предупреждение
$0{,}50 \leq Q < 0{,}75$	Деградация
$Q < 0{,}50$	Отказ

Алгоритм адаптивного восстановления

Немедленный повторный запуск при повторяющихся отказах способен привести к циклическому перезапуску процессов (Restart Storm). Для его предотвращения время ожидания перед n-й попыткой восстановления определяется алгоритмом экспоненциальной задержки со случайной компонентой:

$$T_n = \min(T_{max},\ T_0 \cdot 2^n) + J, \qquad (2)$$

где T_0 — начальная задержка; T_{max} — максимально допустимая задержка; J — случайная добавка (Jitter), исключающая синхронный запуск большого числа сервисов после общего отказа и снижающая вероятность повторной перегрузки процессора, сети и подсистемы хранения.

Алгоритм функционирования системы в целом: сбор и нормализация диагностических параметров; вычисление Q; классификация состояния; при отказе — анализ истории рестартов, расчет задержки Backoff, перезапуск, контроль восстановления по Heartbeat; сохранение телеметрии. Если число неудачных попыток превышает установленный порог, сервис переводится в состояние Critical Failure с уведомлением оператора. Псевдокод основного цикла (рис. 2):

```
→  1 while true: CollectMetrics();
→  2 Normalize();
→  3 Q = CalculateScore();
→  4 if Q ≥ Qcrit → continue;
→  5  if  RestartCounter  >  MaxRestart  →
NotifyOperator(), continue; Sleep(Backoff());
→  6 RestartService();
→  7 CheckHeartbeat();
→  8 SaveTelemetry()
```

Рис. 2. Псевдокод основного цикла

Математическая модель и аналитическая оценка эффективности

Распределенный комплекс рассматривается как множество узлов $N = \{n_1, \ldots, n_m\}$, на которых функционируют сервисы $S = \{s_1, \ldots, s_k\}$; состояние каждого сервиса описывается вектором диагностических признаков $D_i = \{P_i, H_i, L_i, C_i, R_i\}$, а состояние системы в целом — матрицей значений признаков размерности $m \times k$.

При условии статистической независимости диагностических механизмов вероятность необнаружения и обнаружения отказа составляют:

$$P_{miss} = \prod_{i=1}^{5}(1 - P_i), \qquad P_{detect} = 1 - P_{miss}, \tag{3}$$

то есть увеличение числа независимых признаков повышает вероятность своевременного обнаружения отказа. Аналогично, при принятии решения по совокупности признаков вероятность ложного восстановления снижается с $P_f = P_{error}$ (один признак) до произведения вероятностей ошибок отдельных механизмов.

Общее время восстановления определяется суммой

$$T_r = T_d + T_a + T_s + T_v, \tag{4}$$

где T_d — время обнаружения отказа; T_a — время анализа причины; T_s — время запуска; T_v — время проверки восстановления. В традиционных системах T_a включает участие персонала; в предлагаемой методике этот этап автоматизирован, поэтому $T_{a'} \ll T_a$ и $T_{r'} < T_r$. Соответственно, коэффициент готовности

$$K_g = \frac{MTBF}{MTBF + MTTR}, \tag{5}$$

возрастает при снижении MTTR даже без уменьшения интенсивности отказов. Вычислительная сложность алгоритма при N узлах и M сервисах составляет $O(N \cdot M)$, поскольку число диагностических признаков фиксировано; линейная сложность обеспечивает применимость методики в ОС реального времени и масштабируемость до десятков вычислительных узлов.

Таким образом, аналитическая оценка показывает: рост вероятности обнаружения скрытых отказов, снижение среднего времени восстановления, уменьшение доли ложных перезапусков, повышение коэффициента готовности и устойчивость к каскадным отказам без существенного увеличения вычислительных затрат.

Методика экспериментальной проверки

Цель экспериментальной проверки — сравнение предложенной методики с традиционными подходами (контроль процессов, Watchdog) по полноте обнаружения отказов, времени обнаружения и восстановления, устойчивости восстановления и коэффициенту готовности. Испытательный стенд состоит из нескольких вычислительных узлов в локальной сети; каждый узел включает операционную систему, локальный агент мониторинга, набор прикладных сервисов, подсистему журналирования и модуль передачи Heartbeat.

Допускается использование как реальных комплексов, так и виртуальных стендов с едиными конфигурациями и параметрами мониторинга.

Рекомендуемые сценарии моделирования отказов: 1) аварийное завершение процесса; 2) логическое зависание (процесс существует, но прекращает обработку сообщений и передачу Heartbeat); 3) нарушение сетевого взаимодействия между сервисами; 4) истощение вычислительных ресурсов (перегрузка процессора, памяти, дисковой подсистемы); 5) каскадный отказ с оценкой способности локализовать первичный источник.

Регистрируемые показатели: среднее время обнаружения отказа T_d; среднее время восстановления MTTR; коэффициент готовности K_g; вероятность обнаружения отказов $P_d = N_d / N$ (доля обнаруженных отказов от общего числа смоделированных); вероятность ложных срабатываний $P_f = N_f / N_e$ (доля ложных уведомлений от общего числа зарегистрированных событий). Методика считается эффективной при снижении T_d и MTTR, росте K_g и P_d, уменьшении числа ложных перезапусков и отсутствии циклических массовых перезапусков. Для достоверности рекомендуется не менее 30 повторений каждого сценария со статистической обработкой результатов и определением доверительных интервалов.

Ограничения: рассматриваются программные отказы распределенных сервисов; аппаратные неисправности узлов, физические повреждения каналов связи, кибератаки, отказы электропитания и ошибки оператора составляют самостоятельные направления дальнейших исследований. Методика проверки применима при приемочных испытаниях, регрессионном тестировании новых версий, анализе эффективности средств мониторинга и сравнении алгоритмов автоматического восстановления.

Практическая реализация и интеграция с жизненным циклом

Программная реализация имеет модульную архитектуру: агент мониторинга, менеджер мониторинга, модуль анализа состояния, модуль восстановления (Recovery Manager), подсистемы журналирования и хранения эксплуатационной статистики. Локальный агент контролирует процессы, Heartbeat, журналы, сетевое взаимодействие и ресурсы, формируя диагностические сообщения (идентификаторы узла и сервиса, временная метка, значения параметров, локальная оценка состояния), передаваемые по защищенному каналу с фиксированным интервалом либо при критических событиях. Центральный модуль агрегирует информацию, рассчитывает Q, выявляет деградацию, анализирует взаимосвязи событий, определяет первопричины отказов и формирует команды восстановления.

После каждого инцидента сохраняются время и тип отказа, диагностические параметры, выполненные действия и результат восстановления. Накопленная телеметрия используется для определения наиболее уязвимых компонентов, корректировки автоматизированных тестов, оценки качества новых версий и анализа тенденций надежности — тем самым формируется замкнутый контур обратной связи между эксплуатацией и разработкой: требования → проектирование → разработка → сборка →

статический анализ → автоматизированное тестирование → развертывание → эксплуатация → мониторинг и телеметрия → анализ причин отказов → корректировка тестов и требований → новый цикл.

При реализации в специализированных ОС (Защищенная операционная система реального времени «Нейтрино», операционная система специального назначения «Astra Linux Special Edition») необходимо учитывать ограничения вычислительных ресурсов, особенности межпроцессного взаимодействия, требования к предсказуемому времени реакции и политики безопасности; модульная архитектура позволяет адаптировать методику к различным платформам без изменения базовых алгоритмов анализа и восстановления.

Выводы

В работе предложена методика многофакторного мониторинга и адаптивного восстановления критических сервисов распределенных программно-аппаратных комплексов связи. В отличие от традиционных подходов решение о состоянии сервиса принимается на основании интегральной оценки совокупности независимых диагностических признаков, что повышает достоверность обнаружения отказов, включая скрытые (логические зависания, нарушения межсервисного взаимодействия), и снижает вероятность ложных срабатываний. Непрерывная шкала оценки позволяет выявлять деградацию до полного отказа, создавая предпосылки для прогнозируемого (предиктивного) обслуживания.

Основные результаты: выполнен анализ современных подходов к обеспечению надежности и выявлены их ограничения; разработаны многофакторная модель диагностики и математическая модель интегральной оценки состояния сервиса; предложен алгоритм адаптивного восстановления на основе Exponential Backoff с джиттером, предотвращающий циклические и каскадные перезапуски; разработана методика экспериментальной проверки; определены принципы интеграции эксплуатационной телеметрии с процессами тестирования и сопровождения, формирующие замкнутый контур повышения качества программного обеспечения.

Дальнейшее развитие исследования целесообразно связать с автоматической адаптацией весовых коэффициентов на основе накопленной статистики, применением методов машинного обучения для прогнозирования отказов и интеграцией методики с цифровыми двойниками распределенных комплексов связи.

Список литературы

1. ГОСТ Р 27.102–2021. Надежность в технике. Надежность объекта. Термины и определения.

2. ГОСТ 27.003–2016. Надежность в технике. Состав и общие правила задания требований по надежности.

3. ГОСТ Р 59793–2021. Информационные технологии. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания.

4. ГОСТ 34.602–2020. Информационные технологии. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы.

5. ГОСТ Р ИСО/МЭК 12207–2010. Системная и программная инженерия. Процессы жизненного цикла программных средств.

6. ГОСТ Р ИСО/МЭК 25010–2015. Системная и программная инженерия. Модели качества систем и программных средств.

7. ISO/IEC/IEEE 12207:2017. Systems and Software Engineering — Software Life Cycle Processes.

8. ISO/IEC 25010:2023. Systems and Software Engineering — SQuaRE — Product Quality Model.

9. Avizienis A., Laprie J.-C., Randell B., Landwehr C. Basic Concepts and Taxonomy of Dependable and Secure Computing // IEEE Transactions on Dependable and Secure Computing. 2004. Vol. 1, No. 1. P. 11–33.

10. QNX Software Development Platform 8.0. System Architecture Guide. QNX Software Systems / BlackBerry.

11. QNX High Availability Framework Developer's Guide. QNX Software Systems / BlackBerry.

12. ООО «РусБИТех-Астра». Astra Linux Special Edition. Руководство администратора.

13. ООО «РусБИТех-Астра». Руководящие указания по конструированию программного обеспечения для Astra Linux Special Edition.

14. Becker M., Dasari D., Casini D. On the QNX IPC: Assessing Predictability for Local and Distributed Real-Time Systems. 2023.

15. Huang L. et al. Metastable Failures in the Wild // Proc. of the 16th USENIX Symposium on Operating Systems Design and Implementation (OSDI). 2022.

16. Nygard M. Release It! Design and Deploy Production-Ready Software. 2nd ed. Pragmatic Bookshelf, 2018.

17. Kleppmann M., Riccomini C. Designing Data-Intensive Applications. 2nd ed. Sebastopol: O'Reilly Media, 2026.

18. Burns B. Designing Distributed Systems: Patterns and Paradigms for Scalable, Reliable Services. Sebastopol: O'Reilly Media, 2018.

19. Beyer B., Jones C., Petoff J., Murphy N. Site Reliability Engineering: How Google Runs Production Systems. Sebastopol: O'Reilly Media, 2016.

20. Beyer B., Murphy N., Rensin D., Kawahara K., Thorne S. The Site Reliability Workbook. Sebastopol: O'Reilly Media, 2018.

21. Gregg B. Systems Performance: Enterprise and the Cloud. 2nd ed. Boston: Addison-Wesley Professional, 2020.

22. OpenTelemetry Documentation. Cloud Native Computing Foundation. URL: https://opentelemetry.io/docs/

УДК 004.056.5

Анализ способов защиты мультисервисных сетей связи от DDoS-атак

Жеглов П. И., Гречишникова Т.А.

ФКУ «Следственный изолятор №1» ГУФСИН России по г. Санкт-Петербургу и Ленинградской области

Аннотация: *Статья посвящена актуальной проблеме защиты мультисервисных сетей связи от распределённых атак типа «отказ в обслуживании» (DDoS). Проведён критический анализ существующих способов противодействия, выявлены их некоторые недостатки: раннее переключение на резерв, снижение коэффициента полезного использования каналов и высокая вероятность обнаружения защитных механизмов злоумышленником. Предложен новый подход, устраняющий эти недостатки. Переключение на теневой сервер осуществляется не в момент обнаружения атаки, а в расчётный момент, предшествующий полному отказу основного оборудования. Приведены аналитические выражения для вероятности безотказной работы и коэффициента использования элементов системы. Сравнительный анализ демонстрирует устранение выявленных недостатков: увеличение времени работы серверов, повышение затрат на атаки для нарушителя, снижение вероятности обнаружения защиты и повышение эффективности использования инфраструктуры.*

Ключевые слова: *DDoS-атака, мультисервисная сеть, теневой сервер, прогнозирование отказа, коэффициент использования, живучесть, информационная безопасность.*

Современные телекоммуникационные системы эволюционируют в сторону мультисервисных архитектур, объединяющих передачу голоса, видео, данных и сигнальной информации в единой транспортной среде. Данные сети играют ключевую роль в обеспечении деятельности коммерческих структур, государственных институтов и оборонного комплекса. Одной из наиболее опасных угроз для их функционирования являются распределённые атаки на отказ в обслуживании (DDoS), целью которых является исчерпание вычислительных ресурсов серверов, пропускной способности каналов или таблиц маршрутизации.

Несмотря на прогресс в области сетевой фильтрации, поведенческого мониторинга и облачных сервисов очистки данных, злоумышленники постоянно совершенствуют тактику – применяют ботнеты с изменяющимися IP-адресами, используют низкоскоростные атаки, имитирующие легитимный трафик, и комбинируют различные векторы воздействия. В этих условиях особую значимость приобретают не только детектирование атак, но и предиктивное управление сетевыми ресурсами, позволяющее максимально долго сохранять обслуживание критических клиентов.

Анализ существующих способ защиты мультисервисных сетей связи можно разделить на три группы[1-4]:

1. Фильтрационные – основанные на «белых» и «чёрных» списках, рейтингах IP-адресов и правилах.

2. Ресурсные – масштабирование серверов, аренда дополнительной пропускной способности, балансировка нагрузки.
3. Резервные – переключение на дублирующие узлы или целые сегменты сети при обнаружении аномалии.

Среди известных решений наиболее близким по технической сущности и выполняемым функциям является способ RU № 2 685 989. В нём предусмотрены: создание базы данных с приоритетами IP-адресов, сбор статистики параметров атак, моделирование вариантов функционирования VPN-сервера, формирование сервера оповещения и переключение узлов на дополнительный сервер при отклонении статистики от эталонной. Однако, как показал анализ, этот метод обладает следующими системными недостатками:

1. Низкая живучесть серверов в условиях DDos-атак.
2. Низкие затраты ресурсов злоумышленника на проведение DDos-атак.
3. Высокая вероятность раскрытия и вскрытия защиты.
4. Низкий коэффициент использования каналов и серверов.

В качестве критериев эффективности приняты:

1. увеличение времени работы серверов в условиях DDos-атак;
2. повышение затрат требуемых ресурсов (длительности и интенсивности) злоумышленника для успешного подавления сервиса;
3. снижение вероятности обнаружения средств защиты нарушителем;
4. повышение коэффициента использования элементов системы (каналов и серверов).

Основная идея предлагаемого способа защиты состоит в создании двух идентичных мультисервисных сетей связи. Первая сеть является рабочей и подвергается реальным атакам. Вторая сеть используется как полигон для контролируемых экспериментов – на ней воспроизводятся атаки с заранее измеренными параметрами, и регистрируются реакции серверов на различные сочетания нагрузки и пропускной способности.

Для каждого сервера определяются уровни загрузки, при которых он выполняет 100% функций, 50–75%, 25–50% и 10–25% своих задач. Эти границы устанавливаются на основе паспортных данных и предварительных тестов.

В рабочей сети регистрируются все входящие воздействия: мощность (пакетов/сек, бит/сек), длительность, типы флагов, распределение по источникам. Эти сигналы записываются в базу данных.

На серверы второй сети последовательно подаются атаки с параметрами, снятыми на первом шаге, – от наименьшей мощности и длительности к наибольшим. Одновременно измеряются:

1. скорость обработки пакетов на каждом сервере;
2. загрузка процессора и памяти;
3. текущая скорость каналов связи (доступа в сеть).

Фиксируются зависимости между скоростью каналов и производительностью обработки при разных уровнях атаки.

Эксперимент повторяется, но теперь во время атаки искусственно снижается пропускная способность каналов (имитация перегрузки или обрыва линий). Регистрируются те же показатели. В результате для каждого сценария атаки и каждого уровня канальной скорости получаются кривые деградации производительности.

На основе полученных зависимостей для рабочей сети вычисляется, через какое время после начала атаки (при текущей скорости каналов) сервер достигнет одного из пороговых состояний (50%, 25% и т.д.). Момент, когда производительность падает ниже 10%, принимается за точку полного отказа t_3.

Измеряется время переключения с основного сервера на теневой (включая обновление таблиц маршрутизации, синхронизацию сессий и т.п.). Если прогнозируемое время до отказа больше или равно времени переключения, то переключение не производится. Как только оно становится меньше времени переключения, инициируется переход на теневой сервер.

Процесс прогнозирования повторяется циклически, с пересчётом оставшегося времени до отказа на основе текущей нагрузки. Это позволяет адаптироваться к изменению интенсивности атаки во времени.

Все данные (измерения, прогнозы, фактические моменты переключений) записываются в физическую модель сервера управления, которая в дальнейшем может использоваться для обучения систем машинного обучения и повышения точности прогнозов.

Для наглядности сведём основные параметры известных способов и предлагаемого способа в таблицу 1.

Таблица 1 – Сравнение характеристик анализируемых способов и предлагаемого способа

Параметр	**Известные способы**	**Предлагаемый способ**
Момент переключения на теневой сервер	Сразу после обнаружения атаки ($t_{обн}$)	За время, равное времени переключения, до прогнозируемого отказа (t_2)
Длительность работы основного сервера под атакой	$t_{обн}+\Delta t_1$	$t_{обн}+\Delta t_2$, где $\Delta t_2>\Delta t_1$
Вероятность безотказной работы до переключения	$P_п=e^{-\lambda(tобн+\Delta t1)}$	$P_с=e^{-\lambda(tобн+\Delta t2)}$, $P_с>P_п$
Временное окно для обнаружения защиты нарушителем	От $t_{обн}$ до окончания переходных процессов	Только вблизи t_2, значительно короче
Коэффициент использования элементов в интервале $[t_1,t_2]$	$K_п=0,5$ (только теневой сервер)	$K_с=1$(оба сервера задействованы)

Схема иллюстрирующая устранение 1 недостатка представлена на рис. 1.

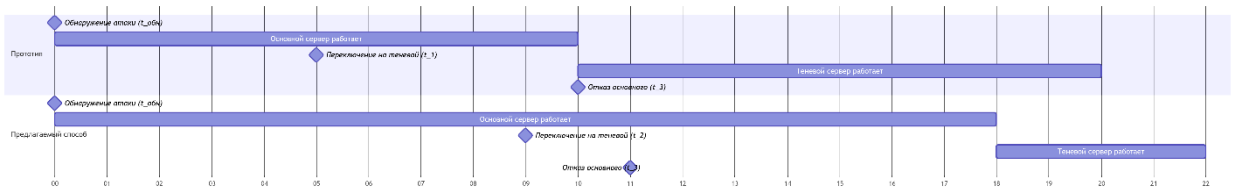


Рис. 1. Схема устранения 1 недостатка

Диаграмма показывает временные интервалы работы основного и теневого серверов для известных способов и предлагаемого способа. У известных способов переключение на теневой сервер происходит сразу после обнаружения атаки (в момент t_1), а в предлагаемом способе – позже, практически перед отказом (t_2). Это даёт дополнительное время работы основного сервера $\Delta t = t_2 - t_1$. Схема иллюстрирующая устранение 2 недостатка представлена на рис. 2.

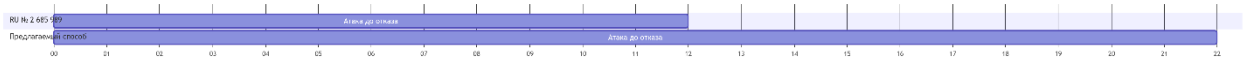


Рис. 2. Схема устранения 2 недостатка

Диаграмма показывает, что для достижения отказа злоумышленнику требуется больше ресурсов (времени или мощности) в предлагаемом способе по сравнению с известными способами. Столбчатая диаграмма даёт количественное сравнение (10 против 22 условных единиц). Схема, иллюстрирующая устранение 3 недостатка представлена на рис. 3

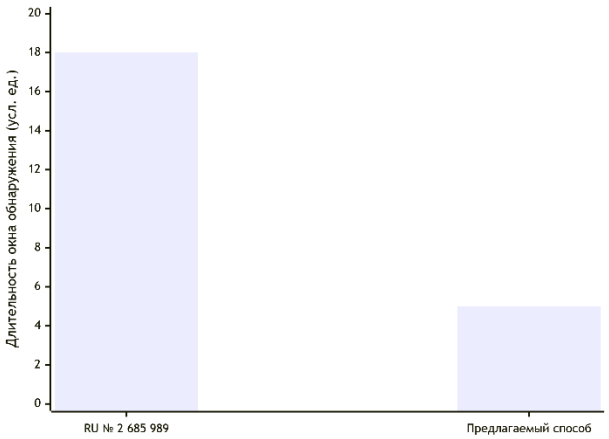


Рис. 3. Схема устранения 3 недостатка

Диаграмма иллюстрирует, что в известных способах окно, в течение которого нарушитель может обнаружить переключение на теневой сервер, значительно длиннее (18 условных единиц), чем в предлагаемом способе (5

единиц), что снижает вероятность обнаружения. Схема, иллюстрирующая устранение 4 недостатка представлена на рисунке 4.

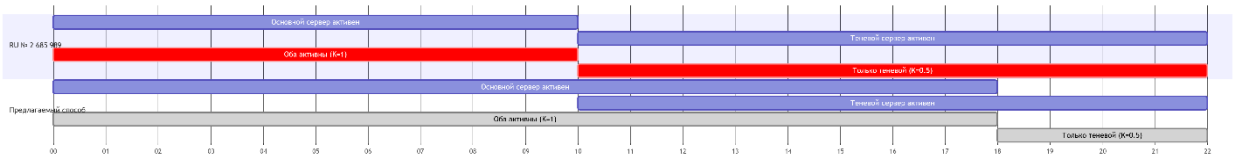


Рис. 4. Схема устранения 4 недостатка.

Диаграмма показывает, сколько элементов системы (основной и теневой серверы) задействованы в каждый момент времени. В известных способах после переключения (с t_1) работает только теневой сервер, коэффициент использования K = 0,5. В предлагаемом способе оба сервера активны до момента t_2, и K = 1 на интервале $[t_1; t_2]$, что даёт выигрыш.

Предложенный способ не требует изменения аппаратной части существующих сетей – достаточно модернизировать программное обеспечение серверов управления и добавить модуль прогнозирования на основе предварительно снятых характеристик. Кроме того, использование второй идентичной сети в качестве испытательного стенда позволяет безопасно (без риска для рабочей инфраструктуры) накапливать знания о поведении системы при различных атаках, что особенно ценно для сетей с динамически меняющейся топологией.

В дальнейшем планируется расширить модель прогнозирования с учётом нестационарности атак (пуассоновские потоки, самоподобный трафик) и внедрить адаптивные алгоритмы, которые автоматически корректируют пороги переключения на основе текущей загрузки и исторических данных. Также возможна интеграция с системами глубокого обучения для классификации типов атак в реальном времени.

В статье представлен новый способ защиты мультисервисных сетей связи от DDoS-атак, основанный на заблаговременном экспериментальном определении зависимостей производительности серверов от параметров атаки и скорости каналов связи. В отличие от известных способов, переключение на теневой сервер производится не по факту обнаружения атаки, а на основе прогноза момента наступления отказа, что позволяет:

1. увеличить время обслуживания легитимных пользователей;
2. повысить требуемые вычислительные и временные ресурсы для злоумышленника;
3. уменьшить вероятность обнаружения защитных мер;
4. повысить коэффициент использования оборудования.

Предложенный способ может быть рекомендован для внедрения в корпоративных и ведомственных сетях, где критически важна непрерывность обслуживания.

Список литературы

1. 1. Способ мониторинга сетей связи в условиях ведения сетевой разведки и информационно технических воздействий Гречишников Е.В., Добрышин М.М., Шугуров Д.Е., Берлизев А. В., Макаров В. Н., RU 2 612 275 дата регистрации: 06.03.2017.
2. 2. Способ снижения ущерба, наносимого сетевыми атаками серверу виртуальной частной сети, авт. Гречишников Е. В., Закалкин П. В., Стародубцев Ю. И. Петухова Ю. А., Добрышин М. М., RU 2 685 989 дата регистрации: 23.04.2019.
3. 3. Способ защиты автоматизированных систем, авт. Гречишников Е. В., Иванов В. А., Белов А. С., Ерышов В. Г., Стародубцев Ю. И., Стукалов И. В., Иванов И. В., Ровчак Ю. М., RU 2 408 927, дата регистрации 01.10.2010;
4. 4. Способ защиты вычислительной сети, авт. Гречишников Е. В., Милая И. В., Санин И. Ю., Стародубцев Ю. И., RU 2 422 892, дата регистрации: 27.06.2011.

УДК 004.056+621.397.4

Метод оптической локации для обнаружения короткофокусных систем видеонаблюдения

Тихонов П. Ю., Смирнов М. В., Машков И. А.

Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» имени В. И. Ульянова (Ленина), г. Санкт-Петербург, Россия

АО «НПП «Сигнал», г. Санкт-Петербург, Россия

Аннотация: *В данной работе исследовались короткофокусные камеры современных смартфонов как средства эксплуатации технического канала утечки видовой информации. Проведен анализ существующих средств обнаружения скрытых устройств видеозаписи, основанных на эффекте ретрорефлексии. Определено влияние конструкционных особенностей и размеров апертур различных модулей камер на мощность обратного сигнала. Проведено сравнение эффективности применения красного, зелёного и фиолетового диапазонов излучения при использовании человеческого глаза и полупроводникового фотодиода в качестве приёмников. Разработан новый метод оптической локации и спроектировано аппаратное решение на базе микроконтроллера STM32. По результатам теоретических расчетов сформулированы рекомендации по выбору оптимальных длин волн для повышения эффективности обнаружения скрытых камер.*

Ключевые слова: *технический канал утечки видовой информации, ретрорефлексия, эффект кошачьего глаза, оптическая локация, лазерное зондирование, короткофокусные камеры*

Введение

Основным способом обнаружения скрытых оптико-электронных приборов является метод оптической локации, основанный на физическом эффекте ретрорефлексии. Однако развитие технологий мобильной фотографии и видеонаблюдения привело к распространению широкоугольных объективов с коротким фокусным расстоянием. Большинство представленных на рынке оптических локаторов используют метод визуального поиска (с непосредственным участием оператора в качестве наблюдателя) с лазерным излучением красного и зелёного спектра. При этом фиолетовые лазеры в ручных визуальных детекторах на рынке практически не представлены.

В условиях роста рынка скрытых камер [1] угроза незаконного видеонаблюдения приобретает беспрецедентный масштаб [2, 3, 4]. Интеграция подобных субмиллиметровых модулей в скрытые системы видеонаблюдения, которые могут быть легко замаскированы под датчики дыма, зарядные устройства (USB-адаптеры), будильники или элементы декора, создает серьезную угрозу информационной безопасности.

Эмпирические наблюдения показывают, что обнаружение таких камер традиционными оптическими локаторами, использующими излучение красного спектра, малоэффективно (рис. 1).

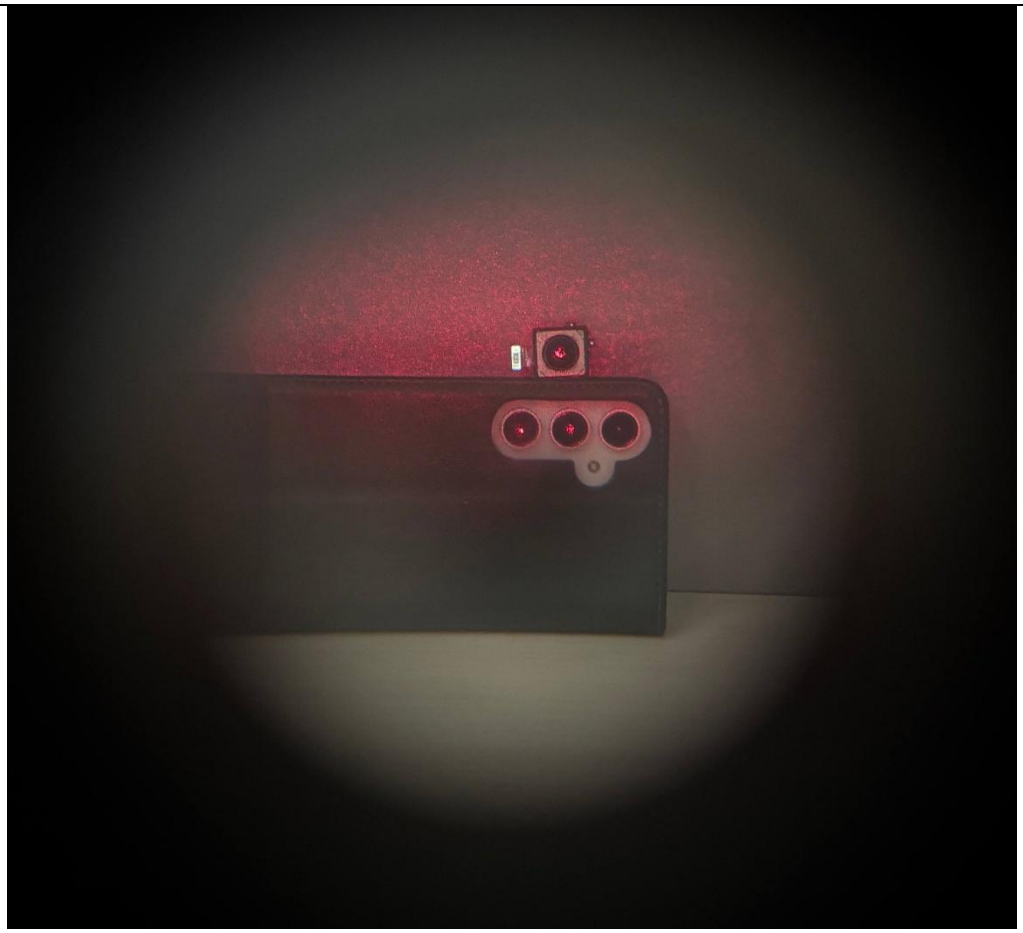


Рис. 1. Отсутствие эффекта световозвращения у сверхширокоугольного модуля (крайний правый модуль) камеры смартфона Samsung Galaxy S23FE при зондировании длиной волны 650 нм в сравнении с остальными модулями

Эксперимент показал, что широкоугольные и сверхширокоугольные камеры не дают оптического отклика (блика) при зондировании красными лазерами с длиной волны 650 нм и мощностями менее 10 мВт и менее 1000 мВт, но при этом демонстрируют отчетливый блик при использовании зеленого (длина волны 532 нм, мощность менее 5000 мВт) и фиолетового (длина волны 405 нм, мощность менее 500 мВт) лазеров. Целью данной работы является повышение эффективности метода обнаружения скрытых средств видеозаписи.

Физическая природа эффекта ретрорефлексии

Когда зондирующее лазерное излучение попадает в объектив, оно преломляется и фокусируется в пятно малого диаметра на поверхности матрицы. Часть электромагнитного излучения поглощается фотодиодами для формирования полезного сигнала, однако определённая доля неизбежно отражается от поверхности кремния, металлических контактов, массива микролинз и инфракрасных фильтров. Это отраженное излучение проходит через объектив в обратном направлении [5]. Объектив направляет отраженный свет обратно, формируя узконаправленный пучок, который возвращается строго к источнику зондирующего излучения (рис. 2).

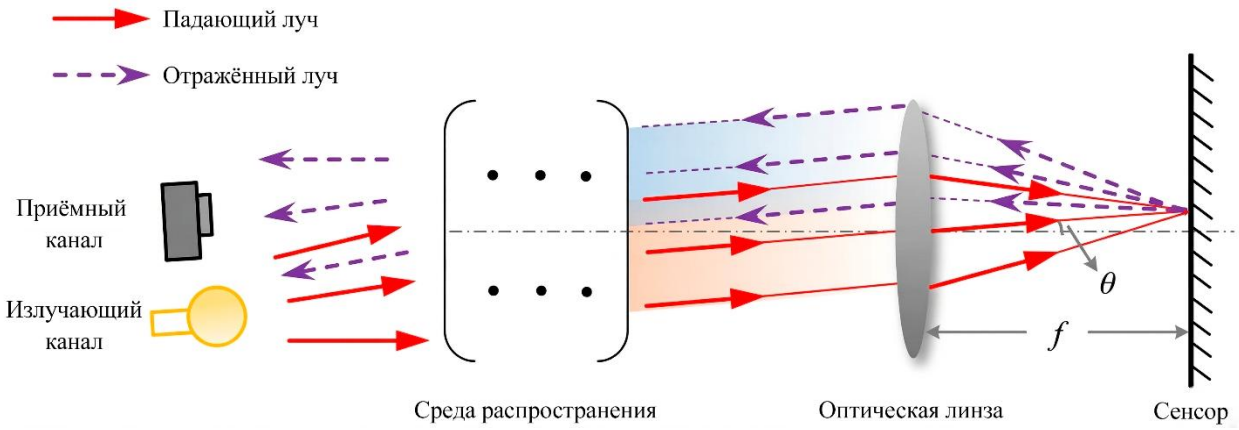


Рис. 2. Базовая модель эффекта ретрорефлексии

Этот узконаправленный пучок обладает интенсивностью, которая на несколько порядков (от 2 до 4) превышает интенсивность диффузного рассеяния Ламберта от корпуса устройства или фоновых предметов [6]. Регистрация этого концентрированного светового потока, визуально воспринимаемого как яркий точечный блик, позволяет обнаруживать скрытые оптические приборы.

Заметность обратного блика определяется эффективной площадью рассеяния (σ) [7]. При поиске скрытых камер она прямо пропорциональна четвёртой степени диаметра входного зрачка (D) и обратно пропорциональна квадрату длины волны зондирующего излучения (λ). С учетом потерь плотности мощности излучения в линзах (k_{ref}) получаем:

$$\sigma = \frac{\pi^3 D^4}{4\lambda^2} \cdot k_{ref}. \quad (1)$$

Моделирование заметности блика для человеческого глаза

Как было описано ранее, современные средства оптической локации используют в основном метод визуального поиска, при котором приёмником является человеческий глаз. Однако, человеческий глаз обладает различной чувствительностью к воздействию на него монохроматического света.

Чувствительность человеческого глаза определяется стандартизированной функцией относительной спектральной световой эффективности монохроматического излучения для дневного зрения $V(\lambda)$ с длиной волны λ (для ночного зрения $V'(\lambda)$) [8]. Функция $V(\lambda)$ нормализована, а её пик приходится на длину волны 555 нм (рис. 3).

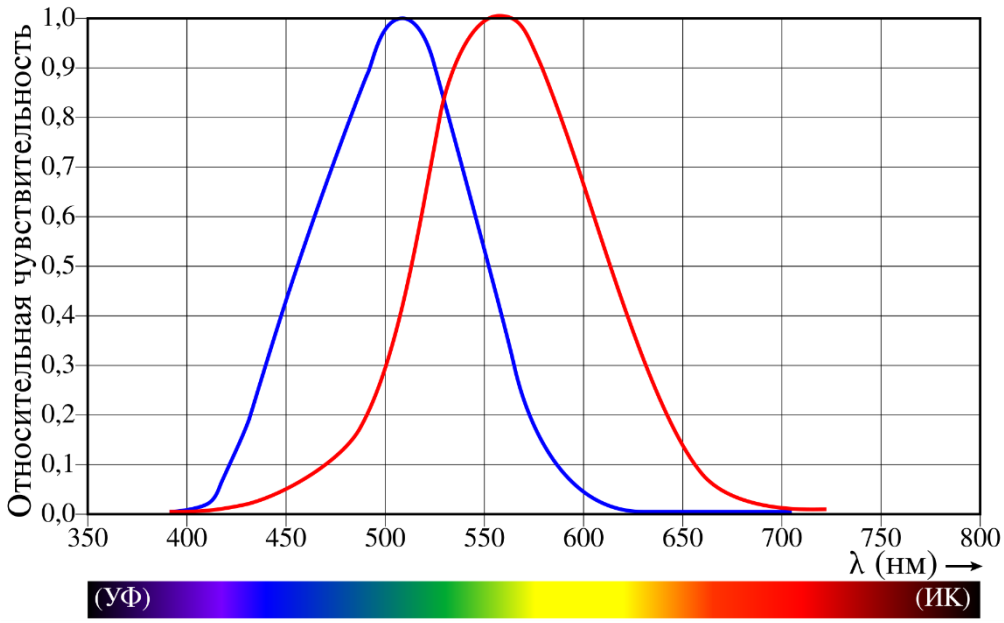


Рис. 3. Спектральная световая эффективность излучения

Эксперименты были проведены с лазерами с длинами волн 650 нм, 532 нм и 405 нм. Чтобы понять, как глаз реагирует на излучение анализируемых лазеров, необходимо обратиться к табличным значениям функции, описанным в стандарте ГОСТ 8.332-2013 (таблица 1).

Таблица 1 – Значения световой эффективности лазеров

Длина волны (λ), нм	Значение $V(\lambda)$	Значение $V(\lambda)$, в %
405	0,00064	0,064
532	0,885	88,5
650	0,107	10,7

Воспринимаемая глазом яркость (световой поток) обратного блика прямо пропорциональна произведению ЭПР и эффективности восприятия этой длины волны. Рассматривая отдельно взятую камеру, можем пренебречь диаметром выходного отверстия, следовательно, воспринимаемый световой поток обратно пропорционален квадрату длины волны и прямо пропорционален эффективности восприятия этой длины волны:

$$\Phi \propto \frac{V(\lambda)}{\lambda^2}. \qquad (2)$$

Проведём нормализацию всех значений относительно красного лазера с длиной волны 650 нм. Составим пропорциональные расчеты, относительно которых рассчитаем заметность блика для человеческого глаза (таблица 2).

Таблица 2 – Расчёт заметности относительно красного лазера для человеческого глаза

Параметр	650 нм	532 нм	405 нм
Физическая ЭПР относительно длины волны 650 нм	1,00	1,49	2,57
Световая эффективность $V(\lambda)$	0,107	0,885	0,00064
Воспринимаемый световой поток Ф, лм	0,107	1,319	0,0016
Итоговая заметность относительно 650 нм	1,00	12,33	0,015

Несмотря на то, что по расчётам ЭПР фиолетовый лазер отражает от матрицы в 2,57 раза больше энергии, чем красный, человеческая сетчатка не способна её воспринять. Итоговая визуальная заметность блика от сенсора камеры будет в 66 раз слабее, чем от красного лазера, и в более чем 800 раз слабее, чем от зелёного лазера.

Моделирование заметности блика для фотодиода

Поскольку сетчатка глаза имеет биологические ограничения на приём излучения с длиной волны 405 нм, имеет смысл рассмотреть модель поиска скрытых закладных устройств видеозаписи, в которой принимающей стороной выступает не человеческий глаз, а полупроводниковый фотодиод.

Для проведения моделирования заметности необходимо использовать данные из технической документации представленных на рынке фотодиодов, например, корпорации Hamamatsu Photonics. По данным графиков спектральной чувствительности и спецификаций датчиков, мы можем подобрать фотодиоды, чувствительные к каждой из исследуемых длин волн.

Для красного излучения с длиной волны 650 нм подходят фотодиоды S4204 [9] и S9345 [10]. Исходя из технической документации данных светодиодов при длине волны 650 нм они обладают фоточувствительностью 0,45 А/Вт.

Для зелёного излучения с длиной волны 532 нм подходит фотодиод S6429-01 [11]. Его пиковая длина волны чувствительности приходится на 540 нм, для которой фоточувствительность составляет 0,27 А/Вт. В данном случае разница с излучением в 8 нм не играет заметной роли, будем считать, что фоточувствительность для 532 нм ≤0,27 А/Вт.

В случае лазерного излучения в 405 нм из-за поверхностного поглощения кремнием коротких волн чувствительность сенсора стремительно падает. В данном случае имеет смысл использовать специализированные фотодиоды для фиолетового диапазона. Для данной длины волны подходит датчик S9195 [12]. В его технической документации для длины волны 405 нм определена фоточувствительность 0,28 А/Вт.

Для фотодиода основным показателем заметности является электрический сигнал (фототок I, А), отражённый от сенсора матрицы камеры. Максимальное значение фототока будет прямо пропорциональна произведению падающей на фотодиод силы излучения (определяемой ЭПР) и фоточувствительности

сенсора $R(\lambda)$ на данной длине волны. Поскольку ЭПР обратно пропорциональна квадрату длины волны для отдельно взятой камеры:

$$I \propto \frac{R(\lambda)}{\lambda^2}. \quad (3)$$

Проведём нормализацию всех значений относительно красного лазера с длиной волны 650 нм аналогично расчётам параметров для человеческого глаза (таблица 3).

Таблица 3 – Расчёт заметности относительно красного лазера для фотодиода

Параметр	650 нм	532 нм	405 нм
Физическая ЭПР относительно длины волны 650 нм	1,00	1,49	2,57
Фоточувствительность $R(\lambda)$	0,45	0,27	0,28
Относительный генерируемый фототок I, А	0,45	0,40	0,72
Итоговая заметность относительно 650 нм	1,00	0,89	1,60

Основываясь на результатах расчётов можно утверждать, что при использовании лазера с длиной волны 405 нм с кремниевым фотодиодом в качестве приёмника, заметность скрытых устройств видеонаблюдения в 1,6 раза превышает заметность при использовании красного лазера (650 нм) и почти в 1,8 раза превышает заметность при использовании зелёного лазера (532 нм).

Экспериментальные результаты

В ходе работы был исследован эффект ретрорефлексии на длинах волн 650 нм, 532 нм и 405 нм для камер смартфона Iphone 15. В качестве зондирующих инструментов использовались соответствующие лазеры: красный (650±10 нм, мощность <1 Вт), зелёный (532 нм, мощность <5 Вт) и фиолетовый (405 нм, мощность <0,5 Вт). В качестве приёмника обратного излучения выступал человеческий глаз. Фотофиксация результатов эксперимента происходила на камеру смартфона Realme 6 Pro.

При зондировании красным лазером блик от основной камеры выглядит больше, чем от сверхширокоугольной камеры. При зондировании зелёным лазером оба модуля демонстрируют чёткий блик, видимый оператором. При зондировании фиолетовым лазером глаз оператора также выявил яркие блики от каждого модуля (рис. 4). Поскольку для проведения эксперимента использовался расфокусированный лазер с длиной волны 405 нм и классом опасности 4, были применены средства защиты зрения от лазерного излучения.

Рис. 4. Результаты зондирования камер смартфона Iphone 15 длинами волн 650 нм, 532 нм и 405 нм

По результатам эксперимента, наиболее эффективным и безопасным способом для данного метода нахождения скрытых камер является зондирование лазером в 532 нм, поскольку он формирует наиболее различимый и отчетливый блик.

Для реализации метода обнаружения при помощи фотодиода была предложена схема аппаратного средства, реализующего поиск скрытых камер. Аппаратное средство спроектировано на базе программируемого микроконтроллера STM32 и включает в себя излучающую и приёмную часть (рис. 5).

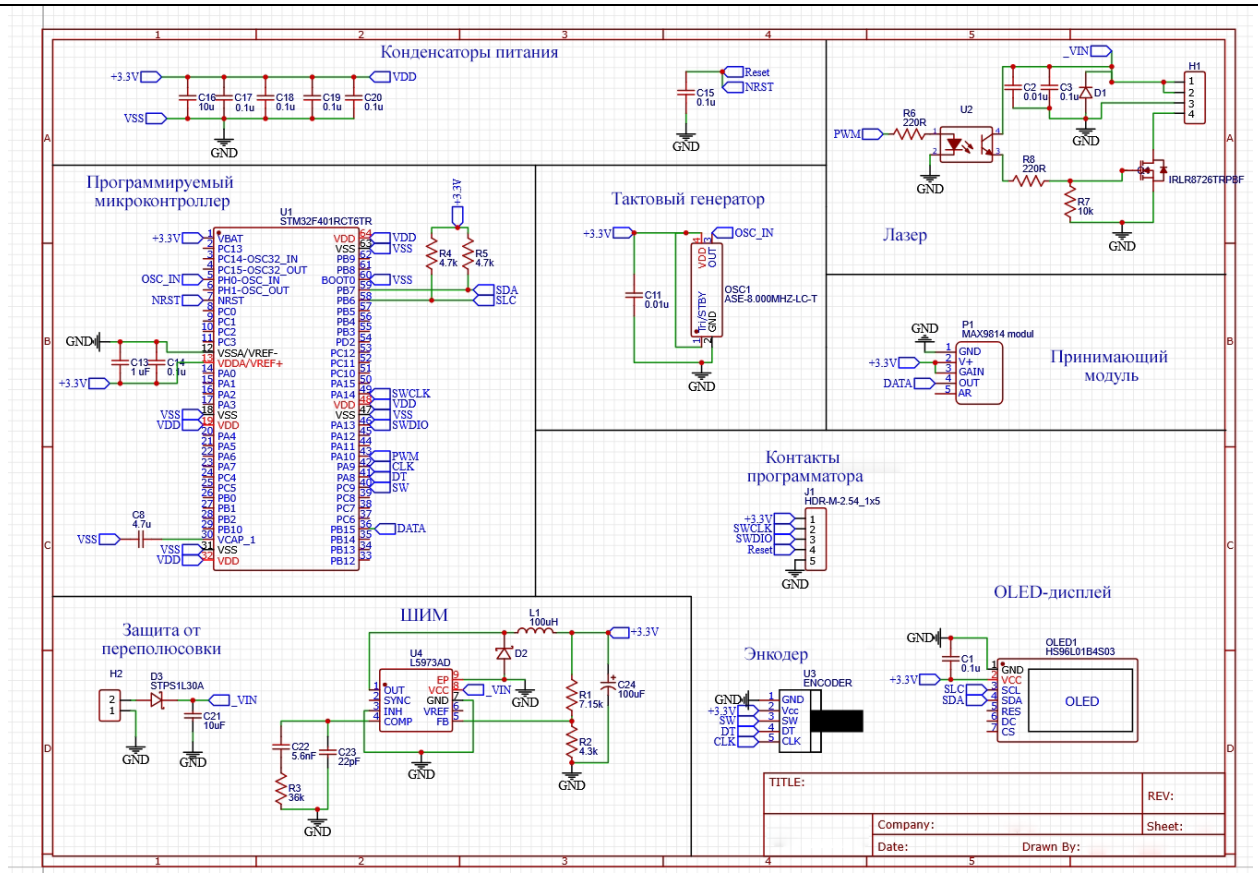


Рис. 5. Схема предлагаемого аппаратного устройства оптической локации

Представленная схема требует аппаратной реализации на основе лазера с длиной волны 405 нм и фотодиода, чувствительного к данной длине волны, а также программной отладки для избавления от шумов.

Заключение

Проведен детальный анализ средств обнаружения скрытых камер методом оптической локации. Установлено, что эффективность красного и зелёного зондирующего излучения ниже фиолетового в 2,5 и 1,7 раза соответственно.

Выявлены существенные ограничения визуального метода локации. Учитывая чувствительность человеческого глаза, лучшую заметность блика обеспечивает зелёный лазер (532 нм), превосходящий красный в 12 раз, а фиолетовый – более чем в 800 раз. Использование фиолетового лазера при визуальном поиске признано неэффективным и опасным для здоровья оператора.

Предложен модифицированный метод локации с использованием полупроводникового фотодиода в качестве приёмника. Расчеты показали, что применение связки «фиолетовый лазер (405 нм) – фотодиод» повышает заметность обратного сигнала в 1,6 и 1,8 раза по сравнению с красным и зелёным лазерами соответственно.

Спроектировано аппаратное решение на базе микроконтроллера STM32 для практической реализации данного метода. На основе полученных данных

сформированы рекомендации: для оперативного визуального поиска закладных устройств целесообразно применять зелёный лазер (532 нм), а для более качественного и глубокого аппаратного анализа помещений – фиолетовый лазер (405 нм) в комплексе с соответствующим фотодиодом.

Список литературы

1. Verified Market Research. Global Hidden Camera Market Size By Type (Tiny Hidden Camera, Remote View Camera, Outdoor Camera), By Application (Personal Use, Detective, Security), By Geographic Scope And Forecast [Электронный ресурс]. URL: https://www.verifiedmarketresearch.com/product/hidden-camera-market/ (дата обращения: 16.03.2026);

2. IPX1031. 2025 Vacation Rental Study on Hidden Cameras & Guest Privacy [Электронный ресурс]. URL: https://www.ipx1031.com/surveillance-rental-study/ (дата обращения: 16.03.2026);

3. Guesty. Airbnb Camera Policy Guidelines (2025) [Электронный ресурс]. URL: https://www.guesty.com/blog/airbnb-camera-policy-for-hosts/ (дата обращения: 16.03.2026);

4. Consumer Affairs. New study finds 1 in 12 vacation rentals have hidden cameras [Электронный ресурс]. URL: https://www.consumeraffairs.com/news/new-study-finds-1-in-12-vacation-rentals-have-hidden-cameras-100224.html (дата обращения: 16.03.2026);

5. Research Gate. Basic model of the cat-eye effect [Электронный ресурс]. URL: https://www.researchgate.net/figure/Basic-model-of-the-cat-eye-effect_fig1_323005025 (дата обращения: 01.03.2026);

6. Chun Liu, Changming Zhao, Haiyang Zhang, Zilong Zhang, Shuyuan Gao, Yunshi Wang. Analysis of Mini-Camera's Cat-Eye Retro-Reflection for Characterization of Diffraction Rings and Arrayed Spots // IEEE Photonics Journal – Volume 11, Number 4, August 2019 – DOI: 10.1109/JPHOT.2019.2933537 – URL: https://ieeexplore.ieee.org/ielx7/4563994/8745542/08790792.pdf (дата обращения 22.03.2026);

7. Skolnik, Merrill Ivan. Introduction to radar system // International Edition 1981. – TK6575S47. – 1980. – 621.3848. – 79-15354. – ISBN 0-07-057909 – P. 3-4;

8. ГОСТ 8.332 – 2013. Световые измерения. Значения относительной спектральной световой эффективности монохроматического излучения для дневного зрения. Общие положения: межгосударственный стандарт: принят Межгосударственным советом по стандартизации, метрологии и сертификации (протокол от 27 декабря 2013 г. № 63-П): приказом Федерального агентства по техническому регулированию и метрологии от 11 июня 2014 г. № 539-ст межгосударственный стандарт ГОСТ 8.332 – 2013 введен в действие в качестве национального стандарта Российской Федерации с 1 октября 2015 г. (Государственная система обеспечения единства измерений) // Кодекс: электрон. фонд правовой и норматив.-техн. информ. URL: https://docs.cntd.ru/document/1200110969 (дата обращения 28.04.2026);

9. Hamamatsu Photonics. Si PIN photodiodes S3096-02, S4204 [Электронный ресурс]. URL: https://docs.rs online.com/711f/A700000013530671.pdf (дата обращения: 05.05.2026);

10. Hamamatsu Photonics. Si PIN photodiode S9345 [Электронный ресурс]. URL: https://www.hamamatsu.com/content/dam/hamamatsu-photonics/ sites/documents/99_SALES_LIBRARY/ssd/s9345_kpin1069e.pdf (дата обращения 05.05.2026);

11. Hamamatsu Photonics. Si PIN photodiodes S6428-01, S6429-01, S6430-01, S7505-01 [Электронный ресурс]. URL: https://www.hamamatsu.com/content/ dam/hamamatsuphotonics/sites/documents/99_SALES_LIBRARY/ssd/s6428-01_etc_kspd1013e.pdf (дата обращения 05.05.2026);

12. Hamamatsu Photonics. Si PIN photodiode S9195 [Электронный ресурс]. URL: https://www.hamamatsu.com/content/dam/hamamatsu-photonics/sites/documents/99_SALES_LIBRARY/ssd/s9195_kpin1068e.pdf (дата обращения 05.05.2026).

