Министерство образования Республики Беларусь

Учреждение образования
«Белорусский государственный университет
информатики и радиоэлектроники»

Военный факультет

ИННОВАЦИОННЫЕ ТЕХНОЛОГИИ В ОБРАЗОВАТЕЛЬНОМ ПРОЦЕССЕ

**62-я научная конференция
аспирантов, магистрантов и студентов
учреждения образования «Белорусский государственный
университет информатики и радиоэлектроники»**

Электронный сборник тезисов (докладов)

15 апреля 2026 года
Минск, БГУИР

УДК 004:378
ББК 32.81+74.48
И66

Инновационные технологии в образовательном процессе: материалы 62-ой научной конференции аспирантов, магистрантов и студентов учреждения образования «Белорусский государственный университет информатики и радиоэлектроники», 15 апреля 2026 г., Минск, Беларусь. – Минск : БГУИР, 2026. – 116 с.; ил.

В сборнике опубликованы материалы докладов, представленных на 62-й научной конференции аспирантов, магистрантов и студентов БГУИР. Материалы одобрены оргкомитетом и публикуются в авторской редакции.

Для научных и инженерно-технических работников, преподавателей, аспирантов, магистрантов и студентов вузов.

УДК 355.4

ТАКТИКА ПСИХОЛОГИЧЕСКОГО ВОЗДЕЙСТВИЯ В УСЛОВИЯХ СПЕЦИАЛЬНОЙ ВОЕННОЙ ОПЕРАЦИИ

Бурштын Е.А. студент гр.434501

Белорусский государственный университет информатики и радиоэлектроники г. Минск, Республика Беларусь

Вербицкий Г.И. – магистр управления

Аннотация. В работе рассматриваются тактические приемы и методы психологического воздействия, применяемые в ходе специальной военной операции. Анализируются основные направления информационно-психологического противоборства: работа с личным составом противника, воздействие на гражданское население, информационное сопровождение боевых действий. Выявляются новые формы психологического воздействия, обусловленные широким применением беспилотных летательных аппаратов, социальных сетей и мессенджеров. Обосновывается необходимость интеграции психологических операций в единую систему управления войсками.

Ключевые слова. Психологическое воздействие, информационно-психологическое противоборство, специальная военная операция, тактика, пропаганда, социальные сети, беспилотные летательные аппараты, морально-психологическое состояние, противодействие дезинформации.

Психологическое воздействие в ходе специальной военной операции (далее − СВО) приобрело качественно новые формы и масштабы, став неотъемлемым элементом общевойскового боя наряду с огневым поражением и радиоэлектронной борьбой. Опыт ведения боевых действий показал, что успех операций во многом определяется способностью влиять на морально-психологическое состояние личного состава противника, гражданского населения и собственных войск. Тактика психологического воздействия в условиях СВО характеризуется синтезом традиционных методов (листовки, радиопередачи, громкоговорящие установки) и инновационных технологий, основанных на применении беспилотных летательных аппаратов, социальных сетей и мессенджеров.

Анализ боевых действий позволяет выделить три основных направления тактики психологического воздействия, применявшихся в ходе СВО. Первое направление − работа с личным составом противника, направленная на снижение боевого духа, побуждение к сдаче в плен или отказу от выполнения боевых задач. Второе направление − воздействие на гражданское население на освобождаемых территориях с целью формирования лояльного отношения к российским войскам и противодействия информационным вбросам противника. Третье направление − информационно-психологическое обеспечение собственных войск, включающее поддержание высокого морально-психологического состояния, противодействие дезинформации и оперативное доведение до личного состава объективной информации об обстановке [1].

Наиболее значимой тактической инновацией в сфере психологического воздействия стало массовое применение беспилотных летательных аппаратов (БЛА) для сброса агитационных материалов и вещания на позиции противника. В отличие от традиционных методов распространения листовок (артиллерийские снаряды, авиация), использование БЛА позволяет осуществлять адресное психологическое воздействие с высокой точностью и минимальным риском для личного состава. Сброс листовок с FPV-дронов и мультироторных БЛА применялся как для информирования личного состава противника о возможности сдачи в плен (с указанием частот радиосвязи и координат пунктов приема), так и для деморализации путем распространения материалов, содержащих информацию о потерях и неудачах.

Одновременно с этим БЛА стали эффективным средством вещания на позиции противника. Установка на дроны громкоговорящих устройств позволяет осуществлять психологическое воздействие в реальном времени, обращаясь к конкретным подразделениям или отдельным военнослужащим. Такая форма воздействия особенно эффективна в условиях позиционного противостояния, когда противник находится на ограниченном расстоянии. Практика показала, что регулярное вещание с использованием БЛА способно существенно снизить боевой дух личного состава противника, особенно в условиях недостаточного снабжения и высоких потерь.

Значительную роль в тактике психологического воздействия играют социальные сети и мессенджеры (Telegram, Viber, WhatsApp, Twitter). В условиях СВО эти платформы стали основным каналом распространения информации как для военнослужащих, так и для гражданского населения. Противоборствующие стороны активно используют телеграм-каналы для ведения информационно-психологических операций, включающих распространение видеоматериалов с результатов боевых действий (часто с элементами манипуляции), дезинформацию о потерях и передвижении войск, а также прямые обращения к личному составу противника. Особенностью данного направления

является высокая скорость распространения информации и возможность таргетированного воздействия на конкретные аудитории [2].

Важным элементом тактики психологического воздействия стала работа с военнопленными и их последующее использование в информационных кампаниях. Видеообращения пленных, в которых они призывают сослуживцев прекратить сопротивление и сдаться, активно распространяются через мессенджеры и телеграм-каналы. Такая практика, с одной стороны, выполняет функцию информирования личного состава противника о гуманном отношении к пленным, а с другой − оказывает деморализующее воздействие, демонстрируя неизбежность поражения и бесперспективность дальнейшего сопротивления.

Параллельно с воздействием на противника осуществляется активная работа с гражданским населением на освобождаемых территориях. В рамках этой работы применяются как традиционные методы (раздача гуманитарной помощи с одновременным распространением агитационных материалов, работа полевых домов культуры), так и инновационные подходы, основанные на использовании мобильных сетей и социальных платформ. Создание локальных телеграм-каналов, информирующих о восстановлении инфраструктуры, выплатах и мерах поддержки, позволяет формировать позитивное восприятие российских войск и противодействовать дезинформации, распространяемой противником.

В таблице 1 представлен сравнительный анализ основных методов психологического воздействия, применявшихся в ходе СВО, с выделением традиционных и инновационных подходов.

Таблица 1 – Основные методы психологического воздействия.

Направление воздействия	Традиционные методы	Инновационные методы (с учетом опыта СВО)
Воздействие на личный состав противника	Радиопередачи, листовки (авиация, артиллерия), громкоговорящие установки	Сброс листовок с БЛА, вещание с БЛА, таргетированные рассылки в мессенджерах, видеообращения пленных
Воздействие на гражданское население	Распространение листовок, работа агитаторов, радиовещание	Телеграм-каналы, социальные сети, мобильные приложения, адресная работа через мессенджеры
Информационное обеспечение собственных войск	Политинформация, боевые листки, радиопередачи	Закрытые телеграм-каналы, чат-боты для информирования, оперативное доведение данных через мессенджеры
Противодействие дезинформации	Опровержения через официальные каналы	Мониторинг социальных сетей, оперативные разъяснения в мессенджерах, создание альтернативных информационных каналов

Опыт СВО показал, что эффективность психологического воздействия напрямую зависит от его интеграции с другими видами боевого обеспечения. В ходе тренировок, проводившихся в Южном военном округе в рамках единого дня огня, отрабатывалась не только передача координат целей на носители высокоточного оружия, но и координация информационно-психологических операций с огневым поражением. Разведчики соединений специального назначения, используя комплексы разведки, управления и связи КРУС «Стрелец», передавали данные о выявленных объектах, которые могли стать целями как для огневого поражения, так и для психологического воздействия. Управление информационно-психологическими операциями организовывалось с подвижных полевых пунктов управления, что позволяло оперативно реагировать на изменение обстановки [3].

В ходе указанных мероприятий, объединивших более ста носителей ракетного вооружения сухопутных, авиационных и морских соединений, было выполнено свыше 400 огневых задач, а также проведен комплекс информационно-психологических акций, направленных на деморализацию условного противника и информирование гражданского населения. К мероприятиям привлекалось более 5 тыс. военнослужащих, включая специалистов по информационно-психологическому противоборству, и задействовано около 2 тыс. единиц техники, в том числе средства распространения агитационных материалов. Разведчики задействовали более 20 беспилотных летательных аппаратов, часть из которых была оснащена оборудованием для сброса листовок и вещания. Данный опыт подтвердил необходимость создания единой системы управления, объединяющей огневое поражение, радиоэлектронную борьбу и психологическое воздействие.

Особое значение в ходе апробированной методики приобрела синхронизация информационно-психологических акций с режимами радиоэлектронной борьбы. Опыт показал, что эффективность воздействия на личный состав условного противника многократно возрастает в периоды временного подавления его каналов связи и навигации. В рамках тренировок в Южном военном округе отрабатывалась последовательность: на первом этапе средствами РЭБ блокировались коммуникации обороняющегося, лишая его возможности получать подтверждение приказов и запрашивать подкрепление; на втором этапе, на фоне созданного информационного вакуума, осуществлялось целенаправленное доведение аудиовизуальных материалов через громкоговорящие установки и сбрасываемые с БЛА носители. Такой подход нарушал систему управления противника на тактическом уровне и способствовал росту дезертирства и снижению сопротивляемости штурмовым группам, действовавшим на направлении главного удара.

Кроме того, полученный в ходе мероприятий опыт позволил сформулировать требования к перспективным средствам ведения информационно-психологической борьбы. Была подтверждена необходимость перехода от эпизодического применения агитационных материалов к созданию контуров постоянного психологического давления вдоль всей линии боевого соприкосновения. Для этого в состав разведывательно-огневых контуров предлагается включать специализированные беспилотные комплексы, способные осуществлять ретрансляцию аудиосигналов на тактические частоты противника, а также средства дистанционного минирования с агитационными вкладышами. Интеграция психологического воздействия в единое информационное пространство наряду с огневым поражением и радиоэлектронной борьбой, по оценке командования, позволяет сократить время перехода, обороняющегося от организованного сопротивления к хаотичным действиям и снизить потери наступающих подразделений при прорыве эшелонированной обороны.

Таким образом, тактика психологического воздействия в условиях специальной военной операции претерпела существенные изменения.

Основными тенденциями стали: адресность воздействия, достигаемая за счет применения БЛА и таргетированных рассылок; синтез традиционных и инновационных методов; интеграция информационно-психологических операций в единую систему управления войсками; использование социальных сетей и мессенджеров как основных каналов распространения информации. Полученный опыт требует пересмотра подходов к подготовке специалистов по информационно-психологическому противоборству, разработки новых методических материалов и оснащения подразделений современными средствами психологического воздействия, включая БЛА с соответствующим оборудованием. Кроме того, дальнейшее развитие тактики требует внедрения систем автоматизированного анализа эффективности воздействия

Список использованных источников:

1.Васильев, А.Н. Информационно-психологическое противоборство в современных конфликтах / А.Н. Васильев, Е.В. Смирнова // Вестник военной академии. − 2024. − № 1. − С. 32–39.

2.Психологические операции в специальной военной операции: опыт и уроки / Под ред. В.И. Леонова. − М.: Издательство Министерства обороны, 2024. − 350 с.

3.Григорьев, Д.А. Применение беспилотных летательных аппаратов для психологического воздействия / Д.А. Григорьев // Армейский сборник. − 2023. — № 8. − С. 22–28.

УДК 355.4

TACTICS OF OFFENSIVE COMBAT IN THE CONDITIONS OF THE SPECIAL MILITARY OPERATION

Burshtyn E.A. student gr.434501

Belarusian State University of Informatics and Radioelectronics

Minsk, Republic of Belarus

Verbitsky G.I. – Master of Management

Annotation. This paper analyzes changes in offensive combat tactics resulting from the experience of special military operations. It examines new challenges facing advancing units: the widespread use of unmanned aerial vehicles, a layered counter-drone defense system, high minefield density, and the widespread use of electronic warfare systems. It identifies key tactical approaches that have evolved during combat operations, including small group tactics, assault squads, the specifics of breaching fortified areas, and the integration of strike UAVs into offensive operations.

Keywords. Offensive combat, tactics, special military operations, assault forces, small groups, unmanned aerial vehicles, counter-drone defense, minefields, electronic warfare, fire support.

ВЛИЯНИЕ АКЦЕНТУАЦИИ ХАРАКТЕРА ЛИЧНОСТИ НА ДЕЯТЕЛЬНОСТЬ ВОЕННОСЛУЖАЩЕГО

Ковалевский А.И.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Вербицкий Г.И. – магистр управления

Аннотация. В работе рассматриваются теоретические основы изучения акцентуаций характера. Анализируются понятие и классификация акцентуаций характера человека и их влияние на специфику деятельности военнослужащего. Выявляются адаптивные и проблемные проявления акцентуаций в военной среде. Обосновывается рекомендации по учету индивидуально-типологических особенностей.

Понятие «акцентуация характера» занимает центральное место на стыке общей и клинической психологии, обозначая такие варианты развития личности, при которых отдельные её черты чрезмерно усилены, что обусловливает повышенную уязвимость индивида к определённым психогенным воздействиям при сохранении общей психической стабильности и адаптации. Данный термин, введённый и глубоко разработанный немецким психиатром Карлом Леонгардом, а впоследствии адаптированный для отечественной науки А.Е. Личко, описывает не болезнь или расстройство, а крайний вариант психической нормы. Это ключевое положение позволяет отграничить акцентуации от психопатий (расстройств личности), где наблюдается тотальная патологическая деформация характера, приводящая к постоянной социальной дезадаптации, нарушению адаптации практически в любых условиях жизни.

Проблема типологии характеров имеет давнюю историю, однако именно Карл Леонгард в середине XX века систематизировал и научно обосновал концепцию акцентуированных личностей. В своей работе «Акцентуированные личности» (1976) он выделил 12 типов, основываясь преимущественно на наблюдениях за взрослыми. Его классификация фокусируется на особенностях стиля социального взаимодействия, эмоциональных реакциях и волевой регуляции. К основным типам по Леонгарду относятся:

1) Демонстративный (истероидный): характеризуется жаждой внимания, театральностью поведения, эгоцентризмом и легкостью самопрезентации.

2) Педантичный: отличается ригидностью, чрезмерной склонностью к порядку, формализму, нерешительностью и совестливостью.

3) Застревающий (паранойяльный): свойственна длительная фиксация на аффектах (обиде, гневе), подозрительность, честолюбие и ригидность установок.

4) Возбудимый (эпилептоидный): проявляется в импульсивности, низком контроле влечений, гневливости, склонности к конфликтам и периодической угрюмости.

5) Гипертимный: оптимизм, повышенная активность и общительность, неугомонность, часто сочетающиеся с поверхностностью и недостатком чувства дистанции.

6) Дистимический: представляет собой противоположность гипертимному – доминирует пессимизм, серьезность, подавленность настроения, замедленность реакций.

7) Тревожно-боязливый (сенситивный): робость, пугливость, повышенная тревожность, неуверенность в себе, исполнительность.

8) Циклотимический: характеризуется периодической сменой фаз гипертимности и дистимии.

9) Аффективно-экзальтированный: крайняя интенсивность и изменчивость эмоциональных реакций, восторженность по незначительным поводам и глубокая отчаянье при неудачах.

10) Эмотивный: родственен экзальтированному, но с более мягкими проявлениями; главная черта – высокая чувствительность и эмпатия [1].

Психологический анализ позволяет структурировать специфику военной службы в ряд взаимосвязанных ключевых факторов, создающих комплексную стрессогенную среду:

1) фактор гиперответственности и морального выбора. Военнослужащий несёт ответственность не только за свою жизнь и выполнение технической задачи, но и за жизнь и благополучие подчинённых, коллег, а в конечном счёте – за безопасность государства. Эта ответственность часто сопряжена с необходимостью принятия решений в условиях моральной дилеммы (например, рисковать ли группой для выполнения миссии), что создаёт колоссальное психоэмоциональное напряжение, несопоставимое с большинством гражданских профессий.

2) фактор перманентного риска. Риск для жизни и здоровья является не вероятностной, а константной составляющей профессионального бытия военнослужащего, даже в мирное время (в ходе учений, несения боевого дежурства, обслуживания техники). Постоянное фоновое осознание этого риска требует особых механизмов психологической защиты и устойчивой системы ценностных ориентаций, где долг и присяга занимают доминирующее положение.

3) фактор жёсткой нормативной регламентации и иерархии. Военная организация – это яркий пример тотального института с предельно чёткой, формализованной системой субординации,

уставных правил и предписанных ролей. Жёсткая иерархическая структура минимизирует пространство для личной инициативы в вопросах дисциплины и подчинения, требуя безусловного принятия авторитета и способности к ролевому перевоплощению из состояния равенства в гражданской жизни в состояние подчинённости.

4) фактор экстремальной когнитивной нагрузки. Деятельность протекает в условиях хронического дефицита времени, высокой динамичности событий, противоречивости и неполноты информации («туман войны»). Это требует от психики способности к сверхбыстрому анализу ситуации, принятию решений при неопределённости, постоянной готовности к смене планов и мгновенной переориентации. Интеллектуальная нагрузка сочетается с высокой сенсорной нагрузкой (шум, вибрация, необходимость отслеживания множества показателей).

5) фактор социально-пространственной изоляции. Длительное нахождение в замкнутых, изолированных коллективах (экипажи, расчёты, гарнизоны) при ограничении контактов с внешним миром и привычной социальной средой (семьёй, друзьями) создаёт феномен «групповой автономии». С одной стороны, это мощный фактор сплочения, с другой – источник напряжённости, когда конфликты становятся трудноразрешимыми, а психологическая совместимость приобретает критически важное значение для выживания и эффективности группы.

6) фактор физиологических и психофизиологических предельных нагрузок. Высокие физические нагрузки, нерегулярный режим дня, депривация сна, воздействие экстремальных климатических и географических условий предъявляют чрезвычайные требования к выносливости организма и, как следствие, к устойчивости психики, её способности сохранять работоспособность и ясность мышления на фоне физического истощения. Значительную роль в тактике психологического воздействия играют социальные сети и мессенджеры. В условиях СВО эти платформы стали основным каналом распространения информации [2].

Рекомендации по назначению могут быть следующими (вариант):

1) Эпилептоидный тип: целесообразно назначать на должности, связанные с административно-хозяйственным обеспечением, контролем, охраной правопорядка (командир взвода обеспечения, дежурный по части, начальник склада ГСМ, инспектор службы безопасности). Следует избегать назначения на должности, требующие гибкого тактического мышления в быстро меняющейся обстановке (командир штурмовой группы).

2) Психастенический тип: оптимальная сфера – штабная, аналитическая, исследовательская работа, работа со сложной документацией и техникой, требующей скрупулёзности (офицер оперативного отдела, криптограф, специалист по топогеодезическому обеспечению, инженер по вооружению). Противопоказаны должности, связанные с принятием сиюминутных волевых решений в условиях неопределённости (командир разведгруппы в тылу врага).

3) Гипертимный тип: наиболее эффективен в родах войск и на должностях, требующих инициативы, коммуникабельности, мобильности и работы в динамичной среде (разведка, связь, десантные подразделения, инструктор по боевой подготовке, воспитательная работа с личным составом). Нежелательно закрепление на монотонных, изолированных постах (караульная служба на удалённом объекте, работа с архивом).

4) Истероидный тип: может быть полезен в сферах, связанных с публичной деятельностью, представительскими функциями, работой с небольшими группами в условиях чёткого сценария (офицер по культурно-досуговой работе, пресс-секретарь, ведущий строевых смотров, актёр военного ансамбля). Требует абсолютного исключения из сфер, связанных с доступом к секретной информации или возможностью сфальсифицировать результат работы.

5) Шизоидный тип: показан для индивидуальной интеллектуальной или технической деятельности, научно-исследовательской работы, программирования, обслуживания сложных систем (оператор беспилотных аппаратов, программист, конструктор, специалист РЭБ). Необходимо минимизировать его участие в обязательных массовых мероприятиях нерабочего характера.

6) Циклоидный тип: требует особого подхода. В период подъёма может эффективно справляться с широким кругом задач, схожих с гипертимными. Однако ввиду непредсказуемости фаз, его не рекомендуется назначать на должности с постоянной, неизменной высокой ответственностью (дежурный по гарнизону, командир боевого дежурного расчета систем ПВО). Предпочтительнее работа в проектных группах с переменной нагрузкой [3].

Учёт акцентуаций характера позволяет повысить эффективность распределения личного состава, снизить риск дезадаптации и улучшить психологическое сопровождение военнослужащих.

Список использованных источников:

1. Леонгард К. Акцентуированные личности. – Ростов н/д: Феникс, 2000.
2. Военная психология: Учебник / Под ред. А.Г. Маклакова. – СПб.: Питер, 2007.
3. Барабанщиков А.В., Давыдов В.П., Феденко Н.Ф. Военная педагогика и психология. – М.: Воениздат, 1986.

УДК 355.4

ТАКТИКА НАСТУПАТЕЛЬНОГО БОЯ В УСЛОВИЯХ СПЕЦИАЛЬНОЙ ВОЕННОЙ ОПЕРАЦИИ

Соловей М.М. студент гр.334201

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Иволгина О.И. – магистр

Аннотация. В работе анализируются изменения в тактике наступательного боя, обусловленные опытом специальной военной операции. Рассматриваются новые вызовы, с которыми сталкиваются наступающие подразделения: массовое применение беспилотных летательных аппаратов, эшелонированная система противодронной обороны, высокая плотность минно-взрывных заграждений и широкое использование средств радиоэлектронной борьбы. Выявляются основные тактические приемы, получившие развитие в ходе боевых действий, включая тактику малых групп, штурмовых отрядов, особенности преодоления укрепленных районов и интеграцию ударных БЛА в наступательные действия.

Ключевые слова. Наступательный бой, тактика, специальная военная операция, штурмовые отряды, малые группы, беспилотные летательные аппараты, противодронная оборона, минно-взрывные заграждения, радиоэлектронная борьба, огневая поддержка.

Опыт специальной военной операции (далее – СВО) коренным образом изменил представления о тактике наступательного боя. Если в предшествующий период наступление рассматривалось как маневренное действие с массированным применением бронетанковой техники и авиации, то реалии СВО продемонстрировали необходимость пересмотра практически всех элементов наступательных действий. Высокая плотность разведывательных и ударных беспилотных летательных аппаратов (БЛА) противника, эшелонированная система противодронной обороны (ПДО), насыщенность оборонительных позиций противотанковыми средствами и массовое применение минно-взрывных заграждений сделали традиционные формы наступления неприемлемыми. Анализ боевых действий позволяет выделить ключевые изменения в тактике наступления, ставшие ответом на новые вызовы современного боя.

Первым и наиболее существенным изменением стал отход от массированного применения бронетанковой техники в пользу тактики малых групп и штурмовых отрядов. Опыт показал, что продвижение колонн бронетехники на открытой местности в условиях непрерывного наблюдения с БЛА и высокой плотности противотанковых средств приводит к неоправданно высоким потерям. Вместо этого наступающие подразделения перешли к действиям штурмовыми группами численностью до отделения-взвода, которые продвигаются пешим порядком, используя складки местности, лесополосы и инженерные сооружения для укрытия. Бронетехника в таких условиях выполняет преимущественно функции огневой поддержки, действуя с закрытых огневых позиций или осуществляя огневые налеты.

Вторым значимым фактором, повлиявшим на тактику наступления, стала необходимость преодоления эшелонированной системы противодронной обороны противника. Наступающие подразделения столкнулись с необходимостью подавления не только традиционных средств ПВО, но и портативных средств РЭБ, антидроновых ружей и сетей-перекрытий, защищающих позиции обороняющихся. В этих условиях важнейшим элементом наступления стала контрбатарейная борьба с использованием разведывательных БЛА и контрбатарейных радаров, а также массированное применение средств радиоэлектронной борьбы для подавления каналов управления дронами противника.

Третьим фактором, определившим эволюцию наступательной тактики, стала высокая плотность минно-взрывных заграждений. Опыт СВО показал, что традиционные методы разминирования (сплошное разминирование саперами, применение тралов) в условиях непрерывного огневого воздействия противника малоэффективны. В ответ на это была разработана тактика «огневого разминирования» – создания проходов в минных полях за счет применения тяжелых огнеметных систем, реактивной артиллерии и ударов авиации. Одновременно с этим широкое распространение получили методы скрытного преодоления заграждений малыми группами с использованием средств индивидуальной защиты и подрывных зарядов.

Особенности организации наступления в условиях позиционного противостояния заслуживают отдельного рассмотрения. В отличие от классической схемы «артиллерийская подготовка – атака – развитие успеха», современное наступление представляет собой серию последовательных и параллельных действий по захвату и закреплению тактически важных объектов. Штурмовые отряды, усиленные огнеметчиками, гранатометчиками и операторами ударных БЛА, последовательно «зачищают» опорные пункты противника, двигаясь по заранее разведанным маршрутам. Особое

внимание уделяется действиям в лесополосах и населенных пунктах, где противник создает наиболее плотную систему огня и инженерных заграждений [1].

Важным элементом современной наступательной тактики стала интеграция ударных беспилотных летательных аппаратов в боевые порядки наступающих подразделений. FPV-дроны и барражирующие боеприпасы используются для поражения выявленных огневых точек, бронетехники и расчетов ПТРК противника на дальностях, превышающих возможности штатного вооружения. Операторы ударных дронов действуют в тесном взаимодействии со штурмовыми группами, обеспечивая подавление целей, препятствующих продвижению. При этом особое значение приобретает устойчивость каналов управления БЛА в условиях радиоэлектронного подавления со стороны противника [2].

Четвертым элементом эволюции наступательной тактики стала принципиально новая логика закрепления захваченных рубежей и ведения контрбатарейной борьбы. Опыт СВО показал, что удержание отбитого опорного пункта традиционными методами (насыщение личным составом) невозможно из-за высокой точности средств поражения противника, в том числе сбросов с коптеров и FPV-дронов. В ответ на это была сформирована тактика «мгновенного фортификационного обустройства»: штурмовые группы после захвата объекта не задерживаются на нем длительное время, оставляя подразделения прикрытия, в то время как основные силы отводятся для ротации или нанесения ударов. Закрепление достигается не столько физическим присутствием пехоты, сколько установлением полного огневого контроля над захваченной территорией (средствами артиллерии и ударных БЛА) и оперативным минированием подступов с использованием дистанционных систем минирования. Такой подход позволил минимизировать потери от встречных контратак и дезорганизовать действия обороняющегося противника, лишив его возможности нанести массированный удар по вклинившимся подразделениям.

В таблице 1 представлен сравнительный анализ основных элементов тактики наступательного боя до начала СВО и с учетом современного опыта.

Таблица 1 – Сравнительный анализ основных элементов тактики наступательного боя.

Элемент наступления	Традиционный подход (до 2022 г.)	Подход с учетом опыта СВО
Построение боевых порядков	Массированное применение бронетанковых групп, линейные порядки	Тактика малых групп, штурмовые отряды, рассредоточение, бронетехника на закрытых позициях
Преодоление заграждений	Сплошное разминирование, применение тралов	Огневое разминирование, скрытный проход малыми группами, использование средств индивидуальной защиты
Противодронная оборона	Штатные средства ПВО прикрытия	Подавление средств РЭБ противника, применение собственных средств РЭБ, использование ударных БЛА для перехвата
Огневая поддержка	Артиллерийская подготовка, удары авиации	Непрерывная огневая поддержка с использованием артиллерии, БЛА, FPV-дронов, корректировка в реальном времени
Управление	Радиосвязь, командиры в боевых порядках	Дублирование каналов, использование закрытых мессенджеров, устойчивость к РЭБ, применение разведывательных БЛА для мониторинга
Действия в населенных пунктах	Штурм с использованием бронетехники	Зачистка штурмовыми группами, огневая поддержка с закрытых позиций, применение огнеметных систем

Опыт наступательных действий в ходе СВО подтвердил эффективность так называемой «штурмовой тактики», получившей развитие в ходе боев за городские агломерации и укрепленные районы. Штурмовые отряды, как правило, состоят из нескольких групп: разведывательно-дозорной (с БЛА), штурмовой (основные силы), огневой поддержки (гранатометчики, пулеметчики) и группы обеспечения (саперы, связисты, медики). Продвижение осуществляется по заранее спланированным маршрутам с последовательным захватом и закреплением зданий, сооружений и опорных пунктов. Особое внимание уделяется действиям в подземных коммуникациях и по созданию «огневых мешков» для уничтожения контратакующих групп противника [3].

Значительный интерес в контексте развития тактики наступления представляет опыт проведения масштабных тренировок в рамках единого дня огня. В ходе мероприятий, проводившихся

в Южном военном округе, отрабатывалась интеграция разведывательных данных в систему огневой поддержки наступающих подразделений. Разведчики соединений специального назначения, используя комплексы разведки, управления и связи КРУС «Стрелец», передавали данные о выявленных целях на носители высокоточного оружия, включая экипажи бомбардировщиков Су-24, расчеты ОТРК «Искандер-М», береговые ракетные комплексы «Бал» и батареи реактивных установок «Торнадо-С». Управление разведывательными и ударными силами организовывалось с подвижных полевых пунктов управления, а информация о разведанных целях и результатах их поражения поступала на объединенный командный пункт в реальном времени. Данный опыт показывает, что успех наступления в современном конфликте напрямую зависит от способности оперативно преобразовывать разведывательную информацию в огневое поражение противника на глубину его обороны.

В ходе указанных тренировок, объединивших более ста носителей ракетного вооружения сухопутных, авиационных и морских соединений, было выполнено свыше 400 огневых задач. К мероприятиям привлекалось более 5 тыс. военнослужащих и около 2 тыс. единиц артиллерийских орудий, ракетных комплексов, самолетов оперативно-тактической авиации и боевых кораблей. Разведчики задействовали более 20 беспилотных летательных аппаратов. Этот масштаб демонстрирует, что наступление в современном конфликте требует координации усилий всех видов и родов войск, а разведывательная информация является ключевым ресурсом, определяющим эффективность наступательных действий.

Важным аспектом наступательной тактики в условиях СВО стала подготовка и ротация подразделений. В отличие от классических представлений о непрерывном наступлении, современные действия характеризуются высокой интенсивностью, но ограниченной продолжительностью активных действий. Штурмовые подразделения, как правило, действуют в течение ограниченного времени (от нескольких часов до нескольких суток), после чего выводятся на отдых и доукомплектование, а их место занимают свежие силы. Такой подход позволяет сохранить боеспособность подразделений и снизить потери от накапливающейся усталости личного состава.

Таким образом, тактика наступательного боя в реалиях специальной военной операции претерпела фундаментальные изменения. Основными тенденциями стали: отказ от массированного применения бронетанковой техники в пользу тактики малых групп и штурмовых отрядов; активное использование ударных БЛА как средства огневой поддержки, интегрированного в боевые порядки; переход к огневому разминированию и скрытному преодолению заграждений; создание эшелонированной системы огневой поддержки с использованием артиллерии, авиации и БЛА; интеграция наступательных действий с разведывательно-огневым контуром, обеспечивающим оперативное поражение выявленных целей. Полученный опыт требует пересмотра уставных документов, корректировки программ боевой подготовки и разработки новых методических материалов по организации наступательного боя.

Список использованных источников:

1. Егоров, А.Н. Тактика наступательного боя в условиях массового применения БЛА / А.Н. Егоров, В.П. Смирнов // Военная мысль. – 2024. – № 4. – С. 22–31.

2. Наступление в специальной военной операции: опыт и уроки / Под ред. С.В. Ковалева. – М.: Издательство Министерства обороны, 2024. – 480 с.

3. Федоров, И.А. Применение штурмовых отрядов в городских условиях / И.А. Федоров // Армейский сборник. – 2024. – № 1. – С. 18–25.

УДК 355.4

TACTICS OF OFFENSIVE COMBAT IN THE CONDITIONS OF THE SPECIAL MILITARY OPERATION

Solovey M.M. student gr.334201

Belarusian State University of Informatics and Radioelectronics

Minsk, Republic of Belarus

Ivolgina O.I. – Master

Annotation. This paper analyzes changes in offensive combat tactics resulting from the experience of special military operations. It examines new challenges facing advancing units: the widespread use of unmanned aerial vehicles, a layered counter-drone defense system, high minefield density, and the widespread use of electronic warfare systems. It identifies key tactical approaches that have evolved during combat operations, including small group tactics, assault squads, the specifics of breaching fortified areas, and the integration of strike UAVs into offensive operations.

Keywords. Offensive combat, tactics, special military operations, assault forces, small groups, unmanned aerial vehicles, counter-drone defense, minefields, electronic warfare, fire support.

УДК 355.4

ТАКТИКА ОБОРОНИТЕЛЬНОГО БОЯ В РЕАЛИЯХ СПЕЦИАЛЬНОЙ ВОЕННОЙ ОПЕРАЦИИ

Зарецкий Г.В. студент гр.334201

Белорусский государственный университет информатики и радиоэлектроники г. Минск, Республика Беларусь

Лялихов К.А. – магистр

Аннотация. В работе анализируются изменения в тактике оборонительного боя, обусловленные опытом специальной военной операции. Рассматриваются новые факторы, влияющие на организацию обороны: массовое применение беспилотных летательных аппаратов, высокоточного оружия и средств радиоэлектронной борьбы. Выявляются основные тактические приемы, получившие развитие в ходе позиционного противостояния, включая создание опорных пунктов, систему огневых мешков, противодронную оборону и особенности инженерного оборудования позиций. Обосновывается необходимость пересмотра уставных документов с учетом современных реалий.

Ключевые слова. Оборонительный бой, тактика, специальная военная операция, позиционная оборона, опорный пункт, беспилотные летательные аппараты, противодронная оборона, инженерное оборудование, радиоэлектронная борьба, огневое поражение.

Опыт специальной военной операции (далее − СВО) кардинальным образом трансформировал представления о тактике оборонительного боя. Если в предшествующий период основное внимание уделялось мобильной обороне с широким применением маневренных действий, то реалии СВО вернули значимость позиционному противостоянию, сопряженному с высокой плотностью огневых средств, массовым использованием беспилотных летательных аппаратов (БЛА) и необходимостью глубокого инженерного оборудования местности. Анализ боевых действий позволяет выделить ключевые изменения в организации и ведении обороны, которые стали ответом на новые вызовы современного боя.

Первым и наиболее существенным фактором, повлиявшим на тактику обороны, стало массовое применение БЛА различных типов − от коммерческих мультироторных аппаратов до специализированных разведывательно-ударных комплексов и FPV-дронов-камикадзе. Противник получил возможность вести непрерывную разведку оборонительных позиций, оперативно корректировать огонь артиллерии и наносить точечные удары по выявленным объектам. В этих условиях традиционная система обороны, построенная на системе опорных пунктов с четко выраженными позициями, оказалась уязвимой. Ответом стало развитие тактики «крепостных опорных пунктов» − хорошо укрепленных позиций, способных вести круговую оборону и автономно функционировать в течение длительного времени.

Вторым значимым фактором стало широкое применение высокоточного оружия, включая артиллерийские снаряды с коррекцией, противотанковые ракетные комплексы и барражирующие боеприпасы. Эффективность поражения целей возросла на порядок, что потребовало пересмотра принципов рассредоточения сил и средств. Если ранее дистанции между элементами боевого порядка обороны составляли десятки метров, то в условиях СВО они увеличились до сотен метров. Обороняющиеся подразделения перешли к эшелонированному построению с глубоким рассредоточением личного состава и техники, что позволило снизить потери от массированных огневых ударов.

Третьим фактором, трансформировавшим подходы к организации обороны, стало массированное применение инженерных заграждений, в первую очередь минно-взрывных. Опыт СВО показал, что плотность минирования на наиболее опасных направлениях достигла значений, сопоставимых с периодами крупных войн прошлого столетия. В ответ на это обороняющиеся подразделения разработали тактику динамического минирования, при котором установка заграждений осуществляется не только заблаговременно, но и в ходе боя с использованием дистанционных систем минирования. Мобильные группы инженерных войск, действуя совместно с расчетами реактивной артиллерии, создают минные поля перед наступающими подразделениями противника в реальном масштабе времени, что позволяет компенсировать недостаток личного состава на угрожаемых направлениях и наносить урон противнику на подступах к основным оборонительным рубежам.

Особенности инженерного оборудования оборонительных позиций в условиях СВО заслуживают отдельного рассмотрения. Опыт показал, что традиционные окопы и траншеи полного профиля не обеспечивают достаточной защиты от сбросов с БЛА и осколочного поражения. Широкое распространение получили так называемые «лисьи норы» −узкие, глубокие укрытия с перекрытиями, защищающими от сбросов сверху. Система ходов сообщения развивается в нескольких уровнях,

включая подземные галереи, обеспечивающие скрытное передвижение личного состава. Важным элементом стало оборудование позиций с использованием железобетонных конструкций, контейнерных укрытий и элементов городской инфраструктуры.

Система огневого поражения в оборонительном бою также претерпела изменения. Массовое применение FPV-дронов создало возможность поражения наступающей техники противника на значительном удалении от переднего края. Операторы ударных дронов интегрированы в систему обороны наравне с расчетами противотанковых ракетных комплексов и артиллерии. Особенностью стало создание «огневых мешков» − участков местности, простреливаемых с нескольких направлений с использованием как традиционных огневых средств, так и ударных БЛА. Наступающий противник, попадая в такой мешок, подвергается одновременному поражению с разных сторон и высот [1].

В таблице 1 представлен сравнительный анализ основных элементов тактики оборонительного боя до начала СВО и с учетом современного опыта.

Таблица 1 – Сравнительный анализ основных элементов тактики оборонительного боя.

Элемент обороны	Традиционный подход (до 2022 г.)	Подход с учетом опыта СВО
Построение обороны	Система опорных пунктов, траншеи полного профиля	«Крепостные» опорные пункты, глубокое рассредоточение, многоуровневые укрытия
Инженерное оборудование	Окопы, траншеи, блиндажи	«Крепостные» опорные пункты, глубокое рассредоточение, многоуровневые укрытия
Противодронная оборона	Штатные средства ПВО	«Крепостные» опорные пункты, глубокое рассредоточение, многоуровневые укрытия
Управление	Радиосвязь, проводная связь	Интеграция ударных БЛА, создание «огневых мешков», контрбатарейная борьба с использованием разведывательных БЛА
Тактика действий	Пассивная оборона, контратаки	Активная оборона с использованием БЛА, мобильные огневые группы, «ротационные» смены подразделений

Важным элементом оборонительной тактики в условиях СВО стало создание эшелонированной системы противодронной обороны (ПДО) на всех уровнях − от позиции отделения до батальонного района обороны. На переднем крае оборудуются позиции для стрельбы по БЛА из стрелкового оружия, устанавливаются сети-перекрытия, защищающие окопы от сбросов, и портативные средства РЭБ, создающие «купол» над позициями. На втором эшелоне размещаются специализированные расчеты с антидроновыми ружьями и зенитными установками. В глубине обороны действуют мобильные группы РЭБ и операторы FPV-дронов, осуществляющие перехват ударных БЛА противника.

Опыт организации обороны в ходе СВО подтвердил эффективность так называемой «активной обороны», сочетающей прочное удержание опорных пунктов с активными действиями мобильных групп. Эти группы, оснащенные БЛА, средствами РЭБ и легким вооружением, действуют на флангах и в промежутках между опорными пунктами, нанося удары по наступающему противнику, осуществляют минирование и проводят разведку [2].

Важным направлением развития оборонительной тактики, подтвержденным в ходе тренировок Южного военного округа, стала интеграция систем противодронной обороны с контурами контрбатарейной борьбы. Практика показала, что способность своевременно вскрывать и подавлять средства огневой поддержки наступающего противника, а именно расчеты ударных беспилотных летательных аппаратов и артиллерийские батареи, напрямую определяет успех удержания позиций. В рамках единого дня огня отрабатывалось взаимодействие, в ходе которого портативные средства радиоэлектронной борьбы, фиксируя каналы управления неприятельскими дронами, одновременно выдавали целеуказания мобильным группам поражения. Подобная архитектура обороны позволила сократить интервал между обнаружением и подавлением до значений, при которых противник лишается возможности нанести прицельный удар по опорным пунктам, и значительно уменьшила нагрузку на личный состав, занимающий передовые позиции [3].

Требует отдельного внимания трансформация подходов к инженерному обустройству оборонительных позиций, вызванная массовым применением FPV дронов и высокоточной ствольной артиллерии. Привычная система траншей и ходов сообщения эволюционировала в направлении создания рассредоточенных ячеечных позиций с усиленной защитой сверху. В ходе мероприятий в Южном военном округе отрабатывалось оборудование опорных пунктов с применением сборных железобетонных конструкций, способных защитить от прямых попаданий сбросов и осколков, а также устройство ложных позиций, оснащенных тепловыми ловушками и имитаторами работы средств связи. Большое внимание уделялось организации скрытых маршрутов для маневра резервами под

прикрытием естественных и искусственных масок, что позволяло сохранять боеспособность подразделений при массированных огневых налетах и обеспечивало внезапность контратак мобильных групп на флангах вклинившегося противника.

Значительный интерес в контексте развития тактики обороны представляет опыт проведения масштабных тренировок в рамках единого дня огня. В ходе мероприятий, проводившихся в Южном военном округе, отрабатывалась интеграция разведывательных данных в систему огневого поражения обороняющихся подразделений.

Разведчики соединений специального назначения, используя комплексы разведки, управления и связи КРУС «Стрелец», передавали данные о выявленных целях на носители высокоточного оружия, включая экипажи бомбардировщиков Су-24, расчеты ОТРК «Искандер-М», береговые ракетные комплексы «Бал» и батареи реактивных установок «Торнадо-С». Управление разведывательными и ударными силами организовывалось с подвижных полевых пунктов управления, а информация о разведанных целях и результатах их поражения поступала на объединенный командный пункт в реальном времени.

Данный опыт показывает, что современная оборона не может быть пассивной −она требует активного использования разведывательной информации для нанесения превентивных ударов по наступающему противнику. В ходе указанных тренировок, объединивших более ста носителей ракетного вооружения сухопутных, авиационных и морских соединений, было выполнено свыше 400 огневых задач. К мероприятиям привлекалось более 5 тыс. военнослужащих и около 2 тыс. единиц артиллерийских орудий, ракетных комплексов, самолетов оперативно-тактической авиации и боевых кораблей. Разведывательная информация является ключевым ресурсом, определяющим эффективность оборонительных действий.

Таким образом, тактика оборонительного боя в реалиях специальной военной операции претерпела фундаментальные изменения.

Основными тенденциями стали: переход к глубоко эшелонированной, рассредоточенной обороне с использованием «крепостных» опорных пунктов; создание многоуровневой системы противодронной обороны, интегрированной в боевые порядки; развитие инженерного оборудования позиций с акцентом на защиту от БЛА и высокоточного оружия; активное использование ударных БЛА и средств РЭБ в рамках единой системы огневого поражения; интеграция оборонительных действий с разведывательно-огневым контуром, обеспечивающим поражение противника на подступах и в глубине его построения. Полученный опыт требует пересмотра уставных документов, корректировки программ боевой подготовки и разработки новых методических материалов по организации оборонительного боя.

Список использованных источников:

1. Белоусов, А.И. Тактика оборонительного боя в условиях применения БЛА / А.И. Белоусов, В.Н. Соколов // Военная мысль. −2024. −№ 3. −С. 28–36.

2. Оборона в специальной военной операции: опыт и уроки / Под ред. С.В. Ковалева. −М.: Издательство Министерства обороны, 2024. −450 с.

3. Лебедев, Д.А. Инженерное оборудование позиций в условиях позиционного противостояния / Д.А. Лебедев // Армейский сборник. −2023. −№ 12. −С. 14–21.4.ЦАМТО. Масштабная тренировка в рамках единого дня огня объединила более ста носителей ракетного вооружения соединений ЮВО. − 11 декабря. − Режим доступа: свободный.

УДК 355.4

TACTICS OF OFFENSIVE COMBAT IN THE CONDITIONS OF THE SPECIAL MILITARY OPERATION

Zaretsky G.V. student gr.334201

Belarusian State University of Informatics and Radioelectronics

Minsk, Republic of Belarus

Lyalikhov K.A. – Master

Annotation. This paper analyzes changes in defensive combat tactics resulting from the experience of special military operations. New factors influencing defense organization are examined, including the widespread use of unmanned aerial vehicles, precision weapons, and electronic warfare systems. Key tactical techniques developed during positional conflict are identified, including the establishment of strongpoints, fire pocket systems, counter-drone defenses, and the specifics of positional engineering. The need to revise statutory documents to reflect current realities is substantiated.

Keywords. Defensive combat, tactics, special military operation, positional defense, strongpoint, unmanned aerial vehicles, counter-drone defense, engineering equipment, electronic warfare, fire damage.

УДК 355.5

ПРИМЕНЕНИЕ БЕСПИЛОТНЫХ ЛЕТАТЕЛЬНЫХ АППАРАТОВ В НАЧАЛЬНОЙ ФАЗЕ СПЕЦИАЛЬНОЙ ВОЕННОЙ ОПЕРАЦИИ

Грошев Е.С. студент гр.334201

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Сименков Е.Л. – магистр техники и технологии

Аннотация. В работе анализируется роль и место беспилотных летательных аппаратов (БЛА) в начальный период специальной военной операции. Рассматриваются основные направления применения БЛА: разведка, корректировка огня, поражение целей и радиоэлектронная борьба. Выявлены ключевые тактические инновации, возникшие в результате массового использования беспилотных систем, а также проблемы, связанные с недостаточной подготовкой личного состава и отсутствием единой системы противодействия средствам разведки противника.

Ключевые слова. Беспилотные летательные аппараты, БЛА, специальная военная операция, начальная фаза, разведка, корректировка огня, FPV-дрон, радиоэлектронная борьба, тактика, контрбатарейная борьба.

Начальная фаза специальной военной операции (далее − СВО), охватывающая период с февраля по апрель 2022 года, характеризовалась интенсивным применением войск в условиях высокой динамики обстановки и недостаточного опыта ведения боевых действий с использованием современных беспилотных систем. Именно в этот период произошла кардинальная переоценка роли беспилотных летательных аппаратов (далее −БЛА) − от вспомогательного средства разведки до одного из ключевых элементов общевойскового боя, способного оказывать непосредственное влияние на ход и исход операций. Анализ боевых действий начального этапа СВО позволяет выделить три основных направления применения БЛА: разведывательное, огневое (ударное) и обеспечение радиоэлектронной борьбы.

На начальном этапе операции российские войска столкнулись с высокой эффективностью турецких БЛА Bayraktar TB2, находившихся на вооружении украинской армии. Эти аппараты среднего радиуса действия демонстрировали способность наносить точные удары по колоннам техники, складам боеприпасов и узлам управления, действуя в условиях отсутствия надежного прикрытия средств противовоздушной обороны (ПВО) наступающих подразделений. Одновременно с этим украинская сторона широко применяла коммерческие БЛА мультироторного типа (DJI Mavic, Autel и другие) для ведения разведки и корректировки артиллерийского огня. Массовость и доступность таких аппаратов создали ситуацию, при которой каждое тактическое подразделение получило возможность оперативно получать разведывательную информацию с высоты птичьего полета, что ранее было доступно только на уровне бригада-дивизия.

Одной из ключевых проблем начальной фазы СВО стала недостаточная оснащенность российских подразделений средствами радиоэлектронной борьбы (РЭБ), способными эффективно подавлять каналы управления и передачи данных коммерческих БЛА. Противник активно использовал этот пробел, организуя непрерывное наблюдение за передвижением войск и оперативно корректируя огонь артиллерии. В результате маршруты выдвижения российских колонн часто простреливались артиллерией, а скопления техники становились целями для высокоточных ударов. Данная ситуация продемонстрировала, что эффективность действий войск в современном конфликте напрямую зависит от наличия эшелонированной системы РЭБ, интегрированной в боевые порядки.

Значимым направлением, проявившимся в начальный период, стало массовое применение беспилотных летательных аппаратов для решения задач психологического воздействия и информационного противоборства. Противник активно использовал сброс листовок с коммерческих дронов над позициями российских войск, а также осуществлял видеосъемку результатов ударов с последующим распространением в информационном пространстве. Такая тактика преследовала цель подорвать морально-психологическое состояние личного состава и создать искаженное представление о реальном положении дел на фронте среди гражданского населения. Опыт показал, что в условиях современного конфликта информационная составляющая применения беспилотных систем становится не менее важной, чем непосредственно огневое поражение противника.

Наиболее значимой тактической инновацией начального этапа СВО стало массовое применение FPV-дронов (first-person view) − коммерческих мультироторных аппаратов, переоборудованных для поражения целей. В отличие от специализированных ударных БЛА, FPV-дроны обладают низкой стоимостью, высокой маневренностью и способностью поражать бронированную технику в наиболее уязвимые места (крыша, моторный отсек). Первые случаи успешного применения FPV-дронов против танков и боевых машин пехоты были зафиксированы уже в апреле-мае 2022 года. Этот опыт впоследствии привел к созданию специализированных подразделений операторов FPV-дронов и появлению нового класса вооружения − барражирующих боеприпасов.

Параллельно с развитием ударных возможностей БЛА происходила эволюция средств противодействия. В начальной фазе СВО обе стороны активно экспериментировали с портативными средствами РЭБ, устанавливаемыми на автомобильную и бронетанковую технику. Широкое распространение получили носимые антидроновые ружья, предназначенные для подавления каналов управления и навигации БЛА на малых дальностях. Однако эффективность таких средств в условиях плотного применения дронов оставалась ограниченной, что обусловило необходимость разработки систем РЭБ с большей мощностью и возможностью работы в автоматическом режиме.

Значительный вклад в развитие системы управления разведкой и огнем в начальной фазе СВО внесло применение комплексов разведки, управления и связи КРУС «Стрелец». Данная система позволяла разведывательным подразделениям в реальном времени передавать координаты выявленных целей на огневые средства, включая артиллерийские батареи, реактивные системы залпового огня и оперативно-тактические комплексы. Опыт применения КРУС «Стрелец» подтвердил эффективность концепции «разведывательно-огневого контура», в котором время от обнаружения цели до ее поражения сокращается до нескольких минут [1].

В таблице 1 представлены основные результаты применения БЛА в начальной фазе СВО.

Таблица 1 – Основные результаты применения БЛА в начальной фазе СВО.

Направление применения	Типы БЛА	Основные результаты	Основные результаты
Разведка и наблюдение	Bayraktar TB2, DJI Mavic, Autel	Обеспечение непрерывного наблюдения за передвижением войск, выявление скоплений техники, корректировка огня артиллерии	Уязвимость для средств ПВО, ограниченное время полета коммерческих БЛА
Ударные действия	Bayraktar TB2, FPV-дроны	Поражение колонн техники, складов боеприпасов, узлов управления, бронированной техники	Уязвимость для средств ПВО, ограниченное время полета коммерческих БЛА
Радиоэлектронная борьба	Антидроновые ружья, портативные средства РЭБ	Подавление каналов управления коммерческих БЛА противника	Недостаточная мощность, отсутствие эшелонированной системы РЭБ
Обеспечение управления	КРУС «Стрелец», разведывательные БЛА	Передача целеуказания в реальном времени, сокращение времени поражения целей	Недостаточная интеграция с огневыми средствами на начальном этапе

Анализ начальной фазы СВО позволяет сформулировать ряд выводов, имеющих значение для развития теории и практики применения БЛА.

Во-первых, массовое использование коммерческих БЛА мультироторного типа привело к демократизации разведывательных возможностей, сделав их доступными на уровне взвод-рота.

Во-вторых, трансформация FPV-дронов из гражданского в военное применение создала новый класс оружия, сочетающий низкую стоимость с высокой эффективностью поражения бронированной техники.

