ТЕЛЕКОММУНИКАЦИИ и СВЯЗЬ

№ 4 (07) 2025

ТЕМА НОМЕРА:

РАСПОЗНАВАНИЕ ЦЕЛЕЙ, НЕЙРОСЕТИ И ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ

СИНТЕЗ СТРУКТУРЫ УЗЛА СВЯЗИ ПОЛЕВОГО ПОДВИЖНОГО ПУНКТА УПРАВЛЕНИЯ

WWW.TELEMIL.RU

DOI: 10.21681/3034-4050

ТЕЛЕКОММУНИКАЦИИ И СВЯЗЬ

НАУЧНЫЙ РЕЦЕНЗИРУЕМЫЙ ЖУРНАЛ
№ 4 (07) 2025 г.
Выходит 6 раз в год

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

Журнал специализируется на публикации статей по специальностям перечня научных специальностей 6.0.0.

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

Над номером работали:
Г. И. Макаренко – *шеф-редактор*, Н. В. Селезенев – *отв. секретарь*, С. С. Игнатов – *верстка*, А. М. Старков – *маркетинг и подписка*

Подписано к печати 15.08.2025 г.
Общий тираж 120 экз. Цена свободная

Адрес: 141006, г. Мытищи Московской обл., 1-й Рупасовский пер.
E-mail: editor.tis@yandex.ru, тел.: +7 (995) 153-43-88

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

СОДЕРЖАНИЕ

Подписка на журнал осуществляется в 2025 году через редакцию журнала

ПРИМЕНЕНИЕ ТЕХНОЛОГИИ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА И МАШИННОГО ЗРЕНИЯ В БОРЬБЕ С АНТИТЕРРОРИСТИЧЕСКОЙ ДЕЯТЕЛЬНОСТЬЮ

Саенко И. Б.[1]

DOI:10.21681/3034-4050-2025-4-2-9

Ключевые слова: *терроризм; машинное обучение; глубокое обучение; обработка изображений; распознавание лиц; обнаружение аномалий; предиктивная аналитика; социальные сети.*

Аннотация

Цель: *анализ содержания и возможностей применения технологий искусственного интеллекта и машинного зрения, которые могут быть применены в антитеррористической деятельности, и формулировка проблем, свойственных этой предметной области, с обоснованием направлений их решения.*

Метод: *системный анализ антитеррористической деятельности и технологий искусственного интеллекта, направленный на выявление проблемной ситуации в новой предметной области.*

Результат: *обосновывается необходимость применения технологии искусственного интеллекта и машинного зрения для повышения эффективности антитеррористической деятельности. Дается характеристика ключевых технологий искусственного интеллекта и машинного зрения, оказывающих существенное воздействие на защиту от терроризма, таких как обработка изображений, распознавание лиц, обнаружение аномалий, предиктивная аналитика и мониторинг социальных сетей. Обсуждаются новые проблемы, порождаемые использованием искусственного интеллекта и машинного зрения, связанные с подготовкой обучающих наборов данных и этичностью применения инструментария искусственного интеллекта.*

Научная новизна: *анализ работ по тематике применения технологий искусственного интеллекта и машинного зрения в области борьбы с терроризмом впервые показал, что в наибольшей степени здесь могут быть применимы технологии обработки изображений и распознавание лиц, обнаружения аномалий, предиктивная аналитика и мониторинг социальных сетей. Применение этих технологий в интересах антитеррористической деятельности приводит к возникновению новых проблем, требующих своего скорейшего решения, которые обусловлены необходимостью качественной подготовки обучающих наборов данных и разработки новых нравственных и юридических норм, касающихся применения инструментария искусственного интеллекта.*

Введение

В настоящее время террористическая деятельность стала одной из основных угроз национальной и общественной безопасности, с которой сталкиваются все страны мира, включая Российскую Федерацию. Характерным примером является теракт, совершенный мигрантами в Москве в «Крокус Сити Холле» 22 мая 2024 года, унесший жизни более 60 человек. К числу последних резонансных террористических событий также следует отнести теракты, в которых погибли одни из высших руководителей нашего военного ведомства – генерал-лейтенант Кириллов И. А. в декабре 2024 года и генерал-лейтенант Москалик Я. Я. в апреле 2025 года. Причем последние два теракта были организованы практически по одной и той же схеме.

Одной из причин, затрудняющей антитеррористическую деятельность и предотвращение терактов, является необходимость обеспечения демократических свобод гражданского населения страны. Противоречие между усилением антитеррористической деятельности, направленной на защиту граждан от внутренних угроз безопасности, и соблюдением прав и свобод личности, которые составляют основу демократического общества, требует своего скорейшего разрешения. Существует

1 Саенко Игорь Борисович, доктор технических наук, профессор, профессор кафедры автоматизированных систем специального назначения Военной академии связи имени Маршала Советского Союза С. М. Будённого, Санкт-Петербург, Россия. E-mail: ibsaen@mail.ru

настоятельная потребность в овладении стратегиями, которые не только смягчают угрозу терроризма, но и защищают основные права и свободы, характерные для открытого демократического общества [1, 2]. Одно из возможных, но достаточно эффективных направлений разрешения этого противоречия видится в применении технологии искусственного интеллекта (ИИ) и машинного зрения в интересах антитеррористической деятельности [3, 4].

ИИ получил значительное внимание и достаточно широкое распространение во всем мире как инструмент, который может обрабатывать в реальном или сопоставимом с реальным масштабе времени огромные объемы данных и обнаруживать закономерности и корреляции в данных, невидимые человеческому глазу, что может повысить эффективность и результативность анализа сложной информации [5]. Однако, несмотря на высокие уровень интеграции ИИ в общество и частоту популярного использования этого термина, универсального определения ИИ не существует. Этот термин обычно понимается для описания дисциплины, связанной с разработкой технологических инструментов, использующих такие человеческие качества, как планирование, обучение, рассуждение и анализ [6]. Наиболее популярными в настоящее время разделами этой научной дисциплины являются методы машинного, в том числе глубокого, обучения. В большинстве случаев применение этих методов ассоциируется с искусственными нейронными сетями. Однако и другие области, такие как обработка нечётких данных (нечётких алгоритмов, нечётких моделей, нейро-нечётких сетей и т.д.) [7] или применение биоинспирированных подходов (эволюционных алгоритмов, методов роевого интеллекта и т.д.) [8], также имеют важное значение.

Под машинным зрением понимается применение компьютерного зрения для промышленности и производства. При этом компьютерное зрение представляет собой общий набор методов, позволяющих компьютерам видеть, в то время как предметной областью машинного зрения, как инженерного направления, являются цифровые устройства ввода-вывода и компьютерные сети, предназначенные для контроля производственного оборудования, такие, например, как роботы-манипуляторы [9]. Таким образом, машинное зрение является подразделом инженерии, связанным с вычислительной техникой, оптикой, машиностроением и промышленной автоматизацией. При этом в последнее время машинное зрение, как и компьютерное зрение в целом, тесно связывается с решением задач распознавания изображений с применением нейронных сетей [10]. Поэтому вполне правомерно считать машинное зрение одним из направлений ИИ [11], которое также имеет особую важность для совершенствования антитеррористической деятельности.

Целью настоящей статьи является рассмотрение возможностей и проблем применения ИИ, включая машинное зрение, в интересах антитеррористической деятельности.

Возможности применения ИИ в интересах антитеррористической деятельности

ИИ привлекает всеобщее внимание способностью обрабатывать большие наборы данных, выявляя при этом скрытые закономерности и идеи, которые зачастую остаются недоступными для человеческого анализа. Эта способность значительно повышает эффективность и результативность анализа сложной информации. Преимущества ИИ, как многогранной технологии, распространяются на многочисленные области, включая борьбу с терроризмом. В этой сфере возможности ИИ являются бесценными и проявляются в быстрой расшифровке и интерпретации сложных данных, что позволяет считать ИИ кладезем инновационных методов обнаружения потенциальных угроз и формулирования эффективных превентивных стратегий. Использование ИИ в борьбе с терроризмом не только демонстрирует его существенный потенциал в организации безопасности и обороны, но и подчеркивает его преобразующее влияние на различные секторы, подчеркивая его важную роль в современных аналитических методологиях.

Прежде всего, крайне важно признать глубокую зависимость технологии ИИ от данных. Без точных и надежных данных для обучения моделей ИИ, особенно в борьбе с терроризмом, существует значительный риск не в полной мере использовать эту новаторскую технологию для решения самых насущных проблем антитеррористической деятельности. По сути, ИИ работает,

тщательно изучая большие наборы данных для выявления закономерностей и составления прогнозов. Учитывая уникальные возможности систем ИИ, задача заключается в навигации по этим огромным резервам данных для извлечения действенных идей. В нынешнюю эпоху, переполненную данными — от взаимодействий в социальных сетях и финансовых транзакций до видеозаписей видеонаблюдения в общественных местах – постоянно собирается огромный объем данных. Этот взрыв «больших данных» представляет собой палку о двух концах: с одной стороны, есть возможность, а с другой – существует проблема их эффективного использования. Поэтому в качестве ключевых технологий ИИ, которые могут быть достаточно эффективно использоваться в антитеррористической деятельности, следует выделить следующие:

- обработка изображений и распознавание лиц;
- обнаружение аномалий;
- предиктивная аналитика;
- мониторинг социальных сетей.

Эти технологии ИИ являются важными инструментами для укрепления мер, а также идентификации и предотвращения потенциальных угроз безопасности. Рассмотрим эти технологии подробнее.

Технология **обработки изображений и распознавания лиц** может значительно повысить меры безопасности, выявляя известных или предполагаемых террористов в режиме реального времени в различных условиях и локациях, таких как аэропорты, вокзалы и публичные мероприятия. По сути, эта технология, используя средства машинного зрения, сканирует лица в толпе, чтобы сопоставить их с базами данных известных лиц. Кроме того, последние разработки в технологической отрасли сделали обычным явлением использование камер на базе ИИ, способных обнаруживать даже оружие.

Используя существующие сети средств машинного зрения в таких масштабных средах, как школы, аэропорты или корпоративные кампусы, алгоритмы могут обнаруживать огнестрельное оружие или дробовики. Сначала система помечает огнестрельное оружие оранжевым цветом как подозрительное, а затем в течение нескольких секунд быстро переходит на красный уровень тревоги [12]. Сотрудник службы безопасности получает уведомление на свой мобильный телефон; впоследствии программное обеспечение предоставляет неподвижное изображение, на котором подробно описано огнестрельное оружие и идентифицируется подозреваемый. Это облегчает процесс принятия решения о том, следует ли задействовать службы быстрого реагирования или отклонить оповещение как ложную тревогу. Например, ИИ может различать пистолет и головку разбрызгивателя. Тем не менее, как упоминалось выше, эта технология в значительной степени опирается на огромные объемы данных, которые необходимо уточнить. Поскольку она продолжает собирать видеоданные и совершенствовать алгоритмы и модели для лучшего распознавания объектов, можно ожидать, что с течением времени точность будет неуклонно повышаться. Однако внедрение технологии обработки изображений и распознавания лиц вызывает опасения относительно конфиденциальности, потенциальной предвзятости и точности идентификации лиц в разных демографических группах.

Технология **обнаружения аномалий** на базе ИИ играет ключевую роль в борьбе с терроризмом, потому что она позволяет выявлять отклонения от обычных моделей и поведения. Системы обнаружения аномалий отлично раскрывают подозрительную деятельность в финансовых транзакциях, схемах поездок и онлайн-коммуникациях, выступая в качестве упреждающих инструментов для раннего обнаружения потенциальных угроз. Их эффективность в упреждающем выявлении угроз помогает предотвращать атаки до их возникновения, уделяя особое внимание сокращению ложных срабатываний и сохранению конфиденциальности.

Особенно важно обнаружение аномалий с помощью ИИ в сфере отчетов о подозрительной деятельности (ОПД) [13]. ОПД, необходимые для обнаружения и противодействия финансовым преступлениям, таким как отмывание денег и финансирование терроризма, традиционно сложны из-за необходимости фильтрации огромных объемов транзакционных данных. ИИ упрощает этот процесс, объединяя скорость, точность и эффективность, чтобы финансовые учреждения могли более эффективно выявлять аномалии. При этом возможно использование предварительно сформированных наборов данных о террористической деятельности, например, Global

Terrorism Database (GTD) [14]. Используя передовое машинное обучение и распознавание образов, ИИ улучшает процесс формирования ОПД, предоставляя возможности мониторинга в реальном времени, которые значительно уменьшают возможность того, что финансовые преступления останутся незамеченными. Тем не менее, включение ИИ в соответствие с требованиями ОПД создает проблемы, включая этические соображения и конфиденциальность данных, а также необходимость идти в ногу с меняющимися правилами. Несмотря на эти препятствия, сохраняется критическая роль человеческого суждения, особенно для оценки сложных или неопределенных ситуаций, выявленных ИИ.

Технология **прогнозной аналитики** использует исторические данные и алгоритмы ИИ для прогнозирования будущих событий, включая потенциальные террористические угрозы [15]. Анализируя огромные объемы данных, включая сообщения, транзакции и перемещения, прогнозные модели могут подсказать, когда и где может произойти террористический акт. Хотя этические соображения относительно наблюдения и риска профилирования многообещающие, они требуют тщательного управления. Кроме того, надежность прогнозов и потенциальная возможность чрезмерной зависимости от автоматизированных систем являются критическими проблемами.

Внедрение такой технологии сталкивается с трудностями, особенно из-за ограничений данных. Террористические атаки с различными мотивами и методами создают уникальные цифровые следы, на которые влияют такие факторы, как убеждения или психическое здоровье, количество участников и режимы связи (возможно, зашифрованные). Выявление закономерностей в пределах одного набора данных затруднено, но улучшается с помощью анализа кросс-наборов данных, который требует детального изучения и увеличивает размерность набора данных. Алгоритмы машинного обучения для массового наблюдения должны обучаться на различных наборах данных, чтобы эффективно обнаруживать закономерности. Это вводит «проклятие размерности» в больших данных, где более сложные наборы данных препятствуют статистическому анализу, снижая точность и производительность алгоритма. Более подробная информация о каждом подозреваемом повышает точность, но требует больших наборов данных, что делает скудные задокументированные террористические атаки недостаточными для тщательного обучения.

С другой стороны, глубокие нейронные сети, такие как известные своей точностью сверточные [16] и рекуррентные [17], значительно усиливают структуру предиктивной аналитики. Превосходно справляясь с распознаванием сложных образов в больших наборах данных, эти типы нейронных сетей хорошо подходят для задач прогнозирования, так как они способны моделировать сложные многомерные данные, не снижая точность прогноза. Благодаря обширному обучению на исторических и текущих данных эти сети достигают более высокой точности прогнозирования, чем многие статистические методы. Их многослойная обработка обеспечивает понимание данных, необходимое для точного прогнозирования результатов в различных контекстах. Глубокие сети также совершенствуют процесс принятия решений, предлагая механизмы визуализации и оценки, тем самым обеспечивая более точные и обоснованные решения. Эти сети могут смягчить некоторые проблемы, вызванные проклятием размерности, путем постепенного уменьшения размерности данных. Это делает их ценным инструментом в предиктивной аналитике и других областях, требующих сложного анализа наборов данных.

Технология **мониторинга социальных сетей** вызывает в последние годы значительный интерес в связи с тем, что объемы данных, связанных с поведением людей в Интернете, особенно на платформах социальных сетей, претерпевает значительное увеличение [18]. Исследователи и службы безопасности усердно изучают использование данных социальных сетей для прогнозирования террористической деятельности. Это исследование основано на убеждении, что закономерности использования и взаимодействия в социальных сетях могут раскрыть важную информацию о намерениях, связях и потенциальных планах человека, что делает их критически важным активом для упреждающего устранения угроз. Действительно верно, что террористические группы часто используют

социальные сети для пропаганды, вербовки и общения. Использование ИИ для мониторинга этих платформ помогает выявлять и пресекать такую деятельность. Технологии ИИ, такие как большие языковые модели [19], искусно анализируют текст, изображения и видео на предмет экстремистского контента, помечая их для последующего просмотра человеком. Эффективность этих инструментов ИИ зависит от их способности понимать контекст и нюансы, тем самым снижая вероятность ошибочной цензуры законного контента при точном выявлении подлинных угроз.

Проблемы применения ИИ в интересах антитеррористической деятельности

В 2017 году в ходе Всероссийского открытого урока Президент России В. В. Путин сделал историческое заявление, заявив следующее: «Искусственный интеллект – это будущее не только России, это будущее всего человечества. Здесь колоссальные возможности и трудно прогнозируемые сегодня угрозы. Тот, кто станет лидером в этой сфере, будет властелином мира. И очень бы не хотелось, чтобы эта монополия была сосредоточена в чьих-то конкретных руках». Это заявление привлекло к ИИ широкое внимание как международной общественности, так и передовых технологических лабораторий. Теперь важно понимать значение и причины потенциального влияния ИИ на национальную безопасность, являются ли его эффекты революционными или просто постепенными.

Эффективность ИИ в значительной степени зависит от качества входных данных, что подчеркивает настоятельную потребность в целостной стратегии обработки данных, которая легко интегрирует ИИ в существующие технологические структуры. Кроме того, эффективность ИИ в обработке данных определяется не только объемом данных, но и их репрезентативностью и отсутствием предвзятости, что имеет решающее значение для точной интерпретации сложного поведения человека.

ИИ играет ключевую роль в усилении усилий по борьбе с терроризмом за счет эффективной обработки и анализа больших наборов данных. Он поддерживает выявление закономерностей и связей в данных, связанных с терроризмом, таких как отчеты об инцидентах и контртеррористические мероприятия, тем самым помогая прогнозировать и предотвращать террористические угрозы.

Использование технологий машинного обучения, таких как обработка изображений, распознавание лиц, обнаружение аномалий, предиктивная аналитика и мониторинг социальных сетей, имеет жизненно важное значение для продвижения мер по борьбе с терроризмом. Эти технологии используют данные уникальным образом; например, обработка изображений и распознавание лиц помогают идентифицировать людей по визуальным данным, в то время как обнаружение аномалий выявляет необычные закономерности, которые могут сигнализировать об угрозах безопасности. Прогностическая аналитика использует исторические данные для прогнозирования будущих событий, а мониторинг социальных сетей заблаговременно обнаруживает угрожающие сообщения. Однако эти технологии часто воспринимаются скептически, рассматриваются как потенциально антиутопические и инвазивные, вызывающие опасения по поводу вторжения в личную жизнь, дискриминации и случайного вреда.

Существует настоятельная необходимость в установлении четких норм использования ИИ в сфере безопасности. Эффективное развертывание ИИ в борьбе с терроризмом требует не только сбора данных, но и этичного управления данными, приоритета конфиденциальности и безопасности данных для обеспечения того, чтобы технологические достижения приносили пользу обществу при соблюдении прав личности [20]. Баланс между улучшением безопасности и защитой свобод представляет собой значительную проблему, требующую тонкого подхода к использованию ИИ в борьбе с терроризмом, учитывающего этические дилеммы, техническую надежность и риск ошибок.

Прозрачное, регулируемое и этичное применение инструментов ИИ имеет важное значение для предотвращения терроризма при защите индивидуальных свобод и прав. Интеграция ИИ в стратегии борьбы с терроризмом представляет собой значительный шаг вперед в улучшении мер безопасности и возможностей прогнозирования. Тем не менее, преодоление этических соображений и технических проблем, связанных с его использованием, остается пока еще нерешенной проблемой.

Заключение

Дальнейшее повышение эффективности антитеррористической деятельности напрямую зависит от успеха в разрешении существующего противоречия между усилением деятельности, направленной на защиту граждан от внутренних угроз безопасности, и соблюдением демократических прав и свобод личности. Наиболее перспективным направлением разрешения этой проблемы является применение ИИ и машинного зрения. Ключевые технологии ИИ и машинного зрения, такие, как обработка изображений, распознавание лиц, обнаружение аномалий, предиктивная аналитика и мониторинг социальных сетей, позволяют эффективно обрабатывать и анализировать большие объемы данных и выявлять скрытые закономерности и идеи.

В то же время применение ИИ и машинного зрения в области борьбы с терроризмом вызывает новые проблемы, связанные с подготовкой обучающих наборов данных и этичностью применения инструментария ИИ. Преодоление этих проблем открывает путь к широкому внедрению технологий ИИ и машинного зрения в антитеррористическую деятельность и существенное повышение ее эффективности.

Литература

1. Карцхия А. А., Макаренко Г. И., Макаренко Д. Г. Правовые перспективы технологий искусственного интеллекта // Безопасные информационные технологии. Сборник трудов Двенадцатой международной научно-технической конференции. Москва, 2023. – С. 154–161. EDN: UCHFJY.
2. Карцхия А. А., Макаренко Г. И. Правовые горизонты технологий искусственного интеллекта: национальный и международный аспект // Вопросы кибербезопасности. – 2024. – № 1(59). – С. 2–14. – DOI: 10.21681/2311-3456-2024-1-2-14. EDN: JTGKFM.
3. Гедгафов М. М. Роль искусственного интеллекта в противодействии терроризму // Журнал прикладных исследований. – 2023. – № 8. – С. 91–95. DOI: 10.47576/2949-1878_2023_8_91. EDN: QSQIIR.
4. Черкесов А. Ю. Искусственный интеллект в противодействии террористическим угрозам в глобальном информационном пространстве // Пробелы в российском законодательстве. – 2023. – Т. 16, № 5. – С. 166–170. EDN: LUUCYI.
5. Канкулов А. Х., Пантелеев В. А. Искусственный интеллект как метод борьбы с преступностью и терроризмом // Аграрное и земельное право. – 2024. – № 1(229). – С. 280–282. DOI: 10.47643/1815-1329_2024_1_280. EDN: SYXWUP.
6. Лаврухин М. В. Использование искусственного интеллекта в противодействии терроризму и оптимизация требований обеспечения транспортной безопасности к объектам дорожного хозяйства // Транспортное право и безопасность. – 2022. – № 4(44). – С. 126–143. EDN: TERJNU.
7. Молотникова А. А., Акуз А. В. Гибридные нейро-нечёткие сети в криминологии // Вестник Таганрогского института имени А. П. Чехова. – 2024. – № 2. – С. 68–76. EDN: ANZQQH.
8. Котенко И. В., Шоров А. В., Нестерук Ф. Г. Анализ биоинспирированных подходов для защиты компьютерных систем и сетей // Труды СПИИРАН. – 2011. – № 3(18). – С. 19–73. EDN: OKHLLL.
9. Молотков П. П., Радайкин А. П. Методы машинного зрения в робототехнике // Наука и образование. Сборник трудов участников XVII Международной научной конференции. – Красноярск, 2025. – С. 74–77. EDN: NUYSTQ.
10. Силионов И. Н. Применение нейронных сетей в области компьютерного зрения для создания систем умного наблюдения и безопасности // Вестник науки. – 2025. – Т. 3, № 3(84). – С. 594–601. EDN: SQQJMF.
11. Сопильняк А. Ю. Современные подсистемы машинного зрения в интеллектуальных информационных системах // Advances in Science and Technology. Сборник статей LXVI международной научно-практической конференции. Москва, 2025. – С. 87–88. EDN: BELVMU.
12. Nale P., Gite S., Dharrao D. Real-Time Weapons Detection System using Computer Vision // 2023 Third International Conference on Smart Technologies, Communication and Robotics (STCR). Sathyamangalam, India, 2023. – Pp. 1–6. DOI: 10.1109/STCR59085.2023.10396960.
13. Sengupta A., Kundu A., Mukhopadhyay A. An Approach to Detect and Classify Potentially Suspicious Activity from Real-Time Log Data using Anomaly Detection Methods // 2024 3rd International Conference for Innovation in Technology (INOCON). Bangalore, India, 2024. – Pp. 1–9. DOI: 10.1109/INOCON60754.2024.10511679.

14. Abdalsalam M., Li Ch., Dahou A., Kryvinska N. Terrorism Attack Classification Using Machine Learning: The Effectiveness of Using Textual Features Extracted from GTD Dataset // Computer Modeling in Engineering & Sciences. – 2024. – Vol. 138, No. 2. – Pp. 1427–1467. DOI: 10.32604/cmes.2023.029911.
15. Pan X., Zhang T. Machine learning-based target prediction for terrorist attacks // Journal of Physics: Conference Series. – 2023. – Vol. 2577. – Article 012007, pp. 1–14. DOI: 10.1088/1742-6596/2577/1/012007.
16. Lu R., Huang J., Qu Y., Li L. Study on Combined-CNN Model for Classification of Terrorism Text // 2024 7th International Conference on Advanced Algorithms and Control Engineering (ICAACE). Shanghai, China, 2024. – Pp. 453–457. DOI: 10.1109/ICAACE61206.2024.10548392.
17. Lansky J. et al. Deep Learning-Based Intrusion Detection Systems: A Systematic Review // IEEE Access. – 2021. – Vol. 9. – Pp. 101574–101599. DOI: 10.1109/ACCESS.2021.3097247.
18. Kibtiah T. M., Miranda E., Fernando Y., Aryuni M. Terrorism, Social Media and Text Mining Technique: Review of Six Years Past Studies // 2020 International Conference on Information Management and Technology (ICIMTech). Bandung, Indonesia, 2020. – Pp. 571–576. DOI: 10.1109/ICIMTech50083.2020.9211148.
19. Hasanov I., Virtanen S., Hakkala A., Isoaho J. Application of Large Language Models in Cybersecurity: A Systematic Literature Review // IEEE Access. – 2024. – Vol. 12. – Pp. 176751–176778. DOI: 10.1109/ACCESS.2024.3505983.
20. Карцхия А. А., Макаренко Г. И. Правовые проблемы применения искусственного интеллекта в России // Правовая информатика. – 2024. – № 1. – С. 4–19. DOI: 10.21681/1994-1404-2024-1-4-19. EDN: NONHLC.

APPLICATION OF ARTIFICIAL INTELLIGENCE AND MACHINE VISION TECHNOLOGY IN THE FIGHT AGAINST ANTI-TERRORIST ACTIVITIES

***Sayenko I. B.*[2]**

Keywords: *terrorism, machine learning, deep learning, image processing, facial recognition, anomaly detection, predictive analytics, social networks.*

Abstract

Objective: *analysis of the content and possibilities of application of artificial intelligence and machine vision technologies that can be used in anti-terrorist activities, and formulation of problems inherent in this subject area, with justification of directions for their solution.*

Method: *system analysis of anti-terrorist activities and artificial intelligence technologies aimed at identifying a problem situation in a new subject area.*

Result: *the need for the use of artificial intelligence and machine vision technology to improve the effectiveness of anti-terrorist activities is substantiated. The characteristics of key technologies of artificial intelligence and machine vision that have a significant impact on protection against terrorism, such as image processing, face recognition, anomaly detection, predictive analytics and monitoring of social networks, are given. generated by the use of artificial intelligence and machine vision, related to the preparation of training datasets and the ethics of using artificial intelligence tools.*

Scientific novelty: *the analysis of works on the use of artificial intelligence and machine vision technologies in the field of counterterrorism for the first time showed that the technologies of image processing and face recognition, anomaly detection, predictive analytics and monitoring of social networks can be most applicable here. The use of these technologies in the interests of anti-terrorist activities leads to the emergence of new problems that require their immediate decisions that are due to the need for high-quality preparation of training datasets and the development of new moral and legal norms regarding the use of artificial intelligence tools.*

2 Igor B. Sayenko, Dr.Sc. (of tech.), Professor, Professor of the Department of Automated Special Purpose Systems, Military Academy of Communications named after Marshal of the Soviet Union S. M. Budyonny, St. Petersburg, Russia. E-mail: ibsaen@mail.ru

References

1. Karchija A. A., Makarenko G. I., Makarenko D. G. Pravovye perspektivy tehnologij iskusstvennogo intellekta // Bezopasnye informacionnye tehnologii. Sbornik trudov Dvenadcatoj mezhdunarodnoj nauchno-tehnicheskoj konferencii. Moskva, 2023. – S. 154–161. EDN: UCHFJY.
2. Karchija A. A., Makarenko G. I. Pravovye gorizonty tehnologij iskusstvennogo intellekta: nacional'nyj i mezhdunarodnyj aspekt // Voprosy kiberbezopasnosti. – 2024. – № 1 (59). – S. 2–14. – DOI: 10.21681/2311-3456-2024-1-2-14. EDN: JTGKFM.
3. Gedgafov M. M. Rol' iskusstvennogo intellekta v protivodejstvii terrorizmu // Zhurnal prikladnyh issledovanij. – 2023. – № 8. – S. 91–95. DOI: 10.47576/2949-1878_2023_8_91. EDN: QSQIIR.
4. Cherkesov A. Ju. Iskusstvennyj intellekt v protivodejstvii terroristicheskim ugrozam v global'nom informacionnom prostranstve // Probely v rossijskom zakonodatel'stve. – 2023. – T. 16, №5. – S. 166–170. EDN: LUUCYI.
5. Kankulov A. H., Panteleev V. A. Iskusstvennyj intellekt kak metod bor'by s prestupnost'ju i terrorizmom // Agrarnoe i zemel'noe pravo. – 2024. – № 1(229). – S. 280–282. DOI: 10.47643/1815-1329_2024_1_280. EDN: SYXWUP.
6. Lavruhin M. V. Ispol'zovanie iskusstvennogo intellekta v protivodejstvii terrorizmu i optimizacija trebovanij obespechenija transportnoj bezopasnosti k ob#ektam dorozhnogo hozjajstva // Transportnoe pravo i bezopasnost'. – 2022. – № 4(44). – S. 126–143. EDN: TERJNU.
7. Molotnikova A. A., Akuz A. V. Gibridnye nejro-nechjotkie seti v kriminologii // Vestnik Taganrogskogo instituta imeni A. P. Chehova. – 2024. – № 2. – S. 68–76. EDN: ANZQQH.
8. Kotenko I. V., Shorov A. V., Nesteruk F. G. Analiz bioinspirirovannyh podhodov dlja zashhity komp'juternyh sistem i setej // Trudy SPIIRAN. – 2011. – № 3(18). – S. 19–73. EDN: OKHLLL.
9. Molotkov P. P., Radajkin A. P. Metody mashinnogo zrenija v robototehnike // Nauka i obrazovanie. Sbornik trudov uchastnikov XVII Mezhdunarodnoj nauchnoj konferencii. – Krasnojarsk, 2025. – S. 74–77. EDN: NUYSTQ.
10. Silionov I. N. Primenenie nejronnyh setej v oblasti komp'juternogo zrenija dlja sozdanija sistem umnogo nabljudenija i bezopasnosti // Vestnik nauki. – 2025. – T. 3, № 3(84). – S. 594–601. EDN: SQQJMF.
11. Sopil'njak A. Ju. Sovremennye podsistemy mashinnogo zrenija v intellektual'nyh informacionnyh sistemah // Advances in Science and Technology. Sbornik statej LXVI mezhdunarodnoj nauchno-prakticheskoj konferencii. Moskva, 2025. – S. 87–88. EDN: BELVMU.
12. Nale P., Gite S., Dharrao D. Real-Time Weapons Detection System using Computer Vision // 2023 Third International Conference on Smart Technologies, Communication and Robotics (STCR). Sathyamangalam, India, 2023. – Pp. 1–6. DOI: 10.1109/STCR59085.2023.10396960.
13. Sengupta A., Kundu A., Mukhopadhyay A. An Approach to Detect and Classify Potentially Suspicious Activity from Real-Time Log Data using Anomaly Detection Methods // 2024 3rd International Conference for Innovation in Technology (INOCON). Bangalore, India, 2024. – Pp. 1–9. DOI: 10.1109/INOCON60754.2024.10511679.
14. Abdalsalam M., Li Ch., Dahou A., Kryvinska N. Terrorism Attack Classification Using Machine Learning: The Effectiveness of Using Textual Features Extracted from GTD Dataset // Computer Modeling in Engineering & Sciences. – 2024. – Vol. 138, No. 2. – Pp. 1427–1467. DOI: 10.32604/cmes.2023.029911.
15. Pan X., Zhang T. Machine learning-based target prediction for terrorist attacks // Journal of Physics: Conference Series. – 2023. – Vol. 2577. – Article 012007, pp. 1–14. DOI: 10.1088/1742-6596/2577/1/012007.
16. Lu R., Huang J., Qu Y., Li L. Study on Combined-CNN Model for Classification of Terrorism Text // 2024 7th International Conference on Advanced Algorithms and Control Engineering (ICAACE). Shanghai, China, 2024. – Pp. 453–457. DOI: 10.1109/ICAACE61206.2024.10548392.
17. Lansky J. et al. Deep Learning-Based Intrusion Detection Systems: A Systematic Review // IEEE Access. – 2021. – Vol. 9. – Pp. 101574–101599. DOI: 10.1109/ACCESS.2021.3097247.
18. Kibtiah T. M., Miranda E., Fernando Y., Aryuni M. Terrorism, Social Media and Text Mining Technique: Review of Six Years Past Studies // 2020 International Conference on Information Management and Technology (ICIMTech). Bandung, Indonesia, 2020. – Pp. 571–576. DOI: 10.1109/ICIMTech50083.2020.9211148.
19. Hasanov I., Virtanen S., Hakkala A., Isoaho J. Application of Large Language Models in Cybersecurity: A Systematic Literature Review // IEEE Access. – 2024. – Vol. 12. – Pp. 176751–176778. DOI: 10.1109/ACCESS.2024.3505983.
20. Karchija A. A., Makarenko G. I. Pravovye problemy primenenija iskusstvennogo intellekta v Rossii // Pravovaja informatika. – 2024. – № 1. – S. 4–19. DOI: 10.21681/1994-1404-2024-1-4-19. EDN: NONHLC.

МНОГОУРОВНЕВАЯ ЛОГИКО-ВЕРОЯТНОСТНАЯ МОДЕЛЬ ИНФОРМАЦИОННОГО ОБМЕНА В ВЕДОМСТВЕННОЙ СИСТЕМЕ УПРАВЛЕНИЯ

Потапчик Н. Н.[1], Пылинский М. В.[2]

DOI:10.21681/3034-4050-2025-4-10-21

Ключевые слова: *информационное превосходство, телекоммуникационная подсистема, информационно-техническое воздействие, дестабилизирующий фактор, безопасность информационного обмена, свойство стойкости, общий логико-вероятностный метод.*

Аннотация

Цель работы: *состоит в разработке многоуровневой логико-вероятностной модели информационного обмена со свойством стойкости в ведомственной системе управления.*

Метод исследования: *проведенное исследование основано на общенаучных методах: анализа, синтеза, абстрагирования, обобщения, моделирования, индукции, дедукции. В качестве ключевого метода обоснованно выбран и использовался общий логико-вероятностный метод, а также теория вероятностей.*

Результаты исследования: *разработана многоуровневая логико-вероятностная модель информационного обмена со свойством стойкости, включающая частные модели исследуемого процесса в уязвимых подсистемах и элементах телекоммуникационной подсистемы ведомственной системы управления. Представленная модель позволяет получить уравнения вероятностных функций свойства стойкости информационного обмена, подверженного воздействию комплекса дестабилизирующих факторов информационно-технического воздействия, установить новые количественно обоснованные зависимости между входными и выходными параметрами и оценить стойкость исследуемого процесса в ведомственной системе управления. Доказана адекватность разработанной модели. В основной части статьи с использованием представленной модели произведен расчет и оценка вероятностно-временных характеристик свойства стойкости информационного обмена в информационном направлении ведомственной системы управления. Результаты оценки указывают на необходимость разработки организационно-технических мероприятий, направленных на обеспечение безопасности информационного обмена в ведомственных системах управления.*

Научная новизна: *представленная многоуровневая логико-вероятностная модель позволяет: выявить закономерности динамики прохождения информационного обмена в ведомственных системах управления; использовать стратифицированный подход, который на основе базовой логико-вероятностной модели информационного обмена, позволяет создавать схемы функциональной целостности исследуемого процесса любого уровня декомпозиции в системах управления различной топологической структуры; учитывать динамику информационного противоборства посредством задания временных параметров дестабилизирующих факторов информационно-технического воздействия.*

Введение

В современных условиях на потенциальные угрозы и вызовы динамично изменяющейся обстановки адекватнее и быстрее сможет реагировать тот участник, управление которого будет более эффективным [1]. Основным мероприятием организации управления является создание системы управления (СУ), важнейшим элементом которой является информационная система (ИС), выполняющая задачи информационного обеспечения процесса управления. В информационных процессах, протекающих в СУ, можно выделить две сугубо отличающиеся по целям и выполняемым задачам компоненты: процесс доставки информации (информационный обмен)

1 Потапчик Николай Николаевич, адъюнкт кафедры связи факультета связи и автоматизированных систем управления Военной академии Республики Беларусь, г. Минск, Республика Беларуссия. E-mail: nikpotapchik89@gmail.com

2 Пылинский Максим Валерьевич, доктор военных наук, профессор, начальник кафедры связи факультета связи и автоматизированных систем управления Военной академии Республики Беларусь, г. Минск, Республика Беларусь. E-mail: pylinskii.maksim@mail.ru

от субъекта управления к объекту управления и процессы обработки, преобразования и использования полученной информации при решении управленческих задач[3]. Как следствие, ИС ведомственной СУ представляет собой совокупность взаимосвязанных телекоммуникационной подсистемы (ТП) и подсистемы обработки информации.

Из всей совокупности информационных процессов, реализуемых ИС, главенствующая роль отводится информационному обмену между распределенными в пространстве объектами управления, что объясняется неизбежностью разрушения самой СУ при ослаблении или потери информационных связей между ее элементами, а также зависимостью уровня управления от объема передаваемой информации [2]. Удовлетворение потребностей ведомственной СУ в передаче заданного объема информации обеспечивается функционированием ее ТП.

Особенностями построения современных ведомственных ТП является использование в качестве транспортной составляющей сети электросвязи общего пользования (СЭОП) [3], а также применение технологий, средств связи (СС) и программного обеспечения (ПО) иностранного производства, имеющих потенциальные уязвимости и незадекларированные возможности [4]. Данные обстоятельства существенно повышают возможности противоборствующей стороны (силовых структур иностранных государств, террористических организаций и отдельных злоумышленников) по осуществлению информационно-технического воздействия (ИТВ), направленного на завоевание и удержание информационного превосходства в информационном пространстве [5–7]. К существенным факторам ИТВ, создающим угрозы процессу обмена информацией в ведомственной СУ, относятся программно-техническое воздействие (ПТВ) и электронное воздействие (ЭВ) преднамеренными радиоэлектронными помехами (ПРП) [2, 6].

Проведенный анализ фактов реализации ПТВ в различных странах мира показал, что в большинстве случаев для нарушения (блокирования) информационного обмена в системах управления различного назначения использовались комплексные кибератаки «Отказ в обслуживании, DDoS-атака» (ККА), которые в своем составе включают этапы ведения сетевой разведки (СР) и реализации распределенной кибератаки «Отказ в обслуживании, DDoS-атака» [8]. Массовое применение указанных ККА вызвано высокой эффективностью, а также относительной простотой реализации и невысокой стоимостью осуществления [9].

Безопасность является одним из главных требований, предъявляемых СУ к информационному обмену. Указанное свойство характеризует способность исследуемого процесса противостоять несанкционированному получению, уничтожению и изменению информации, передаваемой (принимаемой) с использованием технических СС, а также противостоять нарушению обмена информацией вследствие оказания воздействий всех видов на ТП и ее элементы [2]. Из приведенного определения следует, что безопасность информационного обмена отражает состояние защищенности информации и процесса ее передачи в ТП СУ и характеризуется набором следующих свойств: конфиденциальностью и целостностью передаваемой информации, а также стойкостью информационного обмена. Показателями конфиденциальности и целостности являются коэффициент закрытия $K_{\text{з ИО}}$ и вероятность ввода ложной информации $P_{\text{вли}}$. Показателями стойкости информационного обмена – коэффициент стойкости $K_{\text{ст ИО}}$, представляющий собой отношение времени прохождения информационного обмена с вероятностью не меньше требуемой, к суммарному времени обеспечения управления, а также функция стойкости $F_{\text{ст ИО}}(t)$, имеющая смысл распределения вероятности времени прохождения информационного обмена без нарушения (блокирования) в СУ и отображающую динамику изменения стойкости информационного обмена во времени с учетом воздействия комплекса дестабилизирующих факторов (ДФ) [2].

Постановка задачи

Проведенный анализ трудов, посвященных исследованию информационных процессов, протекающих в ведомственных СУ, выявил отсутствие исчерпывающей, не требующей уточнения и пересмотра модели информационного обмена со свойством стойкости, позволяющей выявить закономерности динамики прохождения исследуемого процесса в условиях воздействия комплекса ДФ ИТВ.

3 Боговик А. В., Игнатов В. В. Эффективность систем военной связи и методы ее оценки. СПб.: ВАС, 2006. 184 с.

С учетом вышеизложенного актуализируется задача по созданию такой модели, включающей частные модели информационного обмена в уязвимых подсистемах и элементах ТП, и позволяющей получить уравнения вероятностных функций свойства стойкости, отражающих способность информационного обмена противостоять нарушению (блокированию) в результате воздействия комплекса ДФ ИТВ, установить новые количественно обоснованные зависимости между входными и выходными параметрами и оценить стойкость информационного обмена в соответствии с заданными критериями состояния управления.

Решение задачи

Основным методическим приемом для исследования процесса, реализацию которого обеспечивает структурно-сложная система, является рассмотрение данного процесса в отдельных ее элементах, которые в совокупности обеспечивают выполнение указанного процесса всей системой.

Анализ особенностей построения топологических структур ТП, обеспечивающих передачу заданного объема информации [10], позволил декомпозировать исследуемый процесс в ведомственной СУ на уровни информационного обмена в СС, аппаратной (станции), информационном направлении (ИН) и ТП в целом. Учет функционального аспекта свойства стойкости исследуемого процесса видится особенно важным при сохранении иерархичной структуры уровней декомпозиции информационного обмена в элементах ТП, структурно-логические взаимосвязи которых образуют информационные пути прохождения информации в ведомственной СУ. Нарушение (блокирование) информация в результате воздействия ДФ даже в одном системообразующем элементе в цепи объектов связи ТП, через которые информационного обмена последовательно проходит от субъекта к объекту управления, может привести к снижению степени обеспечения управления, вплоть до его срыва.

На рис. 1 представлена иерархическая структура уровней декомпозиции информационного обмена на примере одного ИН ведомственной СУ, из которой можно сделать вывод, что фундаментом разрабатываемой многоуровневой модели является уровень информационного обмена в СС. Как следствие, указанный уровень декомпозиции принят в качестве базового. Поскольку прохождение информационного обмена в ведомственной СУ определяется структурно-логическими взаимосвязями ее элементов, совокупность моделей исследуемого процесса в условном объекте связи (ОС) позволила создать модели более высоких уровней декомпозиции.