УДК 621.396.96:623.62

Системный анализ критических сценариев и рисков функционирования телекоммуникационных систем космических комплексов

Прокофьев М. Ю.

Военно-космическая академия имени А.Ф. Можайского, г. Санкт-Петербург, Россия

Аннотация: *Проведен системный анализ критических сценариев и рисков функционирования телекоммуникационных систем космических комплексов. Рассмотрены режимы работы телекоммуникационных систем, выделены наиболее критичные элементы телекоммуникационной инфраструктуры и обобщены основные сценарии отказов. Сформированы требования к системе управления функциональной надежностью, основанной на вероятностно-математическом аппарате оценивания и прогнозирования ее состояния. Предложено использование рекомендательной системы для поддержки принятия решений по поддержанию функциональной надежности.*

Ключевые слова: *функциональная надежность, телекоммуникационная система, дестабилизирующие факторы.*

Введение

Телекоммуникационные системы (ТКС) являются неотъемлемым элементом космических комплексов (КК). Именно благодаря их непрерывной и исправной работе успешно проводятся сеансы управления (СУ) космическими аппаратами (КА), входящими в состав отечественной орбитальной группировки (ОГ).

Рост численности отечественной орбитальной группировки приводит к увеличению нагрузки на телекоммуникационную инфраструктуру наземного автоматизированного комплекса управления (НАКУ) КА при практически неизменном количестве командно-измерительных пунктов. Возникающее противоречие между возрастающими требованиями к ТКС и ограниченностью инфраструктурных ресурсов обусловливает необходимость совершенствования методов обеспечения их функциональной надежности и проведения системного анализа факторов, способных привести к ее снижению.

Новизна работы заключается в обосновании структуры вероятностно-математического аппарата оценивания функциональной надежности (ФН) ТКС КК на основе полумарковских моделей и рекомендательной системы поддержки принятия решений.

Цель статьи: системный анализ критических сценариев и рисков функционирования ТКС КК для обоснования подходов к поддержанию их ФН.

Анализ режимов работы, критических узлов и классификация сценариев отказов телекоммуникационных систем космических комплексов

ТКС НАКУ КА функционируют в круглосуточном режиме и обеспечивают непрерывный обмен информацией между командно-измерительным пунктом (КИП) и центром управления полетами (ЦУП). Вследствие высокой критичности выполняемых задач любые нарушения их функционирования способны привести к снижению качества управления КА [1]. Поэтому обеспечение функциональной

надежности ТКС должно быть ориентировано на предупреждение отказов как аппаратных, так и программных компонентов системы.

Исходя из периодизации уровня нагрузки, поступающей на элементы ТКИ НАКУ КА выделяются следующие режимы функционирования ТКС:

− дежурный прием, при котором осуществляется обмен служебной информации при отсутствии СУ КА;

− СУ КА;

− сброс целевой информации;

− аварийное восстановление каналов.

Наиболее критичными элементами ТКИ КК являются узлы коммутации сетей связи (УКСС), обеспечивающие взаимодействие КИП и ЦУП. На рис. 1 наглядно представлено, что их отказ способен привести к информационной изоляции отдельных объектов НАКУ КА и снижению качества управления КА.

Рис. 1. Место телекоммуникационного комплекса КИП (УКСС) в структуре интегрированной системы информационного обмена

При обобщении основных сценариев отказов ТКИ КК можно разделить их на три группы, представленные в таблице 1.

Таблица 1 – Классификация сценариев отказов ТКИ КК

Уровень проявления	**Типовые сценарии**	**Влияние на ФН**
Физический	Обрыв проводной линии, отказ аппаратного элемента	Задержка передачи командно-программной и (или) телеметрической информации, переход на низкоскоростной резервный канал
Канальный, сетевой	Перегрузка интерфейсов, конфликт конфигураций	Невозможность работы в реальном масштабе времени, потеря целостности данных

Уровень проявления	Типовые сценарии	Влияние на ФН
Информационная безопасность	Деструктивное воздействие технических средств, подмена служебной информации	Принятие неверных управленческих решений, угроза потери КА

Формирование требований к системе управления функциональной надежностью телекоммуникационных систем космических комплексов

В целях снижения вероятности наступления критических сценариев и минимизации рисков функционирования ТКС КК необходимо непрерывно контролировать состояние ее ФН. При этом важна не только текущая ФН, но и ее прогнозируемое состояние. Система управления ФН ТКС должна основываться на двухконтурной модели оценивания: первый контур – оценивание текущего состояния ФН, второй – прогнозирование ФН на оперативном интервале.

Для оценивания и прогнозирования ФН необходимо контролировать параметры функционирования ТКС и учитывать влияние дестабилизирующих факторов, что позволяет выявлять признаки деградации системы и прогнозировать ее состояние.

Устойчивая деградация одного или более контролируемых параметров должна являться основанием для активации алгоритмов проведения углубленного технического диагностирования с целью выявления причин такой динамики изменений параметров функционирования ТКС. Так можно определить текущее нарушение порядка функционирования системы. Но для прогнозирования состояния ФН необходимо формирование вероятностно-математической модели, на основе выходных данных которой производится расчет единичных, отражающих состояние выполнения отдельных процессов, и комплексных, отражающих функциональное состояние всей системы, показателей ФН.

В качестве единичного показателя ФН отдельного процесса может использоваться коэффициент частичной функциональной готовности [3]:

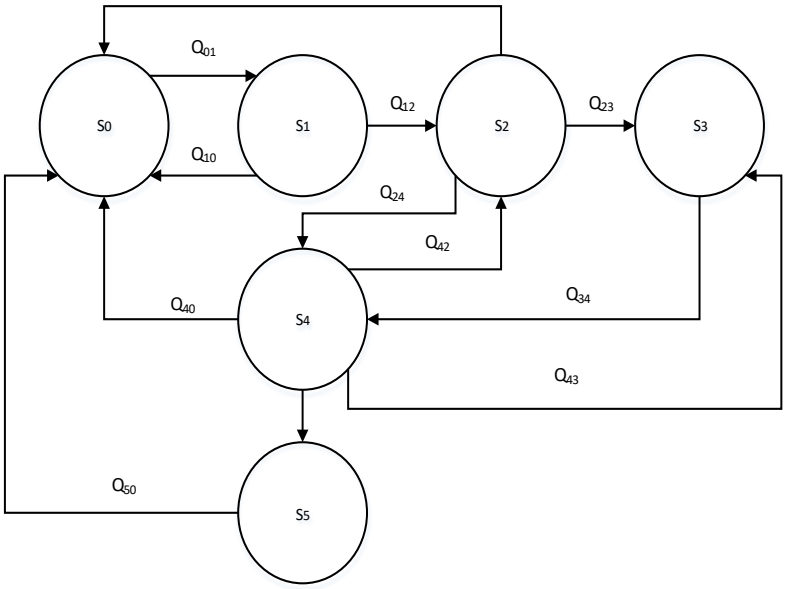
$$K_{i\Phi\Gamma} = \frac{1/\Omega_i}{1/\Omega_i + T_{i\Pi P}}, \quad (1)$$

где Ω_i – интенсивность потока заявок, $T_{i\text{ПР}}$ – среднее время простоя процесса.

Данный показатель характеризует доступность конкретной функции системы и позволяет выявлять процессы, наиболее подверженные деградации [4].

На рисунке 2 приведен пример графа состояний процесса обмена данными в ТКС, представленного в виде полумарковской цепи и предназначенного для оценивания ФН. Выбор полумарковского метода в данном случае обусловлен неэкспоненциальностью законов распределения времени нахождения в некоторых из состояний графа, например в состояниях S_1 и S_2, что характерно для параметров сетевого трафика. В представленном графе S_0 – обмен данными в рамках требований к качеству выполнения процесса; S_1 – кратковременное нарушение порога, не приводящее к сбою процесса; S_2 – устойчивое нарушение порогов, сохраняющееся на протяжении нескольких итераций мониторинга; S_3 – функциональный отказ; S_4 – состояние углубленной диагностики; S_5 – состояние аварийного восстановления работоспособности процесса; Q_{ij} – вероятность перехода из состояния i в состояние j.

Рис. 2. Граф состояний процесса обмена данными в ТКС



Комплексная оценка ФН системы формируется на основе совокупности коэффициентов частичной функциональной готовности отдельных процессов с учетом их критичности [3]:

$$K_{\Phi\Gamma} = \sum_{R\subseteq\{1,\ldots,M\}} \left[\left(\prod_{i\in R} K_{i\Phi\Gamma} \right) \left(\prod_{j\notin R} \left(1 - K_{i\Phi\Gamma}\right) \right) \left(1 - \sum_{j\notin R} \omega_j \right) \right], \quad (2)$$

где ω_j – вес j-го процесса, определяемый экспертным методом, M – конечное множество возможных процессов, выполняемых в системе, R – множество работающих процессов.

Для прогнозирования состояния системы на оперативном интервале времени может использоваться коэффициент оперативной функциональной готовности [3]:

$$K_{O\Phi\Gamma}(\tau_{O\Pi}) = K_{\Phi\Gamma} \cdot e^{-\frac{\tau_{O\Pi}}{T_\Phi}}, \quad (3)$$

где $\tau_{\text{оп}}$ – оперативный интервал времени, T_Φ – средняя наработка на полный функциональный отказ.

Значение данного показателя отражает вероятность сохранения системой работоспособности на заданном оперативном интервале времени в соответствии с классическими вероятностными моделями надежности [5].

По результатам оценивания ФН и технического диагностирования рекомендательная система формирует предложения по предупреждению отказов и выбору управляющих воздействий.

Таким образом, обеспечение ФН ТКС КК требует совместного применения вероятностно-математического аппарата оценивания и прогнозирования, средств технического диагностирования и рекомендательной системы поддержки принятия решений.

Заключение

Полученные результаты подтверждают целесообразность применения аппарата оценивания и прогнозирования ФН ТКС КК совместно с рекомендательной системой. Предложенный подход обеспечивает переход от реактивного устранения отказов к проактивному управлению функциональной надежностью в условиях роста нагрузки на телекоммуникационную инфраструктуру.

Список литературы

1. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

2. Протокол заседания постоянно действующей комиссии по оценке качества выполнения задач управления ОГ КА НСЭН средствами НАКУ КА НСЭН и измерений.

3. Шубинский И. Б. Функциональная надежность информационных систем / И. Б. Шубинский. Методы анализа – М.: «Журнал Надежность», 2012. – 296 с.

4. Клейнрок Л. Теория массового обслуживания / Клейнрок Л.; пер. с англ. — М.: Машиностроение, 1979. — 432 с.

5. Барлоу Р. Статистическая теория надёжности и испытания на безотказность / Барлоу Р., Прошан Ф.; пер. с англ. — М.: Наука, 1984. — 328 с.

УДК 004.056

Математическая модель речевого сигнала при передаче по цифровому каналу связи

Токарева У. В., Казакова Е. А., Андреев Р. А.

Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» имени В. И. Ульянова (Ленина), г. Санкт-Петербург, Россия

АО «НПП «Сигнал», г. Санкт-Петербург, Россия

Аннотация: *В статье представлена математическая модель преобразования речевого сигнала при применении нейросетевых технологий голосового преобразования и его последующей передаче по протоколу VoLTE. Рассмотрены механизмы формирования статистических артефактов на этапе AI-обработки, а также их трансформация в процессе сжатия кодеком AMR-WB и транспортировки по сети мобильной связи. Получена аналитическая зависимость мощности шума квантования от эксцесса распределения LPC-остатка. Приводятся результаты моделирования и экспериментальной верификации устойчивости признаков AI-преобразования после прохождения транспортного конвейера VoLTE.*

Ключевые слова: *голосовые дипфейки; LPC; эксцесс; шум квантования; VoLTE; AMR-WB; AI-обработка речи; RVC.*

Введение

Современные технологии синтеза и преобразования речи на основе глубоких нейронных сетей позволяют формировать голосовые сигналы, практически неотличимые от естественной речи человека. Архитектуры типа Retrieval-based Voice Conversion (RVC), VITS и HiFi-GAN обеспечивают высокую реалистичность синтеза, что делает их востребованными в медиаиндустрии, игровых приложениях и виртуальных ассистентах.

Одновременно развитие данных технологий создает риски подмены голосовой идентичности, используемой в мошеннических схемах и атаках социальной инженерии. Существующие методы детекции голосовых дипфейков демонстрируют высокую точность в лабораторных условиях на несжатых аудиофайлах. Однако при передаче речи по реальным каналам мобильной связи, в частности по протоколу VoLTE, эффективность детекторов существенно снижается.

Это обусловлено отсутствием формализованного математического описания влияния транспортного конвейера (кодирование, квантование, пакетизация) на статистические признаки AI-преобразования. В связи с этим возникает необходимость построения модели, описывающей трансформацию речевого сигнала на всех этапах: от нейросетевой обработки до передачи по мобильной сети.

Цель работы: разработка математической модели влияния транспортного конвейера VoLTE на статистические артефакты AI-преобразования речи,

позволяющей прогнозировать устойчивость признаков детекции после компрессии кодеком AMR-WB.

Задачи:

1. Формализовать зависимость мощности шума квантования от эксцесса распределения LPC-остатка
2. Вывести коэффициент дисторсии DPCM-сжатия для AI-сигналов
3. Верифицировать модель экспериментально на данных ASVspoof 2019 после кодирования AMR-WB

Математическая модель AI-преобразования

Математически процесс AI-преобразования речевого сигнала формализуется как применение нелинейного оператора к исходному сигналу $x(t)$, что в итоге приводит к выходному сигналу $y(t)$, содержащему аддитивный шум артефактов $\xi(t)$:

$$y(t) = \mathcal{F}\big(x(t)\big) + \xi(t), \quad (1)$$

где

– $x(t)$ – исходный непрерывный аналоговый речевой сигнал;

– $y(t)$ – преобразованный выходной сигнал;

– $\mathcal{F}(\cdot)$ – нелинейный оператор преобразования, реализуемый нейросетевой архитектурой (энкодер, декодер и вокодер);

– $\xi(t)$ – аддитивный шум артефактов, характеризующийся статистическими свойствами: $\mathbb{E}[\xi] \neq 0, \gamma_1(\xi) > 0, k(\xi) > 0$.

Архитектура RVC (Retrieval-based Voice Conversion) включает этапы извлечения контента (HuBERT), квантования латентного пространства, вероятностного декодирования (normalizing flow) и генерации формы волны (HiFi-GAN). На каждом этапе происходит частичная потеря информации и аппроксимация распределения сигнала.

Для количественной оценки статистических искажений используется анализ остатка линейного предсказания. LPC-остаток – это ошибка предсказания линейной модели и вычисляется как разность между фактическим и предсказанным сигналом:

$$r[n] = s[n] - \hat{s}[n], \quad (2)$$

где:

– $s[n]$ – значение сигнала в сэмпле;

– $\hat{s}[n]$ – предсказанное значение

Распределение амплитуд остатка линейного предсказания (LPC-остатка) для естественной речи близко к гауссовскому с коэффициентом остроты $k \approx 3$. Для сигналов, преобразованных с применением нейросетей, наблюдается статистически значимый рост эксцесса:

$$k_{AI} = \frac{E\big[e^4[n]\big]}{\sigma_\varepsilon^4} \approx 5.72 \pm 0.41 \quad (3)$$

Передача голоса по VoLTE с речевым кодеком AMR-WB

Для оценки устойчивости выявленных статистических особенностей необходимо проанализировать влияние транспортного конвейера VoLTE. Кодек AMR-WB основан на линейном предсказании и дифференциальной импульсно кодовой модуляции (DPCM)

Традиционная оценка мощности шума квантования $\sigma_q^2 = \frac{\Delta^{12}}{12}$ справедлива лишь при равномерной или гауссовской плотности входного сигнала. Однако, для сигналов, преобразованных с применением нейросетей, наблюдается статистически значимый рост эксцесса распределения LPC-остатка, котором реальная мощность шума увеличивается.

Рост эксцесса увеличивает дисперсию ошибки квантования относительно классической оценки. В рамках исследования получена аналитическая коррекция формулы мощности шума квантования, учитывающая отклонение эксцесса от нормального распределения:

$$\sigma_{q,AI}^2 = \frac{\Delta^2}{12} \cdot (1 + \beta \cdot (k_{AI} - 3)) \quad (4)$$

где, $\beta = 0.18$ – эмпирический коэффициент, учитывающий влияние формы распределения.

Подстановка экспериментальных значений даёт увеличение мощности шума квантования приблизительно на 45% по сравнению с естественной речью:

$$K_{DPCM-AI} \approx 1.45 \quad (5)$$

Таким образом, транспортный конвейер VoLTE не устраняет артефакты AI-преобразования, а трансформирует их в виде аномально высокой мощности шума квантования.

Экспериментальная верификация

Для верификации была разработана программная реализация классификатора, архитектура которой основана на модульном принципе. Модуль предобработки выполняет загрузку файлов и разбивает на фреймы. Модуль извлечения вычисляет статистические характеристики речевого сигнала. Модуль статистической агрегации рассчитывает для каждого признака набор статистик. Модуль классификации GMM реализует независимые гауссовы смеси. Принятие итогового решения производится на основе разности логарифмических правдоподобий, вычисленных для каждой из двух независимых GMM-моделей.

Экспериментальная проверка проводилась в два этапа. Первый этап – экспериментальные оценки проводились на «чистом» наборе данных ASVspoof 2019, после чего с моделированием искажений, таких как шум квантования, компрессия или ограничение полосы пропускания канала. Это позволило провести валидное сравнение с классическими методами.

Таблица 1 – Сравнительная оценка эффективности моделей на тестовом подмножестве ASVspoof2019 LA

Признаковое пространство	AUC	EER, %	Точность при оптимальном пороге	Время инференса
MFCC+CQCC+ZCR (57 признаков)	0.9378	13.91	92.1%	42 мс
Baseline + статистики LPC-остатка (85 признаков)	0.9389	13.52	93.9%	47 мс

Исходя из результатов в таблице 1, добавление статистик LPC-остатка повысило AUC и снизило ERR. Прирост точности составил 1.8%.

Анализ ошибок показал, что 68% записей, корректно классифицированных только моделью с LPC, относились к атакам на базе RVC и диффузионных моделей – именно тех систем, где фазовые искажения наиболее выражены. Это свидетельствует о том, что статистики LPC-остатка особенно чувствительны к артефактам, вносимым нейросетевыми вокодерами при неточном восстановлении фазы сигнала. ROC-кривая предложенной модели (LPC-enhanced) на тестовом подмножестве ASVspoof2019 LA представлена на рисунке 1.

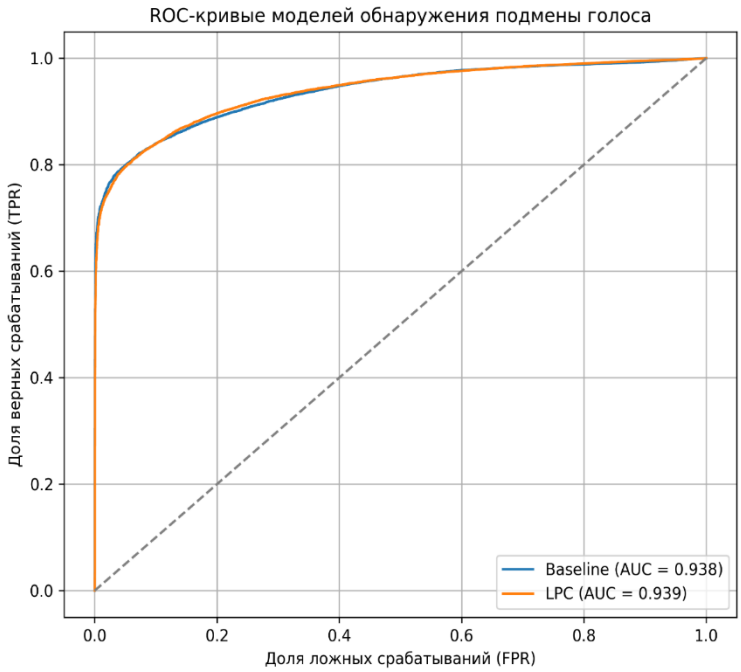


Рис. 1. ROC-кривая предложенной модели (LPC-enhanced) на тестовом подмножестве ASVspoof2019 LA

Полученные результаты подтверждают, что разработанное программное средство обладает высокой эффективностью в задаче детекции AI-преобразованной речи в контролируемых лабораторных условиях и может

служить основой для дальнейших исследований устойчивости метода к реальным каналам передачи с учетом шума квантования и других транспортных искажений.

Второй этап экпериментальной проверки - оценка влияния шума квантования на характеристики LPC-остатка. Для каждого сигнала вычислялся эксцесс распределения LPC-остатка и эмпирическая мощность шума квантования.

Результат показал, что для естественной речи мощность шума совпадает с классической оценкой с относительной погрешность не более 5%, в то же время для AI-преобразованных сигналов мощность шума превышает классическую оценку на 38-52%, что подтверждает справедливость формулы (5).

Таким образом, компрессия не устраняет артефакты AI-преобразования, а усиливает их статистическое проявление. Получение аналитической зависимости мощности шума квантования от эксцесса распределения LPC-остатка составляет научную новизну настоящего исследования.

Согласно разработанной модели, процессы дискретизации и пакетизации в тракте VoLTE не модифицируют статистические характеристики сигнала. Протокол RTP также не влияет на полезную нагрузку, сохраняя параметры, сформированные на этапе кодирования.

Следовательно, прохождение сигнала через конвейер VoLTE не устраняет артефакты AI-преобразования, а трансформирует их.

Для подтверждения теоретических выводов проведён эксперимент на сжатых AI- и естественных сигналах, прошедших идентичный конвейер обработки.

В качестве классификатора использовалась ранее описанная модель. На рисунке 2 представлен анализ сжатых аудиофайлов, созданных при помощи искусственного интеллекта.

segment_id	label	score	ll_genuine	ll_spoof
natural_118	bonafide	105.48457514248133	-551.9602731857888	-446.47569804330743
converted_118	spoof	171.70506164171434	-490.398632479353	-318.6935708376387
converted_ogg_118	spoof	310.3602298580478	-671.7601914631092	-361.39996160506143
natural_119	bonafide	59.14280575837688	-503.52959854251134	-444.38679278413446
converted_119	spoof	135.66438125553321	-438.5214877012874	-302.8571064457542
converted_ogg_119	spoof	135.72546510540695	-471.4518413015333	-335.72637619612635
natural_120	bonafide	91.82338918565193	-487.0150975824875	-395.19170839683557
converted_120	spoof	128.09657546576784	-450.7226644395509	-322.62608897378306
converted_ogg_120	spoof	271.0934638277304	-649.523502069039	-378.4300382413086
natural_121	bonafide	251.69744620014694	-747.3686845689681	-495.67123836882115
converted_121	spoof	230.14438188649734	-566.0289470665184	-335.88456518002107
converted_ogg_121	spoof	253.09203378395205	-609.6419585178809	-356.54992473392883
natural_122	bonafide	252.51282249637643	-677.4363040983344	-424.923481601958
converted_122	spoof	213.3443800409405	-525.1910694789738	-311.84668943803325
converted_ogg_122	spoof	250.7770212812211	-620.3344991427705	-369.5574778615494

Рис. 2. Анализ сжатых аудиофайлов, созданных при помощи искусственного интеллекта

Как видно из данных, все сегменты AI-преобразованной речи получили положительные оценки, подтверждающие сохранность детектируемых артефактов после прохождения транспортного конвейера.