В-третьих, начальный этап СВО выявил критическую зависимость эффективности боевых действий от наличия развитой системы РЭБ, способной противостоять массированному применению БЛА противника.

Особого внимания заслуживает опыт применения БЛА в рамках единых разведывательно-огневых контуров. В ходе тренировок, проводившихся в Южном военном округе, отрабатывалась передача координат целей от разведчиков, оснащенных комплексами «Стрелец», на носители высокоточного оружия, включая экипажи бомбардировщиков Су-24, расчеты ОТРК «Искандер-М», береговые ракетные комплексы «Бал» и батареи реактивных установок «Торнадо-С». Управление разведывательными и ударными силами организовывалось с подвижных полевых пунктов управления, а информация о разведанных целях и результатах их поражения поступала на объединенный командный пункт в реальном времени. Данный подход, отработанный в ходе масштабных мероприятий боевой подготовки, стал закономерным развитием тех тактических приемов, которые зародились именно в начальной фазе СВО [2].

Важным выводом, вытекающим из анализа начальной фазы СВО, стало осознание необходимости унификации и стандартизации беспилотных комплексов, применяемых в войсках. Первоначальный период характеризовался хаотичным использованием разнородных гражданских аппаратов, что создавало серьезные проблемы в логистике, подготовке операторов и интеграции в общую систему управления. В ответ на этот вызов была развернута работа по созданию единой линейки беспилотных систем, адаптированных к специфике боевого применения: от сверхлегких разведывательных аппаратов тактического звена до тяжелых ударных комплексов, способных нести многофункциональную нагрузку. Одновременно с этим была пересмотрена система подготовки специалистов, в рамках которой акцент сместился с эпизодического обучения операторов на создание непрерывного конвейера подготовки, включающего как теоретическую базу, так и интенсивные практические тренировки в условиях, максимально приближенных к боевым.

Другим значимым результатом, полученным в ходе начальной фазы СВО, стало формирование новых подходов к тактике применения ударных беспилотных аппаратов во взаимодействии с другими средствами поражения. Опыт показал, что наиболее эффективным является не изолированное использование FPV-дронов, а их интеграция в единый разведывательно-огневой контур, где они выступают в роли высокоточного инструмента, дополняющего артиллерийские и ракетные средства. В рамках такой архитектуры разведывательные БЛА обеспечивают вскрытие целей и целеуказание, ударные дроны осуществляют поражение мобильных и бронированных объектов, а средства огневого поражения (артиллерия, танки, минометы) наносят удары по стационарным целям и опорным пунктам. Такое распределение функций позволило существенно повысить эффективность огневого поражения при одновременном снижении расхода традиционных боеприпасов, что особенно важно в условиях позиционного противостояния с высокой плотностью обороны противника. Дальнейшее совершенствование данной модели предполагает внедрение элементов искусственного интеллекта для автоматизации процессов целераспределения и повышения устойчивости каналов связи в условиях активного применения средств радиоэлектронной борьбы противником [3].

Таким образом, начальная фаза специальной военной операции стала периодом кардинальной переоценки роли беспилотных летательных аппаратов в современной войне. Опыт, полученный в этот период, показал, что эффективность применения БЛА определяется не столько техническим совершенством отдельных образцов, сколько способностью интегрировать их в единую разведывательно-огневую систему, обеспечивающую оперативное доведение целеуказания и поражение целей в реальном масштабе времени. Дальнейшее развитие беспилотных систем и средств противодействия им будет определять облик будущих вооруженных конфликтов, а уроки начального этапа СВО требуют включения в программы подготовки офицерских кадров и боевой подготовки войск. Полученный опыт требует пересмотра уставных документов, корректировки программ боевой подготовки и разработки новых методических материалов по организации оборонительного боя.

Список использованных источников:

1. Особенности применения войск (сил) в современных конфликтах: анализ опыта СВО / Под ред. В.И. Леонова. – М.: Издательство Министерства обороны, 2024. – 420 с.

2. Сидоров, А.В. Тактика действий мотострелковых подразделений в условиях массового применения БПЛА / А.В. Сидоров // Военная мысль. – 2023. – № 7. – С. 45–53.

3. Кузнецов, Д.Ю. Организация противодронной обороны при передвижении войск / Д.Ю. Кузнецов, И.И. Орлов // Армейский сборник. – 2024. – № 2. – С. 12–19.

УДК 355.5

USE OF UNMANNED AERIAL VEHICLES IN THE INITIAL PHASE OF A SPECIAL MILITARY OPERATION

Groshev E.S. student gr.334201

Belarusian State University of Informatics and Radioelectronics

Minsk, Republic of Belarus

Simenkov E.L. – Master of Engineering and Technology

Annotation. This paper analyzes the role and place of unmanned aerial vehicles (UAVs) in the initial stages of special military operations. The paper examines the primary applications of UAVs: reconnaissance, fire adjustment, target engagement, and electronic warfare. It identifies key tactical innovations resulting from the widespread use of unmanned systems, as well as challenges associated with insufficient personnel training and the lack of a unified system for countering enemy reconnaissance assets.

Keywords. Unmanned aerial vehicles, UAVs, special military operation, initial phase, reconnaissance, fire adjustment, FPV drone, electronic warfare, tactics, counter-battery warfare.

АКТУАЛЬНОСТЬ ПРОВЕДЕНИЯ ПРАКТИЧЕСКИХ ТРЕНИРОВОК СПЕЦИАЛИСТОВ ПО КИБЕРБЕЗОПАСНОСТИ: РАЗРАБОТКА ВЕБ-ПРИЛОЖЕНИЯ ДЛЯ ВООРУЖЕННЫХ СИЛ РЕСПУБЛИКИ БЕЛАРУСЬ

Пучков Е.С.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Савицкий А.Ю. – кандидат военных наук

Аннотация. В работе обоснована необходимость проведения практических тренировок специалистов по кибербезопасности в Вооруженных Силах Республики Беларусь и представлена архитектура разрабатываемого веб-приложения, обеспечивающего автоматизацию данных тренировок. Создаваемое программное средство позволяет моделировать кибератаки, оценивать действия специалистов, вести учет результатов и формировать отчеты, учитывая специфику военных задач, что не в полной мере реализовано в существующих аналогах.

В условиях возрастания числа киберугроз и перехода военных структур на цифровые технологии особое внимание уделяется подготовке высококвалифицированных специалистов по кибербезопасности. В Вооруженных Силах Республики Беларусь проведение практических тренировок (отработка выявления, анализа и отражения кибератак) является критически важным элементом боевой подготовки. Однако существующие методы тренировок зачастую не автоматизированы, не позволяют оперативно создавать реалистичные сценарии атак. Это приводит к снижению эффективности подготовки и увеличивает время на развертывание тренировочной среды.

Анализ доступных аналогов показал, что они не обеспечивают необходимый уровень безопасности и изоляции, имеют ограниченные возможности по интеграции с существующими информационными системами, не поддерживают специфические для военной сферы сценарии. Кроме того, в большинстве решений отсутствует гибкая система оценки действий обучаемого. В связи с этим разработка собственного специализированного веб-приложения является актуальной и практически значимой задачей.

В ходе выполнения работы проектируется веб-приложение, реализующее следующие основные функции:

– аутентификация и авторизация пользователей с ролями «тренер» (руководитель тренировки), «специалист» (курсант/офицер), «администратор»;

– создание и управление тренировочными сценариями (виртуальные сети с заданными уязвимостями, симуляция атакующих действий);

– автоматизированная проверка выполнения заданий (захват флагов, обнаружение инцидентов, написание отчетов);

– ведение личного кабинета с историей тренировок, результатами и динамикой прогресса;

– генерация отчетов о результатах тренировки в формате PDF с графиками успеваемости;

– безопасное хранение данных в PostgreSQL, контейнеризация с помощью Docker.

Архитектура разрабатываемого программного средства строится с использованием языка Java, фреймворка Spring Boot (Spring Security, Spring Data JPA), системы сборки Maven. Для моделирования тренировочных сред планируется применение технологий виртуализации (Docker, Kubernetes). Такой подход обеспечивает изоляцию процессов, масштабируемость и возможность быстрого развертывания на серверах Министерства обороны.

Разрабатываемое веб-приложение позволит повысить качество практической подготовки специалистов по кибербезопасности за счет регулярных автоматизированных тренировок с реалистичными сценариями, сократить временные затраты на организацию и проведение занятий, обеспечить объективность оценки и детальный анализ действий каждого военнослужащего. Применение собственной разработки гарантирует учет всех требований военного ведомства и возможность доработки функционала в ходе эксплуатации. Дальнейшее развитие системы предполагает интеграцию с существующими системами управления обучением военных учебных заведений, внедрение элементов искусственного интеллекта для адаптивной генерации сценариев под уровень подготовки специалиста, а также создание распределенного полигона для проведения совместных тренировок подразделений кибербезопасности.

Список использованных источников:

1. Spring Boot Documentation [Электронный ресурс]. – Электронные данные. – Режим доступа: https://docs.spring.io/spring-boot/docs/current/reference/html/. – Дата доступа: 28.03.2026.

2. NIST SP 800-181: National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework [Электронный ресурс]. – Режим доступа: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181r1.pdf. – Дата доступа: 28.03.2026.

ПРИМЕНЕНИЕ ТЕХНОЛОГИЙ OSINT ДЛЯ ВЫЯВЛЕНИЯ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Лукашевич Е.А.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Супрун Ф.Н.

Аннотация. На протяжении последних десятилетий значительно увеличивается количество информационных атак. В современном мире конфиденциальность данных и стабильность функционирования информационной системы являются необходимым условием бесперебойной и конкурентоспособной деятельности. В связи с этим стремительными темпами развивается противодействие угрозам информационной безопасности. В статье представлены способы применения технологии разведки данных из открытых источников (OSINT) для выявления угроз информационной безопасности.

В условиях новой реальности стабильно увеличивается количество кибератак. Злоумышленники находят все более сложные и неуловимые способы информационного воздействия с целью кражи или уничтожения данных, внедрение вредоносного кода или программного обеспечения.

Наиболее распространёнными видами угроз информационной безопасности являются следующие:

– DDoS (Distributed Denial of Service) – атака, направленная на перегрузку сети или конкретного сервера большим количеством запросов. DDoS-атаки приводят к временной недоступности инфраструктуры.

– Фишинг — мошенническая практика, когда киберпреступники выдают себя за надежные источники для получения личной информации.

– SQL-инъекции — метод атаки, при котором злоумышленники внедряют SQL-код в запросы к базе данных для получения доступа к данным, содержащимся в этой БД.

– Социальная инженерия — манипуляции людьми с целью получения личной информации или выполнения определенных действий. Например, злоумышленник может различными способами втираться в доверие к жертве, ведя с ней переписку в социальных сетях или мессенджерах.

– Advanced Persistent Threat (APT) — продолжительная и хорошо подготовленная целенаправленная кибератака. В отличие от DDoS, APT — комплексная киберугроза, сочетающая различные способы атак на корпоративную инфраструктуру [1].

Исходя из этого возникает необходимость поиска эффективных способов противодействия. Проблема многих систем информационной безопасности в том, что они направленны на противостояние возникающим угрозам, а не на выявление уже существующих уязвимостей для их устранения. Одним из наиболее эффективных методов такого противодействия является OSINT.

OSINT (Open Source Intelligence, разведка на основе открытых источников) — это методика сбора данных из открытых источников информации, таких как публичные базы данных, интернет-сайты, медиа и социальные сети. Эти данные анализируются для получения сведений, которые могут быть использованы в аналитических, разведывательных и стратегических целях [2].

Использование методов разведки из открытых источников позволяет проанализировать структуру сети и базы данных, обнаружить важную коммерческую информации в открытом доступе, тем самым устранить бреши в системе защиты.

Сервисы Shoodan и Censys позволяют обнаружить открытые порты, устаревшие протоколы защиты и неверные конфигурационные настройки сети.

Публичные репозитории исходного кода. Такие платформы, как GitHub, GitLab и Bitbucket, нередко становятся источником утечек конфиденциальной информации вследствие ошибочной публикации учетных данных.

Также активно развивается использование социальной инженерии. Злоумышленники используют публикации в социальных сетях для составления психологического портрета, тем самым находя точки воздействия для достижения своих целей. Использование технологии OSINT позволяет обнаружить в открытых источниках подобную информацию и обучить не оставлять информационные следы, которые могут быть использованы для совершения информационной атаки.

Таким образом применение технологии OSINT позволяет эффективно выявлять уязвимости в информационной безопасности. Методы сбора данных из открытых источников дают возможность оперативно обнаружить риски укреплению информационной безопасности и повышению устойчивости к внешним и внутренним рискам.

Список использованных источников:

1. Академия Selectel [Электронный ресурс]. – Электронные данные. – Режим доступа: https://selectel.ru/blog/security-threats/. – Дата доступа: 25.03.2026.

2. RTM Group [Электронный ресурс]. – Электронные данные. – Режим доступа: https://rtmtech.ru/articles/dlya-chego-nuzhen-osint/. – Дата доступа: 25.03.2026.

АВТОМАТИЗАЦИЯ УПРАВЛЕНИЯ ФИЗИЧЕСКОЙ ПОДГОТОВКОЙ КУРСАНТОВ: РАЗРАБОТКА СЕРВЕРНОГО ПРОГРАММНОГО СРЕДСТВА

Лазовский И.А.

Белорусский государственный университет информатики и радиоэлектроники г. Минск, Республика Беларусь

Томильчик Ю.В.

Аннотация. В работе представлена серверная часть веб-приложения для автоматизации управления физической подготовкой курсантов военных учебных заведений. Разработанное программное средство обеспечивает автоматический расчет оценок по нормативам, ведение дневника тренировок, генерацию отчетов в формате PDF, а также взаимодействие между преподавателями и курсантами через систему сообщений.

Современные подходы к организации физической подготовки в военных учебных заведениях требуют внедрения автоматизированных решений для повышения эффективности контроля и анализа результатов. В работе рассматривается серверная часть веб-приложения, реализующая функции учёта тренировочного процесса, автоматизированной оценки выполнения нормативов, генерации отчётной документации и обеспечения коммуникации между участниками образовательного процесса.

В современных условиях модернизации системы военного образования особое внимание уделяется вопросам физической подготовки курсантов. Существующие методы учета и контроля результатов сдачи нормативов, ведения тренировочного процесса и взаимодействия между преподавателями и курсантами зачастую не автоматизированы, что приводит к увеличению временных затрат и снижению эффективности управления. В связи с этим разработка программного средства, позволяющего автоматизировать данные процессы, является актуальной задачей.

В ходе выполнения работы разработана серверная часть веб-приложения, реализующая следующие основные функции:

– аутентификация и авторизация пользователей с использованием JWT-токенов с разграничением ролей «преподаватель» и «курсант»;

– управление нормативами физической подготовки с автоматическим расчетом итоговых оценок по трем упражнениям с учетом курса обучения;

– ведение дневника тренировок.

– генерация отчетов в формате PDF с графиками динамики веса и прогресса по упражнениям с использованием библиотек JFreeChart и iTextPDF;

– система обмена сообщениями между преподавателями и курсантами с отслеживанием статуса прочтения;

– публикация и поиск статей по тематике спорта, медицины и физиологии;

– интеграция с облачным хранилищем для загрузки изображений;

– безопасное хранение информации в базе данных PostgreSQL.

Архитектура разработанного программного средства построена с использованием следующих технологий: язык программирования Java 24, фреймворк Spring Boot 3.4 (Spring Security, Spring Data JPA), база данных PostgreSQL 17, система сборки Maven, контейнеризация с помощью Docker. Для обеспечения надежности работы системы разработан комплекс тестов с использованием JUnit 5 и Mockito. Общее количество тестов превышает 200, что обеспечивает высокое покрытие кода. Контейнеризация позволяет быстро развернуть приложение на любом сервере без дополнительной настройки окружения.

Разработанное программное средство позволяет автоматизировать процессы контроля и оценки физической подготовки курсантов, сократить временные затраты преподавателей на обработку результатов, повысить наглядность и достоверность отчетных данных, обеспечить оперативное взаимодействие между участниками образовательного процесса. Применение современных технологий и контейнеризации гарантирует надежность работы системы и простоту ее внедрения в учебный процесс. Дальнейшее развитие системы предполагает интеграцию с существующими информационными системами военных учебных заведений, разработку клиентских приложений, а также внедрение системы для автоматизации планирования тренировочного процесса на основе анализа индивидуальных показателей курсантов.

Список использованных источников:

1. Spring Boot Documentation [Электронный ресурс]. – Электронные данные. – Режим доступа: https://docs.spring.io/spring-boot/docs/current/reference/html/. – Дата доступа: 25.03.2026.

2. PostgreSQL: The World's Most Advanced Open Source Relational Database [Электронный ресурс]. – Электронные данные. – Режим доступа: https://www.postgresql.org/docs/. – Дата доступа: 25.03.2026.

ВАЖНОСТЬ АТВТОМАТИЗАЦИИ ПРОЦЕССА ТЕСТИРОВАНИЯ ВОЕННОСЛУЖЕЩИХ ВООРУЖЕННЫХ СИЛ РЕСПУБЛИКИ БЕЛАРУСЬ

Пучков Е.С.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Стогначев Р.В.

Аннотация. В работе обоснована необходимость автоматизации процесса тестирования военнослужащих Вооруженных Силах Республики Беларусь и представлена архитектура разрабатываемого веб-приложения, обеспечивающего автоматизацию тестирования. Создаваемое программное средство позволяет реализовать полный цикл автоматизированного контроля знаний общевоинских уставов.

Поддержание высокой воинской дисциплины и безусловное знание общевоинских уставов (далее — ОВУ) является основой боеготовности и повседневной деятельности Вооруженных Сил Республики Беларусь. В настоящее время контроль знаний уставных норм в подразделениях осуществляется преимущественно в форме устных опросов и письменных контрольных работ. Данный подход обладает рядом системных недостатков: высокая трудоемкость для командиров (подготовка вопросов, проверка, учет), неизбежная субъективность оценки, отсутствие единой централизованной базы результатов и невозможность оперативного анализа типовых ошибок личного состава. Всё это в совокупности снижает эффективность контроля знаний и создает предпосылки для формального подхода к уставной подготовке.

Актуальность и практическая значимость автоматизации процесса тестирования обусловлена следующими факторами. Во-первых, цифровая трансформация системы военного образования Республики Беларусь требует внедрения современных электронных средств обучения и контроля. Во-вторых, значительный объем уставных материалов (Устав внутренней службы, Дисциплинарный устав, Устав гарнизонной и караульной служб) объективно затрудняет регулярную проверку знаний традиционными методами. В-третьих, автоматизация позволяет обеспечить объективность оценки: алгоритмизированная проверка ответов исключает «человеческий фактор» и гарантирует единые критерии для всех тестируемых. В-четвертых, снижается нагрузка на командиров — формирование отчетности и ведомостей успеваемости происходит автоматически, высвобождая время для непосредственной работы с личным составом.Для обоснования важности автоматизации в рамках дипломной работы решаются следующие задачи: анализ текущих проблем при проведении устных и письменных опросов по ОВУ; сравнение трудозатрат командиров при традиционном и автоматизированном контроле знаний; разработка действующего образца приложения как инструмента реализации автоматизации; оценка потенциального повышения объективности, оперативности и регулярности тестирования. Приложение проектируется кроссплатформенным (Windows / Android) с функциями администратора, преподавателя и обучаемого. Оно включает базу данных вопросов с разбивкой по уставам и темам, модуль аутентификации с разграничением ролей, алгоритмы случайной выборки вопросов и ограничения времени ответа, панель администратора для добавления и редактирования вопросов без изменения программного кода, а также модуль аналитики для отслеживания успеваемости и типичных ошибок.

Ожидаемый эффект от внедрения автоматизированного тестирования (на примере разработанного приложения) заключается в следующем: сокращение времени проверки знаний одного военнослужащего с 15–20 минут до 3–5 минут; исключение субъективизма при оценке ответов; централизованный сбор статистики по подразделению и возможность ее анализа в динамике; снижение бумажного документооборота; повышение регулярности контроля знаний за счет уменьшения нагрузки на командиров. Кроме того, приложение генерирует индивидуальные сертификаты о прохождении теста, ведет журнал результатов с возможностью экспорта в Excel и PDF, а также обеспечивает автономную работу без постоянного подключения к сети Интернет, что критически важно для использования в полевых условиях.

Значение для войсковой практики состоит в том, что доказанная важность автоматизации обосновывает необходимость тиражирования подобных решений в учебных центрах, на сборах и в повседневной деятельности подразделений. Разработанное приложение не требует специальных вычислительных мощностей и может быть установлено на планшеты ком андиров взводов и рот. Перспективой дальнейшего развития является интеграция с системой электронного документооборота Министерства обороны Республики Беларусь.

Список использованных источников:

1. Общевоинские уставы Вооруженных Сил Республики Беларусь [Электронный ресурс]. – Электронные данные. – Режим доступа: https://elib.grsu.by/doc/90810. – Дата доступа: 31.03.2026.

2. ЭТАЛОН-ONLINE : мобильное приложение для доступа к законодательству Республики Беларусь [Электронный ресурс]. – Режим доступа: https://etalonline.by – Дата доступа: 31.03.2026.

ВЛИЯНИЕ СПОРТИВНЫХ ИГР НА СПЛОЧЕНИЕ ВОИНСКОГО КОЛЛЕКТИВА

Рысев А.Д., Сиваков В.Л., Янович А.В.

Белорусский государственный университет информатики и радиоэлектроники г. Минск, Республика Беларусь

Хомчик Д.Н.

Аннотация. В работе рассматривается то, как физическая подготовка помогает создать нормальную психологическую обстановку среди военнослужащих. Мы изучили военную педагогику и поняли, как именно навыки из командных игр переносятся на реальные учебно–боевые задачи. Главный вывод: спортивная площадка отлично снимает напряжение в коллективе, убирает лишние барьеры между сослуживцами и делает подразделение по–настоящему единым.

Служба в современных вооружённых силах становится все сложнее. Это связано не только с тем, что в войска поступает новая техника, которую нужно быстро осваивать, но и с огромной психологической и умственной нагрузкой на каждого солдата. Как пишет А.Г. Маклаков в своих трудах по военной психологии, успех любой учебно–боевой задачи очень сильно зависит от того, насколько дружен коллектив и какая атмосфера в нем царит [1]. Солдаты живут по строгому уставу, постоянно подчиняются приказам командиров, находятся в замкнутом пространстве друг с другом и испытывают сильное информационное давление. Если с этим ничего не делать, возникает сильное разочарование и напряжение, что неминуемо приводит к скрытым или даже открытым ссорам между сослуживцами. В нашей современной системе воспитания и физподготовки таким отличным инструментом неформального сплочения стали обычные командные игры, такие как волейбол, а также различные военизированные эстафеты. Если тяжёлая атлетика или гимнастика развивают солдата только индивидуально, то любая игровая дисциплина заставляет всю группу работать как единый механизм.

По мнению А.Г. Караяни, настоящая боевая слаженность строится на глубоком доверии [2]. Солдаты должны уметь сопереживать и понимать друг друга без лишних слов. Влияние таких игр на воинский коллектив происходит через несколько важных механизмов. Во–первых, любая командная игра — это постоянная мини–модель экстремальной ситуации. На поле присутствуют все ключевые элементы настоящего общевойскового боя: у команды всегда есть общая цель, ради которой все собрались, им активно и совершенно непредсказуемо мешает противник, а самим игрокам нужно грамотно распределить между собой роли. При этом обстановка меняется очень быстро, и реагировать на неё нужно мгновенно. Благодаря такому опыту у военнослужащих на уровне мышечной памяти закрепляется привычка помогать товарищу и они начинают чувствовать коллективную ответственность за общий результат.

Во–вторых, во время спортивного матча солдаты активно учатся невербальному общению. В высокой динамике игры часто просто некогда кричать и договариваться словами. Поэтому бойцы начинают интуитивно понимать планы друг друга по языку тела. Они считывают направление взгляда, замечают мелкие движения и следят за тем, как товарищ перемещается по площадке. Как отмечается в профильных учебниках по теории и организации физической подготовки войск, этот специфический навык потом буквально спасает жизни в реальном современном бою [3].

В–третьих, спорт даёт бойцам мощнейшую эмоциональную разрядку и помогает гасить назревающие конфликты ещё в зародыше. Когда человек переносит интенсивную физическую нагрузку и одновременно соревнуется, у него падает уровень гормонов стресса, а нервная система отдыхает и сбрасывает напряжение. Совместные эмоции от сильного спортивного азарта, переживания из–за поражений и общая радость от побед сближают людей.

Кроме того, командный спорт отлично выявляет настоящих лидеров в коллективе. В игре сразу видно, кто из бойцов способен сохранять холодную голову в критической ситуации и может взять на себя ответственность за всю группу. Для командира простое наблюдение за игрой своих подчинённых — это отличный неформальный метод оценки коллектива, который помогает ему безошибочно подбирать лучших кандидатов на должности сержантов. Таким образом, игры выступают тем самым катализатором, который превращает просто формальную и разрозненную группу людей в единый коллектив. Если регулярно включать такие игры в плотное расписание занятий, командиры смогут напрямую управлять морально–психологическим климатом, снижать риск нарушений дисциплины и серьёзно повышать общую боевую готовность своего подразделения.

Список использованных источников:

1. Маклаков, А. Г. Военная психология : учебник для вузов / А. Г. Маклаков. – СПб. : Питер, 2005. – 464 с.

2. Караяни, А. Г. Прикладная военная психология : учебник и практикум для вузов / А. Г. Караяни, И. В. Сыромятников. – М. : Издательство Юрайт, 2023. – 390 с.

3. Теория и организация физической подготовки войск : учебник / под ред. В. В. Миронова. – СПб. : Военный институт физической культуры, 2014. – 435 с.

УСТРОЙСТВО ДИАГНОСТИКИ СОСТОЯНИЯ АККУМУЛЯТОРНЫХ БАТАРЕЙ НОСИМЫХ РАДИОСТАНЦИЙ

Алексеенко А.Д.

Белорусский государственный университет информатики и радиоэлектроники, г. Минск, Республика Беларусь

Федоренко В.А.

Аннотация. В системах радиосвязи широкое применение находят носимые радиостанции, работающие от аккумуляторных батарей (АКБ). Отказ батареи в критический момент приводит к потере связи и снижает эффективность выполнения задач, однако существующие методы контроля (измерение напряжения, встроенные индикаторы) не позволяют достоверно оценить реальное состояние АКБ — степень износа, внутреннее сопротивление, остаточную ёмкость. В связи с этим актуальной является разработка автономного устройства экспресс-диагностики, пригодного для использования в полевых условиях.

В работе предложено и экспериментально исследовано портативное устройство для оценки технического состояния аккумуляторных батарей носимых радиостанций на основе измерения их электрических параметров под нагрузкой. В отличие от штатных индикаторов радиостанций, оценивающих лишь напряжение без тока, разработанное устройство позволяет выявить скрытые дефекты и реальный износ батареи. Устройство построено на микроконтроллерной платформе с возможностью подключения сменных адаптеров для различных типов АКБ (Li-Ion, Ni-MH). В качестве нагрузочных элементов используются мощные полевые транзисторы в линейном режиме и прецизионные шунты, что обеспечивает стабильность тока разряда независимо от степени разряда батареи. Диагностика выполняется в три этапа: измерение напряжения холостого хода; измерение внутреннего сопротивления методом двух нагрузок (по падению напряжения при скачке тока); оценка фактической ёмкости методом контрольного разряда стабилизированным током до уровня отсечки. Для повышения точности измерения внутреннего сопротивления предусмотрена цифровая фильтрация результатов и усреднение по нескольким циклам подключения нагрузки. Управление нагрузочными элементами, сбор данных и их обработка осуществляются микроконтроллером STM32. Использование 12-разрядного АЦП и встроенного эталона напряжения позволяет минимизировать инструментальную погрешность. Результаты отображаются на графическом дисплее и могут сохраняться во внутреннюю энергонезависимую память, а для оценки состояния используется сравнение измеренных параметров с паспортными значениями и с результатами предыдущих тестов. Дополнительно устройство оснащено интерфейсом для передачи данных на внешний компьютер, что даёт возможность формировать журнал эксплуатации аккумуляторного парка [1].

Изготовлен опытный образец устройства, проведены испытания на группе аккумуляторных батарей (7,4 В, Li-Ion) с различным сроком эксплуатации. Испытания включали как новые батареи, так и образцы с явным снижением ёмкости после 300–500 циклов заряда-разряда. Установлено, что погрешность измерения внутреннего сопротивления не превышает 5 % по сравнению с эталонным измерителем; оценка остаточной ёмкости сходится с данными специализированного зарядного устройства в пределах ±8 %; время полного цикла диагностики (включая разряд) не превышает 30 минут для батарей ёмкостью до 3000 мА·ч. Воспроизводимость результатов при повторных измерениях одной и той же батареи составила не хуже 3 %, что подтверждает стабильность работы устройства. Для интерпретации результатов разработана светодиодная индикация: зелёный цвет соответствует состоянию «отлично» (ресурс более 80 %), жёлтый — «удовлетворительно» (50–80 %), красный — «требуется замена» (менее 50 %). Данная система индикации позволяет оператору принимать решение о дальнейшем использовании батареи без необходимости расшифровки числовых значений [2].

Таким образом, созданное устройство позволяет оперативно и достоверно оценивать состояние аккумуляторных батарей носимых радиостанций, что способствует повышению надёжности радиосвязи, оптимизации парка аккумуляторов и сокращению внезапных отказов. Применение предложенного устройства в подразделениях связи позволяет перейти от плановых замены аккумуляторов к обслуживанию по фактическому состоянию, что даёт экономический эффект за счёт продления срока службы исправных батарей. Автономность, малые габариты и простота использования делают его пригодным для эксплуатации в условиях ремонтных мастерских и выездных бригад.

Список использованных источников.

1. Томилов, С. Испытатель аккумуляторных батарей портативных радиостанций [Текст] / С. Томилов // Радио. – 2015. – № 2. – С. 31–32.

2. Борисов, П. В. Исследование характеристик литий-ионной аккумуляторной батареи [Текст] / П. В. Борисов, А. А. Воробьев, К. В. Константинов и др. // Известия Петербургского университета путей сообщения. – 2023. – Т. 20, вып. 1. – С. 207–221.

ПОРТАТИВНОЕ УСТРОЙСТВО ДЛЯ ОБНАРУЖЕНИЯ РАДИОЧАСТОТНОЙ АКТИВНОСТИ

Бузинчик Е.В.

Белорусский государственный университет информатики и радиоэлектроники г. Минск, Республика Беларусь

Дудак М.Н.

Аннотация. Представлено портативное устройство для обнаружения радиочастотной активности, предназначенное для выявления источников радиоизлучения в тактических условиях. Устройство обеспечивает сканирование частотного диапазона 2,4–2,5 ГГц, визуальную и звуковую индикацию уровня сигнала, а также возможность скрытного применения. Разработка ориентирована на оснащение подразделений специального назначения, разведывательных групп и тактических подразделений.

Обнаружение источников радиочастотного излучения становится критически важной задачей в условиях современного ведения боевых действий, где противник активно использует носимые радиостанции, средства дистанционного подрыва взрывных устройств, каналы управления беспилотными летательными аппаратами и радиозакладки. Существующие на рынке профессиональные анализаторы спектра обладают высокой стоимостью, значительными массогабаритными характеристиками и недостаточным временем автономной работы, что делает их непригодными для массового оснащения подразделений, действующих в пешем порядке. Специализированные детекторы, в свою очередь, имеют узкую направленность и закрытую архитектуру, исключающую возможность адаптации под новые угрозы.

Разрабатываемое портативное устройство предназначено для непрерывного мониторинга радиочастотной обстановки и оперативного оповещения оператора о появлении источников излучения. Функционал включает сканирование частотного диапазона 2,4–2,5 ГГц с последовательным анализом всех доступных каналов, измерение уровня принимаемого сигнала (RSSI), цифровую и графическую индикацию на OLED-дисплее, а также звуковую сигнализацию с возможностью отключения для скрытного применения. Внедрение такого устройства позволит повысить ситуационную осведомленность личного состава, сократить время реакции на угрозы и снизить зависимость от дорогостоящего импортного оборудования.

Устройство подходит для использования всеми категориями военнослужащих, нуждающихся в средствах индивидуального радиоконтроля, а также может применяться в образовательных целях для изучения принципов радиомониторинга. Разработка нацелена на обеспечение доступным, легким и автономным средством обнаружения радиочастотной активности.

Конструкция устройства построена на базе микроконтроллера ESP32, обладающего встроенным Wi-Fi модулем, что позволяет осуществлять сканирование без применения дополнительных радиомодулей. Управление осуществляется с помощью двух тумблеров: включения питания и отключения звуковой сигнализации. Визуализация информации обеспечивается OLED-дисплеем с разрешением 128×64 пикселей. Питание устройства осуществляется от литий-ионного аккумулятора типоразмера 18650, обеспечивающего длительное время автономной работы, а зарядка реализована через плату TP4056 с защитой от перезаряда и переразряда. Для преобразования напряжения аккумулятора (3,7 В) в стабильные 5 В используется повышающий преобразователь MT3608. Все компоненты размещены в корпусе, изготовленном методом 3D-печати из пластика, что обеспечивает минимальное затухание сигнала и компактность.

Программное обеспечение разработано в среде Arduino IDE на языке C++ с использованием библиотек для работы с Wi-Fi модулем и OLED-дисплеем. Алгоритм работы устройства предусматривает непрерывное сканирование частотного диапазона, обработку измеренных значений RSSI, формирование визуальной и звуковой индикации, а также контроль уровня заряда аккумулятора. Пороговое значение срабатывания может быть изменено программно, что позволяет адаптировать устройство под различные условия применения.

Таким образом, разрабатываемое портативное устройство не только решает актуальные задачи обнаружения радиочастотной активности, но и обладает критически важными для тактического применения характеристиками: малой массой (менее 200 г), длительным временем автономной работы (до 12 часов), крайне низкой себестоимостью (около 150 BYN) и открытой архитектурой, допускающей оперативную адаптацию под новые угрозы. Его внедрение позволит существенно повысить эффективность радиоконтроля в подразделениях, обеспечив каждого военнослужащего доступным и надежным средством обнаружения источников радиоизлучения.

Список использованных источников:

1. Masaki Kitsunezuka et al., "A 30-MHz–2.4-GHz CMOS Receiver With Integrated RF Filter and Dynamic-Range-Scalable Energy Detector", IEEE Journal of Solid-State Circuits, 2012. – P. 160-185.

ПРОГРАММНЫЙ КОМПЛЕКС ВИЗУАЛИЗАЦИИ И КОНТРОЛЯ ЗНАНИЙ ПРИ ИЗУЧЕНИИ РРС Р-409МБ1

Мисько А.А

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Викторович М.А.

Аннотация. В статье рассматривается проблема визуализации и доступности обучения при изучении сложного телекоммуникационного оборудования на примере радиорелейной станции Р-409МБ1. Актуальность разработки обусловлена необходимостью повышения наглядности учебного материала и возможности самостоятельного изучения конструкции станции без постоянного доступа к физическому образцу.

Современный этап развития профессионального образования характеризуется активным внедрением информационных технологий в учебный процесс. Особую актуальность это приобретает при подготовке специалистов в области телекоммуникаций и радиосвязи, где объектами изучения выступают сложные технические комплексы [1]. Радиорелейная станция Р-409МБ1 является важным элементом систем связи, однако её изучение сопряжено с рядом трудностей. Высокая стоимость оборудования, габариты станции, а также ограниченный ресурс реальных образцов затрудняют доступ обучающихся к материальной части. Кроме того, работа с действующей аппаратурой требует соблюдения строгих мер безопасности, что не всегда возможно в условиях учебной аудитории [3]. В связи с этим возникает потребность в создании программных средств, позволяющих визуализировать учебный материал и обеспечить возможность самостоятельного изучения конструкции станции без постоянного доступа к физическому образцу.

Целью данной работы являлась разработка компьютерной программы, направленной на повышение наглядности и эффективности обучения эксплуатации Р-409МБ1. Разработанный программный комплекс представляет собой интерактивную среду, объединяющую теоретические сведения и практические инструменты отработки навыков.

Архитектура программы построена модульно и включает три ключевых компонента. Первый модуль — информационно-теоретический. Он содержит структурированный учебный материал, описывающий тактико-технические характеристики, принцип работы и состав станции. Особенностью модуля является насыщенность контентом визуальными элементами: схемами блоков, фотографиями элементов конструкции. Это позволяет облегчить восприятие сложной технической информации и снижает когнитивную нагрузку на обучающегося.

Второй модуль — «Виртуальная экскурсия». Данный раздел реализует функцию интерактивного ознакомления со станцией. Пользователь имеет возможность визуально осмотреть станцию, изучить расположение органов управления и коммутации. Такой формат имитирует присутствие на реальном объекте, позволяя запомнить пространственную компоновку оборудования, что критически важно для будущей эксплуатационной деятельности.

Третий модуль — контрольно-оценочный. Он предназначен для закрепления изученного материала и включает систему тестовых заданий. Программа автоматически проверяет ответы, фиксирует ошибки. Это обеспечивает объективный мониторинг знаний и позволяет обучающемуся самостоятельно отслеживать свой прогресс [4].

Внедрение разработанного программного комплекса в учебный процесс позволяет решить проблему дефицита наглядных пособий. Использование программы способствует интенсификации подготовки специалистов: сокращается время на изучение материальной части, повышается безопасность тренировок (исключается риск повреждения оборудования или поражения током на начальном этапе) и обеспечивается возможность дистанционного обучения [3].

Таким образом, созданная компьютерная программа является эффективным инструментом поддержки обучения. Она сочетает в себе функции справочника, тренажера и средства контроля знаний. Дальнейшее развитие проекта может быть связано с добавлением режимов симуляции неисправностей и расширением базы интерактивных моделей для других типов радиорелейных станций.

Список использованных источников:

1. Савчик П.А. Применение электронных тренажеров в образовательном процессе // Доклады БГУИР. – 2016. – № 4 (98). – С. 89–95.

2. Русак Е.Д. Применение виртуальных тренажеров при обучении специалистов связи // Материалы международной научно-технической конференции. – Минск: БГУИР, 2019. – С. 112–115.

3. Утин Л.Л., Козлов А.В., Петрович Д.С. Цифровые радиорелейные станции полевых узлов связи: учебно-методическое пособие. – Минск: БГУИР, 2017. – 104 с.

4. Карпов Ю.Г. Имитационное моделирование систем. Введение в моделирование с AnyLogic 5. – Санкт-Петербург: БХВ-Петербург, 2005. – 336 с.

УДК 621.396.4 – 004.58(075.8)

ВИРТУАЛЬНАЯ ЭКСКУРСИЯ ПО ЦИФРОВОЙ ТРОПОСФЕРНОЙ СТАНЦИИ Р-432 КАК ЭЛЕМЕНТ ФОРМИРОВАНИЯ ПРОСТРАНСТВЕННОГО ПРЕДСТАВЛЕНИЯ ОБ ОБОРУДОВАНИИ

Зелинский И.А., студент гр.233701

Белорусский государственный университет информатики и радиоэлектроники г. Минск, Республика Беларусь

Игнатенко А.А.

Аннотация. В статье анализируется методика использования виртуальной экскурсии в качестве педагогического инструмента, направленного на формирование у курсантов пространственного представления о компоновке и расположении оборудования цифровой тропосферной станции Р-432 «Горизонт». Аргументируется важность создания у обучающихся целостного пространственного образа станции на этапе теоретической подготовки, что выступает предпосылкой для успешного приобретения практических навыков эксплуатации. Описывается структура виртуальной экскурсии, которая включает интерактивную 3D-модель станции, предоставляющую возможность свободного перемещения по отсекам, а также подробного изучения блоков оборудования. В качестве дополнения представлены результаты апробации данного подхода в учебном процессе Военной академии Республики Беларусь, свидетельствующие о росте эффективности усвоения материала.

Ключевые слова. Цифровая тропосферная станция Р-432, виртуальная экскурсия, пространственное представление, компоновка оборудования, интерактивное 3D-моделирование, компьютерный тренажёр, подготовка операторов средств связи.

Введение. Формирование у будущих операторов средств связи комплексного понимания компоновки и взаимного расположения элементов оборудования тропосферных станций представляет собой одну из основных задач педагогического процесса на этапе теоретической подготовки. Отсутствие ясного пространственного образа станции негативно отражается на последующем овладении практическими навыками эксплуатации, что проявляется в увеличении времени поиска необходимых управляющих блоков, возникновении ошибок при коммутации трактов и снижении эффективности функционирования в условиях повышенной психологической нагрузки. Традиционные методы обучения, основанные на изучении статичных схем и фотографий оборудования, оказываются недостаточными для формирования устойчивого трёхмерного восприятия сложной архитектуры современных тропосферных станций. Использование виртуальной экскурсии в качестве педагогического инструмента позволяет частично нивелировать перечисленные ограничения за счёт создания интерактивной трёхмерной модели станции. При этом обучающиеся способны свободно перемещаться между отсеками, подробно изучать оборудование с различных точек обзора и визуализировать взаимосвязи между функциональными блоками. Настоящее исследование направлено на разработку и обоснование методики применения виртуальных экскурсий для формирования пространственного представления об устройстве и его элементах. В качестве примера показан опытный образец виртуальной экскурсии (рисунок 1).

Рисунок 1 – Начальный экран виртуальной экскурсии

Основная часть. Компоновка оборудования станции Р-432 обусловлена рядом технических и эксплуатационных требований. Передний отсек выделен под размещение стойки усилителей мощности (УМ) вследствие необходимости интенсивного охлаждения данных блоков и высокого уровня шума, создаваемого системой принудительной вентиляции. Размещение стойки УМ в отдельном отсеке обеспечивает комфортные условия работы оператора в среднем отсеке, где расположено основное оборудование управления [1].

Средний отсек станции содержит две стойки телекоммуникационного оборудования. В стойке № 1 размещены блоки управления антенной (БУА 1 и БУА 2), блоки дуплексера (БД 1 и БД 2), блоки модема (БМ 1 и БМ 2), абонентский кросс (АК), блоки сетевой служебной связи (БССС) и блок интерфейсов (БИ). В стойке № 2 установлены блоки приемопередатчика (БПП 1 и БПП 2), блоки питания УМ (БПУМ 1 и БПУМ 2), кросс сигналов промежуточной частоты (КПЧ) с анализатором спектра, блок опорного генератора (БОГ), блоки SDSL (1 и 2), оборудование центрального мониторинга (ЦЭВМ) и моноблок KVM-1701 [1].

Такая компоновка создаёт определённые сложности при обучении:

– Необходимость запоминания расположения более 20 основных блоков оборудования в трёхмерном пространстве;

– Понимание взаимосвязей между блоками, расположенными в разных стойках и отсеках;

– Освоение логики коммутации трактов сигналов между блоками;

– Формирование навыка быстрого поиска необходимого блока в условиях ограниченного времени.

Традиционные методы обучения (изучение плоских схем компоновки) не позволяют эффективно решить эти задачи, поскольку человек воспринимает пространственную информацию преимущественно через визуализацию и интерактивное взаимодействие с объектом.

Разработанная виртуальная экскурсия представляет собой интерактивную Virtual Tour-модель станции Р-432, реализованную в приложении Pano2VR Pro 7.1.9 с добавлением некоторых режимов через игровой движок Unity, с применением технологий визуализации реального времени. Экскурсия включает три основных режима взаимодействия:

Режим «Свободное перемещение» позволяет курсанту самостоятельно перемещаться по виртуальной модели станции, изучая оборудование в произвольном порядке. Перемещение осуществляется с помощью клавиатуры и мыши с возможностью изменения точки обзора. При приближении к любому блоку оборудования автоматически отображается его название и краткое назначение. Щелчок левой кнопкой мыши вызывает подробное описание блока с указанием технических характеристик, габаритных размеров и массы.

Режим «Обучение» представляет собой структурированный маршрут, автоматически ведущий курсанта по заранее определённой траектории. Экскурсия начинается с общего обзора станции снаружи, затем переходит к изучению переднего отсека (стойка УМ), среднего отсека (стойки № 1 и № 2) и завершается обзором заднего отсека. На каждом этапе система предоставляет аудио- и текстовое сопровождение с описанием назначения отсека и размещённого в нём оборудования.

Режим «Тестирование» активируется после завершения режима обучения и представляет собой интерактивный опросник. Система задаёт вопросы типа: «Укажите расположение блока опорного генератора ТСО-1701», «Какой блок отвечает за управление антенной?», «В каком отсеке размещена стойка усилителей мощности?». Курсант должен указать правильный элемент на 3D-модели станции. Результаты тестирования фиксируются в журнале обучения для последующего анализа преподавателем.

Методика применения виртуальной экскурсии в учебном процессе включает три этапа:

Этап 1. Формирование общего представления. Курсанты проходят режим «Обучение» под руководством преподавателя. Преподаватель акцентирует внимание на логике компоновки станции, объясняя причины размещения оборудования в том или ином отсеке. Особое внимание уделяется взаимосвязям между блоками: например, объясняется, почему блоки модема и приемопередатчика размещены в разных стойках, но соединены коаксиальными кабелями через кросс ПЧ.

Этап 2. Детализированное изучение. Курсанты самостоятельно работают в режиме «Свободное перемещение», изучая каждый блок оборудования. Для каждого блока необходимо:

– Определить его местоположение в станции (отсек, стойка, ярус);

– Изучить внешний вид передней и задней панелей;

– Ознакомиться с техническими характеристиками;

– Проследить тракты прохождения сигналов к смежным блокам.

Этап 3. Закрепление и контроль. Данный этап представляет собой систему последовательных заданий, направленных на автоматизацию пространственного представления и проверку его устойчивости. Главным звеном этапа является комплексное тестирование включающее в себя 20 вопросов трёх типов:

– Прямые вопросы на знание расположения («Где находится блок опорного генератора?»);

– Ситуационные задачи («Укажите кратчайший маршрут от рабочего места оператора к контрольной точке»);

– Вопросы на понимание логики компоновки («Почему стойка усилителей мощности размещена в отдельном отсеке?»).

Для успешного завершения этапа необходимо правильно ответить не менее чем на 85 % вопросов. При невыполнении норматива система автоматически формирует индивидуальный план повторения, включающий повторное прохождение режима «Обучение» с акцентом на проблемные зоны и дополнительные задания в режиме «Свободное перемещение».

Методика обеспечивает поэтапное формирование пространственного представления: от общего обзора к детализированному изучению и завершая автоматизацией навыка ориентирования в трёхмерном пространстве станции. Каждый этап строится на результатах предыдущего, что обеспечивает непрерывность и системность процесса обучения.

Заключение. Разработанная виртуальная экскурсия по цифровой тропосферной станции Р-432 представляет собой эффективный педагогический инструмент для формирования у курсантов пространственного представления о компоновке и расположении оборудования. Методика применения экскурсии, включающая три последовательных этапа обеспечивает системный подход к освоению материала.

Преимущества виртуальной экскурсии перед традиционными методами обучения:

– Формирование целостного трёхмерного образа станции вместо фрагментарного запоминания отдельных элементов;

– Возможность интерактивного взаимодействия с моделью, что соответствует естественному способу восприятия пространственной информации человеком;

– Визуализация невидимых связей между блоками (трактов прохождения сигналов);

Виртуальная экскурсия будет интегрирована в состав компьютерного тренажёра станции Р-432 как самостоятельный модуль теоретической подготовки и рекомендована к применению в учебном процессе военных вузов Республики Беларусь при подготовке специалистов по эксплуатации тропосферных станций. Дальнейшее развитие методики предполагает интеграцию элементов дополненной реальности (AR) для наложения виртуальной информации на реальное оборудование при проведении практических занятий.

Список использованных источников:

1. Руководство по эксплуатации цифровой тропосферной станции Р-432. – Минск: АГАТ – системы управления, 2021.–248 с.

2. Бысов, А.А. Цифровая тропосферная станция Р-432 : учеб. пособие / А.А. Бысов, А.А. Пилюшко, В.В. Пискун [и др.].–Минск : ВА РБ, 2023.–172 с.

3. Серов, В.В. Частотно-энергетическая эффективность цифровых систем тропосферной связи / В.В. Серов–М.: Горячая линия – Телеком, 2002.–307 с.

4. Нарытник, Т.Н. Радиорелейные и тропосферные системы передачи: учеб. пособие / Т.Н. Нарытник, В.В. Волков, Ю.В. Уткин – Киев: Основа, 2008.–696 с.

5. Пискун, В.В. Анализ эффективности применения пространственно-временного кодирования в военных цифровых системах тропосферной связи / В.В. Пискун, О.В. Шидо // Веснік Сувязі.–2019.–№ 6.–С. 52–56.

6. Белоусов, А.С. Применение технологий виртуальной реальности в подготовке специалистов радиотехнических войск / А.С. Белоусов, Д.В. Соколов // Военная мысль–2022.–№ 4.–С. 112–119.

7. Козлов, Д.И. Тренажёр для станции Р-423АМ: опыт разработки и внедрения / Д.И. Козлов // Вестник связи–2019.–№ 5.–С. 34–41.

8. Международный союз электросвязи. Рекомендация Р.617-3 «Методы прогнозирования и данные о распространении радиоволн, необходимые для проектирования тропосферных радиорелейных систем» [Электронный ресурс]. – Женева : МСЭ, 2013. – Режим доступа: https://www.itu.int/rec/R-REC-P.617 (дата обращения: 15.03.2026).

9. Официальный сайт ВА РБ [Электронный ресурс].– Режим доступа: https://va.mil.by (дата обращения: 10.03.2026)..

UDC 621.396.4 – 004.58(075.8)

VIRTUAL TOUR OF THE DIGITAL TROPOSPHERIC STATION R-432 AS AN ELEMENT OF SPATIAL REPRESENTATION OF EQUIPMENT

Zelinskiy I.A.[1]

Belarusian State University of Informatics and Radioelectronics[1]*, Minsk, Republic of Belarus*

Ignatenco A.A. – lecturer of the department of communications

Annotation. The article analyzes the technique of using a virtual excursion as a pedagogical tool aimed at forming a spatial idea of the layout and location of the equipment of the digital troposphere station of the Horizon R-432 among cadets. The importance of creating a holistic spatial image of the station at the stage of theoretical training is argued, which is a prerequisite for the successful acquisition of practical operating skills. The structure of the virtual tour is described, which includes an interactive 3D model of the station, which provides the ability to freely move around the compartments, as well as a detailed study of the equipment units. As an addition, the results of testing this approach in the educational process of the Military Academy of the Republic of Belarus are presented, indicating an increase in the effectiveness of material assimilation.

Keywords. Digital troposphere station R-432, virtual tour, spatial representation, equipment layout, interactive 3D modeling, computer simulator, training of telecom operators.

МОДЕЛИРОВАНИЕ ОПЕРАТОРСКИХ ПРОЦЕДУР ТРОПОСФЕРНОЙ СТАНЦИИ Р-412МБ В КОМПЬЮТЕРНОМ ТРЕНАЖЁРЕ

Бегаль Д.С.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Сидоров С.В.

Аннотация. Разработана модель операторских процедур для тренажёра тропосферной станции Р-412МБ. Модель описывает последовательности действий оператора (включая запуск, настройку, приём/передачу и диагностику) в виде удобной для программной реализации машины состояний. Для реалистичности добавлены параметры задержек, шумов и генератор аварийных сценариев с настраиваемой вероятностью. Система автоматически фиксирует действия пользователя, оценивает их по набору критериев (время, правильность последовательности, восстановление после отказа) и выдаёт обратную связь. Ожидаемый эффект — более безопасное, повторяемое и эффективное обучение операторов за счёт реалистичной симуляции и объективной оценки.