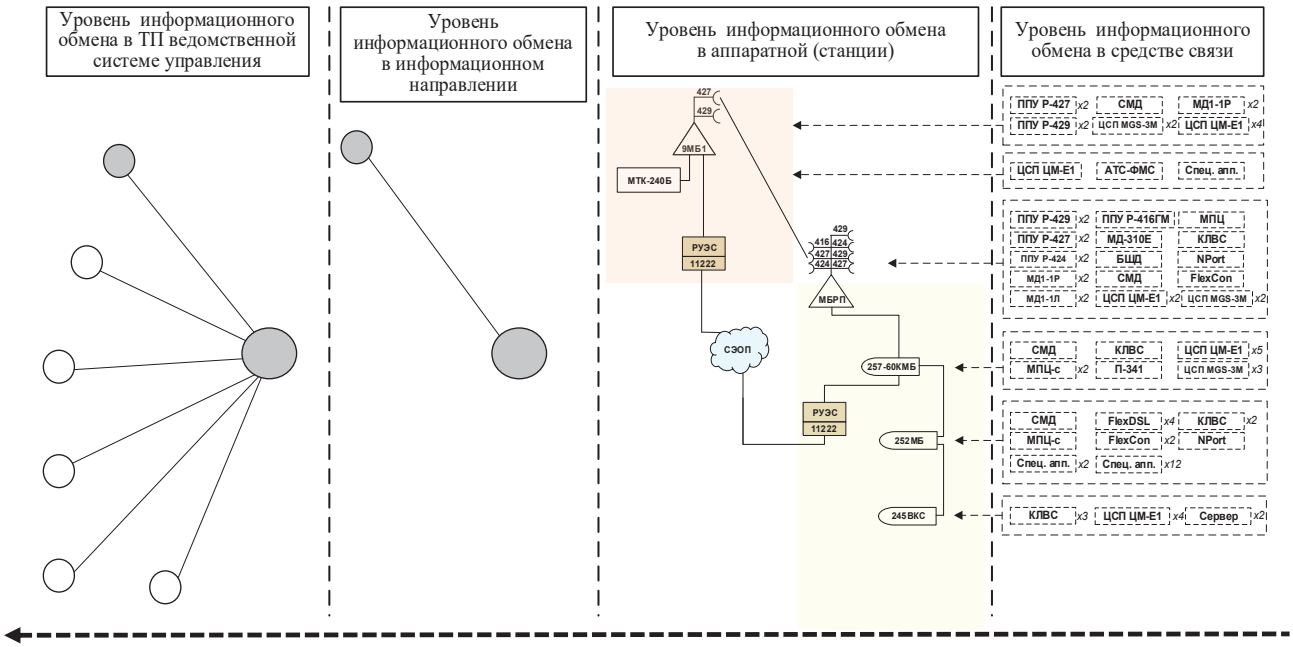

Рис. 1. Иерархичная структура уровней декомпозиции информационного обмена на примере одного информационного направления ведомственной системы управления

Анализ возможностей отечественных и зарубежных методов по решению задач вероятностно-временного моделирования процессов, реализуемых структурно сложными системами, показал, что для решения подобных задач необходимо отдавать предпочтение логико-вероятностным методам. Указанный класс методов позволяет формализовать исходную постановку задачи и создавать модели процесса аналитическими и структурно-логическими средствами, а определение искомых показателей выполняется с использованием средств теории вероятностей. Кроме того, заложенные процедуры преобразования исходных моделей в искомые расчетные математические позволят без дополнительных сложностей алгоритмизировать их с последующей реализацией на электронных вычислительных машинах.

Среди логико-вероятностных методов исследования (методы на основе схем деревьев отказов, деревьев событий, блок-схем, графов состояний и переходов) выделяют общий логико-вероятностный метод (ОЛВМ), создание которого было вызвано необходимостью расширения инструментария указанных методов. Так, по сравнению с другими подобными инструментами ОЛВМ обладает существенными преимуществами[4]:

- ❖ в ОЛВМ уже реализованы все основные возможности как метода деревьев отказов, так и метода блок-схем;
- ❖ реализованная в ОЛВМ функционально полная база логических операций «и», «или» и «не» обеспечивает возможность теоретической разработки и программной реализации методов моделирования и расчетных методик как монотонного, так и немонотонного моделирования процессов различного назначения в структурно сложных системах;
- ❖ ОЛВМ позволяет пользователю выбирать и применять разные подходы (прямой, обратный и их смешанные комбинации) к постановке задач моделирования.

Таким образом, приведенные достоинства позволяют обоснованно выбрать ОЛВМ в качестве универсального средства, наиболее пригодного для решения задач настоящего исследования.

4 Применение общего логико-вероятностного метода для анализа технических, военных организационно-функциональных систем и вооруженного противоборства: моногр. / В. И. Поленин [и др.]; под ред. проф. А. С. Можаева. – СПб.: НИКА, 2011. 410 с.

В целях решения поставленной задачи с помощью возможностей ОЛВМ была разработана модель информационного обмена со свойством стойкости в условном ОС (базовая модель), подверженного воздействию комплекса ДФ ИТВ (рис. 2).

Для задания прогнозируемого сценария воздействия комплекса ДФ ИТВ в представленную модель введены функциональные вершины 3, 4, которые отражают вероятности появления ПТВ в виде ККА и ЭВ в виде ПРП, и позволяют задавать (изменять) сценарий дестабилизирующего воздействия.

Указанные вершины принимают одно из двух значений булева множества: «1» – при осуществлении события (возникновении ДФ), «0» – при его отсутствии – и являются обеспечивающими по отношению к вершинам 1, 2.

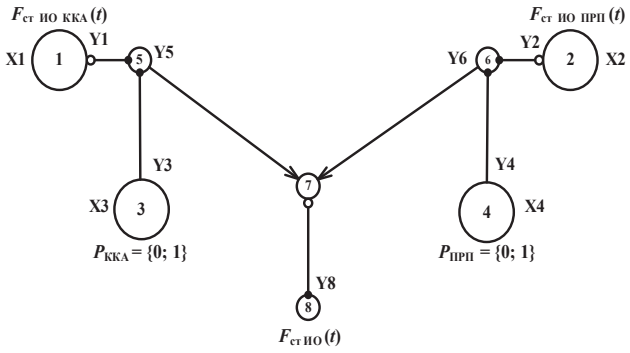

Рис. 2. Модель информационного обмена со свойством стойкости в условном объекте связи

Вершины 1 и 2 отражают функции распределения вероятности времени прохождения информационного обмена без нарушения (блокирования) при воздействии ДФ и отражают его стойкость в условном ОС. В свою очередь фиктивная вершина 8 отражает логическое условие сохранения стойкости информационного обмена в условном ОС.

Логическая функция стойкости информационного обмена в условном ОС описывается равенством

$$Y_{\text{ст ИО}} = x_1 \cdot x_2 \vee \overline{x_3} \cdot x_2 \vee x_1 \cdot \overline{x_4},$$

а вероятностная функция с учетом перехода от вероятностных мер к функциям распределения вероятности времени реализации ДФ – выражением

$$F_{\text{ст ИО}}(t) = F_{\text{ст ИО ККА}}(t) \cdot F_{\text{ст ИО ПРП}}(t) + Q_{\text{ККА}} \cdot Q_{\text{ст ИО ККА}}(t) \cdot F_{\text{ст ИО ПРП}}(t) + Q_{\text{ПРП}} \cdot Q_{\text{ст ИО ПРП}}(t) \cdot F_{\text{ст ИО ККА}}(t),$$

где $F_{\text{ст ИО ККА}}(t)$, $F_{\text{ст ИО ПРП}}(t)$ – функции распределения вероятности времени прохождения информационного обмена без нарушения (блокирования) при воздействии ККА и ПРП; $P_{\text{ККА}}$, $P_{\text{ПРП}}$ – вероятности появления ККА и ПРП; $Q_{\text{ККА}}$, $Q_{\text{ПРП}}$ и $Q_{\text{ст ИО ККА}}(t)$, $Q_{\text{ст ИО ПРП}}(t)$ – величины, обратные $P_{\text{ККА}}$, $P_{\text{ПРП}}$ и $F_{\text{ст ИО ККА}}(t)$, $F_{\text{ст ИО ПРП}}(t)$ соответственно.

Разработанная базовая модель предполагает возможность учитывать и иные ДФ, приводящие к срыву (блокированию) информационного обмена в ведомственной СУ, путем включения в ее структуру дополнительных функциональных вершин, характеризующих свойство стойкости исследуемого процесса в условиях их воздействия.

Для доказательства адекватности представленной модели в ее структуру были введены дополнительные фиктивные вершины (рис. 3). Отражая результаты прямого и обратного подходов к оценке свойства стойкости информационного обмена, фиктивные вершины 9 и 10 являются противоположными по смыслу и образуют полную группу событий, а следовательно, сумма их вероятностей должна быть равна единице, что подтверждают проведенные расчеты по оценке адекватности модели с произвольными исходными данными.

Поскольку аппарат ОЛВМ является математически строгим и позволяет достаточно точно представлять в разрабатываемой модели все существенные логические связи, отношения и зависимости, на основании непротиворечивости полученных результатов и полного

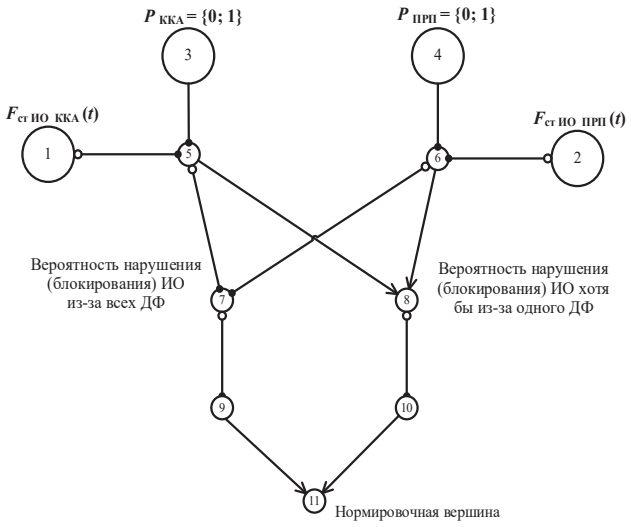

Рис. 3. Модель информационного обмена в условном объекте связи с нормировочной вершиной

подобия эталонному процессу можно утверждать, что базовая модель, а следовательно, и схемы функциональной целостности (СФЦ) информационного обмена более высоких уровней декомпозиции, построенные на ее основе, адекватны моделируемому процессу.

Моделирование информационного обмена более высоких уровней декомпозиции (рис. 1) основывается на идее агрегирования базовой модели в СФЦ информационного обмена в аппаратных (станциях), ИН и ТП ведомственной СУ с учетом структурно-логических взаимосвязей СС, входящих в их состав. Причем любой уровень декомпозиции исследуемого процесса может быть представлен как в виде разработанной базовой модели, так и в виде совокупности взаимосвязанных базовых моделей информационного обмена во вложенных элементах ТП.

В соответствии с приведенной схемой (рис. 4) модель информационного обмена в ведомственной СУ может быть представлена как:

- совокупность СФЦ информационного обмена в ИН, представленных в виде базовой модели (на рис. 4 – переход от блока 1.1 к блоку 2.2), а также в виде совокупности взаимосвязанных СФЦ информационного обмена в аппаратных (станциях), представленных в виде базовой модели (на рис. 4 – переход от блока 1.2 к блоку 3.2);
- совокупность СФЦ информационного обмена в ИН, которые на своем уровне могут быть представлены в виде совокупности взаимосвязанных СФЦ исследуемого процесса в аппаратных (станциях) (на рис. 4 – переход от блока 1.1 к блоку 2.1). Аппаратные (станции) в свою очередь могут быть представлены базовой моделью (на рис. 4 – переход от блока 1.1 к блоку 2.1 с последующим переходом к блоку 3.2), так и совокупностью взаимосвязанных СФЦ информационного обмена в СС, входящих в их состав (на рис. 4 – переход от блока 1.1 к блоку 2.1, далее к блоку 3.1 с последующим переходом к блоку 4.1);
- совокупность взаимосвязанных СФЦ информационного обмена в аппаратных (станциях), которые на своем уровне могут быть представлены совокупностью СФЦ исследуемого процесса в СС, входящих в их состав (на рис. 4 – переход от блока 1.2 к блоку 3.1 с последующим переходом к блоку 4.1).

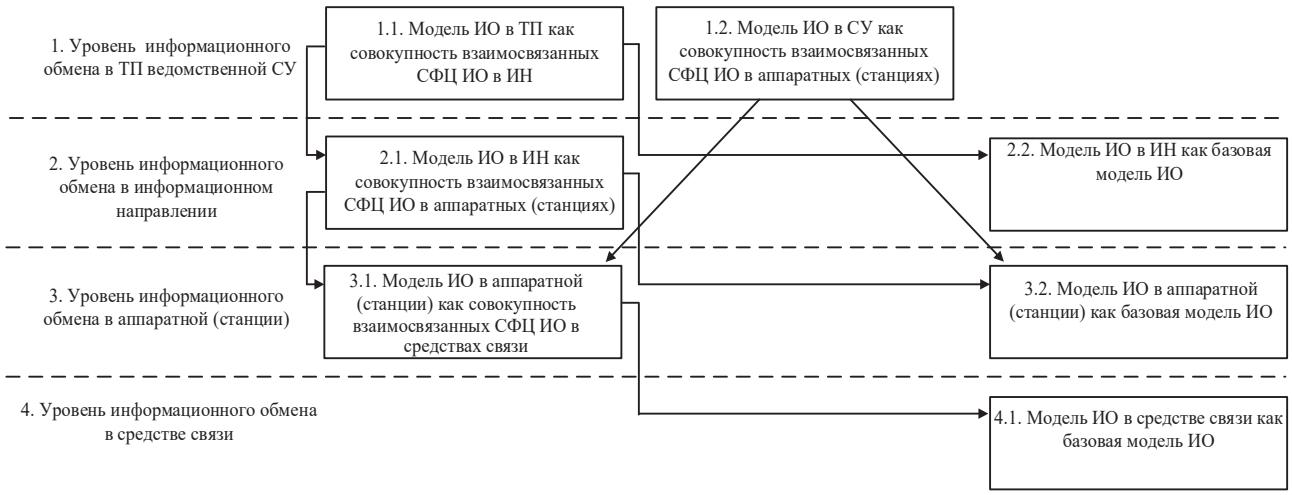

Рис. 4. Возможные варианты представления модели информационного обмена в ведомственной системе управления

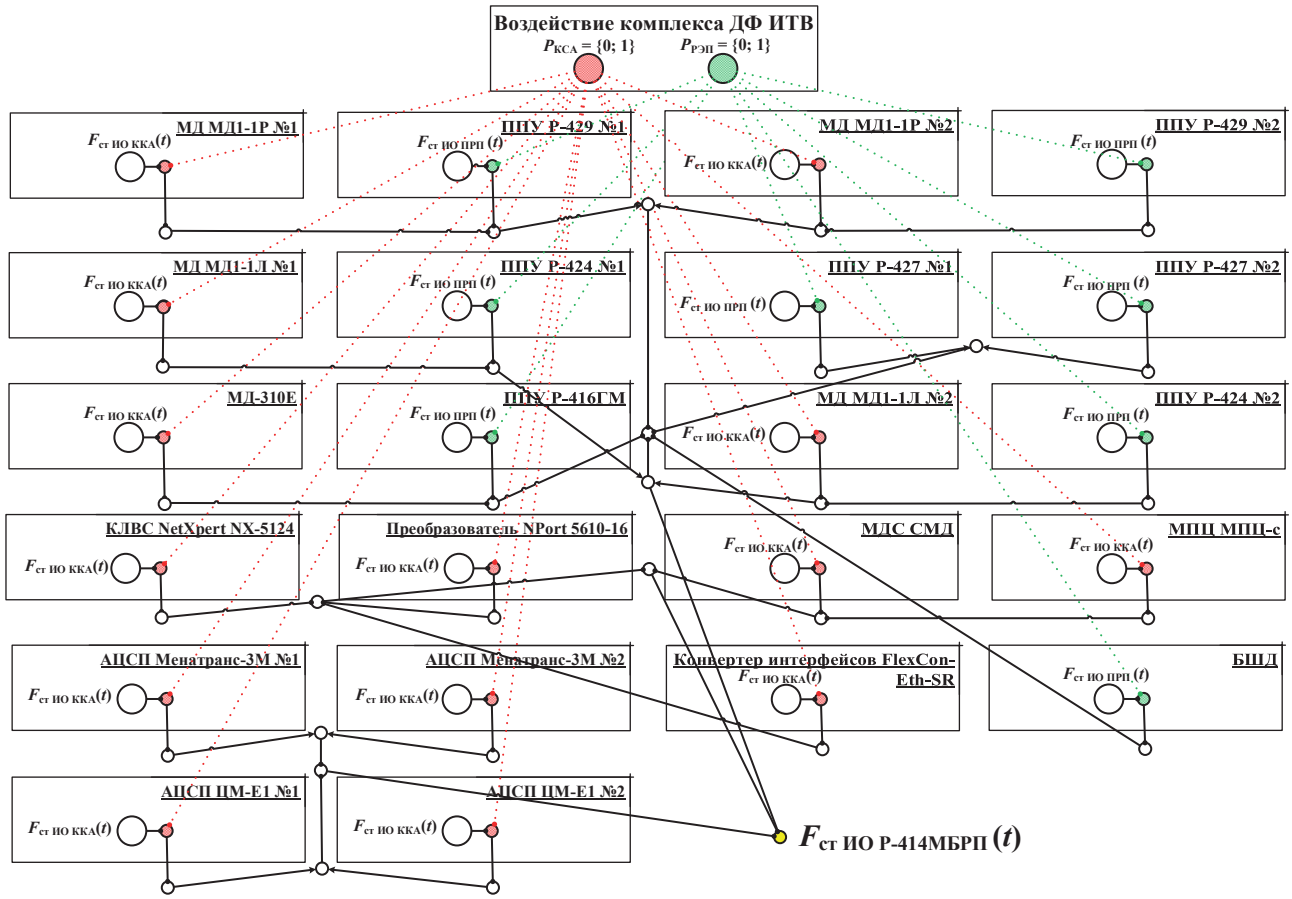

Рис. 5. Модель информационного обмена со свойством стойкости в радиорелейной станции Р-414МБРП

В качестве примера на (рис. 5) приведена модель информационного обмена со свойством стойкости в радиорелейной (РР) станции Р-414МБРП, которая представлена в виде совокупности взаимосвязанных СФЦ исследуемого процесса в СС, входящих в ее состав, которые представлены базовой моделью.

Наиболее точная оценка стойкости информационного обмена в ведомственной СУ обеспечивается посредством использования варианта, при котором осуществляется моделирование исследуемого процесса со свойством стойкости во всех подсистемах и элементах ТП СУ и учитываются все возможные логические взаимосвязи между ними, т. е. цепочка «уровень информационного обмена в ТП ведомственной СУ – уровень информационного обмена в ИН – уровень информационного обмена в аппаратной (станции) – уровень информационного обмена в СС». Такой вариант моделирования целесообразно использовать при достаточном количестве времени, например, в ходе учебной, научно-исследовательской деятельности или проведении опытно-конструкторских работ. При ограниченном временном ресурсе для экспресс-оценки целесообразно использовать менее точные модели, в которых прохождение информационного обмена представлено базовой моделью. При этом следует учитывать, что результаты оценки будут более оптимистичными и менее точными.

Пример расчета вероятностно-временных характеристик (ВВХ) свойства стойкости информационного обмена в ИН ведомственной СУ

Для нахождения ВВХ свойства стойкости информационного обмена в ведомственной СУ, подверженного воздействию комплекса ДФ ИТВ, введены следующие допущения и ограничения:

- вероятность возникновения ДФ ПТВ и ЭВ считалась известной и задана значениями булева множества $P_{ДФi} = \{0; 1\}$ в соответствии с прогнозируемым сценарием ИТВ противоборствующей стороны (рис. 6), разработанного на основе сведений, изложенных в трудах[5];
- исходные данные прогнозируемого сценария ИТВ представлены в таблице 1;
- функции распределения вероятности времени реализации ПТВ в виде ККА и ЭВ в виде ПРП считались известны и рассчитаны для исходных данных, представленных [2];
- время, за которое происходит восстановление информационного обмена в условном ОС после воздействия каждого ДФ, взято и равно $T_в$ = 30 мин;
- для обеспечения передачи информации в ведомственной СУ организовано одно ИН, топологическая структура которого представлена на рис. 7. Информационная взаимосвязь между субъектом и объектом управления обеспечивается функционированием двух направлений связи (НС): РР и проводного (Пр) с использованием цифровых РР станций Р-427 комплексной аппаратной связи Р-409МБ1(КАС) и цифровых систем передачи SHDSL ЦМ-Е1 соответственно.

Требуется с помощью разработанной многоуровневой логико-вероятностной модели

5 а) Макаренко С. И. Информационное противоборство и радиоэлектронная борьба в сетецентрических войнах начала XXI века: моногр. СПб.: Наукоемкие технологии, 2017. 546 с.
б) Валецкий О. В. Уроки Ирака. Тактика, стратегия и техника в Иракских войнах США. М.: Издатель Воробьев А. В. 2015. 212 с.
в) Батюшкин С. А. Подготовка и ведение боевых действий в локальных войнах и вооруженных конфликтах: учеб. пособие. М.: КНОРУС. 2017. 438 с.

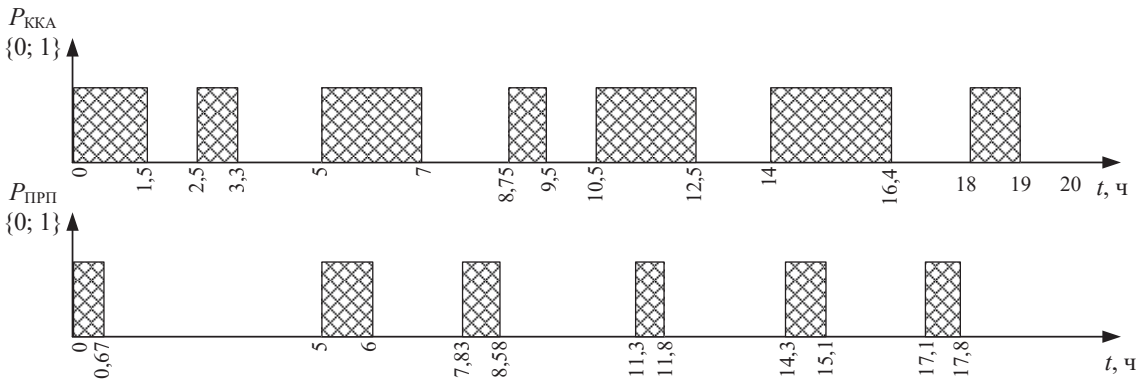

Рис. 6. Сценарий информационно-технического воздействия противоборствующей стороны

Таблица 1.

Исходные данные прогнозируемого сценария информационно-технического воздействия

Параметр	Численное значение (диапазон)	Физический смысл параметра, единица измерения
t_a t_b	0 20	Время начала и окончания рассматриваемого временного интервала соответственно, ч
$K_{\text{ст ИО тр}}$	0,8	Требуемое значение коэффициента стойкости информационного обмена
ПТВ в виде ККА		
$N_{\text{ККА}}$	7	Количество воздействий ККА
$t_{\text{н1}}$ $t_{\text{к1}}$	0 1,5	время начала и окончания 1-го воздействия ККА соответственно, ч
$t_{\text{н2}}$ $t_{\text{к2}}$	2,5 3,3	Время начала и окончания 2-го воздействия ККА соответственно, ч
$t_{\text{н3}}$ $t_{\text{к3}}$	5 7	Время начала и окончания 3-го воздействия ККА соответственно, ч
$t_{\text{н4}}$ $t_{\text{к4}}$	8,75 9,5	Время начала и окончания 4-го воздействия ККА соответственно, ч
$t_{\text{н5}}$ $t_{\text{к5}}$	10,5 12,5	Время начала и окончания 5-го воздействия ККА соответственно, ч
$t_{\text{н6}}$ $t_{\text{к6}}$	14 16,4	Время начала и окончания 6-го воздействия ККА соответственно, ч
$t_{\text{н7}}$ $t_{\text{к7}}$	18 19	Время начала и окончания 7-го воздействия ККА соответственно, ч
ЭВ в виде ПРП		
$N_{\text{ПРП}}$	7	Количество воздействий ПРП
$t_{\text{н1}}$ $t_{\text{к1}}$	0 0,67	Время начала и окончания 1-го воздействия ПРП соответственно, ч
$t_{\text{н2}}$ $t_{\text{к2}}$	5 6	Время начала и окончания 2-го воздействия ПРП соответственно, ч
$t_{\text{н3}}$ $t_{\text{к3}}$	7,83 8,58	Время начала и окончания 3-го воздействия ПРП соответственно, ч
$t_{\text{н4}}$ $t_{\text{к4}}$	11,3 11,8	Время начала и окончания 4-го воздействия ПРП соответственно, ч
$t_{\text{н5}}$ $t_{\text{к5}}$	14,3 15,1	Время начала и окончания 5-го воздействия ПРП соответственно, ч
$t_{\text{н6}}$ $t_{\text{к6}}$	17,1 17,8	Время начала и окончания 6-го воздействия ПРП соответственно, ч

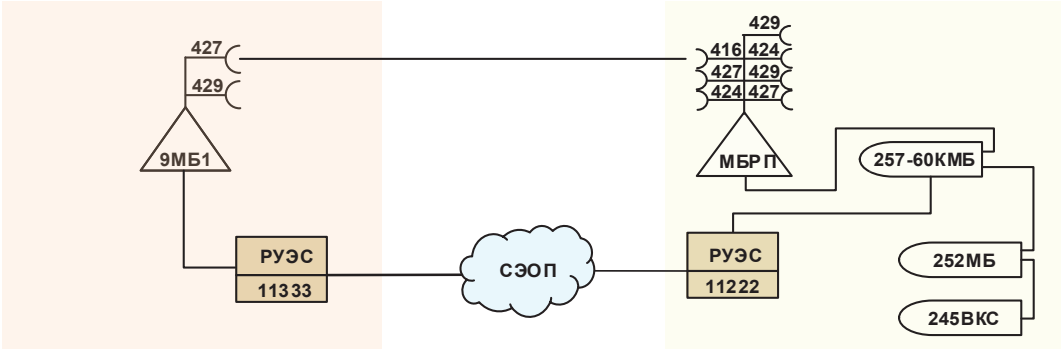

Рис. 7. Структура информационного направления ведомственной системы управления (вариант)

определить ВВХ свойства стойкости информационного обмена в ИН ведомственной СУ и оценить его показатели в условиях прогнозируемого сценария ИТВ (рис. 6) противоборствующей стороны.

Решение. В целях решения поставленной задачи разработана логико-вероятностная модель информационного обмена (рис. 8) в ИН ведомственной СУ заданной структуры (рис. 7). Указанная модель представлена совокупностью взаимосвязанных СФЦ исследуемого процесса в аппаратных (станциях) и районных узлах электросвязи (РУЭС) СЭОП, которые, в свою очередь, представлены базовыми моделями. Функциональные вершины 1, 2, 6, 11, 15, 17 отражают события прохождения информационного обмена без нарушения (блокирования) в аппаратных (станциях) и характеризуются функциями распределения вероятности времени стойкости к воздействию заданного сценария ИТВ. Вершины 4 и 8 отражают события прохождения информационного обмена без нарушения (блокирования) через РУЭС СЭОП.

Система логических уравнений для представленной модели информационного обмена в ИН имеет вид:

$$\begin{cases} y_1 = x_1;\ y_2 = x_2;\ y_3 = y_1; \\ y_4 = x_4;\ y_5 = y_2 \cdot y_4;\ y_6 = x_6; \\ y_7 = y_3 \cdot y_6;\ y_8 = x_8;\ y_9 = y_5 \cdot y_8; \\ y_{10} = y_7 + y_9;\ y11 = x_{11};\ y_{12} = y_{10} \cdot y_{11}; \\ y_{13} = y_{12} \cdot y_{14};\ y_{14} = y_{15};\ y_{15} = x_{15}; \\ y_{16} = y_{13} \cdot y_{17};\ y_{17} = x_{17}, \end{cases}$$

а вероятностная функция с учетом перехода от вероятностных мер к функциям распределения вероятности времени стойкости информационного обмена в аппаратных (станциях) и РУЭС СЭОП, описывается тремя одночленами:

$$F_{\text{ст ИО ИН}}(t) = F_{\text{ст ИО Р-409 МБ1}}(t)\ \text{РР} \times F_{\text{ст ИО Р-414 МБРП}}(t) \times$$
$$\times F_{\text{ст ИО П-257-60 КМБ}}(t) \times F_{\text{ст ИО П-252 МБ}}(t) \times F_{\text{ст ИО П-245 ВКС}}(t) +$$
$$+ F_{\text{ст ИО Р-409 МБ1 (КАС)}}(t)\ \text{Пр} \times F_{\text{ст ИО РУЭС}}(t) \times$$
$$\times F_{\text{ст ИО РУЭС}}(t) \times F_{\text{ст ИО П-257-60 КМБ}}(t) \times F_{\text{ст ИО П-252 МБ}}(t) \times$$
$$\times F_{\text{ст ИОП-245 ВКС}}(t) - F_{\text{ст ИОР-409 МБ1}}(t)\ \text{РР} \times$$
$$\times F_{\text{ст ИОР-409 МБ1(КАС)}}(t)\ \text{Пр} \times F_{\text{ст ИО РУЭС}}(t) \times$$

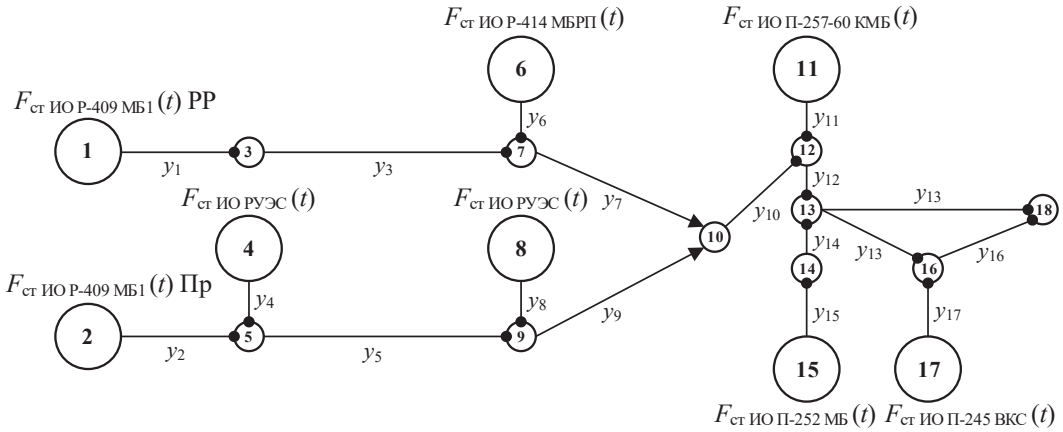

Рис. 8. Логико-вероятностная модель информационного обмена со свойством стойкости в информационном направлении ведомственной системы управления

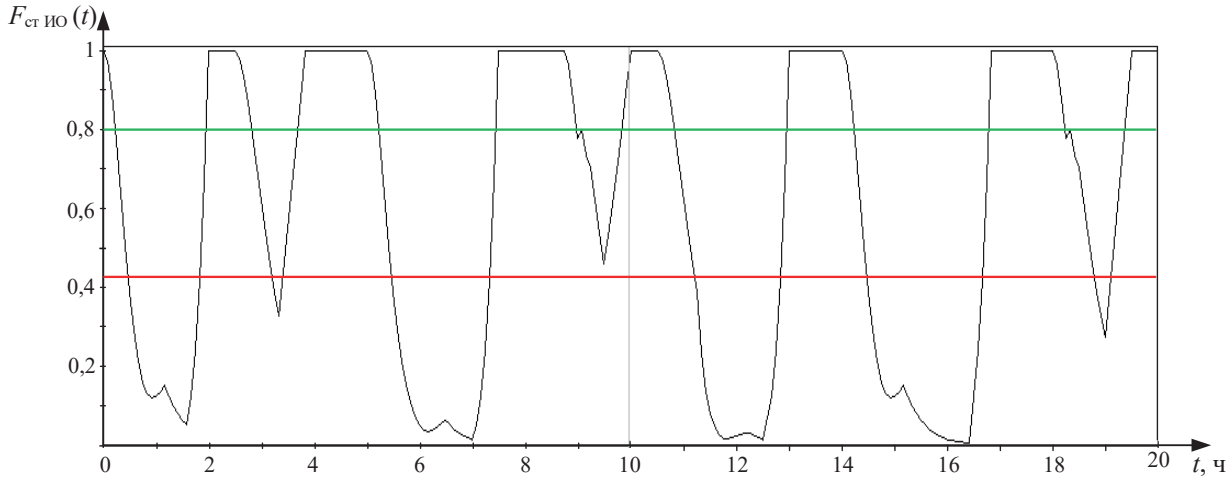

Рис. 9. График функции распределения вероятности времени стойкости информационного обмена в информационном направлении ведомственной системы управления

$$\times F_{\text{ст ИО РУЭС}}(t) \times F_{\text{ст ИО Р-414 МБРП}}(t) \times F_{\text{ст ИО П-257-60 КМБ}}(t) \times$$
$$\times F_{\text{ст ИОП-252 МБ}}(t) \times F_{\text{ст ИО П-245 ВКС}}(t)$$

С помощью программных комплексов автоматизированного структурно-логического моделирования ПК АСМ 2001.1 и Mathcad-2014 при заданных допущениях и ограничениях произведен расчет ВВХ свойства стойкости исследуемого процесса в ИН. График функции распределения вероятности времени стойкости информационного обмена в ИН ведомственной СУ представлен на рис. 9.

Численное значение оцениваемого показателя стойкости – коэффициента $K_{\text{ст ИО}}$ равно 0,418, что не соответствует требуемому ($K_{\text{ст ИО тр}} \geq 0{,}8$). Расчетные значения свидетельствует о том, что стойкость информационного обмена существенно снижена и не соответствует необходимой степени обеспечения управления, что объясняется стратегией комплексного согласованного применения противоборствующей стороной сил и средств ИТВ, а также отсутствием эффективных методов и средств защиты от ПТВ, в частности от СР, успешная реализация которой оказывает основное влияние на эффективность проведения ККА.

Полученный результат свидетельствует о необходимости проведения дальнейшего исследования по разработке организационно-технических мероприятий, направленных на защиту процесса обмена информацией, что позволит обеспечить безопасность информационного обмена в ведомственных СУ.

Выводы

Сущность полученного научного результата заключается в предложенной многоуровневой логико-вероятностной модели информационного обмена, которая позволила:

- выявить закономерности динамики прохождения информационного обмена в ведомственной СУ и оценить его стойкость в условиях воздействия комплекса ДФ ИТВ;
- использовать стратифицированный подход, который на основе базовой логико-вероятностной модели информационного обмена, позволяет создавать СФЦ исследуемого процесса любого уровня декомпозиции в СУ различной топологической структуры;
- учесть на различных уровнях декомпозиции информационного обмена модели исследуемого процесса любого из нижележащих уровней;
- учесть динамику информационного противоборства посредством задания временных параметров ДФ ИТВ.

Литература

1. Иванец В. М., Лукьянчик В. Н., Мельник В. Н. Особенности организации управления войсками в операции с учетом динамики информационных процессов при переходе на военные сетевые технологии // Военная мысль. 2020. № 7. С. 91–101.
2. Потапчик Н. Н. Методический подход к оценке стойкости информационного обмена в условиях информационно-технического воздействия противника // Вестник Военной академии Республики Беларусь. 2024. № 3(84). С. 36–50.
3. Шерстобитов Р. С. Модель маскирования информационных направлений сетей передачи данных ведомственного назначения в условиях компьютерной разведки // Системы управления, связи и безопасности. 2025. № 1. С. 79–104.
4. Леонов Н. В. Противодействие уязвимостям программного обеспечения. Часть 1. Онтологическая модель // Вопросы кибербезопасности. 2024. № 2(60). С. 81–92.
5. Пылинский М. В., Потапчик Н. Н. Организационно-технические требования к функционированию телекоммуникационных сетей группировки войск (сил) в условиях сетевых атак противника // Вестник Военной академии Республики Беларусь. 2024. № 1(82). С. 11–18.
6. Макаренко С. И. Модели системы связи в условиях преднамеренных дестабилизирующих воздействий и ведения разведки. СПб.: Наукоемкие технологии, 2020. 337 с.
7. Стародубцев Ю. И., Закалкин П. В. Структурно-функциональный анализ конфликтной ситуации между государственной системой обеспечения информационной безопасности и иностранной системой деструктивных воздействий // Вопросы кибербезопасности. 2024. № 4(62). С. 82–91. DOI: 10.21681/2311-3456-2024-4-82-91.
8. Богер А. М., Соколов А. Н. Математическая модель вектора DDOS-атаки на сетевую инфраструктуру АСУ ТП с использованием метода топологического преобразования стохастических сетей // Вопросы кибербезопасности. 2023. № 4(56). С. 72–79.
9. Пылинский М. В., Потапчик Н. Н. Методический подход к оценке функционирования системы военной связи в условиях информационно-технического воздействия // Вестник Военной академии Республики Беларусь. 2023. № 1(78). С. 18–23.
10. Тишков В. В., Иванов В. Г., Лукьянчик В. Н. Обоснование облика построения перспективных комплексов и средств связи на основе опыта организации связи при проведении специальной военной операции // Военная мысль. 2023. № 9. С. 59–72.

MULTILEVEL LOGICAL-PROBABILISTIC MODEL OF INFORMATION EXCHANGE IN DEPARTMENTAL MANAGEMENT SYSTEM

Potapchik N. N.[6], Pylinsky M. V.[7]

Keywords: *information warfare, telecommunications subsystem, information technology impact, destabilizing factor, information exchange security, property of stability, general logical-probabilistic method.*

Abstract

The purpose: *of the work: is to develop a multilevel logical-probabilistic model of information exchange with the property of stability in a departmental management system.*

Research method: *the conducted research is based on general scientific methods: analysis, synthesis, abstraction, generalization, modeling, induction, deduction. The general logical-probabilistic method, as well as probability theory, were justifiably chosen and used as the main method.*

Research results: *a multilevel logical-probabilistic model of information exchange with the property of stability has been developed, including private models of the process under study in vulnerable subsystems and elements of the telecommunications subsystem of the departmental control system. The presented model allows to obtain equations of probability functions of the property of stability of information exchange,*

6 Nikolay N. Potapchik, Adjunct of the Department of Communications, Faculty of Communications and Automated Control Systems, Military Academy of the Republic of Belarus, Minsk, Republic of Belarus. E mail: nikpotapchik89@gmail.com

7 Maxim V. Pylinsky, Dr.Sc. of Military Sciences, Professor, Head of the Department of Communications, Faculty of Communications and Automated Control Systems, Military Academy of the Republic of Belarus, Minsk, Republic of Belarus. E-mail: pylinskii.maksim@mail.ru

exposed to the influence of a complex of destabilizing factors of information-technical influence, to establish new quantitatively substantiated dependencies between input and output parameters and to evaluate stability of the studied process in the departmental management system. The adequacy of the developed model has been proven. In the main part of the article, using the presented model, the calculation and assessment of the probabilistic-temporal characteristics of the property of stability of information exchange in the information direction of the departmental management system is carried out. The results of the assessment indicate the need to develop organizational and technical measures aimed at ensuring the security of information exchange in departmental management systems.

Scientific novelty: *the presented multilevel logical-probabilistic model allows: to identify patterns of dynamics of information exchange in departmental control systems; to use a stratified approach, which, based on the basic logical-probabilistic model of information exchange, allows to create schemes of functional integrity of the studied process of any level of decomposition in control systems of different topological structure; to take into account the dynamics of information confrontation by setting time parameters of destabilizing factors of information-technical influence.*

References

1. Ivanec V. M., Luk'janchik V. N., Mel'nik V. N. Osobennosti organizacii upravlenija vojskami v operacii s uchetom dinamiki informacionnyh processov pri perehode na voennye setevye tehnologii // Voennaja mysl'. 2020. № 7. S. 91–101.
2. Potapchik N. N. Metodicheskij podhod k ocenke stojkosti informacionnogo obmena v uslovijah informacionno-tehnicheskogo vozdejstvija protivnika // Vestnik Voennoj akademii Respubliki Belarus'. 2024. № 3(84). S. 36–50.
3. Sherstobitov R. S. Model' maskirovanija informacionnyh napravlenij setej peredachi dannyh vedomstvennogo naznachenija v uslovijah komp'juternoj razvedki // Sistemy upravlenija, svjazi i bezopasnosti. 2025. № 1. S. 79–104.
4. Leonov N. V. Protivodejstvie ujazvimostjam programmnogo obespechenija. Chast' 1. Ontologicheskaja model' // Voprosy kiberbezopasnosti. 2024. № 2(60). S. 81–92.
5. Pylinskij M. V., Potapchik N. N. Organizacionno-tehnicheskie trebovanija k funkcionirovaniju telekommunikacionnyh setej gruppirovki vojsk (sil) v uslovijah setevyh atak protivnika // Vestnik Voennoj akademii Respubliki Belarus'. 2024. № 1(82). S. 11–18.
6. Makarenko S. I. Modeli sistemy svjazi v uslovijah prednamerennyh destabilizirujushhih vozdejstvij i vedenija razvedki. SPb.: Naukoemkie tehnologii, 2020. 337 s.
7. Starodubcev Ju. I., Zakalkin P. V. Strukturno-funkcional'nyj analiz konfliktnoj situacii mezhdu gosudarstvennoj sistemoj obespechenija informacionnoj bezopasnosti i inostrannoj sistemoj destruktivnyh vozdejstvij // Voprosy kiberbezopasnosti. 2024. № 4(62). S. 82–91. DOI: 10.21681/2311-3456-2024-4-82-91.
8. Boger A. M., Sokolov A. N. Matematicheskaja model' vektora DDOS-ataki na setevuju infrastrukturu ASU TP s ispol'zovaniem metoda topologicheskogo preobrazovanija stohasticheskih setej // Voprosy kiberbezopasnosti. 2023. № 4(56). S. 72–79.
9. Pylinskij M. V., Potapchik N. N. Metodicheskij podhod k ocenke funkcionirovanija sistemy voennoj svjazi v uslovijah informacionno-tehnicheskogo vozdejstvija // Vestnik Voennoj akademii Respubliki Belarus'. 2023. № 1(78). S. 18–23.
10. Tishkov V. V., Ivanov V. G., Luk'janchik V. N. Obosnovanie oblika postroenija perspektivnyh kompleksov i sredstv svjazi na osnove opyta organizacii svjazi pri provedenii special'noj voennoj operacii // Voennaja mysl'. 2023. № 9. S. 59–72

ОЦЕНКА ЭФФЕКТИВНОСТИ ИСПОЛЬЗОВАНИЯ Δ-СЛОЯ НЕРАЗЛИЧИМОСТИ ДВОИЧНЫХ СИГНАЛОВ, ПРИНИМАЕМЫХ В УСЛОВИЯХ СЛУЧАЙНЫХ И ПРЕДНАМЕРЕННЫХ ПОМЕХ

Негурица А. О.[1]

DOI:10.21681/3034-4050-2025-4-22-27

Ключевые слова: *алгоритм формирования и приема сигналов, псевдослучайный сигнал, рандомизированное правило приема, гарантированная вероятность ошибки.*

Аннотация

Цель работы: *исследовать эффективность применения решающего правила приемника с Δ-слоем неразличимости двоичных сигналов в условиях воздействия на канал связи случайных и преднамеренных помех, уточнить оценку выигрыша, обеспечиваемого использованием Δ-слоя, с учетом аддитивного воздействия на передаваемый сигнал гауссовского шума, наличие которого в канале сокращает величину этого выигрыша.*

Результаты: *получены аналитические выражения для вероятности ошибочного приема ФМ-сигнала при использовании приемника с Δ-слоем, которые для заданных соотношений мощностей: сигнал-помеха-шум рассчитаны путем проведения вычислительного эксперимента, по результатам которого представлены графики зависимости вероятности ошибки бита сообщения от мощности преднамеренной помехи с наихудшим (оптимальным) распределением при различных уровнях гауссовского шума.*

Установлено, что с ростом уровня шума выигрыш приемника с Δ-слоем сокращается, в канале при средней мощности шума (в полосе частот сигнала) $\sigma^2 > 0{,}1$ эффект практически отсутствует.

Научная новизна: *определены условия эффективности использования решающего правила приема ФМ-сигналов с Δ-слоем неразличимости в условиях воздействия как преднамеренных, так и случайных помех.*

Введение

Вопросы повышения помехозащищенности систем передачи информации (СПИ) обусловлены растущими угрозами целенаправленного радиоэлектронного подавления, которое может использоваться для нарушения работы каналов связи в критически важных сферах – от военных коммуникаций до промышленных и государственных систем управления. В современных условиях злоумышленники применяют оптимизированные помехи, способные анализировать параметры сигнала и подбирать оптимальные стратегии воздействия [1, с. 41; 2, с. 244; 3, с. 1522; 4, с. 457; 5, с. 79-80; 6, с. 41], что требует разработки более совершенных методов защиты.

Особую значимость приобретает обеспечение помехоустойчивости связи при ограниченных энергетических ресурсах, когда источник помех стремится минимизировать эффективность передачи данных в рамках имеющегося ресурса мощности. В таких условиях классические алгоритмы приема не обеспечивают необходимый уровень помехоустойчивости, тогда как специализированные алгоритмы формирования и приема сигналов (АФПС) [1, с. 41; 3, с. 1522; 4, с. 457; 5, с. 79-80] позволяют повысить помехозащищенность систем передачи информации на основе совершенствования методов модуляции/демодуляции.

Таким образом, повышение помехозащищенности остается ключевой задачей, от решения которой зависит безопасность современных и перспективных систем связи и эффективность их функционирования.

Вопросам разработки способов передачи информации в условиях преднамеренных помех уделяется значительное внимание [2, с. 244; 4, с. 457-458; 7, с. 20-21; 8, арт.3348].