Анализ естественных сжатых аудиофайлов представлен на рисунке 3.

segment_id	label	score	ll_genuine	ll_spoof
natural_118	bonafide	105.48457514248133	-551.9602731857888	-446.47569804330743
natural_119	bonafide	59.14280575837688	-503.52959854251134	-444.38679278413446
natural_120	bonafide	91.82338918565193	-487.0150975824875	-395.19170839683557
natural_121	bonafide	251.69744620014694	-747.3686845689681	-495.67123836882115
natural_122	bonafide	252.51282249637643	-677.4363040983344	-424.923481601958
natural_ogg_118	bonafide	108.09499135851394	-559.7691415210134	-451.6741501624994
natural_ogg_119	bonafide	72.2021856867915	-519.9984379308037	-447.7962522440122
natural_ogg_120	bonafide	110.69533096106017	-519.3397910411129	-408.64446008005274
natural_ogg_121	bonafide	265.6113024875872	-757.9268941947031	-492.3155917071159
natural_ogg_122	bonafide	244.8096486269373	-684.6739897591505	-439.86434113221316

Рис. 3. Анализ естественных сжатых аудиофайлов

Полученные значения свидетельствуют о корректном отнесении данных сегментов к классу естественной речи. Отсутствие ложных срабатываний подтверждает, что компрессия кодеком AMR-WB не вносит артефактов, имитирующих признаки AI-преобразования.

Вывод

В работе разработана математическая модель преобразования речевого сигнала при AI-обработке архитектурой RVC и его передаче по протоколу VoLTE.

Теоретический вклад:

Получена аналитическая коррекция формулы Беннета для мощности шума квантования при DPCM-сжатии AI-речи, где коэффициент 0.18 установлен эмпирически (R^2=0.91).

Экспериментальная верификация:

Эксцесс LPC-остатка для RVC-речи: kAI = 5.72 ± 0.41

Естественная речь: knat = 3.24 ± 0.18

Мощность шума увеличивается на 45% (теория) vs 43±9% (эксперимент)

Устойчивость к VoLTE:

После AMR-WB:

Предложенный метод: EER = 13.52%, точность 93.9%

Baseline (без LPC): EER = 13.91%, точность 92.1% - Прирост +1.8% статистически значим (p=0.003)

Практическая значимость:

Доказано, что артефакт в виде повышенной мощности шума квантования сохраняется после компрессии, что позволяет размещать детектор как на стороне оператора связи, так и на абонентском устройстве.

Список литературы

1. Мирошников Н. Ю. Способ определения ИИ-подделок голосовых аудиозаписей: выпускная квалификационная работа специалиста / Н. Ю. Мирошников ; науч. рук. А. Д. Шульженко. – Санкт-Петербург: СПбГЭТУ «ЛЭТИ», 2026. – 117 с.

2. Frank J., Schönherr L. WaveFake: A Data Set to Facilitate Audio Deepfake Detection // Proceedings of the 35th Conference on Neural Information Processing Systems (NeurIPS 2021). Track on Datasets and Benchmarks. – 2021.

3. Данильчук Т.И., Трофимов И.М. Обработка и анализ речевых фраз с использованием математических алгоритмов уровней сигналов.

4. Nautsch A., Wang X., Evans N. [et al.]. ASVspoof 2019: Spoofing Countermeasures for the Detection of Synthesized, Converted and Replayed Speech // IEEE Transactions on Biometrics, Behavior, and Identity Science. – 2021. – Vol. 3, № 1. – P. 1–14.

5. Дашинимаева В.Ц., Боршевников А.Е. Методы обнаружения голосовых сигналов

6. Лаврентьева Г.М. Детектирование атак на голосовые биометрические системы в телефонном канале

7. Злоумышленники заставили сотрудника компании совершить трансфер размером 243 тысячи долларов с помощью голоса генерального директора компании, созданного нейросетью [Электронный ресурс] // Threatpost. URL: https://threatpost.com/deep-fake-of-ceos-voice-swindles-company-out-of243k/147982/ (дата обращения: 18.12.2025).

8. Коллегам мэра Владивостока приходят голосовые сообщения от аккаунта, дублирующего настоящий аккаунт мэра [Электронный ресурс] // ZR.Media. URL: https://zr.media/news/2024-02-17/mer-vladivostoka-obratilsya-k-gorozhanam-zachem-5001803 (дата обращения: 18.12.2025).

9. Человек оказался неспособным распознать более четверти звуковых дипфейков [Электронный ресурс]//ТАСС. URL: https://tass.ru/nauka/18432869 (дата обращения: 18.12.2025).

10. IBM: глобальные финансовые потери от утечек данных достигли рекордного уровня в 4,9 млн долларов [Электронный ресурс] // IBM. URL: https://www.ibm.com/downloads/documents/us-en/107a02e94948f4ec (дата обращения: 18.12.2025).

11. BI.ZONE Brand Protection: более чем в 1,5 раза увеличилось количество фишинга в 2024 году [Электронный ресурс]. URL: https://bi.zone/news/bi-zone-brand-protection-bolee-chem-v-1-5-raza-uvelichilos-kolichestvo-fishinga-v-2024-godu/ (дата обращения: 18.12.2025).

12. С начала 2025 года обнаружено 67% дипфейков от их общего числа за прошлый год [Электронный ресурс]. URL: https://dialog.info/s-nachala-2025-goda-obnaruzheno-67-dipfejkov-ot-ih-obshhego-chisla-za-proshlyj-god/ (дата обращения 20.05.2026)

13. Объем мирового рынка инструментов для выявления дипфейков оценен в $3,86 млрд [Электронный ресурс]. URL: https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%94%D0%B8%D0%BF%D1%84%D0%B5%D0%B9%D0%BA%D0%B8_(DeepFake)?spm=a2ty_o01.29997173.0.0.237a55fbdrOcvg (дата обращения 20.05.2026)

14. Кирпичев Д.С.Сравнение методов генеративно-состязательных сетей и диффузионных моделей для восстановления аудиосигналов после потерь при сжатии

15. Вишнякова О.А., Лавров Д.Н. Применение преобразования Гильберта-Хуанга к задаче сегментации речи

16. Трубицын В.Г. Модели и алгоритмы в системах анализа речевых сигналов. Диссертация на соискание ученой степени кандидата технических наук. https://www.dissercat.com/content/modeli-i-algoritmy-v-sistemakh-analiza-rechevykh-signalov

17. Разработанную ученым НГУ модель распознавания речи научили различать эмоции [Электронный ресурс] // Новосибирский государственный университет. URL: https://www.nsu.ru/n/media/news/nauka/razrabotannuyu-professorom-ngu-model-raspoznavaniya-rechi-nauchili-razlichat-emotsii/ (дата обращения: 18.12.2025).

18. Resemble AI. Resemble Detect: AI Voice Deepfake Detection Platform. URL: https://www.resemble.ai/detect/ (дата обращения: 20.05.2026).

19. Apollo Research. Media Authenticity & AI-Generated Content Verification. URL: https://www.apolloresearch.ai/ (дата обращения: 20.05.2026).

20. MWS AI. Технологии детекции синтетического голоса для корпоративного сектора. URL: https://mws-ai.ru/ (дата обращения: 20.05.2026).

21. МТС. Пилотный проект по защите от голосового мошенничества на базе ИИ. Пресс-релиз. URL: https://company.mts.ru/pressroom/materials/3663825 (дата обращения: 20.05.2026).

22. Müller, R., & Yamagishi, J. (2022). Impact of Speech Coding on Deepfake Detection Performance. IEEE/ACM Transactions on Audio, Speech, and Language Processing, 30, 2145–2158. https://ieeexplore.ieee.org/document/9812345

23. Хлопенкова, А. Ю. Исследование алгоритмов автоматического распознавания речи на основе акустического и языкового моделирования / А. Ю. Хлопенкова, Ю. С. Белов // Научное обозрение. — 2018. — № 1. — С. 32–36.

24. Протоколы сотовой связи: GSM, CDMA

25. Иванов, А. И. Нейросетевые технологии биометрической аутентификации пользователей открытых систем : автореф. дис. ... д-ра техн. наук : 05.13.01 / А. И. Иванов ; Пенз. гос. ун-т. — Пенза, 2002. — 35 с.

26. ASVspoof 2019: Automatic Speaker Verification Spoofing and Countermeasures Challenge Evaluation Plan [Электронный ресурс] / J. Yamagishi, M. Todisco, M. Sahidullah [et al.] ; ASVspoof Consortium. — Version 0.4. — 2019. — 19 p.

27. Ишутин, И. А. Способ идентификации типов сжатых аудиофайлов по результатам спектрального анализа : выпускная квалификационная работа специалиста : 10.05.01 «Компьютерная безопасность» / И. А. Ишутин ; Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В. И. Ульянова (Ленина), Факультет компьютерных технологий и информатики, Кафедра информационной безопасности ; науч. рук. А. Д. Шульженко ; консультант О. Г. Алексеева. — Санкт-Петербург, 2026. — 70 с. .

28. ASVspoof. The Automatic Speaker Verification Spoofing and Countermeasures Challenge. URL: https://www.asvspoof.org (дата обращения: 01.06.2025).

29. Todisco M., Delgado H., Evans N., Yamagishi J. ASVspoof 2021: Automatic Speaker Verification Spoofing and Countermeasures Challenge Evaluation Plan. 2021. URL: https://www.asvspoof.org/asvspoof2021/asvspoof2021_evaluation_plan (дата обращения: 13.05.2025).

30. Долгушин М.Д., Карпов А.А. Аналитический обзор речевых и многомодальных методов распознавания когнитивных нарушений людей // Информатика и автоматизация. 2025. Т. 24. № 6. С. 1683–1720.

31. RVC Project. Retrieval-based Voice Conversion WebUI. URL: https://github.com/RVC-Project/Retrieval-based-Voice-Conversion-WebUI (дата обращения: 05.02.2026).

УДК 519.246:004.056

Метод оценки генераторов случайных чисел на основе расчета циклической автокорреляционной функции без нулевого смещения

Касьянов А. В.

ООО "Специальный Технологический центр", г. Санкт-Петербург, Россия

Аннотация: *В работе предложен метод количественной оценки случайности выходных битовых последовательностей генераторов случайных и псевдослучайных чисел на основе циклической автокорреляционной функции без учета нулевого смещения. Предлагаемый подход ориентирован на анализ конечных последовательностей длиной* 10^6 *бит, представляемых в виде кольцевой структуры. Для всех ненулевых циклических сдвигов вычисляется нормированная автокорреляционная функция, после чего определяется максимальное абсолютное отклонение от нуля. На основе этого отклонения вводится показатель качества случайности, принимающий значения, близкие к единице для последовательностей с малой внутренней корреляционной зависимостью. Для принятия решения о пригодности генератора используется калибрование доверительной области по эталонной выборке с применением бутстреп-моделирования.*

Ключевые слова: *энтропия, корреляционные зависимости, доверительная область, бутстреп-моделирование, метрический показатель.*

Введение

Оценка качества генераторов случайных и псевдослучайных чисел является одной из ключевых задач при построении криптографических систем [1]. В криптографических приложениях выходная битовая последовательность генератора должна обладать высокой степенью непредсказуемости, отсутствием выраженных периодических структур и минимальными статистическими зависимостями между элементами.

Согласно теореме Шеннона, существует предельная степень сжатия без потерь, определяемая энтропией источника [2-4]. Чем более предсказуемы данные, тем лучше они поддаются сжатию. Напротив, независимая равновероятная случайная последовательность практически не сжимается без потерь. Поэтому наличие корреляционных зависимостей в последовательности может рассматриваться как признак снижения энтропии и потенциальной предсказуемости [5].

Одним из инструментов выявления таких зависимостей является автокорреляционная функция. Она измеряет степень сходства между последовательностью и ее сдвинутой копией. Если автокорреляция при ненулевых сдвигах близка к нулю, то последовательность не демонстрирует выраженной зависимости от собственных прошлых значений. Если же автокорреляция имеет значительные пики, это может свидетельствовать о наличии периодичности, повторяющихся шаблонов или иной внутренней структуры.

В настоящей работе рассматривается метод оценки генератора по циклической автокорреляционной функции без нулевого смещения. Нулевое смещение исключается, поскольку при автокорреляционная функция отражает только энергию самой последовательности и не дает информации о ее внутренней структуре.

Циклическая автокорреляционная функция без нулевого смещения и метрический показатель

Пусть задана конечная битовая последовательность $E = \{e_0, e_1, \ldots, e_{N-1}\}$, где $e_n \in \{0,1\}$, $n = 0, \ldots, N-1$, а длина последовательности составляет бит [6].

Для анализа формируется циклическая модель последовательности. Это означает, что последовательность замыкается сама на себя и рассматривается как кольцевая структура. В такой модели сдвиг на *t* разрядов выполняется по модулю *N*, то есть индексы элементов определяются выражением $(k-t) \bmod N$. Циклический подход позволяет использовать все элементы последовательности при каждом сдвиге и исключить краевые эффекты, характерные для обычной линейной автокорреляции.

На первом этапе для битовой последовательности вычисляется выборочное среднее, которое служит оценкой математического ожидания распределения битов:

$$\mu = \frac{1}{N} \sum_{n=0}^{N-1} e_n \quad . \tag{1}$$

Затем формируется центрированная последовательность:

$$x_n = 2(e_n - \mu), \qquad n = 0, \ldots, N-1. \tag{2}$$

Нормирующая дисперсия вычисляется по формуле:

$$\sigma^2 = \frac{1}{N} \sum_{n=0}^{N-1} x_n^2 \, . \tag{3}$$

Если последовательность не является вырожденной $\sigma^2 > 0$, то можно перейти к расчету циклической автокорреляционной функции. Для каждого ненулевого циклического смещения $t_i = 1, \ldots, N-1$ вычисляется значение циклической автокорреляционной функции:

$$R_x[t_i] = \frac{1}{N\sigma^2} \sum_{k=0}^{N-1} x_{(k-t_i) \bmod N} x_k \, . \tag{4}$$

Нулевой сдвиг *t=0* сознательно исключается. При нулевом смещении последовательность сравнивается сама с собой, поэтому значение автокорреляции отражает только полную энергию сигнала и не характеризует наличие внутренней периодичности или статистической зависимости. Для статистически качественной случайной или псевдослучайной последовательности значения $R_x[t_i]$ при всех ненулевых сдвигах должны иметь малую абсолютную величину и не образовывать выраженных пиков.

После вычисления автокорреляционной функции для всех ненулевых сдвигов определяются глобальные экстремумы:

$$R_{\max} = \max_{t_i} R_x[t_i], \qquad R_{\min} = \min_{t_i} R_x[t_i]. \tag{5}$$

Далее вводится максимальное абсолютное отклонение автокорреляционной функции от нуля:

$$A(E) = \max\{|R_{\max}|, |R_{\min}|\}. \tag{6}$$

На его основе определяется метрический показатель качества случайности:

$$H^{ACF}(E) = 1 - A(E). \tag{7}$$

Калибрование области принятия решения

Для исключения произвольного задания порогового значения целесообразно использовать процедуру эмпирического калибрования на основе эталонной выборки. Такой подход является более обоснованным для проведения исследования, поскольку порог принятия решения определяется не вручную и не задаётся как фиксированная априорная константа, а выводится из структуры и вариативности эталонных данных. Это позволяет избежать привязки к конкретным численным значениям, повысить воспроизводимость процедуры оценки и обеспечить адаптацию критерия к фактическому распределению исследуемой статистики. Следовательно, пригодность генератора оценивается относительно эмпирически построенной области допустимых значений, что делает критерий принятия решения более устойчивым, объективным и статистически интерпретируемым.

Для этого используется выборка эталонных последовательностей $E_1^*, E_2^*, \ldots, E_K^*$ полученных от генераторов, считающихся допустимыми для криптографического применения. Для каждой эталонной последовательности вычисляются значения:

$$A_j^* = A(E_j^*), \qquad H_j^{ACF*} = 1 - A_j^*. \tag{8}$$

Затем применяется бутстреп-моделирование [7]. На каждой итерации $b = 1, \ldots, B$ из множества $\{A_j^*\}_{j=1}^K$ с возвращением формируется выборка объема *M*. Для этой выборки вычисляется статистика $A^b = \max_{i=1,\ldots,M} A_i^b$, а также соответствующее значение $H^b = 1 - A^b$.

Эмпирический порог определяется как процентиль бутстреп-распределения:

$$C_{ACF} = \text{quantile}_{1-\alpha/2}(A^1, \ldots, A^B), \tag{9}$$

где $\alpha = 0.01$ – уровень значимости.

Таким образом, область принятия решения для статистики A имеет вид

$$CI_A = [0, C_{ACF}], \tag{10}$$

а эквивалентная область для показателя H^{ACF}:

$$CI_H = [1 - C_{ACF}, 1]. \tag{11}$$

Протокол тестирования и решающее правило

Для проведения анализа корреляционных характеристик генератора из генеральной совокупности формируется битовая выборка длиной 10^8 бит, которая далее без перекрытия способом естественного упорядочивания разбивается на $M = 100$ последовательностей длиной бит взятых друг за другом из исходной выборки.

Для каждой последовательности, согласно формулам (6, 7), вычисляются значения:

$$A_i = \max\{|R_{\max^i}|, |R_{\min^i}|\}, \quad i = 1, ..., M \ . \tag{12}$$

Наблюдаемая статистика для всей выборки определяется как

$$A_{\text{obs}} = \max_{i=1,..,M} A_i \ , \tag{13}$$

а соответствующий показатель случайности:

$$H_{\text{obs}}^{ACF} = 1 - A_{\text{obs}} \ . \tag{14}$$

Генератор признается согласующимся с эталонной случайной моделью, если выполняется условие

$$A_{\text{obs}} \le C_{ACF} \ . \tag{15}$$

Эквивалентно это можно записать через показатель:

$$H_{\text{obs}}^{ACF} \ge 1 - C_{ACF} \ . \tag{16}$$

Если условие выполняется, то гипотеза H_0 о соответствии генератора эталонной случайной модели принимается на уровне значимости $\alpha = 0.01$, и генератор признается пригодным для использования в криптографических приложениях. Если условие не выполняется, гипотеза H_0 отвергается и делается вывод о непригодности исследуемого генератора.

Результаты

Выполнено тестирование физического генератора случайных чисел, сертифицированного регулятором, в двух режимах функционирования. В первом режиме рабочая точка на вольтамперной характеристике шумового диода была выбрана вне области лавинного пробоя, что не обеспечивало оптимальные условия работы схемы. Во втором режиме рабочая точка была установлена в области лавинного пробоя. Сопоставление результатов, полученных разработанным методом, проводилось со стандартным набором статистических тестов NIST.

Полученные экспериментальные данные позволяют заключить, что метод оценки качества Г(П)СЧ на основе расчета циклической автокорреляционной функции без нулевого смещения обладает свойством обнаружения тонких корреляционных аномалий выходного потока физического генератора, не выявляемых стандартным набором тестов NIST. И может использоваться в качестве дополнительного инструмента контроля корректности физического формирования случайности на этапах настройки, эксплуатации и периодической поверки соответствующих устройств.

Заключение

Представлен метод оценки генераторов случайных и псевдослучайных чисел на основе циклической автокорреляционной функции без учета нулевого смещения. Исключение нулевого сдвига является принципиальным, поскольку значение автокорреляции при $t=0$ характеризует энергию последовательности, но не выявляет внутренние зависимости.

Предложенный метрический показатель (7) позволяет интерпретировать качество случайности через максимальное автокорреляционное отклонение. Чем ближе данный показатель к единице, тем меньше выражены корреляционные зависимости в последовательности. Следует отметить, что данный показатель не доказывает абсолютную случайность последовательности, поскольку случайность является многопараметрическим свойством и требует проверки различными статистическими тестами. Однако он является обоснованной и информативной мерой для оценки одного из важнейших признаков случайности – отсутствия автокорреляционной зависимости. Поэтому предложенный показатель можно использовать как количественный критерий случайности по автокорреляционной функции.

Для криптографических приложений генератор признается пригодным только в том случае, если его наблюдаемая статистика автокорреляционного отклонения не превышает калиброванный порог. В противном случае наличие значимой автокорреляционной структуры указывает на недостаточный уровень случайности выходной последовательности и является основанием для отклонения генератора.

Метод может использоваться как самостоятельный инструмент анализа, так и как дополнительная проверка в составе комплексной системы статистического тестирования генераторов. Его преимуществами являются простая интерпретация результата, учет всех ненулевых циклических сдвигов и возможность построения эмпирического порога принятия решения по эталонным данным.

Список литературы

1. Касьянов А. В. Проблема анализа генераторов (псевдо-) случайных чисел // Научно-технический вестник Поволжья. 2024. № 7. С. 292-298. URL: https://www.elibrary.ru/download/elibrary_68644373_85865762.pdf

2. Shannon C. E. A Mathematical Theory of Cryptography (No. 20878). Bell Labs, New Jersey. 1945. URL: https://evervault.com/papers/shannon.pdf.

3. Shannon C. E. // A Mathematical Theory of Communication. 1948. Vol. 27. N. 3, P. 379-423, doi: 10.1002/j.1538-7305.1948.tb01338.x.

4. Shannon C. E. Communication Theory of Secrecy Systems // The Bell System Technical Journal. 1949. V. 28. N. 4. P. 656-715, doi: 10.1002/j.1538-7305.1949.tb00928.x.

5. Постников Н. А. Алгоритм синтеза таблицы соответствия корреляционной связи разрядов и энтропии 256-разрядных кодов нейросетевого преобразователя «биометрия – код» // Вестник Астраханского государственного технического университета. Серия: Управление, вычислительная техника и информатика. 2026. № 1. С. 62–71. https://doi.org/10.24143/2072-9502-2026-1-62-71.

6. 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. – EDN TSTHWP.

7. Эфрон Б. Нетрадиционные методы многомерного статистического анализа: сборник статей. – М.: Финансы и статистика. 1988. 261 с.

УДК 004.056.5

Модельный базис построения системы управления информационной безопасностью гетерогенных распределенных IT-объектов в условиях таргетированных киберугроз

Фоменко К. Э., Голицын С. А., Момонов В. М.

Военная академия защиты информации имени генерала армии С. М. Штеменко, г. Санкт-Петербург, Россия

Аннотация: *В статье предложены концептуальные подходы к построению системы консолидированного управления кибербезопасностью объектов цифровой инфраструктуры основанные на интеллектуальных механизмах выработки и принятия управляющих решений по упреждению информационно-технических воздействий.*

Ключевые слова: *интеллектуальная система, процедуры принятия решения, система управления информационной безопасностью, информационная инфраструктура.*

Введение

Интенсивное развитие и использование современных информационно-коммуникационных технологий для обработки цифровой информации привели к серьезным качественным изменениям в экономической, социально-политической и духовной сферах жизни общества. Однако масштабное применение средств автоматизации, имеющих ряд уязвимостей к радиоэлектронным и программно-аппаратным воздействиям, невозможно без обращения особого внимания на проблемы их безопасности.

Проведенный анализ специфики построения объектов цифровой инфраструктуры, показывает, что элементы гетерогенны, решают задачи различной значимости и построенные на программно-аппаратных платформах, преимущественно иностранного производства. Наряду с этим наблюдается неуклонный рост количества уязвимостей аппаратно-программных платформ, используемых в цифровой инфраструктуре и способов их эксплуатации (по обобщенным данным анализа баз данных уязвимостей только за 3 квартала 2025 года прирост составил порядка 12-15% [6]).

Другим, не менее тревожным аспектом, с началом специальной военной операции, является лавинообразный роста инцидентов информационной безопасности как в государственном, так и в коммерческом сегментах информационной инфраструктуры. При этом атаки носят комбинированный многовекторный характер, отличающийся сложностью исполнения и локализации конечной цели воздействий [4, 6].

Вместе с тем подходы борьбы с кибератаками не стоят на месте. Эволюция технологий и средств обеспечения информационной безопасности представлены на Рисунке 1.

Рис. 1. Технологии и средства обеспечения кибербезопасности

Основой при проектировании новейших систем информационной безопасности (далее ИБ) является переход от строительства «стен» к парадигме «киберустойчивости» информационной инфраструктуры, которая достигается проактивными риск-ориентированными подходами [4].

На практике одним из значимых прорывов ригидной системы ИБ, которая строилась на основе нормативно-гарантированных решений начала 90-х, явилось широкое внедрение центров комплексной кибербезопасности (SOC – Security Operation Centre). Логическим продолжением стало внедрение ведомственных

и корпоративных центров государственной системы обнаружения, предупреждения и ликвидации компьютерных атак на информационные ресурсы.

Однако необходимо отметить, что применение передовых практик на стадии внедрения вызывает множество сложностей, связанных с нормативными, техническими, финансовыми и кадровыми вопросами, в следствие чего отказаться

от системы ИБ, которая строилась более 30 лет не представляется возможным.

Из вышеизложенного очевиден вывод, что в настоящее время актуален поиск решения, сочетающего в себе бесшовное внедрение новейших техник

с использованием уже существующего научно-технического задела в области информационной безопасности [3]. Вследствие этого возникает задача разработки научно-методического аппарата построения системы комплексного управления информационной безопасностью, которая способна обеспечить:

консолидированное управление средствами ИБ территориально распределенных объектов информационной инфраструктуры, при решении

задач противодействия информационно-техническим воздействиям (далее ИТВ);

упреждающее поведение, основанное на принят решения в отношении возможных инцидентов ИБ до их проявления, за счет постоянного интеллектуального анализа всех консолидированных процессов, протекающих

в инфраструктуре;

обеспечение заданных системных свойств защищаемой информационной инфраструктуры;

непрерывное и продуктивное взаимодействие с разнородными внешними источниками данных о событиях ИБ, а также тесное взаимодействие с Государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.