Подготовка операторов тропосферных станций требует отработки сложных последовательностей действий в условиях ограниченного времени и возможных отказов оборудования. Традиционные практические занятия с реальными станциями ограничены доступностью техники, безопасностью и износом оборудования. Компьютерный тренажёр предоставляет контролируемую, повторяемую и безопасную среду для формирования навыков операторов при минимальных затратах.

Целью исследования считается разработать и обосновать модель операторских процедур тропосферной станции Р-412МБ для интеграции в компьютерный тренажёр, обеспечивающую репрезентативную имитацию рабочих сценариев, ошибок и отказов, а также объективную оценку действий обучаемых.

Задачи:

1.формализация набора базовых и аварийных операторских процедур (инициализация, установка рабочих параметров, приём/передача, перестройка частоты, диагностика неисправностей, вывод станции в безопасное состояние);

2.разработка архитектуры программного модуля процедур с выделением подсистем сценариев, состояния станции, событий и контроля времени;

3.моделирование задержек, неточностей и отказов аппаратных компонентов с параметризацией вероятностей, и времени восстановления;

4.определение критериев и алгоритмов автоматической оценки правильности выполнения процедур и построения обратной связи.

Для формализации процедур использована иерархическая модель состояний и переходов (state machine), где каждое действие оператора представлено атомарной операцией с предусловиями и постусловиями. Сценарии строятся как композиции операций с возможностью ветвления по результатам проверок и имитаций отказов. Моделирование аппаратных эффектов (задержки установок, погрешности калибровки, шум приёмника) проводится с применением стохастических процессов и параметрических шумовых моделей. Для генерации отказов используется сценарный генератор с настраиваемыми профилями риска (частота, длительность, тип). Оценка действий реализована через правило-базированную систему и метрики времени реакции, последовательности действий и числа корректировок.

Реализация модели позволит:

1.формировать учебные сценарии от типовых рабочих процедур до сложных аварийных случаев;

2.автоматизировать сбор показателей эффективности работы оператора (время, ошибки, восстановление работы);

3.проводить повторяемые тренировки и сравнение прогресса обучаемых.

Формализованная модель операторских процедур, реализованная как отдельный программный модуль тренажёра, существенно повышает качество обучения операторов тропосферных станций за счёт воспроизводимости сценариев, возможности имитации отказов и объективной автоматической оценки. Дальнейшие исследования целесообразно направить на адаптивные сценарии под уровень обучаемого и интеграцию алгоритмов машинного анализа ошибок для персонализированной обратной связи.

Список использованных источников:

1.Романовский С. В., Григоренко С. И., Сасновский А. А. Тропосферная станция Р-412МБ: учебно-методическое пособие. — Минск: БГУИР, 2020. — 112 с. [9]

2.Касании С. Н., Пискун В. В., Богуш В. А. Компьютерные тренажеры средств связи // Современный подход к подготовке военных специалистов. — [Электронный ресурс]. URL: https://libeldoc.bsuir.by/bitstream/123456789/45898/1/Kasanin_Kompyuternyye.pdf

3.Дозорцев В.М. насколько полезны компьютерные тренажеры для обучения операторов // автоматизация в промышленности. — 2016. — № 7. — С. 1-5. [12]

КОНЦЕПТУАЛЬНЫЕ НАПРАВЛЕНИЯ МОДЕРНИЗАЦИИ ИНФОКОММУНИКАЦИОННОЙ ИНФРАСТРУКТУРЫ ВОЙСК СВЯЗИ В УСЛОВИЯХ ТРАНСФОРМАЦИИ ФОРМ И СПОСОБОВ ВЕДЕНИЯ ВООРУЖЕННОЙ БОРЬБЫ

Лабан К.А.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Дудак М.Н.

Аннотация. В работе обоснована необходимость пересмотра подходов к построению инфокоммуникационной инфраструктуры войск связи Вооруженных Сил Республики Беларусь в условиях эволюции форм вооруженной борьбы (массированное применение беспилотных систем, средств радиоэлектронной борьбы, кибероперациий). Предложены концептуальные направления модернизации, включающие переход к программно-конфигурируемым сетям, гибридным транспортным средам, интеллектуальному управлению частотным ресурсом и созданию унифицированных узлов связи с высокой живучестью.

Современные вооруженные конфликты демонстрируют фундаментальные изменения в способах достижения целей: наряду с традиционными огневыми средствами ключевая роль отводится деструктивному воздействию на системы управления, подавлению каналов связи, дезорганизации обмена данными. В таких условиях инфокоммуникационная инфраструктура войск связи превращается из обеспечивающего элемента в непосредственный объект противодействия. Опыт проведения специальной военной операции, учений «Запад-2025» и анализ тенденций развития средств РЭБ показывают, что существующие системы связи, базирующиеся на жесткой архитектуре и аналоговых каналах, не в полной мере отвечают требованиям живучести, скрытности и оперативности управления. Анализ состояния парка средств связи войск связи Республики Беларусь выявил ряд системных противоречий. С одной стороны, ведется плановое переоснащение командно-штабными машинами Р-185 «Эпоха», цифровыми радиорелейными станциями Р-414МБРП «Сосна-2», современными радиостанциями с псевдослучайной перестройкой рабочей частоты (Р-181-50ВУ-2 и др.). С другой стороны, сохраняется фрагментарность применяемых решений, отсутствует единая архитектура управления ресурсами, недостаточно используются возможности программно-конфигурируемых сетей (SDN) и технологий виртуализации для быстрой реконфигурации узлов связи в условиях динамически меняющейся обстановки.

В ходе выполнения работы определены ключевые концептуальные направления модернизации инфокоммуникационной инфраструктуры:

- Гибридизация транспортной среды. Современный узел связи должен одновременно использовать оптоволоконные линии (включая прокладку с помощью БПЛА), цифровые радиорелейные каналы, защищенные спутниковые каналы национальной системы связи и перспективные тропосферные линии. Единая система управления должна обеспечивать автоматический выбор наиболее устойчивого канала без участия оператора.
- Интеллектуализация управления спектром. В условиях плотного радиопротиводействия необходимы алгоритмы когнитивного радио, позволяющие в реальном масштабе времени анализировать электромагнитную обстановку, прогнозировать возможные помехи и перестраивать рабочие частоты, а также применять широкополосные сигналы с повышенной скрытностью.

Реализация предложенных направлений позволит:

- повысить живучесть системы связи за счет многоканальности и динамической реконфигурации;
- сократить время развертывания узлов связи в 2–3 раза за счет автоматизации настройки;
- обеспечить скрытность управления войсками в условиях активного применения противником средств радиоэлектронной разведки и подавления;
- создать технологическую основу для дальнейшего внедрения элементов искусственного интеллекта в процессы управления связью.

Дальнейшие исследования предполагают разработку имитационной модели оценки эффективности перспективной инфраструктуры связи при воздействии комплексов РЭБ, а также создание экспериментального образца программно-аппаратного комплекса на базе отечественных разработок для апробации предложенных решений в войсках связи.

Список использованных источников:

1. Пункты управления и защищённые узлы связи оборудованы в Белоруссии на учениях "Запад-2025" [Электронный ресурс] // Интерфакс. – 2025. – Режим доступа: https://www.interfax.by. – Дата доступа: 01.04.2026.

2. О развитии системы связи Вооруженных Сил Республики Беларусь на 2021–2025 годы: постановление Совета Министров Республики Беларусь, 12 февр. 2021 г., № 84 // Нац. реестр правовых актов Республики Беларусь. – 2021.

3. Бардашевич, А. В. Актуальные вопросы развития инфокоммуникационных систем и услуг в войсках связи Вооруженных Сил Республики Беларусь / А. В. Бардашевич // Инновационные технологии в образовательном процессе: сб. материалов 60-й науч. конф. БГУИР. – Минск, 2024. – С. 12–13.

ПОДВИЖНЫЕ КОМПЛЕКСЫ Р-443О: ВОЗМОЖНОСТИ И ПЕРСПЕКТИВЫ

Ковалевская А.О.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Ермоленко Д.М.

Аннотация. Данный тезис посвящен внедрению подвижных комплексов Р-443О в Вооруженных Силах Республики Беларусь. Описаны перспективы внедрения подвижных комплексов.

В современной системе управления войсками и гражданскими структурами ключевую роль играет возможность организации устойчивой связи в любых условиях обстановки. Одним из эффективных решений для обеспечения высокоскоростной передачи данных являются подвижные станции спутниковой связи [1].

Станции спутниковой связи Р-443О представляют собой современные подвижные средства связи, предназначенные для развертывания и функционирования в полевых условиях. Основная задача данных комплексов заключается в предоставлении цифровых высокоскоростных каналов связи, всего спектра инфокоммуникационных услуг для должностных лиц пунктов управления. Оборудование разработано с учетом необходимости обеспечения надежного управления как в мирное, так и в военное время. Оно способно функционировать в составе узлов связи различных звеньев управления, обеспечивая интеграцию спутниковых каналов с территориальной сетью связи [1].

Линейка Р-443О включает в себя два основных типа станций: узловые и оконечные. Узловая станция, как правило, предназначена для создания центрального узла связи, агрегирующего потоки данных от нескольких абонентов. Она обеспечивает связь через геостационарные космические аппараты в Ku- и C-диапазонах частот.

В Ku-диапазоне станции взаимодействуют с космическими аппаратами связи и вещания гражданского назначения, включая перспективные аппараты сетей широкополосной спутниковой связи. Это обеспечивает возможность высокоскоростной передачи данных для веонных, гражданских и коммерческих задач.

В C-диапазоне реализуется работа с космическими аппаратами военного назначения. Отличительной особенностью данного режима является возможность организации помехозащищенной спутниковой связи для различных звеньев управления. Это обеспечивает устойчивость каналов связи в условиях радиоэлектронного противодействия.

Оконечная станция отличается повышенной мобильностью и предназначена для обеспечения связи непосредственно на пунктах управления. Оба типа станций поддерживают работу как с гражданскими спутниками связи и вещания, так и с аппаратами военного назначения, что позволяет организовывать как открытые, так и помехозащищенные каналы связи.

Ключевой особенностью станций Р-443О является их высокая мобильность и автоматизация процессов развертывания и свертывания. Время развертывания комплекса минимизировано, что позволяет быстро менять дислокацию узлов связи. Для военного сегмента предусмотрена возможность организации помехозащищенных каналов, что обеспечивает устойчивость, непрерывность, оперативность и скрытность управления в условиях радиоэлектронного противодействия [2].

Актуальность данных комплексов подтверждается их регулярной демонстрацией на крупных международных выставках вооружения и военной техники, таких как MILEX-2025. Развитие платформы Р-443О идет в сторону увеличения пропускной способности и совместимости с перспективными спутниками широкополосной связи.

Подвижные станции спутниковой связи Р-443О являются надежным инструментом для организации связи в условиях отсутствия развитой наземной инфраструктуры. Развитие инфокоммуникационных систем в войсках связи Вооруженных Сил Республики Беларусь направлено на создание высокоманевренной, защищенной и устойчивой системы управления. Основные усилия сосредоточены на внедрении отечественных цифровых средств связи, использовании беспилотных платформ для ретрансляции, переходе к кластерным методам развертывания, обеспечивающим высокую живучесть, и совершенствовании средств защиты информации в условиях активного противостояния с высокотехнологичными силами [2].

Список использованных источников:

1. Белспецвнештехника. Навстречу MILEX-2025: Станции спутниковой связи Р-443 [Электронный ресурс]. – Режим доступа: https://bsvt.by/ru/novosti/post/navstrechu-milex-2025-stancii-sputnikovoj-svyazi-r-443. – Дата доступа: 01.04.2026.

2.Центр информационных технологий при Министерстве обороны Республики Беларусь [Электронный ресурс]. — Режим доступа: https://www.mil.by/ru/itcenter/ — Дата доступа: 01.04.2026 г.

УСТРОЙСТВО ДЛЯ СОЗДАНИЯ ИСКУССТВЕННЫХ ПОМЕХ НА ЦИФРОВЫХ И АНАЛОГОВЫХ ПРОВОДНЫХ ЛИНИЯХ СВЯЗИ

Нестерович М.П.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Томильчик Ю.В.

Аннотация. Представлено устройство для создания искусственных помех и имитации неисправностей в аналоговых и цифровых проводных линиях связи, предназначенное для использования в лабораторных стендах, учебном процессе и при предварительных испытаниях аппаратуры связи. Устройство обеспечивает ручную коммутацию нагрузочных сопротивлений (50, 75, 100, 120, 600, 1200 Ом), имитацию обрыва и короткого замыкания линии, а также генерацию активной FSK-помехи на базе микросхемы XR2206 с тремя режимами работы. Разработка ориентирована на повышение наглядности и доступности лабораторных исследований по дисциплинам «Линии связи», «Защита информации», «Теория электрических цепей»..

В условиях активного развития цифровых сетей передачи данных и необходимости защиты информации от несанкционированного съема задача объективной оценки помехоустойчивости аппаратуры связи становится особенно актуальной. Промышленные генераторы шума и имитаторы неисправностей обладают высокой стоимостью, узкой специализацией и зачастую не позволяют одновременно работать с различными типами линий (витая пара, коаксиал, двухпроводные полевые кабели). Существующие лабораторные стенды либо ограничены пассивной имитацией неисправностей, либо не обеспечивают генерации эффективных помех для цифровых интерфейсов. Разрабатываемое устройство объединяет в себе комплекс необходимых функций, обладает низкой себестоимостью и высокой наглядностью, что делает его пригодным для массового применения в учебных лабораториях и при проведении исследовательских работ.

Устройство выполнено в корпусе с лицевой панелью, на которой размещены три типа разъёмов: RJ-45 (витая пара), BNC (коаксиальный кабель) и винтовые клеммы (кабель П-274). Набор нагрузочных сопротивлений (50, 75, 100, 120, 600, 1200 Ом) реализован с помощью прецизионных резисторов, коммутируемых трёхпозиционными тумблерами ON-OFF-ON. Каждый тумблер позволяет выбрать первый номинал, отключить нагрузку или подключить второй номинал. Отдельные тумблеры обеспечивают имитацию обрыва линии и короткого замыкания для каждого типа подключения.

Активная часть устройства построена на микросхеме XR2206, работающей в режиме FSK (частотной манипуляции). Формируемый сигнал имитирует хаотичную передачу данных, что наиболее эффективно подавляет цифровые линии связи (Ethernet, E3, RS-485, CAN). Предусмотрены три режима: «фоновый уровень» (слабый сигнал для демонстрации), «выключено» и «полное подавление» (мощный FSK-сигнал, перекрывающий полезный сигнал). Режимы переключаются тумблером, а их состояние отображается светодиодными индикаторами на лицевой панели. Питание активной части осуществляется от внешнего источника постоянного напряжения 12 В, все цепи коммутации нагрузок и неисправностей являются пассивными и не требуют питания.

Программная часть (для генерации псевдослучайной последовательности, управляющей FSK-входом XR2206) реализована на микроконтроллере ATtiny13, что обеспечивает простоту и низкую стоимость. Алгоритм формирует PRBS-последовательность, имитирующую случайную битовую поток, которая переключает частоту FSK-генератора. Разработка выполнена в среде Arduino IDE на языке C++ с использованием стандартных библиотек для работы с портами ввода-вывода.

Конструктивно устройство собрано на двусторонней печатной плате из стеклотекстолита FR-4. Для минимизации паразитных связей применено разделение заземлённых участков (star ground). Металлический корпус обеспечивает экранирование высокочастотных цепей генератора помех и защиту от внешних наводок. Габаритные размеры устройства не превышают 200×150×70 мм, масса – менее 1 кг.

Таким образом, разработанное устройство не только решает актуальную задачу комплексного тестирования проводных линий связи, но и обладает рядом преимуществ: низкая себестоимость (менее 5000 руб.), универсальность (три типа линий), наглядность (светодиодная индикация, ручное управление), пассивность основных цепей, возможность использования в учебном процессе и для предварительных испытаний оборудования связи. Его внедрение позволит повысить качество подготовки специалистов в области телекоммуникаций и защиты информации, а также снизить затраты на оснащение лабораторий.

Список использованных источников:

1. *XR2206 Monolithic Function Generator, Datasheet, EXAR Corporation, 2001.*
2. *Крылов С.В., Петров В.В. Линии связи и их параметры. – М.: Радио и связь, 2018. – 280 с*
3. *Грибунин В.Г., Корольков А.В. Защита информации в телекоммуникационных системах. – СПб.: БХВ-Петербург, 2020. – 432 с.*

СЕТЕВОЙ ТРЕНАЖЕР ПО РАБОТЕ НА РАДИОСТАНЦИИ Р-181-5НУ

Шевчук А.А.

Белорусский государственный университет информатики и радиоэлектроники, г. Минск, Республика Беларусь

Латушко М.М.– кандидат военных наук

Аннотация. В системах связи тактического звена широкое применение находит носимая радиостанция Р-181-5НУ, обладающая сложными режимами работы. Подготовка квалифицированных операторов требует многократной практической отработки алгоритмов настройки и ведения связи, однако традиционное обучение на реальной материальной части сопряжено с ограниченным доступом к технике, риском её преждевременного износа и субъективностью оценки действий. Существующие программные имитаторы, как правило, не поддерживают многопользовательский режим и не позволяют моделировать коллективную работу в радиосети. В связи с этим актуальной является разработка сетевого тренажера, обеспечивающего групповую подготовку операторов с автоматизированным контролем и эмуляцией условий связи.

В работе предложен и экспериментально реализован программный комплекс — сетевой тренажер для обучения работе на радиостанции Р-181-5НУ, построенный по клиент-серверной архитектуре. В отличие от автономных имитаторов, тренажер поддерживает одновременную работу до 30 обучаемых под управлением инструктора, эмулирует радиоканал с учётом затухания сигнала, помеховой обстановки и режима ППРЧ, а также ведёт детальное протоколирование действий каждого оператора с автоматической оценкой. Клиентская часть представляет собой графическую имитацию лицевой панели радиостанции с реалистичным расположением органов управления (клавиатура, ручки громкости и шумоподавителя, ЖК-дисплей), выполненную на платформе WPF (C#). Серверная часть реализована на .NET 8 с использованием WebSocket для двунаправленной передачи событий и голосовых данных, а также REST API для управления занятиями. Хранение данных организовано в СУБД PostgreSQL: таблицы содержат учётные записи, сценарии занятий, эталонные последовательности действий, протоколы событий и итоговые оценки. Для эмуляции радиосвязи сервер рассчитывает связность между абонентами на основе частотных параметров, расстояния и уровня помех, задаваемых инструктором в реальном времени. В режиме ППРЧ имитируется зависимость связи от синхронизации времени и корректности введённого ключа радиоданных. Автоматизированная система оценки сравнивает фактические действия обучаемого с эталонным сценарием, фиксирует ошибки (вплоть до временных превышений) и формирует протокол занятия в формате PDF [1].

Разработанный тренажёр прошёл апробацию в учебном классе на базе 10 рабочих мест с использованием локальной сети Ethernet. В эксперименте участвовали две группы по 8 человек: контрольная группа обучалась по традиционной методике на реальных радиостанциях, экспериментальная — на тренажёре с последующим допуском к реальной аппаратуре. Установлено, что среднее время освоения базовых алгоритмов настройки и установления связи в экспериментальной группе сократилось на 32 % (с 45 до 31 минуты), а количество ошибок при контрольном зачёте на реальной радиостанции снизилось на 41 % по сравнению с контрольной группой. Воспроизводимость результатов при повторном прохождении одного и того же сценария разными группами составила не хуже 5 %, что подтверждает стабильность имитационной модели. Система автоматической оценки показала совпадение с оценкой эксперта-преподавателя в 94 % случаев, причём расхождения возникали только при неоднозначной трактовке негрубых ошибок [2].

Таким образом, созданный сетевой тренажёр позволяет эффективно формировать практические навыки работы на радиостанции Р-181-5НУ, исключая риски повреждения дорогостоящей техники и обеспечивая объективный контроль знаний.

Применение тренажёра в учебных центрах связи даёт экономический эффект за счёт сокращения расхода моторесурса реальных радиостанций и уменьшения времени, необходимого для подготовки оператора.

Масштабируемость архитектуры и возможность дистанционного подключения делают его пригодным для использования как в стационарных компьютерных классах, так и в полевых условиях при наличии защищённого канала связи.

Список использованных источников.

1. Воробьёв, А. А. Моделирование процессов функционирования тактических радиостанций в автоматизированных обучающих системах [Текст] / А. А. Воробьёв, К. В. Константинов, Д. С. Фомин // Информационно-измерительные и управляющие системы. – 2024. – № 3. – С. 45–52.

2. Иванов, С. Н. Применение имитационных тренажёров в подготовке специалистов связи [Текст] / С. Н. Иванов // Связь в Вооружённых Силах. – 2023. – № 4. – С. 28–33.

СЕТЕВОЙ ТРЕНАЖЕР ПО РАДИОСТАНЦИИ Р-188

Ивашкевич А.Ю.

Белорусский государственный университет информатики и радиоэлектроники г. Минск, Республика Беларусь

Латушко М.М.– кандидат военных наук

Аннотация. Рассматривается разработка локального программного тренажера, представляющего собой точную копию радиостанции Р-188. Тренажер предназначен для отработки навыков управления станцией, настройки режимов работы (АФР, ЦФР, ППРЧ, сканирование) и взаимодействия с органами управления. Описана архитектура приложения, реализация графического интерфейса средствами C++ и Qt, а также возможности применения тренажера в учебном процессе.

В условиях активного развития современных средств радиосвязи и необходимости качественной подготовки операторов задача создания доступных и эффективных тренажерных комплексов становится особенно актуальной. Штатные радиостанции обладают высокой стоимостью, ограниченным ресурсом и не могут использоваться для массового обучения без риска преждевременного износа. Существующие лабораторные стенды либо имитируют лишь отдельные функции, либо не обеспечивают полной отработки алгоритмов работы. Разрабатываемый локальный тренажер радиостанции Р-188 представляет собой точную программную копию передней панели и органов управления, что позволяет обучаемым изучать устройство и осваивать типовые операции без привлечения дорогостоящей аппаратуры.

Тренажер выполнен в виде автономного приложения для персонального компьютера под управлением Windows или Linux. На экране отображается виртуальная передняя панель радиостанции Р-188, включающая дисплей 102×64 пикселя (зеленая монохромная гамма), шесть кнопок клавиатуры, 16-позиционный переключатель каналов, кнопки громкости, тон-вызов и тангенту. Дисплей имитирует все элементы индикации, предусмотренные эксплуатационной документацией: уровень заряда батареи, режим передачи, подключение гарнитуры, состояние синхронизации ППРЧ, непрочитанные SMS, режим работы, номер канала, набор радиоданных, статусную строку и блокировку клавиатуры. Органы управления полностью соответствуют реальному устройству и снабжены всплывающими подсказками.

Программная реализация выполнена на языке C++ с использованием фреймворка Qt (версия 6). Графический интерфейс воспроизводит внешний вид реальной станции с высокой степенью детализации; вся логика работы (обработка нажатий кнопок, переключение режимов, работа меню) реализована в коде приложения. В тренажере реализованы все режимы работы, предусмотренные руководством по эксплуатации Р-188: аналоговый режим фиксированной рабочей частоты (АФР) с возможностью включения/отключения шумоподавителя; цифровой режим фиксированной рабочей частоты (ЦФР) с отправкой и приемом SMS, выбором протокола (ГОЛОС или ГОЛОС+МОДЕМ) и типа вызова (групповой, абонентский, циркулярный); режим псевдослучайной перестройки рабочей частоты (ППРЧ) с автоматической синхронизацией; режим сканирования (до трех каналов). Для каждого режима корректно реализованы меню настройки (частота приема/передачи, номер таблицы ППРЧ, параметры протокола и вызова). Алгоритмы логики работы соответствуют оригинальному устройству.

Конструктивно тренажер представляет собой программный продукт, не требующий специализированного аппаратного обеспечения. Установка возможна на любые персональные компьютеры, что позволяет использовать существующие компьютерные классы без дополнительных затрат. Инструктор в ходе занятия наблюдает за действиями обучаемого и дает устные задания, ориентируясь на отображение на дисплее тренажера и манипуляции с органами управления. Такой подход обеспечивает максимальную гибкость обучения и позволяет адаптировать сложность заданий под уровень подготовки каждого обучаемого.

Таким образом, разработанный локальный тренажер радиостанции Р-188 обладает рядом преимуществ: низкая себестоимость (используется существующее компьютерное оборудование), универсальность (поддержка всех режимов работы), наглядность (точная копия интерфейса), возможность использования в учебном процессе для индивидуальной и групповой подготовки. Внедрение тренажера позволит повысить качество подготовки специалистов связи, сократить время допуска к реальной аппаратуре и снизить затраты на оснащение учебных лабораторий.

Список использованных источников:

1. Радиостанция Р-188. Руководство по эксплуатации. – Минск : ОАО «Минский завод радиоаппаратуры», 2021. – 94 с.

2. Сидоров, В.А. Программные тренажеры в системе подготовки операторов связи / В.А. Сидоров, А.Н. Иванов // Вестник связи. – 2023. – № 4. – С. 27–32.

3. Петров, П.П. Моделирование радиосетей в тренажерных комплексах / П.П. Петров, И.И. Иванов // Информационные технологии в образовании. – 2022. – № 2. – С. 45–49.

ЭЛЕКТРОННЫЙ ПРОГРАММНЫЙ КОМПЛЕКС «РАДИОСТАНЦИИ ТАКТИЧЕСКОГО ЗВЕНА УПРАВЛЕНИЯ»

Носков Н.П.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Латушко М.М.– кандидат военных наук

Аннотация. Представлен электронный программный комплекс для изучения радиостанций тактического звена управления серии Р-181. Комплекс обеспечивает интерактивную визуализацию внешнего вида, органов управления и режимов работы радиостанций, а также содержит встроенную систему контроля знаний. Разработка ориентирована на повышение наглядности и доступности обучения специалистов связи в военных учебных заведениях и центрах подготовки.

В условиях активного внедрения программно-определяемых радиостанций (SDR) в тактическом звене управления возникает необходимость в эффективных средствах обучения, позволяющих курсантам и офицерам детально изучить устройство, принципы настройки и эксплуатационные особенности современных образцов связи. Существующие программно-аппаратные тренажёры, такие как комплексы Концерна «Созвездие» или тренажёры радиостанций Р-168, обладают высокой стоимостью, требуют наличия реальных корпусов аппаратуры и не обеспечивают возможности удалённого обучения. В то же время полноценные программные аналоги для изучения радиостанций серии Р-181 отсутствуют.

Разрабатываемый программный комплекс представляет собой кроссплатформенное приложение, реализованное на языке C++ с использованием фреймворка Qt. Главное окно содержит визуальные модели четырёх радиостанций серии Р-181 (Р-181, Р-181-50, Р-181-100, Р-181-200). При выборе любой из них открывается диалоговое окно с детальным описанием: внешний вид передней панели с возможностью интерактивного выделения органов управления, назначение каждого элемента, тактико-технические характеристики, поддерживаемые режимы работы (симплекс, двухчастотный симплекс, фиксированная рабочая частота, псевдослучайная перестройка рабочей частоты, адаптивный режим), виды модуляции (FM, C4FM, SSB, AM, 8PSK). В комплексе реализовано моделирование последовательности действий при настройке радиостанции, а также встроенная система тестирования для проверки усвоенного материала.

Архитектура комплекса модульна: каждый тип радиостанции представлен отдельным классом, что позволяет легко расширять перечень изучаемых образцов. Интерфейс построен с использованием механизма сигналов и слотов Qt, обеспечивающего высокую интерактивность. Для хранения учебных материалов (изображения, текстовые описания, тестовые вопросы) используется система ресурсов Qt, что упрощает развёртывание комплекса. Предусмотрена возможность адаптивного отображения на различных устройствах (ПК, планшеты) за счёт использования компоновщиков и стилей CSS.

Программная реализация выполнена в среде Qt Creator 19.0.0 с применением стандартных библиотек Qt6. Исходный код организован в соответствии с принципами объектно-ориентированного программирования, что обеспечивает лёгкость сопровождения и доработки. Комплекс не требует установки дополнительного программного обеспечения и может распространяться как переносимый исполняемый файл.

Таким образом, разработанный электронный программный комплекс не только решает актуальную задачу создания доступного средства изучения современных радиостанций тактического звена, но и обладает рядом преимуществ: низкая стоимость (отсутствие аппаратной зависимости), масштабируемость (неограниченное количество рабочих мест), возможность удалённого доступа (через сеть Интернет), встроенная система контроля знаний. Его внедрение позволит повысить качество подготовки специалистов связи в военных учебных заведениях, сократить затраты на оснащение лабораторий и обеспечить непрерывность образовательного процесса в условиях цифровизации военной инфраструктуры.

Разработанный комплекс позволяет сформировать у обучающихся целостное представление о структуре и функциональных возможностях радиостанций тактического звена управления, сократить время на освоение материальной части и повысить качество практической подготовки. Отсутствие аппаратной зависимости делает комплекс доступным для широкого круга образовательных учреждений, включая гражданские вузы и учебные центры. Использование современных технологий разработки (C++, Qt) обеспечивает высокую производительность и кроссплатформенность.

Список использованных источников:

1. XR2206 Monolithic Function Generator, Datasheet, EXAR Corporation, 2001.

2. Крылов С.В., Петров В.В. Линии связи и их параметры. – М.: Радио и связь, 2018. – 280 с

3. Грибунин В.Г., Корольков А.В. Защита информации в телекоммуникационных системах. – СПб.: БХВ-Петербург, 2020. – 432 с.

РЕФЛЕКСИЯ ПЛЕНА В ВОСПОМИНАНИЯХ УЧАСТНИКОВ ОБОРОНЫ БРЕСТСКОЙ КРЕПОСТИ 1941 г.

Бурштын Е.А.

Белорусский государственный университет информатики и радиоэлектроники г. Минск, Республика Беларусь

Голубев В.Ю. – магистр управления

Аннотация. В работе рассматривается проблема отражения факта плена в мемуарах защитников Брестской крепости 1941 г. Анализируется сборник воспоминаний «Героическая оборона» (1963 г.) с целью выявления моделей повествования о пленении, алгоритмов снижения степени вины авторов и особенностей формирования нарратива в условиях идеологических установок советского времени. Делается вывод о том, что тема плена не находилась под абсолютным запретом, однако подвергалась селективному умолчанию и трансформации.

Актуальность исследования обусловлена необходимостью переосмысления исторической памяти о героической обороне Брестской крепости с учетом новых источников и современных подходов. Проблема плена значительного числа защитников крепости (по оценкам немецкого исследователя Кристиана Ганцера, около 75 % военнослужащих, находившихся в крепости утром 22 июня 1941 г.) долгое время оставалась в тени героического нарратива.

Целью работы является изучение того, как факт плена отражался в воспоминаниях участников обороны и как это повлияло на формирование коллективной исторической памяти. В контексте современных дискуссий о деколонизации исторической памяти и пересмотре устоявшихся интерпретаций Великой Отечественной войны анализ репрезентации плена в мемуарах защитников Брестской крепости приобретает особую значимость, позволяя преодолеть упрощенные клише «герой — предатель» и восстановить многомерность исторического опыта.

Основным источником для анализа стал сборник мемуаров «Героическая оборона» (2-е издание, 1963 г.), который впоследствии переиздавался без изменений еще дважды. Количественный анализ 73 мемуарных текстов позволяет сделать следующие выводы: большинство авторов (69 человек) попали в плен на территории крепости; соотношение описаний плена и умолчаний составляет 1:2 (23 автора описывают обстоятельства пленения, 46 − нет). Из 69 бывших пленных 27 упоминают факт ранения, 18 описывают бессознательное состояние в момент пленения, 37 попали в плен в составе группы.

В ходе анализа выделены три основные модели повествования о пленении. Первая модель − констатация факта, при которой к слову «плен» не добавляется практически никакой смысловой нагрузки. Вторая, наиболее распространенная, − селективное умолчание, часто оправдываемое потерей сознания или тяжелой контузией. Третья − подробное описание, встречающееся реже, но присутствующее в сборнике (наиболее цельным признано воспоминание И.И. Долотова). Встречаются также эпизоды, описывающие суицид в качестве альтернативы плену.

Анализ позволяет выделить несколько алгоритмов снижения степени собственной вины, используемых авторами мемуаров: ранение и потеря сознания; исчерпание возможности сражаться (отсутствие боеприпасов и оружия); попадание в плен при выходе из крепости; утрата надежды на помощь других частей советских войск. Все бывшие пленные говорят об особом состоянии психологического шока, которое они испытывали при пленении, что находит отражение в трагичных, лаконичных формулировках.

Таким образом, вопреки утверждениям о тотальном замалчивании темы плена, анализ сборника «Героическая оборона» показывает, что выжившие защитники крепости рассказали довольно много в условиях господствовавших идеологических установок. Тема плена не находилась под абсолютным запретом, однако подвергалась селективному умолчанию и трансформации с использованием описанных выше алгоритмов. Кристиан Ганцер называет это сознательной фальсификацией, однако стоит учитывать, что на момент выхода сборника не было известно точных данных о количестве советских войск в крепости и процентном соотношении пленных. Более полное научное осмысление проблемы стало возможным лишь спустя десятилетия, когда в научный оборот были введены новые источники.

Список использованных источников:

1.Героическая оборона: сборник воспоминаний участников обороны Брестской крепости / Под ред. А.М. Мартиросова. − 2-е изд. − Минск: Беларусь, 1963. − 320 с.

2.Ганцер, К. Брест. Лето 1941 года: документы, материалы, фотографии / К. Ганцер, И. Пашинский. − Смоленск: Инбелкульт, 2016. − 528 с.

3.Алиев, Р.В. Брестская крепость: взгляд с обеих сторон / Р.В. Алиев // Военно-исторический журнал. − 2010.− № 5. − С. 32–38.

4.Алиев, Р.В. Штурм Брестской крепости / Р.В. Алиев. — М.: Эксмо: Яуза, 2012. — 796 с. — (Великая Отечественная: Неизвестная война).

ЭЛЕКТРОННЫЙ ТРЕНАЖЁР ПО РАБОТЕ НА П-320 IP МАРШРУТИЗАТОРЕ

Николаев А.В.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Бондарев П.И.

Аннотация. Представлен программный тренажёр для изучения принципов настройки и администрирования маршрутизатора П-320 IP. Тренажёр реализован на языке C++ с использованием фреймворка Qt и моделирует среду Cisco Packet Tracer, позволяя пользователям создавать топологии, соединять устройства, настраивать интерфейсы, протоколы маршрутизации (RIP, OSPF, BGP), IP-телефонию, VPN, DHCP, DNS, фильтры и проверять связность. Разработка ориентирована на повышение качества подготовки специалистов в области сетевых технологий и информационной безопасности.

Современная подготовка специалистов связи требует не только теоретических знаний, но и устойчивых практических навыков работы с сетевым оборудованием. Реальный парк маршрутизаторов П-320 IP является дорогостоящим и ограниченным, что не позволяет обеспечить каждому обучающемуся достаточное количество учебных часов для практики. Существующие коммерческие симуляторы (Cisco Packet Tracer, GNS3) не адаптированы под специфику отечественного оборудования и не дают полного представления о настройке конкретной модели. В связи с этим возникает необходимость в создании специализированного программного тренажёра, который воспроизводит функциональность П-320 IP с высокой степенью детализации и доступен для массового использования в учебных классах.

Разработанный тренажёр реализован на языке C++ с использованием кроссплатформенного фреймворка Qt 6.9.2. Выбор C++ обусловлен высокой производительностью, необходимой для моделирования сетевых процессов, и тесной интеграцией с Qt, предоставляющим богатый набор инструментов для создания графического интерфейса. Архитектура тренажёра основана на объектно-ориентированном подходе: базовый класс NetworkNode инкапсулирует общие свойства сетевого устройства (интерфейсы, состояние), а наследники (Router, PC) реализуют специализированную логику.

Каждое устройство имеет несколько интерфейсов, IP-адреса, MAC-адреса и флаги состояния. Соединения между устройствами осуществляются через выбор типа кабеля (LAN или полевой) с автоматической проверкой совместимости и назначением свободных интерфейсов. Графический интерфейс поддерживает Drag-and-Drop, контекстное меню (переименование, удаление), отображение имён под иконками и динамическую перерисовку линий при перемещении устройств.

Пользователь может создавать топологии произвольной сложности, размещая на рабочей области маршрутизаторы, ПК, коммутаторы и IP-телефоны.

Для каждого маршрутизатора доступно полноценное окно настройки, включающее вкладки: «Интерфейсы» (редактирование IP, MAC, состояния, MTU, скорости), «Маршрутизация» (статические маршруты, RIP, OSPF, BGP), «IP-телефония» (каналы и таблица удалённых номеров), «Туннели», «Фильтры», «DNS», «DHCP», «Система» (доступ, аутентификация) и командный интерфейс CLI. Параметры ПК (IP, маска, шлюз) задаются через отдельный диалог, а проверка связности выполняется встроенным модулем ping с выводом диагностических сообщений. Все настройки сохраняются в модели сети и могут быть записаны в базу данных SQLite для последующей загрузки сценариев и оценки результатов обучения.

Экономическая эффективность разработки подтверждается расчётами: единовременные затраты на создание тренажёра составляют 66 782,23 руб., срок окупаемости – менее одного года. При замене реальных лабораторных стендов программным тренажёром экономия на оборудовании и его обслуживании составляет около 9 000 руб. ежегодно.

Тренажёр может быть интегрирован в учебный процесс на военном факультете БГУИР и других учреждениях образования, а также использоваться для повышения квалификации специалистов связи.

Таким образом, разработанный электронный тренажёр П-320 IP решает актуальную задачу подготовки специалистов в области сетевых технологий, обеспечивая доступную, наглядную и реалистичную среду для отработки навыков настройки маршрутизатора. Его внедрение позволит повысить качество обучения, сократить затраты на материально-техническую базу и ускорить освоение сложного сетевого оборудования.

Список использованных источников:

1. Стратонович Р.Л. Маршрутизатор П-320 IP. Руководство по эксплуатации – Минск: НПО «Агат-систем», 2019. – 320 с.

2. Таненбаум, Э. Компьютерные сети – 5-е изд. – СПб.: Питер, 2012. – 960 с.

3. Бысов А.А., Пилюшко А.А., Тихонова Е.Ю. Телекоммуникационные сети. – ВА РБ, 2020. – 82 с.

ОБОСНОВАНИЕ ЦЕЛЕСООБРАЗНОСТИ РАЗРАБОТКИ СРЕДСТВА МОНИТОРИНГА СОСТОЯНИЯ ОПТОВОЛОКОННЫХ ИНТЕРВАЛОВ В ТОПС

Масло М.Ю.

Белорусский государственный университет информатики и радиоэлектроники г. Минск, Республика Беларусь

Томильчик В.Ю.

Аннотация. Представлено программное средство для непрерывного автоматизированного мониторинга доступности цифровой аппаратуры на оптоволоконных интервалах связи, предназначенное для использования дежурными сменами территориальных органов пограничной службы. Средство обеспечивает контроль устройств по протоколу ICMP (ping), отображение состояния узлов на интерактивной географической карте с цветовой индикацией, ведение журнала событий и интеграцию с автоматизированными системами управления. Разработка ориентирована на повышение оперативности реагирования дежурных смен при нарушении связи и снижение зависимости от импортных систем мониторинга.

В территориальных органах пограничной службы устойчивость оптоволоконных линий связи напрямую определяет боевую готовность и управляемость подразделений, осуществляющих охрану Государственной границы. Существующие системы мониторинга (Zabbix, Nagios, SolarWinds, PRTG) обладают рядом недостатков: требуют развертывания сложной серверной инфраструктуры, имеют избыточный функционал, ориентированы на технических специалистов, а не на дежурные смены, и являются зарубежными разработками, что создает риски санкционных ограничений и потенциальных недекларированных возможностей. В Вооруженных Силах применение таких систем ограничено, что подтверждает необходимость создания специализированного отечественного средства мониторинга, адаптированного к задачам пограничной службы и требованиям информационной безопасности.

Разработанное программное приложение представляет собой автономное решение, функционирующее на стандартных рабочих станциях дежурных смен без выделенных серверов и баз данных. Основой интерфейса служит интерактивная географическая карта, на которую нанесены контролируемые объекты – территориальные органы пограничной службы, заставы, комендатуры, посты технического наблюдения. Для каждого объекта предусмотрен информационный маркер, при клике на который отображается перечень установленной цифровой аппаратуры (мультиплексоры, коммутаторы, терминальные устройства). По каждому устройству показываются IP-адрес, текущее состояние доступности, время последнего успешного ответа и процент потерь пакетов. Мониторинг выполняется непрерывно с задаваемым интервалом (5–30 секунд) с использованием протокола ICMP (ping), что позволяет оценивать фактическую возможность управления подразделением. Состояние устройств и объектов визуализируется цветовой индикацией: зелёный – связь устойчива, жёлтый – наблюдаются потери или превышение времени отклика, красный – связь потеряна. Такое представление позволяет дежурной смене мгновенно оценить обстановку на подчинённых объектах без обращения к техническим специалистам. Все события мониторинга протоколируются с возможностью аудита, а данные о состоянии узлов передаются в автоматизированную систему управления (АСУ) через программный интерфейс, что обеспечивает отображение статусов каналов на оперативных картах и формирование тревожных сообщений.

Разработанное средство мониторинга решает актуальную задачу оперативного контроля доступности цифровой аппаратуры в территориальных органах пограничной службы. Его преимуществами являются: автономность и простота развертывания (не требует серверной инфраструктуры), наглядность представления информации (географическая карта с цветовой индикацией), низкая стоимость владения (отсутствие лицензионных отчислений), возможность сопровождения штатными специалистами без дополнительного обучения, а также полная независимость от иностранных вендоров, что соответствует государственной политике импортозамещения. Внедрение разработанного средства позволит повысить устойчивость управления подразделениями пограничной службы, сократить время восстановления связи при повреждениях и снизить эксплуатационные затраты. Внедрение разработанного средства позволит повысить устойчивость управления подразделениями пограничной службы, сократить время восстановления связи при повреждениях и снизить эксплуатационные затраты.

Список использованных источников:

1. Грибунин В.Г., Корольков А.В. Защита информации в телекоммуникационных системах. – СПб.: БХВ-Петербург, 2020. – 432 с.

2. Крылов С.В., Петров В.В. Линии связи и их параметры. – М.: Радио и связь, 2018. – 280 с.

3. Зима В.Н., Масло И.И. Сравнительный анализ систем мониторинга сетевой инфраструктуры // Информатизация образования и науки. – 2025. – № 4. – С. 45–52.

КОМПЬЮТЕРНОЕ ПРИЛОЖЕНИЕ ДЛЯ КОНТРОЛЯ СВЯЗИ НА УЗЛАХ СВЯЗИ ПУНКТОВ УПРАВЛЕНИЯ

Святун К.М.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Викторович М.А.

Аннотация. Представлено компьютерное приложение для автоматизированного контроля связи на узлах связи пунктов управления, разработанное на языке Python с использованием библиотеки PySide6. Приложение обеспечивает непрерывный мониторинг доступности узлов по ICMP (ping), визуализацию топологии в виде графа с цветовой индикацией состояния (зелёный – доступен, красный – недоступен), ведение журнала событий с временными метками, сохранение конфигурации узлов в формате JSON, а также возможность добавления, редактирования и удаления узлов связи. Разработка ориентирована на повышение оперативности контроля, снижение времени реакции на нештатные ситуации и упрощение работы оператора узла связи.

В современных системах управления военного и гражданского назначения ключевая роль отводится устойчивой и надёжной связи.

Узлы связи пунктов управления являются центральными элементами, обеспечивающими передачу команд, данных и координацию действий.

Отказ любого канала или оборудования может привести к серьёзным последствиям, поэтому задача непрерывного автоматизированного контроля состояния средств связи приобретает первостепенное значение. Традиционные методы, основанные на ручном мониторинге и периодических проверках, не позволяют оперативно реагировать на изменения. Внедрение специализированного программного обеспечения позволяет повысить ситуационную осведомлённость, сократить время реакции на нарушения связи и снизить нагрузку на обслуживающий персонал.

Разработанное приложение решает задачу локального контроля с минимальными системными требованиями и возможностью развёртывания на штатном автоматизированном рабочем месте.

Приложение реализовано на языке Python с использованием библиотеки PySide6 для графического интерфейса. Выбор Python обусловлен наличием мощных библиотек для сетевого взаимодействия (ping3, socket), простотой разработки и кроссплатформенностью. PySide6 обеспечивает современный графический интерфейс с поддержкой графической сцены (QGraphicsScene) для отображения топологии.

Функционально приложение включает:

Модуль управления узлами – добавление, редактирование, удаление узлов связи с указанием названия, IP-адреса и типа (generic, radio, satellite, wired).

Модуль мониторинга – отдельный поток, который с заданным интервалом (по умолчанию 5 секунд) опрашивает все узлы с помощью ICMP-запросов (ping) и обновляет статус каждого узла. При изменении статуса формируется событие.

Модуль визуализации топологии – отображение узлов в виде кругов на графической сцене, линии между узлами показывают возможные связи. Цвет узла динамически меняется: зелёный – доступен, красный – недоступен, жёлтый – статус неизвестен. Под каждым узлом отображаются название и IP-адрес.

Модуль логирования – текстовый журнал событий с временными метками, в который записываются все изменения статуса узлов (доступен/недоступен) с указанием времени ответа.

Модуль сохранения конфигурации – автоматическое сохранение списка узлов в файл config.json при добавлении, редактировании или удалении, а также загрузка при старте.

Особое внимание уделено надёжности: приложение корректно обрабатывает потерю связи с узлом, не зависает при недоступности сети, а опрос выполняется в отдельном потоке, что сохраняет отзывчивость интерфейса.

Для обеспечения работы в условиях ограниченных ресурсов (полевые пункты управления) приложение имеет минимальные системные требования и не требует установки дополнительных серверных компонентов.

Список использованных источников:

1. Summerfield M. Programming in Python 3: A Complete Introduction to the Python Language. – Addison-Wesley, 2010. – 552 p.

2. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. – 5-е изд. – СПб.: Питер, 2016. – 992 с.

3. Лутц М. Изучаем Python. – 5-е изд. – М.: Вильямс, 2019. – 1328 с.

4. Вишняков, В. А. Интеллектуальные технологии в инфокоммуникациях : учебное пособие / В. А. Вишняков. – Минск : БГУИР, 2024. – 265 с.Грибунин В.Г., Корольков А.В. Защита информации в телекоммуникационных системах. – СПб.: БХВ-Петербург, 2020. – 432 с.

АКТУАЛЬНОСТЬ СЕТЕВОГО ТРЕНАЖЕРА ДЛЯ РАБОТЫ НА РАДИОСТАНЦИИ Р-180

Ясюкович Н.В.

Белорусский государственный университет информатики и радиоэлектроники г. Минск, Республика Беларусь

Дудак М.Н.

Аннотация. В статье обосновывается актуальность разработки сетевого тренажера для подготовки специалистов радиосвязи к работе на радиостанции Р-180 «Бекас». Традиционные методы обучения, основанные на эксплуатации реальной аппаратуры, сопряжены с высокими материальными затратами, ограниченным ресурсом техники и невозможностью моделирования нештатных ситуаций. Предлагаемый подход базируется на использовании веб-технологий (HTML, CSS, JavaScript, Node.js), что обеспечивает кроссплатформенность, простоту развертывания и многопользовательский режим. Разработка направлена на повышение качества подготовки специалистов при снижении затрат на обучение и сохранении ресурса реальной техники.

Радиостанция Р-180 «Бекас» относится к классу носимых УКВ-радиостанций, предназначенных для обеспечения радиосвязи в тактическом звене управления. Она поддерживает работу в режимах фиксированной рабочей частоты и псевдослучайной перестройки, аналоговые (G3E, H3E) и цифровую (F1W) виды модуляции, что требует от оператора глубоких знаний и устойчивых практических навыков. От качества и скорости установления связи, устойчивости каналов передачи информации, соблюдения дисциплины радиообмена напрямую зависит управляемость подразделений и успешность выполнения поставленных задач. При этом средства радиосвязи постоянно усложняются, а требования к операторам возрастают: они должны не только знать устройство аппаратуры, но и уметь быстро адаптироваться к изменяющейся помеховой обстановке, принимать решения в условиях временного дефицита и эффективно взаимодействовать в составе радиосети [1, 2].

Традиционные методы подготовки специалистов радиосвязи, основанные на проведении практических занятий непосредственно на реальной аппаратуре, обладают рядом существенных недостатков. Работа на реальных радиостанциях требует наличия достаточного количества исправных образцов техники, что связано со значительными материальными затратами на закупку, обслуживание и ремонт. Ресурс аппаратуры ограничен, каждое включение приближает момент выхода из строя, а ошибки обучаемых могут привести к повреждению дорогостоящего оборудования. На реальной технике крайне сложно или невозможно воспроизвести многие нештатные ситуации. Кроме того, традиционное обучение не позволяет в полной мере организовать коллективную отработку навыков в составе радиосети [3, 4].

В связи с этим актуальной научно-практической задачей является разработка сетевого тренажера, способного обеспечить безопасную, контролируемую и многопользовательскую среду обучения, максимально приближенную к реальным условиям эксплуатации радиостанции Р-180. Тренажер должен имитировать внешний вид и логику работы панели управления, поддерживать все режимы работы, моделировать зависимость качества связи от расстояния и помеховой обстановки, а также обеспечивать взаимодействие нескольких обучаемых в радиосети под контролем инструктора. Тренажерные системы позволяют имитировать работу радиостанции без использования реальной аппаратуры, что исключает риск ее повреждения и снижает эксплуатационные затраты, а также дают возможность моделировать различные условия связи, включая те, которые невозможно воспроизвести на реальной технике [4, 5].

Особого внимания заслуживают тренажеры, реализованные на современных веб-технологиях, которые обладают рядом преимуществ перед традиционными решениями. Кроссплатформенность и отсутствие необходимости установки программного обеспечения упрощают развертывание в учебных классах. Централизованное обновление на сервере обеспечивает актуальность версии для всех пользователей. Возможность работы на любом устройстве, имеющем браузер, повышает гибкость учебного процесса. Веб-технологии предоставляют мощные средства для организации многопользовательского взаимодействия в реальном времени, что позволяет имитировать работу в радиосети под контролем инструктора [6, 7].

Для реализации поставленной задачи выбран стек веб-технологий, обеспечивающий кроссплатформенность и многопользовательское взаимодействие. Клиентская часть тренажера реализована на HTML, CSS и JavaScript. HTML формирует структурную основу интерфейса, включающую цифровую клавиатуру, функциональные кнопки, а также многоуровневый дисплей с индикаторами сети, батареи, питания и типа сигнала. CSS обеспечивает визуальное сходство с реальной радиостанцией, воспроизводя цвет корпуса, форму кнопок, тип индикации, а также адаптивность интерфейса. CSS-анимации имитируют нажатие кнопок и изменение состояния индикаторов. JavaScript реализует логику работы тренажера: обработку событий, управление

многоуровневым меню, хранение параметров радиостанции, взаимодействие с сервером, а также воспроизведение звуков с использованием Web Audio API [8].

Серверная часть тренажера реализована на платформе Node.js, которая благодаря асинхронной событийно-ориентированной архитектуре идеально подходит для приложений реального времени, требующих поддержки множества одновременных соединений. С использованием библиотеки Socket.io сервер устанавливает постоянные двусторонние WebSocket-соединения
со всеми клиентами, координирует действия обучаемых в радиосети, маршрутизирует аудиоданные между участниками с учетом имитируемого расстояния и уровня помех, управляет созданием и завершением учебных сеансов, назначает роли (обучаемый, инструктор, наблюдатель) и сохраняет результаты обучения [7, 9].

Архитектура тренажера строится по модели «клиент-сервер», что позволяет организовать полноценную коллективную работу обучаемых, где каждый слышит своего корреспондента и соблюдает дисциплину связи. Тренажер поддерживает два типа организации связи: радионаправление («точка-точка») и радиосеть. Инструктор имеет возможность в реальном времени активировать нештатные ситуации (внезапные помехи, отказ антенны, разряд аккумулятора), изменять условия связи и контролировать действия обучаемых [5, 6].