1 Негурица Анастасия Олеговна, адъюнкт Военной академии связи имени Маршала Советского Союза С. М. Будённого, г. Санкт-Петербург, Россия. E-mail: LadyN98@yandex.ru

В основу этих способов в существующих СПИ положены методы модуляции с формированием псевдослучайных сигналов (ПСС) во временной области: фазомодулированный псевдослучайный сигнал (ФМ-ПСС), амплитудно-фазомодулированный псевдослучайный сигнал (АФМ-ПСС) [1, с. 41; 3, с. 1523], а также в частотной области – алгоритмы псевдослучайной перестройки рабочей частоты (ППРЧ) [4, с. 458]. В настоящее время эти способы помехозащиты в сочетании с приемником Котельникова В. А. широко применяются в системах военной и коммерческой связи для передачи информации в условиях преднамеренных помех.

Вместе с тем в 1971 году Кан С.[2] сделал вывод, что приемник Котельникова не оптимален для приема двоичных ФМ ПСС в условиях преднамеренных помех при ограничении на среднюю мощность источника.

В 1986 году Чуднов А. М.[3] в более общей задаче синтеза АФПС установил оптимальность АФМ-ПСС и привел примеры более эффективных по отношению к приемнику Котельникова решающих правил приема сообщений в условиях преднамеренных помех. В это же время Жодзишский Ю. И.[4] построил в аналитическом варианте оптимальное правило приема двоичных сигналов с базой $n = 1$, а также получил на основе вычислительных методов значения параметров, определяющие оптимальные решающие правила приема ФМ ПСС для относительно небольших значений базы n.

Актуальные на текущий момент границы гарантированной вероятности ошибки приведены: нижние, обеспечиваемые источником помехи, и верхние, гарантируемые СПИ – в [1, с. 45]. Для $n = 1$ верхняя граница определена в соответствии с результатами Жодзишского Ю. И. Для $n = 2$ – результатом, полученным в [1, с. 45; 6, с. 46] на основе использования АФМ сигнала и приемника с Δ-слоем, т. е. областью на плоскости, ограниченной двумя прямыми $x = \pm\Delta$, в которой приемник принимает равновероятно решение в пользу одного из сигналов ±1.

Относительно приемника с Δ-слоем следует отметить [1, с. 48-49]:

- при $\Delta = 0$ приемник с Δ-слоем становится приемником Котельникова, принимающим решение в пользу ближайшего в евклидовой метрике эталонного сигнала;
- оптимальные значения Δ^* параметра Δ-слоя равны: $\Delta_1^* = 3 - 2\sqrt{2} \approx 0{,}1716$ при $n = 1$ и $\Delta_2^* \approx 0{,}2584$ при $n = 2$;
- при оптимальном слое Δ^* приемник обеспечивает энергетический выигрыш в помехоустойчивости по отношению к приемнику Котельникова приблизительно на 1,38 дБ при $n = 1$ и 0,41 дБ при $n = 2$;
- для $n \geq 3$ приемник с Δ-слоем ($\Delta > 0$) оказывается неэффективным;
- приемник имеет простую реализацию.

Учитывая оптимальность приемника Котельникова в условиях гауссовской помехи, можно заключить о снижении выигрыша, обеспечиваемого приемником с Δ-слоем при повышении в канале уровня случайных шумов. Поскольку этот вопрос ранее не исследовался, он является предметом исследования настоящей работы. Рассматривается случай $n = 1$, представляющий наибольший теоретический и практический интерес.

В настоящей работе описана модель СПИ, а также поставлена задача на исследование, предложена методика оценки эффективности приемника с Δ-слоем с учетом воздействия как преднамеренных помех, так и случайных (гауссовских) шумов, подведены итоги, обозначены возможные пути применения полученных результатов, а также направления развития и обобщения решаемой задачи.

Модель СПИ и постановка задачи

Принцип работы СПИ иллюстрируется на рис. 1, где использованы обозначения:

$\mathcal{A}$ – сообщение, поступающее от источника в канал канала связи, представлено случайной величиной (СВ) с равновероятными значениями из $\{\pm 1\}$;

$\mathcal{V}$ – аддитивная преднамеренная помеха описывается СВ с наихудшим для системы распределением $F_V(\cdot)$, выбираемым источником помехи в рамках условия

$$\mathbf{E}[\mathcal{V}^2] = \mathbf{E}_{F_D}[\mathcal{D}] \leq \delta, \qquad (1)$$

где $\mathbf{E}[\cdot]$ – математическое ожидание СВ, δ – максимально допустимое отношение средней мощности помехи к мощности сигнала,

2 Cahn C. Performance of Digital Matched Filter Correlator with Unknown Interference // IEEE Trans. Commun. Techn. 1971. V. 19. № 6. P. 1163–1172. https://doi.org/10.1109/TCOM.1971.1090760

3 Чуднов А. М. О минимаксных алгоритмах формирования и приема сигналов // Пробл. передачи информ. 1986. Т. 22. № 4. С. 49–54. https://www.mathnet.ru/rus/ppi958

4 Жодзишский Ю. И. Максимальная гарантированная помехоустойчивость приема сигналов при ограничении средней мощности мешающих воздействий // Радиотехника. 1986. № 10. С. 56–57.

определенное имеющимся ресурсом источника помехи, $\mathcal{D} = \mathcal{V}^2$ – мощность помехи, выделяемая источником на сигнал; $\sigma\xi$ – случайная аддитивная помеха – белый гауссовский шум (БГШ) с дисперсией σ^2; $\mathcal{W} = \mathcal{A} + \mathcal{V} + \sigma\xi$ – сигнал на выходе физического канала (входе приемника); РПР – решающее правило различения сигналов с Δ-слоем, определенное выражением

$$\mathcal{B} = (1 + \mathrm{sgn}_\Delta(\mathcal{W}))/2, \qquad (2)$$

где $\mathcal{B}$ – выдаваемое получателю сообщение,

$$\mathrm{sgn}_\Delta(z) = \begin{cases} -1, & \text{если } z < -1, \\ 0, & \text{если } |z \le \Delta|, \\ 1, & \text{если } z > 1. \end{cases} \qquad (3)$$

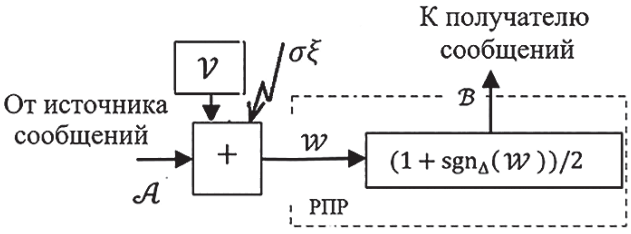

Рис. 1. Функциональная схема СПИ

Вероятность ошибки бита сообщения при фиксированной мощности помехи $d = v^2$ в СПИ при $\sigma > 0$ определяется соотношением

$$\begin{aligned} P(d,\sigma^2,\Delta) &= \Pr\{\mathcal{B} \ne \mathcal{A}\} = \\ &= \frac{1}{4}\Pr\{1-\Delta < -1 - \sqrt{d} + \sigma\xi \le 1 + \Delta\} + \\ &+ \frac{1}{2}\Pr\{-1 - \sqrt{d} + \sigma\xi > 1 + \Delta\} + \\ &+ \frac{1}{4}\Pr\{1-\Delta < -1 + \sqrt{d} + \sigma\xi \le 1 + \Delta\} + \\ &+ \frac{1}{2}\Pr\{-1 + \sqrt{d} + \sigma\xi > 1 + \Delta\} = \\ &= \frac{1}{4}[\Pr\{-1 - \sqrt{d} + \sigma\xi \le 1 + \Delta\} - \\ &- 1 + \Pr\{-1 - \sqrt{d} + \sigma\xi \le 1 - \Delta\}] + \\ &+ \frac{1}{2}[1 - \Pr\{-1 - \sqrt{d} + \sigma\xi \le 1 + \Delta\}] + \\ &+ \frac{1}{4}[\Pr\{-1 + \sqrt{d} + \sigma\xi \le 1 + \Delta\} - \\ &- 1 + \Pr\{-1 + \sqrt{d} + \sigma\xi \le 1 - \Delta\}] + \\ &+ \frac{1}{2}[1 - \Pr\{-1 + \sqrt{d} + \sigma\xi \le 1 + \Delta\}] = \\ &= \frac{1}{4}[\mathrm{F}_\xi(\frac{1}{\sigma}(2 + \Delta + \sqrt{d})) - 1 + \mathrm{F}_\xi(\frac{1}{\sigma}(2 - \Delta + \sqrt{d}))] + \\ &+ \frac{1}{2}[1 - \mathrm{F}_\xi(\frac{1}{\sigma}(2 + \Delta + \sqrt{d}))] + \\ &\frac{1}{4}[\mathrm{F}_\xi(\frac{1}{\sigma}(2 + \Delta - \sqrt{d})) - 1 + \mathrm{F}_\xi(\frac{1}{\sigma}(2 - \Delta - \sqrt{d}))] + \\ &+ \frac{1}{2}[1 - \mathrm{F}_\xi(\frac{1}{\sigma}(2 + \Delta - \sqrt{d}))] = \\ &= \frac{1}{4}\mathrm{F}_\xi(\frac{1}{\sigma}(2 + \Delta + \sqrt{d})) + \frac{1}{4}\mathrm{F}_\xi(\frac{1}{\sigma}(2 - \Delta + \sqrt{d})) - \\ &- \frac{1}{4} + \frac{1}{2} - \frac{1}{2}\mathrm{F}_\xi(\frac{1}{\sigma}(2 + \Delta + \sqrt{d})) + \\ &+ \frac{1}{4}\mathrm{F}_\xi(\frac{1}{\sigma}(2 + \Delta - \sqrt{d})) - \frac{1}{4} + \frac{1}{4}\mathrm{F}_\xi(\frac{1}{\sigma}(2 - \Delta - \sqrt{d})) + \\ &+ \frac{1}{2} - \frac{1}{2}\mathrm{F}_\xi(\frac{1}{\sigma}(2 + \Delta - \sqrt{d})) = \\ &= \frac{1}{2} - \frac{1}{4}\mathrm{F}_\xi(\frac{1}{\sigma}(2 + \Delta + \sqrt{d})) + \frac{1}{4}\mathrm{F}_\xi(\frac{1}{\sigma}(2 - \Delta + \sqrt{d})) - \\ &- \frac{1}{4}\mathrm{F}_\xi(\frac{1}{\sigma}(2 + \Delta - \sqrt{d})) + 1/4\ \frac{1}{4}\mathrm{F}_\xi(\frac{1}{\sigma}(2 - \Delta - \sqrt{d})) = \\ &= \frac{1}{2}(1 + \frac{1}{2}[\mathrm{F}_\xi(\frac{1}{\sigma}(2 + \Delta + \sqrt{d})) - \mathrm{F}_\xi(\frac{1}{\sigma}(2 + \Delta + \sqrt{d})) \\ &- \mathrm{F}_\xi(\frac{1}{\sigma}(2 - \Delta - \sqrt{d}))]), \end{aligned} \qquad (4)$$

которое дополнительно по отношению к [1, с. 44] учитывает воздействие на переданный сигнал случайного шума.

По определению

$$P^{-}(\delta,\sigma^2,\Delta) = \max_{F_d \in \mathbb{F}(\delta)} \mathbf{E}_{F_d}[P(d,\sigma^2,\Delta)], \qquad (5)$$

и поскольку максимум в (5) достигается при $\mathbf{E}[\mathcal{D}] = \delta$, корректным является определение наихудшего (оптимального) распределения помехи (т. е. наихудшей стратегии ИП) в виде

$$F_d^* = \operatorname*{agrmax}_{F_d \in \mathbb{F}(\delta)} P(d,\sigma^2,\Delta). \qquad (6)$$

На основе методики, описанной в [9, с. 129], устанавливается равенство

$$P^{-}(d,\sigma^2,\Delta) = P^{\wedge}(d,\sigma^2,\Delta), \qquad (7)$$

где $P^{\wedge}(\cdot)$ – вогнутая (выпуклая вверх) оболочка функции $P(d,\sigma^2,\Delta)$ по первому аргументу.

Таким образом, исследуемая в работе задача состоит в построении вогнутой оболочки функции $P(d,\sigma^2,\Delta)$ и проведении анализа на этой основе эффективности приемника с Δ-слоем в канале с преднамеренными помехами и случайным шумом.

Основные результаты

Расчеты по формулам (4) осуществлялись путем проведения вычислительного эксперимента средствами Excel-VBA с оценкой значений параметров методом Монте-Карло. Для каждого из 51 значений d от 0 до 2 (значения равномерно распределены) в процессе расчетов осуществляется прогон 100000 случайных наборов данных, соответствующих формируемым данным объектов СПИ и ИП для 4-х значений Δ:

$$\Delta = 0;\ \Delta = 0{,}1;\ \Delta = \Delta^* = 0{,}1716 \text{ и } \Delta = 0{,}3.$$

Время расчетов составляет 15–30 с.

Построение выпуклой оболочки функции $P(d,\sigma^2,\Delta)$ по $d \in [0,\infty)$ осуществлялось на основе

рекуррентной процедуры (обобщающей соответствующую процедуру [1, с. 45]) поочередной коррекции трех точек d_1,d_2,d_3 касания прямых к зависимости $P(d,\sigma^2,\Delta)$, в промежутках $[0,d_1),[d_2,d_3)$, в результате чего функции $P(d,\sigma^2,\Delta)$ были представлены в общем случае в виде:

$$\hat{P}(\delta,\sigma 2,\Delta)=\begin{cases} k_1\delta, & \delta\in[0,d_1),\\ P(\delta,\sigma^2,\Delta), & \delta\in[d_1,d_2),\\ k_2\delta, & \delta\in[d_2,d_3),\\ P(\delta,\sigma^2,\Delta), & \delta\in[d_3,\infty),\end{cases}$$

При этом точки d_1,d_2,d_3 определяют оптимальную стратегию ИП, а именно:

- при $\delta\in[0,d_1)$ ИП с оптимальной стратегией формирует помеху в импульсном режиме с мощностью импульса d_1 и вероятностью его выдачи $p(d_1)=\delta/d_1$;
- при $\delta\in[d_1,d_2)$ в непрерывном режиме с мощностью δ;
- при $\delta\in[d_2,d_3)$ в биимпульсном режиме с мощностями импульсов d_2,d_3 и их вероятностями $p(d_2),p(d_3)$, определяемыми из условия

$$p(d_2)+p(d_3)=1,\ p(d_2)d_2+p(d_3)d_3=\delta;$$

- при $\delta\in[d_3,\infty)$ в непрерывном режиме с мощностью δ.

На рисунках 2–4 показаны зависимости $P(d|\Delta)=P(d,\sigma,\Delta)$ (сплошные линии) и $\hat{P}(\delta|\Delta)=\hat{P}(\delta,\sigma,\Delta)$ (пунктирные линии) построенные соответственно для $\sigma=0;\ 0{,}1;\ 0{,}2$, которые, с одной стороны, показывают примеры и результаты расчетов по оценке помехоустойчивости СПИ при использовании в приемнике РПР с Δ-слоем и, с другой, позволяют оценить выигрыш такого приемника относительно приемника Котельникова и определить целесообразность его применения.

Как видно, при отсутствии случайных помех приемник с Δ-слоем обеспечивает максимальный выигрыш. При увеличении уровня БГШ этот выигрыш снижается и становится практически незаметным при $\sigma\geq 0{,}3$.

Следует отметить, что наибольший практический интерес представляет область значений показателя $\hat{P}(\delta,\sigma^2,\Delta)\leq 0{,}02$, поскольку при больших значениях вероятности ошибки становится невыгодным повышать достоверность передачи информации на канальном и сетевом уровнях СПИ по сравнению с увеличением длительности сигнала и/или базы ПСС на физическом уровне. На графиках эта область представлена окрестностью точки

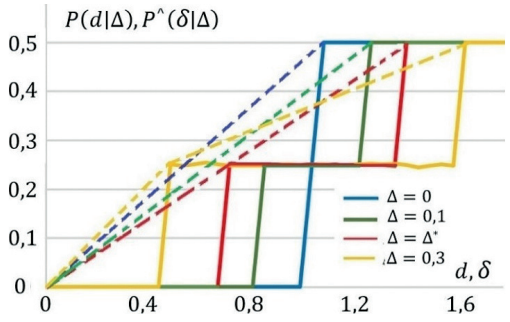

Рис. 2. Зависимость величин $P(d|\Delta)$, $\hat{P}(d|\Delta)$ от значений d,δ текущей и средней мощности для различных при $\sigma=0$

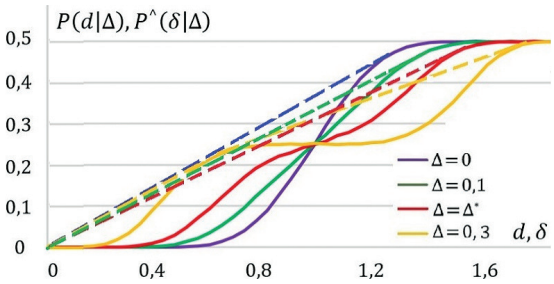

Рис.3. Зависимость величин $P(d|\Delta)$, $\hat{P}(d|\Delta)$ от значений d,δ текущей и средней мощности для различных при $\sigma=0{,}1$

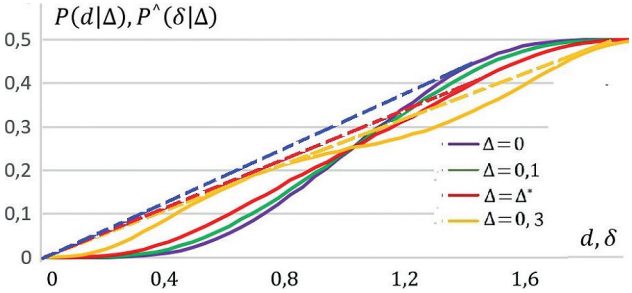

Рис. 4. Зависимость величин $P(d|\Delta)$, $\hat{P}(d|\Delta)$ от значений d,δ текущей и средней мощности для различных при $\sigma=0{,}2$

$\delta=0$, поэтому наиболее важные результаты работы следует отнести к области $\delta\in[0,d_1)$.

Анализ представленных на рис. 2–4 зависимостей показывает, что несмотря на снижение выигрыша, обеспечиваемого приемником с Δ-слоем, он остается более эффективным по равнению с приемником Котельникова. Более того, в рамках проведенных экспериментов оказалось, что с ростом уровня БГШ оптимальное значение параметра Δ^* возрастает. Этот результат свидетельствует о целесообразности теоретической проработки вопросов оптимизации параметра Δ приемника.

Заключение

Исследуемые вопросы подсказывают ряд направлений совершенствования способов повышения помехозащищенности системы связи к воздействию преднамеренных помех при наличии различных факторов: случайных помех с различными свойствами, нестационарной среды распространения сигналов, многолучевости, замираний, некогерентности приема, асинхронности и асинхронности композиции помехи с сигналом и другим.

В силу существенного расхождения верхних и нижних границ вероятности ошибки бита информации весьма актуальными являются обозначенные в [1, с. 58] проблемы повышения помехозащищенности СПИ передаваемых на канальном уровне информационных блоков. В таких АФПС (при условии их существования) вместо Δ-слоя в приемнике (демодуляторе, декодере) должно быть реализовано более сложное рандомизированное правило приема сообщений.

Литература

1. Чуднов А. М., Сазонов В. В., Бикбулатов В. Р. Оптимизация области неразличимости приемником двоичных сигналов, передаваемых по каналу с преднамеренной помехой // Проблемы передачи информации. 2025. Том 61. Вып.1, с. 41–59.
2. Чуднов А. М., Сапунова Л. П., Бикбулатов В. Р. Модель канала передачи данных с обратной связью в условиях воздействия преднамеренных помех с ограниченной средней мощностью // Известия ТулГУ. Технические науки. 2025. Вып. 2. С. 243–249.
3. Nguyen B. V., Nguyen M. T., Jung H., Kim K. Designing Anti-Jamming Receivers for NRDCSK Systems Utilizing ICA, WPD, and VMD Methods // IEEE Trans. Circuits Syst. II Express Briefs. 2018. V. 66. № 9. P. 1522–1526. https://doi.org/10.1109/TCSII.2019.2891254.
4. Chen Y., Yuan W., Xu T. Coding Split and Adjustment to Defend OFDM-IM Against Jamming Attacks // IEEE Commun. Lett. 2023. V. 27. № 2. P. 457–461. https://doi.org/10.1109/LCOMM.2022.3224381.
5. Чуднов А. М., Кирик Д. И., Ермакова Е. М. Оптимизация параметров кода и режима обработки сигналов в условиях преднамеренных помех // Труды учебных заведений связи. 2019. Т. 5. № 4. С. 79–86. https://doi.org/10.31854/1813-324X-2019-5-4-79-86.
6. Chudnov A. M., Sazonov V. V., Bikbulatov V. R. Optimization of the Decisive Rule for a Receiver with Binary Signal Indistinguishability Δ-Layer in a Jamming Channel // Probl. Inf.Transm. 2025. V. 61. № 1. P. 41–55. DOI: 10.1134/S0032946025010041.
7. Чуднов, А. М. Комментарии к статье Н. Н. Плотникова, А. В. Войнова и А. Н. Путилина «Выбор алгоритма адаптации по рабочей частоте в однополосной радиолинии тропосферной связи» / А. М. Чуднов // Вопросы оборонной техники. Серия 16: Технические средства противодействия терроризму. – 2024. – № 11-12(197-198). – С. 20–30. – DOI 10.53816/23061456_2024_11-12_20.
8. Feng Z., Ren G., Chen J., Chen C., Yang X., Luo Y., Xu K. An Anti-Jamming Hierarchical Optimization Approach in Relay Communication System via Stackelberg Game // Appl.Sci. 2019. V. 9. № 16. P. 3348 (14 pp.). https://doi.org/10.3390/app9163348.
9. Чуднов А. М. Математические основы моделирования, анализа и синтеза систем. СПб.: ВАС, 2021.

IESTIMATION OF EFFICIENCY OF USING Δ-LAYER OF INDISTINGUISHABILITY OF BINARY SIGNALS RECEIVED UNDER CONDITIONS OF RANDOM AND DELIBERATE INTERFERENCES

Neguritsa A. O.[5]

Keywords: *signal generation and reception algorithm, pseudorandom signal, randomized reception rule, guaranteed error probability.*

5 Anastasia O. Neguritsa, adjunct of the Military Academy of Communications named after Marshal of the Soviet Union S. M. Budyonny, St. Petersburg, Russia. E-mail: LadyN98@yandex.ru

Abstract

The aim of the work *is to study the effectiveness of the application of the decision rule of the receiver with the Δ-layer of indistinguishability of binary signals under the influence of accidental and deliberate interference on the communication channel, to refine the assessment of the gain provided by the use of the Δ-layer, taking into account the additive effect of Gaussian noise on the transmitted signal, the presence of which in the channel reduces the value of this gain.*

Results: *analytical expressions were obtained for the probability of erroneous reception of the FM signal when using a receiver with a Δ-layer, which for the given power ratios: signal-interference-noise were calculated by conducting a computational experiment, the results of which presented graphs of the dependence of the probability of error of the message bit on the power of deliberate interference with the worst (optimal) distribution at different levels of Gaussian noise.*

It has been established that with an increase in the noise level, the gain of the receiver with the Δ-layer decreases, in the channel with an average noise power (in the signal frequency band) the effect is practically non-existent $\sigma^2 > 0{,}1$.

Scientific novelty: *the article defines the conditions for the effective use of the decision rule for receiving FM signals with a Δ-layer of indistinguishability under the influence of both intentional and accidental interference.*

References

1. Chudnov A. M., Sazonov V. V., Bikbulatov V. R. Optimizacija oblasti nerazlichimosti priemnikom dvoichnyh signalov, peredavaemyh po kanalu s prednamerennoj pomehoj // Problemy peredachi informacii. 2025. Tom 61. Vyp.1, s. 41–59.
2. Chudnov A. M., Sapunova L. P., Bikbulatov V. R. Model' kanala peredachi dannyh s obratnoj svjaz'ju v uslovijah vozdejstvija prednamerennyh pomeh s ogranichennoj srednej moshhnost'ju // Izvestija TulGU. Tehnicheskie nauki. 2025. Vyp. 2. S. 243–249.
3. Nguyen B. V., Nguyen M. T., Jung H., Kim K. Designing Anti-Jamming Receivers for NRDCSK Systems Utilizing ICA, WPD, and VMD Methods // IEEE Trans. Circuits Syst. II Express Briefs. 2018. V. 66. № 9. P. 1522–1526. https://doi.org/10.1109/TCSII.2019.2891254.
4. Chen Y., Yuan W., Xu T. Coding Split and Adjustment to Defend OFDM-IM Against Jamming Attacks // IEEE Commun. Lett. 2023. V. 27. № 2. P. 457–461. https://doi.org/10.1109/LCOMM.2022.3224381.
5. Chudnov A. M., Kirik D. I., Ermakova E. M. Optimizacija parametrov koda i rezhima obrabotki signalov v uslovijah prednamerennyh pomeh // Trudy uchebnyh zavedenij svjazi. 2019. T. 5. № 4. S. 79–86. https://doi.org/10.31854/1813-324X-2019-5-4-79-86.
6. Chudnov A. M., Sazonov V. V., Bikbulatov V. R. Optimization of the Decisive Rule for a Receiver with Binary Signal Indistinguishability Δ-Layer in a Jamming Channel // Probl. Inf.Transm. 2025. V. 61. № 1. P. 41–55. DOI: 10.1134/S0032946025010041.
7. Chudnov, A. M. Kommentarii k stat'e N. N. Plotnikova, A. V. Vojnova i A. N. Putilina «Vybor algoritma adaptacii po rabochej chastote v odnopolosnoj radiolinii troposfernoj svjazi» / A. M. Chudnov // Voprosy oboronnoj tehniki. Serija 16: Tehnicheskie sredstva protivodejstvija terrorizmu. – 2024. – № 11-12(197-198). – S. 20–30. – DOI 10.53816/23061456_2024_11-12_20.
8. Feng Z., Ren G., Chen J., Chen C., Yang X., Luo Y., Xu K. An Anti-Jamming Hierarchical Optimization Approach in Relay Communication System via Stackelberg Game // Appl.Sci. 2019. V. 9. № 16. P. 3348 (14 pp.). https://doi.org/10.3390/app9163348.
9. Chudnov A. M. Matematicheskie osnovy modelirovanija, analiza i sinteza sistem. SPb.: VAS, 2021.

ФОРМИРОВАНИЕ ПОДХОДОВ К РАЗРАБОТКЕ МОДЕЛИ КАНАЛА МНОЖЕСТВЕННОГО ДОСТУПА, ИСПОЛЬЗУЕМОГО В СОСТАВЕ СИСТЕМЫ ОБМЕНА ДАННЫМИ С ДИНАМИЧЕСКОЙ СТРУКТУРОЙ

Шарко Г. В.[1]

DOI:10.21681/3034-4050-2025-4-28-32

Ключевые слова: *внешние помехи, внутрисистемные помехи, необнаруживаемый конфликт, соотношение сигнал-шум, контроль занятости канала, максимальная обслуживаемая нагрузка, максимально допустимое количество корреспондентов в канале множественного доступа.*

Аннотация

Цель работы: *получение расчетных выражений для оценки граничных значений нагрузочных и структурных параметров каналов множественного доступа с целью их практического применения при развертывании и обеспечении функционирования систем обмена данными с динамической структурой.*

Методы исследования: *теория вероятности, методы оценки помехоустойчивости приёма сигналов.*

Результаты исследования: *получены расчетные соотношения для оценки нагрузочных (максимальной обслуживаемой каналом множественного доступа нагрузки) и структурных (максимально допустимого количества корреспондентов в канале множественного доступа) параметров. Применение данного математического аппарата в составе специального программного обеспечения комплексов технических средств передачи данных позволит в реальном масштабе времени адаптировать системы обмена данными с динамической структурой к изменениям ее характеристик. Тем самым будут обеспечены более эффективное распределение ресурсов канала множественного доступа, снижение непроизводительных потерь ресурсов, и, как следствие, повышение пропускной способности системы обмена данными в целом.*

Научная новизна: *в статье сформирован подход к разработке модели канала множественного доступа, учитывающей энергетические соотношения сигналов корреспондентов, функционирующих в канале множественного доступа, полученные выражения позволяют оценить нагрузочные и структурные параметры каналов множественного доступа, в том числе через энергетические характеристики сигналов корреспондентов.*

Введение

В условиях ускоряющегося развития и совершенствования систем обмена данными становится очевидным, что эффективное распределение их ресурсов и, следовательно, их характеристики становятся все более зависимыми от правильной и своевременной оценки ситуаций в сетях и системах [1–8]. Используемые в настоящее время алгоритмы множественного доступа, в которых не используются количественные оценки каналов множественного доступа (КМД) как результат применения прикладных расчетных задач, обладают недостаточной степенью адаптации к воздействию внешних и внутрисистемных помех и не позволяют эффективно использовать энергетические и частотные ресурсы системы обмена данными (СОД).

Статья посвящена отысканию подходов к моделированию КМД на базе радиоканала, которая, при реализации ее в СПО КТСПД СОД в качестве аппарата решения расчетных задач по планированию сетей передачи данных, позволит повысить эффективность управления КМД и СОД в целом.

Постановка задачи

Для группы корреспондентов, являющихся источниками и потребителями информации, выделена группа рабочих частот (при этом

1 Шарко Геннадий Васильевич, кандидат технических наук, доцент, преподаватель кафедры Военной академии связи имени Маршала Советского Союза С. М. Будённого, г. Санкт-Петербург, Россия. E-mail: shgorg@mail.ru

количество выделенных частот значительно меньше организуемых в группе радионаправлений). Каждая из выделенных частот используется парой корреспондентов только на время проведения сеанса связи, а затем освобождается. В силу особенностей пространственного размещения корреспондентов, их стохастического перемещения и случайного характера энергетических соотношений сигналов корреспондентов и поступающей от них нагрузки возможно одновременное использование выделенных частот несколькими парами корреспондентов (то есть возникновение конфликтов).

При допущении отсутствия внешних помех для радиосети внутрисистемные помехи, вызванные одновременным использованием одной и той же рабочей частоты двумя и более корреспондентами, приводят к проявлению некоторых специфических особенностей КМД.

Пусть корреспондент, находящийся в точке О (рис. 1), выбирает частоту, на которой уровень помех меньше заданного порогового значения: $U_{\text{п}} < U_{\text{п0}}$.

При этом вокруг данного корреспондента образуется ряд зон, обусловленных пространственно-энергетическими характеристиками КМД.

- Зона A (площадью $S_{\text{ок}}$) является зоной обнаружения чужой передачи и блокирования собственной (зоной обнаружения конфликта).
- Зона В (площадью $S_{\text{кр}}$) – это зона возникновения необнаруживаемого конфликта двух и более корреспондентов из-за большого расстояния между корреспондентами (что приводит к невозможности определения факта чужой передачи из-за конечного времени распространения сигнала).
- Зона C (площадью $S_{\text{кэ}}$) – это зона возникновения необнаруживаемого конфликта из-за пониженных энергетических характеристик сигнала корреспондента, находящегося в точке О.
- Зона D (площадью $S_{\text{св}}$) является зоной связи, в которой возможно повторное использование частоты, занятой корреспондентом в точке О, так как в данном случае $U_{\text{п}} < U_{\text{п0}}$ и данная частота при анализе состояния канала оценивается как незанятая (свободная).

Выбрав частоту, на которой уровень помех меньше установленного порогового значения, корреспондент, находящийся в точке О, устанавливает связь с другим корреспондентом, находящимся в пределах зоны с радиусом R_0, формируя при этом зону A.

В данной зоне с радиусом $R_{\text{ок}}$ уровень мешающего сигнала от корреспондента в точке О превышает $U_{\text{п0}}$ для всех корреспондентов в данной зоне, что приводит к невозможности занятия анализируемой частоты другим корреспондентом из-за занятия ее корреспондентом из точки О. Таким образом, граница этой зоны определяется уровнем сигнала передатчика корреспондента в точке О, который является помехой для других корреспондентов данной радиосети, пытающихся использовать эту же частоту. Вместе с тем незначительное взаимное удаление корреспондентов позволяет четко идентифицировать передачу пакета корреспондентом «своей» радиосети и блокировать собственную передачу в момент обнаружения занятия КМД (что устраняет возможность возникновения конфликта и тем самым повышает пропускную способность КМД).

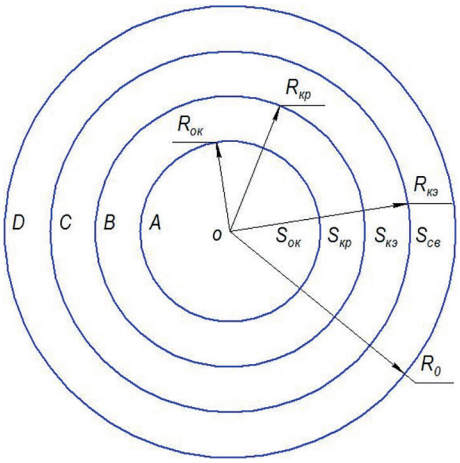

Рис. 1. Образование пространственно-энергетических зон в КМД

Это обеспечивается реализацией алгоритма случайного множественного доступа с контролем занятости канала (МДКЗ) с использованием анализатора занятости канала [9]. В качестве признака занятости канала в данном случае используется наличие в нем сигналов, структура которых соответствует кодовым комбинациям используемого помехоустойчивого кода. При обнаружении в канале заданного количества следующих подряд кодовых комбинаций с необнаруженными ошибками вырабатывается сигнал о занятости канала и вводится временная блокировка,

в течение которой запрещается передача сообщений в канал. Выход из состояния блокировки происходит через определенный интервал времени, отсчитываемый с момента формирования последнего сигнала о занятости канала. В зоне B с радиусом $R_{кр}$ с увеличением взаимного удаления корреспондентов вероятность возникновения конфликта возрастает, но энергетические характеристики сигнала корреспондента, находящегося в точке О, еще заставляют некоторых корреспондентов сети оценивать данную частоту как занятую.

В зоне C с радиусом $R_{кэ}$ при $U_с / U_п < n_{доп}$ возможны конфликты из-за взаимных помех, создаваемых другими корреспондентами радиосети, которые оценивают данную частоту как свободную и пытаются использовать ее для установления связи.

Необходимо получить расчетные соотношения для основных нагрузочных и структурных параметров КМД с учетом энергетических характеристик сигналов корреспондентов КМД.

Решение поставленной задачи

При известных плотностях распределения уровня полезного сигнала и помехи $V(U_с)$ и $V(U_п)$ в точке приема при $n_{доп} = 1$ вероятность возникновения конфликта в зоне C можно выразить следующим образом [10]:

$$P_к^с = P\left[\frac{U_с}{U_п} < n_{доп}\right] = \int_{U_{с_{min}}}^{U_{с_{max}}} V(U_с) \cdot P(U_п > U_с) dU_с = \int_{U_{с_{min}}}^{U_{с_{max}}} V(U_с) \left[\int_{U_{п_0}}^{U_с} V(U_п) dU_п\right] dU_с, \quad (1)$$

где $U_{с_{max}}$ и $U_{с_{min}}$ – максимальный и минимальный уровни сигнала на входе радиоприемника корреспондента в точке О.

Вид плотности распределения уровней сигнала $V(U_с)$ и внутрисистемных помех $V(U_п)$ в каждой точке приема зависит от характера размещения корреспондентов в зоне с радиусом R_0.

При равновероятных удалениях между корреспондентами плотность вероятности взаимных удалений между ними имеет вид:

$$f(r) = \frac{1}{R_0}. \quad (2)$$

Следовательно, как показано в [10],

$$V(U_с) = \frac{U_{с_{max}} \cdot U_{с_{min}}}{U_{с_{max}} - U_{с_{min}}} U_с^{-2} \frac{U_{с_{min}}}{U_с^2}; \quad (3)$$

$$V(U_п) = \frac{U_{п_{max}} \cdot U_{п_{min}}}{U_{п_{max}} - U_{п_{min}}} U_п^{-2} \frac{U_{п_{min}}}{U_п^2}. \quad (4)$$

При этом

$$P_к^с = U_{п_{min}} \left(\frac{1}{2U_{с_{min}}} + \frac{U_{с_{min}}}{2U_{п_0}^2} - \frac{1}{U_{п_0}}\right). \quad (5)$$

Считая при заданном распределении уровней $U_{с_{min}} = U_{п_{min}}$, получаем

$$P_к^с = \frac{1}{2}\left(1 - \frac{U_{с_{min}}}{U_{п_0}}\right)^2. \quad (6)$$

Для случая $n_{доп} \neq 1$ справедливы выражения:

$$P_к^с = 1 - \frac{1}{n_{доп}}\left[1 - \frac{1}{2}\left(1 - \frac{U_{с_{min}}}{U_{п_0}}\right)^2\right], \; n_{доп} > 1, \quad (7)$$

$$P_к^с = \frac{1}{2n_{доп}}\left(1 - \frac{n_{доп} \cdot U_{с_{min}}}{U_{п_0}}\right)^2, \; n_{доп} < 1. \quad (8)$$

Очевидно, что при $n_{доп} = 1$ выражения (7), (8) приводятся к виду (6).

Принимая $U_{с_{min}} / U_{п_0} = \delta$, получаем

$$P_к = \frac{1}{2}(1-\delta)^2. \quad (9)$$

Очевидно также, что при распределении ресурсов КМД наиболее вероятным конфликт будет в том случае, если конфликтующий корреспондент будет находиться на границе зон B и C или внутри зоны C.

Возможно отыскание некоторых параметров КМД для такого наихудшего случая, если решить приведенные ниже уравнения относительно максимально обслуживаемой КМД нагрузки Λ и максима льно допустимого количества корреспондентов в КМД N:

$$\frac{1}{2}(1-\delta)^2 = 1 - \exp[-({}_\Delta t_{оп} + a)(\Lambda - \lambda)], \quad (10)$$

$$\exp[-({}_\Delta t_{оп} + a)(\Lambda - \lambda)] = \frac{1}{1 - \frac{1}{2}(1-\delta)^2},$$

где a – максимальное время распространения сигнала в радиоканале; ${}_\Delta t_{оп}$ – интервал времени, необходимый для однозначного определения конкурирующей передачи в радиоканале; λ – нагрузка, создаваемая в радиоканале одним корреспондентом.

Далее

$$[({}_\Delta t_{оп} + a)(\Lambda - \lambda)] = \ln \frac{1}{1 - \frac{1}{2}(1-\delta)^2}.$$

Отсюда

$$\Lambda = \lambda + \frac{\ln \frac{1}{1 - \frac{1}{2}(1-\delta)^2}}{{}_\Delta t_{оп} + a}, \quad (11)$$

$$N = 1 + \frac{\ln \frac{1}{1 - \frac{1}{2}(1-\delta)^2}}{\lambda\,({}_\Delta t_{оп} + a)}. \quad (12)$$

Заключение

Полученные в ходе исследований выражения (11), (12) в дальнейшем могут быть использованы при разработке модели КМД на базе радиоканала, которая, при реализации ее в СПО КТСПД СОД в качестве аппарата решения прикладных расчетных задач по планированию сетей передачи данных, позволит повысить эффективность управления КМД и СОД в целом.

Литература

1. Кучерявый А. Е., Парамонов А. И., Маколкина М. А., Мутханна А. С. А., Выборнова А. И., Дунайцев Р. А. и др. Трехмерные многослойные гетерогенные сверхплотные сети // Информационные технологии и телекоммуникации. 2022. Т. 10. № 3. С. 1–12.
2. Бакулин М. Г., Бен Режеб Т. Б. К., Крейнделин В. Б., Миронов Ю. Б., Панкратов Д. Ю, Смирнов А. Э. Многостанционный доступ в системах связи пятого и последующих поколений // Электросвязь. 2022. № 5. С. 16–21.
3. Богатырев В. А., Богатырев С. В., Богатырев А. В. Оценка готовности компьютерной системы к своевременному обслуживанию запросов при его совмещении с информационным восстановлением памяти после отказов // Научно-технический вестник информационных технологий, механики и оптики. 2023. Т. 23. № 3. С. 608–617.
4. Росляков А. В. Сети фиксированной связи пятого поколения. М.: ООО «ИКЦ «Колос-с», 2024. 232 с.
5. Захаров М. В., Киричек Р. В. Методы построения сверхплотной сети e-health с использованием граничных вычислений // 75-я Научно-техническая конференция Санкт-Петербургского НТО РЭС им. А. С. Попова, посвященная Дню радио: сб. докладов. СПб.: СПбГЭТУ «ЛЭТИ», 2020. С. 145–147.
6. Росляков А. В., Герасимов А. В. Детерминированные сети связи и их стандартизация. // Стандарты и качество. 2024. № 7. С. 42–47.
7. Гезалов Э. Б. Модель неоднородной локальной сети связи с протоколом синхронного временного доступа с учетом надежности ее элементов // T-Comm: Телекоммуникации и Транспорт. 2021. Т. 15. № 3. С. 25–29.
8. Верзун Н. А., Воробьёв А. И., Пойманова Е. Д. Моделирование процесса передачи информации с разграничением прав доступа пользователей // Известия высших учебных заведений. Приборостроение. 2014. Т. 57. № 9. С. 33–37.
9. Верзун Н. А., Колбанёв М. О., Советов Б. Я. Корпоративный алгоритм множественного доступа в киберпространстве. Труды учебных заведений связи. 2025;11(3):97–107.
10. Доровских А. В., Сикарев А. А. Сети связи с подвижными объектами. – К.: Тэхника, 1989. – 158 с.

FORMATION OF APPROACHES TO THE DEVELOPMENT OF A MODEL OF A MULTIPLE ACCESS CHANNEL USED AS PART OF A DATA EXCHANGE SYSTEM WITH A DYNAMIC STRUCTURE

Sharko G. V.[2]

Keywords: *external interference, intra-system interference, undetectable conflict, signal-to-noise ratio, channel occupancy control, maximum serviced load, maximum allowable number of correspondents in a multiple access channel.*

Abstract

The aim of the work *is to obtain calculated expressions for estimating the boundary values of load and structural parameters of multiple access channels for the purpose of their practical application in the deployment and operation of data exchange systems with a dynamic structure.*

2 Gennady V. Sharko, Ph.D. of Technical Sciences, Associate Professor, Lecturer of the Department of the Military Academy of Communications, St. Petersburg, Russia. E-mail: shgorg@mail.ru

Research methods: *probability theory, methods for assessing the noise immunity of signal reception.*

Results of the study: *Calculated ratios have been obtained for estimating the load (the maximum load served by the multi-access channel) and structural (the maximum permissible number of correspondents in the multi-access channel) parameters. The use of this mathematical apparatus as part of special software of the complexes of technical means of data transmission will make it possible to adapt data exchange systems with dynamic structure to changes in its characteristics. Thus, a more efficient distribution of resources of the multiple access channel will be ensured, a reduction in unproductive resource losses, and, as a result, an increase in the bandwidth of the data exchange system as a whole.*

Научная новизна: *в статье сформирован подход к разработке модели канала множественного доступа, учитывающей энергетические соотношения сигналов корреспондентов, функционирующих в канале множественного доступа, полученные выражения позволяют оценить нагрузочные и структурные параметры каналов множественного доступа, в том числе через энергетические характеристики сигналов корреспондентов.*

References

1. Kucherjavyj A. E., Paramonov A. I., Makolkina M. A., Muthanna A. S. A., Vybornova A. I., Dunajcev R. A. i dr. Trehmernye mnogoslojnye geterogennye sverhplotnye seti // Informacionnye tehnologii i telekommunikacii. 2022. T. 10. № 3. S. 1–12.
2. Bakulin M. G., Ben Rezheb T. B. K., Krejndelin V. B., Mironov Ju. B., Pankratov D. Ju, Smirnov A. Je. Mnogostancionnyj dostup v sistemah svjazi pjatogo i posledujushhih pokolenij // Jelektrosvjaz'. 2022. № 5. S. 16–21.
3. Bogatyrev V. A., Bogatyrev S. V., Bogatyrev A. V. Ocenka gotovnosti komp'juternoj sistemy k svoevremennomu obsluzhivaniju zaprosov pri ego sovmeshhenii s informacionnym vosstanovleniem pamjati posle otkazov // Nauchno-tehnicheskij vestnik informacionnyh tehnologij, mehaniki i optiki. 2023. T. 23. № 3. S. 608–617.
4. Rosljakov A. V. Seti fiksirovannoj svjazi pjatogo pokolenija. M.: OOO «IKC «Kolos-s», 2024. 232 s.
5. Zaharov M. V., Kirichek R. V. Metody postroenija sverhplotnoj seti e-health s ispol'zovaniem granichnyh vychislenij // 75-ja Nauchno-tehnicheskaja konferencija Sankt-Peterburgskogo NTO RJeS im. A. S. Popova, posvjashhennaja Dnju radio: sb. dokladov. SPb.: SPbGJeTU «LJeTI», 2020. S. 145–147.
6. Rosljakov A. V., Gerasimov A. V. Determinirovannye seti svjazi i ih standartizacija. // Standarty i kachestvo. 2024. № 7. S. 42–47.
7. Gezalov Je. B. Model' neodnorodnoj lokal'noj seti svjazi s protokolom sinhronnogo vremennogo dostupa s uchetom nadezhnosti ee jelementov // T-Comm: Telekommunikacii i Transport. 2021. T. 15. № 3. C. 25–29.
8. Verzun N. A., Vorob'jov A. I., Pojmanova E. D. Modelirovanie processa peredachi informacii s razgranicheniem prav dostupa pol'zovatelej // Izvestija vysshih uchebnyh zavedenij. Priborostroenie. 2014. T. 57. № 9. S. 33–37.
9. Verzun N. A., Kolbanjov M. O., Sovetov B. Ja. Korporativnyj algoritm mnozhestvennogo dostupa v kiberprostranstve. Trudy uchebnyh zavedenij svjazi. 2025;11(3):97–107.
10. Dorovskih A. V., Sikarev A. A. Seti svjazi s podvizhnymi ob#ektami. – K.: Tjehnika, 1989. – 158 s.