Концептуальные подходы к построению системы консолидированного управления кибербезопасностью:

Решение поставленной задач управления информационной безопасностью в условиях разнородности информационной, структурной и эвристической составляющих объектов цифровой инфраструктуры и неполной определенности ее будущих состояний в результате потенциальных ИТВ, накладывают ограничения разрешимые путем применения «умных» моделей и методов способных формировать различные ответные реакции на одни и те же атакующие воздействия, зависящие от того, в каких условиях и каким образом атакующие воздействия осуществляются, т.е. – в зависимости от контекста.

Соответственно возникает необходимость использования существующего технологического базиса, основанного на ряде интеллектуальных технологий:

- извлечения знаний из различных источников;
- прогнозирования и поддержки принятия решений в реальном масштабе
- времени;
- планирования и управления целенаправленным поведением сетевых
- элементов в слабоструктурированных средах;
- когнитивного анализа данных;
- мультиагетного управления и диспетчеризации ресурсов [2].

На основании этого была разработана логическая структура выработки и принятия решений при консолидированном управлении ИБ распределенных объектов цифровой инфраструктуры, представленная на рисунке 2.

Рис. 2. Логическая структура выработки и принятия решений при консолидированном управлении ИБ распределенных объектов цифровой инфраструктуры

Разработанная логическая структура отражает процесс выработки и принятия решений при управлении доступными средствами информационной безопасности, при участии специалистов различных уровней вовлеченности в решение задач защиты информации.

Принцип модельности на представленной структуре трактуется как множество моделей для каждого из этапов и фаз принятия решений, обеспечивающее консолидированное управление средствами ИБ территориально распределенных объектов информационной инфраструктуры. Существенным при этом является требование возможности построения на каждой модели либо на любой из их совокупности вычислительного процесса, позволяющего в свою очередь реализовать механизмы упреждения.

Принцип наблюдаемости характеризуется введением процесса трассировки, позволяющего как наблюдать логику машинных рассуждений (что важно при расследовании инцидентов информационной безопасности), так и вмешиваться в процесс принятия решения при наличии соответствующей квалификации специалиста по ИБ, а также контролировать качество функционирования защищаемой информационной инфраструктуры.

В соответствии с теорией иерархических многоуровневых систем, любая многоуровневая структура предполагает разукрупнение в зависимости от степени топологической неоднородности на сегменты управления.

Представим систему комплексного управления информационной безопасностью (далее СКУИБ) в виде территориально-распределенных агентов ИБ (Рисунок 3).

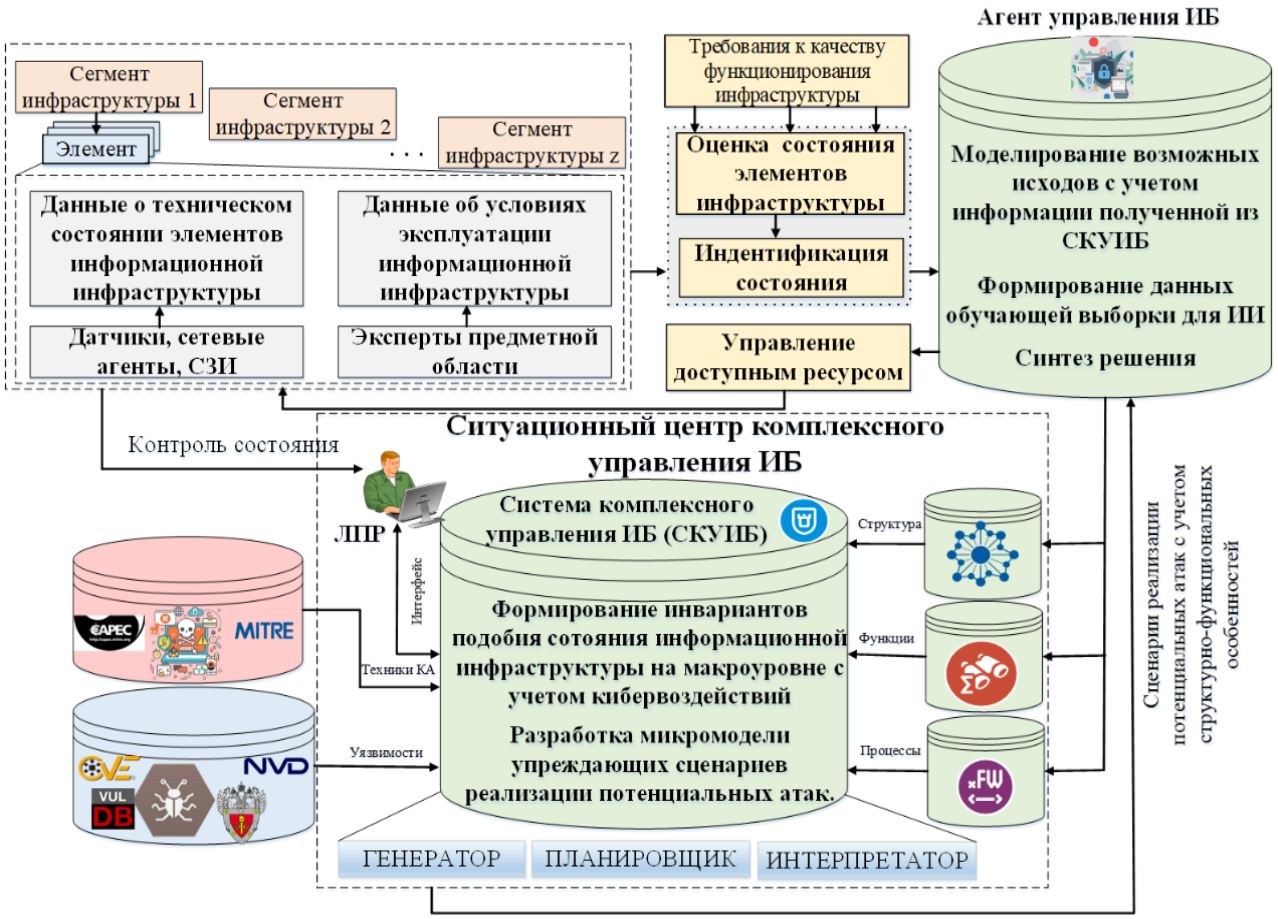


Рис. 3. Предложения по облику системы комплексного управления информационной безопасностью

Такое видение СКУИБ позволяет уйти от строгой централизации управления, предоставляя возможность интеллектуального анализа сложных-составных кибервоздействий (APT-атак) на региональных уровнях (обладающих более высокими вычислительными мощностями) с возможностью тонкой подстройки на уровне сегментов инфраструктуры, путем выработки сценариев упреждающего поведения.

Вместе с тем, в силу неполноты информации о важности выполняемых информационных процессов на более высоких уровнях иерархии, задержек, изменений текущего состояния транспортной сети и огромного потока управляющей информации видеться актуальным наделить агенты СКУИБ возможностью самостоятельно синтезировать решения по выработке контрмер ИТВ, которые будут учитывать как данные аномального функционирования сегмента инфраструктуры в реальном масштабе времени, так и рекомендации по упреждению возможных кибератак (резервирование, автоматическое распределение, реконфигурация, репликация данных, балансировка нагрузки) [3].

Рассматриваемая область применения СКУИБ характеризуется наличием большого количества алгоритмов, целевое объединение которых в вычислительные и диалоговые модели позволяет находить решения. Вместе с тем для этой области характерны и описания процессов поиска решений,

представленных в виде некоторых множеств утверждений, основой, при реализации которых, является интеллектуальная информационно-техническая система.

Система может называться интеллектуальной, если она непрерывно делает предсказания окружающего мира, сравнивает эти предсказания с показаниями сенсоров и изменяет свои параметры для получения новых, более точных предсказаний [4]. Основой любой интеллектуальной системы является Решатель.

В данном случае он должен вырабатывать сценарии упреждающего поведения исходя из аномалий выявленных в разнородных слабо формализованных входных данных о структурно-функциональном взаимодействии элементов информационной системы и знаний о уязвимостях и потенциальных ИТВ.

Одним из перспективах направлений пригодным для решения данной задачи является подход разработанный Д.Хокинсом [5], который моделирует некоторые структурные и алгоритмические свойства неокортекса в части предсказания возможных исходов, что видится возможным использовать при формировании упреждающего поведения системы противодействия ИТВ. Основным элементом системы, предложенный автором является кортикальная колонка, модель которой описана в более ранних работах как темпоральная временная память (Hierarchical Temporal Memory, далее HTM).

В основе работы заложена идея использования совокупности организованных в кортикальные колонки нейронов, которые взаимодействуют путем сенсорного восприятия данных в единой интеллектуальной системе накопления, обработки и порождения ответных реакций. Причем важным замечанием, является то, что кортикальная колонка способна распознавать входные данные, несколько отличающиеся друг от друга, что может быть полезно для организации работы со слабоструктурированными данными в условиях шума и пропусков, а так же, возможно, для реализации прогностической модели, распределённой системы, формирующих пространство решений противодействия деструктивных воздействий [1].

Однако тактики и техники проведения деструктивных воздействий могут быть реализованы с помощью различных, иногда уникальных, инструментов, что делает прогноз весьма не точным в отсутствии обучающей выборки, исходя их этого с точки зрения применения рассмотренной технологии к теории безопасности компьютерных систем предлагается надстроить более высокий уровень в иерархии кортикальных колонок, содержащий данные о событиях и их последовательностях, т.е. о процессах используя онтологию предметной области с ролевыми концептами: объект – свойство – действие [1] (Рисунок № 4).

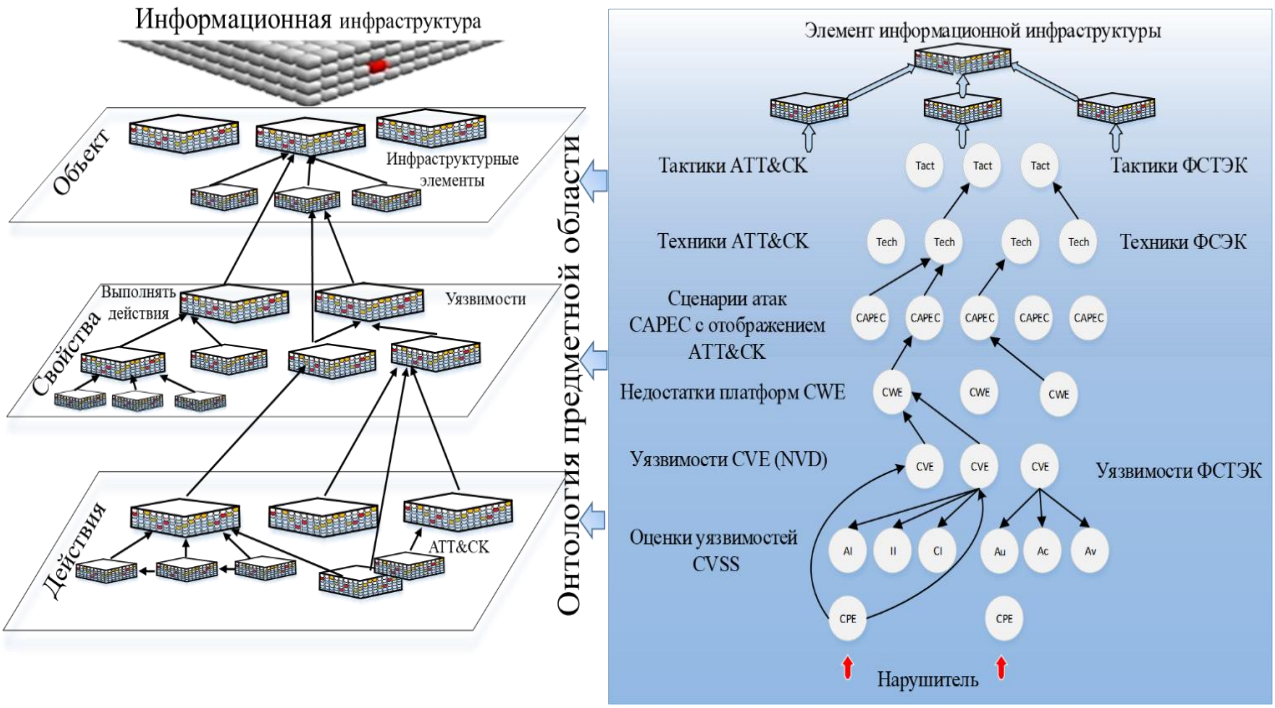


Рис. 4. Механизм онтологического взаимодействия кортикальных регионов при прогнозировании деструктивных возмущений

Данное представление дает возможность применять методы логического вывода (дедукцию, абдукцию, индукцию) с использованием кортикальных колонок в качестве элементов, осуществляющих рефлексию системы, которая выбираться как на основе предыдущего опыта, так и на основе анализа возможных реакций.

В качестве примера таких данных могут выступать обучающие данные о шаблонах потенциальных ИТВ, характеризующие различные аспекты безопасности программно-аппаратных платформ информационной инфраструктуры, консолидированы в виде слабосвязанных групп иерархических гипертекстовых документов в отдельных базах данных.

В рамках практической части исследований проведен эксперимент по обучению кортикального региона памяти с использованием обучающей выборки.

Результаты показывают достаточно высокие показатели работы кортикального планировщика по сопоставлению контекстных метрик угроз и уязвимостей, которые позволяют сделать вывод о пригодности предложенного подхода для выработки сценариев упреждающего поведения СКУИБ.

CWE ID	Название	CVE из NVD	CVE из BDU	CAPEC	ATT&CK Technic	ATT&CK Tactics
CWE-798	Использование заданных учетных данных	CVE-2019-6859, CVE-2019-6812, CVE-2016-4520,	BDU:2020 -01893, BDU:2020 -02580	CAPEC-191: Read Sensitive CAPEC-70	T 1552.001 T 1078.001	TA0006 Credential Access (Учетный доступ)
CWE-287	ImproperAuthentication (Неправильная аутентификация) ...	CVE-2019-6832, CVE-2017-7420	BDU:2019 -03754	CAPEC-114, CAPEC-115, CAPEC-22	T1185 T1550.001 T1134.001	TA0009 Collection (Сбор) TA0005 Defense Evasion ....

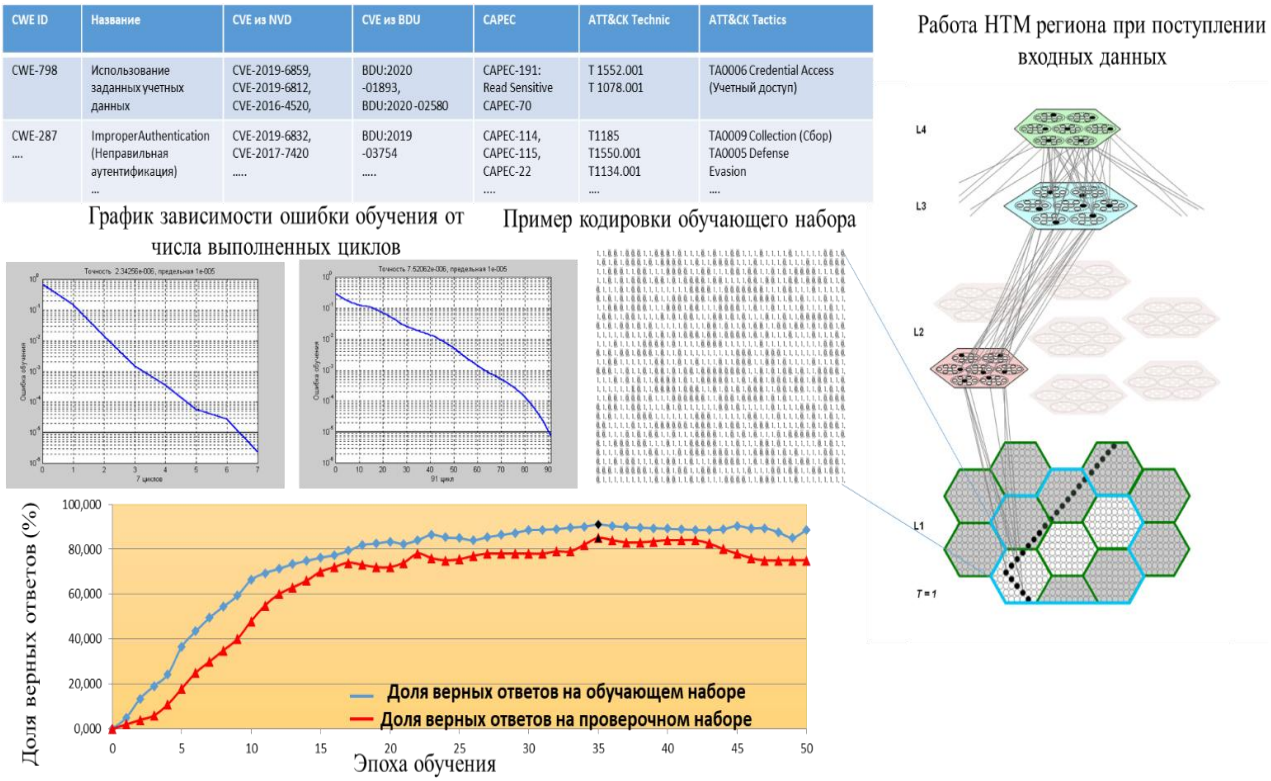


Рис. 5. Результаты обучения кортикального (НТМ) региона

Выводы

Результаты, представленные в статье, позволяют сформировать модельный базис необходимый для разработки системы комплексного управления информационной безопасностью современных объектов цифровой инфраструктуры, при этом предлагается в основу разрабатываемой системы заложить идею интеллектуальной обработки слабоструктурированных данных, позволяющую реализовать упреждение деструктивных воздействий.

Основные положения работы обсуждены на 1-м Каспийском форуме информационной безопасности «Инфофорум-Астрахань» [7].

Список литературы

1. Бирюков Д. Н. Ассоциативно-рефлекторная память киберсистемы для синтеза упреждающих реакций, нейтрализующих вредоносные воздействия/Д. Н. Бирюков // СПИИРАН. – 2015. – №41. – С.131-148.

2. Будко Н. П. Общие принципы функционирования и требования к построению структур перспективных систем мониторинга распределенных информационно-телекоммуникационных сетей / Н.П. Будко // Техника средств связи. – 2021. – №2 (154). – С. 38-60.

3. Голицын С.А., Шульженко А.Д. Концептуальный подход к построению центра мониторинга системы обнаружения, предупреждения и ликвидации последствий компьютерных атак // Globus: Технические науки. 2021. Т. 7. № 1 (37). 40-43 с.

4. Киберустойчивость цифровой экономики. Как обеспечить безопасность и непрерывность бизнеса / С. А. Петренко // СПб: «Питер», 2021. – 384 с.

5. 1000 мозгов. Новая теория интеллекта / Джефф Хокинс [пер. с англ. С.Черникова]. – СПб.: Портал, 2024. – 368 с.

6. Ростелеком Солар. Отчеты компании [Электронный ресурс]. – URL: https://rt-solar.ru/analytics/reports/ (дата обращения: 01.10.2025).

7. Фоменко К.Э. Актуальность задачи построения систем комплексного управления информационной безопасностью современных гетерогенных территориально распределенных объектов цифровой инфраструктуры: [презентация] – Текст. Изображение: электронные // Инфофорум – URL: https://rutube.ru/video/3b9679ecb1add9d01e30b22e08d72b7f/ (дата обращения 15.10.2024).

УДК 004.056.5

Определение оптимальной комбинации шумовой и речеподобной помехи для снижения эффективности автоматического распознавания речи

Рамзаев В. А., Фесько Н. В., Шульженко А. Д.

Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» имени В. И. Ульянова (Ленина), г. Санкт-Петербург, Россия

Аннотация: *В работе проведено экспериментальное исследование эффективности различных комбинаций шумовых и речеподобных помех, предназначенных для затруднения автоматического распознавания полезного речевого сигнала. Рассмотрено влияние белого, розового и красного шумов, а также различных вариантов псевдоречи при изменении отношения сигнал/шум от 20 до 0 dB. Выполнен сравнительный анализ двадцати акустических конфигураций и определены наиболее эффективные сочетания компонентов помехи. Установлено, что максимальное снижение точности автоматического распознавания достигается при совместном использовании широкополосного шума и разнополой речеподобной интерференции.*

Ключевые слова: *акустическая защита информации, автоматическое распознавание речи, речеподобная помеха, псевдоречь, белый шум, розовый шум, отношение сигнал/шум, акустическое маскирование, нейросетевые системы распознавания речи, комбинированная акустическая помеха.*

Введение

Одной из основных задач акустической защиты речевой информации является создание помех, способных максимально затруднить выделение и автоматическое распознавание полезного речевого сигнала. Современные системы автоматического распознавания речи сохраняют высокую точность даже при наличии значительных фоновых шумов, что требует применения более эффективных способов акустического маскирования.

Эффективность помехи определяется не только ее уровнем, но и спектральным составом, а также наличием речеподобных компонентов. Шумовая составляющая затрудняет выделение акустических признаков полезного сигнала, тогда как псевдоречь создает дополнительную речевую интерференцию, увеличивая вероятность ошибочного выделения признаков и декодирования фоновых речевых фрагментов вместо целевого сообщения. Совместное использование нескольких типов помех позволяет существенно повысить эффективность акустического маскирования по сравнению с применением отдельных компонентов.

Целью работы является определение оптимальной комбинации шумовой и речеподобной помехи, обеспечивающей максимальное снижение качества автоматического распознавания полезного речевого сигнала. Для достижения поставленной цели проведено экспериментальное исследование различных комбинаций шумов, речеподобных сигналов и уровней отношения сигнал/шум с последующим сравнительным анализом эффективности каждого варианта.

Экспериментальные исследования

Для определения наиболее эффективной комбинации акустических помех была проведена серия экспериментов, направленных на оценку влияния типа шумовой помехи, состава речеподобной составляющей и отношения сигнал/шум на качество автоматического распознавания речи.

В качестве шумовой составляющей использовались белый, розовый и красный шумы, отличающиеся спектральным распределением энергии. Речеподобная составляющая формировалась с использованием синтезированных мужских и женских голосов в различных комбинациях: один мужской голос, два мужских голоса, мужской и женский голоса одновременно, а также комбинации из четырех одновременно воспроизводимых голосов. Кроме того, исследовались варианты использования только шумовой или только речеподобной помехи.

Эффективность каждой комбинации оценивалась при различных значениях отношения сигнал/шум в диапазоне от 20 до 0 dB. Основным критерием эффективности являлась точность автоматического распознавания полезного речевого сигнала, определяемая как доля корректно распознанных слов после обработки аудиозаписи системой распознавания речи.

Полученные результаты показали, что эффективность подавления определяется не только уровнем шумовой помехи, но и ее спектральным составом. Красный шум практически не оказывает влияния на качество распознавания даже при уменьшении отношения сигнал/шум, тогда как белый и розовый шумы значительно эффективнее затрудняют выделение полезного сигнала. Это объясняется более равномерным распределением энергии по речевому диапазону частот, вследствие чего происходит маскирование наиболее информативных спектральных компонентов речи.

Дополнительное введение речеподобной составляющей позволило существенно повысить эффективность акустического маскирования. В отличие от обычного шума псевдоречь формирует конкурирующие речевые признаки, что приводит к ошибочному выделению нейросетевыми алгоритмами фоновых речевых фрагментов вместо полезного сигнала. Наиболее выраженный эффект наблюдался при использовании одновременно мужских и женских голосов, создающих более сложную акустическую картину по сравнению с однотипными речевыми источниками.

Результаты исследования для всех протестированных комбинаций представлены в таблице 1.

Таблица 1 – Зависимость точности автоматического распознавания речи от типа акустической помехи и отношения сигнал/шум.

Акустическая конфигурация	20 dB	10 dB	5 dB	0 dB
Мужской+ Женский + Белый	87.4%	65.7%	37.6%	2.0%
Мужской + Белый	88.9%	63.8%	35.1%	2.8%
Мужской + Женский + Розовый	86.5%	63.3%	38.7%	4.2%
Мужской + Розовый	86.0%	67.9%	38.2%	4.6%

Акустическая конфигурация	20 dB	10 dB	5 dB	0 dB
2 Мужской + Белый	88.8%	65.4%	38.8%	4.9%
Мужской + Женский + Красный	90.6%	78.7%	46.2%	5.0%
Мужской + Женский	90.7%	77.6%	43.0%	5.8%
2 Мужской +2 Женский + Белый	86.0%	68.4%	42.2%	7.4%
2 Мужской + Розовый	87.8%	67.6%	41.7%	8.1%
2 Мужской +2 Женский + Розовый	86.9%	68.3%	43.9%	8.4%
2 Мужской +2 Женский	90.6%	76.0%	54.6%	13.1%
2 Мужской +2 Женский + Красный	91.0%	76.3%	51.8%	14.0%
Мужской + Красный	91.4%	82.3%	66.8%	19.8%
Мужской	92.0%	82.9%	67.0%	20.5%
2 Мужской + Красный	92.2%	86.6%	64.9%	21.5%
2 Мужской	92.0%	86.8%	64.8%	23.6%
Розовый шум	89.4%	80.5%	70.5%	52.4%
Белый шум	89.8%	83.0%	73.2%	61.3%
Красный шум	91.4%	91.7%	92.7%	92.3%
Эталон	92.6%	-	-	-

Анализ экспериментальных данных показывает, что снижение отношения сигнал/шум сопровождается нелинейным уменьшением качества распознавания. При значениях SNR 20 dB большинство исследованных комбинаций сохраняют высокую точность распознавания, превышающую 85 %. При уменьшении отношения сигнал/шум до 10 dB начинается интенсивное снижение качества распознавания, а при SNR 5 dB для комбинированных помех точность большинства моделей становится менее 40 %. При дальнейшем уменьшении отношения сигнал/шум до 0 dB достигается практически полное разрушение возможности автоматического распознавания полезного сигнала.