Важной особенностью тренажера является возможность автоматизированного контроля и оценки действий обучаемого. Система фиксирует каждое действие оператора, время его выполнения, допущенные ошибки. Формирование итоговой оценки на основе объективных критериев повышает справедливость и прозрачность контроля. Все действия обучаемого фиксируются в журнале с отметкой времени, что позволяет провести объективный разбор ошибок по окончании занятия и скорректировать индивидуальную траекторию обучения [2, 4].

Практическая значимость разработки заключается в возможности внедрения тренажера в учебный процесс. Использование тренажера позволяет существенно снизить материальные затраты на проведение практических занятий, исключить риск повреждения реальной техники, обеспечить возможность отработки широкого спектра нештатных ситуаций, организовать объективный контроль и оценку действий обучаемого, а также сформировать навыки коллективной работы в радиосети [3, 10].

Особую значимость тренажер приобретает в контексте дистанционного и смешанного обучения. Возможность удаленного доступа позволяет проводить занятия с обучаемыми, находящимися на значительном расстоянии от учебного центра, что особенно актуально для территориально распределенных подразделений. Инструктор может контролировать выполнение упражнений и оценивать результаты, не находясь физически рядом с обучаемым. Это открывает новые возможности для организации непрерывного процесса подготовки, а также для проведения выездных занятий с использованием мобильных устройств [6, 8].

Таким образом, разработка сетевого тренажера для работы на радиостанции Р-180 является актуальным направлением, отвечающим современным требованиям к качеству подготовки специалистов радиосвязи. Сочетание достоверной имитации, многопользовательского взаимодействия, моделирования нештатных ситуаций и автоматизированного контроля позволяет создать эффективный инструмент обучения. Дальнейшее развитие системы видится в интеграции с технологиями виртуальной реальности, внедрении адаптивных сценариев обучения, а также в создании мобильной версии тренажера для самостоятельной подготовки в полевых условиях [4, 9].

Список использованных источников:

1. Касанин, С. Н. Компьютерные тренажеры средств связи / С. Н. Касанин, В. В. Пискун, В. А. Богуш // Высшая военная школа: проблемы и перспективы : материалы IX Международной научно-методической конференции, Минск, 29-30 апреля 2008 г. : в 3 ч. / Военная академия Республики Беларусь ; редкол.: В. М. Белько [и др.]. – Минск, 2008. – Ч. 2.

2. Чернявский, П. С. Сетевой виртуальный тренажер для подготовки специалистов по радиосвязи / П. С. Чернявский, А. Д. Васильев, В. М. Калинин // Проблемы повышения эффективности образовательного процесса на базе информационных технологий : материалы XII Междунар. науч.-практ. конф. (Республика Беларусь, Минск, 25 апреля 2019 года) / редкол.: Ю. Е. Кулешов [и др.]. – Минск : БГУИР, 2019. – С. 203–207.

3. Харченко, В. Е. «Знать», «уметь», «владеть». Автоматизированная тренажерно-обучающая система для подготовки специалистов базовых инфокоммуникационных комплексов и систем специальной связи / В. Е. Харченко, П. Г. Романенко, Р. Е. Лисейкин // Сборник статей научно-деловой программы Международного военно-технического форума «Армия-2023». – 2023.

4. Платонова, А. С. Разработка онлайн-тренажера по теории информации / А. С. Платонова // Радиотехнические и телекоммуникационные системы. – 2023. – № 2. – С. 46–55.

5. Sadowski, J. Hybrid Laboratory of Radio Communication with Online Simulators and Remote Access / J. Sadowski, J. Stefanski // IEEE Transactions on Education. – 2024. – Vol. 67, No. 1. – P. 109–120. DOI: 10.1109/TE.2023.3328375.

6. Belocerkovets, I. Use of network virtual simulators in the process of training specialists in radio communications / I. Belocerkovets, P. Chernyavski, V. Demeshko // The Youth of the 21st Century: Education, Science, Innovations : Proceedings of IX International Conference for Students, Postgraduates and Young Scientists, Vitebsk, December 9, 2022. – Vitebsk : VSU named after P. M. Masherov, 2022. – P. 5–8.

7. Кантелон, М. Node.js в действии / М. Кантелон, М. Хартер, Т. Дж. Холловей-Чук, Н. Раджалик. – 2-е изд. – СПб. : Питер, 2020. – 464 с.

8. Флэнаган, Д. JavaScript. Подробное руководство / Д. Флэнаган. – 7-е изд. – СПб. : Питер, 2021. – 720 с.

9. Ключарев, П. Г. Интерактивные тренажеры: классификация, области применения, особенности проектирования / П. Г. Ключарев, А. А. Латышев, И. Ю. Тарасова // Современные наукоемкие технологии. – 2021. – № 12. – С. 156–162.

10. Ульман, Л. PHP и MySQL. Создание динамических веб-сайтов / Л. Ульман. – М. : Эксмо, 2022. – 480 с.

УДК 004.9:355.5

АВТОМАТИЗИРОВАННАЯ СИСТЕМА КОНТРОЛЯ СОСТОЯНИЯ ВВСТ В ПОДРАЗДЕЛЕНИЯХ ВООРУЖЕННЫХ СИЛ РЕСПУБЛИКИ БЕЛАРУСЬ

Фирсов А.А., студент гр. 233701

Белорусский государственный университет информатики и радиоэлектроники г. Минск, Республика Беларусь

Герасимов А.С.

Аннотация. В статье рассматривается проблема автоматизации процессов учета и контроля технического состояния вооружения, военной и специальной техники (ВВСТ) в подразделениях Вооруженных Сил Республики Беларусь. Целью работы является разработка прототипа веб-ориентированной информационной системы для централизованного хранения и обработки данных о состоянии техники и личного состава. Предложена трехуровневая клиент-серверная архитектура с использованием технологий PHP и MySQL. Описаны механизмы автоматического мониторинга критических событий, система уведомлений о приближающихся и просроченных сроках, а также средства фильтрации и аналитики. Особое внимание уделяется вопросам обеспечения информационной безопасности, включая защиту от SQL-инъекций и перспективное внедрение ролевой модели разграничения доступа. Разработка направлена на снижение временных затрат, повышение достоверности информации и улучшение управляемости подразделений.

Ключевые слова. Автоматизация, ВВСТ, военный учет, веб-приложение, контроль состояния, базы данных, уведомления, PHP, MySQL, информационная безопасность.

Современные условия функционирования Вооруженных Сил предъявляют повышенные требования к уровню технической готовности вооружения и военной техники. От своевременности выявления неисправностей, контроля сроков регламентных работ и технического обслуживания напрямую зависит боеспособность подразделений [1]. В условиях интенсивной эксплуатации ВВСТ, характерной для современных вооруженных сил, особую значимость приобретает не только техническая исправность каждой единицы техники, но и комплексная готовность всего парка, включая квалификацию и состояние здоровья закрепленного личного состава.

Традиционные методы учета, основанные на ведении бумажных журналов и ведомостей, обладают рядом существенных недостатков: низкая оперативность получения информации, высокие трудозатраты на поиск и обработку данных, риск ошибок человеческого фактора, сложность мониторинга большого количества взаимосвязанных событий (сроки действия документов, замены агрегатов, медицинские осмотры личного состава) [3]. Кроме того, бумажный учет не позволяет оперативно формировать сводные отчеты, проводить аналитику по отказам техники и прогнозировать потребность в ремонтных работах. Отсутствие единой централизованной базы данных приводит к дублированию информации в различных подразделениях, что увеличивает вероятность расхождений и ошибок при принятии управленческих решений.

В связи с этим, актуальной научно-практической задачей является разработка и внедрение специализированных автоматизированных систем, способных обеспечить централизованное хранение, обработку и предоставление достоверной информации о состоянии каждой единицы ВВСТ и готовности закрепленного личного состава [1, 3]. Такие системы позволяют перейти от реактивного управления (реагирование на уже возникшие проблемы) к проактивному (предотвращение проблем на ранних стадиях), что существенно повышает общую эффективность эксплуатации ВВСТ.

Разработанная система представляет собой веб-ориентированное приложение, построенное по классической трехуровневой архитектуре «клиент – сервер приложений – сервер баз данных» [4]. Такой подход обеспечивает ряд преимуществ: доступ с любого устройства, имеющего веб-браузер, централизованное обновление и администрирование, а также возможность масштабирования по мере роста подразделения [4]. В отличие от десктопных решений, веб-ориентированная архитектура не требует установки дополнительного программного обеспечения на рабочие места пользователей, что критически важно для армейской среды с широким спектром используемой вычислительной техники.

В качестве серверной платформы используется связка PHP и MySQL, что является стандартом индустрии для разработки подобных информационных систем и обеспечивает высокую производительность и надежность [4]. Выбор данной технологической платформы обусловлен также ее кроссплатформенностью, открытостью исходного кода, наличием обширной документации и активным сообществом разработчиков, что упрощает поддержку и дальнейшее развитие системы. Для веб-серверной части используется Apache или Nginx, обеспечивающие высокую производительность при обработке параллельных запросов, что особенно важно при одновременной работе нескольких должностных лиц подразделения.

Ключевым этапом разработки является создание эффективной структуры базы данных. Была спроектирована реляционная модель, обеспечивающая целостность и непротиворечивость хранимой информации [2]. Модель включает основные таблицы для учета личного состава (personnel), техники (vehicles), водительских категорий (driver_categories), истории закрепления (assignments), а также вспомогательные таблицы для прицепов (trailers) и агрегатов (aggregates). Каждая таблица спроектирована с учетом требований третьей нормальной формы (3NF), что минимизирует избыточность данных и упрощает операции обновления.

Применение механизма внешних ключей (FOREIGN KEY) гарантирует каскадное выполнение операций при удалении или обновлении записей, что особенно важно для сохранения истории эксплуатации [2]. Например, при списании единицы техники соответствующая запись помечается как неактивная, но все связанные с ней записи о ремонтах, недостатках и закреплениях сохраняются в архивных таблицах, обеспечивая возможность формирования статистики отказов за длительный период. Для оптимизации производительности запросов к часто используемым полям (таким как идентификаторы подразделений, статусы техники, даты событий) созданы соответствующие индексы.

Отдельного внимания заслуживает таблица настроек (settings), которая хранит гибкие параметры системы, такие как пороговые значения для формирования уведомлений (например, за сколько дней начинать оповещать об истечении срока технического осмотра). Это позволяет адаптировать систему под регламенты конкретного подразделения без изменения программного кода. В таблице настроек также хранятся параметры отображения интерфейса, настройки фильтрации по умолчанию и другие конфигурационные параметры, делающие систему гибкой и настраиваемой.

Приложение построено с использованием паттерна MVC (Model-View-Controller) в упрощенном виде [4]. Логика работы с данными реализована в PHP-скриптах, которые взаимодействуют с базой данных через PDO (PHP Data Objects) – слой абстракции, обеспечивающий безопасную и единообразную работу с различными СУБД [4]. Использование подготовленных выражений (prepared statements) через PDO гарантирует, что любые пользовательские данные интерпретируются исключительно как значения, а не как исполняемый SQL-код, что полностью исключает риски SQL-инъекций.

Пользовательский интерфейс создан с использованием HTML, CSS и JavaScript и адаптирован для отображения на различных устройствах, включая планшеты и ноутбуки с различным разрешением экрана. Применение современных подходов к верстке (Flexbox, Grid) и адаптивного дизайна позволяет комфортно работать с системой как на стационарных компьютерах с большими мониторами, так и на полевых ноутбуках с ограниченным разрешением экрана. Для повышения отзывчивости интерфейса используются AJAX-запросы, позволяющие обновлять отдельные части страницы без полной перезагрузки, что особенно актуально при работе с фильтрами и формами редактирования. В текущей версии прототипа безопасность на уровне приложения обеспечивается параметризацией SQL-запросов через PDO, что полностью исключает риски SQL-инъекций [4, 5]. На уровне базы данных используется система привилегий MySQL, ограничивающая права подключения и выполнения операций для разных категорий пользователей [5]. Для подключения к базе данных созданы отдельные учетные записи с минимально необходимыми привилегиями (SELECT, INSERT, UPDATE, DELETE только для конкретных таблиц), что снижает потенциальный ущерб в случае компрометации учетных данных приложения.

Главной инновационной особенностью системы является модуль автоматического мониторинга событий, реализованный на главной странице. При загрузке страницы выполняются запросы к базе данных, которые рассчитывают разницу между текущей датой и всеми критическими датами: окончанием срока действия водительских прав, медицинского осмотра, технического осмотра, страховки, ресурса аккумуляторных батарей, а также датой увольнения военнослужащего. Полученные значения сравниваются с настройками из таблицы settings.

Информация о просроченных или приближающихся к окончанию событиях, а также о технике, находящейся в ремонте или имеющей задокументированные недостатки, собирается в единый список, сортируется по степени критичности и отображается пользователю с соответствующей цветовой индикацией. Красный цвет сигнализирует о критических проблемах (просрочено), желтый – о событиях, требующих внимания в ближайшее время (например, заканчивающийся срок действия документа), синий – о технике, находящейся в ремонте, зеленый – о полностью исправной и готовой к применению технике.

Интерфейсы управления личным составом и техникой предоставляют расширенные формы для ввода и редактирования всей необходимой информации. Особое внимание уделено удобству ввода повторяющихся данных, таких как списки шин, недостатков или закреплений, с помощью динамического добавления полей [4]. Например, при вводе информации о недостатках техники пользователь может добавить произвольное количество записей в одной форме, указав для каждой наименование недостатка, дату обнаружения и планируемый срок устранения. Система автоматически связывает эти записи с соответствующей единицей техники и включает их в общий мониторинг.

Для удобства работы с большими объемами данных предусмотрена гибкая система фильтрации и сортировки. Пользователь может выполнять множественную фильтрацию по подразделениям, статусам, типам техники, наличию недостатков и другим параметрам. Все фильтры объединяются между собой по принципу логического «И», что позволяет сужать выборку до нужного набора записей. Например, можно отобразить все автомобили КамАЗ в третьей роте, имеющие недостатки, требующие устранения в текущем месяце. Внедрение разработанной автоматизированной системы в деятельность технических частей подразделений Вооруженных Сил Республики Беларусь позволит достичь значительных практических результатов. Во-первых, повысится оперативность управления: должностные лица получают инструмент для мгновенного получения достоверной информации о состоянии каждой единицы техники и готовности водительского состава. Время получения сводной информации по парку техники сокращается с нескольких часов (при ручном обходе и сверке журналов) до нескольких секунд.

Во-вторых, обеспечивается профилактика нарушений и отказов техники: автоматический контроль сроков обслуживания и действия документов позволяет предотвратить эксплуатацию техники с просроченными свидетельствами или неисправностями, что напрямую влияет на безопасность и боеготовность [3]. Система также позволяет отслеживать динамику накопления недостатков по каждой единице техники, выявлять образцы с наибольшим количеством отказов и принимать своевременные решения о выводе их в ремонт или списании.

В-третьих, снижается трудоемкость учетных операций: автоматизация рутинных процессов поиска, систематизации и формирования отчетов высвобождает время личного состава для выполнения прямых обязанностей по обслуживанию и ремонту ВВСТ.

Таким образом, в результате проведенной работы создан и описан прототип автоматизированной системы контроля состояния ВВСТ, адаптированный для условий подразделений Вооруженных Сил Республики Беларусь. Система базируется на современных веб-технологиях (PHP, MySQL) [4], использует эффективную реляционную модель данных [2] и включает модуль автоматического мониторинга критических событий. Такой подход позволяет перейти от пассивного учета к проактивному управлению техническим состоянием и кадровыми ресурсами, что, в свою очередь, способствует повышению боеготовности и эффективности выполнения задач по предназначению [1, 3]. Разработанная система представляет собой готовую к внедрению основу, которая может быть адаптирована под специфику конкретных подразделений и дополнена необходимыми модулями в зависимости от стоящих задач. Дальнейшие исследования будут направлены на расширение функциональных возможностей системы, интеграцию с существующими автоматизированными системами управления войсками и оружием, а также на разработку методического обеспечения для подготовки личного состава к работе с системой.

Список использованных источников:

1. Дейт, К. Дж. Введение в системы баз данных / К. Дж. Дейт. – 8-е изд. – М. : Вильямс, 2019. – 1328 с.

2. Кузнецов, С.Д. Основы баз данных / С.Д. Кузнецов. – 2-е изд. – М. : Интернет-Университет Информационных Технологий, 2020. – 488 с.

3. Лукьянов, В.С. Автоматизированные системы управления войсками и оружием / В.С. Лукьянов, В.В. Ткаченко. – М. : Воениздат, 2021. – 352 с.

4. Ульман, Л. PHP и MySQL. Создание динамических веб-сайтов / Л. Ульман. – М. : Эксмо, 2022. – 480 с.

5. Шварц, Б. MySQL. Оптимизация производительности / Б. Шварц, П. Зайцев, В. Ткаченко. – 3-е изд. – СПб. : Символ-Плюс, 2021. – 1056 с.

UDC 004.9:355.5

AUTOMATED SYSTEM FOR MONITORING THE CONDITION OF ARMAMENT AND MILITARY EQUIPMENT IN THE UNITS OF THE ARMED FORCES OF THE REPUBLIC OF BELARUS

Firsov A.A[1]

Belarusian State University of Informatics and Radioelectronics[1], Minsk, Republic of Belarus

Gerasimov A.S.

Annotation. The article considers the problem of automating the processes of recording and monitoring the technical condition of armament and military equipment in the units of the Armed Forces of the Republic of Belarus. The aim of the work is to develop a prototype of a web-based information system for centralized storage and processing of data on the condition of equipment and personnel. A three-tier client-server architecture using PHP and MySQL technologies is proposed. Mechanisms for automatic monitoring of critical events, a notification system about upcoming and overdue deadlines, as well as filtering and analytics tools are described. Special attention is paid to information security issues, including protection against SQL injections and the prospective implementation of a role-based access control model. The development is aimed at reducing time costs, increasing information reliability, and improving department manageability.

Keywords. *Automation, armament and military equipment, military accounting, web application, condition monitoring, databases, notifications, PHP, MySQL, information security.*

ПРИМЕНЕНИЕ СОВРЕМЕННЫХ МЕТОДОВ ДИАГНОСТИКИ ПСИХОЛОГИЧЕСКОГО СОСТОЯНИЯ ВОЕННОСЛУЖАЩИХ

Никитенко Р.А.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Герасимов А.С.

Аннотация: В работе обоснована необходимость автоматизации процесса диагностики психологического состояния военнослужащих-контрактников. Проанализированы недостатки существующей системы: высокая временная нагрузка на военных психологов, отсутствие инструментов для самодиагностики, сложность сбора и анализа данных, невозможность своевременного выявления критических случаев. В качестве решения предложена архитектура Telegram-бота, автоматический расчет уровня проблемы с цветовой маркировкой (зеленый/желтый/красный) и централизованное хранение результатов в базе данных. Разработаны алгоритмы подсчета баллов, определения уровня проблемы и формирования персонализированных рекомендаций. Внедрение системы позволяет минимизировать влияние человеческого фактора, сократить время обработки результатов диагностики, обеспечить оперативный доступ к данным для военного психолога и своевременно выявлять военнослужащих, нуждающихся в срочной помощи.

Диагностика психологического состояния военнослужащих является одним из ключевых условий поддержания их психического здоровья, боеспособности и успешной адаптации к условиям службы [1]. В соответствии с нормативными документами Министерства обороны Республики Беларусь, психологическая работа с военнослужащими включает проведение психодиагностических мероприятий, оказание индивидуальной и групповой психологической помощи, обучение навыкам саморегуляции и совладания со стрессом, а также выявление военнослужащих, нуждающихся в углубленном психологическом сопровождении [2].

В настоящее время в большинстве воинских частей диагностика психологического состояния военнослужащих проводится очно — в кабинете психолога части с использованием бумажных опросников либо разрозненных электронных таблиц, не объединённых в единую информационную систему. Такой подход порождает ряд системных проблем:

- высокие временные затраты военных психологов на проведение диагностики и обработку результатов;
- отсутствие инструментов для самостоятельной диагностики, что вынуждает военнослужащих обращаться к психологу лично, преодолевая психологический барьер;
- значительный риск ошибок из-за человеческого фактора, несвоевременное отражение данных о психоэмоциональном состоянии личного состава;

Перечисленные недостатки ведут к снижению качества психологической работы, затрудняют своевременное выявление военнослужащих, находящихся в критическом состоянии, а в отдельных случаях могут стать причиной пропуска начальных стадий посттравматического стрессового расстройства, тревожных и депрессивных состояний. В совокупности это приводит к снижению эффективности психологического сопровождения личного состава, росту временных затрат военных психологов и невозможности оперативного принятия решений на основе актуальных данных о психоэмоциональном состоянии военнослужащих [1].

Исходя из этого, существует потребность в разработке собственного программного продукта для автоматизации диагностики психологического состояния военнослужащих-контрактников, адаптированного к требованиям белорусского законодательства и организационной структуре воинских частей.

Внедрение такой системы позволит:

- сократить временные затраты военных психологов на проведение диагностики и обработку результатов;
- повысить достоверность данных за счёт автоматического подсчета баллов, расчёта процента и определения уровня проблемы;

Таким образом, внедрение автоматизированной системы диагностики психологического состояния позволит воинским частям вести учёт психоэмоционального состояния личного состава с необходимой полнотой и достоверностью, исключить ошибки, связанные с человеческим фактором, и, что особенно важно, позволит военным психологам сосредоточиться на оказании адресной помощи военнослужащим, нуждающимся в срочном вмешательстве, непосредственно влияющем на сохранение психического здоровья, боеспособности и эффективности деятельности подразделения.

Список использованных источников:

1. Программа психологического обеспечения в Вооруженных Силах Республики Беларусь: утв. Министром обороны Респ. Беларусь 12.03.2021. — Минск: МО РБ, 2021. — 45 с.-

2. Инструкция о порядке организации психологической работы в Вооруженных Силах Республики Беларусь: утв. Министром обороны Респ. Беларусь 15.06.2022. — Минск: МО РБ, 2022. — 32 с.

НЕОБХОДИМОСТЬ АВТОМАТИЗАЦИИ ПРОЦЕССА УЧЕТА МАТЕРИАЛЬНЫХ СРЕДСТВ

Чернявский В.К.

Белорусский государственный университет информатики и радиоэлектроники г. Минск, Республика Беларусь

Герасимов А.С.

В работе обоснована необходимость автоматизации процесса учёта материальных средств. Проанализированы недостатки существующей системы: высокие временные затраты, риск потери данных, отсутствие оперативного доступа к информации и сложность формирования отчётности. В качестве решения предложена архитектура автоматизированной информационной системы, обеспечивающая централизованное хранение данных. Разработаны алгоритмы формирования отчётности, контроля движения активов и технического состояния материальных средств. Внедрение системы позволяет минимизировать влияние человеческого фактора, сократить время обработки транзакций и обеспечить прозрачность учёта.

Учет материальных средств является одним из ключевых условий обеспечения боеготовности и повседневной деятельности подразделения. В соответствии с инструкцией о порядке учёта материальных средств, учёту подлежат все виды вооружения, техники, боеприпасов, вещевого, инженерного, медицинского имущества и других материальных ценностей, закреплённых за воинскими частями. Документальное оформление приёмки, перемещения, списания и выдачи имущества регламентируется ведомственными нормативными актами и предполагает ведение книг, карточек учёта, накладных, актов и иных первичных документов [1].

В настоящее время в большинстве подразделений учёт ведётся с использованием журналов либо разрозненных электронных таблиц, не объединённых в единую информационную систему. Такой подход порождает ряд серьезных проблем:

-высокие временные затраты должностных лиц на ручное заполнение и регистрацию учётных документов;

-значительный риск ошибок из-за человеческого фактора, несвоевременное отражение данных о состоянии оборудования, потеря и порча документации;

-отсутствие оперативного доступа к актуальным данным о наличии и движении материальных средств для командиров и довольствующих органов;

-сложность и трудоёмкость формирования сводных отчётов.

Перечисленные недостатки ведут к снижению качества учётных процессов, затрудняют планирование закупок и обслуживания, а в отдельных случаях могут стать причиной неучтенного или утраченного оборудования. В совокупности это приводит к снижению эффективности управления материально-техническим обеспечением, а также к увеличению трудоёмкости учетных процессов и невозможности оперативно реагировать на разного рода изменения условий.

Исходя из этого, существует потребность в разработке собственной автоматизированной системы учёта материальных средств, адаптированной к требованиям белорусского законодательства и организационной структуре подразделений.

Внедрение такой системы позволит:

-сократить временные затраты должностных лиц на оформление первичных документов и ведение учёта;

-повысить достоверность данных за счёт автоматической проверки корректности записей;

-обеспечить доступ к информации о наличии и движении материальных средств в режиме реального времени;

-автоматизировать формирование установленных форм отчётности;

-усилить контроль за сохранностью, перемещением и списанием имущества.

Для достижения перечисленных целей наиболее целесообразным решением является создание модульной автоматизированной системы на базе открытого программного обеспечения с использованием веб-технологий.

Данный вариант обеспечивает оптимальный баланс между гибкостью и возможностью самостоятельной доработки системы под специфические требования ведомственного учёта, в отличие от коммерческих решений, требующих значительных лицензионных отчислений, и от полностью заказной разработки, сопряжённой с высокими затратами на проектирование и сопровождение.

Предлагаемая архитектура включает клиентскую часть - веб-интерфейс с ролевой моделью доступа, серверную часть, реализующую бизнес-логику, централизованное хранилище данных на базе реляционной СУБД, а также модуль генерации отчётности с использованием встроенных шаблонов . Для обеспечения отказоустойчивости системы необходимо предусмотреть резервное копирование хранилища данных.

Ключевым элементом автоматизации является реализация алгоритмов, обеспечивающих достоверность и оперативность учёта в полном соответствии с требованиями инструкции о порядке учета материальных средств и установленными в ней формами первичных документов. В рамках разрабатываемой автоматизированной системы предложены следующие алгоритмы, охватывающие ключевые учётные процессы.

Алгоритм приемки материальный средств:

-материально-ответственное лицо вносит в систему данные из товаросопроводительных документов;

-система автоматически определяет код номенклатуры, присваивает объекту уникальный идентификатор и проверяет корректность вводимых данных;

-формирует приходный ордер на основании товарно-транспортной накладной.

Алгоритм перемещения и выдачи имущества:

-система проверяет наличие имущества у передающей стороны;

-фиксируются время, ответственные лица и основание перемещения (приказ, наряд);

-генерируется накладная (при выдаче со склада в подразделение) или раздаточная ведомость;

-при выдаче материальных средств в личное пользование военнослужащим, проходящим военную службу по контракту, система формирует записи в электронных карточках учета.

Все изменения о текущем местонахождении и ответственном лице отражаются в режиме реального времени.

Алгоритм контроля сроков эксплуатации и списания:

-на основе данных о вводе в эксплуатацию, ресурсе и периодичности поверки система ежедневно отслеживает приближение дат списания или поверки;

-формирует уведомления ответственным лицам;

-до завершения инвентаризации и утверждения акта списания система блокирует операции с соответствующими материальными средствами.

Алгоритм отправки оборудования в ремонт:

-на основании акта технического состояния система формирует наряд на ремонт (при плановом ремонте) или накладную (при передаче в ремонтное подразделение);

-при сдаче в ремонт имущество не исключается с учёта, а перемещается на отдельный учет;

-вся история операций фиксируется в отдельном списке с указанием времени и пользователя, обеспечивая.

Однако автоматизация не заменяет должностных лиц в тех процессах, где требуется экспертная оценка, решение командира или ответственного лица. Поэтому необходим алгоритм комиссионного принятия решений, который сопровождает, но не подменяет человеческое участие:

-система выявляет материальные средства, у которых истёк срок эксплуатации и формирует уведомление командиру подразделения;

-командир назначает комиссию;

-члены комиссии вводят в систему результаты осмотра: фактическое техническое состояние, остаточный ресурс, наличие дефектов;

система автоматически формирует акт технического состояния на основе введённых данных, но окончательное заключение комиссии вносится вручную и подписывается электронными подписями всех членов комиссии;

если комиссия рекомендует списание, система подготавливает акт списания, но решение об утверждении принимает командир воинской части (или вышестоящий орган);

-только после подписания акта уполномоченным должностным лицом система выполняет списание и вносит запись в журнал выбытия.

Таким образом, система берёт на себя контроль сроков эксплуатации, формирование документов, проверку корректности и блокировку операций для предотвращения несанкционированного перемещения или выдачи имущества, в отношении которого инициирована процедура списания, ремонта или инвентаризации, до принятия окончательного решения уполномоченным должностным лицом или комиссией. Решение о списании, переводе в другую категорию или ремонте остаётся за человеком.

Внедрение данной автоматизированной системы учёта позволит подразделениям вести учёт материальных средств с четким разделением зон ответственности между системой и должностными лицами, с необходимой полнотой и достоверностью. Это позволяет исключить ошибки, связанные с человеческим фактором, и, что особенно важно, позволяет сотрудникам сосредоточиться на выполнении задач первостепенной важности, непосредственно влияющих на боеспособность и эффективность деятельности подразделения.

Список использованных источников:

1. Инструкция о порядке учета материальных средств в органах пограничной службы Республики Беларусь: утв. приказом Госпогранкомитета Республики Беларусь от 30.12.2014 № 606. – Минск, 2014.

2. Инструкция по техническому обеспечению связи, автоматизированной системы информационного обеспечения и радиотехнического обеспечения полетов в органах пограничной службы Республики Беларусь: утв. приказом Председателя Госпогранкомитета Республики Беларусь от 10.07.2010 № 455. – Минск, 2010.

ИСТОРИЯ РАЗВИТИЯ СЕТЕЙ DMR РАДИОСВЯЗИ

Запариванный А.В.

Белорусский государственный университет информатики и радиоэлектроники г. Минск, Республика Беларусь

Герасимов А.С.

Аннотация. В данной работе прослеживается путь становления стандарта Digital Mobile Radio (DMR) от первых спецификаций ETSI до современных транкинговых систем. Рассматриваются технические особенности технологии TDMA, обеспечивающей два логических канала в одной полосе частот, и этапы эволюции уровней Tier I, II и III.

Истоки стандарта DMR восходят к 1990-м годам, когда на рынке профессиональной радиосвязи стала очевидна необходимость унификации цифровых технологий для малых и средних предприятий. Аналоговые системы уже не справлялись с растущими требованиями по качеству связи и эффективности спектра. В этот период формировались фундаментальные принципы DMR — использование TDMA, цифровое кодирование голоса и базовые протоколы управления вызовами..

Стандарт Digital Mobile Radio (DMR), утвержденный ETSI в 2005 году, стал ответом на острую нехватку радиочастотного спектра и необходимость перехода от устаревающих аналоговых систем к цифровым. Сегодня это не просто протокол двусторонней голосовой связи, а комплексная мультисервисная платформа. Цель доклада — проанализировать историческую трансформацию архитектуры DMR-сетей и рассмотреть векторы их интеграции в современные ИТ-инфраструктуры.[1]

Историческим прорывом DMR стало внедрение технологии временного разделения каналов (TDMA). Организация двух независимых тайм-слотов на одной частоте шириной 12,5 кГц позволила удвоить абонентскую емкость сети без выделения новых номиналов частот, одновременно существенно снизив энергопотребление абонентских терминалов.

В первые годы развития DMR основное внимание уделялось созданию простых и доступных цифровых устройств, способных заменить аналоговые радиостанции с улучшенным качеством звука и повышенной эффективностью использования спектра.

Начальный уровень стандарта DMR — Tier I, он представляет собой простейшее применение технологии, ориентированное на локальную, персональную и маломасштабную радиосвязь. Tier I предназначен для работы в не лицензируемом диапазоне частот и не требует использования ретрансляторов или инфраструктуры базовых станций. В этом режиме устройства функционируют в режиме «точка-точка» или «точка-многоточка» на ограниченном радиусе действия, обеспечивая базовую цифровую голосовую связь и низкую сложность эксплуатации.

Развитие стандарта характеризуется последовательным усложнением сетевой архитектуры:

Tier II (Конвенциональные сети): Переход к использованию ретрансляторов и технологии IP Site Connect. Объединение базовых станций по IP-каналам стерло географические границы радиовидимости, позволив строить распределенные региональные сети. Компании начали массово внедрять Tier II-конвенциональные сети с ретрансляторами и IP Site Connect, что позволило строить распределённые сети с расширенным радиусом действия. Это был важный этап, поскольку он позволил перейти от локальной связи к региональной, интегрированной через IP-инфраструктуру.

Tier III (Транкинговые системы): Внедрение выделенного канала управления (Control Channel) обеспечило динамическое и автоматическое распределение радиоресурсов, что стало обязательным стандартом для крупных промышленных и ведомственных сетей с высокой плотностью абонентов.[2]

Драйвером эволюции DMR стало технологическое соревнование и сотрудничество ведущих вендоров (Motorola Solutions, Hytera и др.). Разработка ими проприетарных расширений — продвинутых алгоритмов роутинга, диспетчеризации и шифрования — сформировала современный облик стандарта, сохранив при этом необходимую межоборудованную совместимость на базовом уровне.

Параллельно с сетевой архитектурой развивалось конечное оборудование. Современный этап требует узкоспециализированных решений: от высокопроизводительных базовых станций до защищенных терминалов (таких как радиостанции серии «Клён» и их аналоги). Фокус сместился на отказоустойчивость, поддержку сложных криптографических протоколов и возможность кастомизации под конкретные задачи заказчика.

Значительным этапом в истории развития DMR стало формирование мощных аппаратно-программных экосистем вокруг решений ведущих производителей. Конкурентная борьба таких гигантов, как Motorola и Hytera, исторически стимулировала быстрое расширение базового стандарта за счет дополнительных функций — от передачи телеметрии до сложных систем диспетчеризации. Однако не менее важным вектором эволюции стала возможность разработки на базе открытого стандарта DMR специализированных, криптографически защищенных платформ. Ярким примером такого развития является создание локализованных линеек оборудования — профессиональных

радиостанций серии «Клён». Появление подобных устройств продемонстрировало, что гибкая архитектура DMR позволяет проектировать высокозащищенные узлы связи, полностью адаптированные под строгие региональные стандарты информационной безопасности, сохраняя при этом все фундаментальные преимущества технологии TDMA.[3]

Основным преимущество цифрового сигнала от аналоговый сигнала является то, что цифровой обработанный сигнал останется четким до тех пор, пока сигнал не будет потерян, в то время как аналоговый сигнал теряет свое качество и разборчивость по мере уменьшения его мощности. Основное отличие в поведении сигналов при снижении мощности заключается в том, что аналоговый сигнал деградирует постепенно, а цифровой — сохраняет качество до резкого обрыва. Цифровой сигнал кодирует информацию в виде дискретных значений (обычно 0 и 1). Благодаря этому цифровой сигнал устойчив к шумам и искажениям: пока уровень сигнала остается выше определенного порога, данные могут быть восстановлены без потерь, что представлено на рисунке 1 [4]

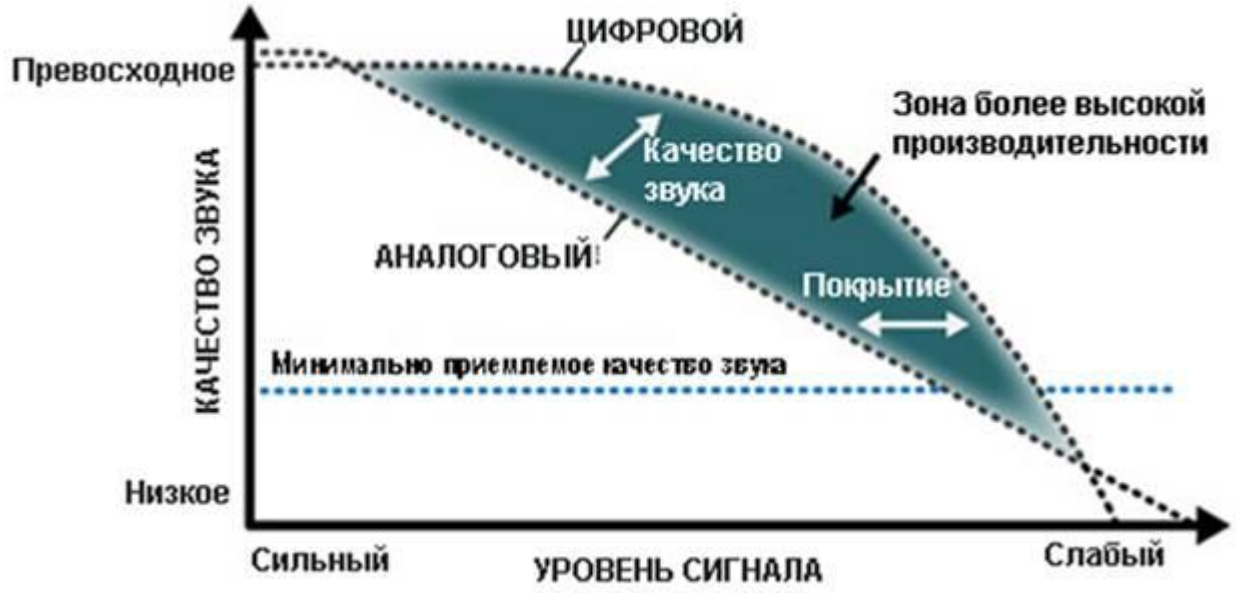

Рисунок 1 — Расширение зоны качественной связи в DMR по сравнению с аналоговыми системами радиосвязи.

Продолжая тему истории развития DMR-сетей радиосвязи, стоит отметить, что с течением времени требования к системам связи значительно выросли, что стимулировало дальнейшее совершенствование стандарта. В частности, с развитием мобильных и корпоративных коммуникаций появилась необходимость интеграции DMR с современными информационными технологиями и сетями передачи данных. Это привело к появлению гибридных решений, сочетающих традиционную радиосвязь с IP-технологиями, что расширило функциональные возможности систем и повысило их масштабируемость.

Важным этапом стало внедрение поддержки передачи данных в реальном времени, включая текстовые сообщения, геолокацию и телеметрию. Эти функции позволили использовать DMR не только для голосовой связи, но и для комплексного мониторинга и управления объектами, что особенно актуально для промышленных и муниципальных служб. Кроме того, развитие криптографических методов защиты информации стало ключевым направлением. С ростом угроз информационной безопасности производители начали активно внедрять в DMR-оборудование современные алгоритмы шифрования и аутентификации, что обеспечило высокий уровень конфиденциальности и устойчивости к внешним воздействиям

Исторический путь узкополосного стандарта DMR сегодня пересекается с широкополосными сетями (LTE/5G). Внедрение гибридных терминалов и PoC-решений, а также использование радиосети как надежного транспортного уровня для интернета вещей и систем телеметрии определяют будущее профессиональной радиосвязи. Развитие сетей DMR демонстрирует пример исключительно успешной и гибкой стандартизации. Начав с решения базовой физической проблемы нехватки частот, архитектура стандарта эволюционировала до уровня глобальных транкинговых систем, способных бесшовно интегрироваться в единую цифровую среду.

Список использованных источников:

1.TS 102 361-1. Digital Mobile Radio (DMR) Systems. – ETSI, 2005. – 121 p.
2.Стандарты и технологии подвижной радиосвязи / Ю.А. Громаков. – М. : Эко-Тренд, 2009. – 232 с.
3.Современное состояние стандарта DMR / А.В. Смирнов [и др.] // Вестник связи, 2018. – С. 15-20.
4. DIGITAL MOBILE RADIO THE VERY BASICS / John 'Miklor', 2018. – 4 с.

УДК 004.7:621.395

IP-ТЕЛЕФОНИЯ: ЭВОЛЮЦИЯ И ПРОБЛЕМЫ ВНЕДРЕНИЯ В СИСТЕМАХ ВОЕННОГО УПРАВЛЕНИЯ

Барковский В.Д.[1], студент гр. 233702

Белорусский государственный университет информатики и радиоэлектроники[1]
г. Минск, Республика Беларусь

Викторович М.А. – преподаватель кафедры связи

Аннотация. Развитие VoIP-технологий кардинально изменило подход к организации связи в системах военного управления. Сегодня IP-телефония рассматривается не просто как альтернатива классической проводной связи, а как ключевой элемент построения гибких, защищенных и масштабируемых сетей специального назначения. Технологии не стоят на месте, и уже сейчас IP-решения интегрируются в контуры тактического и стратегического звена, обеспечивая командованию больше, чем просто голосовую связь.

Ключевые слова. VoIP, IP-телефония, военные системы связи, CTI, ITSP, LCR, 5G, AI, WebRTC, защищенная связь, устойчивость управления, DDoS-атаки, тактический уровень.

В 21 веке бурный рост числа систем передачи данных привел к тому, что многие привычные потребительские услуги предоставляются теперь по-новому: электронная почта заменила традиционную бумажную, электронная коммерция позволяет заказывать и оплачивать товары не выходя из дому, и т.д. Одним из наиболее значимых направлений стала IP-телефония, которая уже давно составляет конкуренцию классическим операторам, а в оборонной сфере приобретает статус критической технологии. Чем же она привлекает военных связистов и командование?

Тенденция интеграции телефонных разговоров в единые сети передачи данных нашла развитие в концепции CTI (Computer Telephone Integration), которая сегодня адаптируется для нужд автоматизированных систем управления войсками. Однако наиболее перспективной с точки зрения оперативности и живучести является IP-телефония, так как при ее реализации достигается не только значительное сокращение затрат на развертывание инфраструктуры, но и повышается гибкость управления связью. В военных приложениях принцип LCR (Least Cost Routing System) трансформируется в принцип выбора наиболее устойчивого и защищенного маршрута связи, что критически важно в условиях радиоэлектронной борьбы и повреждения части инфраструктуры.

IP-телефония в военной среде начиналась с масштабов стационарных узлов связи стратегического уровня. В процессе развития цифровизации армии практически каждое соединение сталкивалось с необходимостью модернизации существующих сетей связи. До недавнего времени выбор ограничивался двумя вариантами: развитие классических проводных линий или аренда ресурсов у гражданских операторов.

Первый вариант, основанный на развертывании собственных физических линий, обеспечивает высокий уровень контроля и безопасности, однако требует значительных капитальных затрат и развертывания сложной эксплуатационной инфраструктуры. Второй вариант, предполагающий использование инфраструктуры гражданских операторов, подходит для тыловых и административных объектов, но не гарантирует требуемого уровня защищенности и устойчивости в условиях военных действий.

Появившаяся в последние десятилетия третья возможность — IP-телефония на базе защищенных ведомственных сетей — позволяет организовать корпоративную военную сеть связи, вкладывая средства в развитие единой цифровой инфраструктуры и сокращая расходы на обслуживание разнородных систем. Однако вопросы безопасности, электромагнитной совместимости и сертификации оборудования IP-телефонии для применения в Вооруженных Силах остаются критически важными. Именно поэтому на вооружении современных армий появляются специализированные решения, аналогичные коммерческим ITSP, но функционирующие в закрытых сегментах и подчиненные требованиям органов военного управления [1].

На сегодняшний день IP-телефония занимает значимое место в системах связи вооруженных сил. По данным аналитических обзоров, более 60% стран НАТО и ОДКБ активно внедряют VoIP-решения в инфраструктуру военных баз, штабов и узлов связи, а перспективные программы модернизации предусматривают полный переход на пакетную передачу голоса и данных [2].

Ключевыми разработчиками в этой области выступают как мировые лидеры оборонной электроники, так и отечественные предприятия, создающие защищенные коммуникационные платформы, соответствующие требованиям по устойчивости, криптостойкости и живучести.

Ключевыми игроками на рынке остаются Cisco, Avaya и отечественные решения вроде МТС Exolve. Эти компании формируют экосистемы для общения, включающие голос, видео, обмен сообщениями и инструменты аналитики.

Основные преимущества:
- снижение затрат на развертывание и эксплуатацию инфраструктуры связи;
- интеграция с автоматизированными системами управления войсками;
- возможность организации защищенной связи с удаленными подразделениями;
- простота масштабирования и быстрого восстановления каналов связи взамен вышедших из строя.

Современная IP-телефония в военном сегменте давно перестала быть просто средством голосовой связи. Это элемент цифровой экосистемы, способный обеспечить командование всеми видами обмена информацией. Технологии IP-телефонии будущего в оборонной сфере определяются несколькими ключевыми трендами. Остановимся более подробно на каждом из них.

WebRTC (веб-коммуникация в реальном времени) — это технология, позволяющая совершать звонки прямо из браузера без установки дополнительных программ и плагинов. Это значительно упрощает процесс коммуникации и открывает новые возможности для нужд военного управления, позволяя организовывать защищенные каналы голосовой и видео-связи прямо из защищенных веб-интерфейсов автоматизированных рабочих мест командного состава без необходимости установки дополнительного оборудования. Это значительно повышает оперативность управления и скрытность связи. Примером могут служить специализированные API-платформы для военных коммуникаций, которые позволяют интегрировать голос, видео, текстовые сообщения и данные телеметрии в единый защищенный контур.

Искусственный интеллект в военных VoIP-системах открывает новые горизонты. Нейросети используются не только для голосового управления, но и для автоматического анализа переговоров, выявления ключевых команд, распознавания эмоционального состояния оператора, а также для фильтрации акустических помех боя. Системы на базе ИИ позволяют автоматизировать рутинные задачи дежурных служб, предоставляя командованию транскрипцию переговоров, сводки ключевых фраз и аналитику принятия решений.

Использование сетей 5G оказывает революционное влияние на качество IP-телефонии в тактическом звене. 5G обеспечивает минимальную задержку сигнала, что критически важно для управления роботизированными комплексами и беспилотными системами. Высокая пропускная способность позволяет передавать видео высокого разрешения с поля боя в реальном времени, что необходимо для ситуационной осведомленности командиров.

Происходят изменения в моделях развертывания IP-телефонии в вооруженных силах. Все большее распространение получают контейнеризированные и мобильные узлы связи, отказывающиеся от стационарных аппаратных комплексов в пользу программно-определяемых решений. Это снижает массогабаритные характеристики техники связи и повышает ее живучесть.

Одним из главных направлений развития военной инфраструктуры связи стала возможность интеграции IP-телефонии с системами боевого управления, что позволяет автоматически привязывать сеансы связи к тактической обстановке, сохранять протоколы переговоров и обеспечивать автоматическое документирование боевых распоряжений.

Вместе с ростом возможностей усиливается внимание к вопросам криптографической защиты и соблюдения режима секретности. Ведь голосовые данные в военной сфере содержат сведения, составляющие государственную тайну.

Основной мерой обеспечения безопасности в военной IP-телефонии является шифрование трафика с использованием сертифицированных криптографических средств. Протоколы TLS и SRTP дополняются отечественными алгоритмами шифрования, что исключает возможность технической разведки и перехвата. Это особенно важно для связи на тактическом уровне, где обсуждаются планы действий и передаются координаты целей.

В соответствии с требованиями ведомственных нормативных актов, операторы военных систем IP-телефонии обязаны обеспечивать не только защиту данных, но и гарантированную устойчивость связи в условиях преднамеренных деструктивных воздействий.

Преимущества IP-телефонии для военного ведомства выходят далеко за рамки экономии: они формируют совершенно новый облик систем управления.

Одним из главных стимулов для перехода на IP-телефонию остается возможность быстрого развертывания узлов связи. В отличие от традиционных каналов, VoIP-связь может быть организована в полевых условиях с использованием спутниковых и радиорелейных каналов, что сокращает время развертывания командных пунктов.

IP-телефония позволяет создавать гибкие системы связи, работающие вне зависимости от географического положения подразделений. Операторы и командиры могут подключаться из любого района выполнения задач — достаточно наличия защищенного канала связи. Это особенно актуально для подразделений специальных операций и распределенных группировок войск.

IP-телефония стирает барьеры между уровнями управления. Командование получает возможность взаимодействовать с подразделениями на тактическом, оперативном и стратегическом уровне, используя единую адресную систему и распределенные виртуальные узлы связи.

Указывая плюсы, стоит упомянуть минусы и возможные риски при использовании IP-телефонии:

Главное преимущество IP-телефонии — работа через интернет — одновременно является и ее слабым местом. Без устойчивого подключения вся система связи оказывается под угрозой. Задержки, прерывания, нестабильная полоса пропускания влияют на качество звонков и негативно сказываются на боевом опыте. Зависимость от качества каналов связи, которая в боевых условиях становится главным уязвимым местом. Без устойчивого подключения вся система управления оказывается под угрозой. Задержки, прерывания, воздействие средств РЭБ влияют на качество связи. В современной армии эту проблему решают путем создания резервированных каналов и использования адаптивных кодеков, устойчивых к помехам.

IP-телефония является объектом пристального внимания противника. Подмена номеров, перехват звонков, DDoS-атаки на узлы связи — реальные угрозы. Если звонки не шифруются, а система слабо защищена, риски компрометации информации возрастают многократно. Что поможет снизить риски? Эффективные системы мониторинга, ограничение по IP, двухфакторная авторизация и автоматические уведомления о подозрительной активности.

Еще один вызов — необходимость интеграции с унаследованными аналоговыми системами связи, которые до сих пор широко используются в Вооруженных Силах. Требуются сложные межсетевые экраны и шлюзы для обеспечения совместимости.

Высокий риск кибератак и радиоэлектронного подавления требует внедрения эффективных систем мониторинга, ограничения доступа по IP, двухфакторной аутентификации и постоянного анализа защищенности.

В эпоху цифровых изменений военному ведомству важно не просто внедрять новые технологии, но и использовать их с максимальной эффективностью для повышения боеспособности. Будущее военной IP-телефонии — это еще более глубокая интеграция с системами разведки, огневого поражения и управления, активное использование искусственного интеллекта и обеспечение гарантированной защиты данных.

Безопасность и соответствие требованиям по защите государственной тайны выходят на первый план: используются шифрование, системы мониторинга и многофакторная аутентификация, а также обязательная сертификация всех компонентов.

IP-телефония становится не просто средством связи, а центральным элементом цифровой трансформации военного управления, обеспечивающим командование полной ситуационной осведомленностью, возможностью быстрого реагирования и высокой живучестью системы управления войсками. Вместе с возможностями растут и риски — требования к защите, устойчивости и боевой готовности ужесточаются. Успех за теми, кто не просто внедряет технологии, а использует их как инструмент достижения превосходства на поле боя.

Список использованных источников:

1. Будущее IP-телефонии [Электронный ресурс]. Режим доступа 31.03.2026 https://www.mtt.ru/support/blog/budushchee-ip-telefonii/

2. IP-телефония: эволюция и проблемы внедрения [Электронный ресурс]. Режим доступа 31.03.26 https://www.ixbt.com/comm/iptelevol.html

3. Гольдштейн Б.С. IP-телефония / Б.С. Гольдштейн, А.В. Пинчук, А.Л. Суховицкий – М. : Радио и связь, 2001. – 336 с.

4. IP-телефония в 2026-2030м: тренды, технологии и перспективы развития [Электронный ресурс]. Режим доступа 31.03.2026 https://media.mts.ru/business/212167-analiz-budushchego-ip-telefonii

UDC 004.7:621.395

IP TELEPHONY: EVOLUTION AND DEPLOYMENT ISSUES

Barkovski V.D.[1]

Belarusian State University of Informatics and Radioelectronics[1]*, Minsk, Republic of Belarus*

Viktorovich M.A.

Annotation. The development of VoIP technologies has fundamentally changed the approach to organizing communications in military command and control systems. Today, IP telephony is considered not merely as an alternative to traditional wired communications, but as a key element in building flexible, secure, and scalable special-purpose networks. Technologies do not stand still, and IP solutions are already being integrated into tactical and strategic command echelons, providing command authorities with more than just voice connectivity.