РЕАЛИЗАЦИЯ БОРТОВОГО АЛГОРИТМА ПОИСКА, ИДЕНТИФИКАЦИИ, РАСПОЗНАВАНИЯ И ПОСЛЕДУЮЩЕГО ПОРАЖЕНИЯ ОБНАРУЖЕННЫХ ЦЕЛЕЙ С ИСПОЛЬЗОВАНИЕМ ОБУЧЕННЫХ НЕЙРОСЕТЕЙ

Ситдиков Д. С.[1], Васильев Н. А.[2]

DOI:10.21681/3034-4050-2025-4-33-42

Ключевые слова: *беспилотный летательный аппарат, групповое управление, позиционирование, определение местоположения, разметка изображения, компьютерное зрение.*

Аннотация

Цель работы: *заключается в разработке и обосновании комплексного подхода к реализации бортового алгоритма поиска, идентификации, распознавания и поражения целей с использованием обученных нейросетей в составе группы БЛА. Работа направлена на повышение автономности и эффективности взаимодействия дронов в условиях динамичной боевой обстановки.*

Результаты исследования: *проведённое исследование позволило выделить и апробировать ряд функциональных компонентов бортовой интеллектуальной системы управления группой БЛА, реализующей задачи поиска, идентификации, распознавания и поражения целей на основе нейросетевых алгоритмов. В результате разработана архитектура взаимодействия дронов с учётом динамики целей и использования сверточных нейронных сетей для детекции и автосопровождения, что обеспечило устойчивую работу системы в условиях ограниченных вычислительных ресурсов. В ходе экспериментов подтверждена эффективность применения алгоритма YOLOv5 в реальном времени, а также обоснована необходимость применения методов трекинга (DeepSORT, ByteTrack) в задачах групповой навигации. Установлены оптимальные параметры обучения нейросетевой модели, включая объем и структуру обучающего набора данных, формат аннотаций и соотношение выборок. Результаты могут быть использованы при создании программного обеспечения для управления роями БЛА в задачах разведки и поражения, что закладывает научную основу для дальнейшего развития автономных систем военного назначения.*

Научная новизна: *разработка и интеграция бортового алгоритма распознавания и поражения целей с использованием обученных нейронных сетей в составе группы БЛА, обеспечит автоматизированное взаимодействие дронов на всех этапах боевой операции. Предложена комплексная структура управления роем с учетом трекинга целей, семантической сегментации и оптимизации маршрутов на основе интеллектуального анализа видеопотока в реальном времени.*

Введение

Проблема взаимодействия беспилотных летательных аппаратов (БЛА) в группе, определения их местоположения и взаимосвязи требует решения задач поиска, идентификации, распознавания целей при действии группы БЛА. Эта проблема является одной из сложнейших в классе реализации алгоритма группового управления. По этой причине эти вопросы являются предметом повышенного интереса зарубежных и отечественных ученых. Интерес к ним вызван перспективностью применения групп БЛА в различных областях человеческой деятельности и одновременно сложностью решаемых задач [1].

Путями решения данной проблемы могут быть применение обученной нейронной сети, представляющей собой набор из файлов конфигурации самой сети и набора весовых коэффициентов.

Цель работы заключается в рассмотрении комплексного подхода к реализации бортового алгоритма поиска, идентификации, распознавания и последующего автосопровождения обнаруженных целей, оптимизации научно-технических и конструктивно-технологических

1 Ситдиков Дмитрий Сергеевич, младший научный сотрудник Военной академии связи имени Маршала Советского Союза С. М. Будённого, г. Санкт-Петербург, Россия. E-mail: dima.sitdikov.99@mail.ru

2 Васильев Никита Алексеевич, кандидат технических наук, заместитель начальника научно-исследовательского отдела научно-исследовательского центра Военной академии связи имени Маршала Советского Союза С. М. Будённого, г. Санкт-Петербург, Россия. E mail: vasn2020@mail.ru

решений системы распознавания БЛА в группе, а также повышение осведомленности БЛА за счет эффективного применения компьютерного зрения и обученных нейронных сетей.

Решение поставленной задачи

Эксплуатируемые в Вооруженных силах Российской Федерации (ВС РФ) комплексы с БЛА позволяют существенно расширить возможности войсковых подразделений при решении широкого спектра задач ведения разведки, ретрансляции связи, радиоэлектронного противодействия, огневого поражения и других задач. Одним из перспективных направлений применения БЛА является групповое применение. Полет строем, т.е. точное выдерживание некоторых заданных относительных положений в процессе полета группы, не только улучшает эффективность выполнения некоторых видов миссий, но и для целого ряда задач становится необходимым условием их решения [2].

Технология группового применения БЛА может обеспечить повышение оперативности решения задач, увеличение территориального охвата, устойчивости к радиоэлектронному противодействию, точности огневого поражения целей с помощью БЛА. Применение алгоритмов машинного и глубокого (нейросетевого) обучения, с возможностью распределенных вычислений, в составе специального программного обеспечения (СПО) комплексов с БЛА, способствует повышению эффективности решения разведывательных и ударных задач, минимизировать зависимость качества их решения от человеческого фактора. Таким образом, предлагаемая технология группового применения БЛА с элементами искусственного интеллекта, в частности компьютерного зрения и детекции (задача, в которой необходимо выделить несколько объектов на изображении посредством нахождения координат их ограничивающих рамок и классификации этих ограничивающих рамок из множества заранее известных классов), позволит существенно расширить оперативно-тактические и технические возможности разведывательных и огневых подразделений ВС РФ [3].

Задача группы БЛА по поражению объектов интереса (выявленных целей) состоит из нескольких последовательно выполняющихся этапов (рис. 1, рис. 2):

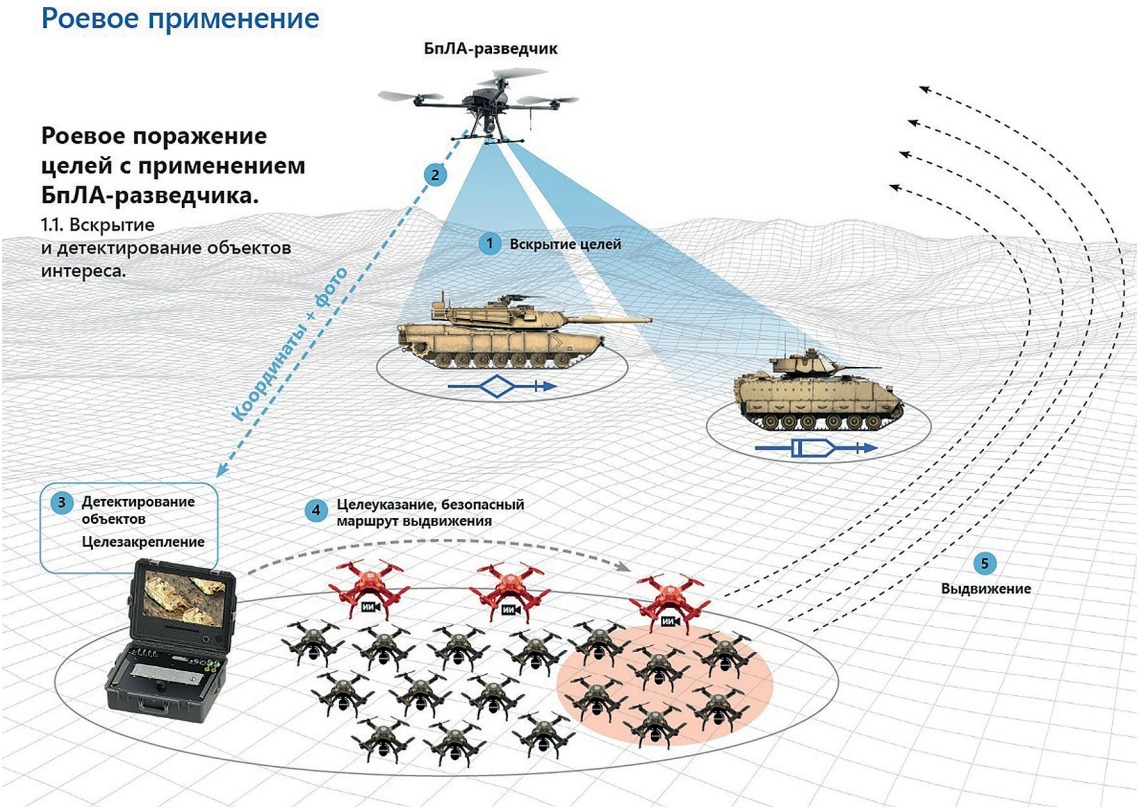

Рис. 1. Вскрытие и детектирование целей группой БЛА

1. Вскрытие объекта – определение по видеопотоку наличия на кадрах «подозрительного» участка местности, который может содержать объект(ы) интереса. Задача решается на борту БЛА-разведчика с помощью применения как классических алгоритмов компьютерного зрения (цветовая сегментация или классификация, выделение шаблонных участков), так и методов машинного и глубокого обучения (сверточных нейронных сетей).

2. Передача координат найденного объекта – в случае нахождения объекта, его геопривязанное изображение передается на автоматизированное рабочее место (АРМ) оператора наземной станции управления (НСУ) или мобильный терминал управления (МТУ). При наличии хорошего канала связи, в условиях отсутствия противодействия противника, видеопоток может передаваться непосредственно на наземную станцию управления с дальнейшим решением задачи вскрытия и детектирования объектов интереса на АРМ оператора.

3. Детектирование объектов и закрепление целей – определения класса вскрытого объекта, его характеристик (направление и скорость движения, боевой потенциал, координаты объекта) и ключевых признаков или отбрасывание такого объекта, если результат идентификации оказался ложным (недостоверным). Данная задача решается на АРМ оператора МТУ, с использованием сверточных нейронных сетей и алгоритмов семантической сегментации.

4. Целеуказание и построение безопасного маршрута движения. Задача целеуказания решается в автоматизированном режиме. На основе боевого потенциала цели определяется количество привлекаемых БЛА, необходимых для поражения цели (далее – ударные БЛА). Затем целеуказания, включающие координаты точки прибытия и характеристики вскрытого объекта передаются на БЛА с интеллектуально-вычислительной системой, управляющие роем (далее – БЛА-лидер). Задача построения безопасного маршрута движения, решается на АРМ оператора НСУ, с дальнейшей передачей опорных точек маршрута на БЛА-лидер. Опорные точки представляют собой пространственные геоданные, такие как координаты точки прибытия и, при необходимости, промежуточные координаты, которые группа должна достигнуть. В ходе расчетов может использоваться информация о запрещенных зонах полета.

5. Выдвижение – задача, решаемая на борту БЛА-лидера, результатом которой является формирование направления движения каждого ударного БЛА. Для устойчивого безопасного группового движения предлагается подход, в основу которого положен расчет величины скорости и направления движения каждого БЛА в группе с определенной частотой, в зависимости от координат всех остальных БЛА. Расчет величины скорости и направления движения складывается из четырех компонент, каждая из которых берется с некоторым постоянным весовым коэффициентом:

- компонента движения к цели – вычисляется единичный вектор направления от БЛА к цели прибытия;
- компонента движения к центру группы – вычисляется единичный вектор направления от БЛА к центру группы, вычисленному как среднее арифметическое координат всех БЛА;
- компонента движения от ближайших соседей – вычисляется результирующий вектор, как сумма направлений от ближайших соседей, взятых величинами, зависящими от расстояния до каждого из соседей. Так, вклад соседа, находящегося критически близко к БЛА, окажется больше более отдаленного соседа и вынудит эту компоненту скорости быть более направленной от критически близкого соседа;
- компонента случайного блуждания – вычисляется единичный вектор произвольного направления. Необходимость этого вектора обусловлена возможностью разрешить критические абсолютные задачи, например, в случае абсолютно зеркального и движения БЛА.

Для решения задачи выдвижения осуществляется многократный пересчет направлений движения МБЛА с некоторой частотой. Данный подход позволяет своевременно реагировать на неожиданные препятствия, вышедшие из строя БЛА или потери связи.

6. Доразведка цели – повторный поиск БЛА-лидером объекта интереса на месте прибытия. Для поиска объекта используется

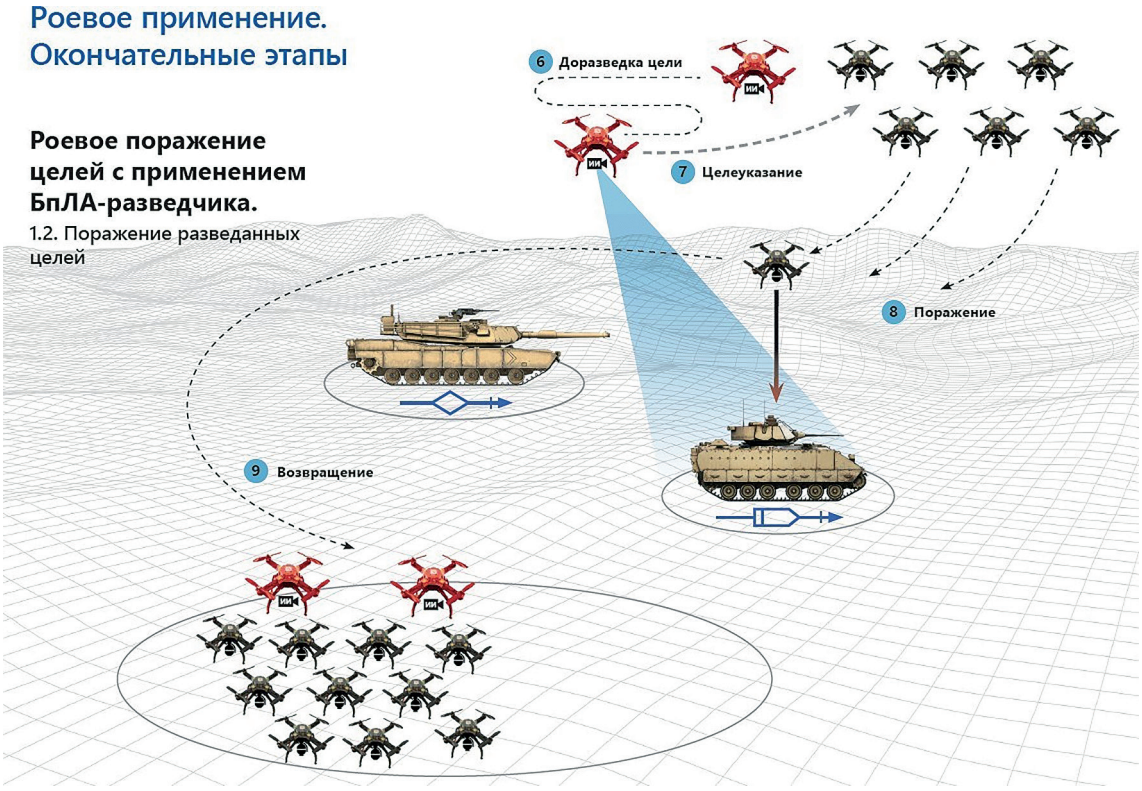

Рис. 2. Поражение целей группой БЛА

информация, полученная с АРМ оператора, которая описывает объект с помощью:

1) набора признаков:
   - ключевые точки;
   - цвет;
2) нейронной сети, обученной распознавать конкретный объект.

7. Целеуказание – формирование индивидуального полетного задания для каждого ударного БЛА с целью поражения объекта. В зависимости от типа поражаемого объекта (стационарный, маневренный, площадной) БЛА-лидером принимается решение об порядке поражении данной цели, производится расчет и передача команд на БЛА для имитации поражения объекта в определенный момент времени и в конкретных координатах.

8. Поражение – непосредственный маневр, выполняемый ударным БЛА с целью сброса средств поражения в район рассчитанных БЛА-лидером координат.

9. Возвращение – после выполнения боевого задания, возвращение ударного БЛА на базу производится путем расчета маршрута к координатам точек посадки, задаваемые и рассчитываемые ударным БЛА каждому их них. Такое движение производится по уже рассмотренным выше правилам движения, игнорируя правило движения к центру группы.

Для поиска, распознавания, идентификации с последующим выделением (и далее взятием на автосопровождение) целей на фоне других объектов и подстилающей поверхности, на борту БЛА в группе требуется организовать вычислительный процесс, который использует определенные алгоритмы и инструментарий (разметку и обучение) на базе нейронных сетей, позволяющие в реальном времени выполнить указанные процедуры [4–6].

Для эффективного применения нейронных сетей в целях распознавания объектов требуется корректно обученная нейронная сеть представляющие собой набор из файлов конфигурации самой сети и набора весовых коэффициентов.

Следовательно, формирование весовых коэффициентов есть результат обучения, который играет значительную роль при использовании нейронной сети в прикладных задачах [7].

Если стоит задача распознавания и детекции объектов в кадре, то в наборе данных для обучения используется набор изображений,

которые для корректного процесса обучения должны быть заранее размечены.

В настоящее время применяются различные архитектуры распознавания и детекции имеющие некоторые как общие, так и отличительные особенности. Подходы к обнаружению объектов разделяются на две группы: классические алгоритмы (на основе вручную спроектированных признаков) и обнаружение объектов на основе применения сверточных нейронных сетей. Наиболее оптимальным алгоритмом с точки зрения скорости работы и точности является алгоритм YOLOv4 и YOLOv5 [8,9].

Применение технологии компьютерного зрения, основанной на архитектуре YOLO, позволяет автоматизировать процессы наблюдения и выделения требуемых объектов на различной фоно-целевой обстановке, что позволяет достичь максимальной эффективности принятия решения нейро сетью, используемой для управления группой БЛА.

YOLO – это набор (последовательность) алгоритмов, позволяющих анализировать изображения, разделяя их на сетку с фрагментами. Каждая ячейка этой сетки отвечает за поиск и обнаружение объектов внутри себя. В основе создания алгоритма YOLO лежат принципы, обеспечивающие максимальное быстродействие и точность проведения такого поиска [10].

Для начала обучения нейросети YOLO требуется определить какие объекты (цель или цели) требуется находить на изображении, полученном от ОЭС БЛА и собрать набор данных. В случае проведения обработки полученных изображений требуется найти и разметить ряд изображений и лучше всего для этого подойдут изображения, сформированные в ходе формулирования задачи поиска нужных объектов.

В случае с поиском на изображении от ОЭС БЛА, требуется получить и обработать ряд изображений, содержащих сами БЛА (как объекты) и также важно, чтобы был различный фон на всех полученных изображениях из набора данных. То есть чем больше разнопланового фона, но одинакового искомого объекта (по форме и/или размеру) на наборах данных будет получено, тем лучше будет результат анализа этих изображений, поскольку фон в данном случае будет играть роль шума. Соответственно, чем больше шума будет отсечено при разметке и обучении сети,

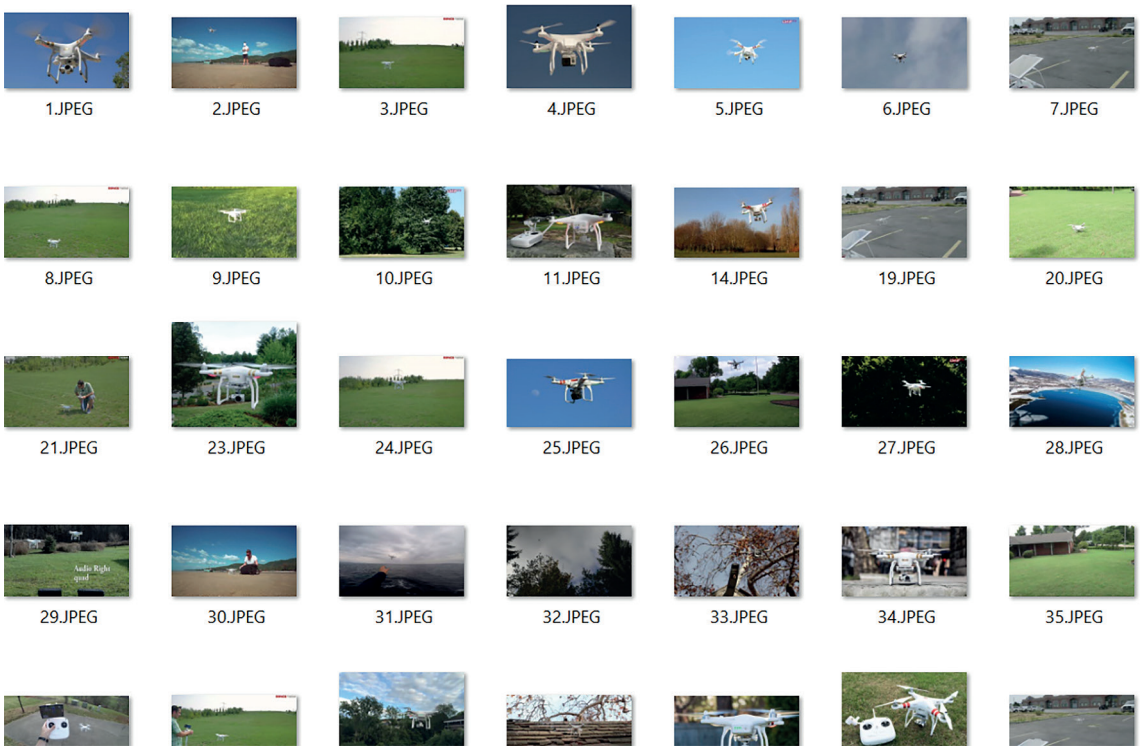

Рис. 3. Внешний вид изображений БЛА-целей в наборе данных

тем выше получится помехозащищенность алгоритма. Также важно указать, что чем больше обучающая выборка (набор данных), тем стабильнее будет работать анализ полученных изображений.

Наборы данных, как готовые картинки (изображения объектов) можно брать из разных источников (например, с помощью поиска в браузере, скачивать ряды изображений или же обращаться к наборам данных на различных платформах и в разных источниках), также можно использовать наборы фотографий объектов в разных ракурсах и с разным разрешением таким образом формируя необходимые для обработки и обучения нейронной сети наборы данных, примером служит открытый набор данных с платформы Kaggle [11]. Рассмотрим пример внешнего вида сформированного набора данных (рис. 3).

Представленные на рисунке 3 изображения находятся в сформированном наборе данных, в котором представлено 1500 изображений различных типов БЛА-целей.

Также в наборе данных присутствуют изображения для проверки промежуточных результатов и проверки итоговых результатов обучения нейронной сети. Важно отметить следующее правило, что данные «тренировки» и данные «проверки» никогда не должны пересекаться, то есть нейронная сеть при обучении никогда не должна иметь среди тренировочных изображений, изображения для проверки и наоборот, это требуется для достижения наилучшего результата.

Для разметки изображений предполагается использовать специализированную программу. Среди известных и популярных программ разметки, можно выделить LabelImg из репозитория GitHub [12].

Данное приложение позволяет производить разметку (аннотацию) изображений одно за другим, последовательно. Также в программе есть возможность выбора в каком формате сохранять аннотацию (Pascal/VOC и YOLO).

Данные для обучения модели разделены на обучающую и проверочную выборку в соотношении 80 % на 20 %. Перед запуском процесса обучения определяем параметры: размер изображения, батча, количество эпох для обучения, загружаем значения гиперпараметров в файле .yaml. В качестве алгоритма оптимизации используем стохастический градиентный спуск.

Процесс обучения производился на 30 эпохах. Значения метрик представлены на рисунках (рис. 4, рис. 5, рис. 6).

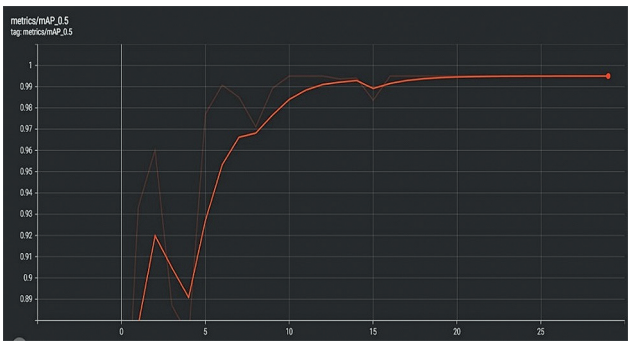

Рис. 4. Значение метрики mAP@0.5

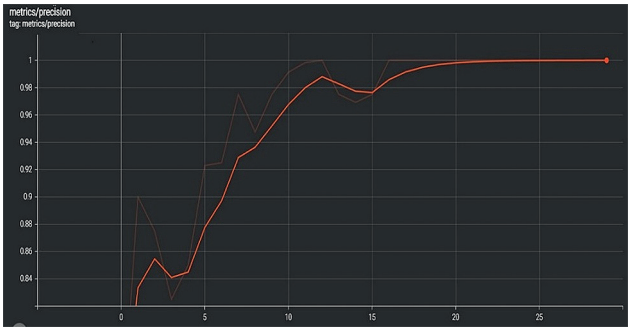

Рис. 5. Значение метрики mAP@0.5

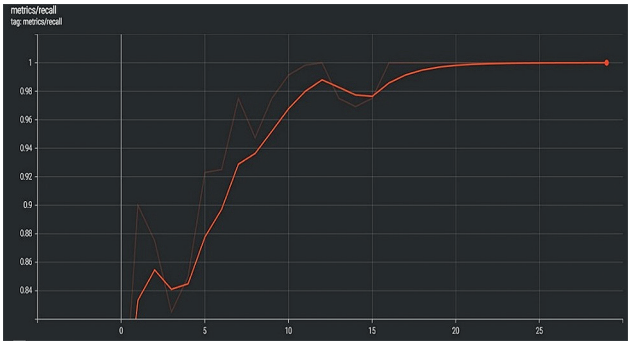

Рис. 6. Значение метрики precision

Зависимости, приведенные на рисунках 4, 5, 6 позволяют сделать вывод о достижении моделью нейронной сети оптимальных результатов на 25 эпохе обучения, значение метрик: mAP@0.5 = 99,5, precision = 99,5, recall = 99,5. Тестирование модели на 500 изображениях БПЛА. Изображения из тестового набора, представленные на рисунках (рис. 7, рис. 8) показывают, что модель отлично определяет bounding box объектов с высоким показателем confidence.

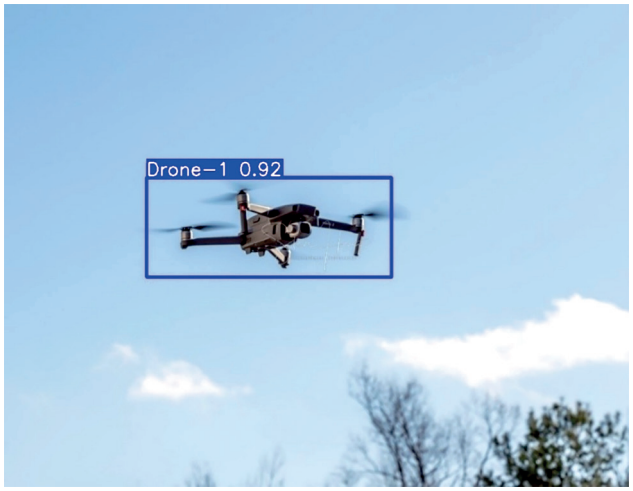

Рис. 7. Результаты тестирования модели

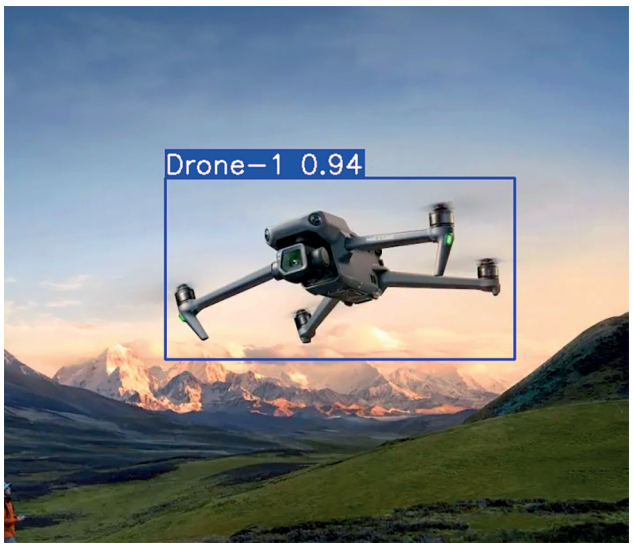

Рис. 8. Результаты тестирования модели

Результаты

Конечным результатом обучения нейронной сети является формирование ряда файлов, среди которых есть файл весовых коэффициентов или файл весов. Несмотря на то, что производится процесс обучения нейронной сети проверка результатов обучения может оценивать, насколько текущая эпоха справляется с наиболее лучшей. То есть, в процессе обучения может выйти так, что последняя итерация обучения не самая выгодная и тогда для получения лучшего результата следует обращаться ко второму файлу, который хранит улучшенную итерацию обучения в сравнении со всеми эпохами.

Необходимо отметить, что применение алгоритмов трекинга [13], учитывающих временные зависимости между кадрами, играет ключевую роль в анализе динамики движения целей, поскольку позволяет не только фиксировать текущее положение объектов, но и прогнозировать их перемещение, анализируя историю движения. Такие методы, как DeepSORT, ByteTrack [14] или LSTM-сети [15], значительно повышают точность сопровождения в условиях окклюзий, изменений освещенности и сложного фона, где традиционные детекторы дают сбои. Однако их использование создает существенную вычислительную нагрузку на бортовые системы БЛА, особенно при групповом применении, когда требуется параллельная обработка множества видеопотоков в реальном времени. Это делает критически важными дальнейшие исследования в области оптимизации — разработку легковесных архитектур, квантование моделей и аппаратное ускорение, — поскольку без таких мер сложные алгоритмы могут оказаться неприменимыми из-за ограниченных вычислительных ресурсов. В то же время, учет временных зависимостей не только улучшает устойчивость системы к ложным срабатываниям и пропускам целей, но и снижает общую нагрузку за счет уменьшения количества повторных детекций, сохраняя идентификацию объектов даже при их кратковременном исчезновении. Таким образом, поиск баланса между точностью трекинга и производительностью остается ключевой задачей, требующей как совершенствования алгоритмов, так и оптимизации их реализации для работы в ресурсоограниченных условиях бортовых систем.

В конечном итоге, используя приведенные в данной статье инструменты, можно сформировать программное обеспечение, которое может быть встроено как на программном уровне в виде дополнительного алгоритма в код большей программы управления группой БЛА, так и в виде отдельного приложения, в различные системы наблюдения и принятия решения.

Литература

1. Моисеев В. С. Групповое применение беспилотных летательных аппаратов: монография. – Казань: Редакционно-издательский центр «Школа», 2017. 572 с.
2. Евдокименков В. Н., Красильщиков М. Н., Оркин С. Д. Управление смешанными группами пилотируемых и беспилотных летательных аппаратов в условиях единого информационно-управляющего поля. МАИ, 2015, 272 с.
3. Васильев С. Н., Евдокименков В. Н., Красильщиков М. Н. Проблемы управления сложными динамическими объектами авиационной и космической техники. М., Машиностроение, 2015, 519 с.
4. Гончаренко В. И., Лебедев Г. Н. Задача оперативной двумерной маршрутизации группового полета беспилотных летательных аппаратов // Известия РАН. Теория и системы управления, 2019, № 1, с. 153–166.
5. Гончаренко В. И., Лебедев Г. Н., Михайлин Д. А., Царева О. Ю. Выбор множества приоритетных наземных объектов наблюдения с помощью беспилотных летательных аппаратов и маршрутизация их полета // Вестник компьютерных и информационных технологий, № 2, 2019 г., С. 3–12.
6. Гончаренко В. И., Желтов С. Ю., Князь В. А., Лебедев Г. Н., Михайлин Д. А., Царева О. Ю. Интеллектуальная система планирования групповых действий беспилотных летательных аппаратов при наблюдении наземных мобильных объектов на заданной территории // Известия Российской академии наук. Теория и системы управления. 2021. № 3, с. 39–56.
7. Небаба С. Г., Марков Н. Г. Сверточные нейронные сети семейства YOLO для мобильных систем компьютерного зрения // Компьютерные исследования и моделирование. – 2024. – Т. 16. – №. 3. – С. 615–631.
8. Использование нейронной сети для детекции пылевого облака в производственном помещении / Н. А. Васильев, К. А. Зарубин, О. С. Лаута, Д. С. Ситдиков // Россия молодая: Сборник материалов XVI всероссийской, научно-практической конференции молодых ученых с международным участием, Кемерово, 16–19 апреля 2024 года. – Кемерово: Кузбасский государственный технический университет имени Т. Ф. Горбачева, 2024. – С. 31675.1–31675.5.
9. Ali M. L., Zhang Z. The YOLO framework: A comprehensive review of evolution, applications, and benchmarks in object detection // Computers. – 2024. – Т. 13. – №. 12. – С. 336.
10. Хрящёв В. В., Котов Н. В., Приоров А. Л. Исследование алгоритмов на базе нейросетевой архитектуры YOLO в задаче детектирования полипов на колоноскопических видеоданных // Графиконференции по компьютерной графике и зрению. – 2023. – Т. 33. – С. 590–597.
11. Drone Dataset (UAV) [Электронный ресурс] // URL https://www.kaggle.com/datasets/dasmehdixtr/drone-dataset-uav/ (дата обращения: 15.03.2025).
12. ModifiedOpenLabelling [Электронный ресурс] // URL: https://github.com/ivangrov/ModifiedOpenLabelling/ (дата обращения: 25.03.2025).
13. Rathore P. S. et al. Benchmarking Object Detection and Tracking for UAVs: An Algorithmic Comparison // 2024 IEEE International Conference on Vehicular Electronics and Safety (ICVES). – IEEE, 2024. – С. 1–6.
14. Мальцева Н. А. и др. Качество методов трекинга с реидентификацией объектов // Вестник Дагестанского государственного технического университета. Технические науки. – 2024. – Т. 51. – №. 3. – С. 103–109.
15. Ситдиков, Д. С. Исследование применимости модели CNN-LSTM для детекции объектов в режиме реального времени / Д. С. Ситдиков, К. А. Зарубин, Н. А. Васильев // Системы интеллектуального управления и искусственный интеллект: теория и практика: Сборник трудов II национальной научно-практической конференции, Санкт-Петербург, 27 июня 2024 года. – Санкт-Петербург: Федеральное государственное бюджетное образовательное учреждение высшего образования Государственный университет морского и речного флота им. адмирала С. О. Макарова, 2024. – С. 102–107.

IMPLEMENTATION OF AN ONBOARD ALGORITHM FOR TARGET SEARCH, IDENTIFICATION, RECOGNITION, AND SUBSEQUENT ENGAGEMENT USING TRAINED NEURAL NETWORKS

Sitdikov D. S.[3], Vasiliev N. A.[4]

Keywords: *military didactics, electronic information and educational environment of a military university, teaching military engineering disciplines, immersive technologies, artificial intelligence in education.*

Abstract

The purpose of the work *is to analyze the didactic features of modern military education using advanced digital technologies.*

Research results: *as a result, the following set of didactic functions of an intellectual learning system can be distinguished: adaptive, transformative, coordinating, forming an integral system, developing, integrating, ensuring the consolidation of knowledge, self-control, individualized approach and differentiation, self-education, methodological, and analytical. The development of didactics of military engineering disciplines in the digital age will be characterized by the following trends: expansion of the conceptual and terminological stock, the emergence of new theoretical concepts, didactic systems and teaching models; preservation of the main scientific functions of didactics: descriptive, explanatory and predictive; clarification of existing or discovery of new laws and patterns of the educational process, which will become the basis for the creation of normative models. The theory will be based on the phenomenological material collected during the study of distance education.*

Scientific novelty: *the introduction of end-to-end digital technologies and innovative techniques significantly improves the quality of education and training of military specialists, as well as enhances the effectiveness of management of military structures and combat units. This approach will make it possible to adapt to changes in technology and the requirements for military training, as well as to anticipate their impact on military education in the coming years.*

References

1. Moiseev V. S. Gruppovoe primenenie bespilotnyh letatel'nyh apparatov: monografija. – Kazan': Redakcionno-izdatel'skij centr «Shkola», 2017. 572 s.
2. Evdokimenkov V. N., Krasil'shhikov M. N., Orkin S. D. Upravlenie smeshannymi gruppami pilotiruemyh i bespilotnyh letatel'nyh apparatov v uslovijah edinogo informacionno-upravljajushhego polja. MAI, 2015, 272 c.
3. Vasil'ev S. N., Evdokimenkov V. N., Krasil'shhikov M. N. Problemy upravlenija slozhnymi dinamicheskimi ob#ektami aviacionnoj i kosmicheskoj tehniki. M., Mashinostroenie, 2015, 519 s.
4. Goncharenko V. I., Lebedev G. N. Zadacha operativnoj dvumernoj marshrutizacii gruppovogo poleta bespilotnyh letatel'nyh apparatov // Izvestija RAN. Teorija i sistemy upravlenija, 2019, № 1, s. 153–166.
5. Goncharenko V. I., Lebedev G. N., Mihajlin D. A., Careva O. Ju. Vybor mnozhestva prioritetnyh nazemnyh ob#ektov nabljudenija s pomoshh'ju bespilotnyh letatel'nyh apparatov i marshrutizacija ih poleta // Vestnik komp'juternyh i informacionnyh tehnologij, № 2, 2019 g., S. 3–12.
6. Goncharenko V. I., Zheltov S. Ju., Knjaz' V. A., Lebedev G. N., Mihajlin D. A., Careva O. Ju. Intellektual'naja sistema planirovanija gruppovyh dejstvij bespilotnyh letatel'nyh apparatov pri nabljudenii nazemnyh mobil'nyh ob#ektov na zadannoj territorii // Izvestija Rossijskoj akademii nauk. Teorija i sistemy upravlenija. 2021. № 3, s. 39–56.
7. Nebaba S. G., Markov N. G. Svertochnye nejronnye seti semejstva YOLO dlja mobil'nyh sistem komp'juternogo zrenija // Komp'juternye issledovanija i modelirovanie. – 2024. – T. 16. – №. 3. – S. 615–631.

3 Dmitry S. Sitdikov, junior researcher, Military Academy of Communications, St. Petersburg, Russia. E-mail: dima.sitdikov.99@mail.ru

4 4 Nikita A. Vasiliev, Ph.D. of Technical Sciences, Deputy Head of the Research Department of the Research Center, Military Academy of Communications, St. Petersburg, Russia. E-mail: vasn2020@mail.ru

8. Ispol'zovanie nejronnoj seti dlja detekcii pylevogo oblaka v proizvodstvennom pomeshhenii / N. A. Vasil'ev, K. A. Zarubin, O. S. Lauta, D. S. Sitdikov // Rossija molodaja: Cbornik materialov XVI vserossijskoj, nauchno-prakticheskoj konferencii molodyh uchenyh s mezhdunarodnym uchastiem, Kemerovo, 16–19 aprelja 2024 goda. – Kemerovo: Kuzbasskij gosudarstvennyj tehnicheskij universitet imeni T. F. Gorbacheva, 2024. – S. 31675.1-31675.5.
9. Ali M. L., Zhang Z. The YOLO framework: A comprehensive review of evolu-tion, applications, and benchmarks in object detection // Computers. – 2024. – T. 13. – №. 12. – S. 336.
10. Hrjashhjov V. V., Kotov N. V., Priorov A. L. Issledovanie algoritmov na baze nejrosetevoj arhitektury YOLO v zadache detektirovanija polipov na kolonoskopicheskih videodannyh // Grafikonferencii po komp'juternoj grafike i zreniju. – 2023. – T. 33. – S. 590–597.
11. Drone Dataset (UAV) [Jelektronnyj resurs] // URL https://www.kaggle.com/datasets/dasmehdixtr/drone-dataset-uav/ (data obrashhenija: 15.03.2025).
12. ModifiedOpenLabelling [Jelektronnyj resurs] // URL: https://github.com/ivangrov/ModifiedOpenLabelling/ (data obrashhenija: 25.03.2025).
13. Rathore P. S. et al. Benchmarking Object Detection and Tracking for UAVs: An Algorithmic Comparison // 2024 IEEE International Conference on Vehicular Electronics and Safety (ICVES). – IEEE, 2024. – S. 1–6.
14. Mal'ceva N. A. i dr. Kachestvo metodov trekinga s reidentifikaciej ob#ektov // Vestnik Dagestanskogo gosudarstvennogo tehnicheskogo universiteta. Tehnicheskie nauki. – 2024. – T. 51. – №. 3. – S. 103–109.
15. Sitdikov, D. S. Issledovanie primenimosti modeli CNN-LSTM dlja detekcii ob#ektov v rezhime real'nogo vremeni / D. S. Sitdikov, K. A. Zarubin, N. A. Vasil'ev // Sistemy intellektual'nogo upravlenija i iskusstvennyj intellekt: teorija i praktika: Sbornik trudov II nacional'noj nauchno-prakticheskoj konferencii, Sankt-Peterburg, 27 ijunja 2024 goda. – Sankt-Peterburg: Federal'noe gosudarstvennoe bjudzhetnoe obrazovatel'noe uchrezhdenie vysshego obrazovanija Gosudarstvennyj universitet morskogo i rechnogo flota im. admirala S. O. Makarova, 2024. – S. 102–107.

СИНТЕЗ СТРУКТУРЫ УЗЛА СВЯЗИ ПОЛЕВОГО ПОДВИЖНОГО ПУНКТА УПРАВЛЕНИЯ ОБЩЕВОЙСКОВОГО ОБЪЕДИНЕНИЯ

Кротов А. С.[1], Мурашко В. П.[2], Сундуков А. П.[3]

DOI:10.21681/3034-4050-2025-4-43-51

Ключевые слова: *разведзащищенность, живучесть, организационно-техническая структура, элементы узла связи, модульность, универсальные комплекты связи, система управления.*

Аннотация

Цель работы: *на основе анализа опыта специальной военной операции и обобщения исходных данных, разработать организационно-техническую структуру узла связи полевого подвижного пункта управления общевойскового объединения, обеспечивающую выполнение требований, предъявляемых к узлам связи в современных условиях.*

Метод исследования *сочетает в себе построение аналитических и имитационных моделей, способных учитывать факторы неопределенности и многоаспектность процессов на этапах построения и функционирования узлов связи полевых подвижных пунктов управления общевойсковых объединений.*

Результаты исследования: *определена степень унификации элементов узлов связи, согласованная с принятыми решениями по созданию типового комплекта средств связи в тактическом звене управления. Модули пунктов управления в новом облике позволят, не снижая способности узлов связи по предоставлению услуг связи должностным лицам органов управления, значительно сократить состав аппаратных (станций) связи, а также существенно снизить затраты на создание перспективных узлов связи и направлены на формирование организационно-технической структуры узлов связи полевых подвижных пунктов управления общевойсковых объединений в радикально изменившихся условиях их боевого применения, обеспечивающей заданную разведзащищенность и живучесть.*

Практическая ценность: *учитываются возросшие возможности средств разведки и поражения противника, влияющие на выполнение требований, предъявляемых к узлам связи, в первую очередь, по разведзащищенности и живучести. При формировании организационно-технической структуры узла связи полевого подвижного пункта управления общевойскового объединения обосновывается принцип модульного их построения на основе закрепления унифицированных (базовых) средств связи и автоматизации за элементами групп боевого управления пунктов управления объединений.*

Введение

В современном вооружённом конфликте, в котором информационные технологии и средства связи играют незаменимую роль, важность узлов связи, являющихся основными элементами в системе связи вех звеньев управления, только возрастает. От их состава, структуры и функционирования во-многом зависит, в первую очередь, разведзащищенность и живучесть полевых подвижных пунктов управления [1], элементами которых они являются.