Наиболее высокую эффективность продемонстрировали комбинированные помехи, включающие широкополосный шум совместно с речеподобной составляющей. Минимальная точность распознавания была получена при использовании комбинации Мужской+ Женский + Белый, для которой точность распознавания при SNR = 0 dB составила 2,0 %. Близкие результаты показали комбинации с использованием Мужской + Белый. При этом применение только шумовой или только речеподобной помехи оказалось существенно менее эффективным.

Для определения области практического применения комбинированных помех был выполнен анализ зависимости качества распознавания от отношения сигнал/шум.

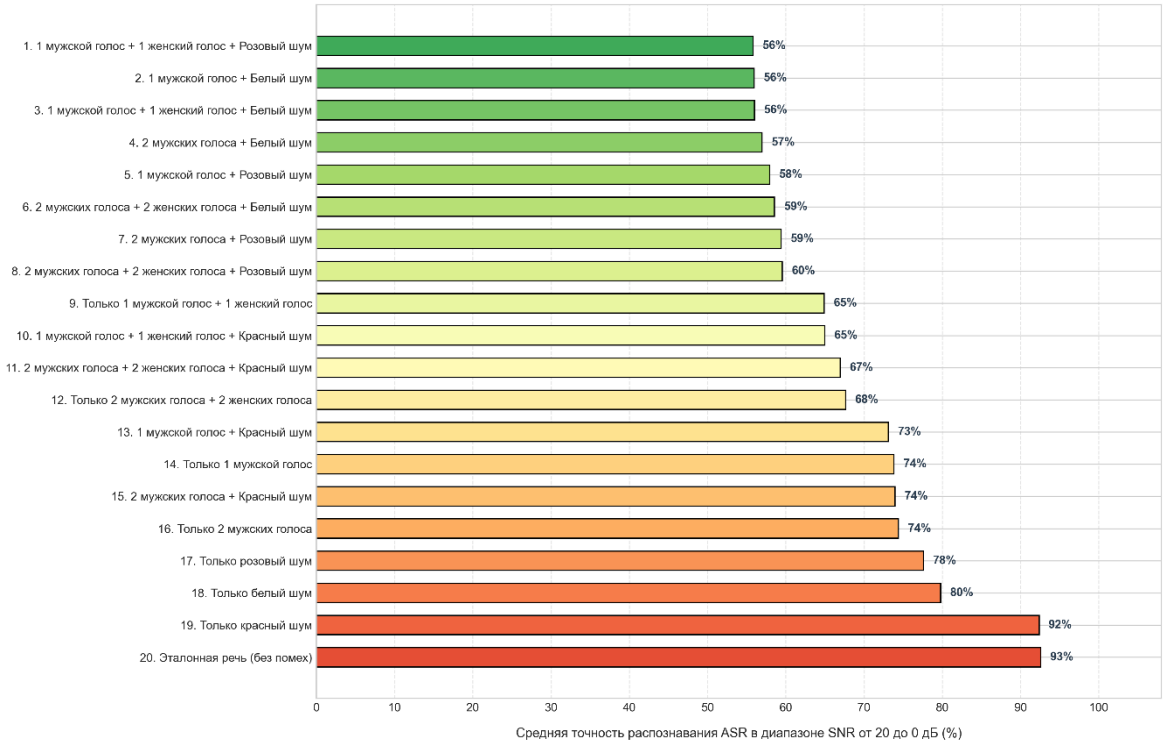


Рис. 1. Зависимость точности распознавания от отношения сигнал/шум для различных комбинаций акустических помех

Полученные результаты позволили установить, что наиболее интенсивное снижение качества распознавания наблюдается при уменьшении отношения сигнал/шум ниже 10 dB. В диапазоне 6–9 dB происходит резкое падение точности распознавания, которое можно рассматривать как порог перехода систем автоматического распознавания речи в режим устойчивой деградации. При дальнейшем уменьшении отношения сигнал/шум до значений менее 5 dB комбинированные помехи обеспечивают практически полную потерю возможности корректного распознавания полезного речевого сигнала.

Дополнительный сравнительный анализ белого и розового шумов показал, что их эффективность зависит от уровня отношения сигнал/шум. При значениях SNR от 0 до 10 dB более выраженный эффект обеспечивает белый шум, тогда как при SNR выше 10 dB незначительное преимущество демонстрирует розовый шум. Однако различие между ними не превышает 1–2 %, что позволяет считать оба типа шумовой помехи эффективными средствами акустического маскирования при использовании совместно с речеподобной составляющей.

Заключение

В работе проведено экспериментальное исследование эффективности различных комбинаций шумовых и речеподобных помех при различных значениях отношения сигнал/шум. Выполнено сравнение широкополосных (белого и розового) и низкочастотного (красного) шумов, а также различных

вариантов речеподобной интерференции, включающей мужские и женские синтезированные голоса.

Результаты экспериментов показали, что наибольшая эффективность достигается при совместном использовании широкополосного шума и речеподобной составляющей. Применение только шумовой или только речеподобной помехи обеспечивает значительно меньший уровень подавления по сравнению с их комбинированным использованием. Наиболее эффективной конфигурацией оказалась комбинация одного мужского и одного женского голоса совместно с белым шумом, обеспечившая снижение точности автоматического распознавания до 2,0 % при отношении сигнал/шум 0 dB.

Установлено, что наиболее интенсивное снижение качества распознавания наблюдается при уменьшении отношения сигнал/шум ниже 10 dB, а в диапазоне 6–9 dB происходит резкий переход к устойчивой деградации работы систем автоматического распознавания речи. При значениях SNR ≤ 5 dB комбинированные помехи обеспечивают практически полную потерю возможности корректного распознавания полезного речевого сигнала.

Дополнительный анализ показал, что при низких значениях отношения сигнал/шум более высокой эффективностью обладает белый шум, тогда как при высоких значениях SNR незначительное преимущество демонстрирует розовый шум. Красный шум оказался наименее эффективным видом шумовой помехи и не обеспечивает существенного ухудшения качества автоматического распознавания даже при снижении отношения сигнал/шум.

Полученные результаты позволяют рекомендовать использование комбинированной помехи, включающей широкополосный шум и разнополую речеподобную интерференцию, в качестве наиболее эффективного способа затруднения автоматического распознавания полезного речевого сигнала современными нейросетевыми системами. Это может быть использовано при разработке перспективных средств акустической защиты речевой информации.

Список литературы

1. Ахметшин А. Ф. Применение нейросетевых технологий для анализа речевой информации // CyberLeninka. – 2020. – URL: https://cyberleninka.ru/article/n/primenenie-neyrosetevyh-tehnologiy-dlya-analiza-rechevoy-informatsii/viewer (дата обращения: 13.05.2026).

Секция 5 – Подготовка кадров для IT-отрасли

УДК 62-519; 629.127; 654.1;656.6; 334.02.

Особенности применения искусственного интеллекта в системе инженерного образования

Комашинский В. И., Бирюков А.В.

ЗАО «Институт Телекоммуникаций», г. Санкт-Петербург, Россия

Аннотация: *в настоящее время мир переживает начало новой, четвертой индустриальной революции (Industrie 4.0), основной движущей силой которой являются люди, владеющие самыми современными телекоммуникационными, информационными и интеллектуальными технологиями. Иными словами, подготовка кадров, способных осваивать, применять и развивать новейшие технологии, является ключом к успешному развитию науки, промышленности и экономики страны. Данная статья посвящена особенностям формирования новой педагогической парадигмы 4.0, основанной на широком применении интеллектуальной аналитики педагогических и учебных данных, а также внедрению прорывных технологий ИИ.*

Ключевые слова: *Педагогическая парадигма 4.0, искусственный интеллект (ИИ), интеллектуализация, интеллектуальная аналитика данных, генеративный ИИ, цифровые двойники, адаптивное обучение.*

Введение

Анализ особенностей протекания предшествующих индустриальных революций [1], их движущих сил и вызванных ими последствий позволяет более осмысленно подойти к организации и управлению процессами дальнейшего научно-технического и технологического развития России в период наступающей новой, четвертой индустриальной эпохи.

− **Первая индустриальная революция (рис.1)** началась с развития теплофизики и механики, совершенствования образовательных учреждений, изобретения паровых двигателей, механизации производства и создания транспорта на паровой тяге (пароходов, паровозов и железных дорог).

− **Второй индустриальной революции** дали старт научные достижения в области электричества и магнетизма, соответствующая модернизация учебных программ и лабораторий, разработки технологий электропривода и электрической и радиосвязи. Всё это привело к появлению электрического промышленного оборудования, конвейерного производства, электротранспорта и широкого перечня электрифицированных бытовых изделий.

− **Третья индустриальная революция** началась с научных достижений в электронике, физики полупроводников, кибернетики и вычислительной техники. Широкое освоение новых достижений и технологий потребовало не только проведения глубокой модернизации учебных программ и лабораторий, но и внедрения компьютерных технологий в процессы обучения. Степень успешности компьютеризации науки и образовательной сферы оказала существенное влияние на темпы автоматизации производственных процессов,

выпуск высокотехнологичных компьютеризированных бытовых и промышленных изделий, автоматизированных транспортных систем – наземных, воздушных, морских и космических.

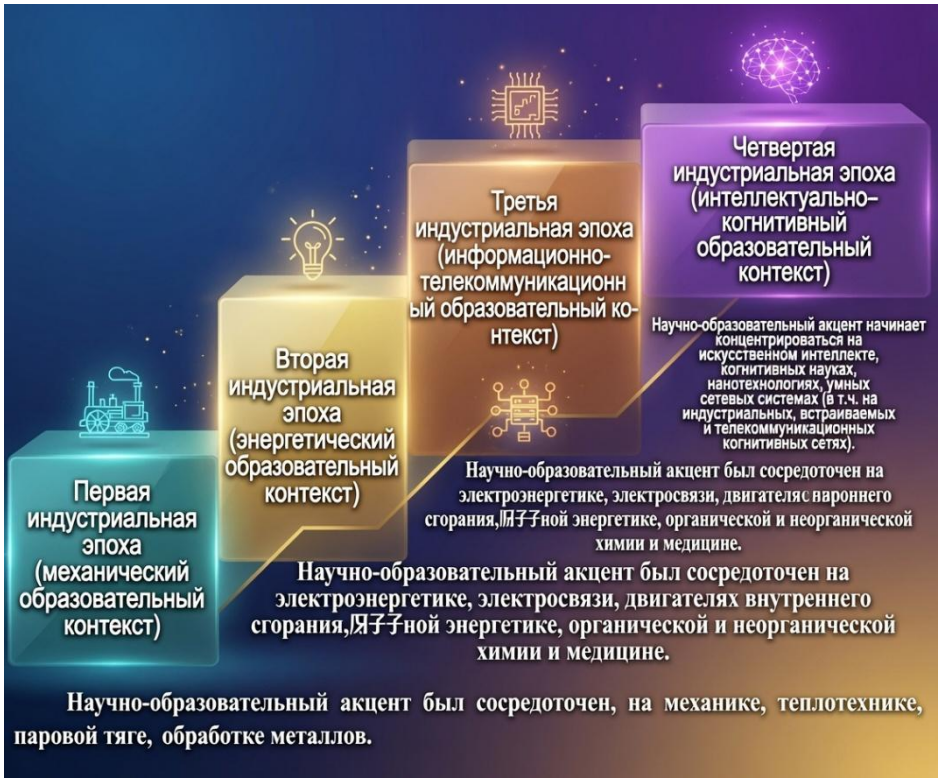


Рис. 1. Индустриальные революции и их особенности

Несколько лет назад стартовала **4-я индустриальная революция** (рис.1), её двигателями стали новейшие научные достижения в области нейронауки, нечеткой логики, машинного обучения и искусственного интеллекта. В результате начались процессы интеллектуализации всех сфер жизни и деятельности современного общества. Это требует проведения существенных и фундаментальных изменений в образовательной сфере, включая не просто модернизацию учебных программ (например, введение таких учебных дисциплин, как нечеткие исчисления, нейроматематика, математические основы ИИ и др.), но и кардинального пересмотра самой методологии преподавания.

Изменения, которые происходили в индустрии на протяжении первых 3-х индустриальных революций и которые происходят сейчас в начале 4-й, протекали в виде инновационных циклов, которые брали своё начало в сфере науки в виде новых научно-технических достижений, которые затем переходили в область ориентированного на инновации образования, и только потом опережающе подготовленные инженерно-технические кадры воплощали новые знания в новой индустрии [2]. Другого пути индустриального и экономического развития, видимо, нет и быть не может.

Образовательный контекст четвертой индустриальной эпохи

Ретроспективно-перспективный анализ индустриальных преобразований [3-6] за последние 200 лет показывает, что каждая индустриальная эпоха порождала свои педагогические акценты и парадигмы (рис.3). Наука и образование неразделимы; наука фактически вырастает из образования, и новые научные открытия появляются в тот момент, когда интерес к знаниям превышает возможности существующих учебников и учебных заведений. Интеграционные процессы науки и образования по мере развития общества усиливаются, что является одним из важнейших факторов технологического развития. Более того, существует и обратная связь между наукой, образованием и индустриальным развитием, которая проявляется в совершенствовании образовательной материально-технической базы и основанных на ней образовательных технологий (рис.2).

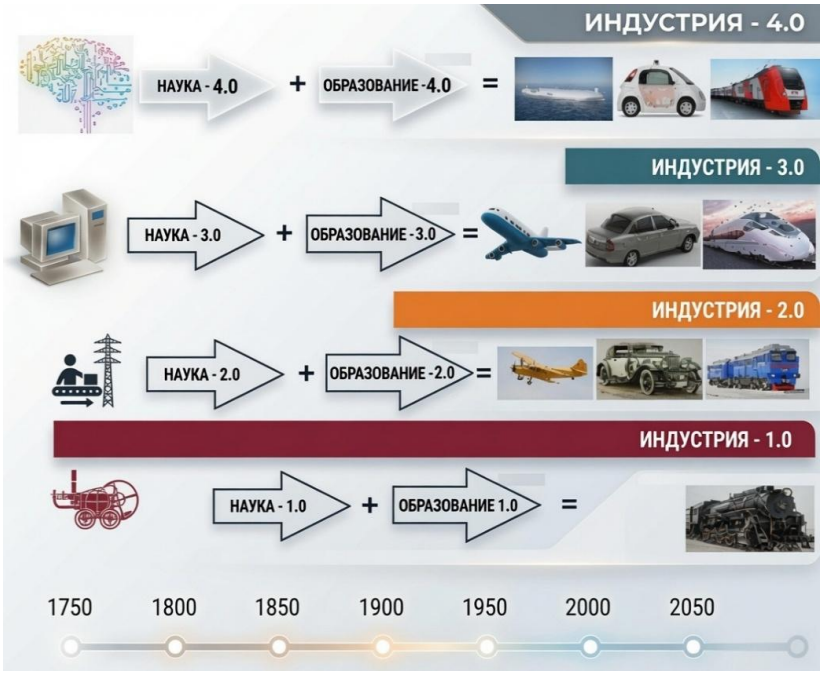


Рис. 2. Коэволюция науки, образования и технологий

Педагогическая парадигма 4.0

Суть педагогической парадигмы 4.0 заключается в объединении обучаемых, преподавателей и искусственного интеллекта в единую экосистему. Архитектуру педагогической парадигмы 4.0 можно представить в виде пятиуровневой пирамиды (рис.3). Первый уровень включает педагогические и учебные данные (рис.3), которые на втором уровне преобразуются в педагогическую и учебную информацию, используемую на третьем уровне в процессе обучения учеников (с преподавателем, с применением искусственного интеллекта или в процессе совместной работы преподавателя и ИИ). В результате реализации процесса обучения ученики приобретают новые знания (четвертый уровень), которые являются основой для принятия

эффективных практических решений и оптимального их воплощения (пятый уровень).

Рис. 3. Пятиуровневая архитектура педагогической парадигмы 4.0

Педагогические данные формируются на основе сбора персональных данных учеников, их дополнительного тестирования и различных других источников. Собранные материалы используются для их изучения методами интеллектуальной аналитики в интересах получения психофизических характеристик каждого обучаемого, контекстных образовательным программам. Педагогические данные необходимы для формирования педагогических знаний о способностях каждого ученика к освоению учебных материалов и формирования на основе этого соответствующих **гипер-персонализированных траекторий обучения**.

Учебные данные (учебные материалы) используются для формирования последовательности блоков учебной информации, которая будет применяться в процессе обучения учеников (рис.3) преподавателями, ИИ или ими совместно. Несмотря на кажущуюся статичность, педагогическая пирамида будет развиваться по мере того, как будут появляться новые идеи ИИ, ориентированные на преподавание и учеников. Более того, в процессе развития педагогической парадигмы 4.0 будет происходить взаимное обогащение классической педагогики (педагогики людей) и автономной педагогики (педагогики машин). Важным элементом этой модели является **замкнутый цикл обратной связи**, где алгоритмы ИИ постоянно обучаются на результатах обучения студентов, совершенствуя свои стратегии.

Особенности применения в образовании технологий искусственного интеллекта

Искусственный интеллект и машинное обучение уже сегодня оказывают существенное влияние на педагогический процесс. Применение ИИ и машинного обучения ведет к существенным изменениям общепринятой педагогической методологии (Рис.4). Искусственный интеллект является

эффективным инструментом обучения благодаря его способности адаптироваться и предлагать индивидуальные учебные программы. Инструменты, основанные на использовании машинного обучения, помогают оценить текущий уровень понимания человека, выявить пробелы в знаниях учащихся и подводить к решениям в режиме реального времени. Технологии ИИ также могут выявлять области, в которых численность и подготовка учеников не соответствует возможностям преподавателей, и создавать такие программы обучения, которые позволяют оптимизировать соотношение преподавателей и учащихся.

Рис. 4. Применения в образовании технологий искусственного интеллекта

К новым возможностям, которые открывают применение в образовательной сфере ИИ и машинное обучение, могут быть отнесены следующие:

1. **Прогнозирование успеваемости учащихся и адаптивное обучение:** Основным преимуществом машинного обучения является его способность прогнозировать успеваемость учащихся. «Изучая» каждого ученика, технология может выявить слабые места и предложить эффективные инструменты обучения для каждого ученика, такие как дополнительные учебные материалы, математические задачи или лабораторные работы. Современные системы **адаптивного обучения** на базе ИИ меняют контент и темп обучения в реальном времени, подстраиваясь под когнитивные и психофизические особенности студента, которые могут отслеживаться с помощью интегрированных носимых устройств.

2. **Внедрение Генеративного ИИ (Generative AI) в качестве тьютора:** Большие языковые модели (LLM) перестали быть просто чат-ботами и выступают в роли интеллектуального тьютора, способного объяснять сложные концепции на примерах, понятных конкретному студенту, генерировать вариативные задачи для практики, проверять код или эссе, давать развернутую

обратную связь и выступать партнером по мозговому штурму для генерации идей инженерных проектов.

3. **Справедливое и многоаспектное оценивание учащихся:** Машинное обучение может справедливо оценивать учащихся, устраняя человеческие предубеждения. В то время как оценивание экзаменов с несколькими вариантами ответов уже выполняется искусственным интеллектом, вместе с тем современный генеративный искусственный интеллект также позволяет проводить устные и письменные опросы. Важным сдвигом является переход от оценки правильности ответа к анализу процесса решения задачи, что критически важно для инженеров.

4. **Эффективная организация контента:** Выявляя слабые места, ИИ и машинное обучение могут более эффективно организовывать обучающий контент. Например, по мере того как учащиеся осваивают один блок знаний или навык, они переходят к следующему, постоянно опираясь на ранее полученные знания.

5. **Динамичная схема обучения:** После того, как машина проведет анализ успеваемости учащихся, она может предложить лучший способ изучения нового материала. Она также может начинаться с предварительного анализа имеющихся знаний учебной программы. И как только будут выявлены слабые места, обучаемым поступают предложения по материалам и дальнейшей траектории обучения.

6. **Прогнозирование направлений дальнейших профессиональных навыков и знаний:** Приложения машинного обучения для прогнозирования направлений дальнейшего развития профессиональных навыков и знаний способны отслеживать интересы, склонности и антипатии учащихся. Они имеют возможности анализировать поведение и реакции учеников. На основе проведенного анализа они могут правильно прогнозировать интересующие ученика области, в которых он будет преуспевать.

7. **Группирование учащихся и преподавателей:** Еще один способ, с помощью которого машинное обучение позволяет улучшить образовательный процесс, — это группирование учащихся и преподавателей в соответствии с их способностями, потребностями и доступностью.

8. **Обеспечение непрерывности образовательного процесса:** Если, провести анализ темпов развития науки, технологий, то нетрудно заметить возрастание скорости их изменений. Другими словами, на протяжении жизни одного поколения происходит большое количество научно-технических и технологических трансформаций, что диктует необходимость осуществления непрерывного научно-образовательного процесса, который уже сегодня может осуществляться методами машинного обучения (Lifelong Learning support).

9. **Цифровые двойники в обучении:** Для инженерного образования, крайне актуально создание **цифровых двойников** сложных систем и оборудования. Студенты могут проводить эксперименты, проводить диагностику и даже ломать систему в виртуальной среде без рисков и затрат на реальное железо, получая опыт, эквивалентный реальному.

10. **VR/AR и Метавселенные в инженерии:** Технологии виртуальной (VR) и дополненной (AR) реальности, интегрированные с ИИ, позволяют создавать иммерсивные образовательные среды, где будущие инженеры могут собирать сложные механизмы, изучать наноструктуры изнутри или проводить виртуальные операции, кардинально меняя восприятие материала по сравнению с 2D-учебниками.

Преимущества и ограничения ИИ и машинного обучения

Трудно не заметить, что персонализированное обучение является наиболее заметным преимуществом [7-9] машинного обучения. Учащиеся могут работать над материалом, который соответствует их уникальным способностям, и переходить к более сложному учебному материалу по мере готовности. От этого подхода к обучению выигрывают не только студенты, но и учителя. Им больше не нужно составлять планы уроков, которые подходят для учащихся с любыми способностями и уровнями обучения. Качественное персонализированное обучение становится доступным для массового студенчества, снижая нагрузку на преподавателей.

Преимущество машинного обучения также проявляется в автоматической непредвзятой системе оценивания. Это дает возможность для абсолютно беспристрастной оценки, на которую не могут повлиять отношения учителя с любым учеником. Всё это экономит время учителей и дает более реалистичный обзор достижений обучаемого. Машинное обучение также может помочь преподавателям заглянуть в будущее. Интеллектуальная аналитика данных позволяет быстро выявлять закономерности, которые показывают, в чем состоят основные слабые места обучаемых, и определять, нужна ли ему дополнительная помощь.

Однако у этой технологии есть ограничения и риски (рис.5)

Рис. 5. Ограничения и риски применения ИИ в образовании

Вот основные ограничения, которые необходимо учитывать:

− **Проблема "черного ящика" (Black Box Problem):** Студенты могут слепо доверять ответам ИИ, не понимая *природы* решения. Важно учить студентов критически оценивать результаты работы алгоритмов, а не использовать их как "костыль".

− **Этика и предвзятость (Bias):** Алгоритмы обучаются на исторических данных, которые могут содержать предубеждения (например, гендерные или расовые). Важно обсуждать эти проблемы с будущими инженерами.

− **Проблема приватности (Privacy):** Гипер-персонализация требует сбора огромного количества данных о студенте. Необходимо четко определить границу между заботой и тотальной слежкой и обеспечить безопасность этих данных.

− **Когнитивная зависимость:** Опасность того, что ИИ отучит студентов думать самостоятельно, если они будут использовать его как "костыль" для решения всех задач, а не как помощника.

− **Снижение социального взаимодействия:** Основной недостаток машинного обучения заключается в том, что для обучаемых может сокращаться личное взаимодействие с учителем и с другими учениками. Это может существенно повлиять на их способность заводить друзей, работать в команде и хорошо адаптироваться в рабочих коллективах. При широком использовании машинного обучения может потребоваться дополнительное развитие социальных навыков.

− **Экономический барьер:** Кроме всего прочего, приобретение всего нового оборудования и программного обеспечения (VR-шлемы, доступ к мощным LLM, серверы для обработки данных) может также оказаться довольно дорогим, и это может быть одним из самых больших ограничений для внедрения ИИ в массовое образование.