Keywords. VoIP, IP telephony, military communication systems, CTI, ITSP, LCR, 5G, AI, WebRTC, secure communications, command resilience, DDoS attacks, tactical level.

УДК 621.396.4

БАЗОВЫЕ ПРИНЦИПЫ ПОСТРОЕНИЯ БЕСПРОВОДНЫХ СЕНСОРНЫХ СЕТЕЙ

Рац Р.А., магистрант

Учреждение образования «Военная академия Республики Беларусь», г. Минск, Республика Беларусь

Аскерко А.В. – кандидат военных наук, доцент

Аннотация: В статье рассмотрены состав и структура беспроводных сенсорных сетей (БСС), типовая архитектуры сенсорного узла как элемента сети. Представлен стандарт IEEE 802.15.4 для организации связи между узлами. Описаны технологии организации связи узлов в БСС. Проведен сравнительный анализ таких технологий организации связи как ZigBee, Bluetooth, Wi-Fi.

Ключевые слова: беспроводные сенсорные сети, сенсоры, стандарты беспроводных сенсорных сетей

Современный этап развития информационно-коммуникационных технологий характеризуется активным внедрением распределенных систем мониторинга и управления, основу которых составляют БСС Они представляют собой самоорганизующиеся сети и состоят из множества распределенных в пространстве беспроводных сенсорных узлов, предназначенных для мониторинга характеристик окружающей среды или объектов, расположенных в ней. Актуальность исследований в области БСС обусловлена широким спектром их применения: от экологического мониторинга и промышленной автоматизации до систем охраны, здравоохранения и оборонных приложений.

Сенсорные узлы развертываются с высокой плотностью и часто в больших количествах и поддерживают распознавание, обработку данных, встроенные вычисления и связь. Ресурсы сенсорных узлов в беспроводных сенсорных сетях ограничены с точки зрения возможности обработки информации, пропускной способности, объема памяти, вычислительных возможностей, что существенно отличает беспроводные сенсорные сети от других сетей [2]. Именно эти ограничения определяют основные требования к архитектуре, протоколам и технологиям, используемым при построении БСС. Они состоят из двух основных типов узлов [1]:

- сенсоры (сенсорные узлы), которые развертывают в местах мониторинга (сенсорное поле) для сбора данных изучаемого явления или процесса и их передачи на базовые станции;
- базовая станция (БС), также известная как шлюз или приемник, является интерфейсом, соединяющим сенсорную сеть с внешним миром. БС может являться центральной точкой в сенсорном поле или находиться в отдалении от него (рисунок 1).

БС несет ответственность за получение данных от сенсоров, их обработку и доставку конечному пользователю разнообразными способами, включая телекоммуникационную сеть онлайн или через спутник и другие сети. В современных реалиях базовая станция часто интегрируется с облачными платформами, что позволяет осуществлять хранение и анализ больших объемов данных. Структура беспроводной сенсорной сети приведена на рисунке 2 [1].

Каждая БСС состоит из беспроводных сенсорных узлов. Беспроводные сенсорные узлы представляют собой миниатюрные устройства с ограниченными ресурсами, связанными с зарядом батареи, объемом памяти и вычислительными возможностями.

Параметры узлов сети в зависимости от назначения сети могут варьироваться. При проектировании того или иного вида сети необходимо учитывать возможности узлов: энергоэффективность, вычислительные способности, возможность автономной работы и т. п.

Примеры конструкций современных сенсорных узлов приведены на рисунке 3.

Типовая архитектура сенсорного беспроводного узла состоит из четырех основных компонентов: источник питания, датчик, блок обработки, система связи (рисунок 4) [1].

Датчик собирает аналоговые данные из физического мира, и АЦП преобразует эти данные в цифровые данные. Основной процессор, который обычно является микропроцессором или микроконтроллером, выполняет интеллектуальную обработку данных и манипулирование ими. В современных узлах широко используются архитектуры ARM Cortex-M, а также специализированные чипы с поддержкой аппаратного шифрования.

В зависимости от решаемой задачи число сенсорных узлов в беспроводных сенсорных сетях, размещенных в сенсорном поле, может изменяться от нескольких сотен до тысяч или более.

Несмотря на название, сенсорный узел состоит не только из сенсорного компонента, но и из других важных объектов, таких как устройства обработки, связи и хранения. Благодаря всем этим функциям, компонентам и усовершенствованиям узел датчика отвечает за сбор данных физического мира, анализ сети, корреляцию данных и объединение данных другого датчика

с собственными данными. В зависимости от определенного конкретного применения сенсорные узлы могут также включать в себя дополнительные компоненты, такие как система позиционирования, чтобы определить их положение, мобилизатор, чтобы изменить их местоположение или конфигурацию (например, ориентация антенны), и так далее.

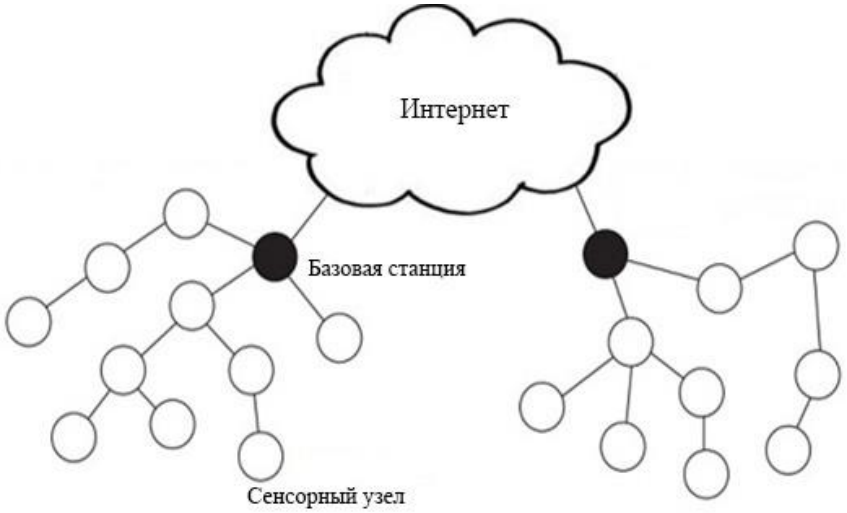

Рисунок 1 – Базовая станция в сети

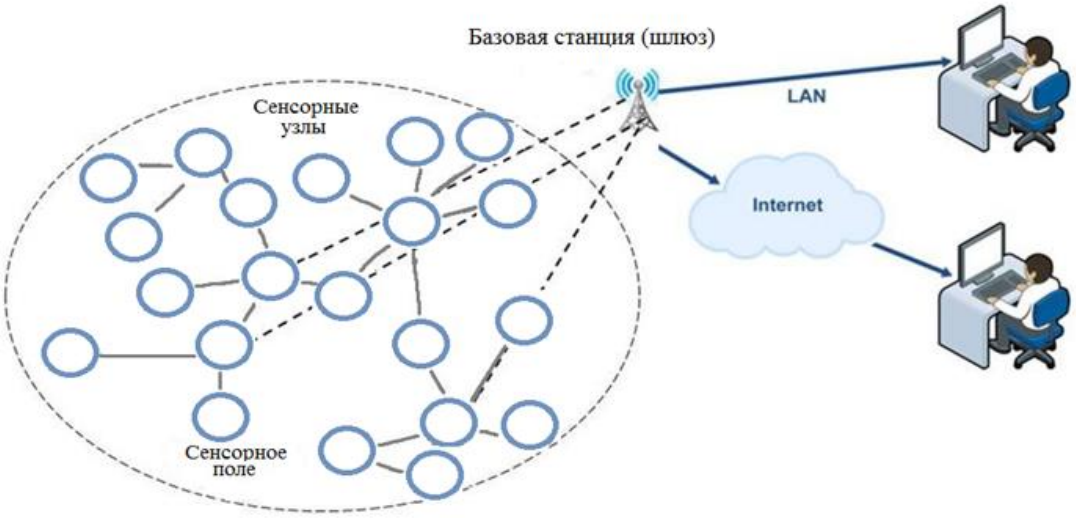

Рисунок 2 – Структура БСС

Рисунок 3 – Сенсорные узлы

Рисунок 4 – Типовая архитектура сенсорного узла

Для организации связи между узлами разработан стандарт *IEEE* 802.15.4. К этому стандарту относится технология *ZigBee* [2], позволяющая создавать самоорганизующиеся и самовосстанавливающиеся беспроводные сети с автоматической ретрансляцией сообщений и поддержкой батарейных и мобильных узлов. Сети *ZigBee* при относительно небольших скоростях передачи данных обеспечивают гарантированную доставку пакетов и защиту передаваемой информации.

Стандарт *ZigBee* предусматривает частотные каналы в диапазонах 868 МГц, 915 МГц и 2,4 ГГц. Наибольшие скорости передачи данных и наивысшая помехоустойчивость достигаются в диапазоне 2,4 ГГц. Скорость передачи данных вместе со служебной информацией в эфире составляет 250 кбит/с. При этом средняя пропускная способность узла для полезных данных в зависимости от загруженности сети и числа ретрансляций может лежать в пределах 5…40 кбит/с [2].

Расстояние между узлами сети составляют десятки метров при работе внутри помещения и сотни метров на открытом пространстве. За счет ретрансляций зона покрытия сети может значительно увеличиваться. В основной сети *ZigBee* лежит ячеистая топология (*mesh*-топология). В такой сети каждое устройство может связываться с любым другим устройством как напрямую, так и через промежуточные узлы сети. Ячеистая топология предлагает альтернативные варианты выбора маршрута между узлами. Сообщения поступают от узла к узлу, пока не достигнут конечного получателя.

Исключением из стандарта можно считать технологию *Bluetooth*, описываемую стандартом *IEEE* 802.15.1. Беспроводная сеть *Bluetooth* в классическом понимании – это беспроводная одноранговая динамическая сеть с переменным числом мобильных узлов с децентрализованным управлением, которая может быть развернута в ограниченном пространстве (с числом узлов до 80). Радиосвязь *Bluetooth* осуществляется в безлицензионном *ISM*-диапазоне (2,4…2,4835 ГГц) со скоростями 1 Мбит/с (версия 1.2); 3 Мбит/с (версия 2.0); 24 Мбит/с (версия 3.0) [2].

Для *Bluetooth* характерно стихийное создание мобильной сети массового пользователя, когда практически любой человек, владея таким радио интерфейсом, может к ней без труда подключиться, если, конечно, не решена политика безопасности от несанкционированного доступа. Это становится первостепенной задачей при использовании технологии *Bluetooth* для БСС.

Если говорить о *ZigBee*, то для этой технологии уже предусмотрены программно-аппаратные средства в виде *AES*-криптозащиты. В отличие от *Bluetooth*, *ZigBee* сеть представляет собой распределенную самоорганизующуюся беспроводную структуру, которая может простираться на многие километры и состоять из большого числа узлов. В ее архитектуре помимо возможностей подключения датчиков предусмотрено наличие центрального узла управления (в виде точки доступа с возможностью для подключения стационарного ПК или переносного компьютера, выполняющего функции управления и обработки информации). В настоящее время технология *ZigBee*, разработанная непосредственно для БСС, является по сути единственной технологией, с помощью которой можно решить любые задачи мониторинга и контроля, которые в том числе критичны ко времени отклика от датчиков.

Wi-Fi технология позволяет строить беспроводные самоорганизующиеся сети инфраструктурного типа, т. е. создавать многоточечную топологию с беспроводной точкой доступа для подключения мобильных абонентов. Однако такая топология, скорее является одним из недостатков, если рассматривать ее как вариант самоорганизующейся сети – выход из строя базовой станции приводит к падению мобильной радиосети в целом. В сетях *Wi-Fi* используются несколько модификаций стандарта 802.11 [3]. Основным преимуществом технологии являются простота принципов построения и настроек мобильного абонента под беспроводную сеть, но при этом *Wi-Fi* существенно проигрывает *ZigBee* по мобильности и энергопотреблению.

Сравнительный анализ технологий организации связи узлов БСС приведен в таблице 1.

Таблица 1 – Стандарты организации связи

Параметр	Стандарт		
	Bluetooth	*ZigBee*	*Wi-Fi*
Частота, ГГц	2,4	0,868/0,915/2,4	2,4,5…6
Число каналов	79	1/10/16	14
Скорость передачи	3 Мбит/с	20…250 кбит/с	11…10 Гбит/с
Уровень OSI	Физический, канальный	Физический, канальный (сетевой – приложения)	Физический, канальный
Радиус действия, м	10	10…100	100
Полоса пропускания канала, МГц	1	0,3/0,6; 2	22
Модуляция	*GFSK*	*BPSK, O-QPSK*	*BPSK, QPSK, COFDM, CCK, MQAM, QAM*
Число устройств в Сети	8	65 000	2007
Уровень мощности, дБ	0…30	От 0 (1 мВт)	20
Потребляемая мощность	40 мА TX, в режиме ожидания 0,2 мА	30 мА TX, в режиме ожидания 3 мкА	400 мА, в режиме ожидания 20 мА

Свойства сети зависят от многих факторов, таких как характеристики зоны (области) обслуживания, число и распределение узлов на плоскости или в пространстве, их параметры и других. Сеть может состоять из огромного числа узлов, для взаимодействия которых и обеспечения передачи данных используется кластеризация сети. Кластерная организация является эффективной и масштабируемой для функционирования БСС [2], но лишь при условии рационального выбора головного узла кластерной сети в конкретный момент времени.

Список использованных источников:

1. Авдеев А.А., Долматов Е.А. и др. Инфокоммуникационные системы специального назначения. Учебное пособие – СПб.: ВАС, 2017. – 456 с.

2. Лихтциндер Б.Я., Киричек Р.В., Федотов Е.Д., Голубничая Е.Ю. Беспроводные сенсорные сети. Учебное пособие для вузов / Б.Я. Лихтциндер, Р.В. Киричек, Е.Д. Федотов.;Под общей редакцией Б.Я. Лихтциндера. – М.: Горячая линия – Телеком, 2021. – 236 с.

3. Олифер В., Олифер Н. Компьютерные сети. Принципы, технологии, протоколы (6-е издание) – СПб.: Питер, 2021. – 1008 с.

UDC 621.396.4

BASIC PRINCIPLES OF BUILDING WIRELESS SENSOR NETWORKS

Rats R.A.

Military Academy of the Republic of Belarus, Minsk, Republic of Belarus

Askerko A.V., PhD of military science, assistant professor

Annotation: This article examines the composition and structure of wireless sensor networks (WSNs) as well as the typical architecture of a sensor node as a network element. The IEEE 802.15.4 standard for establishing communications between nodes is presented. Technologies for establishing communications between nodes in WSNs are described. A comparative analysis of communication technologies such as ZigBee, Bluetooth and Wi-Fi are provided.

Keywords: wireless sensor networks, sensors, wireless sensor technology standards.

РОЛЬ КОМПЬЮТЕРНЫХ ПРОГРАММ В ИЗУЧЕНИИ СЛОЖНЫХ КОМПЛЕКСОВ СВЯЗИ: СРАВНИТЕЛЬНЫЙ АНАЛИЗ ТРАДИЦИОННЫХ И ИНТЕРАКТИВНЫХ МЕТОДОВ

Высоцкий Д.М.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Викторович М.А.

Аннотация. В данной работе рассматриваются традиционные и интерактивные методы изучения сложных комплексов связи. Анализируются ограничения печатных руководств, схем и плакатов, а также преимущества компьютерных программ для изучения аппаратуры. Выделяются ключевые факторы эффективности интерактивного обучения: визуализация, доступность, безопасность и возможность многократного повторения. Показано, что компьютерные программы не заменяют работу с реальным оборудованием, но существенно повышают качество начальной теоретической подготовки специалистов связи.

Исторически сложились два основных подхода к изучению сложной аппаратуры связи. Первый — традиционный, основанный на использовании печатных руководств по эксплуатации, структурных и принципиальных схем, плакатов и макетов. Второй — современный, предполагающий применение компьютерных программ, визуализирующих устройство и логику работы комплекса в интерактивном режиме. Цель данной работы — провести сравнительный анализ этих подходов и определить роль компьютерных программ в процессе подготовки специалистов.

Традиционные методы обладают рядом неоспоримых достоинств. Руководства по эксплуатации содержат полную и достоверную информацию, проверенную разработчиками аппаратуры. Схемы позволяют проследить электрические и логические связи между блоками. Плакаты дают общее представление о внешнем виде и компоновке. Однако эти методы имеют существенные ограничения. Печатные материалы статичны и не позволяют динамически исследовать аппаратуру. Для понимания общей картины обучаемому необходимо одновременно удерживать в памяти информацию из разных разделов и с разных схем. Кроме того, доступ к качественным полноцветным иллюстрациям и схемам в печатном виде часто ограничен.

Компьютерные программы для изучения аппаратуры предлагают принципиально иные возможности. Во-первых, это интерактивная визуализация. Обучаемый может не просто смотреть на общую фотографию комплекса, а перемещаться между отдельными блоками, увеличивать интересующие участки, получать всплывающие подсказки при наведении на любой орган управления. Это превращает изучение из пассивного просмотра в активное исследование.

Во-вторых, компьютерные программы обеспечивают доступность. Электронное учебное пособие может быть размножено без потери качества, доступно в любое время и в любом месте, не требует выделения отдельных аудиторий для хранения плакатов и макетов. Это особенно важно при подготовке специалистов в условиях ограниченных ресурсов.

В-третьих, компьютерные программы обеспечивают безопасность изучения. На этапе знакомства с аппаратурой обучаемый неизбежно совершает ошибки в понимании назначения органов управления и последовательности действий. В реальных условиях такие ошибки могут привести к выходу аппаратуры из строя. В компьютерной программе ошибка не имеет материальных последствий, но фиксируется с последующим разбором.

В-четвертых, компьютерные программы позволяют многократно повторять материал без дополнительных затрат времени преподавателя и ресурсов. Обучаемый может возвращаться к сложным разделам столько раз, сколько необходимо для полного усвоения.

Таким образом, компьютерные программы для изучения сложных комплексов связи занимают важное место в системе подготовки специалистов. Они не заменяют традиционные методы, но эффективно дополняют их, обеспечивая интерактивность, доступность, безопасность и возможность многократного повторения. Наиболее рациональной представляется двухэтапная модель обучения: сначала компьютерное изучение устройства и логики работы комплекса, затем — практическая работа на реальной аппаратуре с уже сформированным пониманием. Данный подход может быть рекомендован для применения в учебных заведениях, готовящих специалистов в области связи.

Список использованных источников:

1. Захарова И.Г. Информационные технологии в образовании : учебное пособие для вузов. — М. : Академия, 2018. — 192 с.

2. Роберт И.В. Современные информационные технологии в образовании: дидактические проблемы, перспективы использования. — М. : ИИО РАО, 2019. — 248 с.

3. Красильникова В.А. Использование информационных и коммуникационных технологий в образовании : учебное пособие. — Оренбург : ОГУ, 2017. — 150 с.

4. Герасимов А.С. Применение интерактивных средств обучения при подготовке специалистов радиосвязи // Вестник БГУИР. — 2022. — Т. 20, № 3. — С. 55–60.

РОЛЬ КОМПЬЮТЕРНОЙ ФОРЕНЗИКИ В ОБЕСПЕЧЕНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В УСЛОВИЯХ ЦИФРОВОЙ ТРАНСФОРМАЦИИ

Шутко А.П.

Белорусский государственный университет информатики и радиоэлектроники г. Минск, Республика Беларусь

Герасимов А.С.

Аннотация: В статье обоснована необходимость автоматизации процесса удаленного сбора цифровых артефактов. Проанализированы недостатки существующих решений: высокая сложность развертывания, отсутствие гарантированной доставки данных, ограниченная гибкость настройки. В качестве решения предложена модульная архитектура системы, обеспечивающая централизованное хранение данных, локальное сохранение информации и расширяемость функциональности. Внедрение системы позволяет минимизировать потерю данных, сократить время получения информации и обеспечить прозрачность расследования.

Цифровая трансформация всех сфер деятельности общества привела к значительному росту числа компьютерных инцидентов и киберпреступлений. По данным Генеральной прокуратуры Республики Беларусь, в январе-феврале 2026 года количество зарегистрированных киберпреступлений увеличилось на 22 % по сравнению с аналогичным периодом прошлого года и составило более 3,1 тыс. преступлений [3]. В этих условиях особую значимость приобретает компьютерная форензика – область знаний, занимающаяся сбором, анализом и хранением цифровых доказательств, пригодных для использования в судебных процессах и внутренних расследованиях организаций [1].

Ключевыми принципами компьютерной форензики являются:

- неизменность доказательств (исходные данные не должны изменяться в процессе исследования);
- документирование всех операций (обеспечение цепочки хранения);
- воспроизводимость результатов.

Соблюдение данных принципов позволяет обеспечить юридическую значимость собранных цифровых доказательств [2].

Процесс расследования компьютерных инцидентов включает несколько последовательных этапов: идентификация инцидента, сбор цифровых доказательств, их исследование и анализ, документирование результатов, а также извлечение уроков для предотвращения подобных инцидентов в будущем. Схематичное представление данного процесса приведено на рисунке 1.

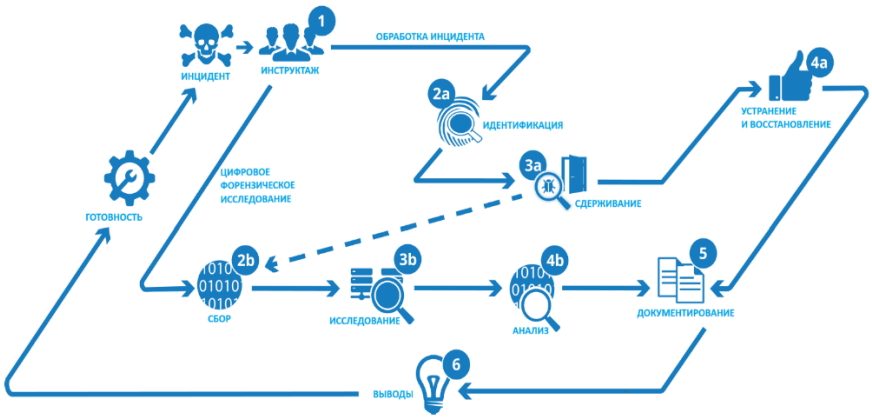

Рисунок 1 – Процесс обнаружения и расследования компьютерных инцидентов

Современные вызовы в области цифровой криминалистики обусловлены усложнением информационных инфраструктур, переходом на удаленные рабочие места и использованием распределенных систем. Это требует от специалистов:

- оперативного сбора данных с сотен компьютеров в различных сегментах сети;
- проведения исследований без физического доступа к оборудованию;
- обеспечения сохранности данных при нестабильных сетевых соединениях;
- обработки больших объемов разнородной информации.

Развитие методов удаленной форензики позволяет решать данные задачи с помощью специализированных программных агентов, устанавливаемых на исследуемые компьютеры. Современные подходы к удаленному сбору данных базируются на модульности архитектуры, минимальном воздействии на систему, локальном хранении данных при недоступности сервера и применении криптографических методов для обеспечения целостности [6].

Важное значение в подготовке специалистов в области компьютерной форензики имеет практико-ориентированное обучение. В учебных пособиях БГУИР [1, 2] рассматриваются основные методы сбора и анализа цифровых артефактов в операционных системах Windows, а также особенности документирования результатов форензического исследования. Лабораторный практикум [2] позволяет освоить практические навыки работы с криминалистически значимыми данными, включая извлечение информации из реестра, журналов событий, файловой системы и оперативной памяти.

Методологические подходы к обеспечению информационной безопасности, включая вопросы организации защиты информации и управления инцидентами, изложены в учебно-методическом пособии [6]. Авторы акцентируют внимание на необходимости системного подхода к построению защиты информационных систем, что напрямую связано с задачами компьютерной форензики. В рамках практикума рассматриваются сценарии реагирования на инциденты, что позволяет сформировать у специалистов целостное представление о процессе расследования.

Особенности расследования компьютерных преступлений в Республике Беларусь регламентируются ведомственными методическими материалами [4], которые учитывают специфику национального законодательства и правоприменительной практики. В учебном пособии Академии МВД рассматриваются организационные и процессуальные аспекты проведения следственных действий, связанных с изъятием и исследованием цифровых доказательств. Особое внимание уделяется вопросам обеспечения цепочки хранения доказательств и соблюдения процессуальных норм при проведении форензических исследований.

Современные научные исследования в области цифровой криминалистики отражены в сборнике научных трудов БГУИР [5], где представлены результаты разработок в области методов сбора и анализа цифровых артефактов, а также подходы к автоматизации форензических исследований. Среди актуальных направлений исследований можно выделить:

- разработку методов обнаружения скрытых и удаленных данных;
- создание алгоритмов автоматизированного анализа больших объемов цифровых доказательств;
- совершенствование методов извлечения информации из памяти работающих систем;
- развитие подходов к удаленному сбору данных в распределенных сетях.

Компьютерная форензика находит широкое применение в правоохранительной деятельности, корпоративном секторе, а также в образовательном процессе при подготовке специалистов в области информационной безопасности [4, 5]. В правоохранительной деятельности методы форензики используются для раскрытия киберпреступлений и сбора доказательств, имеющих юридическую силу. В корпоративном секторе компьютерная форензика применяется при расследовании инсайдерских угроз, утечек конфиденциальной информации и нарушений политик безопасности.

Дальнейшее развитие компьютерной форензики связано с автоматизацией процессов сбора и анализа данных, внедрением методов искусственного интеллекта для выявления скрытых закономерностей, а также разработкой специализированных программных средств, учитывающих особенности современных операционных систем и сетевых инфраструктур.

Таким образом, компьютерная форензика является неотъемлемым элементом системы обеспечения информационной безопасности, позволяющим не только эффективно расследовать произошедшие инциденты, но и вырабатывать превентивные меры по их предотвращению. Развитие методологических основ, совершенствование практических методик и подготовка квалифицированных кадров в этой области являются важнейшими факторами противодействия современным киберугрозам.

Список использованных источников:

1. Веленто, И.И. Компьютерная криминалистика : учеб.-метод. пособие / И.И.Веленто. – Минск : БГУИР, 2021. – 87 с.

2. Веленто, И.И. Компьютерная криминалистика. Лабораторный практикум : учеб.-метод. пособие / И.И. Веленто, Т.А. Пархимович. – Минск : БГУИР, 2022. – 63 с.

3. В Беларуси с начала 2026 года зарегистрировано более 3 тысяч киберпреступлений [Электронный ресурс] // Беларусь сегодня. – 2026. – 31 марта. – Режим доступа: https://www.sb.by/articles/kolichestvo-kiberprestupleniy-v-etom-2026-vyroslo-na-20-protsentov.html (дата обращения: 01.04.2026).

4. Методика расследования компьютерных преступлений : учеб. пособие / под ред. В.А. Гусева. – Минск : Академия МВД Республики Беларусь, 2023. – 145 с.

5. Основы цифровой криминалистики : сб. науч. тр. / Белорусский государственный университет информатики и радиоэлектроники ; редкол.: И.И. Веленто – Минск : БГУИР, 2024. – 110 с.

6. Борботько, Т.В. Методология информационной безопасности. Практикум : учеб.-метод. пособие / Т.В. Борботько, О.В. Бойправ. – Минск : БГУИР, 2024.

ПОВЫШЕНИЕ ЭФФЕКТИВНОСТИ УПРАВЛЕНИЯ ПОДРАЗДЕЛЕНИЯМИ НА ОСНОВЕ ВНЕДРЕНИЯ ПРОГРАММНЫХ СРЕДСТВ ВИЗУАЛИЗАЦИИ ЗАДАЧ С УЧЕТОМ СОВРЕМЕННЫХ ТЕНДЕНЦИЙ РАЗВИТИЯ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ

Волков П.А., Франковский В.В.

Белорусский государственный университет информатики и радиоэлектроники
Минск, Республика Беларусь

Гусаков П.Б.

Аннотация. В тезисах обосновывается необходимость внедрения программных средств визуализации задач на основе методологии канбан в деятельность подразделений. Проведен анализ актуального опыта применения боевых ИИ-систем планирования и управления (Palantir Maven) в операциях вооруженных сил США (март 2026 г.). Показано, что ключевым элементом эффективности таких систем является визуализация потоков задач и ситуационная осведомленность. Предложены направления адаптации канбан-методологии для решения задач планирования ресурсов, технического обслуживания и оперативного управления.

Современное управление подразделениями характеризуется высокой интенсивностью потоков заявок, необходимостью оперативного перераспределения ресурсов и жесткими временными рамками выполнения задач. Традиционные методы (устные распоряжения, бумажные журналы, разрозненные электронные сводки) не обеспечивают требуемой прозрачности и скорости реагирования. В этой связи возрастает потребность во внедрении инструментов визуального управления, позволяющих в реальном времени отслеживать статусы задач, загрузку личного состава и техники, а также координировать действия различных подразделений. Одним из наиболее эффективных и универсальных инструментов такого рода является канбан-доска, получившая широкое распространение в различных сферах – от промышленного производства до военного управления.

Канбан-доска как инструмент визуализации и управления потоками задач. Канбан-доска представляет собой систему визуального управления, в которой задачи отображаются в виде карточек, перемещаемых по колонкам, отражающим этапы их жизненного цикла («К выполнению», «В работе», «На проверке», «Выполнено»). Такой подход позволяет:– сократить время доведения задач до исполнителей с нескольких часов до 15–20 минут;

– обеспечить единую картину текущей загрузки для всех участников процесса;

– исключить потерю или дублирование заявок;

– наглядно контролировать соблюдение сроков исполнения;

– оперативно выявлять узкие места и перераспределять ресурсы.

В военной сфере принципы визуального управления потоками задач находят всё более широкое применение. Показательным является опыт использования системы Maven (Palantir) в вооруженных силах США. В марте 2026 года эта система получила статус основной боевой ИИ-платформы, однако её ключевой элемент – визуальная доска управления задачами – оказался решающим фактором сокращения времени цикла планирования и нанесения ударов в ходе операций в Иране. Не углубляясь в технические детали ИИ, важно отметить, что именно визуализация статусов целей, ответственных исполнителей и временных меток позволила свести разрозненные данные в единую картину и ускорить принятие решений. Внутренняя архитектура Maven строится на принципах, близких к методологии канбан: задачи проходят четкие этапы жизненного цикла «обнаружение – идентификация – утверждение – назначение средств поражения – контроль поражения – оценка результата». Каждый этап визуализирован, снабжен статусами, ответственными исполнителями и временными метками. Единая картина оперативной обстановки доступна всем участникам планирования независимо от их географического расположения. Этот опыт наглядно демонстрирует, что визуализация потоков задач и централизованное управление их исполнением становятся критически важными факторами боевой эффективности.

Помимо описанного выше боевого применения, канбан-методология активно используется в вооруженных силах различных стран для решения широкого круга задач материально-технического обеспечения, управления запасами и подготовки специалистов. На военно-морской верфи Портсмута внедрена канбан-система управления запасами запасных частей для подводных лодок. В рамках программы «batch manufacturing» (пакетное производство) осуществляется изготовление избыточного количества деталей, которые складируются и используются по мере необходимости. Канбан-система обеспечивает наличие деталей на полке до того, как они понадобятся заказчику, что исключает задержки в производственном процессе. Процесс начинается с того, что деталь рекомендуется как подходящий кандидат для пакетного производства. Группа материально-технического обеспечения проводит исторический анализ для подтверждения целесообразности. Используя канбан-систему

учета запасов, базу данных, отслеживающую наличие деталей на складе, управление осуществляется через систему заказов. Результатом стало значительное сокращение времени выполнения заказов и повышение боеготовности подводных лодок. Как отмечает руководство верфи, «внедрение программы позволило изготавливать компоненты для пополнения складской системы предметами с высоким спросом».

Канбан-доска не только ускоряет выполнение задач, но и кардинально повышает качество планирования. Использование визуальных досок в штабах оперативного управления позволяет моделировать различные сценарии, перераспределять ресурсы в реальном времени и оперативно корректировать планы при изменении обстановки. При этом все изменения фиксируются, что обеспечивает сохранность управленческой информации и возможность анализа принятых решений. В частях постоянной готовности, где требуется высокая мобильность и быстрая реакция, цифровые канбан-доски, развёрнутые на планшетах и ноутбуках, позволяют командирам в любой момент видеть состояние подразделений, наличие запасов и готовность техники, а также оперативно ставить задачи личному составу.

В сфере боевой подготовки канбан-доски находят применение как инструмент планирования занятий, контроля посещаемости и успеваемости, а также визуализации этапов подготовки. На специальных досках отражаются этапы проведения занятий, результаты стрельб, нормативы по специальной подготовке, что позволяет командирам наглядно видеть уровень подготовки каждого военнослужащего и своевременно корректировать программу обучения. Кроме того, канбан-методология успешно используется при проведении командно-штабных тренировок, где визуализация этапов принятия решений и распределения задач способствует выработке единого алгоритма действий штаба и сокращает время на отработку вводных.

Применение канбан-методологии в военной сфере обеспечивает комплекс преимуществ, которые напрямую влияют на боеспособность и эффективность управления:

Повышение оперативности управления. Визуализация потоков задач и централизованное управление их исполнением позволяет сократить время доведения распоряжений, ускорить получение обратной связи и оперативно реагировать на изменения обстановки. Как показал опыт использования Maven, единая картина оперативной обстановки доступна всем участникам независимо от их географического расположения, что исключает задержки, связанные с обменом информацией.

Прозрачность и подотчётность. Каждая задача на канбан-доске имеет ответственного исполнителя, сроки выполнения и текущий статус. Это создаёт условия для объективного контроля и повышает личную ответственность военнослужащих. Командиры на любом уровне могут в реальном времени оценивать загрузку подразделений, выявлять отстающих и своевременно принимать меры.

Оптимизация использования ресурсов. Ограничение незавершённого производства (WIP-лимиты) предотвращает перегрузку личного состава и техники, позволяя сосредоточиться на наиболее важных задачах. Визуальное отображение занятости каналов связи, техники, складских запасов и личного состава даёт возможность командирам рационально распределять ресурсы, избегая как простоев, так и перерасхода.

Снижение потерь и дублирования. Канбан-доска служит единым источником правды, исключая ситуацию, когда одна и та же задача выполняется несколькими подразделениями или, наоборот, теряется из виду. Уменьшается количество ошибочных действий, вызванных неверной или несвоевременной информацией. В материально-техническом обеспечении это позволяет сократить запасы на складах, уменьшить затраты на хранение и избежать списания материалов с истекшими сроками годности.

Непрерывное совершенствование процессов. Канбан-система предполагает регулярный анализ потока задач с использованием диаграммы накопленного потока, выявление узких мест и проведение кайдзен-мероприятий. Накопленная статистика позволяет объективно оценивать загрузку подразделений, прогнозировать потребности и разрабатывать меры по повышению эффективности. Такой подход создаёт основу для формирования культуры постоянного совершенствования в воинских коллективах.

Снижение временных затрат на управленческие процедуры. Автоматизация процессов учета, контроля и отчётности, заложенная в цифровых канбан-досках, высвобождает время командиров и штабных офицеров, позволяя им сосредоточиться на содержательной части управления, анализе обстановки и принятии решений. Исчезает необходимость в составлении многочисленных бумажных сводок и проведении длительных совещаний для выяснения статуса задач.

Список использованных источников:

1. Пентагон принял боевую ИИ-систему Palantir Maven в качестве основной для армии США [Электронный ресурс] // 3DNews. – 2026. – 21 марта. – Режим доступа: https://3dnews.ru/1138679.

2. Palantir стал постоянным поставщиком ИИ для Пентагона. Внутри все еще работает запрещенный Claude [Электронный ресурс] // Habr. – 2026. – 21 марта. – Режим доступа: https://habr.com/ru/news/1013066/

3. Андерсон, Д. Дж. Канбан: Альтернативный путь в Agile / Д. Дж. Андерсон; пер. с англ. – М.: Манн, Иванов и Фербер, 2013. – 256 с.

4. Чердынцев, В. А. Радиотехнические системы / В. А. Чердынцев – Минск: Вышэйшая школа, 1988. – 369 с.

ВНЕДРЕНИЕ RAG-СИСТЕМЫ В УЧЕБНЫЙ ПРОЦЕСС ПОДГОТОВКИ ИНЖЕНЕРОВ ПО ТЕЛЕКОММУНИКАЦИЯМ

Бардашевич А.В.

Белорусский государственный университет информатики и радиоэлектроники г. Минск, Республика Беларусь

Федоренко В.А.

Аннотация. Рассмотрен вопрос внедрение локальной защищённой системы на основе архитектуры Retrieval-Augmented Generation в учебный процесс подготовки инженеров по телекоммуникациям. Кратко описана архитектура решения, функционирующего в изолированной среде и опирающегося на верифицированные источники информации. Обоснованы преимущества подхода для обеспечения достоверности ответов, информационной безопасности и адаптивности образовательного контента. Определены ключевые направления интеграции системы в различные этапы профессиональной подготовки специалистов связи.

Цифровизация Вооружённых Сил Республики Беларусь требует от инженеров связи способности оперативно работать с большими объёмами технической информации, что актуализирует задачу совершенствования методов их профессиональной подготовки. Традиционные методы обучения не обеспечивают необходимой гибкости, в связи с чем перспективным направлением представляется использование технологий искусственного интеллекта, в частности больших языковых моделей. Однако их прямое применение сопряжено с рисками утечки данных и генерации недостоверной информации. Решением является внедрение локальной RAG-системы, функционирующей в изолированном контуре и опирающейся исключительно на верифицированные источники. Архитектура системы построена по модульному принципу и включает три функциональных уровня [1].

Первый уровень – база знаний – реализована на основе реляционной СУБД PostgreSQL с расширением pgvector, обеспечивающим хранение и эффективный поиск векторных представлений текстовых фрагментов в закрытой вычислительной среде [2]. Выбор данной платформы обусловлен ее надежностью, масштабируемостью, поддержкой стандарта SQL и возможностью развертывания в изолированных сетях без доступа к глобальному интернету. Процесс формирования базы состоит из четырех последовательных этапов. На этапе отбора источников используются только документы официального статуса (учебные пособия, руководства по эксплуатации, нормативная документация) в машинном формате (PDF, DOCX, TXT). Второй этап предполагает предварительную обработку: конвертацию в UTF-8, удаление колонтитулов и номеров страниц, нормализацию пробельных символов и декодирование специальных знаков. Третий этап – разбиение текста на семантические целостные чанки (текстовый фрагмент) объемом 300 – 500 слов. Разбиение производится с учетом лингвистической структуры документа (границы абзацев и разделов), допускается частичное перекрытие соседних фрагментов (5-10%) для сохранения контекста, а формулы и таблицы обрабатываются как отдельные блоки. Завершающий этап включает генерацию эмбеддингов (числовой вектор, фиксированной размерности) с использованием предобученной мультиязычной модели, преобразующей каждый чанк в эмбеддинги. Такой подход позволяет обновлять корпус знаний путём добавления новых документов без необходимости переобучения языковой модели.

Второй уровень – серверная часть – реализован на языке Python с использованием асинхронного фреймворка FastAPI. Выбор данной технологии обусловлен высокой производительностью, автоматической генерацией документации и поддержки неблокирующих операций, что критично для обработки множественных запросов в реальном времени.

Сервер выступает центральным элементом системы и выполняет три ключевые функции. Первая функция – преобразование пользовательских запросов в эмбеддинг. Входящий текстовый запрос нормализируется и передается в локально развернутую модель эмбеддигов, которая преобразует текст в числовой вектор фиксированной размерности, идентичной векторам в базе знаний. Вторая функция – семантический поиск релевантных фрагментов. Сформированный вектор используется в SQL-запросе к СУБД PostgreSQL с расширением pgvector. Поиск осуществляется путём вычисления метрики косинусного сходства между вектором запроса и векторами чанков в базе. Система извлекает топ-5 наиболее релевантных фрагментов, обеспечивая баланс между полнотой контекста и нагрузкой на модель [3]. Третья функция – генерация ответа языковой моделью. Найденные фрагменты объединяются в единый контекст и встраиваются в системный промт, содержащий строгую инструкцию использовать только предоставленную информацию. Промт передается в языковую модель и ответ возвращается клиенту в структурированном формате JSON. Важной особенностью является механизм контроля релевантности, предотвращающий недостоверные ответы. При семантическом поиске устанавливается минимальный порог косинусного сходства (по умолчанию 0,75). Если один фрагмент не достигает установленного порога, система явно сообщает пользователю об отсутствии информации в базе знаний, вместо генерации ответов.

Третий уровень – пользовательский интерфейс – реализован как веб–приложение на фреймворке Srteamlit. Выбор данной технологии обусловлен простотой развертывания, кроссплатформенностью и минимальными требованиями к клиентскому устройству. Приложение доступно через любой современный браузер и не требует установки дополнительного программного обеспечения на рабочих местах курсантов и преподавателей. Структура интерфейса включает поле ввода текстового запроса, панель элементов управления и область отображения сгенерированного ответа. Важной функциональной особенностью является обязательное цитирование источников: каждый ответ сопровождается метаданными об используемых документах и конкретных разделах, что позволяет оперативно перейти к исходному тексту для самостоятельной верификации информации. Доступ к системе строго регламентирован: вход возможен только после успешной аутентификации по логину и паролю, привязанных к учётной записи. В соответствии с ролевой моделью, функционал интерфейса адаптируется под права пользователя. После окончания сессии история диалога автоматически удаляется, что исключает накопление конфиденциальной информации на клиентской стороне и обеспечивает конфиденциальность работы.

Безопасность системы обеспечивается комплексом взаимосвязанных мер. Локальное развертывание в Docker-контейнерах гарантирует изоляцию всех компонентов системы и исключает доступ к глобальной сети, что соответствует требованиям к военным информационным системам. Аутентификация на основе JWT-токенов обеспечивает безопасную передачу учетных данных и контроль сессий без хранения паролей на клиентской стороне. Ролевая модель доступа строго регламентирует функциональные возможности (курсанты –только запросы, преподаватели – управления базой знаний, администраторы – техническое сопровождение). Отсутствие сохранения текстов запросов после завершения сессии, что исключает накопление конфиденциальной информации. Фиксируются только анонимизированные метрики для мониторинга производительности.

В учебном процессе система интегрируется на всех этапах подготовки: от теоретического изучения дисциплин до практических занятий и самостоятельной работы. Система берет на себя функции оперативного информационного поиска и первичной структуризации данных, освобождая время для углубленного разбора практических задач и индивидуальной работы. В рамках самоподготовки курсанты используют систему для оперативного поиска тактико-технических характеристик и нормативных документов, что сокращает время работы с бумажными носителями. При выполнении лабораторных работ система выступает как справочно-консультативный модуль: обучающийся может оперативно запросить методику расчёта или допустимые значения параметров, сверяя их с полученными результатами. Обучающийся формулирует запросы, анализирует ответы с указанием источников и несет ответственность за принятое решение.

Эффективность применения обеспечивается чётким разграничением ролей. Преподаватель контролирует актуальность базы знаний и анализирует статистику запросов для корректировки учебного плана [4]. Техническую поддержку и обновление программного окружения осуществляет администратор учебного заведения. Такой подход формирует компетенции по работе с технической документацией, анализу информации и обеспечению информационной безопасности.

Использование RAG-системы направлено на формирование профессиональных компетенций по специализации «Системы и сети инфокоммуникаций» и профилизации «Системы телекоммуникаций специального назначения», включающих владение основами исследовательской деятельности, осуществлять поиск анализ и синтез информации; решение стандартных задач профессиональной деятельности на основе применения информационно-коммуникационных технологий; определение параметров поиска и хранения мультимедийных данных, осуществление логического и физического проектирования баз данных; организацию информационной безопасности и защиту государственной тайны; применение положения основных нормативных правовых актов Республики Беларусь в повседневной деятельности подразделений.

Внедрение RAG-архитектуры повышает качество подготовки инженеров за счёт гарантированной достоверности информации, сокращения времени поиска данных и возможности адаптации под конкретные типы аппаратуры связи. Система не заменяет преподавателя, а усиливает образовательный процесс, беря на себя функции оперативного информационного поиска и первичной структуризации данных. Дальнейшее развитие предполагает модульную адаптацию под профили воинских частей и интеграцию с существующими LMS-платформами.

Список использованных источников:

1. Lewis, P. Retrieval-Augmented Generation for Knowledge-Intensive NLP Tasks / P. Lewis [et al.] // Advances in Neural Information Processing Systems. – 2020. – Vol. 12. – P. 9459–9474.

2. Pgvector: Vector similarity search for PostgreSQL. – URL: https://github.com/pgvector/pgvector (дата обращения: 25.01.2026).4. Кузнецов А.А., Левкович М.В. Кибербезопасность в условиях цифровизации: проблемы и решения. – Минск: НЦПИ РБ, 2022. – 154 с.

3. FastAPI: Modern, fast web framework for building APIs with Python. – URL: https://fastapi.tiangolo.com/ (дата обращения: 25.01.2026).

4. Корчагин, П. А. Использование больших языковых моделей в образовании / П. А. Корчагин // Вестник Казанского университета. – 2023. – № 4. – С. 45–52

СОВРЕМЕННЫЕ ВОЕННЫЕ ИННОВАЦИИ

Жолудь В.А.

Учреждение образования «Белорусский государственный технологический университет»

Борисовец А.В.

Аннотация: Статья посвящена анализу ключевых направлений современных военных инноваций, определяющих облик вооруженных сил в настоящее время. Рассматривается влияние прорывных технологий, таких как искусственный интеллект (далее – ИИ), автономные беспилотные системы, гиперзвуковое оружие и средства радиоэлектронной борьбы (далее – РЭБ), на тактику и стратегию ведения боевых действий.

Современные военные инновации фокусируются на автоматизации, ИИ, беспилотных системах и высокоточном оружии. Ключевые направления включают БПЛА, роботизированные комплексы, лазерное оружие (HEL), гиперзвуковые ракеты и защищенные киберсистемы. ИИ используется для анализа действий противника, моделирования, а также интеграции AR/VR в тренировках.

Военные инновации оказывают непосредственное влияние на характер современных конфликтов, трансформируя способы ведения боевых действий и увеличивая значение информационных, технологических и высокоточных решений. Для Беларуси, расположенной в центре Европы и уделяющей большое значение обороне, модернизация вооруженных сил с использованием передовых технологий является не просто актуальной, но и стратегически важной задачей. В условиях стремительного развития научных дисциплин и роста спектра угроз, особую важность приобретает способность государства быстро внедрять инновации и укреплять сотрудничество военной сферы с научным и техническим потенциалом нации для эффективного противодействия новым вызовам.

Современные военные инновации охватывают широкий спектр областей – от цифровизации управления и разведки до использования робототехники, биотехнологий и передовых материалов. Среди ключевых тенденций выделяется развитие систем ИИ, которые могут обрабатывать огромные объемы данных, распознавать угрозы, предсказывать динамику обстановки и оказывать поддержку в принятии оперативных решений. Беларусь обладает особым потенциалом в этом направлении благодаря сильной подготовке специалистов в области ИТ и наличию технологической инфраструктуры, которая позволяет внедрять интеллектуальные системы в сферу управления войсками, связи и радиоэлектронной борьбы. Это создает благоприятные условия для развития данной сферы [1].

Беспилотные системы получают значительное внимание в современной армии. БЛА прочно вошли в арсенал военных, применяются для разведки, корректировки огня, наблюдения за периметрами, доставки грузов и контроля объектов. Беларусь активно инвестирует в развитие этого направления, разрабатывая собственные модели БПЛА, которые совершенствуются в плане дальности действия, устойчивости к помехам и точности передачи данных. Применение таких технологий позволяет минимизировать риски для личного состава и повысить результативность выполнения задач в экстремальных условиях [1].

Робототехника занимает значимое место среди современных инноваций. Боевые и инженерные роботы способны выполнять задачи, представляющие опасность для человека, например, разминирование, разведку местности или поддержку войск в условиях повышенной угрозы. Благодаря этим системам повышается мобильность войск и снижается число потерь при выполнении высокорисковых операций.

Одним из направлений развития является создание новых материалов и совершенствование экипировки военнослужащих. Лёгкие композиты, термостойкие ткани, современные бронированные пластины и эргономичные элементы снаряжения повышают защищённость личного состава и его боеспособность в любых ситуациях. В связи с климатическими особенностями и широким спектром задач белорусская армия активно внедряет современные образцы формы, средств индивидуальной защиты и коммуникационных устройств, что позволяет ей эффективно действовать в различных условиях.

Военные инновации возникают в результате тесного взаимодействия армии, промышленности, научно-исследовательских институтов и образовательных учреждений. Беларусь нацелена на использование своего внутреннего научно-технологического потенциала, при этом сохраняя ориентацию на собственные решения, гарантирующие независимость и устойчивость оборонной системы. Это позволит обеспечить автономность и надежность оборонной отрасли.

Республика Беларусь последовательно совершенствует свои вооруженные силы, уделяя приоритет цифровым технологиям, робототехнике, беспилотным системам, кибербезопасности и модернизации вооружения для повышения эффективности обороны. Стремясь обеспечить армию современными решениями, повышающими её эффективность и позволяющими оперативно реагировать на новые вызовы, страна активно использует свой сильный научный и промышленный потенциал. Инновации в оборонной сфере укрепляют обороноспособность, стимулируют развитие национальной промышленности и обеспечивают стратегическую устойчивость государства на долгосрочную перспективу, что способствует его безопасности.

Список использованных источников:

1.Белорусский ВПК: от лазеров до беспилотников». topwar.ru, 8 июля 2025. военное обозрение https://topwar.ru/267687-belorusskij-vpk-ot-lazerov-do-bespilotnikov.html.

ПРИМЕНЕНИЕ РЕКТЕНН В РАДИОТЕХНИЧЕСКИХ ВОЙСКАХ

Никончук Ю.А.

УО «Военная академия Республики Беларусь»,
г. Минск, Республика Беларусь

Янцевич М.А. – канд. техн. наук

Аннотация. Предлагается использовать известный способ рекуперации энергии электромагнитного поля окружающей среды применительно к радиолокационной техники войск противовоздушной обороны с целью снижения экономических затрат.

Одной из особенностей организации покрытия радиолокационного поля радиотехническими войсками − это его наращивание за счёт специальных выездных компактных команд (подвижная маловысотная радиолокационная группа), в составе которых имеется мощный радиолокатор. Одной из возможных ситуаций при этом является отсутствии возможности подключения к промышленной сети. Также следует учесть, что боевая работа обеспечивается не от промышленной сети, а за счёт дизельных генераторов, а для обеспечения хозяйственных нужд используются бензиновые генераторы. Данный фактор приводит к существенному росту энергетических и топливных расходов, что диктует необходимость проведения оптимизационных мероприятий.

Радиочастотный сбор энергии является перспективным направлением для исследований и находит всё большее применения в различных отраслях, таких, как: медицина, логистика, охранные системы, технологии построения «умного дома». На рисунке 1 представлен общий принцип работы технологии «Radio frequency energy scavenging» [1].

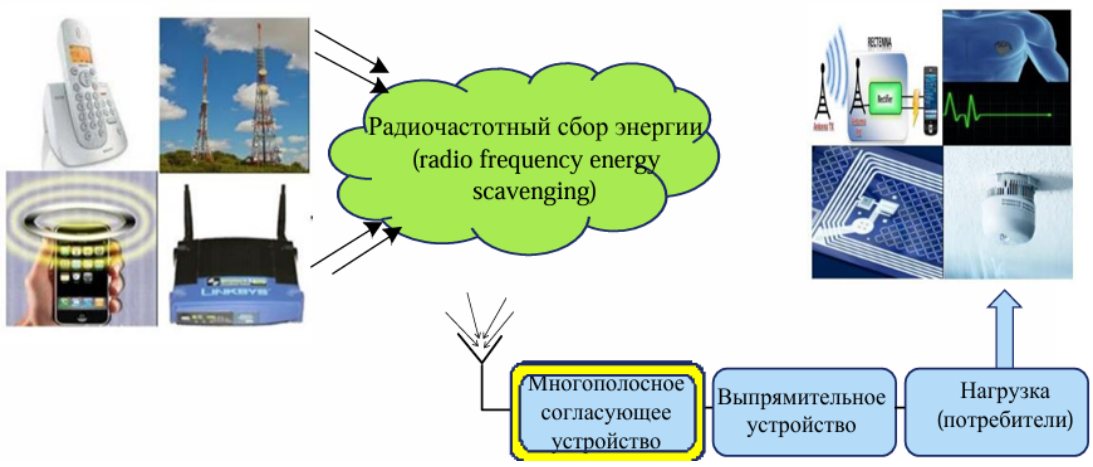

Рисунок 1 – Принцип работы технологии «Radio frequency energy scavenging»

Большинство устройств запитываемых от ректенн маломощны, что связано с низким уровнем энергии окружающего электромагнитного фона. Поэтому, наибольший интерес в этих технологиях сохраняется к задачам сбора энергии от мощных источников электромагнитной энергии, к примеру, радиолокационной станции.