До настоящего времени во всех работах, посвящённых синтезу структуры узлов связи (УС) пунктов управления (ПУ) объединений, в качестве исходных данных всегда выступали сведения о стоящих перед УС задачах, условиях их функционирования, наличии и состоянии сил и средств связи. Этот подход оправдан и для дальнейших исследований. Однако, современные боевые действия показали значительно возросшие возможности вероятного противника как в области средств разведки, так и в средствах поражения.

1 Кротов Антон Сергеевич, адъюнкт кафедры боевого применения войск связи Военной академии связи имени Маршала Советского Союза С. М. Будённого, г. Санкт-Петербург, Россия. E-mail: kas.krotov@yandex.ru

2 Мурашко Вячеслав Павлович, доцент кафедры боевого применения войск связи Военной академии связи имени Маршала Советского Союза С. М. Будённого, г. Санкт-Петербург, Россия. E-mail: murashko1945@yandex.ru

3 Сундуков Анатолий Петрович, доцент кафедры боевого применения войск связи Военной академии связи имени Маршала Советского Союза С. М. Будённого, г. Санкт-Петербург, Россия. E-mail: as25p@yandex.ru

Особенно явно это проявилось в ходе специальной военной операции. Вооружённые Силы Российской Федерации были вынуждены менять подходы к построению системы управления и, соответственно, системы связи[4]. Так называемые «классические» решения по построению УС и ПУ[5] оказались уязвимыми. Из всей совокупности требований к УС, как основным элементам ПУ, на первый план были выдвинуты задачи по решению обеспечения разведзащищенности и живучести. Решение этих задач практически привело к тому, что на УС применение разработанных промышленностью аппаратных связи существенно ограничилось, а все больше находят применение «самодельные» аппаратные, малозаметные как военные объекты и оборудованные силами войск.

Предлагаемая синтезируемая структура узлов связи полевых подвижных пунктов управления общевойсковых объединений позволит в конечном итоге сократить потери сил и средств связи. Кроме того, появляется возможность научно обосновать состав базовых средств связи, на основе которых реализуется модульная структура УС и ПУ в целом.

Постановка задачи

Будем считать заданными сведения о стоящих перед УС задачах, условиях функционирования УС, наличии и состоянии сил и средств узловых и взаимодействующих подразделений связи, представленные в формализованном виде [2, 3].

К исходным данным отнесем следующие сведения:

1) определяемые структурой и порядком функционирования системы управления:

- количество информационных направлений, обеспечиваемых от данного ПУ с указанием их категории важности (отражается в ОТД УС ПУ, схеме-приказе (задаче) УС ПУ);
- состав данного ПУ (количество рабочих мест должностных лиц ПУ, на которых устанавливаются оконечные устройства связи и автоматизированного управления войсками, согласно утвержденного начальником штаба объединения расчету на их установку);
- порядок размещения элементов ГБУ на местности и их состав[6];
- прогнозируемый поток сообщений или интенсивность нагрузки, создаваемой должностными лицами ПУ на информационных направлениях в часы набольшей нагрузки, по видам связи и категориям абонентов и срочности сообщений;
- порядок перемещения ПУ;
- требования к ПУ (системе управления) по скрытности и устойчивости функционирования, мобильности;

2) определяемые структурой и порядком функционирования системы связи:

- потребное количество связей и каналов на информационных направлениях, организуемых от УС;
- порядок приема каналов и трактов из стационарной, полевой опорной сети связи и элементов единой сети электросвязи;
- порядок использования выделяемых в интересах УС ПУ радиопередающих средств и организации каналов дистанционного управления ими;

3) формируемые внешней средой:

- группировка средств разведки и радиоэлектронной борьбы вероятного противника и ее возможности по разведке и радиоэлектронному подавлению средств УС;
- стратегия применения вероятным противником ядерного и обычного оружия в целях воздействия на систему и УС;
- поражающие факторы ядерного и других видов оружия, их влияние на личный состав, технику и состояние связи;
- физико-географические и климатические условия;

4) обусловлена состоянием и развитием самих узлов связи:

- принципы построения УС ПУ и их элементов;
- требования, предъявляемые к УС;
- требования по размещению УС на местности;
- имеющиеся в наличии средства узла связи;
- численность личного состава и уровень его подготовки;
- порядок и способы каблирования и электроснабжения УС и его элементов;

4 Концепция развития системы управления ВС РФ на период до 2030 года. – М.: МО РФ, 2020

5 Жарский А. П., Шептура В. Н. Развитие организационно-технической структуры и способов боевого применения узлов связи пунктов управления оперативно-стратегических и оперативных объединений в 1945–1980 гг. // Военно-исторический журнал № 6. – М.: МО РФ, 2016.

6 Руководство по применению полевых подвижных пунктов управления объединений, соединений и воинских частей. – М.: ГОУ ГШ ВС РФ, 2018.

- количество транспортных единиц (аппаратных), размещаемых в районе ГБУ и в непосредственной близости от нее;
- эшелонирование сил и средств и предполагаемый порядок перемещения УС в ходе операции.

В качестве ограничений будем понимать фиксированные финансовые, временные, людские и технические ресурсы и возможности, различные нормативы, которых должен придерживаться начальник узла связи при определении варианта построения организационно-технической структуры УС ПУ [3].

Целью формирования структуры УС является определение множества элементов и связей между ними, распределения задач, возлагаемых на технические средства элементов УС и выбора комплекта средств связи, обеспечивающий решение задач, стоящих перед УС.

Решение задачи

Для решения разведывательных задач средствами радио и радиотехнической разведки по обнаружению и вскрытию УС и ПУ в целом наиболее важными факторами являются излучение и отражение энергии (радиоволн, света и т.д.) элементами, позволяющие оперативно обнаруживать наличие и деятельность разведываемого объекта в определённом районе. Именно на этом основывался подход по определению разведывательной защищенности при формировании структуры УС [4].

В настоящее время технический прорыв в области военной разведки позволяет наиболее эффективно применять видовую разведку в оптическом и инфракрасном диапазонах, которая является наиболее информативной для противника с применением летно-подъемных средств и средств низкоорбитальной группировки [5]. Данный вид разведки является наиболее эффективным, так как средства и комплексы связи обладают выраженными демаскирующими признаками, которые позволяют однозначно определить их оперативно-тактическое предназначение и принадлежность к звену управления. Так же необходимо учитывать и разведпризнаки, позволяющие агентам противника из числа местного населения определять места размещения и принадлежность УС.

Вероятность вскрытия объекта рассчитывается по формуле:

$$P_{\text{вскр}} = P_{\text{обз}} \cdot P_{\text{м}} \cdot P_{\text{р}},$$

где $P_{\text{обз}}$ – вероятность обзора участка местности; $P_{\text{м}}$ – вероятность выявления объекта на фоне местности; $P_{\text{р}}$ – вероятность распознания объекта.

$$P_{\text{обз}} = \frac{S_{\text{пол}}}{S_{\text{общ}}},$$

где $S_{\text{пол}}$ – площадь обозреваемой полосы; $S_{\text{общ}}$ – общая площадь размещения объекта.

$$P_{\text{м}} = f(D_{\text{ст}}, L, Z),$$

где $D_{\text{ст}}$ – признаковая структура; L – расстояние до объекта; Z – условия местности.

При вскрытии пункта управления противника интересуют в первую очередь сложные объекты и, в частности, определение их оперативно-тактической принадлежности [6]. Сложные объекты распознаются по особым, присущим только им демаскирующим признакам. Информативность (вес) простых объектов и их совокупность в сложном объекте характеризует их роль в процессе распознавания (определения оперативно-тактической принадлежности). Каждый элемент несет в себе долю информации о сложном объекте, частью которого он является. Распознавание любого дополнительного элемента или совокупности элементов приводит к повышению достоверности распознавания сложного объекта.

Структура пункта управления играет ключевую роль, так как она позволяет выделить существенные характеристики, которые помогают классифицировать или идентифицировать объект (признаковая доступность).

Признаковая доступность определяет возможности видов разведки противника по распознаванию УС ПУ. Особенности размещения и функционирования УС ПУ обусловливают наличие группы демаскирующих признаков, которые могут быть использованы противником при различных видах разведки (оптико-электронной, радиолокационной, инфракрасной, и т.п.). Основным демаскирующим признаком является совокупность одиночных объектов разведки, по которой вычисляется сложный объект.

Живучесть УС как объекта с распределённой структурой оценивается на трех уровнях:

- объектовая живучесть $p_{\text{ож}}$ – вероятность сохранения автономного элемента УС; такое

событие возможно, когда i-ый поражающий фактор применяемого оружия не превышает расчетного значения этого поражающего фактора для элемента УС;

- структурная живучесть $p_{сж}$ – вероятность сохранения минимальной топологической связности его элементов, при которой еще возможно управление войсками, т.е.

$$p_{сж} = p_{выж\ эл.ВСС} \cdot p_{выж\ эл.ПСС},$$

где $p_{выж\ эл.ВСС}$ – вероятность выживания хотя бы одного элемента УС, относящегося ко вторичным сетям связи; $p_{выж\ эл.ПСС}$ – вероятность выживания хотя бы одного элемента УС, относящегося к первичным сетям связи;

- функциональная живучесть $p_{фж}$ – вероятность сохранения связей на основных информационных направлениях не ниже заданного количества:

$$p_{фж} = p(N_{ост\ св} \geq N_{тр\ св}),$$

где $N_{ост\ св}$ – количество оставшихся действующих связей; $N_{тр\ св}$ – минимально требуемое количество действующих связей.

$$N_{тр\ св} = N_{св\ 1\ кат} + N_{св\ 2\ кат} + N_{св\ 3\ кат},$$

где $N_{св\ 1\ кат}$, $N_{св\ 2\ кат}$, $N_{св\ 3\ кат}$ – минимально требуемое количество действующих связей для направлений связи первой, второй и третьей группы важности соответственно.

Уничтожение УС ПУ и нарушение системы управления – это суть ведения боевых действий в XXI веке. Сегодня командные пункты практически невозможно спрятать и крайне сложно защитить. Поиск пункта управления и нанесение по нему удара – первоочередная задача противника [7].

При определении структуры полевого узла связи до начала специальной военной операции главенствовал принцип объединения однотипных средств связи в элементы УС по их функциональному предназначению в системе связи. В связи с этим существующие структуры узлов связи не могут являться ориентирами при синтезе перспективных УС, когда необходимо прежде всего ориентироваться на радикально изменившиеся оперативные условия и на современную интеграцию вторичных сетей связи на основе применения единой Ethernet технологии коммутации пакетов [8].

Таким образом, на сегодняшний день классический подход по формированию структуры УС должен быть существенно изменён. Необходимо существенно уменьшить состав УС. Например, УС командного пункта объединения при «классическом» построении включал несколько десятков машин различного назначения.

Должен быть изменён и подход, при котором УС считается вскрытым радиоразведкой противника, если вскрыто не менее 80 % радиосетей (радионаправлений), организованных от этого УС. Для противника приоритетным является не вскрытие УС, а выявление значимых с точки зрения связи объектов, в т.ч. и «одиночных», поражение которых может затруднить или даже сорвать управление войсками.

Необходимо уточнять и требования к разведзащищенности УС ПУ, в соответствии с которыми допустимое время функционирования УС $T_{доп\ УС}$ для различных звеньев управления должно составлять не менее 25 ч ($T_{доп\ УС} \geq 25$ ч) в оперативном и не менее 5–10 ч ($T_{доп\ УС} \geq 5$–10 ч) в тактическом звеньях управления. В современном противостоянии противник не будет вскрывать такое количество радиосетей (радионаправлений), организованных от УС, и затрачивать на это значительные средства и время [9]. Допустимое время функционирования УС $T_{доп\ УС}$ предопределяло и необходимость перемещения УС ПУ один раз в сутки-двое в оперативном звене управления и несколько раз в сутки в тактическом звене управления. Опыт специальной военной операции показал, что перемещение УС ПУ в соответствии с указанными интервалами времени приводит к его обнаружению средствами разведки противника с последующим воздействием на него огневыми средствами.

Всё это предопределило дальнейшую задачу по разработке новой, адаптивной к изменившимся условиям ведения боевых действий, структуре УС. Соответственно необходимо скорректировать методику синтеза структуры узла связи полевого подвижного пункта управления (ППУ) объединения.

В процессе разработки структуры УС возникает необходимость учесть множество факторов, влияющих на порядок функционирования УС, что вносит определенные трудности в формализацию процесса разработки

и не позволяет достичь поставленной цели сразу, в один этап. Поэтому задачу формирования структуры УС предлагается решать в несколько этапов.

На первом этапе необходимо решить оптимизационную задачу по выбору основных показателей. Наиболее часто встречаемый подход при решении вопроса по оценке эффективности функционирования узла связи, когда определяется один (главный) показатель, а далее стремление обратить его в максимум. Остальные показатели переводятся в разряд ограничений. По главному показателю и производится выбор предпочтительного варианта узла связи. Вместе с тем, однокритериальная оценка, в ряде случаев, может привести к неадекватности решаемой задачи. Выбор основных показателей, по которым можно дать оценку эффективности узла связи, должны быть увязаны с решаемыми им задачами и условиями обстановки.

Требования, предъявляемые к УС ПУ, полностью определяются его свойствами, важными с точки зрения обеспечения цели функционирования:

1) постоянная готовность к немедленной передаче (приему) всех видов информации (сообщений);

2) своевременная и достоверная передача заданного потока сообщений и безопасность связи;

3) устойчивость функционирования УС, которая включает:

- живучесть узла связи;
- надежность средств связи и образованных на УС каналов (трактов) связи;
- помехоустойчивость и электромагнитную совместимость всех развертываемых на УС радиоэлектронных средств;

4) разведзащищенность УС;

5) мобильность (для подвижных узлов связи);

6) максимальное удобство пользования средствами связи и автоматизации должностным лицам органов управления;

7) доступность УС к ресурсу опорной сети связи;

8) обеспечение маневра средствами, каналами, видами и услугами связи.

Анализ требований к узлам связи позволяет выделить ряд существенных свойств, на основании которых могут быть выделены частные показатели. Такими свойствами являются разведзащищенность, живучесть и мобильность.

Таким образом, для оценки функционирования УС ППУ при синтезе его структуры предлагается применить группу показателей, достаточно полно характеризующих УС с точки зрения выполнения целевого предназначения в прогнозируемых условиях.

На втором этапе необходимо выбрать принцип построения организационно-технической структуры узла связи и в соответствии с выбранным принципом определить тип и количество элементов, входящих в состав УС.

В настоящее время существует три принципа построения ОТС полевого узла связи [10]:

1) объединение однотипных средств связи и автоматизации в элементы по их функциональному предназначению в системе связи (как правило, по родам и видам связи);

2) объединение разнотипных средств связи и автоматизации в элементы по их оперативно-тактическому предназначению в системах управления и связи;

3) модульный.

При этом под модульным построением зачастую понимают, формирование традиционных элементов групп боевого управления ПУ, что не соответствует сущности модульности. Модульный принцип построения предполагает наличие в составе каждого модуля на элементе ГБУ унифицированных средств и комплексов связи[7], с помощью которых можно изменять возможности модуля в зависимости от выполняемых задач и количества ДЛ на данном элементе ПУ.

Каждый из этих принципов в равной степени может быть использован при разработке структуры УС. В ходе специальной военной операции произошел переход от объединения однотипных средств связи и автоматизации в элементы УС по их функциональному предназначению в системе связи к закреплению разнотипных средств связи и автоматизации по их оперативно-тактическому предназначению в системах управления и связи, то есть к закреплению за элементами ГБУ, а одновременная унификация телекоммуникационного оборудования влечёт за собой переход к модульному построению УС.

Переход к модульному построению УС позволит более эффективно распределять

7 Аппаратные полевых узлов связи: учебное пособие. Часть 1 и 2. 3-е изд., доп. и перераб./ под ред. В. Г. Иванова. СПб.: ВАС, 2021.

информационные потоки между группами должностных лиц ПУ, которые в сложившейся обстановке в большинстве своем распределены территориально на определенном расстоянии от центра боевого управления [11].

Разработка и принятие на снабжение унифицированного комплекта средств связи для перспективных УС объединений позволит, в том числе, снизить их стоимость для ВС РФ [12, 13]. При этом в тактическом звене управления аналогичный по назначению унифицированный комплект средств связи уже имеется.

Таким образом, структура УС будет связно зависима от предлагаемой системы пунктов управления объединения, которая исходя из распределения оперативного состава объединения будет состоять из элементов, равных по составу, количество которых соответствует элементам ГБУ ППУ.

Важно учесть, что основной элемент ГБУ, а именно центр боевого управления, должен дублироваться. Для выбора рационального варианта его состава, необходимо определить точное количество элементов в прогнозируемых условиях функционирования и задать каждому из них коэффициент важности.

На третьем этапе, после определения состава УС, формируется его организационно-техническая структура, главным образом связность между элементами УС и ПУ в целом (рис. 1).

Каждый модуль имеет унифицированный комплект связи, который является узлом связи элемента ППУ и способен предоставить следующие виды услуг связи:

- автоматическую телефонную засекреченную связь (АТС-Р);
- передачи данных и файлового обмена в закрытом сегменте сети передачи данных (ЗС СПД);
- защищенную видеотелефонную и видеоконференцсвязь (ЗВКС);
- защищенную аудиоконференцсвязь (ЗАКС) в интересах работы оперативных дежурных ПУ, системы оповещения ПВО и системы связи;

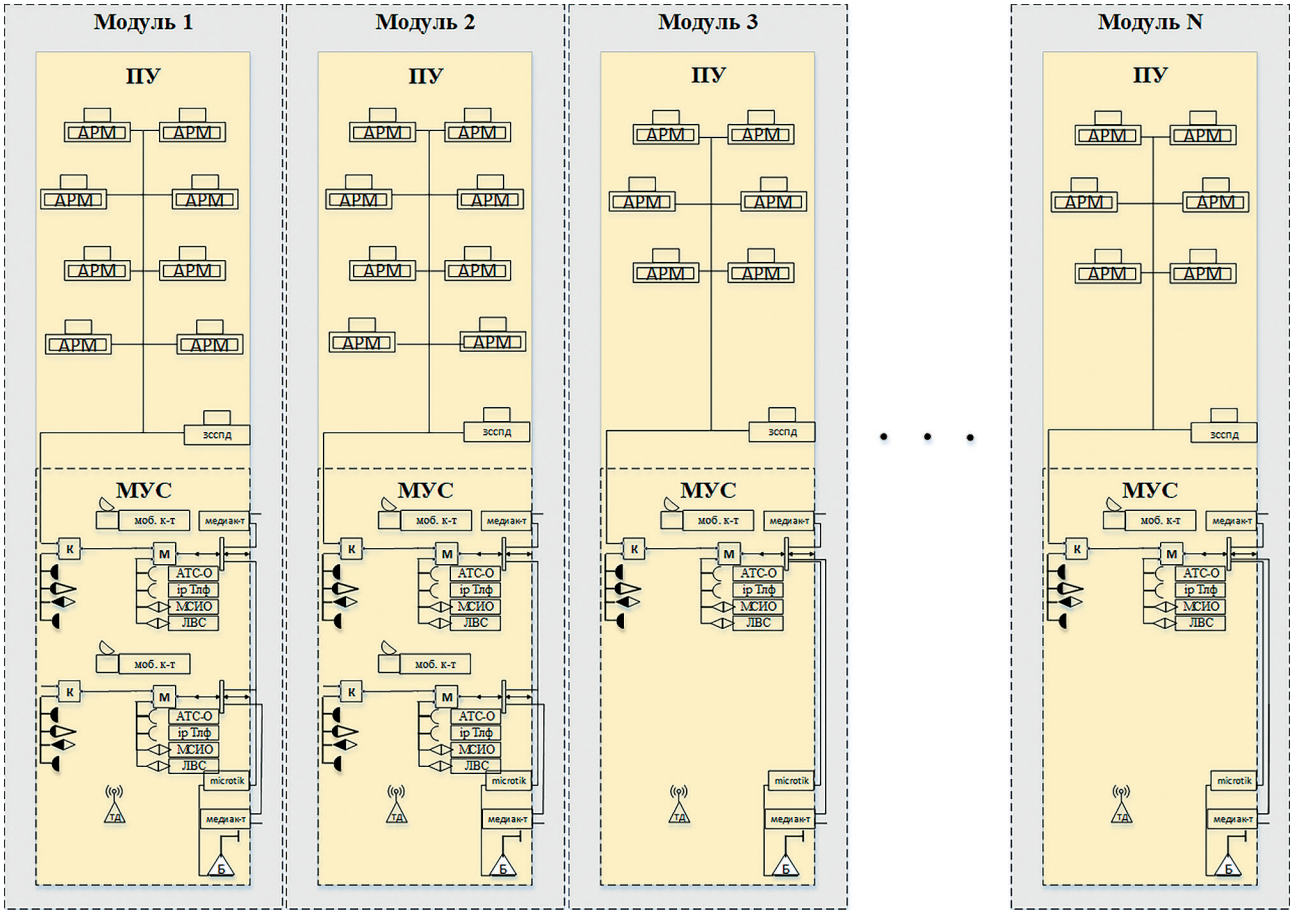

Рис.1. Организационно-техническая структура УС ППУ

- предоставление канального ресурса и подключения к ЗС СПД базы автоматизированной системы управления «Объединение – 2020», АСУ разведкой «Дозор», ПВО «Поляна», «Бастион»;
- обеспечение телефонных переговоров в сети *IP*-телефонии и в радиолиниях на радиостанциях тактического звена управления с применением ключей шифрования;
- обеспечение телефонной засекреченной связи по каналам спутниковой (с применением ССС типа Р-444 различных модификаций) и радиосвязи;
- обеспечение передачи данных в МСИО;
- обеспечение видеотрансляции как от БПЛА, так и от стационарных комплексов видеотрансляции и *IP*-камер.

Заключение

Новый подход к формированию УС, где к каждому элементу ППУ связно закреплены группы предоставления услуг связи с унифицированными комплектами связи (модули ПУ), позволит таким модулям действовать самостоятельно на значительном удалении друг от друга. Тем самым существенно повышается разведзащищенность ПУ, а взаимозаменяемость одного модуля на другой позволит повысить его функциональную живучесть.

Литература

1. Кравцов Е. В. Модели обоснования разведзащищенности критически важных объектов // Материалы IV международной научно-практической конференции. – Елец, 2020.
2. Иванов В. Г., Тевс О. П., Сарафанников В. С., Корягин С. А., Савицкий А. Ю. Обоснование обобщенных тактико-технических требований к средствам и комплексам связи // Стратегическая стабильность, № 3. – СПб.: ВАС, 2023.
3. Алексеев П. Н., Баранов Р. П. Новая парадигма управления войсками (силами) // Военно-теоретический журнал: Военная мысль № 5. – М.: МО РФ, 2021.
4. Корепанов В. О., Шумов В. В. Моделирование военных, боевых и специальных действий // Военно-теоретический журнал: Военная мысль № 1. – М.: МО РФ, 2023.
5. Andrew Eversden. Army's testbed ISR business jets are opening doors to new mission possibilities // Breaking Defense. – New York City, 2023.
6. Пермяков А. С., Лепешкин О. М., Митрофанов М. В. Проблемы защищенности информационно-телекоммуникационных сетей специального назначения // Радиолокация, навигация, связь. Сборник трудов XXVI Международной научно-технической конференции., № 3. – Воронеж: ВГУ. 2020.
7. John Antal. Preparing Tactical Command Posts for the Next War // European Security & Defence. – Bonn: 2023.
8. Падишин С. А., Сазыкин А. М., Савицкий А. Ю. Модель планирования и постановки задач на обеспечение связи объединения, учитывающая возможность использования технологии цифровых двойников // Известия Российской Академии Ракетных и Артиллерийских наук, № 4 – СПб.: РАРАН, 2024.
9. Самохин Е. С., Иванов Р. М. Предложения по сокращению времени развертывания (свертывания) элементов пункта управления объединения в условиях применения противником высокоточного оружия // Сборник статей III Всероссийской научно-технической конференции. Том 3. – Анапа, 2021.
10. Иванов В.Г. Модель технической основы системы управления специального назначения в едином информационном пространстве на основе конвергентной инфраструктуры системы связи: монография (монография). – СПб.: СПбПУ, 2018.
11. Иванов Р. М. Логико-вероятностная модель структуры узла связи специального назначения, функционирующего в условиях дестабилизирующего воздействия противника // Вопросы оборонной техники. Серия 16: № 3, – СПб.: МО РФ, 2022.
12. Тевс О. П., Исаченко В. Г. Особенности и выводы организации и обеспечения связи при проведении специальной военной операции // Итоги науки и техники: Научно-технический сборник № 120. Труды академии. – СПб.: ВАС, 2022.
13. Тишков В. В., Иванов В. Г., Лукьянчик В. Н. Обоснование облика построения перспективных комплексов и средств связи на основе опыта организации связи при проведении специальной военной операции. Военно-теоретический журнал: Военная мысль № 9. – М.: МО РФ, 2023.

SYNTHESIS OF THE STRUCTURE OF THE COMMUNICATION CENTER OF THE FIELD MOBILE CONTROL POST OF THE COMBINED ARMS ASSOCIATION

Krotov A. S.[8], Murashko V. P.[9], Sundukov A. P.[10]

Keywords: *intelligence protection, survivability, organizational and technical structure, elements of the communication center, modularity, universal communication sets, control system.*

Abstract

The purpose of the work: *on the basis of the analysis of the experience of a special military operation and the generalization of the initial data, to develop the organizational and technical structure of the communication center of the field mobile control post of the combined arms formation, ensuring the fulfillment of the requirements for communication centers in modern conditions.*

The research method *combines the construction of analytical and simulation models that can take into account the factors of uncertainty and multifaceted processes at the stages of construction and operation of communication centers of field mobile command posts of combined arms formations.*

Results of the study: *the degree of unification of the elements of communication centers was determined, coordinated with the decisions made on the creation of a standard set of communication facilities in the tactical command and control level. The modules of the control points in the new look will allow, without reducing the ability of communication centers to provide communication services to officials of the management bodies, to significantly reduce the composition of communication equipment (stations), as well as to significantly reduce the cost of creating promising communication centers and are aimed at forming the organizational and technical structure of communication centers of field mobile control posts of combined arms formations in radically changed conditions of their combat use. providing a given reconnaissance protection and survivability.*

Practical value: *the increased capabilities of reconnaissance and destruction of the enemy, which affect the fulfillment of the requirements for communication centers, primarily in terms of reconnaissance protection and survivability, are taken into account. When forming the organizational and technical structure of the communication center of a field mobile control post of a combined arms formation, the principle of their modular construction is substantiated on the basis of consolidation of unified (basic) means of communication and automation for the elements of combat control groups of command posts of formations.*

References

1. Kravcov E. V. Modeli obosnovanija razvedzashhishhennosti kriticheski vazhnyh ob#ektov // Materialy IV mezhdunarodnoj nauchno-prakticheskoj konferencii. – Elec, 2020.
2. Ivanov V. G., Tevs O. P., Sarafannikov V. S., Korjagin S. A., Savickij A. Ju. Obosnovanie obobshhennyh taktiko-tehnicheskih trebovanij k sredstvam i kompleksam svjazi // Strategicheskaja stabil'nost', № 3. – SPb.: VAS, 2023.
3. Alekseev P. N., Baranov R. P. Novaja paradigma upravlenija vojskami (silami) // Voenno-teoreticheskij zhurnal: Voennaja mysl' № 5. – M.: MO RF, 2021.
4. Korepanov V. O., Shumov V. V. Modelirovanie voennyh, boevyh i special'nyh dejstvij // Voenno-teoreticheskij zhurnal: Voennaja mysl' № 1. – M.: MO RF, 2023.
5. Andrew Eversden. Army's testbed ISR business jets are opening doors to new mission possibilities // Breaking Defense. – New York City, 2023.
6. Permjakov A. S., Lepeshkin O. M., Mitrofanov M. V. Problemy zashhishhennosti informacionno-telekommunikacionnyh setej special'nogo naznachenija // Radiolokacija, navigacija, svjaz'. Sbornik trudov XXVI Mezhdunarodnoj nauchno-tehnicheskoj konferencii., № 3. – Voronezh: VGU. 2020.
7. John Antal. Preparing Tactical Command Posts for the Next War // European Security & Defence. – Bonn: 2023.

8 Anton S. Krotov, Adjunct of the Department of Combat Use of Signal Troops, Military Academy of Communications, St. Petersburg, Russia. E-mail: kas.krotov@yandex.ru

9 Vyacheslav P. Murashko, Associate Professor of the Department of Combat Use of Signal Troops, Military Academy of Communications, St. Petersburg, Russia. E-mail: murashko1945@yandex.ru

10 Anatoly P. Sundukov, Associate Professor of the Department of Combat Use of Signal Troops, Military Academy of Communications, St. Petersburg, Russia. E-mail: as25p@yandex.ru

8. Padishin S. A., Sazykin A. M., Savickij A. Ju. Model' planirovanija i postanovki zadach na obespechenie svjazi ob#edinenija, uchityvajushhaja vozmozhnost' ispol'zovanija tehnologii cifrovyh dvojnikov // Izvestija Rossijskoj Akademii Raketnyh i Artillerijskih nauk, № 4 – SPb.: RARAN, 2024.
9. Samohin E. S., Ivanov R. M. Predlozhenija po sokrashheniju vremeni razvertyvanija (svertyvanija) jelementov punkta upravlenija ob#edinenija v uslovijah primenenija protivnikom vysokotochnogo oruzhija // Sbornik statej III Vserossijskoj nauchno-tehnicheskoj konferencii. Tom 3. – Anapa, 2021.
10. Ivanov V. G. Model' tehnicheskoj osnovy sistemy upravlenija special'nogo naznachenija v edinom informacionnom prostranstve na osnove konvergentnoj infrastruktury sistemy svjazi: monografija (monografija). – SPb.: SPbPU, 2018.
11. Ivanov R. M. Logiko-verojatnostnaja model' struktury uzla svjazi special'nogo naznachenija, funkcionirujushhego v uslovijah destabilizirujushhego vozdejstvija protivnika // Voprosy oboronnoj tehniki. Serija 16: № 3, – SPb.: MO RF, 2022.
12. Tevs O. P., Isachenko V. G. Osobennosti i vyvody organizacii i obespechenija svjazi pri provedenii special'noj voennoj operacii // Itogi nauki i tehniki: Nauchno-tehnicheskij sbornik №120. Trudy akademii. – SPb.: VAS, 2022.
13. Tishkov V. V., Ivanov V. G., Luk'janchik V. N. Obosnovanie oblika postroenija perspektivnyh kompleksov i sredstv svjazi na osnove opyta organizacii svjazi pri provedenii special'noj voennoj operacii. Voenno-teoreticheskij zhurnal: Voennaja mysl' № 9. – M.: MO RF, 2023.

ПОВЫШЕНИЕ ЭФФЕКТИВНОСТИ ПРИМЕНЕНИЯ СРЕДСТВ И КОМПЛЕКСОВ СВЯЗИ ПУТЕМ ПРОВЕДЕНИЯ МЕРОПРИЯТИЙ ПО ОБЕСПЕЧЕНИЮ ЖИВУЧЕСТИ

Вольхин С. Д.[1], Пустошкин М. М.[2]

DOI:10.21681/3034-4050-2025-4-52-58

Ключевые слова: *живучесть, эффективность, модель воздействия, разведзащищенность, огневое поражение, система связи, система управления.*

Аннотация

Цель работы: *на основе анализа и обобщения исходных данных, разработать модель огневого воздействия противника, сформулировать основные направления повышения эффективности применения средств и комплексов связи путем обеспечения живучести элементов системы связи в современном вооруженном противоборстве.*

Метод исследования *основан на разработке комплексных аналитических и имитационных моделей, оценивающих процессы неопределенности и многоаспектности ведения боевых действий.*

Результаты исследования *обеспечили внедрение алгоритмов математического моделирования, способных воспроизводить вероятностные события, возникающие при эксплуатации средств связи в современном конфликте. Это, в свою очередь, обеспечивает аналитическую основу для оценки живучести элементов системы связи, прогнозирования критических точек системы, оптимизации ресурсов восстановления.*

Сформулированная система критериев позволяет формализовать процесс выбора стратегий, технических решений и организационных мер для повышения живучести инфраструктуры связи. Данный механизм направлен на выполнение ключевой задачи – гарантировать бесперебойность, оперативность и надежность управления войсками даже в условиях интенсивного противодействия. Реализация подхода обеспечивает адаптацию систем связи к многофакторным рискам современного театра военных действий через приоритезацию защищенных технологий передачи, а распределенное резервирование критических узлов позволят оценить возможный ущерб элементам системы связи который может нанести противник средствами огневого поражения в ходе боевых действий, разработать структуру системы связи в боевых действиях и порядок и сроки ее развертывания и обеспечения функционирования. При этом полученные результаты позволят спланировать направления и мероприятия обеспечения живучести элементов системы связи, сил и средств связи.

Результаты моделирования определят научно обоснованные требования к тактико-техническим характеристикам комплексов и средств связи, которые способны реализовать систему связи с требуемыми характеристиками при выполнении мероприятий по живучести. Результаты будут положены в основу предложений по разработке форм, способов обеспечения живучести элементов системы связи.

Научная новизна: *на основе созданной модели оценки уязвимости элементов систем связи к огневому воздействию предложен инновационный метод анализа эффективности применения средств связи и их структурных компонентов. Обновленный подход акцентирует внимание на поддержании живучести системы связи на протяжении всего цикла операции (боевых действий), что позволяет прогнозировать сценарии боевого применения подразделений связи в условиях динамично меняющейся оперативной обстановки и противодействия противника, позволяя динамическое перераспределение ресурсов сети.*

1 Вольхин Сергей Дмитриевич, адъюнкт Военной академии связи имени Маршала Советского Союза С. М. Будённого, г. Санкт-Петербург, Россия. E-mail: volkhin21@mail.ru

2 Пустошкин Максим Михайлович, адъюнкт Военной академии связи имени Маршала Советского Союза С. М. Будённого, г. Санкт-Петербург, Россия. E-mail: max.pustoshckin@yandex.ru

Введение

Анализ опыта специальной военной операции выявил ключевые тенденции трансформации современного военного противостояния:

1. Изменение пространственной динамики боевых действий:

- переход к мозаичному формату операций с автономными тактическими группами, действующими рассредоточено на изолированных направлениях при отсутствии сплошной линии фронта;
- смещение акцента на урбанизированные территории и зоны критической инфраструктуры, что усложняет логистику и применение классических схем управления.

2. Дефицит инженерной подготовки ТВД:

- ограниченное развертывание фортификационных сооружений, узлов связи и других элементов оперативного обустройства, снижающее устойчивость систем управления.

3. Асимметризация угроз:

- эскалация диверсионно-разведывательной активности с массовым использованием БПЛА различного класса, включая роевые тактики и точечные удары по элементам связи;
- рост технологического паритета за счет интеграции оптико-электронных комплексов, радиотехнической разведки и систем РЭБ нового поколения.

4. Технологический перелом в средствах поражения:

- критическое увеличение доли высокоточных боеприпасов с дистанционным наведением, требующее пересмотра принципов маскировки и живучести объектов системы связи.

Современные боевые действия предъявляют высокие требования к средствам и комплексам связи, а постоянно меняющаяся оперативная обстановка и высокая степень угрозы требуют эффективного и гибкого подхода к их применению.

Специальная военная операция (СВО) кардинально трансформировала принципы ведения современных боевых действий. «Второстепенная» задача – дезорганизации системы управления противника вышла на первые роли в структуре общевойсковых операций:

- созданы специальные подразделения для проведения целевых операций по подавлению систем управления;
- разработаны новые комплексы разведки, поражения и тактические алгоритмы их применения.

Ключевым вызовом стала необходимость противодействия комплексным атакам на систему и войска связи.

Сформирован принцип «асимметричной живучести», основанный на:

1. Многоуровневом резервировании каналов передачи данных (спутниковые, радиорелейные, мобильные сети).
2. Автоматизированном перераспределении потоков информации при повреждении критических узлов.
3. Внедрении квантово-защищенных протоколов для блокировки киберфизического воздействия.

Практика СВО подтвердила, что даже в условиях превосходства противника в разведывательно-ударных системах (высокоточное оружие, БПЛА, средства РЭБ) живучесть связи достигается за счет:

- динамической топологии сетей, исключающей статичные уязвимые точки;
- использования AI-алгоритмов для прогнозирования и парирования атак в реальном времени;
- интеграции гражданских инфраструктурных решений (например «mesh»-сетей) для обеспечения избыточности.

Эти меры не только минимизируют потери техники и личного состава, но и создают оперативный дисбаланс в пользу сторон, способных гибко адаптировать технологии к меняющемуся театру военных действий [2].

Постановка задачи

Выполнение мероприятий по обеспечению живучести позволяет сократить потери сил и средств связи и как следствие повысить эффективность функционирования системы связи.

Практика СВО показала, что в условиях активного воздействия противника эффективность и высокой динамики боевых действий, эффективность системы связи актуально рассматривать по живучести средств связи в течение всей операции воинского

формирования. При этом в условиях современного вооруженного конфликта достигаются необходимые устойчивость, непрерывность и оперативность управления войсками в условиях деструктивного воздействия противника [2, 6]. Немаловажным фактором в данном контексте являются сокращение материально-финансовых затрат на восполнение потерь и времени на восстановление системы связи.

В ходе операции объекты развернутой системы связи будут подвержены постоянному воздействию средств разведки и поражения. При этом огневое поражение можно разделить на две группы:

- к первой группе относятся удары обычного и ВТО, которые воздействуют на систему связи или отдельные ее элементы точечно и непродолжительное время. Они характеризуются вероятностным законом распределения по времени с параметрами работы сети связи по живучести. В сети связи при этом происходит весь набор событий – функционирование, поражение, выход из строя, восстановление, функционирование;
- к другой группе можно отнести виды воздействий, которые не могут устойчиво повторяться при функционировании сети связи в каждом этапе операции и приводящие, как правило, к большому количеству безвозвратных потерь сил и средств связи на большой площади и приводящие к длительному их восстановлению. Это характерно при массированных ракетно-авиационных ударах.

Показатели живучести сети связи должны быть сочетаться с требованиями по устойчивости, непрерывности, оперативности, мобильности и качества управления.

Для решения этих задач требуется научно-методический аппарат, позволяющий осуществлять моделирование огневого воздействия противника на протяжении всего периода боевых действий.

Решение задачи

При разработке модели огневого поражения объектов системы связи положен метод, сочетающий построение комплексных моделей, которые учитывают факторы неопределенности и многоаспектность процессов и методик расчета и оценки численных значений необходимых показателей. Этот подход основан на функциональной, системной и структурной сложности предмета исследования.

Вероятность поражения элементов системы связи зависит от многочисленных факторов и в целом является случайной величиной. При этом вероятность поражения ($P_{пор}$) по l-му элементу определяется выражением:

$$P_{пор_i} = 1 - \prod_{j=1}^{J} [1 - K_{jl}^{ну} \cdot P_{jl}(V) \cdot P_{jl}(D)]$$

где $K_{jl}^{ну}$ – коэффициент возможности нанесения удара j-го типа по l-му элементу; $P_{jl}(V)$ – вероятность того, что противником своевременно нанес удар по разведанному объекту; $P_{jl}(D)$ – вероятность доставки j-го средства по l-му элементу.

Коэффициент ($K_{jl}^{ну}$) определяет возможность j-го средства поразить l-й элемент системы связи и определяются по формуле:

$$K_{jl}^{ну} = \begin{cases} 1, \text{ если } Д_j min \le Д_l \le Д_j max, \\ 0, \text{ если } Д_l < Д_j min \text{ или } Д_j max < Д_l. \end{cases}$$

где $Д_l$ – расстояние до объекта; $Д_j min$, $Д_j max$ – тактико-технические характеристики средств поражения по минимальной и максимальной дальности поражения.

Вероятность своевременного нанесения противником удара по объекту зависит от времени подготовки вооружения к применению и от времени нахождения «вскрытого» элемента системы связи районе и определяется по формуле:

$$P_{jl}(V) = \left[\frac{\vartheta \cdot m_{t_ф}}{1 + \vartheta \cdot m_{t_ф}} \right]^k,$$

где $k = \left] \frac{m_t^2}{D_T} \right[$, $\vartheta = \frac{k}{m_t}$ – параметры γ (*гамма*)-распределения времени на подготовку удара; m_t – математическое ожидание времени, необходимого для огневого воздействия; D_T – дисперсия времени, которое необходимого для удара; $m_{t_ф}$ – математическое ожидание времени функционирования элемента системы связи в районе.

Время для подготовки к нанесению удара, включает время на обнаружение объекта, обработку информации, принятие решения на воздействие, подготовку вооружения. Математическое ожидание времени m_t, для подготовки и нанесение удара, определяется как:

$$m_t = m_{t_р} + m_{t_у} + m_{t_{ну}},$$

где $m_{t_р}$ – математическое ожидание времени на разведку объекта системы связи; $m_{t_у}$ – математическое ожидание времени для принятия решения на воздействие;

$m_{t_{пу}}$ – математическое ожидание времени на подготовку вооружения и сам удар.

Противодействие поражению ВТО и БПЛА средствами противовоздушной обороны (ПВО), характеризуется вероятностью поражения средствами ПВО ($P_i^{ПВО}$). Опыт СВО показывает, что на современном этапе развития вооружения ПВО, $P_i^{ПВО} \leq 0{,}4–0{,}5$, что будет соответствовать уничтожению от 40 % до 50 % носителей.

Исходя из вышеизложенного, модель огневого воздействия противника на элементы системы связи можно представить в виде структурно-логической схемы [3,10] (рис. 1).

По опыту СВО можно выделить ряд эффективных мероприятий и способов повышения живучести элементов системы связи.

Так применение средств беспроводного широкополосного доступа позволяет организовывать высокоскоростные линии привязки, не имеющие ярко выраженных демаскирующих признаков.

Необходимо отдельно остановиться на одном из перспективных направлений активно применяющимся в ходе СВО – использование малозаметных антенно-мачтовых устройств, которые сложно обнаружить средствами видовой разведки и их маскировка под окружающую местность, в том числе с учетом времени года. Особенно это касается антенно-мачтовых устройств.