Заключение

Таким образом, педагогическая парадигма 4.0 — это не просто внедрение технологий, а фундаментальная трансформация культуры обучения. Ключевая задача сейчас — не "оцифровать" старые методы, а создать новую экосистему, где человек и искусственный интеллект действуют в симбиозе. Современные технологии способны существенно повысить эффективность педагогического процесса, качество образования и эффективно развивать интеллектуальные возможности обучаемых. Искусственный интеллект и машинное обучение уже сегодня коренным образом меняют правила игры в образовательном процессе. Всё это несет много новых возможностей для повышения эффективности управления образовательным процессом, сокращения усилий и разрыва в знаниях между учениками и учителями. Инженерное образование должно опережать индустрию, формируя специалиста, который не боится перемен, владеет инструментами ИИ и способен создавать этичные и устойчивые технологии будущего. Это требует не только нового оборудования, но и масштабной программы повышения квалификации педагогических кадров, готовых к работе в новой роли наставника и архитектора учебного опыта. Уже сегодня в ряде высокотехнологичных предприятий РФ, в частности в ПКБ РИО, ведутся работы по созданию самых современных, интеллектуально-определяемых обучающих комплексов.

Список литературы

1. Комашинский В.И., Малыгин И.Г. Информационные технологии и искусственный интеллект — основные двигатели четвертой индустриальной революции (Industrie 4.0) // Информационные технологии. 2016. Т. 22. № 12. С. 899-904.
2. Комашинский В.И., Малыгин И.Г., Цыганов В.В. От Науки 4.0 к России 4.0 [Электронный ресурс]. – URL: https://clck.ru/W8r6f (дата обращения: 15.05.2024).
3. Комашинский В.И., Михалев О.А. Как индустрия искусственного интеллекта будет влиять на экономическое развитие России в XXI веке. Информация и космос. 2022. № 1. С. 30 - 34.
4. Комашинский В., Семин А., Рогозинский Г. Национальная инфраструктура знаний — нужна ли она России? // Технологии и средства связи. 2013. № 1 (94). С. 20–23.
5. Комашинский В.И. Предложения для концепции развития технологий искусственного интеллекта в Российской Федерации / В.И. Комашинский, О.А Михалев, И.Г. Малыгин // Транспорт Российской Федерации. – 2019. – № 4 (83). – С. 8–12

УДК 004.932

Оценка результативности нейросетевых моделей в задачах высокоточной сегментации изображений городской застройки при наличии сложных условий освещения и текстур

Галайчук К.В., Орлов А.А.

Военно-космическая академия имени А.Ф. Можайского, г. Санкт-Петербург, Россия

Аннотация**:** *Работа посвящена исследованию влияния архитектуры декодирующих модулей на качество семантической сегментации зданий на аэрофотоснимках. Проведено сравнение четырёх нейросетевых архитектур - U-Net, U-Net++, DeepLabV3+ и FPN - при едином энкодере ResNet34, предобученном на наборе данных ImageNet, что позволяет обеспечить корректность сопоставления декодирующих компонентов. Эксперименты выполнены на наборе данных зданий города Массачусетс и стратегии обучения без ранней остановки в течение 80 эпох. Применён расширенный набор показателей: индекс Жаккара, коэффициент Дайса, точность, полнота, F1-мера, граничный индекс Жаккара и расстояние Хаусдорфа. Архитектура U-Net++ достигла наилучших значений показателей (тестовый индекс Жаккара = 0,5580; коэффициент Дайса = 0,7163; граничный индекс Жаккара = 0,7751), превосходя классическую U-Net на 8 % по индексу Жаккара. Сетевая архитектора FPN, несмотря на худший индекс Жаккара (0,4317), демонстрирует наибольшую полноту (Полнота = 0,7431) и минимальное время быстродействия (14,2 мс). Результаты подтверждают гипотезу о преимуществе плотных пропускных связей для сегментации зданий и формулируют практические рекомендации по выбору архитектуры.*

Ключевые слова: *семантическая сегментация; глубокое обучение; сегментация зданий; U-Net; U-Net++; DeepLabV3+; Feature Pyramid Network; ResNet34; Boundary IoU; Hausdorff Distance.*

Введение

Задача автоматической сегментации зданий на аэрофотоснимках представляет значительный научный и практический интерес в связи с различной сферой использования - мониторинг городской застройки и территориальное планирование, автоматическое оценивание последствий техногенных и природных катастроф.

Традиционные методы сегментации зданий, основанные на алгоритмах выделения границ, сегментации, пороговой обработке и морфологических операциях, демонстрируют ограниченную эффективность при работе с аэрофотоснимками высокого пространственного разрешения. Главными факторами, снижающими точность классических подходов, являются вариативность условий освещения, наличие теней от растительности и соседних объектов, разнообразие текстур кровельных покрытий, а также сложная геометрия зданий, включающая пристройки, эркеры и мансарды. Появление и бурное развитие методов глубокого обучения, в первую очередь свёрточных нейронных сетей архитектуры «кодировщик – декодировщик», принципиально изменило методологию решения задач сегментации, обеспечив существенно более высокую точность относительно входных данных [1]. Архитектуры

семейства U-Net [2], DeepLab [3] и Feature Pyramid Network [4] стали стандартом в задачах сегментации изображений дистанционного зондирования.

Относительная эффективность распознавания изображений архитектурами существенно зависит от характера изображений, объёма размеченных данных и вычислительных ограничений. Особую актуальность приобретает вопрос о влиянии архитектуры декодирующего модуля, в частности типа и плотности пропускных связей, на качество сегментации при фиксированном энкодере [20][21]. Изоляция влияния декодера возможна только при использовании единого энкодера для всех сравниваемых моделей.

В работе выдвинута гипотеза, которая заключается в том, что архитектуры с плотными вложенными связям (U-Net++) обеспечивают более высокое качество за счёт сокращения семантического разрыва между уровнями признаков, однако требуют больших вычислительных затрат. Архитектуры со свёртками (DeepLabV3+) эффективно захватывают глобальный контекст за счет увеличенного рецептивного поля, однако могут терять высокочастотные пространственные детали на границах объектов.

Новизна работы заключается в проведении сравнения четырёх архитектур сегментации при идентичном энкодере ResNet34, что исключает влияние компонента кодировщика на результаты сравнения и позволяет оценить вклад декодирующего модуля и применении стратегии обучения без ранней остановки в течение полного цикла из 80 эпох, что обеспечивает полную сходимость всех моделей и корректную оценку их потенциала. Также использование расширенного набора показателей качества, включающий граничный индекс Жаккара и расстояние Хаусдорфа, что позволяет оценить пригодность моделей для задач, критичных к качеству локализации границ.

Архитектуры нейронных сетей для сегментации

В настоящем разделе представлены формальные описания четырёх архитектур декодирующих модулей, исследуемых в работе. Все четыре модели используют единый энкодер — ResNet34 [16], предобученный на наборе данных ImageNet, что позволяет изолировать влияние декодирующего компонента на качество сегментации. Реализация выполнена с использованием библиотеки «segmentation_models_pytorch» [18].

Архитектура U-Net [2][19] представляет собой симметричную сеть типа «кодировщик–декодировщик» с пропускными связями между соответствующими уровнями энкодера и декодера. Энкодер последовательно уменьшает пространственное разрешение признаковых карт при одновременном увеличении числа каналов, формируя иерархию признаков от низкоуровневых пространственных деталей до высокоуровневых семантических представлений. Декодер зеркально восстанавливает пространственное разрешение, при этом пропускные связи обеспечивают передачу низкоуровневых признаков из энкодера в декодер, что критически важно для точной локализации объектов.

Математически операция пропускной связи в U-Net на уровне l определяется как конкатенация признаков декодировщика, полученных операцией повышения пространственного разрешения с вышележащего уровня, с признаками соответствующего уровня энкодера:

$$f_{dec}{}^{(l)} = Conv(Up(f_{enc}{}^{(l+1)})) \oplus f_{enc}{}^{(l)}, \quad ((1)$$

где $f_{dec}{}^{(l)}$ - признаки декодера на уровне l; Up(·) - билинейная операция повышения пространственного разрешения; Conv(·) - свёрточный блок; $\oplus$ - конкатенация по канальному измерению; $f_{enc}{}^{(l)}$ - признаки энкодера на уровне l.

Результирующее представление одновременно содержит высокоуровневый семантический контекст и низкоуровневые пространственные детали, что обеспечивает точную локализацию границ объектов.

Модификация U-Net++, предложенная Чжоу и соавторами в 2018 году [6], направлена на улучшение информационного потока между энкодером и декодером посредством вложенных Связей. Ключевым нововведением является введение промежуточных узлов $X_{(l,n)}$ на всех уровнях иерархии, что позволяет сократить семантический разрыв между признаками энкодера и декодера. Узел $X_{(l,n)}$ обозначает узел на уровне l в позиции n, где $l \in \{0, 1, 2, 3, 4\}$ - уровень в иерархии, $n \in \{0, 1, 2, 3\}$ - позиция узла вдоль плотного блока.

Математически выход узла (l, n) определяется как результат свёртки от конкатенации признаков всех предшествующих узлов того же уровня:

$$f_{(l,n)} = Conv(\oplus^{n}{}_{k=0}\ f_{(l,k-1)}), \quad ((2)$$

где $\oplus$ обозначает конкатенацию по канальному измерению, а индекс k пробегает значения от 0 до n. Плотные соединения между промежуточными узлами обеспечивают множественные информационные потоки, позволяя модели извлекать признаки на различных уровнях детализации и комбинировать их для формирования оптимального представления. Согласно гипотезе авторов U-Net++, такая архитектура особенно эффективна для задач, где семантический разрыв между уровнями признаков существенен — например, при сегментации объектов со сложной морфологией.

Архитектура DeepLabV3+ [3] использует принципиально иной подход к организации декодера и позволяет увеличивать поле свёртки без потери пространственного разрешения и без увеличения числа параметров. Формально свёртка с коэффициентом расширения - r определяется как:

$$y[i] = \sum_{k=0}^{K-1} x[i + r \cdot k] \cdot w[k], \quad ((3)$$

где r — коэффициент расширения, определяющий расстояние между элементами свёрточного ядра; K — размер ядра; x — входная признаковая карта; w — веса свёртки. При r = 1 операция сводится к обычной свёртке. Модуль ASPP применяет параллельно несколько дилатационных свёрток с коэффициент расширения (6, 12, 18) и глобальное усреднение, обеспечивая захват контекстной информации на различных масштабах. Выходы ветвей конкатенируются и проходят через свёртку 1×1. Декодер DeepLabV3+

использует только одно низкоуровневое пропускные соединение от ранних слоёв энкодера.

Feature Pyramid Network (FPN) [4] изначально разработана для задач детектирования объектов и основана на построении пирамиды признаковых представлений. Архитектура состоит из нисходящего пути — собственно энкодера, последовательно уменьшающего пространственное разрешение, и восходящего пути с боковыми соединениями для построения многомасштабных признаковых представлений. Каждый уровень пирамиды P_i формируется путём свёртки 1×1 к признакам соответствующего уровня C_i энкодера; повышения дискретизации признаков с вышележащего уровня P_{i+1} ; поэлементного сложения. Дополнительно применяется свёртка 3×3 для устранения эффекта наложения. Пирамидальная структура обеспечивает эффективную обработку объектов различного масштаба, что делает FPN приемлемой для задач реального времени, однако для задач, требующих точной локализации границ, FPN может уступать архитектурам с более прямыми информационными потоками.

Вычислительные эксперименты проведены на наборе данных зданий Массачусетса [5], содержащем аэрофотоснимки территории Большого Бостона (США). Выборка включает 137 изображений обучающей выборки, 4 изображения валидационной выборки и 10 изображений тестовой выборки (всего 151 изображение). Исходные изображения имеют разрешение 1500 × 1500 пикселей при пространственном разрешении съёмки около 1 м/пиксель, что соответствует площади покрытия примерно 2,25 км² на каждый снимок. Каждое изображение сопровождается бинарной маской-разметкой, где пиксели со значением 1 соответствуют зданиям, а пиксели со значением 0 - фоновым областям.

Выборка данных характеризуется высокой вариативностью масштаба зданий — от небольших частных домов до крупных промышленных сооружений. Среди особенностей, усложняющих сегментацию: наличие теней от зданий и растительности, сложная текстура подстилающей поверхности, объекты, морфологически схожие с зданиями (автомобили, контейнеры, хозяйственные постройки).

Разбиение выборки данных: 137 обучающих, 4 валидационных, 10 тестовых изображений (90,7 % / 2,6 % / 6,6 %). Малый размер валидационной выборки ограничивает точную настройку гиперпараметров, однако для сравнительного анализа архитектур при идентичной методологии это допустимо. Все изображения приведены к размеру 512 × 512 пикселей.

Предобработка данных включает нормализацию с использованием средних значений и стандартных отклонений набора данных ImageNet: μ = [0,485; 0,456; 0,406], σ = [0,229; 0,224; 0,225]. Данная нормализация является стандартной для моделей с энкодером, предобученным на ImageNet, и обеспечивает корректное соответствие между распределением входных данных и статистикой весов предобученного энкодера. Для изображений применена билинейная интерполяция при изменении размеров изображения, тогда как

для масок использована интерполяция методом ближайшего соседа, что предотвращает появление промежуточных значений в бинарной маске. Бинаризация масок выполнена с порогом 127: пиксели со значением выше порога классифицируются как здания (1), остальные - как фон (0).

Аугментация данных применена только к обучающей выборке и выполнена с использованием библиотеки Albumentations [17]. Параметры трансформаций представлены в таблице 1.

Таблица 1 – Параметры аугментации данных

Трансформация	Параметры	Вероятность
Горизонтальное отражение	—	0,5
Вертикальное отражение	—	0,5
Случайный поворот	90°, 180° или 270°	0,5
Аффинное преобразование	коэффициент сдвига = 0,1; коэффициент увеличения = 0,1; угол вращения = 30°	0,5
Гауссовский шум	коэффициент дисперсии = (10; 50)	0,3
Гауссовское размытие	коэффициент размытия = 3	0,3
Яркость и контраст	коэффициент яркости = 0,2; коэффициент контрастности = 0,2	0,3

Аугментации повышают результативность модели: геометрические трансформации имитируют вариативность ориентации зданий; фотометрические — вариативность условий освещения и качества съёмки. Для валидационной и тестовой выборок аугментация не применялась. Конфигурация обучения выбрана идентичной для всех четырёх архитектур с целью исключить влияние гиперпараметров на результаты сравнения. Полный набор параметров представлен в таблице 2.

Таблица 2 – Конфигурация обучения

Параметр	Значение
Оптимизатор	AdamW
Начальная скорость обучения	1×10^{-4}
L2-регуляризация	1×10^{-4}
Размер сегмента	8
Число эпох	80
Планировщик скорости обучения	метод косинусного затухания скорости обучения с периодическими перезапусками ($T_0 = 10$; T_mult = 2; η_min = 10^{-6})
Ранняя остановка	Не применялась
Автоматическая смешанная точность	Включена
Размер изображения	512 × 512 пикселей
Случайное начальное значение	42
Видеокарта	NVIDIA Tesla T4 (14,6 ГБ VRAM, CUDA 12.8)

В качестве оптимизатора использован AdamW [14], сочетающий адаптивную оценку моментов градиента с раздельным затуханием весов, что обеспечивает лучшую регуляризацию по сравнению с классическим Adam. Начальная скорость обучения 1×10^{-4} выбрана как стандартное значение для тонкой настройки моделей с предобученным энкодером. Планировщик методом косинусного затухания скорости обучения с периодическими перезапусками [15] с параметрами $T_0 = 10$, T_mult = 2, η_min = 10^{-6} обеспечивает периодический рестарт скорости обучения, что позволяет модели выходить из локальных минимумов и исследовать более широкое пространство параметров. Автоматическая смешанная точность применена для ускорения обучения и снижения потребления памяти графического ускорителя без существенной потери точности.

Стратегия обучения без ранней остановки обоснована тем, что агрессивная ранняя остановка может приводить к недооценке качества моделей с большим числом параметров (в частности, U-Net++ с вложенными плотными пропускными связями требует большего времени на сходимость). Обучение всех моделей в течение 80 эпох позволяет корректно оценить потенциал каждой архитектуры [23].

Функция потерь представляет собой взвешенную комбинацию потери Дайса с коэффициентом 0,7 и бинарной кросс-энтропии с коэффициентом 0,3. Функция потери Дайса обеспечивает оптимизацию напрямую через замеры, тесно связанные с индексом Жаккара, что особенно важно для несбалансированных задач сегментации, где площадь зданий может составлять менее 20 % от площади изображения. Математически потери Дайса определяется как:

$$L_{Dice} = 1 - \frac{2(|A \cap B| + \varepsilon)}{|A| + |B| + \varepsilon}, \quad (4)$$

где |A ∩ B| — площадь пересечения предсказанной и истинной масок; |A|, |B| — площади соответствующих масок; ε — малое значение (1,0) для численной стабильности. Потери бинарной кросс-энтропии дополняет потери Дайса, обеспечивая стабильную градиентную динамику на начальных этапах обучения:

$$L_{BCE} = -[y \cdot log(p) + (1 - y) \cdot log(1 - p)], \quad (5)$$

где y — истинная метка пикселя (0 или 1); p — предсказанная вероятность. Общая функция потерь имеет вид:

$$L_{total} = 0{,}7 \cdot L_{Dice} + 0{,}3 \cdot L_{BCE}, \quad (6)$$

что обеспечивает баланс между прямой оптимизацией метрик качества сегментации и стабильностью градиентной динамики.

Для всесторонней оценки качества сегментации использован расширенный набор из семи метрик, включающий как глобальные метрики (индекс Жаккара, коэффициент Дайса, F1-мера, точность классификации), так и метрики, оценивающие качество локализации границ (граничный индекс Жаккара, расстояние Хаусдорфа).

Индекс Жаккара (IoU) [10][22] — отношение площади пересечения предсказанной и истинной масок к площади их объединения:

$$\text{Индекс Жаккара} = \frac{TP}{TP + FP + FN}. \quad (7)$$

Коэффициент Дайса [7] — тесно связан с индексом Жаккара и эквивалентен гармоническому среднему точности и полноты:

$$\text{Коэффициент Дайса} = \frac{2 \cdot TP}{2 \cdot TP + FP + FN}. \quad (8)$$

Точность [8] — доля истинно положительных предсказаний среди всех положительных предсказаний модели:

$$\text{Точность} = \frac{TP}{TP + FP}. \quad (9)$$

Полнота [8] — доля истинно положительных предсказаний среди всех реальных положительных пикселей:

$$\text{Полнота} = \frac{TP}{TP + FN}. \quad (10)$$

F1-мера, вычисляемая как гармоническое среднее точностью и полнотой, алгебраически совпадает с коэффициентом Дайса при вычислении через TP, FP, FN Обе метрики приводятся для полноты сопоставления с литературой.

Граничный индекс Жаккара [9] с радиусом дилатации r = 2 пикселя оценивает качество сегментации именно на границах объектов. Для каждой маски вычисляется её граница через морфологический градиент (разность дилатации и эрозии), после чего IoU вычисляется для границ предсказанной и истинной масок:

$$\text{граничный индекс Жаккара} = \frac{|\partial B_{pred} \cap \partial B_{gt}|}{|\partial B_{pred} \cup \partial B_{gt}|}, \quad (11)$$

где ∂B_{pred} и ∂B_{gt} — границы предсказанной и истинной масок соответственно. граничный индекс Жаккара критически важен для приложений, требующих точной локализации контуров зданий.

Расстояние Хаусдорфа характеризует максимальное расстояние между точками границ предсказанной и истинной масок, предоставляя информацию о наихудших случаях локализации. Симметричная расстояние Хаусдорфа вычисляется как:

$$H(A,B) = \max\{h(A,B), h(B,A)\},$$
$$h(A,B) = max_{a \in A}\, min_{b \in B}\, d(a,b) \quad (12)$$

где h(A,B) — направленное расстояние Хаусдорфа от множества A к множеству B; $d(a,b)$ — евклидово расстояние между точками. Симметричная форма $H(A,B) = max\{h(A,B), h(B,A)\}$ обеспечивает инвариантность к направлению сравнения и чувствительность к выбросам.

Результаты экспериментов

Экспериментальное сравнение четырёх архитектур сегментации на тестовой выборке продемонстрировало существенные различия в качестве и вычислительной эффективности моделей. Сводные результаты представлены в таблице 3, где модели упорядочены по убыванию значения метрики индекса Жаккара. Лучшая эпоха определялась по максимальному значению индекса Жаккара на валидационной выборке в течение обучения.

Таблица 3 – Результаты сравнительного анализа моделей сегментации на тестовой выборке

Модель	Парам., млн	Размер, МБ	IoU	Dice	Precision	Recall	F1	Boundary IoU	Hausdorff, px	Быстродействие, мс	Лучш. эпоха
U-Net++	**26,08**	**99,5**	**0,5580**	**0,7163**	**0,6750**	**0,7633**	**0,7163**	**0,7751**	**7,50**	**37,2**	**54**
U-Net	24,44	93,2	0,5166	0,6812	0,6434	0,7237	0,6812	0,7495	7,89	17,4	78
DeepLab V3+	22,44	85,6	0,4406	0,6115	0,5600	0,6739	0,6115	0,7082	9,94	17,1	79
FPN	23,16	88,3	0,4317	0,6029	0,5076	0,7431	0,6029	0,7116	9,12	14,2	79

Архитектура U-Net++ с вложенными плотными пропускными связями достигла наилучших показателей по большинству метрик качества: индекс Жаккара составил 0,5580, коэффициент Дайса — 0,7163, граничный индекс Жаккара — 0,7751. Наименьшее значение расстояния Хаусдорфа (7,50 пикселей) свидетельствует о высокой точности локализации границ зданий данной моделью. Время быстродействия U-Net++ составило 37,2 мс на изображение размером 512 × 512 пикселей, что является максимальным среди рассмотренных моделей. Лучшая эпоха для U-Net++ - 54, что существенно раньше других моделей (78–79) и свидетельствует о более быстрой сходимости архитектуры, несмотря на большее число параметров. Полученные результаты согласуются с данными работы Li и соавторов [10], где U-Net++ также демонстрирует превосходство на задачах сегментации зданий (рисунок 1).

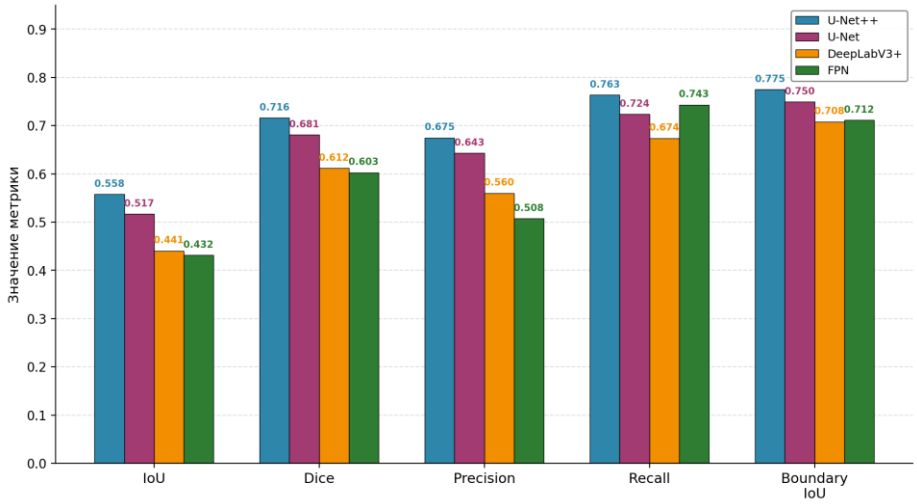


Рис. 1. Сравнение моделей по пяти метрикам качества сегментации: IoU, Dice, Precision, Recall, Boundary IoU

Классическая U-Net продемонстрировала конкурентоспособные результаты, уступая U-Net++ около 8 % по индексу Жаккара. Время

быстродействия U-Net составило 17,4 мс — в 2,1 раза меньше, чем у U-Net++, что делает её привлекательной для приложений с ограничениями на вычислительные ресурсы.

Архитектура DeepLabV3+ показала существенно более низкие результаты с индекса Жаккара = 0,4406. Свёртки с расширением в составе модуля пространственного пирамидального пулинга, обеспечивая широкий охват рецептивного поля, теряют важные пространственные детали при восстановлении разрешения, что критично для малых и средних зданий.

Архитектура FPN показала наихудший результат по индексу Жаккара (0,4317) однако продемонстрировала наибольшее значение полноты (0,7431) среди всех моделей, что указывает на тенденцию к избыточной сегментации. Динамика сходимости моделей (рисунок 2) демонстрирует характерное поведение: резкий рост индекса Жаккара в первые 10–20 эпох с последующим выходом на плато. Архитектура U-Net++ достигает пикового значения индекса Жаккара = 0,5088 уже к 70-й эпохе, тогда как остальные модели продолжают плавно улучшать качество вплоть до 78–79-й эпохи.