Учитывая вышесказанное целесообразно организовать сбор электромагнитной энергии вблизи радиолокатора и частично компенсировать имеющиеся затраты. Такой подход к рекуперации энергии позволит выполнять боевую работу с меньшими экономическими затратами, что в масштабах вооруженных сил достаточно значимо и позволит сохранить как энергетические так и топливные ресурсы государства. Реализация предложенного подхода не требует кардинальной модернизации существующей техники — достаточно дополнить радиолокатор пассивными элементами в виде ректенн. При успешной апробации такую систему рекуперации можно тиражировать на другие объекты ПВО, получая многократную отдачу от сэкономленных средств и топлива

Список использованных источников:

1. Янцевич, М. А. Многополосные согласующие устройства для ректенн / М. А. Янцевич // Молодежь в науке – 2025 : тез. докл. XXII Междунар. конф. молодых ученых, Минск, 16–18 сен. 2025 г. / НАН Беларуси, Совет молодых ученых; редкол.: В. Л. Гурский (гл. ред.) [и др.]. – Минск, 2025. – С. 251–253.

РАЗРАБОТКА КОМПЛЕКСА НАГЛЯДНО-ОБУЧАЮЩИХ ПРОГРАММ ДЛЯ ПРОФЕССИОНАЛЬНОЙ ПОДГОТОВКИ СПЕЦИАЛИСТОВ ПО РАДИОЭЛЕКТРОННОМУ ОБОРУДОВАНИЮ

Маликов А.С.

Белорусская государственная академия авиации г. Минск, Республика Беларусь

Боровой А.Г. – кандидат технических наук, доцент

Анотация. В докладе обосновывается методологическая база и инструментарий разработки (Borland C++ Builder). Последовательно рассматриваются четыре программы, каждая из которых иллюстрирует определенный класс задач: визуализация физических принципов модуляции (VTPofM), эмуляция работы супергетеродинного приемника с контрольно-проверочной аппаратурой (далее – КПА) (VTPofA-611), моделирование аварийной радиостанции с протоколом КОСПАС-САРСАТ (VTPofR855A1M) и комплексная симуляция автоматического радиокомпаса с КПА (VTPofARC). Анализ педагогической эффективности и перспектив внедрения.

Введение

Современная авиация насыщена сложными радиотехническими системами: от маркерных приемников до спутниковых аварийных систем. Подготовка специалиста требует не только теоретических знаний, но и устойчивых практических навыков работы с контрольно-проверочной аппаратурой (КПА). Однако проведение занятий на реальных стендах и изделиях сопряжено с риском их повреждения, высоким расходом ресурса и необходимостью подачи питающих напряжений. Разработанный комплекс наглядно-обучающих программ позволяет полностью имитировать рабочие процессы без включения питания стенда, обеспечивая безопасную и экономичную образовательную среду.

1. Методологическая основа и инструментарий

Все программы разработаны в среде Borland C++ Builder, что обеспечивает поддержку стандартов ANSI/ISO, интеграцию графических компонентов для отображения виртуальных лицевых панелей и визуализацию сигналов в реальном времени. Базовым принципом является дискретизация сигналов по времени и преобразование непрерывных сигналов в импульсные для наглядности обучения.

2. Программа VTPofM: Визуализация модуляции

Программа демонстрирует формирование управляющих (модулирующих) сигналов и радиосигналов. Реализована логика в функции ChangeFunc(), вызываемой по таймеру. Пользователь через вспомогательную форму изменяет параметры сигнала (амплитуда, частота, фаза, длительность импульса, период повторения импульсов). Реализованы функции сохранения и печати графиков для использования в качестве раздаточного материала.

3. Программа VTPofA-611 эмуляции маркерного приемника

Программа моделирует работу маркерного приемника А-611 и двух устройств контроля: стенда СА-611 и имитатора МИП-70. С использованием компонента MediaPlayer генерируются звуковые частоты 400, 1300 и 3000 Гц. Реализована имитация режимов «МОД.» (непрерывный сигнал) и «МАН.» (импульсный режим «точка/тире»). Обучающийся видит загорание сигнальных ламп и слышит звук, отрабатывая алгоритмы проверки без реального включения.

4. Программа VTPofR855A1M: Аварийная радиостанция

Программа эмулирует работу аварийного передатчика Р-855А1М с учетом протоколов системы КОСПАС-САРСАТ. Автоматически запускается при включении программы встроенная система контроля (далее – ВСК) на 20 секунд (мигание ламп) с блокировкой кнопок до окончания ВСК, проработаны режимы «Маяк» и «Связь». Реализован механизм «тестового сигнала»: первый сигнал на спутник генерируется как проверочный (не учитывается), последующие — как истинное бедствие, ошибка оператора дублируется окном предупреждения.

5. Программа VTPofARC: Автоматический радиокомпас

Программа симулирует взаимодействие КПА Е017-1, блока антенн Е017-2 и пульта управления АРК-19. Позволяет выполнять регулировку напряжений (27В, 36В), проверку времени возврата стрелки (норма ≤ 4 с), имитацию пролета дальнюю и ближнюю приводные радиостанции. Использование трех таймеров с разными периодами обновления, для независимости каналов измерения, обеспечивает генерацию псевдослучайных чисел. Это позволяет отобразить реалистичность поведения стрелки индикатора и отображение измеряемых напряжений.

Пример разработанной обучающей программы и з комплекса VTPof* представлен на рисунке 1.

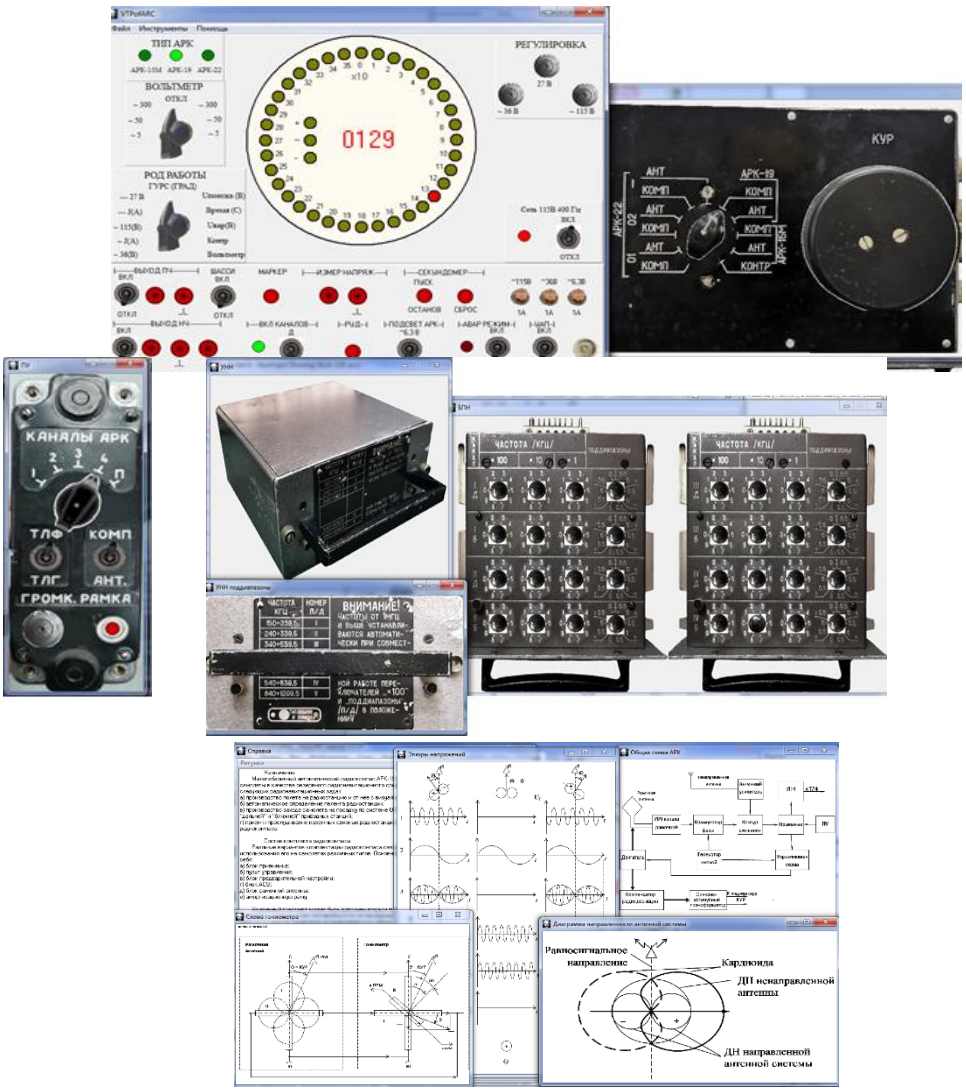

Рисунок 1 - Внешний вид программы: контрольно-проверочная аппаратура; окна состава изучаемого оборудования; окна описания работы принципа работы с графиками

6. Эргономика и структура интерфейса

Архитектура унифицирована: основная форма — виртуальная панель КПА (тумблеры, кнопки, лампы, переключатели) в соответствии с реально действующей аппаратурой; вспомогательные формы — меню настроек, справочная информация, структурные схемы, графики.

Заключение

Разработанный комплекс программ VTPof* решает три ключевые задачи профессиональной подготовки. Во-первых, обеспечивается наглядность: обучающийся видит осциллограммы модуляции, свечение ламп и движение стрелки индикатора в ответ на свои действия. Во-вторых, достигается безопасность: исключен риск выхода из строя реальной авиационной техники (А-611, Р-855А1М, АРК) и КПА стендов из-за некорректных действий обучающихся. В-третьих, формируются правильные алгоритмы работы: программно реализованы критические ошибки (тестовый сигнал КОСПАС-САРСАТ не учитывается, время возврата стрелки контролируется секундомером), что акцентирует внимание на важных деталях эксплуатации. Внедрение VTPof* в учебный процесс позволяет сократить затраты на электроэнергию и ремонт оборудования, увеличить плотность практических занятий и использовать сгенерированные графики в качестве раздаточного материала для лекционных курсов.

Список использованных источников:

1. Автоматический радиокомпас АРК-19. Руководство по технической эксплуатации. 1.244.024. РЭ – 214 с.
2. Архангельский А.Я., Программирование в C++Builder 6. – М.: «Издательство БИНОМ», 2003 г. – 1152 с.
3. Баженов, А.В. Радионавигационные системы/ Учебное пособие. [Текст]/ А.В. Баженов, Г.И. Захаренко, А.Н. Бережнов, К.Ю. Савченко./ Под ред. А.В. Баженова – Ставрополь: СВВАИУ(ВИ), 2007. – 202с.
4. Радиокомпас автоматический АРК-35-1. Руководство по технической эксплуатации. ФБМИ.461531.022 РЭ – 128 с.
5. Рубцов Е.А., Шикавко О.М. Радиооборудование воздушных судов и его летная эксплуатация: Учебное пособие / СПб ГУ ГА. С. - Петербург, 2017. 120 с.

ВЛИЯНИЕ СРЕДСТВ РАЗВЕДКИ И ОГНЕВОГО ПОРАЖЕНИЯ НА БАЗЕ БЕСПИЛОТНЫХ ЛЕТАТЕЛЬНЫХ АППАРАТОВ НА ЭЛЕМЕНТЫ ТАКТИЧЕСКОЙ ПОДГОТОВКИ ПОДРАЗДЕЛЕНИЯ

Волков П.А., Франковский В.В.

Белорусский государственный университет информатики и радиоэлектроники
Минск, Республика Беларусь

Коношенко А.В.

Аннотация. На основе анализа опыта специальной военной операции (СВО) в статье рассматривается трансформация тактики общевойскового боя под влиянием массового применения беспилотных летательных аппаратов (БПЛА). Выявлены ключевые изменения: переход от наступления крупными подразделениями к действиям штурмовых групп «двойками» и «тройками», кардинальный пересмотр требований к маскировке и инженерному оборудованию позиций, изменение роли бронетехники, появление новых воинских специальностей, внедрение в штатное оснащение портативных детекторов дронов. Предложены направления корректировки тактической подготовки подразделений и системы нормативов с учётом полученного опыта.

С начала специальной военной операции (СВО) принципы классического общевойскового боя, выработанные в середине XX века, претерпели кардинальные изменения. Массовое применение беспилотных летательных аппаратов (БПЛА) всех типов – от разведывательных коптеров до FPV-дронов-камикадзе – превратило воздушное пространство над полем боя в наиболее динамичную и опасную среду. Как отмечает военный аналитик, полковник Генерального штаба в отставке Андрей Демуренко, традиционные концепции «концентрации сил», «участка прорыва», «изоляции района боевых действий» утратили прежнее значение [1]. В этих условиях тактика Вооруженных сил России полностью трансформировалась, что требует переосмысления подходов к тактической подготовке подразделений.

Одним из наиболее существенных изменений стал отказ от наступления стрелковыми цепями под прикрытием боевых машин пехоты – основы общевойскового боя последних десятилетий. Как констатирует военный корреспондент Валентин Трушнин, сегодня войска больше не следуют скопом на бронетехнике, чтобы не превратиться в легкую мишень для дронов [2]. Вместо этого наступательные задачи решаются малыми штурмовыми группами, получившими в войсках обозначение «двойки» (2 человека) и «тройки» (3 человека) [3].

Каждый штурмовой взвод разбивается на три отделения: первое – непосредственно штурмующее, второе и третье – группы огневой поддержки. Отделения, в свою очередь, делятся на элементарные штурмовые единицы. Такая организация продиктована необходимостью максимального рассредоточения и скрытности, которых можно добиться только предельной индивидуализацией наступательных действий.

Возможности современных средств разведки – БПЛА с тепловизионными и мультиспектральными камерами, работающими круглосуточно – сделали традиционные приемы маскировки недостаточно эффективными. Дроны способны залетать за линию боевого соприкосновения на глубину до 40 километров, поэтому траншеи и блиндажи больше не гарантируют безопасности. Как подчеркивается в репортажах с передовой, единственным, что реально работает, становится маскировка [2].

Опыт СВО показал необходимость формирования у личного состава принципиально иных навыков скрытного размещения и передвижения:

1. использование естественных складок местности и лесонасаждений как основного способа сокрытия от оптических и тепловизионных средств разведки.
2. обязательное оборудование ложных позиций для отвлечения внимания противника и вскрытия его разведывательных средств.
3. быстрое возведение укрытий с защитой от ударов сверху – навесные перекрытия, противодронные сетки («мангалы»), которые стали неотъемлемым элементом полевой фортификации.

В тактическую подготовку подразделений необходимо включать нормативы по скрытному выдвижению с применением естественных укрытий, развертыванию ложных позиций и оборудованию защищенных огневых точек с противодронной защитой. Эти навыки становятся столь же важными, как и огневая подготовка.

Массовое применение FPV-дронов противником привело к необходимости пересмотра штатного вооружения подразделений. Одним из наиболее эффективных средств поражения малоразмерных беспилотников на малых дистанциях стал дробовик. Как отмечается в репортажах с передовой, дробовик оказался незаменим для защиты личного состава и техники от атакующих дронов-камикадзе [4]. Его преимущество – большая площадь поражения дробью, позволяющая поражать быстро движущуюся малоразмерную цель без точного прицеливания. В подразделениях дробовики используются как для стационарной охраны позиций, так и для сопровождения колонн и штурмовых групп.

Параллельно в войска активно поступают портативные детекторы дронов «Булат». Это устройство предназначено для раннего обнаружения БПЛА по каналам связи и управления. Детектор способен определить тип дрона, его удаление (радиус обнаружения достигает 1,5–2 км) и направление, оповещая оператора звуковым и световым сигналом [5, 6]. Применение таких детекторов меняет тактику работы подразделений: вместо пассивного наблюдения за воздушной обстановкой бойцы получают возможность заблаговременно обнаружить угрозу, укрыться, применить средства РЭБ или открыть огонь из дробовика на опережение. Как подчеркивается в публикациях, «Булат» позволяет «увидеть» оператора дрона по сигналу управления, что открывает возможности для контрбатарейной борьбы с расчетами БПЛА противника [7].

Бронетехника в условиях насыщенности поля боя FPV-дронами утратила роль средства прорыва. При проектировании танков и боевых машин не учитывалось, что удары будут наноситься преимущественно с воздуха: бронирование в основном защищало лоб и борта, оставляя крышу уязвимой [2]. Наступление крупными бронегруппами сменилось работой с закрытых огневых позиций [1]. Для доставки личного состава и грузов на передовую все чаще используются багги и квадроциклы, с которых удобнее отстреливаться от дронов [2].

Изменение тактики ведения боя требует пересмотра системы боевой подготовки подразделений. Как отмечается в военно-аналитических публикациях, в настоящее время идет активная работа по обобщению фронтового опыта и внесению изменений в боевые уставы [8]. На основе анализа опыта СВО предлагается включить в тактическую подготовку следующие направления:

1. Действия «двоек» и «троек»: отработка скрытного передвижения, занятия огневых позиций, ведения ближнего боя в траншеях и городской застройке.
2. Маскировка и инженерное оборудование: отработка скрытного выдвижения с использованием естественных укрытий, развертывания ложных позиций, быстрого возведения укрытий с защитой от сверху (навесные перекрытия, противодронные сетки).
3. Противовоздушное прикрытие малых групп: алгоритмы обнаружения дронов с помощью детектора «Булат», целеуказания, применения дробовика и стрелкового оружия для поражения БПЛА, укрытия от атак.
4. Взаимодействие с беспилотной авиацией: вызов и целеуказание для ударных FPV-дронов, организация прикрытия штурмовых групп с воздуха.
5. Работа средств РЭБ в составе малых групп: внедрение портативных средств радиоэлектронной борьбы в штатное оснащение отделений, отработка их применения для защиты личного состава и техники.

Опыт СВО демонстрирует, что современный общевойсковой бой трансформировался в пространство, где доминируют средства разведки и поражения на базе БПЛА. Основными тактическими единицами стали штурмовые группы «двойками» и «тройками», бронетехника перешла к работе с закрытых позиций. Принципиально изменились подходы к маскировке и инженерному оборудованию: использование естественных укрытий, обязательное создание ложных позиций и возведение укрытий с защитой от сверху стали обязательными элементами полевой выучки. В ответ на угрозу со стороны FPV-дронов в подразделениях получили широкое распространение дробовики и портативные детекторы дронов «Булат», что потребовало отработки новых тактических приемов и пересмотра нормативов боевой подготовки.

В связи с этим возникает необходимость в систематизации фронтового опыта, пересмотре подходов к тактической подготовке подразделений и внедрении в учебный процесс новых методов, ориентированных на высокую автономность бойца, работу в малых группах и эффективное противодействие средствам воздушного нападения противника. Предложенные направления корректировки тактической подготовки позволят повысить живучесть подразделений и эффективность выполнения боевых задач в условиях массового применения БПЛА.

Список использованных источников:

1. Описаны главные изменения в тактике армии России с начала СВО / Lenta.ru [Электронный ресурс]. – 2026. – Режим доступа: https://lenta.ru/news/2026/01/12/opisany-glavnye-izmeneniya-v-taktike-armii-rossii-s-nachala-svo/.

2. Русские изменили тактику ведения боя: На фронте появилась новая воинская специальность – «ноги» / Царьград [Электронный ресурс]. – 2025. – Режим доступа: https://tsargrad.tv/dzen/russkie-izmenili-taktiku-vedenija-boja-na-fronte-pojavilas-novaja-voinskaja-specialnost-nogi_1215227.

3. «Двойки» и «тройки»: штурмовая тактика Вооруженных Сил Российской Федерации / Военное обозрение [Электронный ресурс]. – 2025. – Режим доступа: https://topwar.ru/269614-zavtra-na-shturm-taktika-vooruzhennyh-sil-rossijskoj-federacii.html.

4. Спецрепортаж WG Артерии фронта: огненная трасса на Покровск / Rutube [Электронный ресурс]. – 2025. – Режим доступа: https://rutube.ru/video/cc7f5d77d8e1380233cb0a1b9a016acc/.

5. «Они спасут жизни нашим бойцам»: челябинские предприниматели передали пять детекторов дронов «Булат» для бойцов в зоне СВО / КП-Челябинск [Электронный ресурс]. – 2025. – Режим доступа: https://www.chel.kp.ru/daily/27731.5/5157796/.

6. Сотрудники аэропорта Южно-Сахалинска отработали перехват дронов / Ассоциация «Транспортная безопасность» [Электронный ресурс]. – 2025. – Режим доступа: https://atb-tsa.ru/archives/27522.

7. Бойцу СВО из Каширы передали детектор дронов «Булат v.4» / Администрация городского округа Кашира [Электронный ресурс]. – 2025. – Режим доступа: https://kashira.su/novosti/v-centre-vnimanija/bojcu-svo-iz-kashiry-peredali-detektor-dronov-bulat-v-4/.

БОЙ В ГОРОДЕ ПРИ НАСЫЩЕНИИ ПРОТИВНИКОМ БПЛА

Некрашевич А.А.

Белорусский государственный университет информатики и радиоэлектроники г. Минск, Республика Беларусь

Алисевич С.А.

Аннотация. В статье рассматриваются особенности ведения общевойскового боя в городских условиях при массовом применении противником беспилотных летательных аппаратов различных классов. Анализируются изменения в тактике действий подразделений, роль инженерного оборудования городских построек, интеграция средств радиоэлектронной борьбы и войсковой ПВО, а также адаптация методических подходов Вооружённых Сил Республики Беларусь и Российской Федерации к новым угрозам.

Современный городской бой претерпел кардинальные изменения: исторически считавшиеся надёжным укрытием каменные лабиринты превратились в «стеклянные коробки» для операторов вражеских дронов. Высокая плотность застройки не спасает от разведывательных и ударных БПЛА, способных зависать над улицами, проникать во дворы и вести прицельное наблюдение за перемещениями пехоты и техники. Опыт последних конфликтов подтверждает, что традиционные схемы штурма и обороны населённых пунктов без учёта тотального воздушного контроля ведут к резкому росту потерь ещё на этапе выхода на рубежи атаки [1]. В этих условиях командирам тактического звена приходится перестраивать замысел боя, исходя из предпосылки постоянного визуального и тепловизионного контроля со стороны противника.

Первый принцип — адаптация городской среды для минимизации демаскирующих факторов. Маршруты выдвижения и позиции подразделений смещаются в подвальные помещения, подземные коммуникации и внутренние дворы, экранирующие сигнал от внешней разведки. Важнейшим требованием становится ограничение пребывания на открытых участках улиц, крышах и верхних этажах. В белорусских и российских наставлениях особо подчёркивается необходимость оборудования ложных позиций на фасадах зданий, применения маскировочных экранов с пониженной теплоотдачей и использования естественных помех в виде «городских каньонов» для затруднения наведения барражирующих боеприпасов [2].

Второй принцип — органичное встраивание средств РЭБ и войсковой ПВО в городскую застройку. В условиях ограниченной видимости и многолучевого распространения сигналов эффективны мобильные комплексы подавления каналов управления и навигации, разворачиваемые на ключевых перекрёстках и высотах. Огневые группы прикрытия, оснащённые ПЗРК, крупнокалиберными пулемётами и противодронными ружьями, должны действовать в тесной связке с расчётами РЭБ по единому плану командира. Своевременное создание локальных «зон радиоэлектронного молчания» позволяет подразделению совершать короткие, но решительные броски между укрытиями, лишая противника возможности корректировать огонь в реальном времени [3].

Особое внимание уделяется децентрализации управления и тактике малых групп. Увеличение интервалов, дробление штурмовых отрядов на расчёты из 3–5 человек, синхронизация действий с временными окнами работы РЭБ и применение дымовых завес на улицах становятся нормой. Темп боя перестаёт быть линейным: чередование активных фаз штурма с выдержкой в подготовленных укрытиях сбивает алгоритмы распознавания целей автоматизированными системами дронов. Это требует от личного состава высокой тактической выучки и умения быстро реагировать на звуковые и визуальные сигналы приближения БПЛА.

Таким образом, бой в городе при насыщении противником БПЛА представляет собой комплексную тактическую задачу, где выживание и успех зависят от системного сочетания инженерного обустройства, радиоэлектронного прикрытия и гибкого применения малых подразделений. Практика показывает, что снижение потерь достигается не за счёт отдельных технических новинок, а благодаря внедрению устойчивых стандартов действий, учитывающих беспилотную угрозу как доминирующий фактор современного городского сражения. В связи с этим особую значимость приобретает постоянная тактическая подготовка личного состава, направленная на отработку навыков действий в условиях ограниченной видимости и внезапного обнаружения противником. Командирам необходимо формировать культуру «антидроновой бдительности», при которой каждый боец осознаёт свою роль в общей системе противодействия воздушным угрозам.

Список использованных источников:

1. Министерство обороны Российской Федерации (2024). Тактика общевойсковых подразделений в городских условиях: учебное пособие. М.: Военное издательство.2. Фортификация и маскировка : учеб.-метод. пособие / Белорусский национальный технический университет. – Минск : БНТУ, 2022. – 140 с.

2. Ковалёв, Д.А., Михайлов, И.С. Противодействие БПЛА в плотной городской застройке / Сборник научных трудов Академии военного образования. Минск: ВА РБ, 2023. С. 45–52.

3. Радиотехническое обеспечение боя в современном конфликте: учеб.-метод. комплекс / под ред. В.Н. Сидорова. СПб.: ВА МТО, 2024. 186 с.

РОЛЬ ЦИФРОВЫХ ТЕХНОЛОГИЙ В ПОДГОТОВКЕ КОМАНДИРОВ К ВЕДЕНИЮ ОБЩЕВОЙСКОВОГО БОЯ

Дрозд А.А.

Белорусско–Российский университет, г. Могилёв, Республика Беларусь

Усов Е.С.

Аннотация. В докладе рассматриваются перспективы развития цифровых технологий и их интеграция в процесс подготовки командиров к ведению общевойскового боя. Анализируются основные направления: внедрение искусственного интеллекта, повышение реализма моделирования, групповое применение сетевых симуляторов. Делается вывод о неизбежности качественных изменений в системе военного образования под влиянием цифровых технологий, позволяющих максимально приблизить обучение к реальным условиям современного боя.

За последние несколько лет цифровые технологии прошли путь от вспомогательных средств визуализации до полноценного инструмента подготовки командиров, без которого сегодня не обходится ни одна современная программа военного образования. Опыт локальных конфликтов последних лет показывает, что успех в общевойсковом бою во многом зависит от умения командира быстро принимать решения в условиях информационной перегрузки, неопределенности и сильного противодействия. Цифровые технологии прочно заняли свою нишу в учебном процессе, и их роль будет только возрастать. Но что дальше? Куда движется развитие цифровых средств подготовки командиров, и как изменится система военного образования через пять-десять лет? Анализ современных тенденций позволяет выделить несколько ключевых направлений, по которым будет развиваться применение цифровых технологий в ближайшие годы.

1. Повышение реализма моделирования и внедрение искусственного интеллекта.

В настоящее время большинство симуляторов сильно зависит от заранее подготовленных сценариев и действий инструктора. Противник в учебном бою часто действует предсказуемо, что снижает ценность тренировки. Здесь оптимальным решением становится внедрение искусственного интеллекта, способного самостоятельно генерировать динамичные, непредсказуемые сценарии боя. Предлагая для решения нестандартные задачи и ситуации, мы тем самым вырабатываем умение обходить известные шаблоны и принимать четкие решения в способах достижения поставленных целей.

ИИ позволит моделировать поведение противника, гражданского населения, погодных условий и даже сбоев в системах связи. Командиру останется только принимать решения в условиях, максимально приближенных к реальным. В перспективе цифровые системы смогут проводить анализ действий обучаемого в реальном времени, подсказывать ошибки и предлагать оптимальные варианты без участия инструктора.

Особенно это важно для подготовки к общевойсковому бою в условиях радиоэлектронной борьбы и киберугроз. Симуляторы смогут часами «жить» своей жизнью, анализировать обстановку и только в ключевые моменты запрашивать решения у командира. Это кардинально повышает качество подготовки и делает ее практически неуязвимой для традиционных методов обучения.

2. Развитие группового применения и сетевых технологий.

Один командир в симуляторе — это полезный опыт. Группа командиров разных уровней, действующих в едином цифровом пространстве, — это уже полноценное отрабатывание взаимодействия в общевойсковом бою. Речь идет о так называемых «сетевых» тренировках, где в виртуальной среде одновременно работают десятки участников: от командира взвода до командира бригады.

Можно представить следующую ситуацию: в цифровом полигоне разворачивается общевойсковой бой. Командиры подразделений обмениваются информацией в реальном времени, распределяют задачи, координируют действия артиллерии, авиации, разведки и тыла. Для обучаемых такая группа выглядит как настоящий бой с множеством переменных. Прорвать такую тренировку «традиционными» методами обучения крайне проблематично — она дает опыт, который невозможно получить на обычных учениях.

Сетевые технологии открывают новые возможности для отработки взаимодействия родов войск и видов вооруженных сил, при этом стоимость проведения таких тренировок в десятки раз ниже, чем реальных учений. Зачастую, именно перенимание опыта от более опытных коллег и смотр на их действия со стороны способны выработать «рефлекс» к такого рода мудрым решениям.

Цифровые технологии будут развиваться по пути повышения реализма моделирования и внедрения искусственного интеллекта. Упор делается на сокращение времени от получения задачи до принятия решения, на способность действовать в условиях сильного информационного и радиоэлектронного противодействия, на групповое сетевое обучение и создание цифровых двойников. Такой подход поможет выстроить слаженную и целенаправленную подготовку командиров.

УДК 159.9

ПСИХОЛОГИЧЕСКАЯ УСТОЙЧИВОСТЬ ВОЕННОСЛУЖАЩИХ В УСЛОВИЯХ СПЕЦИАЛЬНЫХ БОЕВЫХ ДЕЙСТВИЙ

Ведерников В.Д., курсант гр.533701

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Лепесий И.А. – маг. воен. наук

Аннотация. В этой статье рассматривается доклад, посвящённый проблеме, которая в современных условиях выходит на первый план не только в военной психологии, но и в тактике ведения боевых действий. Речь идёт о психологической устойчивости военнослужащего.

Ключевые слова. Резистентность, резильентность, посттравматический рост.

Психологическая устойчивость можно охарактеризовать как способность индивида адаптироваться к трудным жизненным ситуациям, сохранять эмоциональное равновесие и сохранять работоспособность в условиях стресса. В контексте военной службы это становится особенно актуальным, поскольку бойцы сталкиваются с высокими нагрузками и рисками физической и психологической травмы.

Сегодня я предлагаю опираться на определение, которое объединяет три ключевых компонента: Резистентность – способность выдерживать удар, не разрушаясь. Резильентность – способность восстанавливаться после травмирующего события в максимально короткие сроки. Посттравматический рост – способность использовать опыт боевых действий как точку опоры для развития новых профессиональных и личностных качеств.

Именно третий компонент часто остаётся за рамками внимания. Мы привыкли говорить «не сломайся», но забываем о том, что боевой опыт при правильной психологической поддержке может стать не минусом, а мощнейшим плюсом военнослужащего.

Специальная военная операция оставляет глубокий след в психике её участников. Вездесущая опасность, неизвестность, неопределённость, внезапность наступления боевых событий, гибель и ранения боевых товарищей, участие в физическом уничтожении противника, высокая ответственность за результаты боевой работы, запредельная длительность сроков пребывания в зоне боевых действий, отрыв от родных и близких, резкое снижение уровня повседневного быта – эти и другие обстоятельства, действуя разрозненно и сочетано, накапливаясь до «критической массы», способны порождать у военнослужащих и сотрудников боевой дистресс, вызывать боевую психическую травму, а позже проявляться в различных неблагоприятных психологических последствиях клинического уровня.

Существует множество факторов, способствующих развитию психологической устойчивости у военнослужащих:

Образование и тренировка: Использование специальных тренингов по управлению стрессом и психологической подготовке перед отправкой в зону боевых действий. Например, многие армии обращаются к методам когнитивно-поведенческой терапии, позволяющим военнослужащим справляться с навязчивыми мыслями и страхами.

Социальная поддержка: Группа поддержки среди коллег и командиров может значительно повысить психологическое состояние бойцов. Сильные межличностные связи позволяют военнослужащим делиться своими переживаниями и находить поддержку в сложные времена.

Личностные качества: Важным аспектом является наличие таких личностных качеств, как уверенность в себе, настойчивость и оптимизм. Например, военнослужащие, которые занимались спортом или имели определённые достижения до службы, могут проявлять более высокую степень устойчивости в сложных условиях.

Развитие психологической устойчивости требует комплексного подхода, охватывающего различные аспекты функционирования личности. Методы могут быть классифицированы в соответствии с уровнями воздействия:

1**.** На физиологическом уровне:

- Дыхательные техники: Диафрагмальное (брюшное) дыхание, квадратное дыхание для быстрого снижения уровня тревоги и активации парасимпатической нервной системы [1].
- Прогрессивная мышечная релаксация: Снятие мышечного напряжения, связанного со стрессом.

- Физическая подготовка и выносливость: Повышение общей стрессоустойчивости организма, улучшение сна и гормонального баланса.

- Обучение саморегуляции: Биологическая обратная связь (далее – БОС) для контроля физиологических параметров.

2. На когнитивном уровне:

- стресс-инокуляционный тренинг (далее – СИТ): Постепенное воздействие на стрессовые ситуации в контролируемой среде для выработки адаптивных реакций.

- когнитивная реструктуризация: Обучение выявлению и изменению иррациональных или негативных мыслей, заменяя их на более реалистичные и адаптивные [9].

- тренинг принятия решений в условиях неопределённости: Развитие способности быстро анализировать информацию и действовать в условиях дефицита данных.

- техники фокусировки внимания: Обучение переключению внимания с угрожающих стимулов на выполнение конкретных задач.

3. На ценностно-смысловом и социальном уровне:

- командообразование и развитие лидерских качеств: Укрепление внутригрупповых связей, формирование чувства взаимной ответственности и доверия.

- обучение этике и морали боевых действий: Помощь в осмыслении и принятии сложных решений, предотвращение моральных травм.

- развитие коммуникативных навыков: Эффективное взаимодействие в стрессовых ситуациях, умение запрашивать и оказывать поддержку.

- формирование позитивного образа будущего: Обсуждение целей, ценностей, смысла службы и жизни после боевых действий [1].

Рассмотрим примеры конкретных ситуаций, когда военнослужащие сталкивались с высокими стрессовыми нагрузками и смогли преодолеть их, демонстрируя принципы системной устойчивости:

1. Физиологический уровень.

В ходе операции по спасению заложников в условиях ограниченного пространства и времени, бойцы спецподразделения, регулярно практикующие техники диафрагмального дыхания, смогли поддерживать стабильный сердечный ритм и ясность мышления, что позволило им действовать максимально эффективно и без паники.

2. Когнитивный уровень.

Пилоты боевой авиации, столкнувшиеся с внезапным отказом систем в условиях интенсивного противодействия, благодаря предварительному тренингу по когнитивной гибкости и фокусировке на микрозадачах, смогли последовательно выполнить аварийные процедуры и успешно посадить повреждённый самолёт, избежав катастрофы.

3. Ценностно-смысловой уровень.

Подразделения, прошедшие интенсивные курсы командообразования и имеющие высокий уровень сплочённости, демонстрируют значительно более низкий уровень боевых потерь и психологических срывов. Чувство "боевого братства" и взаимной ответственности становится мощным буфером против стресса, трансформируя индивидуальный страх в коллективную решимость [2].

Исследования показывают, что солдаты, которые активно участвуют в комплексных психологических тренингах, интегрирующих все три уровня, имеют значительно более низкий уровень посттравматического стрессового расстройства и более высокую скорость реинтеграции в гражданскую жизнь по сравнению с теми, кто не участвовал в таких программах.

В рамках практической работы мною была разработана и апробирована модель формирования психологической устойчивости, построенная на трёх уровнях. Её отличие от традиционных подходов в том, что она не требует специального оборудования, может применяться в полевых условиях и ориентирована на проактивность, а не на реагирование.

Первый уровень – физиологический («Тело – опора психики»).

Устойчивость начинается с тела. В условиях боевых действий военнослужащий часто теряет связь с физиологическими процессами: сбивается дыхание, нарушается сон, блокируется восприятие сигналов голода и жажды. Простейшие, но регулярно применяемые техники диафрагмального дыхания (квадратное дыхание), контрастные водные процедуры в полевых условиях, а также принцип «ритмизации» – чередование нагрузки и восстановления – позволяют удерживать физиологический фундамент устойчивости. Без этого все когнитивные и смысловые техники работают в разы хуже.

Второй уровень – когнитивный («Управление вниманием»).

Главный враг устойчивости на уровне сознания – это «залипание» на негативном сценарии: страх смерти, страх ошибки, чувство вины. Техника «фокусировки на микрозадачах», доказавшая свою эффективность, заключается в переключении внимания с того, *над чем я не властен*, на то, *что я могу сделать в следующие 30 секунд*. Это позволяет разорвать петлю тревоги и вернуть чувство контроля. Второй важный элемент – «когнитивная гибкость»: способность быстро пересматривать оценку ситуации при появлении новых вводных, не цепляясь за неактуальные установки.

Третий уровень – ценностно-смысловой («Боевое братство как ресурс»).

Самый мощный ресурс психологической устойчивости находится не внутри человека, а между людьми. Исследования показывают: военнослужащие, которые имеют устойчивые горизонтальные связи в подразделении, переносят стресс в разы легче. Чувство взаимной ответственности трансформирует страх: из «я боюсь умереть» он превращается в «я не могу подвести своих». Задача психолога и командира – не подавлять страх, а переводить его из эгоцентрической формы в альтруистическую.

На основе изложенной модели я предлагаю три конкретных шага, которые могут быть реализованы в рамках психологического сопровождения подразделений:

1. Внедрение «психологической разминки» до выхода на задачу.

5–7 минут групповой работы: дыхательная синхронизация, проговаривание зон ответственности, краткое смысловое якорение (напоминание о значимости задачи). Это снижает уровень хаотичной тревоги и повышает слаженность.

2. Создание «ритуалов восстановления» после возвращения.

Психологическая устойчивость формируется не только в бою, но и в паузах между ним. Ритуалы (чаепитие с обсуждением прошедшего дня, краткий разбор без оценки «кто виноват», физическая разрядка) работают как маркеры переключения: «опасность позади, можно выдохнуть».

3. Обучение командиров базовым навыкам психологической самопомощи и помощи.

В условиях специальных боевых действий психолог не может быть рядом с каждым. Поэтому ключевая фигура – командир отделения, взвода, который умеет распознать начальные признаки дистресса и применить простые техники стабилизации (переключение внимания, возвращение к дыханию, восстановление социального контакта).

Позвольте подвести итог. Психологическая устойчивость военнослужащего в условиях специальных боевых действий – это не статичная характеристика, а динамическая система, включающая тело, внимание и смыслы. Она не даётся раз и навсегда, она требует постоянной тренировки, так же как тренируется стрельба или физическая выносливость.

Но главное, на чём я хочу сделать акцент в завершение: устойчивость не означает бесчувственности. Ошибочно полагать, что психологически устойчивый военнослужащий – это тот, кто ничего не чувствует. Напротив, устойчивый военнослужащий – это тот, кто умеет быть в контакте со своими эмоциями, управлять ими и направлять их энергию на выполнение задачи и сохранение своих товарищей.

Мы не можем отменить страх. Мы не можем отменить боль потерь. Но мы можем сделать так, чтобы эти переживания не разрушали личность, а становились частью её опыта, закаляли её и делали профессиональнее. Именно в этом, на мой взгляд, заключается высшая цель психологической работы: не защитить военнослужащего от реальности, а дать ему инструменты, чтобы он мог оставаться Человеком в самых нечеловеческих условиях и выполнять поставленные задачи с максимальной эффективностью.

Список использованных источников:

1. Маркелова, Т. В. Теоретико-методологические основы заблаговременной устойчивости будущих офицеров запаса к условиям военно-профессиональной деятельности: диссертация доктора психологических наук: 19.00.07 / Маркелова Т. В. – Москва, 2011. – 402 с.

2. Красковская, В. В. Взаимосвязь личностных характеристик и стресса у военнослужащих в условиях служебной деятельности: диссертация доктора психологических наук / Красковская Вероника Владимировна. – Кишинёв, 2020. – 268 с.

UDC 159.9

A COMPARATIVE ANALYSIS OF WARS OF THE 20TH AND 19TH CENTURIES

Vedernikov V.D., cadet gr. 533701

Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus

Lepesiy I.A. – Master of Military Sciences

Annotation. This article examines a report devoted to an issue that is becoming increasingly important in modern military psychology and combat tactics. This issue concerns the psychological resilience of military personnel.

Keywords. Resilience, resilience, post-traumatic growth.

ПРИМЕНЕНИЕ ПРОТИВОТАНКОВЫХ УПРАВЛЯЕМЫХ РАКЕТ В СОВРЕМЕННОМ ОБЩЕВОЙСКОВОМ БОЮ

Мороговский А.А.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Степанец Е.В.

Аннотация. Рассматривается вариант применения противотанковых управляемых ракет в ходе ведения боевых действий с учетом внедрения систем видеоконтроля полета боеприпаса ПТУРа при выносе рабочего места оператора на безопасное расстояние от пусковой установки. Пусковая установка выступает в роли «спящего» выносного орудия, позволяя оператору работать из защищенного укрытия. Данное техническое решение минимизирует потери от ответного огня противника и позволяет расчету управлять несколькими пространственно-разнесенными комплексами, создавая эффект огневого взвода. Уделяется внимание синергии дистанционно управляемых ПТУР с беспилотными разведывательными средствами. Совокупность представленных новшеств, формирует принципиально новую модель ведения общевойскового боя, где ключевым фактором становится живучесть расчета при эшелонированном поражении противника.

В современном общевойсковом бою, характеризующемся массовым применением беспилотных летательных аппаратов, средств радиоэлектронной борьбы и комплексов активной защиты (далее – КАЗ). Роль противотанковых управляемых ракет (далее – ПТУР) претерпевает существенную трансформацию. Высокая демаскировка пуска, уязвимость каналов наведения к подавлению и способность КАЗ перехватывать боеприпасы снижают эффективность ПТУР в современных сценариях ведения боевых действий. Дополнительными проблемами являются психологическая нагрузка на оператора и низкая целесообразность применения в городской застройке.

Техническим решением некоторых проблем применения ПТУР в современном общевойсковом бою стало внедрение систем видеоконтроля полета боеприпаса, при котором оператор сохраняет над ним полный контроль на всем участке полета благодаря передаче видеоизображения с камеры, установленной на оптических приборах пусковой установки, по кабелю или защищенному радиоканалу.

Специалисты Тульского конструкторского бюро приборостроения им. академика А.Г.Шипунова создали опытные образцы модуля дистанционного управления противотанкового ракетного комплекса (далее – ПТРК) «Корнет», которые сейчас проходят всесторонние испытания. Представители предприятия полагают, что подобная система позволит сохранить жизнь оператора ПТРК в случае ответного огня противника. По словам аналитиков, ПТРК «Корнет» остаётся одним из лучших средств борьбы с бронетехникой в мире. Появление системы дистанционного управления станет для «Корнета» дополнительным преимуществом на поле боя, считают эксперты. Когда противник засекает пуск ракеты, он по месту пуска начинает вести огонь. При дистанционном управлении противник будет стрелять по пусковой установке, в то время как оператор будет находиться на безопасном удалении. Расстояние, на котором работает дистанционный комплекс, пока неизвестно, предполагается, что оно может составить от 100 до 500 метров [1].

Это кардинально меняет логику засадных действий: Сама пусковая установка, замаскированная в складках местности, за строением или в лесополосе, выступает в роли выносного орудия, в то время как оператор работает из защищенного укрытия, бункера или здания, имея лишь видеоканал с оптических приспособлений установки и пульт управления. В результате ответный огонь противника, даже если ему удается засечь тепловой след старта, ложится на пустую позицию, а расчет остается в безопасности, готовый немедленно задействовать следующую установку или перенацелить уже выпущенную ракету.

Такая архитектура применения может породить новый способ применения ПТУР, основанной на принципе засадных замаскированных комплексов. В отличие от традиционной противотанковой засады, где расчет с комплексом занимал позицию и после пуска демаскировал себя, новая методика предполагает заблаговременное размещение нескольких пусковых установок на ключевых направлениях – вдоль дорог, на опушках леса, в руинах зданий – с тщательной маскировкой, исключающей визуальное и тепловое обнаружение. Сами установки часто выполняются в малозаметном исполнении либо оборудуются дистанционно управляемыми приводами наведения. Оператор, находящийся на удалении, ведет наблюдение за сектором через оптические средства, дроны-разведчики или стационарные камеры. При появлении цели он активирует выбранную установку, производит пуск и затем, уже по видеоизображению с оптических устройств, корректирует ее наведение, добиваясь поражения объекта.

Еще одним существенным решением является возможность одним оператором одновременно управлять несколькими системами ПТУР. Технически это реализуется за счет создания единого командного пункта, в котором на мониторы выводится видеоинформация в режиме реального времени с нескольких позиций, что позволяет оператору поразить цель из наиболее выгодной позиции разнесенными по фронту и в глубину ПТУР. Например, одна установка может вести огонь по наступающей бронетехнике на ближнем рубеже после чего, расположенный на фланге комплекс, готовится к удару по резервам. В такой конфигурации один расчет фактически выполняет функции огневого взвода, обеспечивая эшелонированное поражение противника.

Важной сутью новейших технических решений стала возможность изменения организации ведения засадных действий в целом. Так пусковые установки могут быть размещены в передовых районах без операторов – по сути, как управляемые «спящие» огневые средства. Оператор управляет ими с постоянно оборудованного защищенного пункта, связанного с установками кабельными линиями или защищенными радиоканалами. Такое устройство позволяет оператору ПТРК удаленно поочередно управлять тремя пусковыми установками «Конкурс-М» в светлое время суток. Их целями становятся основные боевые танки и другая бронетехника, вертолеты, огневые точки, блиндажи и живая сила противника [2].

Такой подход резко повышает живучесть расчетов: даже если противник вскрывает местоположение пусковой установки с помощью огневого поражения или ударов FPV-дронов, оператор и часть оборудования остаются вне зоны поражения. Кроме того, появляется возможность создавать ложные позиции – муляжи установок имитируя активность, отвлекая на себя огонь и вскрывая огневые средства противника.

Не менее значимой инновацией стала интеграция дистанционно управляемых ПТУР с беспилотными разведчиками. Оператор, находясь в укрытии на удалении от установки, получает возможность мониторить подход целей не только с помощью собственных оптических приборов, но и с видеопотока, передаваемого с дрона, который может барражировать на удалении в несколько километров. В этом случае цикл «обнаружение – решение – поражение» замыкается на одного человека, который одновременно выполняет функции разведчика, огневого расчета и оператора наведения. Данное решение позволяет осуществлять поражение цели, при достижении внезапности, и сохранение безопасности оператора пусковой установки.

При данных технических решениях наступающие бронетанковые группы вынуждены действовать в условиях постоянной неопределенности, поскольку вскрыть реальное расположение управляемых установок традиционными средствами разведки крайне сложно – оператор может находиться в стороне от установки, а канал управления устойчив к радиоэлектронному подавлению, особенно при использовании оптоволокна. В ответ на это противник вынужден тратить значительные ресурсы на сплошное огневое поражение районов, где предполагается наличие замаскированных установок, что снижает темп наступления и повышает расход боеприпасов.

Испытания модернизированного дистанционного управления для ПТРК «Фагот» могут стать важным шагом в развитии тактических возможностей противотанковых подразделений [3].

Новые технические решения открывают новые тактические возможности. Использование систем ПТУР с дистанционным управлением выводят противотанковую борьбу на качественно новый уровень. Вынос оператора на удаление 500 метров и более от пусковой установки, в сочетании с полным контролем над полетом ракеты, превращает каждый комплекс в высокоживущее средство поражения противника, практически неуязвимое для его ответного огня. Использование замаскированных засадных ПТУР, размещаемых без личного состава на передовых позициях, позволяет наносить удары с неожиданных направлений, сохраняя расчеты в безопасности. Одновременное управление одним оператором несколькими разнесенными системами обеспечивает эффект численного превосходства без увеличения штатной численности подразделений.

Вышеперечисленные технические новшества формируют необходимость пересмотра модели ведения общевойскового боя, смещаемой в сторону охраны и прикрытия зон, где развернуты дистанционно управляемые ПТУРные системы.

Таким образом совокупность данных факторов требует пересмотра подходов к боевой подготовке. Вместо подготовки узких специалистов-противотанкистов необходима подготовка операторов многофункциональных систем, способных одновременно вести разведку, управлять несколькими пусковыми установками. Тактическая значимость таких подразделений выходит за рамки противодействия танкам – они становятся универсальным средством высокоточного поражения любых наземных целей, включая укрепления, легкобронированную технику и скопления живой силы противника. Дальнейшее развитие средств ПТУР с дистанционным управлением будет идти по пути еще большего удаления оператора от установки, автоматизации процессов распределения целей и глубокой интеграции с разведывательными беспилотными системами, что окончательно закрепит за ними роль одного из ключевых факторов тактического успеха в современной войне.

Список использованных источников:

1. «Сохранить жизни бойцов»: тульские оружейники разработали систему дистанционного управления ПТРК «Корнет» / Латышев А. : [сайт]. – URL: https://russian.rt.com/russia/article/1189047-ptrk-kornet-distancionnoe-upravlenie?ysclid=mng72bcyu5219010401 (дата обращения: 29.03.2026).

2. «Калашников»: современное дистанционное управление ПТРК «Конкурс-М»: [сайт] – URL: https://kalashnikovgroup.ru/news/kalashnikov-_sovremennoe_distantsionnoe_upravlenie_ptrk_-konkurs-m-_ispytano_i_gotovo_k_boyu . (дата обращения: 29.03.2026).

3. Усовершенствованное дистанционное управление ПТРК "Фагот" испытывают в зоне СВО / Максимов И.: [сайт] – URL: https://rg.ru/2025/08/14/usovershenstvovannoe-distancionnoe-upravlenie-ptrk-fagot-ispytyvaiut-v-zone-svo.html?utm_referrer=https%3A%2F%2Fyandex.by%2F (дата обращения: 29.03.2026).

ТАКТИКА ПРИМЕНЕНИЯ ДРОНОВ В УСЛОВИЯХ ПРОТИВОДЕЙСТВИЯ РЭБ И ПВО

Недбайлик С.В.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Бабич В.Н.

Аннотация. Настоящая работа посвящена исследованию актуальных тактических подходов к использованию беспилотных летательных аппаратов (БПЛА) в условиях интенсивного противодействия со стороны средств радиоэлектронной борьбы (РЭБ) и систем противовоздушной обороны (ПВО). Проводится анализ динамики развития стратегий применения дронов, рассматриваются инновационные методы преодоления систем радиоэлектронного подавления, включая применение оптоволоконных технологий, а также исследуются перспективные направления развития в области роевого применения и интеграции с искусственным интеллектом. На основе изучения опыта современных вооруженных конфликтов определены ключевые факторы, влияющие на эффективность применения беспилотников в условиях насыщенной системы противодействия.