В СВО ключевым способом повышения живучести элементов системы связи стало формирование «серого фона» – системы мер, направленных на маскировку элементов связи среди множества аналогичных объектов. Это затрудняет противнику идентификацию критически важных целей, увеличивая

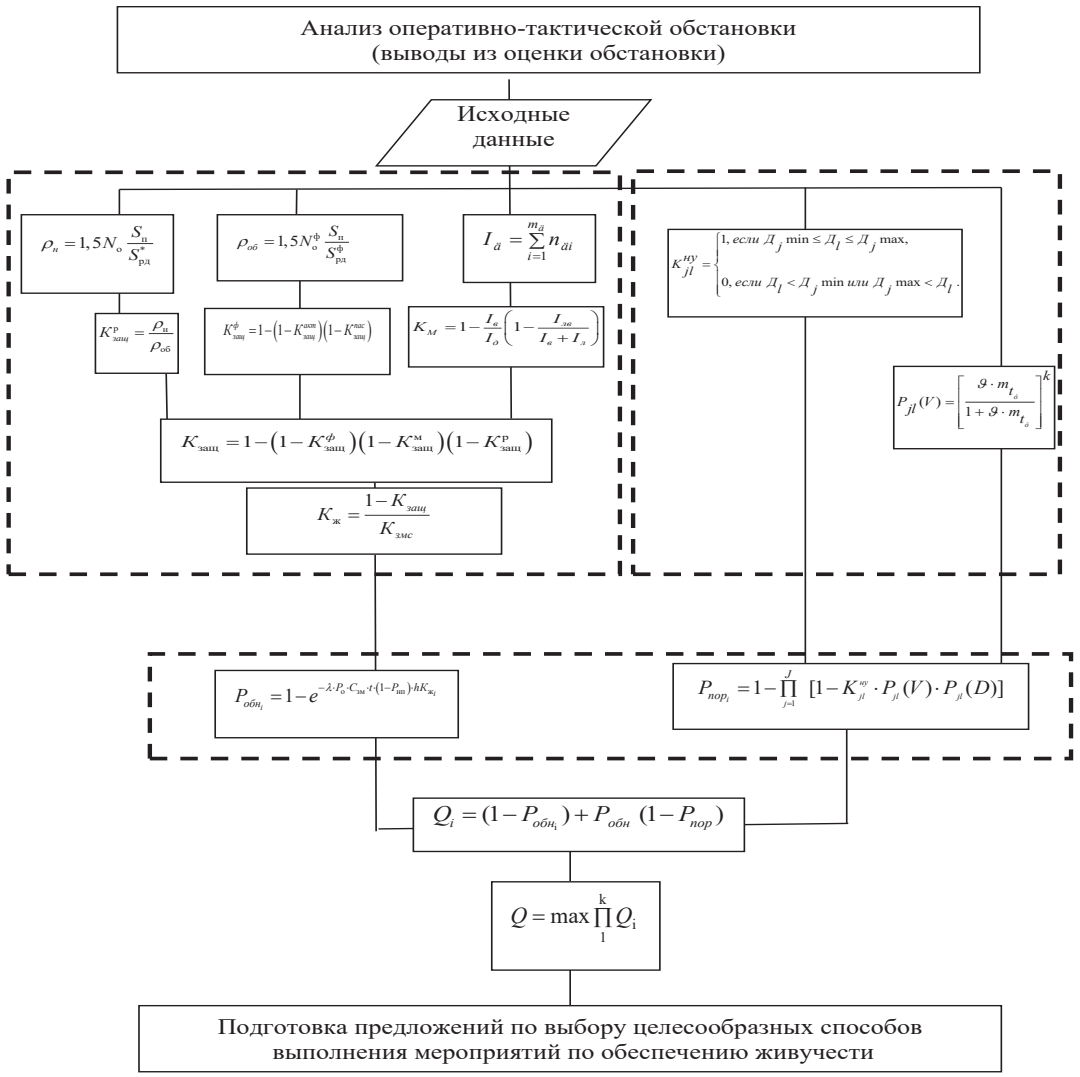

Рис. 1. Модель огневого воздействия на элементы системы связи

среднее время их обнаружения разведкой. Концепция «серого фона» реализуется через четыре взаимосвязанных направления:

1. Использование во всех звеньях управления средств связи с одинаковыми тактико-техническими характеристиками.
2. Применение средств связи, стоящих на снабжении в вооруженных силах, средств связи «двойного» назначения, использование ресурса сетей сотовой связи, сетей Интернет.
3. Маскировка аппаратных связи под «гражданский» автотранспорт, создание командно-штабных машин и комплексных аппаратных связи на базе линейных боевых машин.
4. Применение антенн, не имеющих ярко выраженных «демаскирующих» признаков.

Результаты внедрения «серого фона»:

- ❖ увеличение времени вскрытия элементов системы связи (среднее время идентификации цели разведкой противника возрастает на 40–60 %, что критически снижает эффективность высокоточных ударов);
- ❖ повышение живучести и снижение потерь (на 25–30 % уменьшается вероятность поражения узлов связи в первых 3 часа после их развертывания, система сохраняет управляемость даже при потере 30–40 % элементов).

«Серый фон» не только усложняет работу разведки противника, но и формирует асимметричное преимущество, где живучесть достигается не технологическим превосходством, а тактической изобретательностью.

Заключение

Разработанная модель огневого воздействия противника позволяет спрогнозировать и оценить потенциальный ущерб, который будет нанесен системе в ходе операции (боя).

В качестве результатов использования модели появляется возможность:

- ❖ выявить потенциальный ущерб воздействия противника и определить наиболее опасные средства огневого поражения;
- ❖ разработать структуру системы связи в операции, обеспечивающую лучшую эффективность по показателю живучести;
- ❖ правильно использовать боевые возможности подразделений и системы связи;
- ❖ определить необходимость применения тех, или иных способов активной или пассивной защиты элементов системы связи.

Эти факторы формируют «гибридную» среду ведения боевых действий, где успех определяется способностью систем связи:

- ❖ обеспечивать управление в условиях фрагментированного оперативного пространства;
- ❖ противостоять многоуровневым помеховым и огневым воздействиям;
- ❖ сохранять функциональность при дефиците времени на восстановление критических узлов.

Адаптация к данным вызовам требует внедрения нейросетевых алгоритмов прогнозирования угроз, модульной архитектуры комплексов связи и интеллектуальных систем динамической реконфигурации сетей.

Статья публикуется по рекомендации доктора военных наук, доцента Иванова Василия Геннадьевича. Москва, Россия. E-mail: wasj2006@yandex.ru

Литература

1. Воробьев И. Г., Романов В. М. Развитие форм и способов построения системы связи тактического звена управления // Военная Мысль. 2022. № 6. С. 61–70.
2. Тевс О. П., Пустошкин М. М.. Моделирование тактики подразделений связи в условиях современного вооруженного противоборства // Телекоммуникации и связь. № 3. 2024. С.5–12.
3. Корепанов В. О., Шумов В. В. Моделирование военных, боевых и специальных действий // Военная мысль № 1, 2023. С. 28.
4. Иванов В. Г. Основы построения и оценки эффективности функционирования системы связи специального назначения в международном вооруженном конфликте на основе многосферной и конвергентной структуры ее элементов: Монография. – СПб.: ПОЛИТЕХ, 2023. – 298 с.
5. Иванов В. Г. Модель технической основы системы управления специального назначения в едином информационном пространстве на основе конвергентной инфраструктуры системы связи: Монография. – СПб.: СПбПУ, 2018. – 214 с.

6. Вольхин С. Д Анализ воздействия системы разведки и РЭБ, средств огневого поражения на систему связи современном вооруженном конфликте // Сборник статей по материалам XIII Международной научно-технической конференции. Воронеж: ВУНЦ ВВС России, 2024, с. 13–17.
7. Пустошкин М. М., Степынин Д. В., Филимоненков М. Х., Васильева Т. Г., Ульянов В. В. Направления развития вооруженной борьбы, влияющие на тактику войск связи // Стратегическая стабильность. № 4(109). 2024. С. 37–40.
8. Вольхин С. Д. Обеспечение живучести системы связи и ее элементов в современных условиях ведения вооруженной борьбы // Сборник трудов Военно-научной конференции – Спб: ВАС. 2024. С. 21–25.
9. Пустошкин М. М., Анализ тактики применения соединений (воинских частей, подразделений) связи в условиях современного вооруженного противоборства // Сборник научных трудов III международной научно-практической конференции: Карбышевское чтение «Наше дело правое – победа будет за нами». Тюмень: ТВВИКУ. Т. 6, 2024. С. 62–67.
10. Пустошкин М. М., Ульянов В. В., Шамсутдинова Е. Ю. Основные направления совершенствования тактики соединений, частей и подразделений связи в условиях современного вооруженного противоборства // Сборник научных трудов научной конференции «Повышение обороноспособности государства 2024» – Военный учебный центр СПбПУ. – СПб.: 2024. С. 13–17.

IMPROVING THE EFFICIENCY OF THE USE OF COMMUNICATION FACILITIES AND COMPLEXES BY CARRYING OUT MEASURES TO ENSURE SURVIVABILITY

Volkhin S. D.[1], Pustoshkin M. M.[2]

Keywords: *survivability, effectiveness, impact model, reconnaissance protection, fire damage, communication system, control system.*

Abstract

The purpose of the work: *on the basis of the analysis and generalization of the initial data, to develop a model of the enemy's fire impact, to formulate the main directions for improving the effectiveness of the use of communication means and complexes by ensuring the survivability of the elements of the communication system in modern armed confrontation.*

The research method *is based on the development of complex analytical and simulation models that assess the processes of uncertainty and multifaceted nature of warfare.*

The results of the study *provided the introduction of mathematical modeling algorithms capable of reproducing probabilistic events that arise during the operation of communication facilities in a modern conflict. This, in turn, provides an analytical basis for assessing the survivability of communication system elements, predicting critical points of the system, and optimizing recovery resources.*

The formulated system of criteria makes it possible to formalize the process of selecting strategies, technical solutions and organizational measures to increase the survivability of the communication infrastructure. This mechanism is aimed at fulfilling the key task – to guarantee the continuity, efficiency and reliability of command and control of troops even in conditions of intense counteraction protected transmission technologies, and distributed redundancy of critical nodes will make it possible to assess the possible damage to the elements of the communication system that can be caused by the enemy by means of fire damage in the course of hostilities, to develop the structure of the communication system in combat operations and the procedure and timing of its deployment and operation. At the same time, the results obtained will make it possible to plan the directions and measures to ensure the survivability of the communication system elements, forces and means of communication.

The simulation results will determine scientifically based requirements for the tactical and technical characteristics of complexes and communication facilities that are capable of implementing a communication system with the required characteristics when performing survivability measures. The results will form

1 Sergey D. Volkhin, Adjunct of the Military Academy of Communications, St. Petersburg, Russia. E-mail: volkhin21@mail.ru
2 Maxim M. Pustoshkin, Adjunct of the Military Academy of Communications, St. Petersburg, Russia. E mail: max.pustoshckin@yandex.ru

the basis of proposals for the development of forms, methods to ensure the survivability of communication system elements.

Scientific novelty: on the basis of the created model for assessing the vulnerability of communication system elements to fire impact, an innovative method for analyzing the effectiveness of the use of communication equipment and their structural components is proposed. The updated approach focuses on maintaining the survivability of the communication system throughout the entire cycle of operation (combat operations), which makes it possible to predict scenarios for the combat use of communication units in the context of dynamically changing operational situation and counteraction of the enemy, allowing dynamic redistribution of network resources.

References

1. Vorob'ev I. G., Romanov V. M. Razvitie form i sposobov postroenija sistemy svjazi takticheskogo zvena upravlenija // Voennaja Mysl'. 2022. № 6. S. 61–70.
2. Tevs O. P., Pustoshkin M. M.. Modelirovanie taktiki podrazdelenij svjazi v uslovijah sovremennogo vooruzhennogo protivoborstva// Nauchnyj recenziruemyj zhurnal: Telekommunikacii i svjaz'. № 3. – M.: MO RF, 2024. S. 5–12.
3. Korepanov V. O., Shumov V. V. Modelirovanie voennyh, boevyh i special'nyh dejstvij// Voenno-teoreticheskij zhurnal: Voennaja mysl' № 1. – M.: MO RF, 2023. S. 28.
4. Ivanov V. G. Fundamentals of construction and evaluation of the efficiency of functioning of a special-purpose communication system in an international armed conflict based on the multi-sphere and convergent structure of its elements: Monograph. - St. Petersburg: POLYTECH, 2023. – 298 p.
5. Ivanov V. G. Model' tehnicheskoj osnovy sistemy upravlenija special'nogo naznachenija v edinom informacionnom prostranstve na osnove konvergentnoj infrastruktury sistemy svjazi: Monografija. SPb.: SPbPU, 2018. 214 s.
6. Vol'hin S. D Analiz vozdejstvija sistemy razvedki i RJeB, sredstv ognevogo porazhenija na sistemu svjazi sovremennom vooruzhennom konflikte // Sbornik statej po materialam XIII Mezhdunarodnoj nauchno-tehnicheskoj konferencii – Voronezh: VUNC VVS Rossii, 2024, str. 13–17.
7. Pustoshkin M. M., Stepynin D. V., Filimonenkov M. H., Vasil'eva T. G., Ul'janov V. V. Napravlenija razvitija vooruzhennoj bor'by, vlijajushhie na taktiku vojsk svjazi // Nauchno-prakticheskij mezhdisciplinarnyj zhurnal: «Strategicheskaja stabil'nost'» № 4(109). – 2024, S. 37–40.
8. Vol'hin S. D. Obespechenie zhivuchesti sistemy svjazi i ee jelementov v sovremennyh uslovijah vedenija vooruzhennoj bor'by // Sbornik trudov Voenno-nauchnoj konferencii – Spb: VAS, 2024, S. 21–25.
9. Pustoshkin M. M., Analiz taktiki primenenija soedinenij (voinskih chastej, podrazdelenij) svjazi v uslovijah sovremennogo vooruzhennogo protivoborstva // Sbornik nauchnyh trudov III mezhdunarodnoj nauchno-prakticheskoj konferencii: Karbyshevskoe chtenie «Nashe delo pravoe – pobeda budet za nami». Tjumen': TVVIKU. T. 6, 2024. S. 62–67.
10. Pustoshkin M. M., Ul'janov V. V., Shamsutdinova E. Ju. Osnovnye napravlenija sovershenstvovanija taktiki soedinenij, chastej i podrazdelenij svjazi v uslovijah sovremennogo vooruzhennogo protivoborstva // Sbornik nauchnyh trudov nauchnoj konferencii «Povyshenie oboronosposobnosti gosudarstva 2024» – Voennyj uchebnyj centr SPbPU. – SPb.: 2024. S. 13–17.

.

МЕТОДИКА АНАЛИЗА УСТОЙЧИВОСТИ ФУНКЦИОНИРОВАНИЯ СЕТИ РАДИОСВЯЗИ В УСЛОВИЯХ ВОЗДЕЙСТВИЯ ДЕСТАБИЛИЗИРУЮЩИХ ФАКТОРОВ

Киселев В. Н.[1], Козориз Д. А.[2], Триполин А. М.[3], Селезенев Н. В.[4]

DOI:10.21681/3034-4050-2025-4-59-67

Ключевые слова: *помехозащищенность, радиоэлектронная борьба, сеть связи, система радиосвязи, разведзащищенность, вероятность связности, информационное направление, отношение сигнал/шум.*

Аннотация

Цель статьи *в обобщении и доработке отдельных этапов оценки показателей структурной устойчивости системы радиосвязи, функционирующей в условиях воздействия дестабилизирующих факторов.*

Результат: *в статье обосновывается применение показателя устойчивости для оценки качества сетей радиосвязи, выполняющих свои функции в условиях воздействия дестабилизирующих факторов и для анализа влияния частотно-энергетических характеристик радиолиний, образующих сеть радиосвязи, на ее устойчивость.*

В качестве показателя устойчивости рассмотрена связность сети радиосвязи. Разработанная методика базируется на частных методиках анализа показателей помехозащищенности, разведзащищенности, коэффициентов устойчивости информационных цепей и направлений.

Рассмотрен пример использования разработанной методики в задачах оценки вероятности связности и обоснования высоты подъема антенн в сети радиосвязи, построенной на радиосредствах шестого поколения.

Практическая полезность: *результаты статьи могут и должны быть учтены при проектировании новых образцов техники связи.*

Введение

Система военной связи (СВС) представляет собой достаточно сложное объединение сил и средств связи, создаваемое с целью реализации функций управления войсками в различных условиях обстановки. На аппаратном уровне СВС представляет собой гетерогенную сеть связи, интегрирующую сети, отличающиеся по физической среде передачи, технологии разделения доступа к среде передачи, способам организации мультисервисного обмена информацией и др. Особое место в СВС занимают сети радиосвязи (СРС). Задачи анализа качества функционирования СРС не потеряли актуальности и в настоящее время, что обусловлено, в частности, постановкой на снабжение войск радиосредств шестого поколения и получением определенного опыта боевого применения этих средств в рамках проведения СВО.

Оценка качества функционирования СРС осуществляется по степени соответствия значений частных показателей качества системы нормативным требованиям. Современными нормативными документами предусмотрены следующие характеристики качества функционирования системы радиосвязи: боевая готовность, устойчивость, мобильность, пропускная способность, разведзащищенность, доступность, управляемость.

Оценка качества функционирования СРС по совокупности более чем двух показателей всегда является нетривиальной задачей. Поэтому перед исследователем стоит выбор между двумя путями решения задачи: попытаться свернуть частные показатели

1 Киселев Владимир Николаевич, кандидат технических наук, профессор, ведущий разработчик «АО НПО «Ангстрем», г. Москва, Зеленоград, Россия. E-mail: vkicelev@yandex.ru

2 Козориз Денис Александрович, кандидат технических наук, начальник научно-технического центра «АО НПО «Ангстрем», г. Москва, Зеленоград, Россия. E-mail: kozorizda@npo-angstrem.ru

3 Триполин Александр Михайлович, кандидат технических наук, ведущий специалист «АО НПО «Ангстрем», г. Москва, Зеленоград, Россия. E-mail: tripolin@yandex.ru

4 Селезенев Николай Витальевич, кандидат технических наук, главный научный сотрудник ФГБУ «16 ЦНИИИ» Минобороны России. E-mail: nik-selezenev@yandex.ru

5 ГОСТ 5311–2008. Устойчивость функционирования сети связи общего пользования.

качества функционирования системы радиосвязи в единый обобщенный показатель или, с учетом условий решаемой задачи, выбрать один или два основных показателя, а другие задать в виде ограничений на основе опыта и нормативных документов.

В задачах анализа эффективности функционирования СРС в условиях воздействия дестабилизирующих факторов наиболее часто в качестве основного показателя рассматривается устойчивость системы связи. Согласно ГОСТ 5311-2008[5], устойчивость характеризует способность сети электросвязи выполнять свои функции при выходе из строя части элементов сети в результате воздействия дестабилизирующих факторов. Источником дестабилизирующего фактора является физический или технологический процесс внутреннего или внешнего по отношению к сети электросвязи характера, приводящий к выходу из строя элементов сети. Актуальность вопросов анализа устойчивости определяется высокими требованиями к СРС в установленные сроки и в различных условиях обстановки обеспечить управления войсками и оружием.

Свойство устойчивости системы радиосвязи является интегральным, объединяя такие показатели как [1]:

живучесть – способность системы военной связи обеспечивать управление войсками в условиях воздействия оружия;

- помехоустойчивость – способность системы военной связи обеспечивать управление войсками (силами) и оружием в условиях помех различных видов;
- помехозащищенность – способность системы военной связи обеспечивать управление войсками (силами) и оружием в условиях воздействия преднамеренных помех противника;
- надежность – способность системы военной связи обеспечивать связь, сохраняя во времени значение эксплуатационных показателей в период применения, технического обслуживания, восстановления и ремонта.

С другой стороны, приведенная трактовка термина устойчивость не учитывает в прямой постановке такие свойства системы радиосвязи как пропускная способность, разведзащищенность, доступность, а также частотно-энергетические характеристики радиолиний, образующих систему радиосвязи: энергетический бюджет или энергетический запас радиолинии, затухание радиосигналов в радиолинии, диапазон и полосу рабочих частот, протяженность интервалов ретрансляции и другие. Это в известной степени ограничивает аппарат анализа влияния на устойчивость системы технических решений, принятых при разработке радиосредств или, наоборот, влияние требуемой устойчивости СРС на выбор технических решений. Необходимо отметить, что в работах, посвященных анализу систем связи, функционирующих в условиях воздействия дестабилизирующих факторов, некоторые авторы используют понятия структурной, функциональной или информационной устойчивости [2, 3].

В связи с определенной подвижностью границ понятия устойчивости СРС [2], различными исследователями рассматриваются собственные подходы к анализу устойчивости системы радиосвязи, которые проявляются в разработке методик, использующих оригинальные методы оценки частных показателей или оригинальное сочетание известных методов.

Цель настоящей статьи – обобщение и доработка отдельных этапов оценки показателей структурной устойчивости системы радиосвязи, функционирующей в условиях воздействия дестабилизирующих факторов, для анализа влияния частотно-энергетических характеристик радиолиний, образующих систему радиосвязи, на устойчивость СРС.

Устойчивость информационного направления

Информационный обмен в сети радиосвязи осуществляется посредством информационного направления, образованного между узлами сети в виде совокупности одного и более путей (маршрутов или информационных цепей) [1]. Следовательно, устойчивость СРС характеризуется коэффициентом устойчивости информационного направления, который определяется готовностью технических средств связи и образованных ими линий связи к передаче сообщений на направлении связи в произвольный момент времени с использованием всех возможных маршрутов доставки сообщения. Расчет устойчивости информационного направления связи следует проводить на основе графа сети связи, где вершинами являются сетевые узлы, а ребрами – линии связи их соединяющие.

Показателем устойчивости системы связи является значение вероятности связности информационного направления[6], которая характеризует вероятность того, что на заданном направлении существует хотя бы один путь (информационная цепь) из M возможных, обеспечивающий передачу информации с требуемым качеством [1]

$$K_{у\,ИН} = P(L \geq 1/M) = \\ = \sum_{l=L}^{M} C_M^l \prod_{m=1}^{l} (K_{уИЦm}) \prod_{m=1}^{M-l} (1 - K_{уИЦm}), \quad (1)$$

где: L – число работоспособных информационных цепей в заданном направлении; $K_{уИЦm}$ – коэффициент, характеризующий устойчивость m-й информационной цепи; M – число информационных цепей для передачи информации в заданном направлении, предоставляемых протоколом маршрутизации; C_M^l – число сочетаний из M по L.

Коэффициент устойчивости учитывает влияние на узлы и линии связи дестабилизирующих факторов, основным из которых будет воздействие противника (РЭБ, физическое разрушение). Минимальная вероятность связности информационного направления сохраняется при L = 1 и равна

$$K_{у\,ИН} = P(L = 1/M) = 1 - \prod_{m=1}^{M} (1 - K_{уИЦm}). \quad (2)$$

Число возможных информационных цепей M в информационном направлении определяется топологическими особенностями сетей системы радиосвязи. Каждая информационная цепь может быть однозвенной (непосредственная связь узлов) или многозвенной (связь с ретрансляцией). Коэффициент устойчивости последовательной многозвенной информационной цепи определяется произведением парциальных коэффициентов устойчивости в виде

$$K_{уИЦm} = \prod_{n=1}^{N} (K_{уИЦm}), \quad (3)$$

где N – число интервалов ретрансляции в информационной цепи.

При рассмотрении информационных направлений в пределах фрагментов сети радиосвязи, ограниченных незначительными размерами, например, радиосеть тактического звена управления (ТЗУ), можно допустить равенство парциальных коэффициентов устойчивости так, что $K_{уИЦn} = K_{уИЦ1}$. Тогда, с учетом топологии сети радиосвязи, можно определить функциональную зависимость вероятности связности (коэффициента устойчивости информационного направления) от коэффициента устойчивости однозвенной информационной цепи

$$K_{у\,ИН} = \Phi[M;N;K_{уИЦm}(K_{уИЦ1})]. \quad (4)$$

В боевых порядках ТЗУ посредством сети радиосвязи организуются информационные направления «батальон – рота – взвод». В качестве архитектурных решений построения сети радиосвязи могут быть использованы сети прямых связей (СПС) с непосредственной связью и последовательно-параллельной ретрансляцией, а также распределенные сети радиосвязи (СР). Вероятность связности в СПС определяется посредством формул (1) ÷ (3) перебором параметров (L, M, N). Например, для радиолиний с двойным резервированием, когда L = 1, M = 2 и N = 1, коэффициент устойчивости информационного направления будет равен

$$K_{у\,ИН} = 1 - \prod_{m=1}^{2} (1 - K_{уИЦm}) = 1 - (1 - K_{уИЦ1})^2. \quad (5)$$

При организации информационных направлений в рамках распределенной сети радиосвязи с автоматической маршрутизацией и самовосстановлением высокая связность на сетевом уровне обеспечивается применением информационных цепей как с непосредственной связью, так и с ретрансляцией. Максимальное число возможных ретрансляций ограничивается протоколами СР с учетом обеспечения требуемого качества обслуживания. В этом случае вероятность того, что на заданном направлении существует хотя бы один путь (информационная цепь) можно оценить выражением

$$K_{у\,ИН} = 1 - \prod_{n=1}^{N_{max}} (1 - K_{уИЦ1}^n)^{C_{S-2}^{n-1}}, \quad (6)$$

где: N_{max} – максимальное число возможных интервалов ретрансляции в информационной цепи; S – число узлов в распределенной сети радиосвязи; C_{S-2}^{n-1} – число информационных цепей с n интервалами ретрансляции в направлении связи.

В задачах анализа устойчивости сетей радиосвязи, когда неприменимо допущение о равнозначности информационных направлений, в ряде работ [1,2] в качестве показателя

6 ГОСТ 5311 – 2008. Устойчивость функционирования сети связи общего пользования

устойчивости предлагается использовать средневзвешенную устойчивость, полученную сверткой устойчивостей информационных направлений с учетом их нормированных значимостей (весовых коэффициентов) в виде

$$K_y = \sum_{r=L}^{R} \alpha_r K_{y\,\text{ИН}r};\ \sum_{r=L}^{R} \alpha_r = 1, \qquad (7)$$

где: α_r – коэффициент значимости r-го направления связи, определяемый на основе экспертных оценок или анализа свойств графа сети и распределения циркулирующего в сети трафика; R – число организуемых на сети направлений связи.

Таким образом, устойчивость функционирования сети радиосвязи оценивается связностью сети и определяется ее топологией (наличием резервных информационных цепей) и устойчивостью однозвенных информационных цепей, образующих информационные направления.

Устойчивость однозвенной информационной цепи

В рамках поставленной ранее цели, устойчивость однозвенной информационной цепи определим при условии, что на интервале времени информационного обмена узлы сети исправны и готовы к использованию. Деструктивным фактором является воздействие помех в процессе РЭБ. Тогда устойчивость функционирования однозвенной радиолинии определяется выражением вида [2, 5, 6]

$$K_{y\text{ИЦ1}} = 1 - (1 - K_{\text{э.ПЗ}})(1 - K_{\text{в.ПЗ}})(1 - K_{\text{РЗ}})\, P_{\text{ПП}}, \qquad (8)$$

где: $K_{\text{РЗ}}$ – комплексный показатель разведзащищенности радиолинии; $P_{\text{ПП}}$ – вероятность постановки помех; $K_{\text{в.ПЗ}}$ – коэффициент временной помехозащищенности; $K_{\text{э.ПЗ}}$ – коэффициент энергетической помехозащищенности.

В качестве оценки комплексного показателям разведзащищенности может быть принята вероятность вскрытия радиолинии противником ($P_{\text{вскр}}$) [2, 5, 6] так, что

$$K_{\text{РЗ}} = (1 - P_{\text{вскр}}). \qquad (9)$$

Величина вероятности вскрытия радиолинии в задачах анализа качества функционирования СРС задается в виде требований. При необходимости оптимизации СРС с учетом параметров средств РЭБ вероятность вскрытия радиолинии определяется на основе принятых методик анализа вероятностно-временных характеристик случайных процессов, составляющих цикл разведки: обнаружение РЭС; определение местоположения РЭС; перехват сообщений за определенное время.

Коэффициент временной помехозащищенности соответствует вероятности сохранения работоспособности радиолинии в динамике ведения радиосвязи в условиях РЭП и выражается в форме отношения среднего времени реакции системы РЭП $\overline{\tau_{\text{РЭП}}}$ и среднего времени ухода от помехи системой радиосвязи $\overline{t_{\text{пер}}}$ [2]

$$K_{\text{в.ПЗ}} = \frac{\overline{\tau_{\text{РЭП}}}}{\overline{t_{\text{пер}}} + \overline{\tau_{\text{РЭП}}}}. \qquad (10)$$

Энергетическая помехозащищенность количественно оценивается отношением максимально допустимой мощности преднамеренной помехи к мощности сигнала на входе приемника, при котором обеспечивается требуемое качество приема сообщений, т.е. не превышается допустимое значение средней вероятностью ошибки на бит [2, 5]. Коэффициент энергетической помехозащищенности определим как вероятность не превышения текущим значением отношения мощностей помеха/сигнал на входе приемника радиолинии допустимой величины при условии, что средняя вероятность ошибки приема элемента сигнала не превышает допустимое значение, т.е.

$$K_{\text{э.ПЗ}} = P\left\{\left(\frac{P_{\text{п}}}{P_c}\right)_{\text{вх.}} \le \left(\frac{P_{\text{п}}}{P_c}\right)_{\text{вх.доп}};\ p_{\text{ош}} \le p_{\text{ош.доп}}\right\}, \qquad (11)$$

где $P_{\text{п}}$ – мощность помехи на входе приемника радиолинии; P_c – мощность полезного сигнала на входе приемника радиолинии; $p_{\text{ош}}$ – средняя вероятность ошибки приема элемента (бита) сигнала; $p_{\text{ош.доп}}$ – допустимая средняя вероятность ошибки приема элемента сигнала.

Средняя вероятность битовой ошибки в формуле (11) зависит от энергетического отношения сигнал/шум (h^2). Для видов модуляции, применяемых в радиосредствах шестого поколения, функциональные зависимости $p_{\text{ош}}(h^2)$ в случае аддитивного белого гауссовского шума приведены в таблице 1 [8], где:

$$h^2 = \frac{E_{\text{б}}}{N_{\text{ш}}} = \frac{P_c}{W_c N_{\text{ш}}}; \qquad (12)$$

где $E_{\text{б}}$ – энергия бита; W_c – ширина спектра радиосигнала; $N_{\text{ш}}$ – спектральная плотность мощности шума приемного тракта; $erfc(\cdot)$ – дополнительная функция ошибок.

Таблица 1.

Средняя вероятность ошибки приема элемента сигнала

№ п/п	Вид модуляции	Средняя вероятность ошибки
1	BPSK	$p_{ош} = 0{,}5 \cdot erfc(\sqrt{h^2})$
2	BFSK	$p_{ош} = 0{,}5 \cdot erfc(\sqrt{h^2/2})$
3	QPSK, QAM 4	$p_{ош} = 0{,}5 \cdot erfc(\sqrt{h^2})$
4	QAM 16	$p_{ош} = 0{,}375 \cdot erfc(\sqrt{0{,}4 \cdot h^2})$
5	QAM 64	$p_{ош} = (\frac{7}{24}) \cdot erfc(\sqrt{h^2/7})$

Существенное влияние на коэффициент энергетической помехозащищенности оказывает характер распространения сигналов в радиолиниях СРС. В частности, радиоканалы наземных УКВ радиолиний характеризуются наличием медленных замираний, что приводит к мультипликативным искажениям огибающей передаваемого радиосигнала. Распространенным видом замираний являются рэлеевские, для которых случайный множитель r, характеризующий глубину замираний огибающей радиосигнала подчинен закону распределения Релея. Тогда отношение сигнал/шум h_r^2, с учетом (12), имеет распределение xu-квадрат с двумя степенями свободы [6, 7]

$$h_r^2 = r^2\, h^2 = r^2 \frac{E_б}{N_ш};\ w(h_r^2) = \frac{1}{2 \cdot (h^2)} e^{-\frac{h_r^2}{2 \cdot (h^2)}}. \qquad (13)$$

В условиях замираний радиолиния будет работоспособна, если отношение сигнал/шум превысит некоторое минимально допустимое значение $h_r^2 \geq h_{доп}^2$, при котором обеспечивается выполнение условия $p_{ош} \leq p_{ош.доп}$ в выражении (11). Допустимое энергетическое отношение сигнал/шум определяется как значение обратной функции средней вероятности ошибки бита (таблица 1) при максимально допустимой вероятности ошибки, т.е.

$$h_{доп}^2 = p_{ош}^{-1}\,(p_{ош.доп}). \qquad (14)$$

Таким образом, коэффициент энергетической помехозащищенности радиолинии без преднамеренных помех с учетом формул (11)–(14) равен

$$K_{э.ПЗ} = P\{h_r^2 \geq h_{доп}^2\} = \int_{h_{доп}^2}^{\infty} w(h_r^2)\, dh_r^2 =$$

$$= exp\left[- \frac{p_{ош}^{-1}\,(p_{ош.доп})}{2 \cdot \frac{E_б}{N_ш}} \right]. \qquad (15)$$

В случае применения заградительной помехи в пределах диапазона работы радиолинии (в том числе радиолинии с ППРЧ) или сканирующей по частоте помехи в части диапазона спектральная плотность мощности помех определяется выражением [9]

$$N_{шп}\,(\gamma) = \frac{P_п\, \gamma}{\Delta F_{пом}} + N_ш, \qquad (16)$$

где: $\gamma = \frac{\Delta F_{пом}}{\Delta F_{ППРЧ}}$ – вероятность частотно-временного совпадения помехи и сигнала; $\Delta F_{пом}$ – ширина полосы частот помехи; $\Delta F_{ППРЧ}$ – ширина полосы частот радиолинии с ППРЧ.

Коэффициент энергетической помехозащищенности радиолинии с ППРЧ по отношению к шумовой преднамеренной помехе с учетом формул (12), (15) и (16) будет равен

$$K_{э.ПЗ} = exp\left[-\frac{1}{2} h_{доп}^2 \cdot \left(\left(\frac{P_п}{P_c} \right)_{вх.} \gamma + \frac{1}{h^2} \right) \right]. \qquad (17)$$

При отсутствии режима ППРЧ заградительная шумовая помеха действует в полосе частот подавляемого радиосигнала. Тогда $\gamma = 1$, а коэффициент энергетической помехозащищенности радиолинии (17) равен

$$K_{э.ПЗ} = exp\left[-\frac{1}{2} h_{доп}^2 \cdot \left(\left(\frac{P_п}{P_c} \right)_{вх.} + \frac{1}{h^2} \right) \right]. \qquad (18)$$

Таким образом, в процессе анализа структурной устойчивости системы радиосвязи доработаны отдельные этапы оценки связности информационных направлений на сети связи в условиях воздействия дестабилизирующих факторов (особенностей распространения радиоволн, ведения РЭБ). Приведенные соотношения (1)–(18) позволяют оценить связность информационных направлений с учетом влияния частотно-энергетических характеристик радиолиний, образующих систему радиосвязи, а также разведзащищенности и других характеристик системы радиосвязи.

Пример применения методики

Применение методики оценки связности СРС состоит в последовательном выполнении ряда этапов, в процессе которых определяются показатели помехозащищенности радиолиний, образующих сеть радиосвязи, рассчитываются с применением известных методик [1,9] или задаются на основе нормативных документов показатели разведзащищенности, анализируется коэффициент устойчивости однозвенной информационной цепи и определяется вероятность связности (устойчивость) информационного направления.

В качестве примера использования представленной методики проведен анализ устойчивости сети радиосвязи тактического звена управления, построенной на основе радиосредств шестого поколения Р-187-В. Принятые в примере ограничения и значения параметров средств радиосвязи приведены в таблице 2.

На рис. 1 в совмещенных осях координат приведены графики, иллюстрирующие результаты анализа устойчивости сети радиосвязи.

- Линия 1 – зависимость коэффициента энергетической помехозащищенности $K_{э.ПЗ}$ от высоты подъема антенны передающей станции Hb с коэффициентом усиления антенны – 2 дБ, интервал связи 10 км и отношение мощностей помехи и сигнала равно 1.
- Линия 2 – зависимость коэффициента энергетической помехозащищенности $K_{э.ПЗ}$ от высоты подъема антенны передающей станции Hb с коэффициентом усиления антенны 6 дБ, интервал связи 10 км и отношение мощностей помехи и сигнала равно 1.
- Линия 3 – зависимость коэффициента устойчивости однозвенной информационной цепи $K_{уИЦ1}$ от коэффициента энергетической помехозащищенности $K_{э.ПЗ}$ при вероятности вскрытия радиолинии противником равной 1.
- Линия 4 – зависимость коэффициента устойчивости однозвенной информационной цепи $K_{уИЦ1}$ от коэффициента энергетической помехозащищенности $K_{э.ПЗ}$ при вероятности вскрытия радиолинии противником равной 0,6.
- Линия 5 – зависимость вероятности связности информационного направления $K_{у\,ин}$ от коэффициента устойчивости однозвенной информационной цепи $K_{уИЦ1}$ при использовании резервных маршрутов.
- Линия 6 – зависимость вероятности связности информационного направления $K_{у\,ин}$ от коэффициента устойчивости однозвенной информационной цепи $K_{уИЦ1}$ без резервирования.
- Линии 7÷14 являются результирующими и представляют зависимости связности информационного направления в сети радиосвязи от высоты подъема антенны передающей станции при различных коэффициентах усиления антенн, вероятностях вскрытия радиолиний и способах организации резервирования радионаправлений. Из анализа этих графиков видно, что в пределах варьируемых параметров при штатной высоте подъема антенн Hb = 4 м вероятность связности не превышает 0,6 (линии 13 и 14).

Для обеспечения более высокой вероятности связности, представленная методика позволяет сформировать перечень вариантов системы радиосвязи, реализующих

Таблица 2.

Принятые ограничения и параметры средств радиосвязи

Параметры измерения	Значения	Единицы
Число узлов в сети радиосвязи	32	
Максимальное число интервалов ретрансляции	2	
Число резервных маршрутов	3	
Мощность передающего устройства с учетом коррекции пик-фактора	6	дБВт
Коэффициент усиления антенны	-2 ÷ +6	дБ
КПД антенно-фидерного тракта	0	дБ
Чувствительность приемного устройства	-118	дБВт
Спектральная плотность мощности шума тракта приема	-164	дБм/Гц
Вид модуляции OFDM с QAM16, полоса частот радиосигнала	5	МГц
Диапазон частот	520 ÷ 2500	МГц
Меры помехозащиты: ППРЧ в полосе частот	100	МГц
Допустимая средняя вероятность ошибки бита	0,005	
Протяженность радиолинии	10	км
Отношение мощностей помехи и сигнала в точке приема	1	
Вероятность вскрытия радиолинии противником	0,6 ÷ 1	
Вероятность постановки помех	1	
Методика определения потерь на трассе распространения радиоволн	Окамура – Хата[7]	

7 Рекомендация МСЭ – R 1546-4. Метод прогнозирования для трасс связи «пункта с зоной» для наземных служб в диапазоне частот от 30 МГц до 3000 МГц. – Женева: МСЭ, 2010.

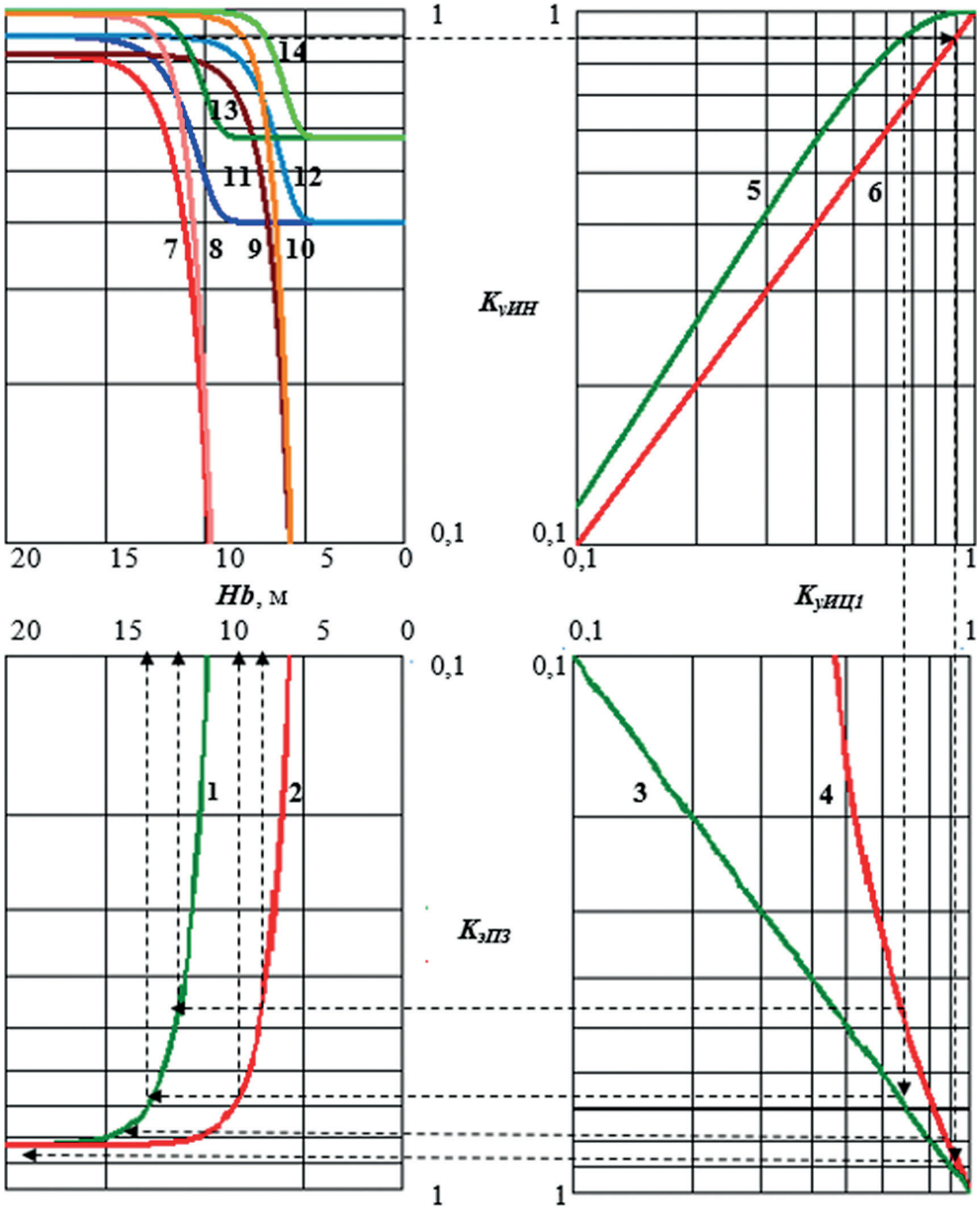

Рис. 1. Результаты анализа устойчивости сети радиосвязи, построенной с использованием радиосредств шестого поколения

нормативные требования. Так, вероятность связности 0,9 (пунктирные линии на рис. 1) в сети связи с резервированием направлений (линия 5) и вероятностью вскрытия радиолинии 0,6 (линия 4) обеспечивается при высоте подъема антенны 7 м (линия 2 – коэффициент усиления антенны 6 дБ) или 12 м (линия 1 – коэффициент усиления антенны – 2 дБ).

Заключение

Разработанная методика оценки устойчивости функционирования системы радиосвязи учитывает особенности построения структуры сети радиосвязи, порядок формирования резервных маршрутов при организации информационных направлений, устойчивость, разведзащищенность и помехозащищенность однозвенных информационных цепей, образующих информационные направления. Отмеченные показатели качества системы радиосвязи посредством аналитического аппарата теории вероятностей свернуты в обобщенный показатель устойчивости функционирования системы, которым является связность информационного направления. Ряд параметров, используемых в методике, задаются в виде ограничений на основе нормативных документов. Увязка результата оценки

связности направлений связи с помехозащищенностью радиолиний сети связи позволяет расширить пределы методики для решения практических задач анализа и проектирования СРС, функционирующих при воздействии РЭП и в различных условиях распространения радиоволн, что продемонстрировано примером. Необходимо отметить, что полученная в рамках методики оценка связности информационного направления является основой для анализа таких показателей качества военной связи, как своевременность и достоверность.

Литература

1. Боговик А. В., Игнатов В. В. Эффективность систем военной связи и методы ее оценки. СПб.: ВАС, 2006. 183 с.
2. Михайлов Р. Л., Макаренко С. И. Оценка устойчивости сети связи в условиях воздействия на неё дестабилизирующих факторов // Радиотехнические и телекоммуникационные системы. 2013. № 4. С. 69–79.
3. Одоевский С. М., Лебедев П. В. Методика оценки устойчивости функционирования системы технологического управления инфокоммуникационной сетью специального назначения с заданной топологической и функциональной структурой // Системы управления, связи и безопасности. 2021. № 1. С. 152–189. DOI: 10.24411/2410-9916-2021-10107.
4. Беккиев А. Ю. Оценка помехозащищенности каналов радиосвязи в условиях действия помех от средств радиоэлектронной борьбы / А. Ю. Беккиев, В. И. Борисов // Радиотехника и электроника. – 2019. – Т. 64, № 9. – С. 891–901. – DOI 10.1134/S0033849419080035. – EDN PPLRCH.
5. Борисов В. И. Помехозащищенность систем радиосвязи. Вероятностно-временной подход / В. И. Борисов, В. М. Зинчук. – Москва: Научно-техническое издательство «Радио и связь», 1999. – 252 с. – ISBN 5-256-01397-1. – EDN SGNCYB.
6. Прокис Джон Дж. Цифровая связь / Прокис Дж.; Пер. с англ. под ред. Кловского Д. Д. – Москва: Радио и связь, 2000. – 797 с.: ил.; 30 см.; ISBN 5-256-01434-X (рус.)
7. Феер К. Беспроводная цифровая связь. Методы модуляции и расширения спектра: Пер. с англ. / Под ред. В. И. Журавлева. – М.: Радио и связь, 2000. – 520 с.: ил.
8. Борисов В. И. Помехозащищенность систем радиосвязи с расширением спектра сигналов методом псевдослучайной перестройки рабочей частоты / В. И. Борисов, В. М. Зинчук, А. Е. Лимарев. – 2-е издание, переработанное и дополненное. – Москва: Радио Софт, 2008. – 512 с. – ISBN 978-5-93274-014-9. – EDN SMIHSV.
9. Моисеев А. А. Оценка основных свойств применения мобильных аппаратных связи / А. А. Моисеев, А. А. Киселев // Техника средств связи. – 2021. – № 1(153). – С. 55–66. – EDN GRNORY.