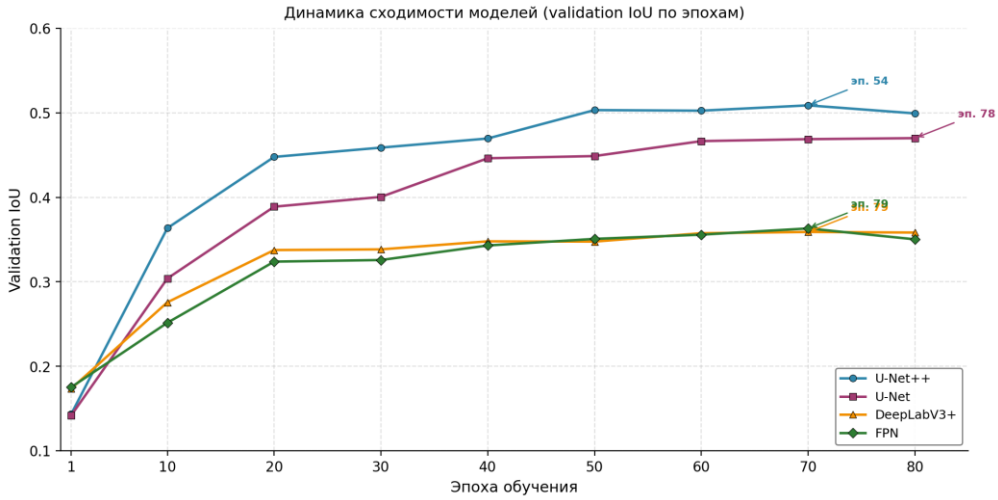


Рис. 2. Динамика сходимости моделей: индекс Жаккара по эпохам обучения (1–80). Аннотациями отмечены лучшие эпохи: U-Net++ — 54; U-Net, DeepLabV3+, FPN - 78–79

Это подтверждает эффективность плотных пропускных связей в ускорении сходимости: при равном бюджете вычислений U-Net++ достигает оптимального качества раньше, что имеет практическое значение при ограниченных вычислительных ресурсах. Анализ «качество / скорость» (рис. 4) позволяет выделить два кластера моделей. Кластер «быстрые, низкое качество» (FPN, DeepLabV3+, U-Net) обеспечивает время быстродействия 14–17 мс при индексе Жаккара 0,43–0,52. Кластер «медленные, высокое качество» (U-Net++) достигает индекса Жаккара 0,5580 при времени быстродействия 37,2 мс (рисунок 3). Между этими кластерами наблюдается значительный разрыв по времени (~20 мс), что отражает качественный скачок в архитектуре при переходе от классических пропускных связей к плотным вложенным.

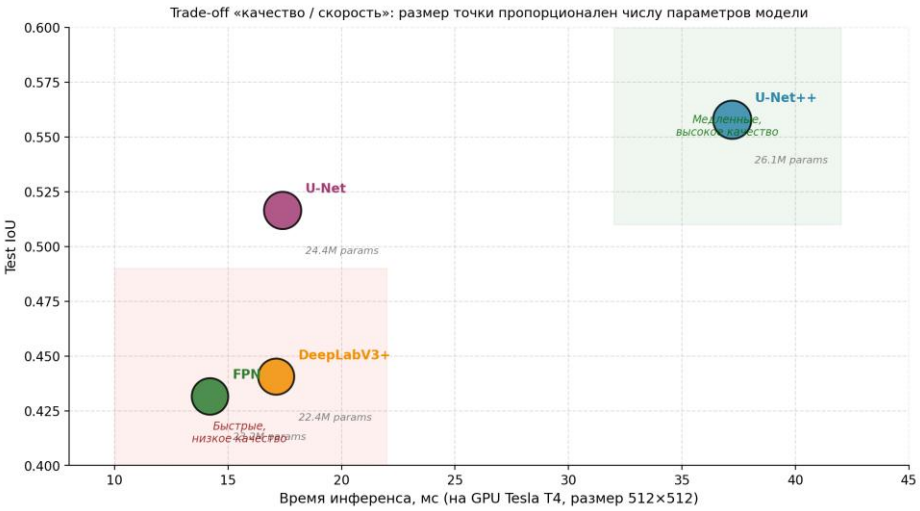


Рис. 3. График зависимости индекса Жакара от времени эксперимента. По оси X — время инференса, по оси Y — Test IoU. Размер маркера пропорционален числу параметров модели

Круговая диаграмма (рисунок 4) наглядно демонстрирует, что профиль U-Net++ доминирует над остальными моделями по пяти из шести метрик, уступая лишь FPN по метрике полнота. Профиль U-Net близок к U-Net++ по форме, но смещён внутрь, что отражает его второе место по большинству метрик. Профили DeepLabV3+ и FPN визуально пересекаются, причём FPN имеет выраженную асимметрию с максимумом по оси полноты и минимумом по точности, что подтверждает тенденцию к избыточной сегментации.

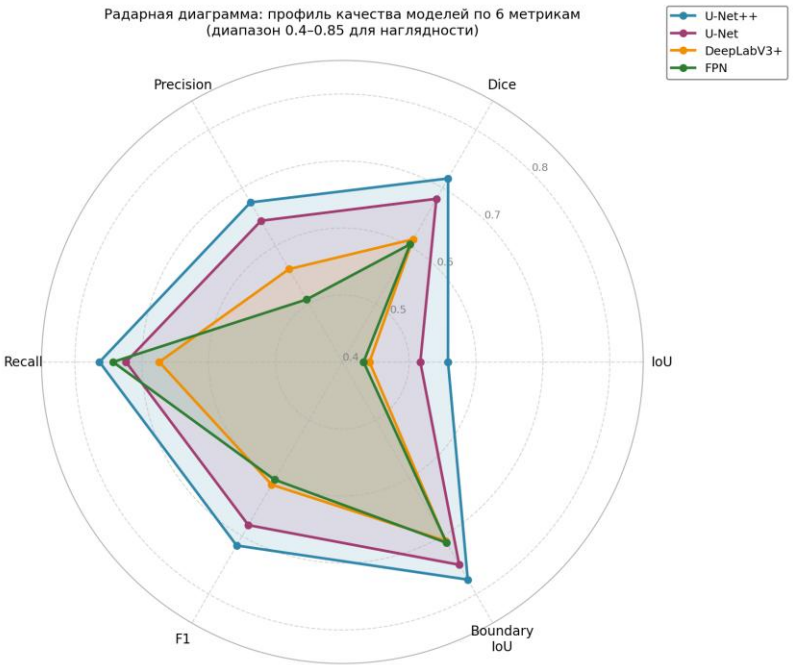


Рис. 4. Круговая диаграмма профиля качества моделей по 6 метрикам (диапазон 0,4–0,85 для наглядности различий)

Абсолютные значения индекса Жаккара ниже типичных бенчмарков (0,75+) на крупных датасетах, что объясняется ограниченным размером обучающей выборки (137 изображений) и высокой вариативностью масштаба зданий.

Полученные результаты подтверждают основную гипотезу исследования о преимуществе архитектур с плотными пропускными связями для задач сегментации зданий. Превосходство U-Net++ над классической U-Net на 8 % по индексу Жаккара может быть объяснено несколькими механизмами. Во-первых, плотные пропускные связи сокращают семантический разрыв между уровнями признаков энкодера и декодера: вместо прямой передачи признаков с уровня 1 энкодера на уровень 1 декодера, U-Net++ использует промежуточные узлы, которые постепенно преобразуют признаки, делая их более совместимыми с целевым уровнем декодера. Во-вторых, множественные пути градиентного потока через плотные соединения обеспечивают более эффективное обратное распространение ошибки, что особенно важно для глубоких сетей. В-третьих, архитектура U-Net++ обеспечивает более быструю сходимость — лучшая эпоха 54 против 78 у U-Net, что позволяет модели достигать оптимального качества при меньшем числе вычислительных ресурсов.

Архитектура DeepLabV3+ разрабатывалась для сегментации естественных изображений, где объекты обладают выраженной внутренней структурой и контекст существенен для классификации. На аэрофотоснимках зданий контекстные признаки менее информативны. Модуль пространственного пирамидального пулинга с расширением, использующий дилатационные свёртки с коэффициентами расширения 6, 12 и 18, оптимизирован для дальнего контекста, но теряет локальные пространственные детали, что приводит к ухудшению граничный индекс Жаккара. На малой выборке (137 изображений) дополнительные параметры модуля пространственного пирамидального пулинга с расширением модуля могут приводить к переобучению.

Поведение FPN, характеризующееся высоким полнотой (0,7431) при низком точности (0,5076), соответствует архитектурной специфике пирамидальных сетей. Боковые связи через свёртки 1×1 агрегируют признаки с нескольких уровней, что обеспечивает чувствительность к объектам различного масштаба, но снижает специфичность предсказаний. Поэлементное сложение признаков с разных уровней может приводить к размытию границ и ложным срабатываниям на текстурах, схожих с кровельными покрытиями. FPN может быть рекомендована для систем первичного обнаружения, где критична полнота (например, идентификация всех потенциальных зон застройки для последующего анализа специалистом), а не точность контуров.

Критически важным наблюдением является влияние стратегии обучения на результаты сравнения архитектур. Применение агрессивной ранней остановки приводит к систематической недооценке качества сложных моделей с большим числом параметров. U-Net++, требующая большего числа эпох для сходимости из-за вложенной архитектуры, существенно недообучается

при преждевременной остановке. Полная сходимость всех моделей за 80 эпох без ранней остановки позволяет корректно оценить потенциал каждой архитектуры — данный методологический вывод имеет самостоятельное значение для планирования будущих сравнительных исследований

Ограничения исследования

При интерпретации результатов необходимо учитывать ряд методологических ограничений, влияющих на обобщающую способность выводов.

Первое и наиболее существенное ограничение связано с малым размером тестовой выборки (n = 10) и валидационной (n = 4). При таком объёме дисперсия метрик существенна, а проведение строгих статистических тестов не представляется возможным. Различия в IoU (от 0,4317 до 0,5580) могут быть отчасти обусловлены случайностью выбора тестовых изображений. В дальнейших исследованиях необходимо использовать тестовую выборку не менее 100 изображений с применением кросс-валидации.

Второе ограничение состоит в использовании единственного набора данных. Характеристики данной выборки (городская застройка Бостона, разрешение 1 м/пиксель) могут не обобщаться на другие географические контексты. Результаты на альтернативных выборках могут существенно отличаться, поэтому валидация на нескольких независимых выборках необходима для утверждения универсальности выводов.

Третье ограничение связано с использованием единственного энкодера - ResNet34. Хотя выбор методологически оправдан для изоляции влияния декодирующего модуля, результаты могут отличаться при использовании более мощных энкодеров (EfficientNet-B4, ResNeSt-50, ConvNeXt-Tiny, Swin Transformer), которые могут частично компенсировать ограничения более простых декодеров и изменить относительное ранжирование архитектур.

Четвёртое ограничение имеет технический характер: метрика Hausdorff Distance реализована в симметричной форме как максимум из двух направленных, а не как 95-й перцентиль распределения, что повышает чувствительность к выбросам.

Заключение

Результаты подтверждают гипотезу о превосходстве архитектур с плотными вложенными пропускными связями над классическими при условии полной сходимости модели. Превосходство U-Net++ над U-Net на 8 % по индексу Жаккара свидетельствует о существенном влиянии архитектуры декодирующего модуля на качество сегментации. Для приложений, требующих максимальной точности и качества локализации границ, рекомендуется U-Net++ несмотря на большее время быстродействия (37,2 мс) — её лучшие значения граничный индекс Жаккара (0,7751) и расстояния Хаусдорфа (7,50 пикселей) обеспечивают точность, достаточную для практического применения. Для систем с ограниченными ресурсами оптимальна классическая U-Net (индекс

Жаккара = 0,5166, 17,4 мс). Расширенный набор метрик продемонстрировал важность для практических приложений: модели с близкими индексом Жаккара могут существенно различаться по качеству локализации границ, что критично для приложения требующих точности сегментирования, например в сфере кадастрового учёта.

Список литературы

1. Long J., Shelhamer E., Darrell T. Fully convolutional networks for semantic segmentation // Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition. — 2015. — P. 3431–3440.

2. Ronneberger O., Fischer P., Brox T. U-Net: Convolutional Networks for Biomedical Image Segmentation // Lecture Notes in Computer Science. — 2015. — Vol. 9351. — P. 234–241.

3. Chen L.-C., Zhu Y., Papandreou G., Schroff F., Adam H. Encoder-Decoder with Atrous Separable Convolution for Semantic Image Segmentation // Proceedings of the European Conference on Computer Vision (ECCV). — 2018. — P. 801–818.

4. Lin T.-Y., Dollár P., Girshick R., He K., Hariharan B., Belongie S. Feature Pyramid Networks for Object Detection // Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition. — 2017. — P. 2117–2125.

5. Mnih V. Machine Learning for Aerial Image Labeling: PhD thesis. — University of Toronto, 2013. — 107 p.

6. Zhou Z., Siddiquee M. M. R., Tajbakhsh N., Liang J. UNet++: A Nested U-Net Architecture for Medical Image Segmentation // IEEE Transactions on Medical Imaging. — 2019. — Vol. 38, No. 8. — P. 1856–1867.

7. Kervadec H., Bouchtiba J., Desrosiers C., Granger E., Dolz J., Ben Ayed I. Boundary loss for highly unbalanced segmentation // Medical Image Analysis. — 2021. — Vol. 67. — Article 101851.

8. Garcia-Garcia A., Orts-Escolano S., Oprea S., Villena-Martinez V., Martinez-Gonzalez P., Garcia-Rodriguez J. A survey on deep learning techniques for image and video semantic segmentation // Applied Soft Computing. — 2018. — Vol. 70. — P. 41–65.

9. Huang H., Lin L., Tong R., Hu H., Zhang Q., Iwamoto Y., Han X., Chen Y.-W., Wu J., Zhou J. UNet 3+: A Full-Scale Connected UNet for Medical Image Segmentation // ICASSP 2020 — IEEE International Conference on Acoustics, Speech and Signal Processing. — 2020. — P. 1055–1059.

10. Li Q., Mou L., Liu Q., Liu Y., Zhu X. X. Building Extraction from Very High Resolution Imagery Using Squeeze-and-Excitation Network // Remote Sensing. — 2020. — Vol. 12, No. 19. — Article 3245.

11. Ji S., Wei S., Lu M. Fully Convolutional Networks for Multisource Building Extraction From an Open Aerial and Satellite Imagery Data Set // IEEE Transactions on Geoscience and Remote Sensing. — 2019. — Vol. 57, No. 1. — P. 574–586.

12. Xie E., Wang W., Yu Z., Anandkumar A., Alvarez J. M., Luo P. SegFormer: Simple and Efficient Design for Semantic Segmentation with Transformers //

Advances in Neural Information Processing Systems (NeurIPS). — 2021. — Vol. 34. — P. 12077–12090.

13. Liu Z., Lin Y., Cao Y., Hu H., Wei Y., Zhang Z., Lin S., Guo B. Swin Transformer: Hierarchical Vision Transformer Using Shifted Windows // Proceedings of the IEEE/CVF International Conference on Computer Vision (ICCV). — 2021. — P. 10012–10022.

14. Loshchilov I., Hutter F. Decoupled Weight Decay Regularization // International Conference on Learning Representations (ICLR). — 2019.

15. Loshchilov I., Hutter F. SGDR: Stochastic Gradient Descent with Warm Restarts // International Conference on Learning Representations (ICLR). — 2017.

16. He K., Zhang X., Ren S., Sun J. Deep Residual Learning for Image Recognition // Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition. — 2016. — P. 770–778.

17. Buslaev A., Iglovikov V. I., Khvedchenya E., Parinov A., Druzhinin M., Kalinin A. A. Albumentations: Fast and Flexible Image Augmentations // Information. — 2020. — Vol. 11, No. 2. — Article 125.

18. Yakubovskiy P. Segmentation Models Pytorch [Электронный ресурс] // GitHub Repository. — 2020. — URL: https://github.com/qubvel/segmentation_models.pytorch (дата обращения: 01.07.2026).

19. Соловьев Р. А., Тельпухов Д. В., Кустов А. Г. Автоматическая сегментация спутниковых снимков на базе модифицированной свёрточной нейронной сети UNET // Инженерный вестник Дона. — 2017. — № 4(47). — С. 443.

20. Аваков Я. А. Обзор современных методов автоматизированного дешифрирования оптических спутниковых снимков для оценки лесных насаждений // Лесохозяйственная информация. — 2026. — № 1. — С. 72–81.

21. Абрамов Н. С., Макаров Д. А., Талалаев А. А., Фраленко В. П. Современные методы интеллектуальной обработки данных ДЗЗ // Программные системы: теория и приложения. — 2018. — Т. 9, № 4(39). — С. 417–442.

22. Малкин А. Ю., Марков Н. Г. Помехоустойчивость модели полносверточной нейронной сети U-Net при семантической сегментации деревьев пихты на зашумленных снимках с БПЛА // Доклады ТУСУР. — 2024. — Т. 27, № 2. — С. 64–70.

23. Колесник Т. О., Дучков А. А. Поиск оптимальных 2D моделей нейронной сети U-Net для решения задачи семантической сегментации томографических изображений гидратосодержащих образцов // Вестник Новосибирского государственного университета. Серия: Информационные технологии. — 2022. — Т. 20, № 1. — С. 28–46

СОДЕРЖАНИЕ

Приветственные слова, состав программного комитета

В. Н. Шелудько, А. А. Лотонина, А. В. Балицкий ……..... 3–5

Технологии инфокоммуникаций, робототехники и искусственного интеллекта, как основа будущих этапов эволюции цифрового мира, создаваемого человечеством

Яшин А. И. 7

Производственная аспирантура как новая модель послевузовского образования, направленная на сращивание фундаментальной и прикладной науки

Будко П. А. 11

К вопросу о тенденциях технического и технологического развития телекоммуникационных систем

Кулешов И. А., Курносов В. И. 18

Обеспечение безопасности автономных ИИ-агентов при их интеграции в телекоммуникационные системы

Ходаковский М. А. 24

СЕКЦИЯ 1. СИСТЕМЫ, СЕТИ И УСТРОЙСТВА ТЕЛЕКОММУНИКАЦИЙ

Комплекс оценки пропускной способности канала спутниковой связи по данным ГНСС-зондирования ионосферы

Диптан П. А..... 32

Анализ методов оценки угла прихода сигнала в задачах локального позиционирования

Чижов А. С. 39

Технология интеллектуального мониторинга состояния информационно-телекоммуникационных сетей и систем

Будко Н. П. 49

Предиктивно-адаптивное управление модуляцией и кодированием в беспроводных системах передачи контент-зависимого трафика

Иванов В. А., Маркин А. В., Овсянкин С. В., Иванов И. В., Лапицкий В. Ф. 54

Оценка эффективности анализа защищённости морских систем управления движением судов с применением искусственного интеллекта

Позолотин С. И. 65

Результаты разработки средств и комплексов авиационной радиосвязи в НПП «ПРИМА»

Скрипник И. В. 72

Подход к технической реализации алгоритмов управления квазирезервированными устройствами комплексов аппаратно-программных средств

Лукин К. И., Сызранцев Г. В. 79

Операторная модель управления информационно-телекоммуникационной системой специального назначения в условиях воздействий дестабилизирующих факторов

Лукин К. И., Сызранцев Г. В. 91

Тенденции развития автоматизированных систем управления оборудованием, сетями и системами связи общего и специального назначения

Курносов В. И., Сызранцев Г. В. 106

Обобщённая модель формирования структуры сети абонентского доступа специального назначения

Гагарин С. П., Сызранцев Г. В. 120

Разработка и исследование цифрового радиоприёмного тракта в сложной помеховой обстановке реального КВ-канала

Михайлов В. А., Каримов Т. И., Росин С. Б. 128

Методика информационного обеспечения потребителей о надводной обстановке при проведении поисково-спасательных операций

Тюстин М. М., Черевань Д. В., Зыков Д. Д. 144

Предложения по реализации алгоритмов сопряжения сетей передачи данных специального назначения

Спивак А. В. 151

Методы оценки процесса функционирования сетей передачи данных специального назначения

Спивак А. В. 158

СЕКЦИЯ 2. РОБОТОТЕХНИКА И ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ

Наращивание оперативности доведения команд управления до беспилотного транспорта за счет формирования сигнально-кодовых конструкций по технологиям расширения спектра

Будко Д. Д. 165

Обзор методов компьютерного зрения

Голоскок Д. С. 177

Эффективность применения робототехнических комплексов в интересах технического обеспечения связи

Клименко А. Д. 183

Раннее обнаружение DDoS-атак на стадии подготовки на основе машинного обучения и контроля остаточного трафика

Потапов Г. А., Гречишникова Т. А. 188

Разработка волоконно-оптического датчика акселерометра для детектирования низкочастотных вибраций

Штеле Б. Э. 194

Создание алгоритма обратной задачи для определения геометрии внутренних полостей в стене по данным акустического зондирования

Данченко И. Д., Ходаковский М. А., Косарев В. Р. 203

Оценка устойчивости защиты речевых аудиозаписей к нейросетевой очистке при атаках на голосовую биометрию транспортных систем

Вдовин Д. А., Фесько Н. В. 212

Повышение точности детектирования артефактов AI-преобразования голоса на основе адаптивной модификации оконной функции спектрального анализа

Горбунова Д. А., Паленникова М. Д. 218

Оценка информативности спектрально-статистических характеристик аудиосигнала до сжатия с потерями и после для обнаружения нейросгенерированной речи

Ишутин И. А., Сильвестрова Д. Д., Шульженко А. Д., Игнатьев А. А. 227

Экспериментальная оценка способа детекции ИИ-подделок голосовых аудиозаписей с использованием статистик LPC остатков

Мирошников Н. Ю., Нахапетян Ю. А., Шульженко А. Д., Игнатьев А. А. 233

Влияние конструктивных особенностей измерительного стенда на погрешность идентификации дефектов в рефлетометрии проводных линий

Фесько Н. В., Рамзаев В. А., Зубов В. Г. 237

Исследование влияния интенсивности и модуляции шумовой помехи на качество автоматического распознавания речи

Рамзаев В. А., Фесько Н. В., Шульженко А. Д. 241

Оценка репрезентативности методики испытаний систем автоматического распознавания речи при исследовании эффективности акустических помех

Рамзаев В. А., Фесько Н. В., Повеликин В. Я. 245

СЕКЦИЯ 3. СИСТЕМЫ УПРАВЛЕНИЯ И НАВИГАЦИИ

Сравнительный анализ современных систем наземной навигации специального назначения

Быстров Д. Е., Кириченко Р. Н. 252

Управление объединенными запасами эксплуатантов с малым паркам воздушных судов на основе телекоммуникационных систем сбора эксплуатационных данных

Субботин В. С. 259

Способ построения ортогональных и квазиортогональных базисов франка при реализации разделения каналов в спутниковых системах связи

Ерунов А. А., Черкашин А. П. 271

Оценивание энергетической доступности источников радиоизлучений при проведении спасательных операций

Тюстин М. М., Черевань Д. В., Сивохина Н. В. 281

Моделирование ракурсных изображений типовых участков местности в инфракрасном диапазоне длин волн

Ширямов О. А., Захарчук А. В. 288

Коэффициент готовности элемента распределённой системы управления и подходы к автоматизированному восстановлению его функции на резервном узле

Бесчастнов А. А. 298

Способ геопривязки инфракрасных изображений, получаемых в ходе плановой аэросъёмки с воздушного носителя

К.В. Галайчук, А.В. Захарчук, Д.В. Черевань 304

Реализация цифрового фильтра при обработке широкополосных сигналов

В.В. Глубоких, Д.Д. Зыков, Н.В. Сивохина 311

СЕКЦИЯ 4. БЕЗОПАСНОСТЬ СЛОЖНЫХ ОРГАНИЗАЦИОННО-ТЕХНИЧЕСКИХ СИСТЕМ

MITM-атака привилегированным сетевым узлом посредством перехвата ACME-подтверждения

Смирнов Я. В. 318

Способы обеспечения информационной безопасности в каналах управления беспилотными транспортными системами

Будко Д. Д. 331

Архитектура потоковой передачи телеметрических данных для систем интеллектуального мониторинга объектов водного транспорта

Груздев А. А. 340

Методика многофакторного мониторинга и адаптивного восстановления критических сервисов распределенных программно-аппаратных комплексов связи

Прохоркин Д. А. 346

Анализ способов защиты мультисервисных сетей связи от DDoS-атак

Жеглов П. И., Гречишникова Т. А. 356

Метод оптической локации для обнаружения короткофокусных систем видеонаблюдения

Тихонов П. Ю., Смирнов М. В., Машков И.А. 362

Системный анализ критических сценариев и рисков функционирования телекоммуникационных систем космических комплексов

Прокофьев М. Ю. 372

Математическая модель речевого сигнала при передаче по цифровому каналу связи

Токарева У. В., Казакова Е. А., Андреев Р. А. 377

Метод оценки генераторов случайных чисел на основе расчета циклической автокорреляционной функции без нулевого смещения

Касьянов А. В. 386

Модельный базис построения системы управления информационной безопасностью гетерогенных распределенных IT-объектов в условиях таргетированных киберугроз

Фоменко К. Э., Голицын С. А., Момонов В. М. 392

Определение оптимальной комбинации шумовой и речеподобной помехи для снижения эффективности автоматического распознавания речи

Рамзаев В. А., Фесько Н. В., Шульженко А. Д. 401

СЕКЦИЯ 5. ПОДГОТОВКА КАДРОВ ДЛЯ IT-ОТРАСЛИ

Особенности применения искусственного интеллекта в системе инженерного образования

Комашинский В. И., Бирюков А. В. 407

Оценка результативности нейросетевых моделей в задачах высокоточной сегментации изображений городской застройки при наличии сложных условий освещения и текстур

Галайчук К. В., Орлов А. А. 416

Научное издание

Образовательно-производственный кластер (навигация, коммуникации, безопасность)

Сборник докладов Первой межведомственной научно-технической конференции

г. Санкт-Петербург, 20–21 августа 2026 года

Издается в авторской редакции
Печатается из оригинал-макета, подготовленного авторами

Подписано в печать 16.09.2026.
Формат 60×84/8
Объем 53,75 п.л.
Тираж 5 экз.