Современные вооруженные противостояния, в частности, события на Украине, кардинально трансформировали наше понимание роли и значения беспилотных летательных аппаратов (далее – БПЛА) на поле боя. Если на ранних этапах их применения дроны рассматривались преимущественно как инструменты для ведения разведки и корректировки артиллерийского огня, то сегодня они стали полноправными участниками оперативно-тактических действий, способными оказывать существенное влияние на ход боевых операций. Массовое внедрение беспилотников поставило перед системами ПВО и РЭБ беспрецедентные вызовы, требующие переосмысления традиционных методов ведения вооруженной борьбы.

Современная тактика использования дронов базируется на принципиально новой парадигме, где беспилотник перестает быть эксклюзивным и дорогостоящим высокотехнологичным изделием, трансформируясь в элемент с высокой степенью расходности. Как отмечают эксперты, западная модель применения дронов, ориентированная на дорогие платформы со сложной инфраструктурой и точечное применение, продемонстрировала недостаточную эффективность в противостоянии массовому использованию более дешевых аппаратов [1]. Российская тактика, напротив, сделала ставку на массовость, упрощенный цикл внедрения и быструю адаптацию под конкретные боевые задачи. Ключевым тактическим преимуществом становится способность создавать высокую плотность применения дронов, что существенно затрудняет работу систем противовоздушной обороны. Скорость запуска и смены позиций, интеграция средств РЭБ и эфирной разведки приобретают первостепенное значение. Как подчеркивает офицер войск РЭБ с позывным «Реле», «если оборона заточена под редкие крупные атаки, а не под постоянные волны малых аппаратов, она теряет темп» [2]. Важным тактическим приемом является использование различных частотных диапазонов и оперативная смена рабочих частот. Постоянное взаимодействие с инженерами заводов-изготовителей позволяет оперативно вносить изменения в программное обеспечение и технические характеристики дронов, повышая их устойчивость к помехам. Современные модификации разведывательных беспилотников обладают повышенной устойчивостью к сигналам РЭБ и способны находиться в воздухе на протяжении нескольких часов на значительном удалении от точки запуска [3].

Современные системы радиоэлектронной борьбы (далее –РЭБ) представляют собой серьезную угрозу для БПЛА, поскольку они способны нарушать каналы управления и связи. В ответ на это тактика использования дронов постоянно совершенствуется. Операторы российских БПЛА на различных участках фронта демонстрируют эффективные методы обхода радиоэлектронных барьеров: при входе в зону подавления беспилотник автоматически меняет курс, а после восстановления связи оператор корректирует траекторию и высоту полета, стремясь обнаружить уязвимость в системе РЭБ противника [3].

Особое внимание привлекает появление оптоволоконных дронов, которые кардинально меняют баланс сил в противостоянии с системами РЭБ. Использование физического кабеля вместо радиоканала связи делает такие беспилотники абсолютно невосприимчивыми к радиоэлектронному подавлению. Впервые в текущем конфликте оптоволоконные FPV-дроны были применены российской стороной – модель «Князь Вандал Новгородский» появилась в августе 2024 года. Украинские силы обнаружили, что их средства РЭБ способны подавлять практически все российские дроны, за исключением тех, которые используют оптоволоконную связь. Этот опыт был незамедлительно учтен, и уже в 2025 году американские военные приступили к испытаниям оптоволоконных беспилотников в рамках учений Silent Swarm 25, что подтверждает признание эффективности данной технологии [4].

Эффективность применения дронов во многом зависит от слаженности взаимодействия между разведывательными и ударными БПЛА. Типовая тактика предполагает, что разведывательные дроны осуществляют поиск и обнаружение целей, определяют их координаты и передают информацию на пункты управления, после чего принимается решение о поражении. Ударные дроны, как правило,

наводятся на цель с использованием данных, полученных от разведчиков. Существенное значение имеет применение дронов-ретрансляторов, которые позволяют увеличить дальность управления ударными беспилотниками и обеспечить стабильную связь в условиях сложного рельефа местности или городской застройки. Ретрансляторы могут размещаться как на наземных, так и на воздушных платформах, формируя эшелонированную систему связи.

Одним из наиболее перспективных направлений развития тактики использования дронов является создание роевых структур. Современные исследования в этой области основываются на бионическом подходе, в частности, на моделировании механизмов защиты пчелиных семей. Роевое применение дронов позволяет децентрализовать управление, повысить устойчивость системы за счет избыточности и создать качественно новый уровень угрозы для средств ПВО и РЭБ противника. Концептуальные основы применения роев дронов в качестве интеллектуальных средств РЭБ предполагают создание адаптивной архитектуры, реализующей принципы децентрализованного управления с использованием алгоритмов машинного обучения и мультиагентного подхода. Это позволяет значительно повысить эффективность воздействия на радиоэлектронную среду противника за счет динамического пространственно-временного распределения помех с учетом тактической обстановки и спектральных характеристик угроз.

Анализ современных тенденций позволяет выделить несколько ключевых направлений развития тактики применения дронов в условиях противодействия РЭБ и ПВО:

- массовое производство и миниатюризация – переход к широкому использованию многочисленных, экономичных и легкозаменяемых беспилотников создает значительные трудности для традиционных систем ПВО, изначально ориентированных на нейтрализацию дорогостоящих воздушных целей. Это требует пересмотра стратегий перехвата и поражения;
- оптоволоконные каналы связи – отказ от радиоуправления в пользу физических оптоволоконных кабелей обеспечивает дронам устойчивость к радиоэлектронному подавлению. Такая технология позволяет эффективно применять БПЛА даже в условиях интенсивного использования средств РЭБ противником, делая их практически неуязвимыми для традиционных методов глушения;
- искусственный интеллект на борту – интеграция автономных систем искусственного интеллекта (ИИ) позволяет дронам самостоятельно распознавать и классифицировать цели, определять приоритеты и принимать тактические решения даже при потере связи с оператором. Это значительно повышает автономность и эффективность выполнения миссий;
- роевое применение – разработка децентрализованных, самоорганизующихся групп беспилотников, способных действовать как единый организм, открывает новые возможности для выполнения сложных задач. Такие «рои» могут эффективно подавлять системы ПВО и РЭБ противника, создавая много векторные угрозы;
- комплексная информационная интеграция – объединение разведывательных, ударных и радиоэлектронных средств в единое информационное пространство с возможностью автономной координации действий является следующим шагом в развитии беспилотных систем. Это позволяет достигать синергетического эффекта и повышать общую боевую эффективность.

Современные подходы к использованию дронов в условиях активного противодействия РЭБ и ПВО представляют собой динамично развивающуюся область военного искусства. Опыт недавних конфликтов убедительно демонстрирует, что успех сопутствует той стороне, которая способна оперативно адаптироваться к меняющейся обстановке, внедрять передовые технологии и гибко реагировать на действия противника. Масштабное применение беспилотников, использование защищенных оптоволоконных каналов, роевые структуры и глубокая интеграция с системами искусственного интеллекта становятся определяющими факторами в достижении превосходства. Ключевым выводом является настоятельная необходимость непрерывного совершенствования систем ПВО и РЭБ в ответ на эволюционирующие угрозы. Создание многоуровневой эшелонированной обороны, сочетающей радиоэлектронное подавление с огневым поражением, а также разработка эффективных методов противодействия роевым структурам дронов, являются приоритетными направлениями развития систем противовоздушной обороны на ближайшую перспективу.

Список использованных источников

1. Эксперт: ПВО НАТО бессильна против массового применения беспилотников – URL: https://www.mk.ru/politics/2025/11/09/ekspert-pvo-nato-bessilna-protiv-massovogo-primeneniya-bespilotnikov.html (дата обращения: 30.03.2026).

2. Аналитик Алехин: ВСУ теряют элитные подразделения и иностранных наемников – https://sm.news/analitik-alexin-vs-rf-unichtozhayut-ukrainskie-reb-71659-u3t5/ (дата обращения: 30.03.2026).

3. *Операторы дронов Zala: Противостояние с врагом вызывает у нас азарт охотника – URL: https://rg.ru/2025/04/01/operatory-dronov-zala-protivostoianie-s-vragom-vyzyvaet-u-nas-azart-ohotnika.html?utm_referrer=https%3A%2F%2F www.google.com%2F (дата обращения: 30.03.2026).*

4. Полковник Алехин рассказал о тактике РФ по борьбе с беспилотниками противника – URL: https://www.osnmedia.ru/obshhestvo/polkovnik-alehin-rasskazal-o-taktike-rf-po-borbe-s-bespilotnikami-protivnika/ (дата обращения: 30.03.2026).

ПРИМЕНЕНИЕ ИСКУСТВЕННОГО ИНТЕЛЛЕКТА В ВОЕННОМ ДЕЛЕ

Соколов Д.С., Павелко В.С.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Коношенко А.В.

Аннотация. В статье обоснована необходимость внедрения искусственного интеллекта в системы разведки и управления в связи с ростом объема данных и динамичностью современных конфликтов. Проанализированы основные направления применения ИИ: поддержка принятия решений, кибернетические и информационные операции, а также интеграция в автономные системы вооружений. Отмечены риски (ненадёжность, уязвимость к помехам, ошибки распознавания). Сделан вывод о необходимости сохранения «осмысленного контроля человека» и развития человеко-машинного партнёрства, где ИИ берёт на себя рутинные операции.

Особенностями современных вооруженных конфликтов является увеличение объема разведывательных данных, высокая динамичность боевых действий и необходимость принятия решения в кратчайшие сроки. С учетом этого, традиционные методы анализа большого объема информации уже не позволяют реализовать в полной мере принцип опережения. Одним из возможных направлений выхода из сложившейся ситуации является внедрение технологий искусственного интеллекта (далее – ИИ) в системы разведки, целеуказания и управления. Под искусственным интеллектом подразумевается применение компьютерных систем для решения задач, которые обычно требуют осмысления, планирования и обоснования человеком [1].

Хотелось бы обратить внимание на то, что ИИ не что-то новое. Так, еще в середине 80-х годов прошлого столетия уделялось серьезное внимание качественно новому, что вносилось в само военное дело современной информационной технологией, приобретающей черты «усилителя интеллекта». Несомненно, что ее использование осуществлялось для решения важнейших проблем, таких как проблемы войны и мира в целом, то есть решаемых на государственном, стратегическом уровне, с учетом стоимости технологий.

Одной из первых публикаций, посвященных прикладным проблемам анализа использования указанной информационной технологии, являлся научно-теоретический труд «Искусственный интеллект и вооружения. Военно-политические аспекты», подготовленный авторским коллективом Академии наук СССР в 1987 году.

В нем были изложены основные направления применения ИИ, к числу которых относятся:

- автоматизация управления. Указанное направление связанно, в первую очередь, с созданием на новой технической основе комплексных автоматизированных систем, что позволяет в итоге не просто обеспечить, но и повысить оперативность, устойчивость и непрерывность управления. Кроме того, речь идет о возможности использования ИИ в анализе и имитации военно-политических решений;
- «интеллектуализация оружия». Речь идет о возможности наделения боевых систем способностью самостоятельного выбора целей (в соответствии с некоторым их описанием) и самонаведения на них, что в итоге повышает эффективность новых систем вооружений.

Кроме того, еще одним направлением применения ИИ является возможность использования в сфере преподавания международных отношений. Это связано с тем, что принятие решений предполагает наличие этапов формирования информационной базы и анализа информации. На обоих этапах возможно применение методов ИИ в сфере международных отношений, как наиболее сложной и требующей осуществления анализа большого объема информации.

На современном этапе вооруженные силы различных государств масштабно инвестируют в системы ИИ. Уже есть примеры их применения на поле боя для информационного обеспечения военных операций или в составе различных систем вооружений.

В настоящее время основными направлениями применения ИИ являются:

- создание военных «систем поддержки процесса принятия решений», основанных на ИИ.
- применение ИИ в кибернетических и информационных операциях;
- интеграция ИИ в системы вооружений.

Системы поддержки процесса принятия решений на базе ИИ решают две задачи: сбор разведывательных данных и сокращение сроков цикла принятия решений. Для этого объединяются подсистемы сбора данных, модули анализа и контуры поддержки решений

ИИ позволяет осуществлять сбор информации со спутников, беспилотных летательных аппаратов, средств радиоэлектронной разведки и других источников в единую картину в режиме, близком к реальному времени».

Кроме того, ИИ осуществляет автоматизацию операций, на решение которых затрачивается, как правило большое количество времени, таких как сбор, классификация, сопоставление с существующими базами данных. Это что освобождает командиров, должностных лиц штабов для решения других задач. Это в итоге позволяет сократить время цикла OODA (наблюдение – ориентирование – решение – действие) в несколько раз» [3].

В указанном направлении широкое применение находят алгоритмы компьютерного зрения, обучение и подготовку которых осуществляют на размеченных снимках: эксперты заранее отмечают образцы вооружения и военной техники, позиции и инфраструктуру. Затем нейросеть применяет полученные знания к новым изображениям. Она осуществляет поиск нужных объектов, сравнивает новые данные со старыми и подсвечивает изменения: появления укреплений, складов, переправ, «следов» активности войск [2].

Еще одно перспективное направление, это применение ИИ в кибернетических и информационных операциях.

Предполагается, что ИИ изменит как способы защиты от кибератак, так и методы их проведения.

Так, системы с ИИ и возможностями машинного обучения могут в автоматическом режиме искать уязвимости в компьютерных системах противника и одновременно обнаруживать слабые места в своих собственных. Подобные разработки могут расширить масштабы кибератак, а также изменить их характер. Это в итоге может привести к более серьезным последствиям, особенно для гражданского населения и инфраструктуры.

Информационная война уже давно стала частью вооруженных конфликтов. Однако цифровое поле боя и системы с ИИ изменили способы распространения информации и создания дезинформации. В настоящее время системы с ИИ широко применяются для создания фальшивых текстовых, аудио-, фото- и видеоматериалов, которые все труднее отличить от подлинных, что приводит к затруднению адекватной оценки происходящего.

Автономное оружие, по сути самый яркий и спорный сегмент военного ИИ. Технически речь идет о платформах, которые после запуска могут самостоятельно осуществлять поиск цели, оценку обстановки и принимать решение об атаке, с учетом заданных параметров. К числу таких образцов вооружения следует отнести ударные дроны, наземные роботы, морские аппараты.

С точки зрения разработки автономная платформа с ИИ объединяет в себе несколько сложных модулей, таких как [2]:

- навигация и планирование маршрута (в том числе с учетом препятствий и угроз);
- компьютерное зрение для распознавания целей и объектов;
- системы принятия решений, который осуществляют выбор действий в текущей ситуации;
- контуры связи с оператором и другими платформами.

Однако, следует отметить, что наряду с положительными сторонами разработки и применения ИИ в военном деле существуют проблемы и ограничения. К числу основных следует отнести:

- ненадёжность в нестандартных условиях. Системы, обученные на исторических данных, могут давать ошибки при изменении параметров применения, таких как освещение, маскировка или активные радиопомехи;

- проблема распознавания «свой-чужой». В ходе испытаний боевых роботизированных систем неоднократно фиксировались случаи ошибочного наведения оружия на свои войска, что делает необходимым сохранение человека в контуре принятия решений;

- уязвимость перед системами радиоэлектронной борьбы и кибератаками. Использование радиоканалов и централизованных систем обработки данных создаёт новые векторы поражения. Отказ даже одного элемента может привести к отказу системы управления.

Следует отметить, что приведенные направления применения ИИ в военном деле существенно улучшают работу командиров и штабов в ходе анализа данных и принятия решения, а также существенно повышают эффективность применения вооружения за счет точности поражения. Вместе с тем, дальнейшее развитие и применение ИИ необходимо связывать с концепцией человеко-машинного партнёрства, где ИИ выступает в роли «коллеги», берущего на себя рутинные операции, а за человеком должна сохраняться ответственность за принятие решений. Это связано с этическими и правовыми аспектами. Ключевым требованием остаётся «осмысленный контроль человека» при применении оружия. С учетом этого общепринятой позицией является сохранение человека в контуре для решений, связанных с применением силы.

Список использованных источников:

1. Что нужно знать о роли искусственного интеллекта в вооруженных конфликтах // Международный Комитет Красного Креста [Электронный ресурс] – 2023. – Режим доступа: https://www.icrc.org/ru/document/chto-nuzhno-znat-o-roli-iskusstvennogo-intellekta-v-vooruzhennyh-konfliktah - Дата доступа: 06.10.2023

2. Искусственный интелект и война: как ИИ-симстемы меняют ПВО, разведку и автономное оружие // Минское суворовское военное училище [Электронный ресурс] – 2026. – Режим доступа: https://mnsvu.org/news/it/iskusstvennyj-intellekt-vojna-ai-menyayut-pvo-razvedku-oruzhie – Дата доступа: 14.02.2026

3. Воробьев, А.Е. Искусственный интеллект в обороне, военных операциях, разведке и контрразведке западных стран : учебное пособие / А. Е. Воробьев, Р. М. Нумахаджиев. – Москва; Вологда: Инфра-Инженерия, 2026. – 244 с.

4.. Ромашкина Н.П., Искусственный интеллект в военном деле: возможности, угрозы, перспективы // ВОКИБ, 2025 - DOI: 10.21681/2311-3456-2025-6-158-165

УДК 004.056:621.39

АППАРАТНО-ПРОГРАММНЫЙ ШЛЮЗ С АППАРАТНОЙ ИЗОЛЯЦИЕЙ КАНАЛОВ

Бабич Н.В[1]., курсант гр. 233701

Белорусский государственный университет информатики и радиоэлектроники[1]
г. Минск, Республика Беларусь

Дудак М.Н.

Аннотация. В статье рассматриваются вопросы разработки аппаратно-программного шлюза с аппаратной изоляцией каналов для применения в специальных инфокоммуникационных системах. Актуальность темы определяется необходимостью обеспечения защищенного обмена данными между сегментами сети с различной степенью доверия в интересах войск связи Вооруженных Сил Республики Беларусь. Особое внимание уделяется аппаратному разграничению каналов как способу исключения несанкционированного обратного информационного воздействия и повышения устойчивости функционирования системы в условиях повышенных требований к безопасности. Показано, что использование подобных решений позволяет повысить надежность сопряжения изолированных контуров связи и обеспечить контролируемую передачу служебной информации.

Ключевые слова. Аппаратно-программный шлюз, аппаратная изоляция каналов, однонаправленная передача данных, data diode, защищенный обмен данными, межсегментное взаимодействие, уровень доверия, изолированные контуры, инфокоммуникационные системы, сети специального назначения, исключение обратного канала, физическая изоляция, контроль целостности данных, защита информации, журналирование событий.

Современный этап развития инфокоммуникационных систем характеризуется постоянным ростом требований к защищенности межсегментного обмена данными. Для войск связи Вооруженных Сил Республики Беларусь данная задача имеет прикладное значение, поскольку в специальных системах связи и автоматизации нередко требуется организовать передачу служебной, технологической или телеметрической информации между сегментами сети с различным уровнем доверия. При этом принципиально важно исключить возможность обратного информационного воздействия со стороны менее доверенного сегмента. В подобных условиях традиционные программные средства разграничения доступа, включая межсетевые экраны и маршрутизирующие устройства с фильтрацией трафика, не всегда обеспечивают требуемый уровень гарантированности, так как сохраняют саму физическую возможность двустороннего обмена. Поэтому актуальной научно-технической задачей является разработка аппаратно-программного шлюза с аппаратной изоляцией каналов [1].

В научной литературе для описания подобных решений применяются термины data diode, unidirectional gateway, однонаправленная передача данных. При этом следует различать собственно аппаратную однонаправленную передачу и более сложные программно-аппаратные шлюзовые комплексы. В работе X. Okhravi и F. Sheldon показано, что data diode реализует физический механизм передачи данных только в одном направлении, тем самым устраняя возможность удаленного сетевого воздействия на защищаемый сегмент через канал связи. В более современных обзорах отмечается, что однонаправленные решения сегодня рассматриваются как отдельный класс средств защиты для критической инфраструктуры, промышленных систем, IoT-сред и сетей с жесткими требованиями к доверенности обмена. Российские и белорусские исследователи также подчеркивают, что однонаправленные сети передачи информации являются эффективным способом организации защищенного взаимодействия между средами с различным уровнем безопасности.

Для специальных инфокоммуникационных систем военного назначения данная проблематика приобретает дополнительное значение. На практике часто возникает необходимость вывода данных из изолированного контура: журналов событий, телеметрии, диагностической информации, данных мониторинга, сведений о техническом состоянии средств связи и автоматизации. Одновременно с этим необходимо исключить обратную передачу управляющих воздействий, вредоносного кода, деструктивных пакетов и иных форм сетевого проникновения. Таким образом, задача заключается не просто в фильтрации нежелательного трафика, а в построении такого рубежа обмена, который на физическом уровне не допускает формирования обратного канала (см. рисунок 1). Именно в этом заключается принципиальное отличие аппаратной изоляции каналов от программных методов защиты. Дополнительно следует учитывать, что применение аппаратной изоляции каналов позволяет существенно снизить зависимость уровня защищенности от корректности настройки программных средств и человеческого фактора. В отличие от традиционных решений, основанных на политике фильтрации, физическое ограничение направления передачи формирует детерминированную модель взаимодействия между сегментами сети. Это особенно важно в условиях эксплуатации систем специального назначения, где недопустимы даже единичные случаи нарушения установленного режима обмена. Таким образом, использование шлюзов с аппаратной изоляцией каналов обеспечивает переход от вероятностных методов защиты к гарантированному обеспечению безопасности межсегментного взаимодействия.

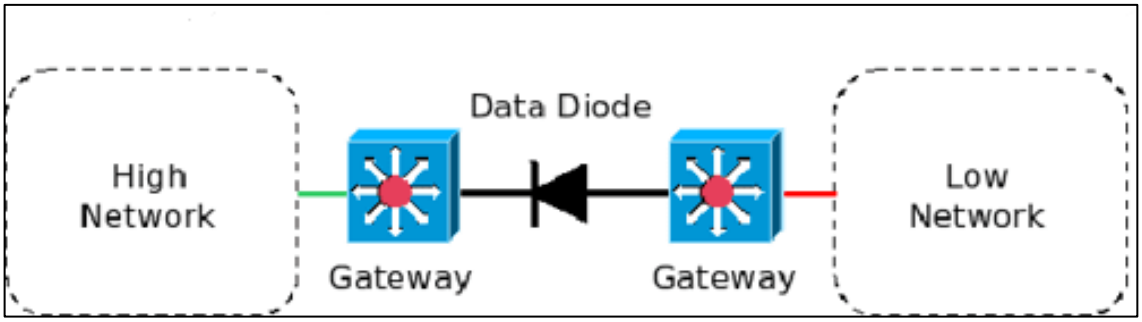

Рисунок 1 – Обобщенная схема однонаправленного шлюза между доверенным и менее доверенным сегментами

Архитектурно аппаратно-программный шлюз с аппаратной изоляцией каналов целесообразно рассматривать как совокупность трех взаимосвязанных подсистем: передающей, аппаратно-изолирующей и принимающей. Передающая подсистема размещается в доверенном сегменте и выполняет сбор, предварительное преобразование, буферизацию и подготовку данных к передаче. Аппаратно-изолирующая подсистема обеспечивает физическое ограничение направления потока. Принимающая подсистема располагается на стороне менее доверенного сегмента и реализует восстановление, верификацию, контроль целостности и предоставление данных вышестоящим приложениям. Такой подход соответствует архитектуре, описанной в работе Ю. И. Воротницкого, где аппаратно-программное средство однонаправленной передачи данных строится как совокупность модулей обмена, управления передачей и аппаратного канала с физически заданным направлением [2]. Зарубежные работы по unidirectional gateway дополнительно показывают целесообразность применения прокси-компонентов, протокольного разрыва и фильтрации содержимого.

С инженерной точки зрения аппаратная изоляция каналов может быть реализована различными способами, однако наиболее типичным является использование оптического однонаправленного тракта, в котором физически отсутствует обратный передатчик. В этом случае доверенная сторона имеет только передающий модуль, а принимающая сторона — только приемный модуль. Подобная схема обеспечивает аппаратно детерминированную однонаправленность передачи, то есть делает невозможным формирование стандартного сетевого сеанса в обратном направлении [3]. Однако физической однонаправленности самой по себе недостаточно. Для практического применения в составе инфокоммуникационной системы необходим программный уровень, который обеспечивает устойчивую доставку данных, последовательность кадров, контроль целостности, подтверждение корректности на локальном уровне и адаптацию пользовательских протоколов к однонаправленному режиму. Именно поэтому в современных однонаправленных шлюзах аппаратная защита дополняется программными модулями проксирования и реконструкции сервисов.

Для применения в войсках связи особенно важным является вопрос функционального назначения такого шлюза. Наиболее реалистичными сценариями являются: передача данных мониторинга из изолированного сегмента сети связи в сегмент централизованного наблюдения; вывод эксплуатационной информации о состоянии аппаратуры связи; передача журналов регистрации событий безопасности; вывод результатов диагностики и телеметрии из защищенных подсистем на внешние аналитические рабочие места. Во всех указанных случаях критерием эффективности выступает не полнота сетевого взаимодействия, а гарантированное отсутствие обратного управляющего воздействия на исходный сегмент. Иными словами, приоритет смещается с удобства сетевой интеграции на гарантированную безопасность сопряжения. Такой подход соответствует международной практике применения data diode в критически важных и технологических системах.

Сравнение аппаратно-программного шлюза с аппаратной изоляцией каналов и классического межсетевого экрана показывает, что эти средства не являются прямыми конкурентами, а решают различные задачи. Межсетевой экран допускает двусторонний обмен и управляет им посредством правил фильтрации, контроля соединений и анализа пакетов. Его преимуществами являются гибкость, поддержка широкого спектра протоколов и относительная простота интеграции. Вместе с тем при компрометации политики безопасности, программной реализации либо управляющей плоскости сохраняется риск несанкционированного воздействия через существующий двусторонний канал. Однонаправленный шлюз, напротив, существенно ограничивает сетевую функциональность, но обеспечивает более высокий уровень гарантированности за счет физического устранения обратного пути. Поэтому в специальных системах связи он целесообразен на тех рубежах, где цена риска обратного проникновения выше, чем потери от ограничения сетевой универсальности.

Отдельного внимания заслуживает вопрос надежности передачи данных через однонаправленный канал. В классических сетевых протоколах надежность часто обеспечивается за

счет квитирования, повторной передачи и управления сеансом в обоих направлениях. В условиях аппаратной однонаправленности такая модель неприменима в прямом виде. Поэтому в исследованиях по unidirectional gateway предлагается использовать внутренние механизмы пакетирования, последовательной нумерации, локальной буферизации, коррекции ошибок, избыточного кодирования и протокольного разрыва. В практических решениях также применяются программные прокси, которые на стороне доверенного сегмента имитируют наличие обычного сервиса, а на стороне получателя восстанавливают данные в форме, пригодной для стандартных приложений. Такой подход позволяет совместить физическую безопасность однонаправленного канала с эксплуатационной пригодностью системы.

В более широком научном контексте тематика защищенного межсегментного обмена поддерживается и смежными диссертационными исследованиями в области безопасности телекоммуникационных сетей. Так, в диссертации М. М. Монаховой исследуются модели и алгоритмы контроля инцидентов информационной безопасности в корпоративной телекоммуникационной сети, а в работе А. И. Кураленко рассматриваются методы аудита информационной безопасности информационно-телекоммуникационных систем [4], [5]. Хотя эти исследования не посвящены непосредственно однонаправленным шлюзам, они подтверждают устойчивый научный интерес к средствам, повышающим доверенность сетевого взаимодействия, контролируемость каналов обмена и устойчивость телекоммуникационной инфраструктуры в условиях усложнения угроз. Для вашей темы это важно как для обоснования научной значимости, так и для демонстрации принадлежности исследования к более широкой области специальных телекоммуникаций и защиты информации.

С учетом изложенного можно предложить следующую обобщенную структуру разрабатываемого аппаратно-программного шлюза: модуль сбора и нормализации исходных данных; модуль предварительного форматирования и буферизации; аппаратный однонаправленный канал; модуль контроля целостности и последовательности; модуль восстановления прикладного представления данных; модуль журналирования и технического контроля. При необходимости в состав шлюза могут вводиться функции криптографической защиты передаваемых данных, однако криптографические механизмы не должны подменять собой аппаратную изоляцию, а должны рассматриваться как дополнительный уровень защиты. Для условий войск связи перспективным представляется построение шлюза как специализированного изделия, ориентированного не на универсальный сетевой обмен, а на ограниченный перечень строго регламентированных сервисов передачи. Это соответствует требованиям специальных систем, где преимущество от узкой функциональной специализации часто выше, чем выгода от универсальности (см. рисунок 2).

Рисунок 2 – Предлагаемая структурная схема однонаправленного шлюза

Таким образом, разработка аппаратно-программного шлюза с аппаратной изоляцией каналов является актуальным направлением развития инфокоммуникационных систем, ориентированных на применение в специальных и защищенных контурах передачи данных. Научная и практическая значимость данной темы определяется тем, что аппаратная изоляция позволяет перейти от вероятностного ограничения угроз к физически обеспечиваемому исключению обратного сетевого воздействия. Для войск связи Вооруженных Сил Республики Беларусь это создает предпосылки для построения более устойчивых и доверенных средств сопряжения изолированных сегментов связи, предназначенных для безопасной передачи служебной информации, данных мониторинга и телеметрии. В дальнейшем развитие данной тематики может быть связано с обоснованием конкретной схемотехнической реализации шлюза, выбором интерфейсов передачи, исследованием показателей пропускной способности, задержки, отказоустойчивости и оценкой его эффективности в составе специальных инфокоммуникационных систем.

Дополнительным аспектом, требующим рассмотрения при разработке аппаратно-программного шлюза с аппаратной изоляцией каналов, является обеспечение его интеграции в существующую инфраструктуру инфокоммуникационных систем. В условиях эксплуатации сетей специального назначения важно учитывать не только функциональные возможности шлюза, но и его совместимость с используемыми протоколами передачи данных, форматами представления информации и средствами управления сетью. При этом внедрение однонаправленного шлюза не должно приводить

к нарушению штатных режимов функционирования сопрягаемых сегментов, а также должно обеспечивать минимальные задержки при передаче данных в пределах допустимых значений для конкретного типа информации.

Особое значение имеет вопрос масштабируемости предлагаемого решения. В зависимости от структуры инфокоммуникационной системы и объема передаваемых данных шлюз должен поддерживать возможность расширения пропускной способности и адаптации к изменяющимся условиям эксплуатации. Это может достигаться за счет модульного построения устройства, позволяющего наращивать вычислительные и интерфейсные ресурсы без изменения базовой архитектуры. Кроме того, при проектировании необходимо учитывать требования к отказоустойчивости, включая возможность резервирования ключевых компонентов и организацию непрерывного функционирования системы в случае отказа отдельных модулей.

Не менее важным является обеспечение контроля и диагностики работы шлюза в процессе эксплуатации. Для этого в его составе целесообразно предусмотреть средства мониторинга технического состояния, регистрации событий и анализа параметров передачи данных. Наличие таких механизмов позволяет своевременно выявлять отклонения от нормального режима работы, а также повышает общую управляемость системы. При этом доступ к диагностической информации должен быть организован таким образом, чтобы не нарушать принцип однонаправленности передачи данных и не создавать дополнительных каналов потенциального воздействия.

С точки зрения практической реализации значительное внимание должно уделяться вопросам энергопотребления и конструктивного исполнения устройства. В условиях применения в составе специальных систем связи, в том числе в полевых или ограниченных по ресурсам условиях, шлюз должен обладать компактностью, энергоэффективностью и устойчивостью к внешним воздействиям. Это накладывает дополнительные требования на выбор элементной базы, схемотехнические решения и компоновку устройства.

Таким образом, комплексный учет факторов интеграции, масштабируемости, отказоустойчивости, диагностируемости и эксплуатационных характеристик позволяет обеспечить не только функциональную реализуемость аппаратно-программного шлюза с аппаратной изоляцией каналов, но и его эффективное применение в составе современных инфокоммуникационных систем специального назначения.

Список использованных источников

1. Организация однонаправленных сетей передачи информации в условиях защищённой среды / А. Г. Воронцов, С. А. Петунин // Информационная безопасность, 2017. – С. 32–38.

2. Архитектура аппаратно-программного средства однонаправленной передачи данных в компьютерных сетях / Ю. И. Воротницкий // Вестник современных технологий, 2023. – С. 45–52.

3. Data Diodes in Support of Trustworthy Cyber Infrastructure / Hossein Okhravi, Frederick T. Sheldon // Proceedings of the 6th Annual Workshop on Cyber Security and Information Intelligence Research, 2010. – P. 1–4.

4. Модели и алгоритмы контроля инцидентов информационной безопасности в корпоративной телекоммуникационной сети : дис. … канд. техн. наук / М. М. Монахова. – М., 2015. – 150 с.

5. Методика аудита информационной безопасности информационно-телекоммуникационной системы: дис. канд. техн. наук / А. И. Кураленко. – М., 2012. – 140 с.

UDC 004.056:621.39

HARDWARE-SOFTWARE GATEWAY WITH HARDWARE ISOLATION OF CHANNELS

Babich N.V.[1]

Belarusian State University of Informatics and Radioelectronics[1]*, Minsk, Republic of Belarus*

Dudak M.N.

Annotation. The article addresses the development of a hardware-software gateway with hardware-based channel isolation intended for use in specialized info communication systems. The relevance of the topic is determined by the need to ensure secure data exchange between network segments with different levels of trust in the interests of the Signal Corps of the Armed Forces of the Republic of Belarus. Particular attention is paid to hardware-based channel separation as a means of preventing unauthorized reverse information flow and enhancing system resilience under stringent security requirements. It is shown that the use of such solutions improves the reliability of interconnection between isolated network domains and ensures controlled transmission of service information.

Keywords. Hardware-software gateway, hardware-based channel isolation, unidirectional data transmission, data diode, secure data exchange, inter-segment interaction, trust level, isolated domains, info communication systems, special-purpose networks, elimination of reverse channel, physical isolation, data integrity control, information security, event logging.

РАЗРАБОТКА МОБИЛЬНОГО ПРИЛОЖЕНИЯ ДЛЯ ПРОВЕРКИ ДОКУМЕНТОВ И ИДЕНТИФИКАЦИИ ЛИЧНОСТИ

Некраш М.А.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Савицкий А.Ю.

Аннотация. В работе представлена архитектура и реализация мобильного приложения для автоматизированной проверки удостоверений личности и биометрической идентификации. Разработанное программное средство обеспечивает сканирование и распознавание данных документов с помощью камеры мобильного устройства, проверку их подлинности, сравнение лица владельца с фотографией в документе, а также формирование электронных протоколов проверки.

Современные требования к безопасности и контролю доступа, а также рост числа случаев мошенничества с документами обусловливают необходимость создания мобильных инструментов для оперативной и надёжной верификации личности. В работе рассматривается клиент-серверная архитектура мобильного приложения, реализующая функции распознавания текста (OCR), анализа защитных элементов документов, сравнения биометрических образцов и взаимодействия с удалённой базой данных для проверки действительности документов.

В сфере обеспечения безопасности и контроля доступа всё большее значение приобретают мобильные средства верификации, позволяющие проводить проверку документов вне стационарных пунктов пропуска. В работе предложена архитектура приложения, включающая модули оптического распознавания, анализа защитных элементов, сравнения биометрических образцов и удалённого доступа к базам данных недействительных документов.

В условиях повсеместного использования цифровых удостоверений и роста подделок традиционные методы ручной проверки документов становятся недостаточно надёжными и трудоёмкими. Оператору требуется высокая квалификация для выявления признаков фальсификации, а временные затраты на верификацию могут быть значительными. В связи с этим создание мобильного приложения, автоматизирующего процессы распознавания, проверки подлинности и идентификации, является своевременной и практически значимой задачей.

В ходе выполнения работы реализовано мобильное приложение для платформы Android, выполняющее следующие основные функции:

– регистрация пользователей с разграничением прав (инспектор, администратор) и вход по PIN-коду или биометрии (отпечаток пальца);

– захват изображений документов (внутренний паспорт, водительское удостоверение, служебное удостоверение) с автоматическим обнаружением границ, коррекцией перспективы и устранением бликов;

– распознавание реквизитов документа (серия, номер, орган, выдавший документ, дата рождения) с использованием библиотеки Tesseract OCR, адаптированной для мобильных устройств;

– проверка подлинности на основе анализа микротекста, изменения цвета при наклоне устройства и контрольного суммирования цифр в номере бланка;

– идентификация личности путём сравнения «живого» снимка с камеры с портретом из документа: применяется свёрточная нейронная сеть MobileFaceNet, оптимизированная для работы на смартфоне;

– формирование электронного протокола проверки в формате JSON и PDF с приложением фото документа и лица, итоговой оценкой совпадения и временной меткой;

Архитектура приложения построена на Kotlin, Android SDK (CameraX, BiometricPrompt, SQLCipher), OpenCV, Tesseract OCR и PyTorch Mobile для сравнения лиц. Серверная часть реализована на Python (FastAPI), СУБД – PostgreSQL 17. Взаимодействие защищено TLS и JWT-токенами. Разработано более 180 тестов, обеспечивающих устойчивость приложения. Серверный компонент упакован в Docker.

Дальнейшее развитие предполагает интеграцию с государственными информационными системами (реестры ЗАГС, МВД), поддержку заграничных паспортов и видов на жительство, внедрение liveness detection, а также выпуск версии для iOS на SwiftUI.

Список использованных источников:

1. Android Developers: CameraX Guide ЭлектронныйресурсЭлектронныйресурс. – Электронные данные. – Режим доступа: https://developer.android.com/training/camerax. – Дата доступа: 06.04.2026.

2. Tesseract OCR Documentation ЭлектронныйресурсЭлектронныйресурс. – Электронные данные. – Режим доступа: https://tesseract-ocr.github.io/tessdoc/. – Дата доступа: 06.04.2026.

3.FastAPI Framework ЭлектронныйресурсЭлектронныйресурс. – Электронные данные. – Режим доступа: https://fastapi.tiangolo.com/. – Дата доступа: 06.04.2026.

ОНТОЛОГИЧЕСКАЯ МОДЕЛЬ АНАЛИЗА СООБЩЕНИЙ О ПРОИСШЕСТВИЯХ ДЛЯ ЗАДАЧ ИНФОРМАЦИОННОЙ ПОДДЕРЖКИ ДЕЖУРНЫХ СЛУЖБ МВД

Мысько Н.А.

Белорусский государственный университет информатики и радиоэлектроники[1]
г. Минск, Республика Беларусь

Савицкий А.Ю. – канд. воен. наук

Аннотация. В работе рассматривается подход к созданию автоматизированной системы поддержки принятия решений для первичного анализа сообщений о происшествиях в органах внутренних дел. Актуальность исследования обусловлена необходимостью повышения оперативности и обоснованности решений дежурных частей в условиях растущего потока неструктурированной информации. Предложена онтологическая модель предметной области, формализующая понятия и связи между участниками, объектами, временем и местом происшествия, а также регламентными нормами.

В современных условиях дежурные части органов внутренних дел (далее – ОВД) ежедневно сталкиваются с необходимостью обработки большого количества сообщений о происшествиях, требующих первичного анализа, классификации и определения порядка реагирования [1].

Ключевое противоречие заключается между потребностью в быстрой и точной семантической обработке входящих сообщений и отсутствием формализованных, пригодных для автоматизации моделей знаний, отражающих структуру предметной области (типы происшествий, их признаки, участников, квалифицирующие обстоятельства и нормативные предписания). Традиционные подходы, основанные на жестких правилах или статистических методах, часто неспособны учесть сложные связи между элементами описания, что снижает качество классификации и затрудняет объяснение принятых решений [2].

Целью настоящей работы является разработка онтологической модели и методики анализа сообщений о происшествиях для последующей реализации в автоматизированной системе поддержки принятия решений дежурных частей ОВД.

Процесс первичного анализа сообщения о происшествии, осуществляемый оперативным дежурным, включает несколько последовательных этапов. На начальной стадии фиксируются время поступления, источник и контактные данные заявителя. Далее из текста выделяются ключевые элементы: тип события (кража, хулиганство, ДТП), участники (потерпевшие, подозреваемые, свидетели), предмет посягательства, точное или приблизительное место, время совершения, способ и орудия. На основе этой информации дежурный относит событие к определенной категории ведомственного классификатора, оценивает степень общественной опасности и приоритетность реагирования, после чего принимает решение о направлении наряда или передаче материала в соответствующее подразделение. Весь процесс должен быть задокументирован с возможностью последующего контроля.

Анализ действующих нормативных документов МВД, регламентирующих порядок приема, регистрации и разрешения заявлений и сообщений позволили выделить ключевые требования к автоматизированной системе поддержки. Система должна обеспечивать семантическую обработку естественно-языкового текста, поддерживать классификацию по официальным справочникам (виды преступлений по Уголовному кодексу, составы административных правонарушений), учитывать возможные связи между текущим сообщением и ранее зарегистрированными инцидентами (например, совпадение адреса или фигурантов). Для формализации знаний о происшествиях наиболее адекватным представляется онтологический подход, позволяющий представить понятия предметной области и связи между ними в виде, пригодном для машинной обработки и логического вывода. Разработанная онтология «IncidentAnalysis» реализована на языке OWL 2 DL в среде Protégé. Иерархия основных классов включает абстрактный класс «Происшествие», от которого наследуются конкретные типы (Кража, Разбой, ДТП, Хулиганство и другие). Класс «Участник» описывает физических и юридических лиц, а также транспортные средства, которые могут выступать в ролях «Подозреваемый», «Потерпевший» или «Свидетель». Класс «Объект» охватывает предметы посягательства (деньги, ценности, документы, транспорт). Пространственная привязка обеспечивается классом «Место» с атрибутами административно-территориального деления, а временная – классом «Время», позволяющим фиксировать как абсолютные метки, так и интервалы. Для связи с нормативной базой введены классы «Квалификация» и «Признак», отсылающие к статьям Уголовного кодекса или Кодекса об административных правонарушениях.

На основе разработанной онтологии спроектирована архитектура автоматизированной системы, включающая несколько взаимосвязанных компонентов. Модуль ввода и предобработки представляет собой веб-интерфейс для оператора, обеспечивающий структурированный ввод данных либо автоматическое извлечение сущностей из текстового описания с применением методов

NLP, основанных на словарях и регулярных выражениях. Далее информация преобразуется в набор экземпляров классов онтологии и загружается в модуль онтологического хранилища – RDF-триплетор (Apache Jena Fuseki), который хранит все данные о происшествиях, участниках и связях между ними.

Модуль логического вывода использует семантический reasoner (Pellet), применяющий SWRL-правила к данным, загруженным в хранилище. В результате генерируются но-вые факты – классификационный код, уровень приоритета, перечень рекомендуемых действий и подразделение для маршрутизации. Параллельно работает модуль проверки связанности, который выполняет SPARQL-запросы к хранилищу для выявления совпадений по параметрам (адрес, ФИО, госномер) с ранее зарегистрированными инцидентами. При обнаружении связей оператору выводится предупреждение.

Результаты анализа визуализируются в модуле представления, где кроме стандартной карточки происшествия может отображаться граф связей текущего случая с другими элементами базы знаний (библиотека vis.js). Наконец, модуль управления знаниями предоставляет административный интерфейс для модификации онтологии и правил, доступный ограниченному кругу экспертов предметной области.

В качестве технологического стека выбраны Java (Spring Boot) для серверной части, React для клиентского интерфейса, Apache Jena для работы с RDF-данными, PostgreSQL для хранения служебной информации и журналов аудита.

Для оценки эффективности предложенного подхода был сформирован тестовый набор данных, включающий 200 синтетических сообщений о происшествиях, сгенерированных на основе реальных кейсов и размеченных экспертами. Каждое сообщение сопровождалось эталонной классификацией (тип происшествия, приоритет, рекомендуемые действия). Сравнивались три подхода: ручная обработка оператором без системы поддержки (контрольная группа), классификация на основе жестких правил (таблиц решений) и предложенная онтологическая система.

Таблица 1 – Сравнительные результаты апробации

Показатель	Ручной метод	Правиловой метод	Онтологический метод
Точность классификации, %	87,5	79,0	94,5
Среднее время обработки, сек	210	95	45
Полнота рекомендаций, %	72,0	68,5	96,0
Объяснимость (субъективная оценка экспертов, 1-10)	10	4	9

Полученные результаты подтверждают эффективность применения онтологического моделирования для задач первичного анализа сообщений в ОВД. Ключевыми преимуществами разработанного подхода являются формализация экспертных знаний, позволяющая представить знания опытных операторов в машиночитаемом виде, адаптируемость к изменениям нормативной базы за счет модификации SWRL-правил без перепрограммирования, а также объяснимость решений, что повышает доверие к системе и позволяет использовать ее результаты в качестве обоснования при документировании.

Ограничения исследования связаны с использованием синтетических данных – в реальных условиях возможны проблемы, связанные с неполнотой, противоречивостью или искажением информации в сообщениях граждан. Кроме того, разработанная онтология требует дальнейшего расширения для охвата всего многообразия составов преступлений и административных правонарушений по законодательству Республики Беларусь.

Перспективными направлениями развития являются интеграция с системой электронного документооборота МВД, разработка методов автоматического извлечения сущностей из текста на русском и белорусском языках, а также создание распределенного реестра для обеспечения неизменности протокола аудита.

Экспериментальная апробация на синтетическом наборе данных подтвердила эффективность предложенного подхода: точность классификации повысилась до 94,5%, время обработки сократилось до 45 секунд, полнота рекомендаций достигла 96%. Полученные результаты могут быть использованы при создании интеллектуальных информационных систем в правоохранительной сфере, а также в учебном процессе при подготовке специалистов соответствующего профиля.

Список использованных источников:

1. Министерство внутренних дел Республики Беларусь. Статистический сборник о состоянии правопорядка в Республике Беларусь за 2024 год. – Минск: МВД РБ, 2025. – 156 с.

2. Rollo, F. CEM: an Ontology for Crime Events in Newspaper Articles / F. Rollo, L. Po // Proceedings of the 38th ACM/SIGAPP Symposium on Applied Computing (SAC '23). – New York: Association for Computing Machinery, 2023. – P. 1917–1920. DOI: 10.1145/3555776.3577862

ПЕРСПЕКТИВЫ ПРИМЕНЕНИЯ И ИНТЕГРАЦИИ РОБОТИЗИРОВАННЫХ КОМПЛЕКСОВ СВЯЗИ В СУЩЕСТВУЮЩУЮ ИНФРАСТРУКТУРУ ВОЙСК ВС РБ

Мастибродский В.В.

Белорусский государственный университет информатики и радиоэлектроники г. Минск, Республика Беларусь

Сидоров С. В.

Аннотация. В докладе анализируются перспективы применения и интеграции роботизированных комплексов связи в Вооруженных Силах Республики Беларусь. Рассматриваются воздушные и наземные платформы и вопросы сопряжения с существующей инфраструктурой.

Современная военная доктрина Республики Беларусь характеризуется возрастающей ролью информационно-управляющих систем. В условиях, когда управление войсками напрямую зависит от качества, устойчивости и защищенности каналов связи, вопросы модернизации войск связи приобретают стратегическое значение, так как устойчивое управление является необходимым условием для успешного выполнения войсками боевых задач и обеспечения военной безопасности государства.

Важным и современным направлением развития становится внедрение роботизированных элементов в систему связи. Наиболее динамично развивающимся направлением роботизации войск связи является применение беспилотных летательных аппаратов (БЛА) для решения задач связи и ретрансляции. Хотя традиционно БЛА ассоциируются с ударными или разведывательными функциями, их применение для прокладки линий связи открывает новые возможности. Применение БЛА в качестве ретрансляторов позволяет решать несколько критически важных задач [1]:

1. Обеспечение связи с подразделениями, действующими в условиях пересеченной местности или в зоне низкокачественного приема наземных средств связи.

2. Существенное повышение мобильности системы связи, так как ретранслятор может изменять свое положение в зависимости от складывающейся обстановки.

3. Снижение уязвимости системы ретрансляции, так как в отличие от стационарных вышек или наземных ретрансляционных пунктов, беспилотник менее заметен и может быть быстро заменен в случае уничтожения.

Параллельно с развитием воздушных роботизированных средств активно разрабатываются наземные робототехнические комплексы (НРТК), способные выполнять задачи по обеспечению связи. Такие комплексы оснащены гусеничной платформой на электротяге и управляются дистанционно, а также оснащаются плугом для рытья канав и устройствами для укладки кабеля. Такие платформы часто действуют в паре с БЛА, которые помогают корректировать маршрут с учетом особенностей местности и текущей обстановки [2].

Преимущества такого способа прокладки линий связи заключаются в том, что кабель, уложенный в канаву и засыпанный землей, практически невидим для противника, защищен от повреждений осколками бронированной оплёткой и менее уязвим для случайных воздействий, а также позволяет уменьшить риск получения увечий связистами.

Ключевым условием эффективного применения роботизированных комплексов связи является их бесшовная интеграция в существующую инфраструктуру войск. Такой подход позволяет формировать единую информационно-управляющую среду без необходимости замены всего парка техники и значительно сокращает финансовые и временные затраты на переоснащение войск [3].

Таким образом, воздушные и наземные роботизированные комплексы связи представляют собой одно из наиболее перспективных направлений развития Вооружённых Сил Республики Беларусь. Комплексное применение БЛА-ретрансляторов и наземных роботизированных кабелеукладчиков в единой автоматизированной системе управления позволяет создать многоуровневую, износоустойчивую и помехоустойчивую систему связи, способную гарантированно обеспечивать управление войсками в любых условиях современного общевойскового боя.

Список использованных источников:

1. Каштанов, В. В. Анализ организации связи с применением беспилотных летательных аппаратов малой дальности / В. В. Каштанов, В. А. Немтинов // URL: https://cyberleninka.ru/article/n/analiz-organizatsii-svyazi-s-primeneniem-bespilotnyh-letatelnyh-apparatov-maloy-dalnosti/viewer. – 2022.

2. В зоне СВО начали дистанционно прокладывать линии связи [Электронный ресурс]. – Режим доступа: https://iz.ru/1968415/bogdan-stepovoi-andrei-buevic/setevoi-boi-na-fronte-nacali-distancionno-prokladyvat-linii-svazi. – Дата доступа: 02.04.2026.

3. Белорусская армия получила новые комплексы связи [Электронный ресурс]. – Режим доступа: https://sputnik.by/20251127/belorusskaya-armiya-poluchila-novye-kompleksy-svyazi-1102029528.html. – Дата доступа: 02.04.2026.

ИНТЕГРАЦИЯ БЕСПИЛОТНЫХ И РАДИОЭЛЕКТРОННЫХ СИСТЕМ В ОБЕСПЕЧЕНИИ БЕЗОПАСНОСТИ ВОЗДУШНОГО ПРОСТРАНСТВА ГОСУДАРСТВА

Бондарович А.С.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Беккеров Д.С.

Аннотация. Тезис рассматривает современные вызовы в сфере охране государственных границ, требующие совершенствования системы противовоздушной обороны (ПВО) Беларуси, включая защиту границ от воздушных угроз, использования беспилотников для провокации и раскрытия мест вооруженных формирований. В нем подчеркивается необходимость модернизации вооружения, внедрения новых технологий и укрепления международного сотрудничества для обеспечения национальной безопасности.

Современные угрозы в сфере безопасности – от трансграничной преступности до наращивания военной активности у границ – требуют продуманного и комплексного подхода к их нейтрализации. Беларусь, находясь в центре Европы, вынуждена постоянно совершенствовать систему пограничной защиты, в том числе за счет модернизации противовоздушной обороны (ПВО). Важно не только развивать современные средства защиты, но и усиливать координацию военных структур, внедряя передовые технологии для эффективного противодействия угрозам в воздухе.