METHODOLOGY FOR ANALYZING THE STABILITY OF THE RADIO COMMUNICATION NETWORK UNDER THE INFLUENCE OF DESTABILIZING FACTORS

Kiselev V. N.[8], Kozoriz D. A.[9], Tripolin A. M.[10], Selezenev N. V.[11]

Keywords: *noise immunity, electronic warfare, communication network, radio communication system, intelligence security, probability of connectivity, information direction, signal-to-noise ratio.*

Abstract

The purpose of the article *is to generalize and refine certain stages of assessing the structural stability of a radio communication system operating under the influence of destabilizing factors*

Result: *The article substantiates the use of the stability indicator to assess the quality of radio communication networks performing their functions under the influence of destabilizing factors to analyze*

8 Vladimir N. Kiselev, Ph.D., Professor, Leading Developer, JSC NPO «Angstrem», Moscow, Zelenograd, Russia. E-mail: vkicelev@yandex.ru

9 Denis A. Kozorez, Ph.D. in Technical Sciences, Head of the Scientific and Technical Center of JSC NPO «Angstrem», Moscow, Zelenograd, Russia. E-mail: kozorizda@npo-angstrem.ru

10 Alexander M. Tripolin, Ph.D.,, Leading Specialist of JSC NPO «Angstrem», Moscow, Zelenograd, Russia. E-mail: tripolin@yandex.ru

11 Nikolay V. Selezenev, Ph.D.,, Chief Researcher of the Federal State Budgetary Institution «16 Central Research Institute of the Ministry of Defense of Russia». E-mail: nik-selezenev@yandex.ru

the impact of the frequency and energy characteristics of radio links forming a radio communication network on the stability of the system.

As an indicator of stability, the connectivity of the radio communication network is considered. The developed methodology is based on specific methods for analyzing the indicators of noise immunity, intelligence protection, stability coefficients of information circuits and directions.

An example of using the developed technique in the problems of assessing the probability of connectivity and substantiating the height of antenna elevation in a radio communication network built on the sixth-generation radio facilities is considered.

***Practical usefulness:** the results of the article can and should be taken into account when designing new samples of communication equipment.*

References

1. Bogovik A. V., Ignatov V. V. Jeffektivnost' sistem voennoj svjazi i metody ee ocenki. SPb.: VAS, 2006. 183 s.
2. Mihajlov R. L., Makarenko S. I. Ocenka ustojchivosti seti svjazi v uslovijah vozdejstvija na nejo destabilizirujushhih faktorov // Radiotehnicheskie i telekommunikacionnye sistemy. 2013. № 4. S. 69–79.
3. Odoevskij S. M., Lebedev P. V. Metodika ocenki ustojchivosti funkcionirovanija sistemy tehnologicheskogo upravlenija infokommunikacionnoj set'ju special'nogo naznachenija s zadannoj topologicheskoj i funkcional'noj strukturoj // Sistemy upravlenija, svjazi i bezopasnosti. 2021. № 1. S. 152–189. DOI: 10.24411/2410-9916-2021-10107.
4. Bekkiev A. Ju. Ocenka pomehozashhishhennosti kanalov radiosvjazi v uslovijah dejstvija pomeh ot sredstv radiojelektronnoj bor'by / A. Ju. Bekkiev, V. I. Borisov // Radiotehnika i jelektronika. – 2019. – T. 64, № 9. – S. 891–901. – DOI 10.1134/S0033849419080035. – EDN PPLRCH.
5. Borisov V. I. Pomehozashhishhennost' sistem radiosvjazi. Verojatnostno-vremennoj podhod / V. I. Borisov, V. M. Zinchuk. – Moskva: Nauchno-tehnicheskoe izdatel'stvo «Radio i svjaz'», 1999. – 252 s. – ISBN 5-256-01397-1. – EDN SGNCYB.
6. Prokis Dzhon Dzh. Cifrovaja svjaz' / Prokis Dzh.; Per. s angl. pod red. Klovskogo D. D. – Moskva: Radio i svjaz', 2000. – 797 s.: il.; 30 sm.; ISBN 5-256-01434-X (rus.)
7. Feer K. Besprovodnaja cifrovaja svjaz'. Metody moduljacii i rasshirenija spektra: Per. s angl. / Pod red. V. I. Zhuravleva. – M.: Radio i svjaz', 2000, 520 s.: il.
8. Borisov V. I. Pomehozashhishhennost' sistem radiosvjazi s rasshireniem spektra signalov metodom psevdosluchajnoj perestrojki rabochej chastoty / V. I. Borisov, V. M. Zinchuk, A. E. Limarev. – 2-e izdanie, pererabotannoe i dopolnennoe. – Moskva: RadioSoft, 2008. – 512 s. – ISBN 978-5-93274-014-9. – EDN SMIHSV.
9. Moiseev A. A. Ocenka osnovnyh svojstv primenenija mobil'nyh apparatnyh svjazi / A. A. Moiseev, A. A. Kiselev // Tehnika sredstv svjazi. – 2021. – № 1(153). – S. 55–66. – EDN GRNORY.

МЕТОДИКА ОРГАНИЗАЦИИ СЕТИ ОБМЕНА ДАННЫМИ ДЛЯ РОЯ БЕСПИЛОТНЫХ ЛЕТАТЕЛЬНЫХ АППАРАТОВ С ЦЕЛЬЮ ОБЕСПЕЧЕНИЯ УСТОЙЧИВОГО ВЗАИМОДЕЙСТВИЯ

Деркач А. Е.[1], Чуднов А. М.[2]

DOI:10.21681/3034-4050-2025-4-68-73

Ключевые слова: *рой, беспилотные летательные аппараты, сеть обмена данными, устойчивость обмена данными, вероятность, своевременная доставка сообщений, кластеризация, таблицы маршрутизации.*

Аннотация

Цель работы: *разработка инновационного подхода к организации сетевой инфраструктуры для роевых систем беспилотных летательных аппаратов, функционирующих в составе распределенных систем управления.*

Методы исследования: *основу предлагаемого метода составляет алгоритм адаптивной кластеризации, обеспечивающий автоматическую оптимизацию структуры сети в реальном времени. Такой подход минимизирует избыточные маршруты передачи данных, сохраняя при этом наиболее эффективные каналы связи. Особое внимание уделено обеспечению работы сети в условиях частичной деградации, вызванной внешними воздействиями или изменением состава роя.*

Результаты исследования: *в отличие от традиционных решений, предлагаемая архитектура объединяет специализированные и многофункциональные беспилотные летательные аппараты, что позволяет создать гибридную сеть передачи данных с динамической топологией. Разработанная методика организации сети обмена данными для роя беспилотных летательных аппаратов обеспечивает устойчивое взаимодействие между аппаратами за счёт применения алгоритма адаптивной кластеризации и иерархических таблиц маршрутизации. Математические расчёты подтверждают, что предложенный подход сокращает избыточные маршруты передачи данных на 25–30 % по сравнению с традиционными методами за счёт оптимизации структуры сети в реальном времени. Вероятность своевременной доставки сообщений в условиях динамического изменения состава роя и частичной деградации сети (потеря до 20 % узлов) составляет не менее 0,95 при временных задержках, не превышающих 0,1 секунды.*

Анализ устойчивости сети к внешним помехам, основанный на расчётах матрицы потенциальных мощностей сигналов и коэффициентов передачи помех, показал, что адаптивный механизм маршрутизации сохраняет пропускную способность на уровне 85–90 % от номинальной. Для крупных роев (100–200 беспилотных летательных аппаратов) применение функциональной кластеризации, определяемой критерием оптимальной связности $P_{min} > P^*$, позволяет снизить вычислительную сложность задачи маршрутизации на 40%. Дополнительно математическое моделирование подтвердило повышение энергоэффективности системы на 15 % за счёт минимизации числа ретрансляций. Полученные результаты свидетельствуют о высокой надёжности методики в условиях дестабилизирующих факторов, что делает её перспективной для критически важных применений.

Научная новизна. *Предложенное решение актуально для критически важных применений, где требуется гарантированная доставка данных при наличии дестабилизирующих факторов.*

1 Деркач Алексей Евгеньевич, адъюнкт Военной академии связи имени Маршала Советского Союза С. М. Будённого, г. Санкт-Петербург, Россия. E-mail: alder2000@inbox.ru

2 Чуднов Александр Михайлович, доктор технических наук, профессор, профессор кафедры Военной академии связи имени Маршала Советского Союза С. М. Будённого, г. Санкт-Петербург, Россия. E-mail: chudnow@yandex.ru

Введение

Совершенствование системы связи для территориально распределенных роев беспилотных летательных аппаратов (БЛА), актуальные проблемы и перспективные решения.

В последние годы наблюдается стремительный рост применения роевых систем беспилотных летательных аппаратов в самых различных областях человеческой деятельности. Как показывают исследования [1–3], такие системы находят применение не только в традиционных военных и оборонных задачах, но и активно внедряются в гражданские сферы, включая промышленное производство, образовательные технологии и системы комплексной безопасности. Столь широкое распространение БЛА-технологий закономерно приводит к повышенным требованиям к надежности и эффективности систем их взаимодействия.

Как отмечается в работах [1–5; 7], ключевым аспектом проектирования современных роевых систем становится организация бесперебойной связи между отдельными аппаратами и другими элементами управляющей инфраструктуры. Особую сложность представляет обеспечение устойчивой коммуникации для территориально распределенных групп БЛА, где необходимо постоянно адаптировать маршруты передачи данных в условиях динамически изменяющейся обстановки.

Специфика работы таких распределенных систем, согласно исследованиям[3] [2–4, 8] заключается в чрезвычайно высокой скорости устаревания передаваемой информации. Временные рамки актуальности данных сокращаются до секундных интервалов, а в некоторых критических случаях – до долей секунды. Это предъявляет исключительные требования к временным характеристикам системы связи, где даже минимальные задержки могут привести к потере актуальности информации и, как следствие снижению эффективности всего роя.

Следует особо подчеркнуть, что физическое состояние и операционные возможности всего роя БЛА находятся в прямой зависимости от качества функционирования коммуникационной системы. Современные требования предполагают не просто наличие связи между аппаратами, но и гарантированное обеспечение строго определенных параметров обмена данными. Это включает в себя не только временные характеристики, но и такие важные показатели, как пропускная способность, устойчивость к помехам и способность к оперативной реконфигурации при изменении условий работы.

Анализ современных исследований [6, 7] показывает, что решение указанных проблем требует комплексного подхода, сочетающего передовые достижения в области сетевых технологий, алгоритмов маршрутизации и методов обработки информации в реальном времени. Особое внимание при этом уделяется разработке адаптивных протоколов обмена данными, способных подстраиваться под изменяющиеся условия эксплуатации без потери основных характеристик системы.

Постановка задачи

Современные исследования в области сетей обмена данными (СОД) для роев БЛА приобретают особую актуальность в свете необходимости обеспечения устойчивой работы сложных распределённых систем [1–4, 8]. Особое внимание уделяется не только вопросам оптимизации самих сетевых структур, но и анализу потенциальных угроз, способных нарушить их функционирование[4] [4, 5].

Ключевое значение приобретает разработка принципов построения отказоустойчивых СОД, учитывающих комплекс показателей:

- вероятностные характеристики связности сети;
- вероятностно-временные параметры передачи[5] [4];
- устойчивость к внешним воздействиям;
- способность к оперативной реконфигурации.

В работах [4] представлен значимый вклад в решение задач маршрутизации данных в условиях внешних воздействий, где предложена методика формирования адаптивных таблиц маршрутизации (ТМП). Данный подход обеспечивает оптимальное соотношение между вероятностью своевременной доставки сообщений и ресурсными ограничениями системы, демонстрируя эффективность

3 Соколов Н. А. Системные аспекты построения и развития сетей электросвязи специального назначения // International Journal of Open Information Technologies. 2014. Т. 2. № 9. С. 4–8.

4 Шнепс-Шнеппе М. А. От IN к IMS. О сетях связи военного назначения // International Journal of Open Information Technologies. 2014. Т. 2. № 1. С. 1–11.

5 Соколов Н. А. Системные аспекты построения и развития сетей электросвязи специального назначения // International Journal of Open Information Technologies. 2014. Т. 2. № 9. С. 4–8.

при управлении потоками данных между 10–20 объектами в зависимости от доступных вычислительных мощностей. Однако существующие подходы имеют ограничения при масштабировании для крупных роев.

Решение поставленной задачи

Настоящее исследование развивает указанные подходы, применяя их для организации как внутрикластерного, так и межкластерного взаимодействия.

Разрабатываемая методика структурирования СОД основана на следующих ключевых математических моделях и алгоритмах.

1. Алгоритм адаптивной кластеризации узлов БЛА.

Кластеризация узлов БЛА осуществляется на основе критерия оптимальной связности:

$P_{min} > P^*$, где:

- $P_{min} = min\{P_{ij}\}$ – минимальная вероятность связи между узлами кластера;
- $P^* = 1 - (1 - p)k$ – пороговое значение вероятности доставки;
- p - вероятность успешной передачи;
- k - число попыток передачи.

2. Механизм внутрикластерной маршрутизации.

Для каждого кластера строится оптимальная таблица маршрутизации, решающая задачу:

$$\min_{(\alpha,\beta,\gamma)} \sum(\alpha D_i + \beta E_i + \gamma L_i),$$

где:

- D_i – задержка передачи в i-м канале;
- E_i – энергозатраты на передачу;
- L_i – нагрузка канала;
- α, β, γ – весовые коэффициенты.

Весовые коэффициенты (α, β, γ) в предложенной модели представляют собой числовые параметры, которые определяют относительную важность различных критериев оптимизации при построении маршрутов в сети БЛА. Их назначение и свойства раскрываются ниже.

Назначение коэффициентов.

Каждый коэффициент регулирует вклад соответствующего фактора в целевую функцию оптимизации:

- α – вес задержки передачи (D) (определяет приоритет минимизации временных задержек. Чем выше α, тем сильнее алгоритм стремится сократить время доставки данных);
- β – вес энергопотребления (E) (учитывает энергоэффективность маршрута. Большие значения β акцентируют экономию энергии узлов);
- γ – вес нагрузки на каналы (L) (контролирует равномерность распределения трафика. Высокий γ снижает риск перегрузки отдельных каналов).

Математическая интерпретация.

В целевой функции

$$F = \alpha D + \beta E + \gamma L \to \min_{(\alpha,\beta,\gamma)},$$

коэффициенты:

- нормируются так, что $\alpha + \beta + \gamma = 1$ (для сравнимого вклада факторов);
- определяются экспериментально или аналитически, исходя из требований системы.

Практическое применение:

- военные задачи: высокий α (минимизация задержек), умеренный β;
- гражданский мониторинг: высокий β (экономия энергии), средний γ;
- условия помех: увеличение γ для балансировки нагрузки при деградации каналов.

Связь с другими параметрами системы.

Коэффициенты корректируются динамически на основе:

- текущей топологии сети (матрицы связности $C = [P_{ij}]$);
- уровня помех (матрицы $H = [h_{ij}]$);
- остатка энергии узлов.

3. Протокол межкластерного обмена.

Межкластерная маршрутизация реализуется через узлы, выбираемые по критерию:

$$argmax_j (\sum P_{ij} \cdot B_j),$$

где:

- P_{ij} – вероятность устойчивой связи;
- B_j – пропускная способность узла.

Математическая модель сети включает:

- матрицу связности $C = [P_{ij}]$;
- матрицу трафика $\Lambda = [\lambda_{ij}]$;
- матрицу энергопотребления $E = [e_{ij}]$.

Реализация алгоритмов обеспечивает:

1. Автоматическое перераспределение ролей узлов при изменении топологии.

2. Балансировку нагрузки между кластерами.

3. Адаптацию к внешним помехам с сохранением:

- пропускной способности ≥85 % от номинальной;
- вероятности доставки ≥ 0.95;
- задержек ≤ 100 мс.

Особенностью предлагаемого решения является учет динамического характера потенциальных соединений, реализуемых различными режимами работы радиосредств. Такой подход расширяет традиционные задачи распределения информационных потоков, устраняя ограничения фиксированной канальной структуры, хотя и требует дополнительных вычислительных ресурсов [4, 8].

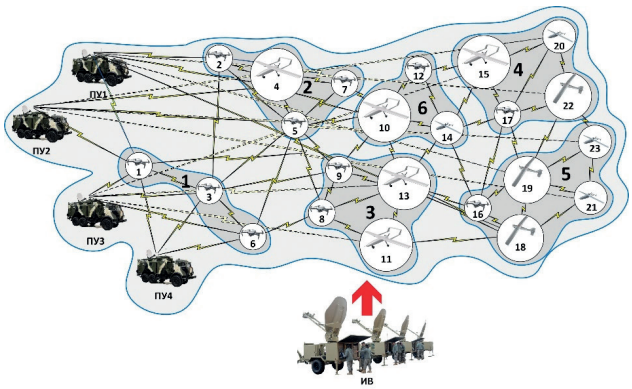

Рис. 1. Пример структуры роя БЛА

Рассматриваемая архитектура роя БЛА включает летательные аппараты различного функционального назначения (разведка, транспортировка, связь) и наземный комплекс управления [4, 9].

На рис. 1 показана архитектура решения, где:

- сплошные линии – активные каналы передачи;
- пунктирные – резервные маршруты;
- выделенные зоны –кластеры с автономной маршрутизацией.

Особое место в модели занимает модуль деструктивных воздействий, способный ухудшать качество связи или выводить из строя отдельные узлы связи.

Математическая модель СОД включает следующие параметры:

- количество узлов n в группе БЛА;
- матрицу интенсивностей потоков данных;
- матрицу потенциальных мощностей сигналов;
- векторы характеристик приемо-передающих устройств;
- систему рандомизированных таблиц маршрутизации.

Параметры воздействия помех описываются:

- суммарной мощностью помехи;
- вектором распределения помех по узлам;
- матрицей коэффициентов передачи помех.

На основе этих параметров возможно построение ТМП, максимизирующих вероятность своевременной доставки сообщений [4]. Однако вычислительная сложность задачи резко возрастает с увеличением размерности системы, что ограничивает практическое применение метода для крупных роев (100–200 объектов). Предлагаемый принцип функциональной кластеризации позволяет преодолеть это ограничение за счет разбиения сети на структурные единицы по критерию оптимальной связности, определяемому неравенством $P_{min} > P^*$, где P^* – минимально допустимая вероятность успешной передачи пакета за заданное время.

Алгоритм кластеризации реализует итеративный процесс формирования групп узлов, на каждом шаге оценивая вероятность установления надежной связи между элементами. Центральные узлы связи кластеров определяются по критерию максимальной связности, что обеспечивает эффективную организацию как внутригруппового, так и межгруппового обмена данными.

Заключение

Представленная методика демонстрирует высокую эффективность в управлении потоками данных внутри роевых систем БЛА, обеспечивая стабильность информационного обмена даже при наличии внешних дестабилизирующих воздействий. Разработанный подход открывает новые перспективы для создания адаптивных алгоритмов маршрутизации и обработки информации в распределенных сетях беспилотных летательных аппаратов.

Литература

1. Bujari A., Calafate C. T., Cano J. C., Manzoni P., Palazzi C. E., Ronzani D. Flying ad-hoc network application scenarios and mobility models // Int. J. Distrib. Sensor Netw. 2017. Vol. 13. No. 10. P. 1–17. DOI: 10.1177/1550147717738192.
2. Довгаль В. А., Довгаль Д. В. Анализ систем коммуникационного взаимодействия дронов, выполняющих поисковую миссию в составе группы // Вестник АГУ. 2020. № 4(271). С. 87–94.
3. Ананьев А. В., Стафеев М. А., Филатов С. В. Оценка эффективности систем связи и боевого управления на базе беспилотных летательных аппаратов межвидовой группировки войск // Воздушно-космические силы. Теория и практика. 2017. № 3(3). С. 75–84.
4. Чуднов А. М., Положинцев Б. И., Кичко Я. В. Анализ помехозащищенности обмена данными группы беспилотных летательных аппаратов в условиях оптимизированных помех // Радиотехника. 2022. Т. 86. № 12. С. 33–46. DOI: https://doi.org/10.18127/j00338486-202212-03.
5. Макаренко С. И. Перспективы и проблемные вопросы развития сетей связи специального назначения // Системы управления, связи и безопасности. 2017. № 2. С. 18–68. DOI: 10.24411/2410–9916–2017–10202.
6. Макаренко С. И. Усовершенствование функций многоуровневой иерархической кластеризации протокола маршрутизации pnni с целью повышения устойчивости сети связи // I-methods. 2020. Т. 12. № 2. С. 1–21.
7. Будко П. А., Жуков Г. А. Групповое использование робототехнических комплексов при выполнении миссий на глобальных удалениях от пункта управления // T-Comm: Телекоммуникации и транспорт. 2017. Т. 11. № 9. С. 4–14.
8. Чуднов А. М., Кичко Я. В. Губская О. А. Методика анализа вероятностно-временных характеристик обмена сообщениями в комплексе беспилотных летательных аппаратов //Известия ТулГУ. Технические науки. 2021. Вып. 11. С. 117–124. DOI: 10.24412/2071-6168-2021-11-117-124.
9. Чуднов А. М. Математические основы моделирования, анализа и синтеза систем. – СПб.: ВАС, 2021. – 192 с.

METHODOLOGY FOR ORGANISING A DATA EXCHANGE NETWORK FOR A SWARM OF UNMANNED AERIAL VEHICLES TO ENSURE SUSTAINABLE INTERACTION

Derkach A. E.[6], Chudnov A. M.[7]

Keywords: *swarm, unmanned aerial vehicles, data exchange network, data exchange stability, probability, timely delivery of messages, clustering, routing tables.*

Abstract

The purpose of the work *is to develop an innovative approach to the organization of network infrastructure for swarm systems of unmanned aerial vehicles operating as part of distributed control systems.*

Research methods: *the proposed method is based on the adaptive clustering algorithm, which provides automatic optimization of the network structure in real time. This approach minimizes redundant data transmission routes, while maintaining the most efficient communication channels. Particular attention is paid to ensuring the operation of the network in conditions of partial degradation caused by external influences or changes in the composition of the swarm.*

Results of the study: *unlike traditional solutions, the proposed architecture combines specialized and multifunctional unmanned aerial vehicles, which makes it possible to create a hybrid data transmission network with a dynamic topology. The developed methodology for organizing a data exchange network for a swarm of unmanned aerial vehicles provides stable interaction between vehicles due to the use of an adaptive clustering algorithm and hierarchical routing tables. Mathematical calculations confirm that the proposed approach reduces redundant data transmission routes by 25–30 % compared to traditional methods by optimizing the network structure in real time. The probability of timely delivery of messages under*

6 Alexey E. Derkach, Adjunct of the Military Academy of Communications, St. Petersburg, Russia. E-mail: alder2000@inbox.ru

7 Alexander M. Chudnov, Dr.Sc. of Technical Sciences, Professor, Professor of the Department of the Military Academy of Communications, St. Petersburg, Russia. E-mail: chudnow@yandex.ru

conditions of dynamic changes in the composition of the swarm and partial degradation of the network (loss of up to 20 % of nodes) is at least 0.95 with time delays not exceeding 0.1 seconds. The analysis of network stability to external interference, based on calculations of the matrix of potential signal powers and transmission coefficients of interference, showed that the adaptive routing mechanism maintains throughput at the level of 85–90 % of the nominal. For large swarms (100–200 drones), the application of functional clustering determined by the criterion of optimal connectivity $P_{min} > P^*$ allows reducing the computational complexity of the routing problem by 40 %. Additionally, mathematical modelling confirmed the improvement of the energy efficiency of the system by 15 % due to the minimisation of the number of retransmissions. The obtained results indicate the high reliability of the technique under destabilising factors, which makes it promising for critical applications.

Scientific novelty. *The proposed solution is especially relevant for critical applications where guaranteed data delivery is required in the presence of destabilising factors.*

References

1. Bujari A., Calafate C. T., Cano J. C., Manzoni P., Palazzi C. E., Ronzani D. Flying ad-hoc network application scenarios and mobility models // Int. J. Distrib. Sensor Netw. 2017. Vol. 13. No. 10. P. 1–17. DOI: 10.1177/1550147717738192.
2. Dovgal' V. A., Dovgal' D. V. Analiz sistem kommunikacionnogo vzaimodejstvija dronov, vypolnjajushhih poiskovuju missiju v sostave gruppy // Vestnik AGU. 2020. № 4(271). S. 87–94.
3. Anan'ev A. V., Stafeev M. A., Filatov S. V. Ocenka jeffektivnosti sistem svjazi i boevogo upravlenija na baze bespilotnyh letatel'nyh apparatov mezhvidovoj gruppirovki vojsk // Vozdushno-kosmicheskie sily. Teorija i praktika. 2017. № 3(3). S. 75–84.
4. Chudnov A. M., Polozhincev B. I., Kichko Ja. V. Analiz pomehozashhishhennosti obmena dannymi gruppy bespilotnyh letatel'nyh apparatov v uslovijah optimizirovannyh pomeh // Radiotehnika. 2022. T. 86. № 12. S. 33–46. DOI: https://doi.org/10.18127/j00338486-202212-03.
5. Makarenko S. I. Perspektivy i problemnye voprosy razvitija setej svjazi special'nogo naznachenija // Sistemy upravlenija, svjazi i bezopasnosti. 2017. № 2. S. 18–68. DOI: 10.24411/2410–9916–2017–10202.
6. Makarenko S. I. Usovershenstvovanie funkcij mnogourovnevoj ierarhicheskoj klasterizacii protokola marshrutizacii pnni s cel'ju povyshenija ustojchivosti seti svjazi // I-methods. 2020. T. 12. № 2. S. 1–21.
7. Budko P. A., Zhukov G. A. Gruppovoe ispol'zovanie robototehnicheskih kompleksov pri vypolnenii missij na global'nyh udalenijah ot punkta upravlenija // T-Comm: Telekommunikacii i transport. 2017. T. 11. № 9. S. 4–14.
8. Chudnov A. M., Kichko Ja. V. Gubskaja O. A. Metodika analiza verojatnostno-vremennyh harakteristik obmena soobshhenijami v komplekse bespilotnyh letatel'nyh apparatov //Izvestija TulGU. Tehnicheskie nauki. 2021. Vyp. 11. S. 117–124. DOI: 10.24412/2071-6168-2021-11-117-124.
9. Chudnov A. M. Matematicheskie osnovy modelirovanija, analiza i sinteza sistem. – SPb.: VAS, 2021. – 192 s.

СХЕМНЫЕ РЕШЕНИЯ ИСТОЧНИКА ПИТАНИЯ ПОЛЕВОГО ТЕЛЕФОННОГО АППАРАТА

Гусеница Я. Н.[1], Квасов М. Н.[2], Ефремов А. В.[3]

DOI:10.21681/3034-4050-2025-4-74-78

Ключевые слова: *проводная телефонная связь, аккумуляторная батарея, микроконтроллер, ток заряда, светодиод*

Аннотация

Цель статьи *состоит в улучшении эксплуатационных характеристик источников питания полевых телефонных аппаратов.*

Результаты: *проведен анализ технических характеристик существующих источников питания полевых телефонных аппаратов ТА-57 на основе гальванических соляных или щелочных элементов. Предложено заменить указанные элементы в источниках питания на аккумуляторные перезаряжаемые батареи, включив в состав контроллер заряда, а также светодиоды индикации степени заряженности. Разработаны варианты исполнения источника питания за счет использования аналогичных по назначению и доступности контроллеров.*

Практическая ценность: *разработаны схемные решения перезаряжаемого источника питания для полевого телефонного аппарата на основе использования литий-ионных аккумуляторов и модуля зарядки со встроенной системой индикации заряда, что позволяет увеличить в два раза срок службы источника питания, а также обеспечить визуализацию контроля заряда.*

Введение

В настоящее время для организации проводной связи в Вооруженных Силах Российской Федерации используются военно-полевые телефонные аппараты ТА-57. Разработанные более полувека назад, они, тем не менее, активно применяются в позиционных боях в ходе проведения специальной военной операции [1].

Надежность связи с использованием ТА-57 во многом определяется работоспособностью источников питания, в качестве которых выступают галетные батареи ГБ-10У номинальным напряжением 10 В [2].

На сегодняшний день семейство батарей, используемых в телефонном аппарате ТА-57 включает: ГБ-10У-1,3, ГБ-10У-1,6, ГБ-10У-2,0, ГБ-10У-2,6, ГБ-10У-2,7, ГБ-10У-3, «Элемс 10Т», «АТАКА», 7LR6.

Перечисленные источники питания имеют в своем составе последовательно соединенные углеродно-цинковые или марганцевого-цинковые щелочные элементы, которые заключены в пластиковый корпус с контактами для подключения телефонного аппарата. Основным различием перечисленных источников питания является их емкость: от 1,3 до 3,0 А·ч. Величина емкости определяется классом используемых элементов. Например, в источнике питания 7*LR*6 устанавливаются по 7 элементов *R*6 или *LR*6 фирм «*Duracell*» или «*Varta*», что обеспечивает их емкость на уровне до 3,0 А·ч. Выходное напряжение на внешних клеммах перечисленных источников питания составляет 10 В.

При этом габаритно-установочные и присоединительные размеры источников питания разных производителей, например, ООО НПО «Энергетические системы» (г. Новокузнецк), ООО «Энергия» (г. Елец), ООО «Центр связи и специальной техники» (г. Нижний Новгород), идентичны и соответствуют размерам батарейной камеры телефонного аппарата.

Общими недостатками перечисленных источников питания являются:

1. Относительно небольшой срок эксплуатации, который при отрицательных температурах может быть значительно ниже ресурса

1 Гусеница Ярослав Николаевич, кандидат технических наук, начальник научно-исследовательского отдела. ФГАУ «Военный инновационный технополис «ЭРА». Тел. +7 (495) 693-30-99 (25-60). E-mail: era_otd1@mil.ru

2 Квасов Михаил Николаевич, кандидат технических наук, заместитель начальника научно-исследовательского отдела. ФГАУ «Военный инновационный технополис «ЭРА». Тел. +7 (495)693-30-99 (21-83). E-mail: era_otd1@mil.ru

3 Ефремов Александр Васильевич, кандидат технических наук, научный сотрудник научно-исследовательского отдела. ФГАУ «Военный инновационный технополис «ЭРА». Тел. +7 (495) 693-30-99 (25-66). E-mail: era_otd1@mil.ru

батарей, указанного в Технических условиях, т.е. менее 6 месяцев.

2. Отсутствие средств контроля заряда батарей. Из-за этого для обеспечения бесперебойной связи у связиста всегда должен быть в запасе дополнительный полностью заряженный источник питания.

3. Отсутствие возможности перезарядки. Источники питания являются одноразовыми и, ввиду высокой токсичности из-за наличия в них солей тяжелых металлов, после разряда подлежат утилизации. Разборки и замены батарей в указанных источниках питания не предусмотрено.

4. Завышенная цена при небольшом сроке службы.

Для частичной компенсации указанных недостатков в войсковых частях в качестве источника питания используют аккумуляторы типа «Крона». Однако, ввиду сложности их крепления в батарейной камере, возможно нарушение электрического контакта между аккумулятором и клеммами телефонного аппарата, вследствие чего возможен обрыв связи с абонентами при небольших толчках аппарата. Этот недостаток может быть нивелирован изготовлением переходников под аккумуляторы типа «Крона» методом 3*D*-печати. Вместе с тем, в полевых условиях сложно обеспечить заряд аккумулятора типа «Крона», в результате чего использование этих аккумуляторов широкого применения не нашло.

Поэтому вопросы, связанные с улучшением эксплуатационных характеристик источников питания военно-полевых телефонных аппаратов, являются весьма актуальными.

Техническое решение

Для обеспечения бесперебойного электропитания ТА-57 в Военном инновационном технополисе «ЭРА» разработана, изготовлена и апробирована в реальных условиях эксплуатации новая конструкция источника питания.

Задача разработанной конструкции – повышение долговечности источника питания полевых телефонных аппаратов путем обеспечения возможности заряда используемых в батарее аккумуляторов, а также повышение удобства эксплуатации за счет световой индикации степени заряда.

Поставленная задача решена следующим образом.

В качестве источника питания ТА-57 используются электрически соединенные в батарею литиевые аккумуляторы и контроллер, размещенные в пластиковом корпусе, аналогичном по размеру штатным батареям ГБ-10У.

Для заряда аккумуляторной батареи (АКБ) в усовершенствованной конструкции источника питания предлагается использовать электрическую схему на основе модуля заряда *Li-ion* с повышающим *DC-DC* преобразователем, который построен на микросхеме *TP*4056 – контроллере зарядки *Li-ion* и *Li-Po* аккумуляторов на 3,7 В со встроенным термодатчиком. Это завершенное изделие с линейным зарядом по принципу постоянное напряжение/постоянный ток для одноэлементных литий-ионных аккумуляторов. Модуль имеет индикацию процесса заряда за счет включенных в электрическую схему двух светодиодов. В момент заряда светится красный светодиод. Когда батарея будет полностью заряжена, загорается зеленый светодиод, красный при этом гаснет.

На основе *TP*4056 серийно выпускаются несколько модификаций модулей зарядки с системами защиты, например, *J*-5019. Этот модуль состоит из регулируемого повышающего *DC-DC*-преобразователя на микросхеме *MT* 3608 и контроллера заряда на микросхеме *TP*4056 с разъемом *micro-USB* на входе питания (рис. 1).

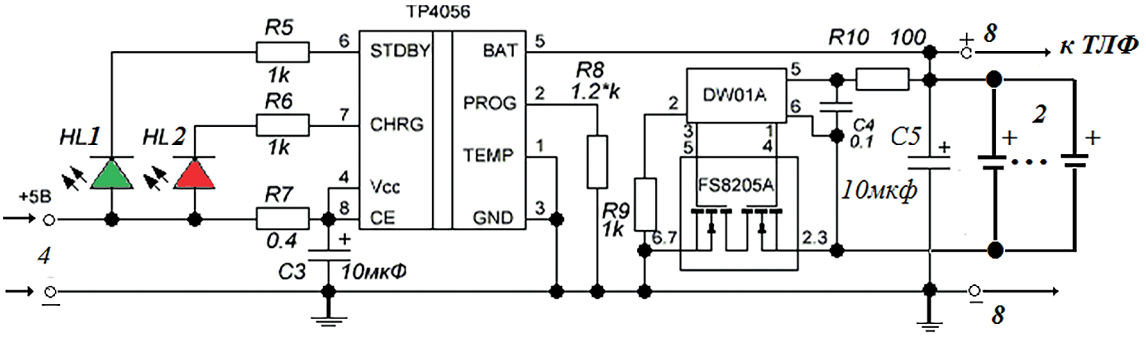

Рис. 1. Электрическая схема модуля заряда источника питания

Рекомендованный ток заряда для аккумуляторов емкостью более 2 А·ч составляет 1 А, он выставлен на модуле по умолчанию. Аккумуляторы, монтируемые в корпус источника питания, должны иметь одинаковую маркировку. Электрическая схема заряда аккумуляторов, исходя из величины максимального зарядного тока, позволяет использовать в источнике питания параллельно соединенные аккумуляторы общей емкостью не менее 2 А·ч.

Схемные решения

Внутренняя полость корпуса источника питания ТА-57 имеет размеры 54×50×45 мм. Исходя из этого, в источнике питания могут быть использованы соединенные в батарею литиево-ионные (*Li-ion*), литиево-полимерные (*Li-Po*) или литий-железо-фосфатные (*Li-Fe-PO*$_4$) аккумуляторы, номинальные напряжения которых составляют 3,3–3,7 В.

Количество аккумуляторов в батарее определяется их габаритными размерами, т.е. возможностью размещения в корпусе источника питания. Увеличение количества параллельно соединенных аккумуляторов в источнике питания ведет к увеличению их общей емкости. Однако, продолжительность заряда при этом также увеличивается.

Схема параллельного соединения аккумуляторов в батарею обеспечивает напряжение на выходе батареи 3,7 В. Повышение до рабочего напряжения 10 В осуществляется за счет *DC-DC* преобразователя.

Монтаж аккумуляторов и платы модуля заряда в источнике питания показан на рис. 2, на котором приняты следующие обозначения: 1 – пластиковый корпус источника питания с крышкой; 2 – литиевые аккумуляторы; 3 – контроллер; 4 – электрические клеммы разъема *micro-USB*; 5 – изолирующая прокладка из поролона; 6 – светодиоды индикации процесса заряда, 7 – соединительные электрические провода; 8 – электрические клеммы источника питания; 9 – электрические выводы АКБ.

Источник питания работает следующим образом. При подаче внешнего питания через разъем *micro-USB* 4 загорается красный светодиод 6, свидетельствующий о начале заряда аккумуляторов. Одновременно подается напряжение 10 В на выходные клеммы 8 источника питания, что позволяет прямо в процессе зарядки обеспечивать электропитанием телефонный аппарат.

Заряд аккумуляторных батарей проводится напряжением 4,2 В и током зарядки 1 А. После полного заряда аккумуляторов загорается зеленый светодиод. Источник питания отключают от внешнего питания и устанавливают в телефонный аппарат. Питание телефонного аппарата напряжением 10 В осуществляется через повышающий преобразователь *DC-DC* от аккумуляторной батареи напряжением 3,7 В.

При этом схему контроллера *J*5019 при подаче внешнего питания можно использовать как источник бесперебойного питания телефонного аппарата. При отключении внешнего питания питание телефонного аппарата будет осуществляться от заряженной АКБ.

Общий вид перезаряжаемого источника питания представлен на рис. 3. Корпус источника питания предлагается изготавливать из *PETG*-пластика путем 3*D*-печати. В корпус

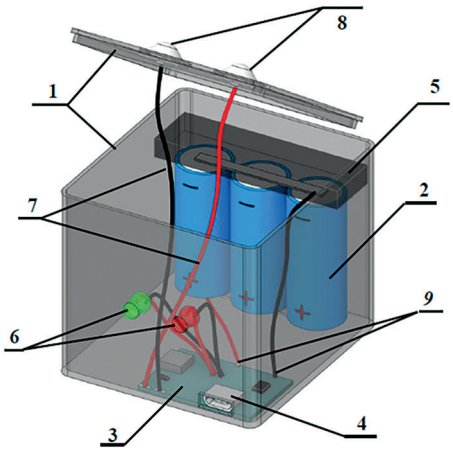

Рис. 2. Общий вид источника питания в сборе в виде электронной геометрической модели изделия

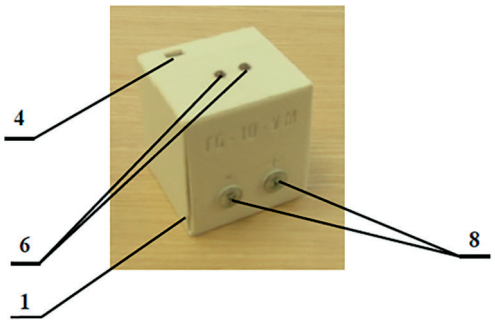

Рис. 3. Внешний вид готового источника питания

монтируют: предварительно собранную электрическую схему контроллера 3; литиевые аккумуляторы 2; два светодиода 6 разных цветов, соединенные электрическими проводами 7 с двумя электрическими клеммами 8 (рис. 2, 3).

Разъем *micro-USB* 4 модуля зарядки и светодиоды 6 размещаются на внешней грани корпуса источника в специально высверленных отверстиях и подключаются к электрической цепи.

Заряд аккумуляторной батареи может проводиться от внешнего источника питания:

- переменного тока – через сетевое зарядное устройство, например, *REXANT USB* 5 V 21 A с выходным током 2,1 A и напряжением 5 В с помощью кабеля источник питания *SOCKS* 1 A;
- постоянного тока – от внешнего аккумулятора, например, *POWER BANK Xiaomi Mi* 22,5 Вт.

Для обеспечения неподвижности в корпусе, а также влагоустойчивости и пылезащищенности, аккумуляторы, модуль зарядки и светодиоды, после размещения их в корпусе источника питания фиксируют термоклеем. Кроме того, торцевые части аккумуляторов закрывают изолирующим слоем поролона. Крышку корпуса источника питания после монтажа всех элементов также фиксируют термоклеем.

Изготовленные источники питания с литиевыми АКБ в ходе практического использования показали следующие достоинства:

- продолжительность непрерывного разговора по телефонному аппарату при полном заряде аккумуляторов составляет не менее 200 часов при потребляемом аппаратом токе 6–8 мА;
- не менее 400–500 циклов заряд-разряд при использовании литиевых аккумуляторов типа *Li-ion* и *Li-Po* и не менее 2000 циклов – при использовании аккумуляторов типа *Li-Fe-PO*$_4$, что гарантирует срок службы источника питания при периодическом заряде аккумуляторной батареи не менее 5 лет;
- снижение затрат на утилизацию источников питания за счет обеспечения их долговечности. При этом при выходе из строя аккумуляторов имеется возможность их извлечения из корпуса и замены новыми;
- высокую тиражируемость. Простота и прочность корпуса источника питания, изготовленного из полимерного материала обеспечивают его промышленную применимость;
- возможность заряда АКБ в процессе работы полевого телефонного аппарата без прерывания связи;
- широкую вариативность используемых модулей контроля заряда, исходя из их наличия на рынке и стоимости, а также имеющихся типов разъемов внешнего питания.

По разработанному техническому решению источника питания телефонного аппарата ТА-57 с использованием аккумуляторных батарей получен патент на полезную модель [3].

Выводы

1. Разработанный и изготовленный источник питания военно-полевого телефонного аппарата ТА-57 с использованием литиевых аккумуляторов имеет ряд существенных преимуществ над используемыми в настоящее время серийными аналогами, в том числе:

- возможность заряда во время хранения или в процессе эксплуатации (в ходе работы телефонного аппарата) от внешних источников постоянного или переменного тока;
- значительно (не менее чем в два раза) увеличенный срок службы;
- удобство эксплуатации с обеспечением визуального контроля заряда аккумуляторной батареи;
- технологичность конструкции;
- широкий выбор литиевых аккумуляторов для комплектования источников питания, а также, за счет увеличения их числа, потенциальная возможности повышения общей емкости батареи источника питания;
- сопоставимые стоимости в серийном производстве источника питания с использованием литиевых аккумуляторов и существующих источников питания.

2. В ходе разработки предложены несколько вариантов исполнения источника питания за счет использования аналогичных по назначению и доступности контроллеров (в части типа используемых литиевых аккумуляторов, а также разных типоразмеров и с различными входными разъемами).

Литература

1. Тевс О. П., Пустошкин М. М. Моделирование тактики подразделений связи в условиях современного вооруженного противоборства // Телекоммуникации и связь. – 2024. № 3. – С. 5–13.
2. Тишков В. В., Иванов В. Г., Лукьянчик В. Н. Обоснование облика построения перспективных комплексов и средств связи на основе опыта организации связи при проведении специальной военной операции // Военная мысль. – 2023. – № 9. – С. 59–72.
3. Патент RU 229461 U1, Российская Федерация, МПК H02J 7/04. Источник питания телефонного аппарата; Заявка: № 2024110470; заявл. 16.04.2024; опубл. 08.10.2024 // Малаховецкий А. А., Гусеница Я. Н., Квасов М. Н., Ефремов А. В.

CIRCUITRY OF POWER SUPPLY FOR FIELD TELEPHONE SET

Gusenitsa Ya. N.[4], Kvasov M. N.[5], Efremov A. V.[6]

Keywords: *wired communication, rechargeable battery, microcontroller, charge current, LED.*

Abstract

The purpose of the work: *performance enhancement of power supplies for field telephone sets.*

The results: *existing power supplies for field telephone sets TA-57, based on dry and alkaline non-rechargeable (primary) cells, were analyzed, their drawbacks observed; it was proposed to replace them with rechargeable (secondary) cells, combined with charging controller and control LEDs into a power supply unit; power supply unit variants utilizing various charging controllers, cells and power connectors were developed.*

Practicality: *circuitry of rechargeable power supply with Li-ion cells and in-built charging controller with control LEDs was developed, which doubles the service life of the power supply and allows for battery charge control.*

References

1. Tevs O. P., Pustoshkin M. M. Modelirovanie taktiki podrazdelenii svyazi v usloviyakh sovremennogo vooruzhennogo protivoborstva [Modeling of tactics of communication units in the conditions of modern armed confrontation]. Telekommunikatsii i svyaz, 2024, no. 3, pp. 5–13 (in Russian).
2. Tishkov V. V., Ivanov V.G., Lukyanchik V. N. Obosnovanie oblika postroeniya perspektivnikh kompleksov i sredstv svyazi na osnove opita organizatsii svyazi pri provedenii spetsialnoi voennoi operatsii [Justification of the scheme of advanced communications complexes and facilities on the basis of the experience of the communications organization during the special military operation]. Military Thought, 2023, no 9, pp. 59–72 (in Russian).
3. Malakhovetskii A. A., Gusenitsa Ya. N., Kvasov M. N., Efremov A. V. Istochnik pitaniya telefonnogo apparata [Power supply for telephone set]. Patent Russia, no. 229461, 08.10.2024.

4 Gusenitsa Yaroslav Nikolaevich, Ph.D. of Technical Sciences, Head of the Research Department. FSAU «Military Innovation Technopolis «ERA». Tel. +7 (495) 693-30-99 (25-60). E-mail: era_otd1@mil.ru

5 Mikhail Nikolaevich Kvasov, Ph.D. of Technical Sciences, Deputy Head of the Research Department. Federal State Autonomous Institution «Military Innovation Technopolis «ERA». Tel. +7 (495) 693-30-99 (21-83). E-mail: era_otd1@mil.ru

6 Efremov Alexander Vasilyevich, Ph.D. of Technical Sciences, Researcher of the Research Department. Federal State Autonomous Institution «Military Innovation Technopolis «ERA». Tel. +7 (495) 693-30-99 (25-66). E-mail: era_otd1@mil.ru

ИНФОРМАЦИОННАЯ ЖИВУЧЕСТЬ КОРАБЛЯ, СУДНА: ПРИКЛАДНАЯ ТЕОРИЯ ОБЕСПЕЧЕНИЯ ВОЕННО-ТЕХНОЛОГИЧЕСКОГО ПРЕВОСХОДСТВА

Алексеев А. В.[1], Дригола В. К.[2], Михальчук А. В.[3]

DOI:10.21681/3034-4050-2025-4-79-89

Ключевые слова: *целеполагание; модель; живучесть судна; мониторинг; валидный контроль; уязвимость; угроза; конфиденциальность; доступность; целостность.*

Аннотация

Цель работы *состоит в обосновании необходимости расширения понятия живучести корабля, судна и разработке основных положений прикладной теории информационной живучести корабля, судна (И ЖС) в обеспечение военно-технологического превосходства.*

Метод исследования: *систематизация данных анализа, синтеза и оптимизации ИЖС на основе квалиметрической оценки агрегированного показателя проектного качества и эффективности эксплуатации системы комплексной защиты информации (СКЗИ) в составе автоматизированной системы обработки информации в защищенном исполнении (АСЗИ).*

Результаты исследования: *приведены типовые структурные модели ИЖС, СКЗИ, вербальная модель уязвимостей и угроз ИЖС, комплексная математическая модель оценки и оптимизации ИЖС, структурно-информационная модель цифрового двойника СКЗИ и пример программной реализации в варианте роботизированного проектного комплекса «КАСОР-24.4», обобщены полученные результаты формирования прикладной теории ИЖС.*

Научная новизна и практическая ценность *исследования состоит в обобщение и развитие прикладных теоретических аспектов введения и модельного представления анализа, синтеза и оптимизации нового для судостроительной отрасли понятия «информационная живучесть корабля, судна». Это позволило расширить категорию живучесть судна и впервые количественно учитывать/цифровизовать такие актуальные сегодня факторы развития информационных технологий как защищенность информационных ресурсов корабля, судна, их конфиденциальность, доступность, целостность при обеспечение военно-научно-технологического превосходства над потенциальным противником.*

Введение

Среди современных системных категорий и свойств судов, как основного класса объектов морской техники и морской инфраструктуры (ОМТИ), продолжает оставаться и является важнейшим понятие ***живучести судна (ЖС)***, введенное в 1894 г. в теорию и практику судостроения адмиралом С.О. Макаровым.

Регламентированное в том числе наставлениями по борьбе за живучесть кораблей (ВМФ), морских и речных судов (таможенных органов РФ) понятие ЖС определяется сегодня как способность противостоять последствиям аварийных повреждений, возникновению и распространению пожаров, возникновению взрывов и радиационных заражений, сохранять, восстанавливать и поддерживать при этом в достаточной мере свои мореходные качества и обеспечивать безопасность находящихся на его борту людей, сохранность грузов и судового имущества [1]. В общем случае ЖС обеспечивается и определяется (ГОСТ 27.002-2015) следующими его свойствами: непотопляемостью (Н), взрыво-пожаро-радиационной безопасностью (ВПРБ), живучестью технических средств и оружия (ЖТС), защищенностью и подготовленностью экипажа судна к борьбе за ЖС (ЗЭ), устойчивостью системы управления ЖС (УСУ) [2].

1 Алексеев Анатолий Владимирович, доктор технических наук, профессор, профессор кафедры судовой автоматики и измерений Санкт-Петербургского государственного морского технического университета, г. Санкт-Петербург, Россия. E-mail: iapbgks@bk.ru

2 Дригола Владимир Кириллович, кандидат военных наук, старший научный сотрудник Военного учебно-научного центра ВМФ «Военно-морская академия им. Н. Г. Кузнецова», г. Санкт-Петербург, Россия. E-mail: velena.spb@mail.ru

3 Михальчук Андрей Васильевич, кандидат технических наук, доцент кафедры судовой автоматики и измерений Санкт-Петербургского государственного морского технического университета, г. Санкт-Петербург, Россия. E-mail: 335mav@mail.ru

Постановка задачи

Живучесть (survivability) в соответствии с определением профессора Рябинина И. А. рассматривается как способность системы сохранять свойства, необходимые для выполнения заданного назначения при форс-мажорных поражающих воздействиях, не предусмотренных условиями нормальной эксплуатации, т.е. при взрывах, пожарах, затоплениях и прочих факторах, которые сегодня могут и должны быть расширены ***информационными факторами и угрозами живучести корабля, судна (ИФЖ)*** типа:

1. Угрозы несовершенства проектных решений/средств и систем защиты информации (СЗИ), организации, управления и нарушения регламентов комплексной защиты информации (КЗИ), угрозы физических атак и нанесения ущерба судовым информационным ресурсам (ИР) на отчуждаемых и встроенных носителях информации долговременного хранения, на средствах обработки и хранения оперативной информации, на средствах (портах) ввода / вывода информации.
2. Угрозы конфиденциальности информации (неправомерного / несанкционированного доступа, блокирования, утечки, потери, перехвата, съема, копирования, хищения, разглашения, компрометации информации.
3. Угрозы доступности информации вследствие воздействия вредоносных кодов (вирусы, черви, троянские программы, спам, фишинг), DDoS-атак, ….
4. Угрозы целостности информации (модификация данных, деструктивные воздействия / уничтожение / утрата.
5. Антропогенные угрозы (недостаточная квалификация и ошибки операторов, экипажа, инсайдеры, хакерские атаки / групповые атаки, утечка информации от экипажа, социальная инженерия
6. Техногенные угрозы (отказы оборудования и программного обеспечения (уязвимости операционных систем, сетевых протоколов, программных приложений, программные закладки) аварии и аварийные ситуации.
7. Угрозы форс-мажорных обстоятельств / ситуаций (природные катастрофы, затопление, пожары, взрывы, радиационная активность).

В этой связи встает актуальная научно-методическая и организационная задача определения роли и места, прикладной теории обеспечения ***информационной живучести судна (ИЖС***, информационной безопасности судна и ОМТИ в целом) при *обеспечении* ***военно-технологического информационного превосходства*** (ВТПи) над противником в ряду основных факторов, показателей и технологий обеспечения ЖС, ВТП в целом.

Решение поставленной задачи

Живучесть как одно из важнейших свойств корабля, судна развивается и совершенствуется на протяжении всего исторического опыта судостроения и эксплуатации кораблей, судов. В этой связи расширение понятия ЖС с учетом специфики этапа современного технологического развития следует рассматривать как вполне естественное в условиях цифровой трансформации личности, общества, государства на базе интенсивного развития современных информационных технологий.

Введение понятия ИЖС в контексте [1–4] позволяет учитывать ***основные тенденции современного развития кораблей, судов***:

- интеллектуализацию управления за счет совершенствования алгоритмов, автоматизации процессов обоснования проектных решений, поддержки принятия и регистрации решений, визуализации, мониторинга и автоматического контроля их исполнения, использования элементов искусственного интеллекта [2–12];
- усложнение информационно-управляющих и роботизированных систем путем наращивания функционала, интеграции средств и подсистем [2, 3];
- комплексную интеграцию систем управления с соответствующим укрупнением и исключением рабочих мест операторов нижестоящих уровней и контуров управления [3–5];
- переход на дистанционное, распределенное и роботизированное управление отдельными судовыми системами и судном в целом [9–10].

При этом статистика международных инцидентов демонстрирует ***устойчивый рост кибератак на морскую инфраструктуру***. Только за последние три года зафиксировано более 400 значимых киберинцидентов в морском секторе, что на 67 % превышает показатели предыдущего трехлетнего периода [11].

Рис. 1. Возможные варианты судовых информационных инцидентов

Рис. 2. TOP-21 событий и фактов противоборства в информационной сфере

С учетом возрастания политической нестабильности в ряде регионов перспективными инцидентами в части воздействия на морские суда могут быть (рис. 1) действия по блокировке (отключению), перехвату управления судовыми системами, блокировка обмена данными и пр.

Реализация указанных инцидентов будет направлена на нанесение ущерба путем создания аварийных ситуаций, перетекающих в аварии различного характера и аварийные ситуации.

Международными и государственными стандартами определены системные требования к информационной безопасности судна, однако, инциденты, связанные с воздействием на информационные системы, сегодня не трактуются как аварийные ситуации.

По мнению авторов, с учетом возможных последствий нарушения информационной безопасности (ИБ) судна, ***все инциденты ИБ следует рассматривать как аварийные ситуации***, а их своевременное предотвращение и безусловное устранение должно осуществляться в рамках такого важного элемента борьбы за живучесть как информационная живучесть судна.

Обуславливается это тем, что наносимый при этом ущерб, как показывает анализ исторических примеров обеспечения информационного превосходства в информационной сфере (рис. 2 [10]), может ***существенно превосходить*** стоимость самих судов и грузов, причем, во много раз, включая человеческие жертвы.

В обеспечение развития прикладной теории ИЖС ***понятие ИЖС*** в контексте [2, 3, 12] предлагается рассматривать как способность корабля, судна *обеспечивать постоянную готовность к действиям* по прямому назначению, способность сохранять и восстанавливать свои свойства *при* ***информационных инцидентах*** **(ИнИ)**, а также *готовность противостоять* последствиям ИнИ, воздействию атак, *сохранять и восстанавливать* при этом в достаточной мере управляемость судна и *обеспечивать безопасность* находящихся на борту судна пассажиров и экипажа, сохранность грузов и судового имущества.

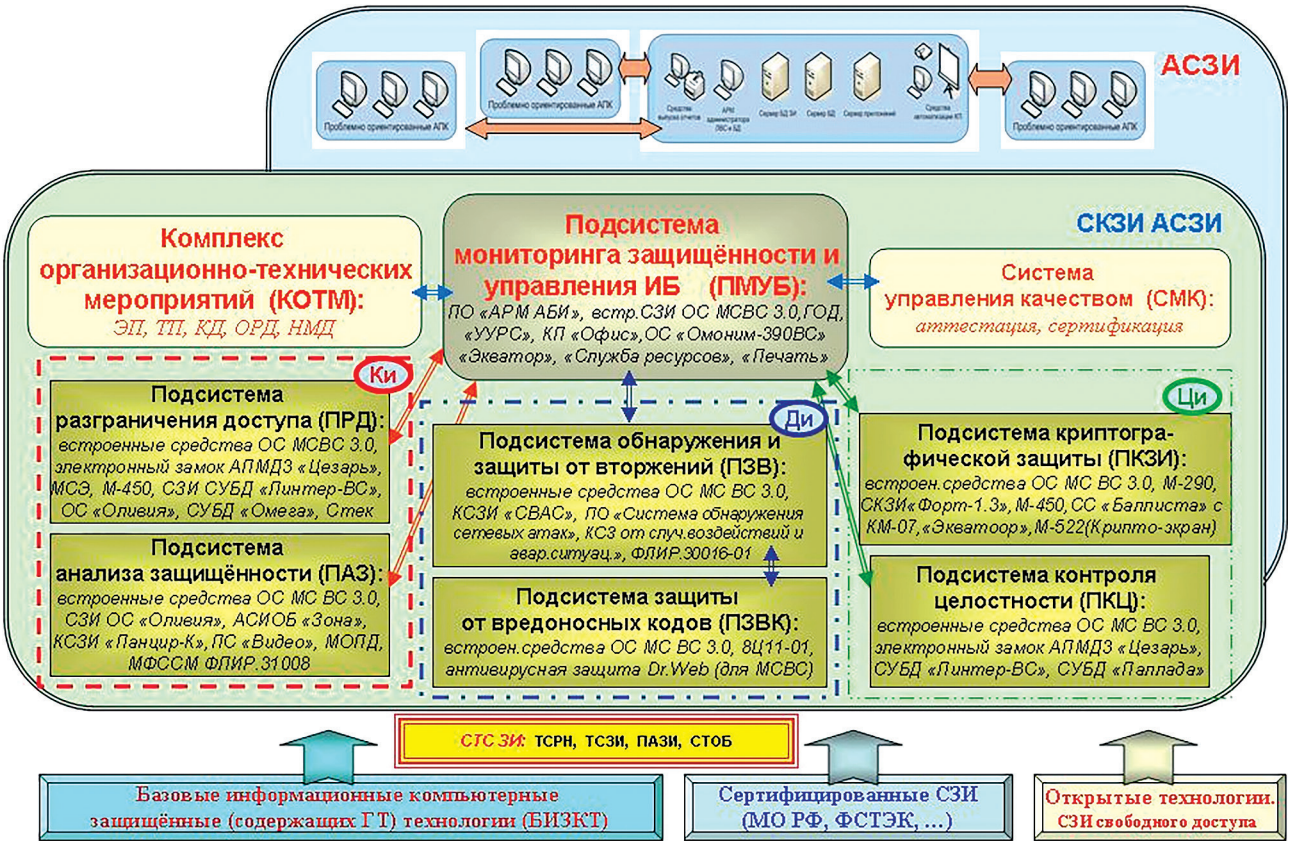

Рис. 3. Типовая архитектура и технологии СКЗИ в составе АСЗИ типового ОМТИ с наиболее характерными представителями подсистем защиты информации

Под ***борьбой за ИЖС*** предлагается понимать своевременные энергичные, инициативные и квалифицированные действия его экипажа *по обеспечению*:

- проектного качества и эффективности эксплуатации ***системы комплексной защиты информации*** **(СКЗИ)** в составе судовой ***автоматизированной системы в защищенном исполнении*** **(АСЗИ)**, типовая структурная модель которой приведена на рис. 3 [8–10];
- конфиденциальности, доступности, целостности ***информационных ресурсов*** **(ИР)** судна и ИБ в целом;
  предупреждению возникновения и неуправляемого развития ИнИ, а также – по поддержанию в постоянной готовности к действию ***информационно-коммуникационных*** **(ИКС)** и ***информационно-управляющих средств и систем*** судна **(ИУС)**.

Требования к организации обеспечения информационной живучести судна

Борьба за ИЖС должна быть отработанной на тренировках и учениях обязанностью всех членов экипажа, а также регламентироваться Уставом службы на судах, Наставлением по борьбе за живучесть судов (НБЖС, ЦНИИМФ, 2004) и документами по Системе управления безопасностью (СУБ) судна, требованиями Международного кодекса по управлению безопасностью (МКУБ) [2, 3].

Отработка организации борьбы за ИЖС должна быть составной частью повседневной службы на судне и направлена на рациональное распределение членов экипажа в интересах эффективного использования стационарных и мобильных ИКС и ИУС при ИнИ, воздействии атак и вторжений как в портах, включая иностранные, так и на переходе морем.

ИЖС включает в себя ряд *организационно-технических мероприятий* по следующим направлениям:

- готовность СКЗИ в составе судовых АСЗИ к действиям по прямому назначению с обеспечением научно-технологического и военно-технологического превосходства по критерию $\text{ВТП} = Q / Q_{\text{П}}$, где Q – агрегированный (обобщенный, интегрированный, системный, адмиральский) показатель проектного качества/эффективности эксплуатации СКЗИ в составе АСЗИ, а $Q_{\text{П}}$ – аналогичный показатель для СКЗИ потенциального противника с прогнозируемыми по данным разведки и военно-научной экспертизы характеристиками, оцениваемые по алгоритмам, приведенным в [8–10];
- своевременное выявление уязвимостей, угроз и информационных воздействий (ИВ) с их классификацией, идентификацией и оценкой возможностей по нанесению ущерба;
- сохранение и восстановление функциональных свойств систем (комплексов) судна за счет отработанных и слаженных действий экипажа по эффективному использованию СКЗИ;
- устранение последствий информационных инцидентов и их всевозможных проявлений;
- военно-научный анализ и прогнозирование возможных аварий по результатам реализации киберугроз, в том числе представленных на рис. 4.

Рис. 4. Типовой характер возможных аварий по результатам реализации киберугроз

Структура

В этой связи особое внимание при разработке и эксплуатации объектов морской техники и инфраструктуры сегодня следует уделять СКЗИ, как одному из ключевых элементов АСЗИ, в состав которой согласно рис. 3, как правило, входят следующие подсистемы [2, 3]:

1. **Подсистема мониторинга, прогнозирования, контроля и управления ИЖС (ПМУБ)**, реализуемая сегодня средствами защиты информации корабля, судна типа 4789.ИАСЗИ ГК, 4451.DATAPK, 2720.Dallas Lock 8.0-K (цифры в сокращенном название средств означают номер сертификата в Государственном реестре сертифицированных средств ФСТЭК РФ).

2. **Подсистема разграничения доступа к информационным ресурсам (ИР) корабля, судна (ПРД)**, реализуемая сегодня средствами типа 4795.ПО «Реестр РВК», 3474.ARMlock, 4792.ПО СА СЦ ЭП.

3. **Подсистема криптографической защиты ИР (ПКЗИ)** корабля, судна, реализуемые сегодня средствами типа 4268. Континент-СОВ.4, 4125.АПК «VPN/FW ЗАСТАВА-150», 4145.АПКШ Континент.3.9.

4. **Подсистема обнаружения и защиты от вторжений в ИР (ПЗВ)** корабля, судна, реализуемая сегодня средствами защиты информации от вторжений типа 4042.СОПВ PosTechnNetAttDiscovery, 4759.Реализация ГОЗ, 3597.ЭЗ «Витязь 2.2».

5. **Подсистема оценки, мониторинга, анализа и контроля защищенности ИР корабля, судна (ПАЗ)**, реализуемая сегодня средствами типа 4451.ПК ОМ ИБиЗ «DATAPK», 4159.СМИБ SIEM, 4574.Security Vision ЦИМУ ИБ.

6. **Подсистема контроля целостности ИР корабля в составе соединения (ПКЦ)**, реализуемая сегодня средствами типа 2557.ОС СН Astra Linux Special Edition, 4742.ГосКонтроль, 4293.АИТ «АИСТ-С».

7. **Подсистема защиты ИР корабля, судна от вредоносных (вирусов, спама, фишинга и т.п.) кодов (ПЗВК)**, реализуемая сегодня средствами типа 3676.Kaspersky Security 9.0 Exchange Servers, 2840.Kaspersky Security 8.0, 4604.Positive Technologies Sandbox.

8. **Комплекс организационно-технических мероприятий по обеспечению ИЖС корабля, судна (КОТМ)**, по управлению проектным качеством и эффективностью (мерой практической реализации проектного качества) подсистемы ИЖС, включая мероприятия по контролю, оценке технической готовности судна [9–10], реализуемые сегодня регламентами типа «Положение о Службе ИБ НИЦ СПбЭТУ», «Положение о КИС АО «Концерн «МПО «ГидроПрибор», «Политика в области ИБ № ПЗ-11.01 П-01 в.2.00», РосНефть [10].

9. **Система менеджмента качества обеспечения ИБ корабля, судна (СМИБ)**, реализуемая сегодня регламентами и средствами типа «Программный комплекс мониторинга качества вооружений, военной и специальной техники «ПК СМК ВВСТ», «Русский Регистр. Системы МК ИБ», «Система менеджмента качества. Стандарт организации. СТО 6.5-1. Политика информационной безопасности».

При этом ***типовыми моделями тактических уязвимостей*** (существующих дефектов построения, функционирования и использования АСЗИ в части ИЖС) и соответствующих ***информационно-тактических угроз ИЖК*** (ИТУ, потенциальных событий по реализации уязвимостей, нарушению регламентов обработки информации) следует считать:

ИТУ-1: Возможность потери военно-технологического превосходства над потенциальным противником в следствие **негативного влияния субъективных свойств членов экипажа** (**ЧФ**, «человеческий фактор»). Угроза ЧФ может быть обусловлена недостаточной подготовкой (знаниями, навыками, способностями, опытом) и соответствующими ошибками эксплуатации, ограниченной мотивируемостью (безинициативностью, безответственностью) и нелояльностью (злоупотреблением должностным положением) членов экипажа и т.п.

ИТУ-2: Киберсетевые воздействия (КСВ), осуществляемые установленными/неустановленными субъектами информационного взаимодействия по информационно-коммуникационным каналам. Угроза КСВ реализуется с использованием средств разведки (включая технический шпионаж), средств противодействия, формирования напряженной и ложной обстановки, провоцирования экипажа на нерациональные действия, шантажа, заражения вредоносными кодами с деструктивными функциями, спама и т.п.

ИТУ-3: Технологические угрозы (ТУгр), обусловленные спецификой программно-аппаратных средств и процессов (включая «зависания» программного обеспечения, потеря целостности и доступности данных).

Рис. 5. Комплексная математическая модель оценки и оптимизации ИЖС

ИТУ-4: Угрозы рефлексивного воздействия (УРВ), обусловленные формированием установленными и/или неустановленными субъектами информационного взаимодействия «целевой» обстановки в информационной среде в интересах рефлексивного управления членами экипажа, кораблем и соединением кораблей в целом.

ИТУ-5: Другие возможные и ранее не идентифицированные угрозы (**ДрУ**), обусловленные интенсивным развитием информационных технологий, включая искусственный интеллект, роботизацию управления.

В обеспечение прикладной теории ИЖС модельное представление процессов и качества создаваемых систем обеспечения ИЖС и управления мероприятиями по ее обеспечению, по нашему мнению, прежде всего целесообразно использовать **Полимодельный квалиметрический метод системной оптимизации** [2, 3] и соответствующую ***аналитическую модель***, приведенную на рис. 5 [10].

Реализация прикладной теории

Парадигма обеспечения ИЖС, по мнению авторов, должна включать системообразующую идею проектного обоснования, оптимизации, мониторинга и прогнозирования свойств **комплексных судовых систем** защиты информации с учетом всего множества системных критериев и показателей проектного качества. В настоящее время группой специалистов СПбГМТУ разработан и используется в исследованиях вопросов ИЖС Роботизированный проектный комплекс (РПК) «КАСОР-24» [8–10], экранная форма приведена на рис. 6.

Преимуществом РПК является возможность моделирования и исследования свойств комплексных систем обеспечения ИЖС с цифровой оценкой, как показано на рис. 6 агрегированного показателя качества СКЗИ (значение АПК = 80,5 %) и соответствующих значений конфиденциальности ИР (К = 77,9 %), доступности (Д = 80,9 %), целостности (Ц = 82,6 %). А также реализованы возможности технологии цифрового двойника СКЗИ, как цифровой модели СКЗИ в составе АСЗИ с режимами функционирования «1.ЦП» (цифровой паспорт), «2.ЦМ» (цифровая модель, с вводом сценарных исходных данных), «3.ЦТ» (цифровая тень, с вводом исходных данных с реального объекта типа СКЗИ).

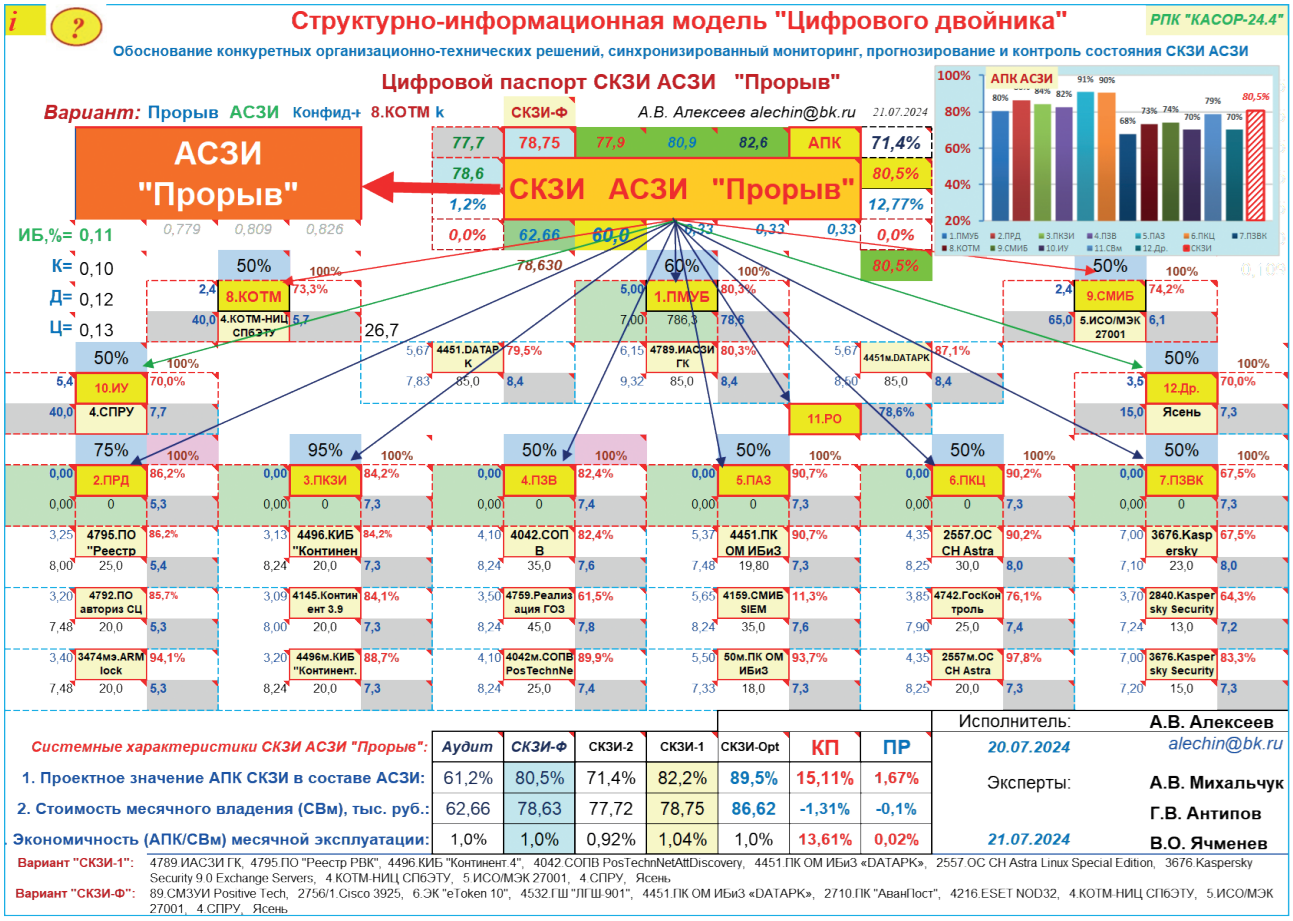

Рис. 6. Структурно-информационная модель «Цифрового двойника» (экранная форма РПК)

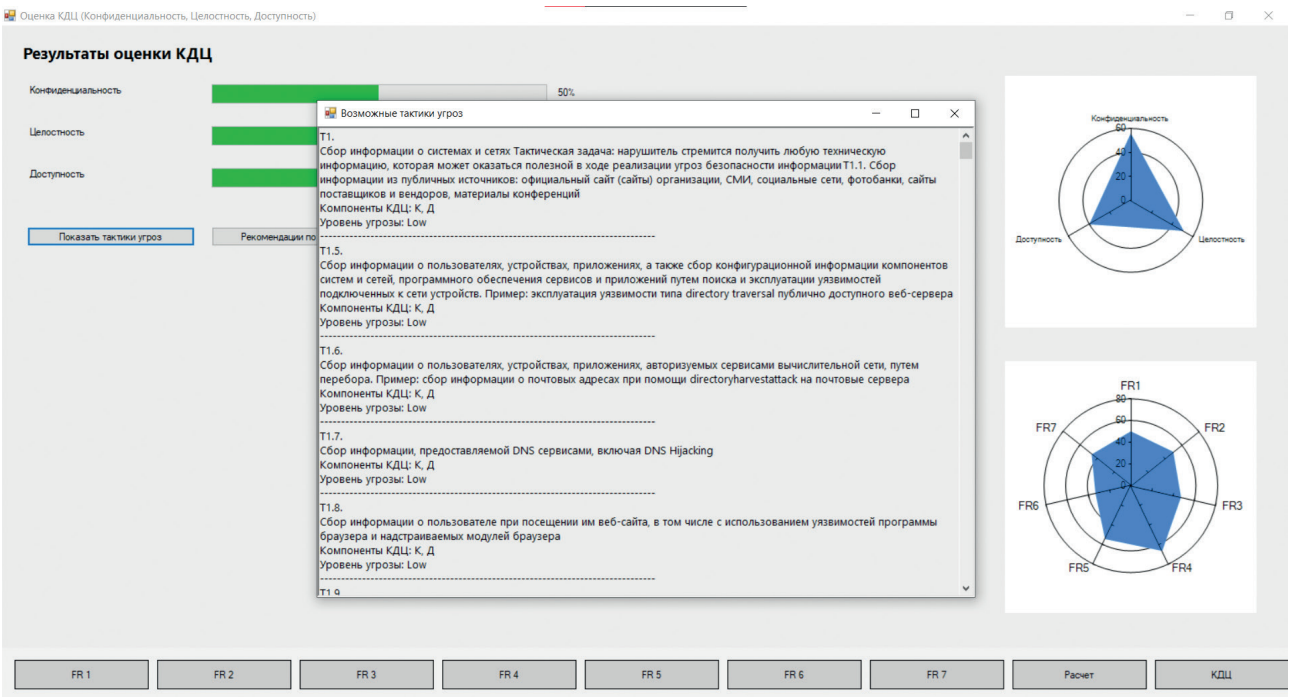

Рис. 7. Пример экранной формы ПК ИЖС (в части контроля ФТ и СТ)

Апробация

В рамках научно-исследовательских и выпускных квалификационных работ уже сегодня студентами СПбГМТУ [8] РПК используется при обосновании мер КЗИ и разрабатываются программные комплексы цифровой оценки проектного качества ИЖС, ожидаемой эффективности частных мероприятий по обеспечению ИЖС, например, при контроле реализации названных в РМРС «фундаментальными требованиями» (ФТ, конфиденциальности, доступности, целостности) и системных требований (СТ, комплексной защиты информации/информационной безопасности, военно-технологического превосходства) корабля, судна (рис. 7) с учетом соответствующих тактик, используемых для построения сценариев реализации угроз безопасности информации корабля, судна.

Заключение

Проведенные исследования по разработке прикладной теории ИЖС в обеспечение научно-технологического превосходства в информационной сфере, приведенные результаты анализа и систематизации вопросов формирования понятия «информационная живучесть корабля, судна» (ИЖС) и практические аспекты решения системной проблемы обеспечения информационного превосходства в управлении ИЖС на базе анализа технологических решений максимизации ИЖС типовых объектов морской техники и морской инфраструктуры показали, что:

- сегодня первостепенное значение имеют вопросы **системного управления ЖС** по традиционным критериям оперативности, достоверности используемых данных, устойчивости, скрытности, непрерывности, ресурсной обеспеченности с соответствующими частными показателями качества типа работное время решения комплекса функциональных задач, адекватность используемых данных;
- при необходимости одновременной оценки, мониторинга и контроля критически важных показателей комплексной защищенности ИР корабля, их соединений, судна в составе флота, конфиденциальности, доступности, целостности информационных ресурсов;
- а также необходимости перехода к метасистемному цифровому анализу и синтезу киберустойчивости СКЗИ в составе АСЗИ корабля, судна, рефлексивности и ментальности управления, его имитоскрытности, эргогномичности.

Показано, что обеспечение ИЖС ОМТИ в условиях интенсивного информационно-технологического развития является *сложнейшей и высоко востребованной задачей* целеполагания, роботизированного управления с использованием технологий полимодельного мониторинга, анализа, синтеза и оптимизации управленческих решений с мониторингом контроля их реализации по технологии цифровых двойников, адаптивной корректировки, верификации и валидного контроля.

Приведенные теоретико-прикладные положения системного анализа аспектов ИЖС, систематизации угроз ИБ, разработанных вариантов их модельного представления позволяют сформулировать системные требования по ИЖС и определить наиболее перспективные пути реализации этих требований в интересах обеспечения радиоэлектронного и информационного превосходства в информационной сфере, живучести ОМТИ в целом на базе приведенных моделей и реализующих их программных комплексов анализа, синтеза и оптимизации ИЖС.

Анализ понятийного аппарата, проблем и технологий реализации ИЖС в свете современных требований и регламентов обеспечения безопасности мореплавания указывает на *особую актуальность* решения сравнительно новой организационно-технической и военно-научной **задачи гарантированного обеспечения информационной живучести корабля, судна** как одного из критических сегментов системы управления безопасностью и живучестью судна.

Литература

1. Бондаренко Д. Л., Жбанов И. Л. Анализ существующих подходов к трактовке понятия «живучесть» информационно-управляющей подсистемы асу специального назначения / Актуальные вопросы технических наук, 2017, с. 100–104.
2. Алексеев А. В. Информационная живучесть судна: понятие, проблемы, технологии / Региональная информатика и информационная безопасность. Сборник трудов. Выпуск 7 / СПОИСУ. – СПб., 2019, с. 345–348.
3. Алексеев А. В. Информационная живучесть управления: теория и практика обеспечения информационного превосходства / Информационная безопасность регионов России (ИБРР-2023). XIII Санкт-Петербургская межрегиональная конференция. Санкт-Петербург, 25–27 октября 2023 г.: Материалы конференции / СПОИСУ. – СПб, 2023, с. 224–226.
4. Информационные технологии в судостроении: существующие системы, сферы и возможности их использования [Электронный ресурс] URL: https://uchimsya.com/a/qC363Pr9 (дата обращения 24.05.2023).
5. Анфилатов В. С., Емельянов А. А., Кукушкин А. А. Системный анализ в управлении. – М.: Финансы и статистика, 2002.
6. Алексеев А. В., Смольников А. В., Сус Г. Н., Ушакова Н. П. Когнитивные технологии системы поддержки принятия решений и управления борьбой за живучесть корабля, судна // Системы управления и обработки информации: научн.-техн. сб. /АО «Концерн «НПО «Аврора». СПб, 2019. Вып. 3(46), с. 18–27.
7. Алексеев А. В., Кузнецов В. В., Согонов С. А., Мусатенко Р. И., Тычинин И. Ю., Балицкая К. В. Обоснование системы критериев оценки информационной живучести судна / Региональная информатика и информационная безопасность. Сборник трудов. Выпуск 7 / СПОИСУ. – СПб., 2019, с. 353–358.
8. Алексеев А. В., Кузнецов В. В., Согонов С. А., Мусатенко Р. И., Тычинин И. Ю., Балицкая К. В. Система критериев оценки информационной живучести судна / Информационная безопасность регионов России (ИБРР-2019). – СПб., 2019, с. 329-330.
9. Бобрович В. Ю., Алексеев А. В., Антипов В. В., Смольников А. В. Информационная живучесть корабля: угрозы, модель, системные требования, пути реализации / Информационная безопасность регионов России (ИБРР – 2021). – СПб., 2021, с. 265–267.
10. Алексеев А. В. Модель и программный комплекс цифровой трансформации кибербезопасности / Вопросы обеспечения безопасности в киберпространстве: материалы Всероссийской НТК – Махачкала: ДГТУ, 2022 г. – 387 с. с. 251–255.
11. Кибербезопасность в 2023-2024 гг.: тренды и прогнозы. URL: https://ptsecurity.com/ru-ru/research/analytics/kiberbezopasnost-v-2023-2024-gg-trendy-i-prognozy-chast-pyataya/ (дата обращения: 25.05.2025).
12. Бондырев В. Е., Дригола В. К., Устинович Е. С., Алексеев А. В. Применение искусственного интеллекта в ВМФ при разработке и принятии управленческих решений / Региональная информатика и информационная безопасность. Сборник трудов. Выпуск 13 / СПОИСУ. – СПб., 2024, 415–420.

INFORMATION SURVIVABILITY OF A SHIP: AN APPLIED THEORY OF ENSURING MILITARY AND TECHNOLOGICAL SUPERIORITY

Alekseev A. V.[4], Drigola V. K.[5], Mikhalchuk A. V.[6]

Keywords: *goal setting; model; ship survivability; monitoring; valid control; vulnerability; threat; confidentiality; accessibility; integrity.*

4 Anatoly V. Alekseev, Dr.Sc. of Technical Sciences, Professor, Professor of the Department of Ship Automation and Measurements, St. Petersburg State Marine Technical University, St. Petersburg, Russia. E-mail: iapbgks@bk.ru

5 Vladimir K. Drigola, Ph.D. of Military Sciences, Senior Researcher of the Military Training and Research Center of the Navy «Naval Academy named after N. G. Kuznetsov», St. Petersburg, Russia. E-mail: velena.spb@mail.ru

6 Andrey V. Mikhalchuk, Ph.D. of Technical Sciences, Associate Professor of the Department of Ship Automation and Measurements, St. Petersburg State Marine Technical University, St. Petersburg, Russia. E-mail: 335mav@mail.ru

Abstract

The purpose of the work *is to substantiate the need to expand the concept of survivability of a ship and to develop the basic principles of the applied theory of information survivability of a ship, vessel (and LC). to ensure military and technological superiority.*

Research method: *systematization of data from the analysis, synthesis and optimization of IHS based on a qualimetric assessment of the aggregated indicator of the design quality and operational efficiency of the integrated information protection system (ICSI) as part of an automated information processing system in a secure design (ASSI).*

The results of the study *include typical structural models of residential housing, the SCSI, a verbal model of residential housing vulnerabilities and threats, a complex mathematical model for assessing and optimizing residential housing, a structural information model of the digital twin of the SCSI and an example of software implementation in the variant of the KASOR-24.4 robotic design complex, and the results of the formation of the applied theory of residential housing.*

The scientific novelty and practical value *of the research consists in the generalization and development of applied theoretical aspects of the introduction and model representation of the analysis, synthesis and optimization of a new concept for the shipbuilding industry, «information survivability of a ship». This made it possible to expand the survivability category of the vessel and for the first time quantify/digitalize such relevant factors of information technology development today as the security of the ship's information resources, their confidentiality, accessibility, integrity, while ensuring military, scientific and technological superiority over a potential adversary.*

References

1. Bondarenko D. L., Zhbanov I. L. Analiz sushhestvujushhih podhodov k traktovke ponjatija «zhivuchest'» informacionno-upravljajushhej podsistemy asu special'nogo naznachenija / Aktual'nye voprosy tehnicheskih nauk, 2017, s. 100–104.
2. Alekseev A. V. Informacionnaja zhivuchest' sudna: ponjatie, problemy, tehnologii / Regional'naja informatika i informacionnaja bezopasnost'. Sbornik trudov. Vypusk 7 / SPOISU. – SPb., 2019, s. 345 – 348.
3. Alekseev A. V. Informacionnaja zhivuchest' upravlenija: teorija i praktika obespechenija informacionnogo prevoshodstva / Informacionnaja bezopasnost' regionov Rossii (IBRR – 2023). XIII Sankt-Peterburgskaja mezhregional'naja konferencija. Sankt-Peterburg, 25–27 oktjabrja 2023 g.: Materialy konferencii / SPOISU. – SPb, 2023, s. 224–226.
4. Informacionnye tehnologii v sudostroenii: sushhestvujushhie sistemy, sfery i vozmozhnosti ih ispol'zovanija [Jelektronnyj resurs] URL: https://uchimsya.com/a/qC363Pr9 (data obrashhenija 24.05.2023).
5. Anfilatov V. S., Emel'janov A. A., Kukushkin A. A. Sistemnyj analiz v upravlenii. – M.: Finansy i statistika, 2002.
6. Alekseev A. V., Smol'nikov A. V., Sus G. N., Ushakova N. P. Kognitivnye tehnologii sistemy podderzhki prinjatija reshenij i upravlenija bor'boj za zhivuchest' korablja, sudna //Sistemy upravlenija i obrabotki informacii: nauchn.-tehn. sb. / AO «Koncern «NPO «Avrora». SPb, 2019. Vyp. 3(46), s. 18–27.
7. Alekseev A. V., Kuznecov V. V., Sogonov S. A., Musatenko R. I., Tychinin I. Ju., Balickaja K. V. Obosnovanie sistemy kriteriev ocenki informacionnoj zhivuchesti sudna / Regional'naja informatika i informacionnaja bezopasnost'. Sbornik trudov. Vypusk 7 / SPOISU. – SPb., 2019, s. 353–358.
8. Alekseev A. V., Kuznecov V. V., Sogonov S. A., Musatenko R. I., Tychinin I. Ju., Balickaja K. V. Sistema kriteriev ocenki informacionnoj zhivuchesti sudna / Informacionnaja bezopasnost' regionov Rossii (IBRR – 2019). – SPb., 2019, s. 329-330.
9. Bobrovich V. Ju., Alekseev A. V., Antipov V. V., Smol'nikov A. V. Informacionnaja zhivuchest' korablja: ugrozy, model', sistemnye trebovanija, puti realizacii / Informacionnaja bezopasnost' regionov Rossii (IBRR – 2021). – SPb., 2021, s. 265–267.
10. Alekseev A. V. Model' i programmnyj kompleks cifrovoj transformacii kiberbezopasnosti / Voprosy obespechenija bezopasnosti v kiberprostranstve: materialy Vserossijskoj NTK – Mahachkala: DGTU, 2022 g. – 387 s. s. 251–255.
11. Kiberbezopasnost' v 2023-2024 gg.: trendy i prognozy. URL: https://ptsecurity.com/ru-ru/research/analytics/kiberbezopasnost-v-2023-2024-gg-trendy-i-prognozy-chast-pyataya/ (data obrashhenija: 25.05.2025).
12. Bondyrev V. E., Drigola V. K., Ustinovich E. S., Alekseev A.V. Primenenie iskusstvennogo intellekta v VMF pri razrabotke i prinjatii upravlencheskih reshenij / Regional'naja informatika i informacionnaja bezopasnost'. Sbornik trudov. Vypusk 13 / SPOISU. – SPb., 2024, 415–420.

TELECOMMUNICATIONS and COMMUNICATIONS

SCIENTIFIC PEER-REVIEWED JOURNAL
№ 4 (07) 2025
Published 6 times a year

The journal is registered by the Federal Servicefor Supervision of Communications, Information Technology and Mass Communications.
Registration Certificate
PI № FS77-88069 от 16.08.2024

Founder and publisher
Federal State Budgetary Institution
«16 Central Research and Testing Institute»
of the Ministry of Defense
of the Russian Federation

Signed to the press on 15/08/2025.
The total circulation is 120 copies. The price is free.

Postal address: 1st Rupasovsky lane, 1, 141006, Mytishchi, Moscow region, Russia.

E-mail: editor.tis@yandex.ru. Tel.: +7 (995) 153-43-88.

The requirements for the manuscripts are posted on the website: **https://telemil.ru/**

CONTENTS