Современные условия международной безопасности характеризуются ростом количества асимметричных угроз в воздушном пространстве.

Активное применение беспилотных летательных аппаратов, средств радиоэлектронной борьбы и высокоточного оружия требует совершенствования существующих подходов к контролю и защите воздушных рубежей государства. В этих условиях особую актуальность приобретает интеграция беспилотных авиационных комплексов и средств радиоэлектронного противодействия в единую систему мониторинга и реагирования.

Одним из ключевых факторов обеспечения безопасности воздушного пространства становится использование многоуровневой системы наблюдения. В нее входят радиолокационные станции различной дальности, пассивные средства обнаружения, а также беспилотные летательные аппараты разведывательного назначения. Совместное применение этих средств позволяет повысить точность обнаружения малозаметных целей и сократить время реагирования на потенциальные угрозы.

Особую роль играют беспилотные системы, способные выполнять длительное патрулирование приграничных районов. Они обеспечивают оперативный контроль обстановки, передачу данных в реальном времени и сопровождение обнаруженных объектов. Использование БПЛА также снижает нагрузку на пилотируемую авиацию и позволяет эффективно контролировать труднодоступные участки местности.

Дополнительным элементом повышения эффективности является использование автоматизированных систем управления.

Применение технологий искусственного интеллекта и обработки больших данных позволяет анализировать воздушную обстановку, прогнозировать развитие ситуации и принимать решения в минимальные сроки. Это особенно важно при отражении массированных атак беспилотных средств или комбинированных воздушных угроз.

Современные тенденции развития оборонных технологий также предусматривают создание единого информационного пространства, объединяющего средства наблюдения, управления и поражения. Такой подход обеспечивает согласованную работу подразделений, ускоряет передачу данных и повышает устойчивость системы к внешним воздействиям, включая кибератаки.

Таким образом, интеграция беспилотных авиационных комплексов, средств радиоэлектронной борьбы и автоматизированных систем управления позволяет существенно повысить эффективность защиты воздушного пространства государства. Комплексное развитие данных направлений обеспечивает своевременное обнаружение угроз, оперативное реагирование и устойчивость системы безопасности в условиях современных вызовов.

Список использованных источников:

1. «Лапшин, В.И. Современные системы противовоздушной обороны: тактика и стратегия» / В.И. Лапшин. – М.: Военное издательство, 2023. – 320 с

2. «Михайлов, А.Н. Беспилотные летательные аппараты в современных вооруженных конфликтах» / А.Н. Михайлов. – СПб.: Наука, 2022. – 280 с.

3. «Гаврилов, Е.П. Гибридные угрозы и национальная безопасность: вызовы XXI века» / Е.П. Гаврилов. – Минск: Академия безопасности, 2023. – 200 с.

СОВРЕМЕННЫЕ ПОДХОДЫ К ПРОТИВОВОЗДУШНОЙ ОБОРОНЕ В УСЛОВИЯХ ГИБРИДНЫХ УГРОЗ

Возный П.С.

Белорусский государственный университет информатики и радиоэлектроники г. Минск, Республика Беларусь

Хожевец О.А.

Аннотация. В условиях трансформации характера вооружённой борьбы противовоздушная оборона приобретает качественно новое значение. Современные военные конфликты всё в большей степени характеризуются переходом к гибридным формам противоборства, в которых сочетаются как традиционные, так и нетрадиционные средства воздействия. Воздушная угроза в таких условиях носит комплексный, многокомпонентный характер и требует адекватного реагирования со стороны систем ПВО.

Гибридный характер современных угроз проявляется в одновременном применении высокоточного оружия, беспилотных летательных аппаратов, средств радиоэлектронной борьбы, а также кибер- и информационного воздействия. Это существенно усложняет задачу противовоздушной обороны, поскольку противник стремится не только нанести удар, но и дезорганизовать систему управления, снизить её устойчивость и эффективность.

Особую актуальность приобретает проблема противодействия беспилотным летательным аппаратам. Массовое применение малозаметных, дешёвых и технологически доступных БПЛА приводит к необходимости пересмотра традиционных подходов к ПВО. Классические системы, ориентированные на ограниченное количество высокоскоростных целей, оказываются недостаточно эффективными в условиях насыщения воздушного пространства множеством объектов. В связи с этим требуется адаптация средств обнаружения и поражения, а также разработка новых методов борьбы с подобными угрозами.

Неотъемлемым элементом современной системы ПВО становятся средства радиоэлектронной борьбы. Их применение позволяет эффективно подавлять каналы управления беспилотными аппаратами, нарушать работу навигационных систем и снижать точность применения высокоточного оружия. В ряде случаев использование

РЭБ позволяет нейтрализовать угрозу без применения огневых средств, что повышает экономическую эффективность обороны.

Важным направлением остаётся повышение живучести системы противовоздушной обороны. В условиях применения противником высокоточного оружия особое значение приобретают мобильность, рассредоточение, маскировка и создание ложных позиций. Эти меры позволяют сохранить боеспособность системы даже при нанесении ударов по её ключевым элементам.

Эффективная противовоздушная оборона невозможна без тесного межвидового взаимодействия.

Координация действий ВВС, войск ПВО, подразделений разведки и киберзащиты обеспечивает комплексный подход к отражению угроз. Формирование единого информационного пространства становится основой для повышения согласованности и результативности действий всех компонентов системы обороны.

В условиях усложнения характера угроз возрастает значение подготовки кадров. Современные специалисты ПВО должны обладать не только глубокими профессиональными знаниями, но и навыками работы с высокотехнологичными системами, способностью быстро принимать решения в условиях неопределённости и высокой динамики обстановки.

Таким образом, развитие противовоздушной обороны в условиях гибридных угроз представляет собой комплексную задачу, включающую техническую модернизацию, совершенствование организационных структур и внедрение новых подходов к управлению. Перспективы развития ПВО связаны с дальнейшей цифровизацией, внедрением автономных систем, расширением возможностей обнаружения и нейтрализации современных воздушных угроз.

Список использованных источников:

1. Фёдоров, И.П. Радиолокационные технологии XXI века: развитие и применение / И.П. Фёдоров. – Новосибирск: Военно-инженерный институт, 2023. – 230 с.

2. Лебедев, Ю.М. Повышение эффективности ПВО с использованием фазированных антенных решеток / Ю.М. Захаров. – М.: Оборонное издательство, 2021. – 250 с.

3. Федотов, Д.И. Инновации в радиолокации: адаптивные алгоритмы обработки сигналов / Д.И. Романов. – Минск: Научно-исследовательский институт радиотехники, 2023. – 190 с.

4. Морозов, П.В. Радиолокационные станции нового поколения: принципы работы и перспективы / П.В. Калинин. – СПб.: Военно-технический университет, 2022. – 280 с.

РАЗВИТИЕ БЕСПИЛОТНОЙ АВИАЦИИ В СИСТЕМЕ ПРОТИВОВОЗДУШНОЙ ОБОРОНЫ БЕЛАРУСИ

Пеунов Т.А.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Лавринчик Н.Н.

Аннотация. Развитие беспилотной авиации в системе противовоздушной обороны Республики Беларусь приобретает всё большую актуальность в условиях современных вызовов и трансформации военных технологий. Беспилотные летательные аппараты (БПЛА), или дроны, становятся важным элементом обеспечения эффективности ПВО, и Республика Беларусь активно интегрирует их в свою оборонную систему.

Применение БПЛА открывает широкие возможности, включая снижение рисков для личного состава, повышение эффективности разведки и наблюдения, обеспечение точечного воздействия на цели, а также оптимизацию затрат на подготовку и эксплуатацию техники. В этой связи развитие беспилотной авиации в системе ПВО Вооружённых Сил Республики Беларусь рассматривается как одно из приоритетных направлений, требующее комплексного и детального анализа.

На современном этапе развитие беспилотной авиации в системе противовоздушной обороны Республики Беларусь характеризуется активным использованием БПЛА как отечественного, так и зарубежного производства. Преимущественно применяются аппараты ближнего и среднего радиуса действия, предназначенные для решения задач разведки, наблюдения и корректировки огня в интересах ПВО.

Беспилотные летательные аппараты играют важную роль в обеспечении контроля воздушного пространства и мониторинга обстановки: они используются для наблюдения за государственной границей, выявления передвижений противника, обнаружения диверсионных групп, а также оценки последствий чрезвычайных ситуаций. Оснащение БПЛА современными сенсорами (оптическими, тепловизионными, радиолокационными) обеспечивает получение информации в круглосуточном режиме и при различных погодных условиях, что существенно повышает эффективность системы ПВО.

Важным направлением является применение беспилотной авиации для патрулирования стратегически значимых объектов, включая военные базы, склады вооружения и участки государственной границы. Это позволяет своевременно выявлять угрозы в воздушном и наземном пространстве и оперативно реагировать на возможные нарушения.

Особое значение приобретает развитие средств радиоэлектронной борьбы на базе БПЛА. Такие комплексы способны подавлять каналы связи и управления противника, что усиливает возможности противовоздушной обороны. Одновременно ведётся работа по созданию и производству собственных беспилотных систем, что позволяет снизить зависимость от внешних поставок, адаптировать технику к национальным условиям и повысить общий уровень технологической независимости.

Перспективным направлением является повышение уровня автономности и интеллектуализации БПЛА, что позволит эффективно применять их в сложной радиоэлектронной обстановке. Разработка ударных беспилотных комплексов также расширяет возможности системы ПВО за счёт точечного воздействия по важным объектам, при условии соблюдения международных норм и ограничений.

Ключевой задачей остаётся интеграция беспилотной авиации в единую систему управления войсками, что обеспечит оперативную передачу разведывательной информации и повысит скорость принятия решений. Наряду с этим требуется развитие средств противодействия БПЛА противника, включая системы обнаружения, подавления и уничтожения воздушных целей малого размера.

Реализация данных направлений связана с необходимостью значительных финансовых вложений, а также развитием научно-технической базы, в частности в области микроэлектроники и сенсорных технологий. Сокращение технологического отставания от ведущих стран является важным условием повышения конкурентоспособности отечественных разработок.

Неотъемлемой частью развития беспилотной авиации в системе ПВО является подготовка квалифицированного персонала, способного эффективно эксплуатировать современные комплексы. В целом, внедрение и совершенствование БПЛА способствует снижению потерь среди личного состава, повышению уровня безопасности и расширению возможностей применения сил ПВО, включая задачи невоенного характера, такие как экологический мониторинг. Это делает развитие беспилотной авиации стратегически значимым направлением для Республики Беларусь.

Список использованных источников:

1. Гуторов А.В. “Система активной стабилизации навесного оборудования для БПЛА” — Минск: БГУ, 2024.
2. Макаревич М.В. "Применение беспилотных летательных аппаратов в интересах Вооруженных сил." — Брест: БрГТУ, 2024
3. Петров В.А.. "Современные технологии беспилотной авиации." — Минск: Академия наук, 2020.

ВЗАИМОДЕЙСТВИЕ ДЕЖУРНЫХ СИЛ ПВО С ВОЙСКАМИ ТЕРРИТОРИАЛЬНОЙ ОБОРОНЫ ПРИ ОХРАНЕ КРИТИЧЕСКИ ВАЖНЫХ ОБЪЕКТОВ

Ревенко С.А.

Белорусский государственный университет информатики и радиоэлектроники г. Минск, Республика Беларусь

Беккеров Д.Э.

Аннотация. Современные вызовы и изменения в системе глобальной безопасности ставят перед Вооруженными Силами Республики Беларусь новые задачи, требующие модернизации Военно-Воздушных Сил (ВВС) и войск противовоздушной обороны (ПВО). Учитывая геополитическое положение страны, интеграцию в систему коллективной безопасности ОДКБ и необходимость защиты суверенитета, развитие ВВС и ПВО является одним из приоритетных направлений оборонной политики Беларуси.

В условиях роста геополитической напряженности и усиления военной активности у границ Республики Беларусь, защита критически важной инфраструктуры (АЭС, крупных промышленных узлов, транспортных хабов) становится приоритетом национальной безопасности. Опыт современных конфликтов показывает, что основную угрозу для таких объектов представляют высокоточное оружие и рои беспилотных летательных аппаратов (БПЛА). В этой связи ключевой задачей становится выстраивание эффективного взаимодействия между кадровыми дежурными силами ПВО и подразделениями территориальной обороны.

Основу защиты составляют регулярные войска ПВО, однако их возможности по обнаружению низколетящих малоразмерных целей могут быть ограничены особенностями рельефа или городской застройки.

Здесь роль территориальных войск становится решающей: создание сети постов визуального и радиотехнического наблюдения силами территориальной обороны позволяет значительно расширить информационное поле ПВО.

Охрана критических объектов требует не только наличия современных ЗРК (таких как «Тор-М2К» или «Панцирь-С1»), но и активного участия территориальных сил в инженерном оборудовании позиций и обеспечении живучести объектов. В рамках взаимодействия дежурные силы ПВО обеспечивают высокотехнологичный зонтик «дальнего радиуса», в то время как войска территориальной обороны сосредотачиваются на непосредственном прикрытии периметра от диверсионных. Важным аспектом является совместное использование аэродромной и логистической инфраструктуры, модернизированной для нужд как регулярной армии, так и резервных формирований.

Одним из главных вызовов остается отработка слаженности действий. Программы подготовки специалистов ПВО в Беларуси и вузах РФ всё чаще включают компоненты взаимодействия с территориальными войсками. Регулярные совместные учения позволяют отработать алгоритмы оповещения и разграничения зон ответственности, что критически важно для исключения случаев «дружественного огня» и обеспечения непрерывного контроля воздушного пространства. Особое внимание уделяется подготовке расчетов территориальной обороны к работе с современными оптико-электронными системами обнаружения.

При развертывании временных позиций ПВО и постов территориальной обороны вблизи охраняемых объектов учитываются экологические стандарты. Внедрение энергоэффективных систем мониторинга и снижение шумового воздействия техники вблизи населенных пунктов позволяют минимизировать антропогенную нагрузку при сохранении высокого уровня боеготовности.

Таким образом, интеграция дежурных сил ПВО и войск территориальной обороны создает гибкую и устойчивую систему защиты критически важных объектов Республики Беларусь. Сочетание высокой технологичности регулярных войск и массовости территориальных формирований позволяет сформировать «интеллектуальный щит», способный эффективно противодействовать как традиционным средствам воздушного нападения, так и новейшим асимметричным угрозам. Стратегический курс на такое взаимодействие обеспечивает надежную защиту национальных интересов в условиях меняющегося характера современных войн.

Список использованной источников:

1. Военный информационный портал Беларуси (mod.mil.by)

2. Российские средства массовой информации(СМИ) (РИА Новости, ТАСС)

3. Аналитические отчеты Центра стратегических и внешнеполитических исследований (Республика Беларусь)

4. Материалы совместных учений Российской Федерации и Республики Беларусь (2021–2024 гг.).

ПЕРСПЕКТИВЫ РАЗВИТИЯ СИСТЕМ РАДИОЛОКАЦИОННОГО КОНТРОЛЯ МАЛЫХ ВЫСОТ В ВВС И ВОЙСКАХ ПВО ВООРУЖЕННЫХ СИЛ РЕСПУБЛИКИ БЕЛАРУСЬ

Якубовский А.С.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Маргель А.Б.

Аннотация. Тезис посвящён актуальным вопросам развития систем радиолокационного контроля малых высот в ВВС и войсках ПВО Республики Беларусь. В работе рассмотрены современные вызовы, такие как массированное применение малоразмерных беспилотников и крылатых ракет, обоснована необходимость модернизации радиолокационных станций, внедрения алгоритмов цифровой обработки сигналов и подготовки квалифицированных специалистов для повышения эффективности защиты нижнего эшелона воздушного пространства.

Современные тенденции в развитии средств воздушного нападения и смещение тактического акцента на предельно малые высоты диктуют необходимость постоянного совершенствования системы противовоздушной обороны (ПВО). В этом контексте радиолокационные комплексы малых высот в Военно-воздушных силах (ВВС) и войсках ПВО Республики Беларусь играют ключевую роль в обеспечении национальной безопасности и создании сплошного радиолокационного поля.

Основная задача таких систем заключается в своевременном обнаружении, сопровождении и идентификации низколетящих объектов, а также в оперативной выдаче целеуказаний зенитным ракетным комплексам.

Одним из важнейших направлений развития является внедрение передовых технологий цифровой обработки сигналов и современных автоматизированных систем управления (АСУ). Современные АСУ позволяют автоматизировать процессы завязки трасс целей, минимизируя влияние человеческого фактора и повышая скорость реакции комплексов ПВО.

Например, алгоритмы на базе элементов искусственного интеллекта способны эффективно селектировать истинные малоразмерные цели на фоне интенсивных помех от подстилающей поверхности и метеообразований, передавая очищенную информацию на командные пункты для принятия оперативных решений.

Это особенно важно в условиях высокой интенсивности боевых действий, когда время на реакцию критически мало.

Не менее важным аспектом является аппаратная модернизация радиолокационного парка. Многие из радаров предыдущих поколений обладают недостаточной помехозащищенностью, что снижает их потенциал в условиях современных радиоэлектронных угроз.

Среди первоочередных задач – переход на твердотельные передатчики и активные фазированные антенные решетки (АФАР), которые обеспечивают высокую точность координат, увеличенную дальность действия и способность работать в условиях активного радиоэлектронного подавления противником.

Еще одним стратегическим направлением выступает повышение мобильности радиолокационных станций. Стационарные посты уязвимы для высокоточного оружия. Современные мобильные радары малых высот, смонтированные на высокопроходимых колесных или гусеничных шасси, способны в кратчайшие сроки развертываться на неподготовленных позициях, обеспечивая гибкий подход и высокую живучесть группировки ПВО.

Особое внимание должно быть уделено подготовке личного состава радиотехнических войск. Эксплуатация новейших радиолокационных комплексов требует глубоких инженерных знаний и навыков работы с высокотехнологичной аппаратурой, чтобы операторы могли оперативно адаптироваться к сложной обстановке.

Важнейшим условием успеха является глубокая интеграция маловысотных радаров с другими элементами системы ПВО, такими как комплексы визуального наблюдения, зенитные ракетные системы и авиация. Это позволит создать единую информационную сеть для оперативного обмена данными.

Комплексный подход, включающий обновление парка РЛС, внедрение цифровых алгоритмов, повышение маневренности комплексов, качественную подготовку кадров и учет международного опыта, позволит создать надежный щит для защиты воздушного пространства.

Список использованных источников:

1. Романов, Д.И. Инновации в радиолокации: адаптивные алгоритмы обработки сигналов / Д.И. Романов. – Минск: Научно-исследовательский институт радиотехники, 2023. – 190 с.

2. Смирнов, Е.Н. Интеграция оптико-электронных систем в автоматизированные комплексы ПВО / Е.Н. Смирнов, А.И. Петров. – М.: Воениздат, 2019. – 270 с.

3. МЕЖДУНАРОДНЫЙ ОПЫТ ОРГАНИЗАЦИИ ПРОТИВОВОЗДУШНОЙ ОБОРОНЫ В СОВРЕМЕННЫХ УСЛОВИЯХ: СБОРНИК МАТЕРИАЛОВ МЕЖДУНАРОДНОЙ КОНФЕРЕНЦИИ. – МИНСК: БГТУ, 2022. – 312 С.

ИСПОЛЬЗОВАНИЕ МЕТОДА ОПОРНЫХ ВЕКТОРОВ ДЛЯ ФОРМИРОВАНИЯ ОДНОМЕРНОЙ РЕШАЮЩЕЙ СТАТИСТИКИ ПРИ РАСПОЗНАВАНИИ МАЛОРАЗМЕРНЫХ БЕСПИЛОТНЫХ ЛЕТАТЕЛЬНЫХ АППАРАТОВ И ПТИЦ

Чигряй В.Г.

Военная академия Республики Беларусь г. Минск, Республика Беларусь

Храменков А.С. – канд. тех. наук, доцент

Аннотация. Предложен способ формирования решающей статистики в задаче последовательного радиолокационного распознавания малых беспилотных летательных аппаратов и птиц с использованием алгоритмов машинного обучения. На этапе обучения оцениваются условные вероятности правильного и ложного распознавания с использованием метода опорных векторов, которые используются для вычисления логарифмических приращений решающей статистики в последовательном критерии отношения вероятностей. Это позволяет осуществить переход от многомерного пространства признаков к одномерной статистике расстояния до разделяющей гиперплоскости и реализовать последовательный критерий Вальда без задания аналитических моделей распределений признаков.

Задача радиолокационного распознавания (РЛР) малоразмерных беспилотных летательных аппаратов (МБЛА) на фоне птиц является одной из актуальных задач радиолокационного обеспечения и противодействия малоразмерным воздушным объектам. Сходство эффективной площади рассеяния, скоростных и траекторных характеристик МБЛА и птиц, а также нестационарный характер отраженных сигналов существенно затрудняют их надежное различение при ограниченном времени наблюдения и наличии помех.

Современные подходы к РЛР развиваются, как правило, по двум направлениям. Первое направление связано с применением статистических методов распознавания, в том числе последовательных процедур принятия решений [1], обеспечивающих оптимальность по быстродействию при заданных вероятностных показателях качества. Второе направление основано на использовании методов машинного обучения [2], позволяющих автоматически формировать разделяющие правила в многомерном пространстве классификационных признаков, включая признаки различной физической природы.

При этом статистические методы последовательного распознавания традиционно предполагают наличие априорных моделей распределения наблюдаемых величин, что существенно ограничивает их практическое применение в условиях сложных и слабо формализуемых сигналов. В свою очередь, методы машинного обучения, широко используемые для классификации радиолокационных объектов, как правило, ориентированы на одношаговое принятие решений и не учитывают возможности адаптивного управления длительностью наблюдения и накопления информации.

В докладе представлен способ формирования решающей статистики, основанный на разделении этапов обучения и распознавания. На этапе обучения по размеченной выборке длинной *N* методом опорных векторов строится линейная разделяющая гиперплоскость в пространстве признаков [2 – 5]:

$$\{(\mathbf{x}_n, y_n)\}_{n=1}^{N}, \qquad 1)$$

где $y_n = +1$ – метка, соответствующая объектам класса МБЛА, а $y_n = -1$ – объектам класса птиц в *n*-й реализации обучающей выборке;

$\mathbf{x}_n = \left| x_n^{(1)} \;\; x_n^{(2)} \;\; x_n^{(3)} \;\; \ldots \;\; x_n^{(L-1)} \;\; x_n^{(L)} \right|^{\mathrm{T}}$ – *L*-мерный вектор классификационных признаков МБЛА и птиц.

На рисунке 1 представлен пример двумерной обучающей выборки и разделяющей гиперплоскости.

а *б*

Рисунок 1 – Визуализация этапа обучения: *а* – обучающая выборка, *б* – разделяющая гиперплоскость

Разделяющая гиперплоскость рассчитывается по критерию максимизации «зазора» между признаками двух альтернативных классов [5]:

$$d_n = d(\mathbf{x}_n) = \frac{\mathbf{w}^T \mathbf{x}_n + b}{\| \mathbf{w} \|}. \qquad 2)$$

где $\| \mathbf{w} \| = \sqrt{\mathbf{w}^T \mathbf{w}} = \sqrt{\sum_{i=1}^{L} w_i^2}$ – евклидова норма вектора весов разделяющей гиперплоскости.

По обучающей выборке оцениваются условные вероятности правильного (D_{UAV}) и ложного (F_{UAV}) распознавания МБЛА относительно порога $d = 0$.

Условные вероятности правильного и ложного распознавания МБЛА определяются по обучающей выборке как относительное число реализаций соответствующих классов, для которых выполняется условие d > 0:

$$D_{UAV} = \frac{1}{N} \sum_{n: y_n = +1} \mathrm{I}(d_n > 0), \; F_{UAV} = \frac{1}{N} \sum_{n: y_n = -1} \mathrm{I}(d_n > 0), \qquad 3)$$

где $\mathrm{I}(d_n > 0) = \begin{cases} 1, \text{ если } d_n \geq 0 \\ 0, \text{ если } d_n < 0 \end{cases}$ – индикаторная функция.

Оцененные значения вероятностей D_{UAV} и F_{UAV}, а также параметры разделяющей гиперплоскости $\mathbf{w}$ и b сохраняются и используются на этапе РЛР.

На k-м шаге процедуры РЛР по имеющейся входной реализации $\mathbf{x}_k$ классификационных признаков и положению разделяющей гиперплоскости оценивается расстояние d_k. На основании знака d_k и рассчитанных вероятностей правильного и ложного распознавания формируется приращение решающей статистики последовательного критерия отношения вероятностей ΔZ_k:

$$\text{при } d_k \geq 0, \;\; \Delta Z_k = \lg\left(\frac{D_{UAV}}{F_{UAV}}\right), \;\; \text{если } d_k < 0, \text{ то } \Delta Z_k = -\lg\left(\frac{1 - D_{UAV}}{1 - F_{UAV}}\right) \qquad 4)$$

Тем самым многомерная задача сводится к рекуррентному накоплению одномерной статистики, сопоставляемой с порогами Z^*_{up} и Z^*_{low} последовательного критерия Вальда, что обеспечивает адаптивную длительность наблюдения и требуемые показатели достоверности $D_{тр}$ и $F_{тр}$ [1]:

$$Z^*_{up} = \ln\left(\frac{D_{тр}}{F_{тр}}\right), \;\; Z^*_{low} = \ln\left(\frac{1 - D_{тр}}{1 - F_{тр}}\right) \qquad 4)$$

На рисунке 2 представлена иллюстрация процедуры формирования решающей статистики и принятия решения в соответствии с последовательным критерием отношения вероятностей.

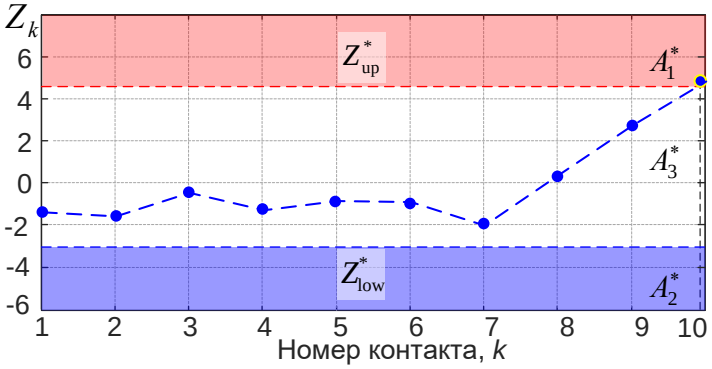

Рисунок 2 – Формирование решающей статистики и принятия решения по последовательному критерию Вальда

Предложенный способ является комбинацией методов машинного обучения и статистических методов распознавания, что создает основу для дальнейших исследований, направленных на выбор и анализ конкретных сигнальных и траекторных признаков, а также на экспериментальную оценку показателей качества распознавания в различных условиях наблюдения.

Список использованных источников:

1. Wald, A. Sequential Analysis. – New York: Wiley, 1947.

2. Murphy, K. P. Machine Learning: A Probabilistic Perspective. – Cambridge: MIT Press, 2012.

3. Yan, J., Hu, H., Gong, J., Kong, D., Li, D. Exploring Radar Micro-Doppler Signatures for Recognition of Drone Types // Drones. 2023. Vol. 7, № 4. Art. 280. DOI: 10.3390/drones7040280.

4. Kretzschniar, R., Karayiannis, N. B., Richner, H. A Comparison of Feature Sets and Neural Network Classifiers on a Bird Removal Approach for Wind Profiler Data // Proc. IJCNN. 2000. Vol. 2. P. 279–284. DOI: 10.1109/IJCNN.2000.857909.

Lin, Q. et al. Ground-Based Radar Detection Dataset of «Low Slow Small» UAVs under Simple Field Background Conditions // Journal of Signal Processing. 2024. Vol. 40, № 11. P. 2095–2104. DOI: 10.12466/xhcl.2024.11.014.

АНАЛИЗ СУЩЕСТВУЮЩИХ АЛГОРИТМОВ ОРИЕНТАЦИИ В БИНС

Тищенко Т.А., Маликов А.С.

Белорусская государственная академия авиации г. Минск, Республика Беларусь

Боровой А.Г. – кандидат технических наук, доцент

Анотация. В докладе производится анализ алгоритмов ориентации БИНС (алгоритм с углами Эйлера-Крылова, алгоритм с направляющими косинусами (алгоритм на основе обобщенного уравнения Пуассона), алгоритм с кватернионами (параметрами Родрига – Гамильтона)).

В настоящее время существует зависимость при определении навигационных параметров от спутниковых систем навигации (СНС). Для устранения этой зависимости в качестве навигационной системы беспилотных летательных аппаратов (БЛА) предлагается использовать бесплатформенные инерциальные навигационные системы (БИНС).

Преимуществом БИНС перед другими навигационными системами заключается в их полной независимости от внешних источников данных, повышенной защите от помех, высокой информативности и возможности передавать информацию на большой скорости, не требует информации о магнитном поле Земли, не излучает энергию.

Отсутствием какого-либо излучения при работе БИНС обеспечивается скрытность объекта,на котором она используется. Недостатком БИНС можно назвать ошибки, которые накапливаются с течением времени в получаемой от приборов информации. Это могут быть как методические ошибки, так и ошибки, связанные с неверной начальной настройкой оборудования.

Рассматриваются алгоритмы ориентации и их техническая реализация в виде стохастической компьютерной модели в программе MATLAB-SIMULINK (БИНС) (алгоритм с углами Эйлера-Крылова, алгоритм с направляющими косинусами (алгоритм на основе обобщенного уравнения Пуассона), алгоритм с кватернионами (параметрами Родрига – Гамильтона).

Недостатками рассмотренных алгоритмов БИНС с углами Эйлера–Крылова и уравнениями Пуассона являются нелинейность преобразования пространственной ориентации БЛА в связанной и географической системах координат по всем трем углам и неспособность решать задачу ориентации при угле тангажа в 90°. Наиболее удобными для БИНС являются параметры Родрига – Гамильтона (кватернионы), которых четыре в отличие от трех углов Эйлера–Крылова и кинематические уравнения с кватернионами линейны и интегрируемы при любых углах курса, тангажа и крена.

В компьютерных моделях БИНС с углами Эйлера – Крылова взаимное положение связанной системы координат БЛА и географической системы координат определяется тремя углами Эйлера – Крылова и девятью направляющими косинусами, которые в БИНС в кватернионах можно заменить с помощью четырех параметров Родрига – Гамильтона.

Таким образом в БИНС реализуются алгоритмы ориентации с использованием различных кинематических параметров и алгоритмы навигации для определения координат местоположения БЛА. Точность БИНС на микрогироскопах и микроакселерометрах обратно пропорциональна времени полета БЛА, поэтому для повышения точности траекторного управления летательным аппаратом необходимы сложные алгоритмы формирования навигационных параметров и их коррекция. В качестве альтернативной системы СНС можно использовать радиотехническую систему дальней навигации (РСДН «Чайка»), где существует избыточность первичных измеряемых параметров (разностей дальностей). Навигационные параметры, полученные с помощью РСДН «Чайка», не имеют тенденции к накоплению погрешностей, как БИНС, однако существует относительно невысокая точность определения координат объекта (максимальная ошибка определения местоположения – 100…1000 м). Комплексирование БИНС и РСДН позволяет получить высокоточный надежный навигационный комплекс, сочетающий в себе преимущества БИНС и РСДН.

Список использованных источников:

1. Матвеев, В.В. Основы построения бесплатформенных инерциальных навигационных систем : учеб. пособие / В.В. Третьяков, В.Я. Распопов. – СПб.: ГНЦ РФ ОАО «Концерн «ЦНИИ «Электроприбор», 2009.– 280 с.

2. Гриднев, Ю.В. Компьютерная модель БИНС с углами Эйлера-Крылова / Ю.В. Гриднев, А.Н. Пальцев, А.И. Мельник // Инженер механик. – 2011. №1. – С. 17-26.

3. Гриднев, Ю.В. Стохастическая компьютерная модель БИНС с уравнениями Пуассона / Ю.В. Гриднев, А.Н. Пальцев, Ю.Ф. Яцына // Инженер механик. – 2011. №1. – С. 27-30.

4. Гриднев, Ю.В. Стохастическая компьютерная модель БИНС БЛА с параметрами Родрига – Гамильтона (кватернионами) / Ю.В. Гриднев, А.Н. Пальцев, Ю.Ф. Яцыгин // Инженер механик. – 2012. №1. – С. 6-14.

5. Вовасов В.Е. Комплексирование радиотехнических систем управления с другими информационными датчиками / В.Е. Вовасов, С.А. Герко – М. : Горячая линия – Телеком, 2021. – 242 с.

6. Бабич, О.А. Обработка информации в навигационных комплексах / – М.: Машиностроение, 1991. – 512 с.

ИСПОЛЬЗОВАНИЕ ДЕМОНСТРАЦИОННОГО СТЕНДА «ОПТОЭЛЕКТРОННЫЙ ЛОГИЧЕСКИЙ ЭЛЕМЕНТ *ИЛИ-НЕ*» В ОБРАЗОВАТЕЛЬНОМ ПРОЦЕССЕ УЧРЕЖДЕНИЯ ОБРАЗОВАНИЯ «ВОЕННАЯ АКАДЕМИЯ РЕСПУБЛИКИ БЕЛАРУСЬ»

Медушевская Н.В.

Учреждение образования «Военная академия Республики Беларусь» г. Минск, Республики Беларусь

Мацкевич А.Н. – к.т.н., доцент

Аннотация. В работе рассмотрены принципы построения и результаты использования разработанного демонстрационного стенда «Оптоэлектронный логический элемент ***ИЛИ-НЕ***» в образовательном процессе Учреждения образования «Военная академия Республики Беларусь»

При реализации цифровых алгоритмов обработки информации и управления в радиоэлектронной аппаратуре специального назначения применяются логические элементы, в том числе и оптоэлектронные. Анализ способов повышения эффективности обучения показывает, что на кафедре радиотехники и электроники учреждения образования «Военная академия Республики Беларусь» изучение принципов и режимов работы логических элементов производится на лекционных занятиях с использованием мультимедийных технологий. Наглядность при изучении назначения, режимов работы оптоэлектронных логических элементов дополнительно может быть обеспечена за счёт применения в образовательном процессе на кафедре радиотехники и электроники демонстрационных стендов.

Демонстрационный стенд «Оптоэлектронный логический элемент ***ИЛИ-НЕ***» предназначен для демонстрации принципа действия оптоэлектронного логического элемента (ЛЭ) ***ИЛИ-НЕ*** при изучении дисциплины «Оптоэлектронные приборы и цифровые устройства» («ОЭП и ЦУ»).

Демонстрационный стенд позволяет:

– наглядно пояснить принцип функционирования оптоэлектронного ЛЭ ***ИЛИ-НЕ,*** выполняющего операцию «логическое сложение и отрицание»;

– наглядно пояснить принцип функционирования транзисторного оптрона.

На рисунке 1 показана принципиальная схема демонстрационного стенда для изучения оптоэлектронного логического элемента ***ИЛИ-НЕ***.

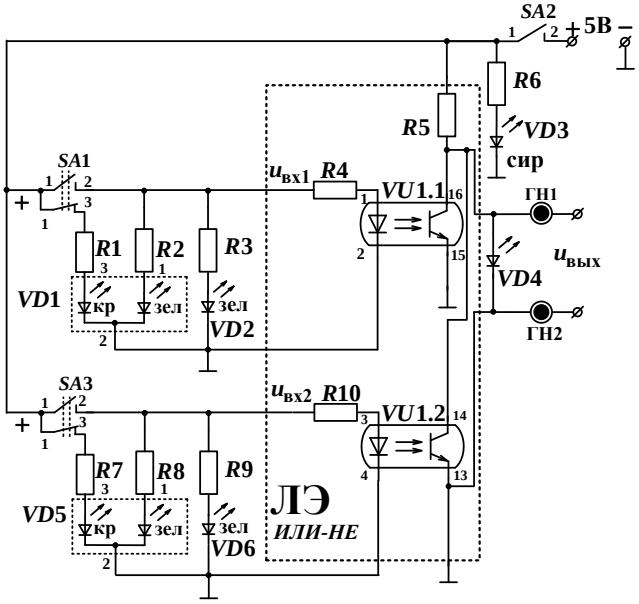

Рисунок 1 – Принципиальная схема демонстрационного стенда для изучения оптоэлектронного ЛЭ ***ИЛИ-НЕ***

Назначение элементов демонстрационного стенда для изучения оптоэлектронного ЛЭ ***ИЛИ-НЕ***:

– переключатели ***SA***1 и ***SA***3 обеспечивают подачу на входы ЛЭ напряжений, соответствующих уровням логической единицы и логического нуля, а также напряжения питания светоизлучающих диодов ***VD*1, *VD*2, *VD*5, *VD*6**;

– светоизлучающие диоды ***VD*1** и ***VD*5** обеспечивают визуальную фиксацию состояния фототранзисторов оптронов ***VU*1.1** и ***VU*1.2**;

– переключатель ***SA***2 обеспечивает подключение источника питания;

– светоизлучающий диод ***VD3*** обеспечивают визуальную фиксацию наличия напряжения источника питания;

– светоизлучающие диоды ***VD*2** и ***VD*6** обеспечивают визуальную фиксацию напряжения на входах ЛЭ, соответствующего логической единице;

– светоизлучающий диод ***VD*4** обеспечивает визуальную фиксацию напряжения на выходе;

– резисторы ***R*1**-***R*10** предназначены для ограничения токов, протекающих через светоизлучающие диоды.

Для подключения источника питания к схеме необходимо замкнуть переключатель ***SA*2**, при этом СИД ***VD*3** светит, что свидетельствует о наличии напряжения в схеме.

Для подачи на оба входа ЛЭ ***ИЛИ-НЕ*** напряжения логического нуля необходимо разомкнуть переключатели ***SA*1** и ***SA*3** (перевести рычаги в верхнее положение). При этом на СИД ***VD*2 зел** и ***VD*6 зел** напряжение питания не подается, они не светят (что свидетельствует о подаче на соответствующий вход ЛЭ ***ИЛИ-НЕ*** логического нуля). В этом случае оба фототранзистора оптронов ***VU*1.1** и ***VU*1.2** будут находиться в режиме отсечки (об этом свидетельствуют светящиеся СИД ***VD*1 кр** и ***VD*4 кр**, к ним через замкнутые контакты 1 и 3 переключателей ***SA*1** и ***SA*3** подано напряжение питания). Ток от источника питания протекает по цепи *R*5 – СИД ***VD*4**, который будет светить зеленым цветом. На рисунке 2 показана фотография внешнего вида стенда при подаче на оба входа ЛЭ ***ИЛИ-НЕ*** напряжения логического нуля.

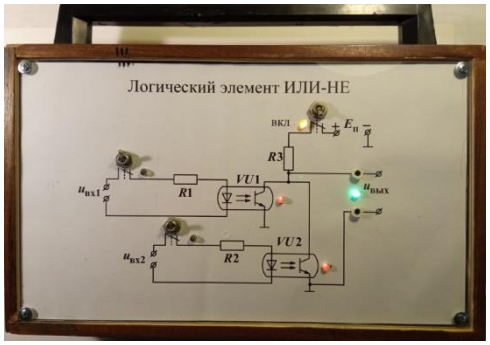

Рисунок 2 – Внешний вид демонстрационного стенда для изучения оптоэлектронного логического элемента ***ИЛИ-НЕ***

Для подачи на оба входа (или один из входов) ЛЭ ***ИЛИ-НЕ*** напряжения логической единицы необходимо замкнуть соответствующие переключатели ***SA*1** и ***SA*2** (перевести рычаги в нижнее положение). В этом случае через замкнутые контакты 1 и 2 этих переключателей на СИД ***VD*2 зел** и ***VD*6 зел** будет подано напряжение питания, они светят (что свидетельствует о подаче на соответствующий вход ЛЭ ***ИЛИ-НЕ*** логической единицы). В этом случае соответствующие фототранзисторы оптронов ***VU*1.1** и ***VU*1.2** будут находиться в режиме насыщения, (об этом свидетельствуют светящиеся СИД ***VD*1 зел** и ***VD*5 зел**, к ним через замкнутые контакты 1 и 3 переключателей ***SA*1** и ***SA*3** подано напряжение питания). СИД ***VD*4** не светит.

Эффективность использования разработанных демонстрационных стендов в учебном процессе оценивалась при проведении семинарских занятий (Семинар №2. Занятие 3.1.4. Применение оптоэлектронных приборов) темы 3.1 (Оптоэлектронные приборы) раздела 3 (Оптоэлектронные приборы и устройства) дисциплины «ОЭП и ЦУ» в учебных группах (421а и 421б) с курсантами второго курса факультета связи и автоматизированных систем управления учреждения образования «Военная академия Республики Беларусь».

Для проведения эксперимента были выбраны две практически одинаковые по успеваемости учебные группы 421а и 421б. Эксперимент заключался в изучении первого вопроса семинара (Применение оптронов для выполнения логических операций) с использованием демонстрационных стендов только в одной учебной группе (421б). Далее в конце учебного занятия проводился экспресс-опрос по усвоению учебного материала по второму вопросу семинара № 2 со всеми курсантами в каждой из учебных групп. По сравнительному анализу результатов (оценок) экспресс-опроса оценивалась эффективность использования демонстрационных стендов при изучении оптоэлектронных логических элементов.

На экспресс-опрос выносились следующие вопросы:

– вариант №1 – изобразить условное графическое обозначение и таблицу режимов работы оптоэлектронных логических элементов ***И*** и ***ИЛИ-НЕ***;

– вариант №2 – изобразить условное графическое обозначение и таблицу режимов работы оптоэлектронных логических элементов ***ИЛИ*** и ***И-НЕ***.

На выполнение заданий экспресс-опроса выделялось время – 10 минут.

Анализ результатов экспресс-опроса курсантов 421а и 421б учебных групп на семинаре № 2 по дисциплине «ОЭП и ЦУ» показывает, что при практически одинаковом рейтинге учебных групп средний балл по результатам проведения экспресс-опроса в учебной группе 421б, где использовались на занятии разработанные демонстрационные стенды для изучения оптоэлектронных логических элементов, средний балл был на 1,3 выше, чем в 421а учебной группе.

ОБЗОР ТЕХНИЧЕСКИХ ОСОБЕННОСТЕЙ ПРИ СОВМЕСТНОМ ИСПОЛЬЗОВАНИИ ТЕПЛОВИЗИОННОГО И ТЕЛЕВИЗИОННОГО КАНАЛОВ ОБНАРУЖЕНИЯ ЦЕЛИ

Гуцев П.А.

Учреждение образования «Военная академия Республики Беларусь»
г. Минск, Республика Беларусь

Казарин А.В. – канд. тех. наук, доцент

В статье рассмотрены принципы построения двухканальных оптико-электронных систем, объединяющих телевизионный и тепловизионный каналы. Проанализированы оптические схемы (раздельные объективы и общий объектив с дихроичным светоделителем), методы пространственного совмещения изображений на основе гомографии, особенности тепловой стабилизации микроболометрических матриц и алгоритмы адаптивного слияния с динамическим расчетом весов. Показано, что эффективность системы определяется глубиной алгоритмической интеграции и выбором вычислительной платформы (FPGA, GPU, SoC) для обработки в реальном времени.

Современные оптико-электронные системы наблюдения и прицеливания должны обеспечивать круглосуточную и всепогодную работу. Для решения этой задачи широко применяется совместное использование телевизионного (ТВ) и тепловизионного (ТПВ) каналов. ТВ-канал функционирует в видимом диапазоне спектра и обеспечивает высокую пространственную детализацию изображения, тогда как ТПВ-канал регистрирует тепловое излучение объектов в инфракрасной области и позволяет обнаруживать цели при низкой освещённости, а также в условиях задымления, тумана и облачности.

В докладе рассматривается особенности интеграции ТВ и ТПВ каналов в единый оптико-электронный модуль. Проводится обзор решений ряда технических задач, связанных с оптической компоновкой системы, пространственным совмещением изображений, синхронизацией видеопотоков, учетом особенностей фотоприёмных устройств и обеспечением механической стабильности конструкции.

Основные схемы построения двухканальных систем: схема с раздельными объективами, схема с общим объективом и светоделителем, а также схема со встроенным каналом. Использование раздельных объективов отличается конструктивной простотой и отсутствием потерь светового потока, однако приводит к возникновению параллакса между каналами. Схема с общим объективом и светоделителем обеспечивает совпадение оптических осей и полей зрения каналов, но сопровождается потерями энергии излучения и усложняет коррекцию оптических аберраций в широком спектральном диапазоне.

Пространственное совмещение изображений ТВ и ТПВ каналов осуществляется с использованием проективного преобразования, описываемого матрицей гомографии, связывающей координаты соответствующих точек двух изображений. Оценка параметров гомографии выполняется на основе обнаружения и сопоставления характерных точек изображений.

Тепловизионные каналы, особенно на основе микроболометрических матриц, характеризуются сравнительно низким пространственным разрешением и частотой кадров. Для повышения стабильности и качества изображений применяются методы коррекции неоднородности чувствительности и термоэлектрическая стабилизация фотоприёмной матрицы.

Обработка и синхронизация видеопотоков реализуется на вычислительных платформах FPGA, GPU или системах-на-кристалле и включает захват видеопотоков, приведение изображений к единому масштабу, геометрическую коррекцию и наложение служебной информации.

Таким образом, эффективность двухканальных систем зависит не только от качества сенсоров, но и от глубины их алгоритмической интеграции. Современные вычислительные архитектуры позволяют осуществлять такую обработку в реальном времени и обеспечивают дальнейшее развитие методов комплексной обработки телевизионных и тепловизионных данных.

Список использованных источников:

1. Holst G. Electro-Optical Imaging System Performance / G. Holst. – Winter Park : JCD Publishing, 2017. – 450 p.

2.Rogalski A. Infrared Detectors / A. Rogalski. – 2nd ed. – Boca Raton : CRC Press, 2010. – 876 p.

3.Szeliski R. Computer Vision: Algorithms and Applications / R. Szeliski. – London : Springer, 2010. – 812 p. – (Texts in Computer Science).

4. Ефимов А.И. Алгоритм поэтапного уточнения проективного преобразования для совмещения изображений в многоканальных системах / А.И. Ефимов, А.И. Новиков // Компьютерная оптика. – 2016. – Т. 40, № 4. – С. 512–519.

5. Даниленко В.И. Метод адаптивной фильтрации в задачах обработки многозональных изображений / В.И. Даниленко // Программные системы и вычислительные методы. – Москва : НБ-Медиа, 2016. – № 1. – С. 64–79.

6. Михеев С.В. Основы инфракрасной техники : учеб. пособие / С.В. Михеев. – Санкт-Петербург : Университет ИТМО, 2017. – 128 с.

7. Бадертдинов Э.Р., Денисов И.Г., Козлов А.В. Особенности построения телевизионного канала в совмещенных теплотелевизионных системах / Э. Р. Бадертдинов, И. Г. Денисов, А. В. Козлов // Прикладная физика. – 2015. – № 1. – С. 92–95.

ЧИСЛЕННО-АНАЛИТИЧЕСКИЕ МЕТОДЫ АППРОКСИМАЦИИ ПРИ ИЗУЧЕНИИ СВЧ ХАРАКТЕРИСТИК РАДИОЭЛЕКТРОННЫХ СИСТЕМ

Швец В.С., учреждение образования «Военная академия Республики Беларусь»;
Исаев В.О., канд. техн. наук, оперативно-аналитический центр при Президенте Республики Беларусь;
Бойкачев П.В., доктор техн. наук, доцент, учреждение образования «Военная академия Республики Беларусь»

Аннотация. В работе рассматривается применение численно-аналитических методов аппроксимации при изучении частотных характеристик СВЧ устройств, используемых в радиоэлектронной технике. Предложен подход к построению математических моделей элементов матрицы рассеяния на основе дробно-рациональных функций, позволяющий перейти от дискретных табличных данных к непрерывным аналитическим моделям. Данный метод может быть использован в учебном процессе при подготовке специалистов в области радиолокации, радионавигации и систем связи военного назначения.

Современное состояние радиоэлектронных устройств (РЭУ) характеризуется широким внедрением систем сантиметрового и миллиметрового диапазонов волн. Это относится к бортовым радиолокационным станциям (РЛС), системам государственного опознавания, радиолиниям передачи данных, станциям активных помех и другим специальным системам.

При проектировании СВЧ РЭУ (СВЧ транзисторные усилители, преобразователи и умножители частоты, активные фильтры, антенные устройства и др.) важное значение имеет решение задач широкополосного согласования. При задании параметров рассеивания согласуемых СВЧ устройств в виде численных дискретных зависимостей модуля и аргумента от частоты задача согласования может быть решена исключительно численными методами.

По-иному обстоит дело, когда согласующая цепь находится аналитическими методами. Здесь успех в решении задач согласования напрямую связан с определением адекватных математических моделей (дробно–рациональных функций) согласуемых нагрузок. Таким образом, актуальным является вопрос о нахождении математических моделей СВЧ РЭУ, представленных в численном виде на дискретном ряде частот, которые бы описывали параметры этих устройств с требуемой точностью. Это позволит применять современные аналитические методики широкополосного согласования и послужит толчком для их дальнейшего развития.

Матрица рассеивания четырехполюсников

Для пассивного линейного четырехполюсника (ЧП), включенного в СВЧ тракт с волновым сопротивлением Z_0, можно записать уравнения, определяющие линейную связь между падающими и отраженными волнами на входе и выходе ЧП, в виде:

$$\begin{aligned} U_{\text{отр1}} &= S_{11}U_{\text{пад1}} + S_{12}U_{\text{отр1}}; \\ U_{\text{пад2}} &= S_{21}U_{\text{пад1}} + S_{22}U_{\text{отр2}}. \end{aligned} \quad (1)$$

Матрицу [*S*] называют матрицей рассеяния. Для ЧП эта матрица имеет размер 2×2. Она устанавливает связь между комплексными нормированными амплитудами отраженных и падающих волн в плечах ЧП. В матричной записи уравнения (1) приобретают вид:

$$\begin{bmatrix} U_{\text{отр1}} \\ U_{\text{отр2}} \end{bmatrix} = \begin{bmatrix} S_{11} & S_{12} \\ S_{21} & S_{22} \end{bmatrix} \times \begin{bmatrix} U_{\text{пад1}} \\ U_{\text{пад2}} \end{bmatrix}. \quad (2)$$

Элементы волновой матрицы рассеяния имеют ясный физический смысл и могут быть измерены сравнительно простым способом, в частности с помощью измерительной линии.

При работе СВЧ – четырехполюсника на согласованную нагрузку отраженная волна, на его выходе, отсутствует, а из соотношения (2) следует:

$$S_{11} = \frac{U_{\text{отр1}}}{U_{\text{пад1}}};\ S_{21} = \frac{U_{\text{пад2}}}{U_{\text{пад1}}};$$

где S_{11} – комплексный коэффициент отражения от входа исследуемого ЧП, а S_{21} – комплексный коэффициент передачи ЧП. В общем случае он учитывает как активные потери в четырехполюснике, так и потери на отражение.

Элементы S_{22} и S_{12} имеют аналогичный смысл, но соответствуют обратному включению ЧП (при этом выход ЧП соединяют с генератором, а на вход его включают согласованную нагрузку).

Значения матрицы рассеяния описывают свойства ЧП лишь на заданной частоте. Для представления ЧП в полосе частот элементы матриц рассеяния преобразуются в рациональную функцию вида:

$$f(s) = \frac{a_0 + a_1 s + a_2 (s)^2 + \ldots + a_n (s)^n}{b_0 + b_1 s + b_2 (s)^2 + \ldots + b_m (s)^m} \quad (4)$$

Алгоритм аппроксимации частотных характеристик СВЧ транзисторов, представленных в численном виде, на дискретном ряде частот

Взяв за основу дробно–рациональную функцию (4) с неизвестными коэффициентами при переменной *s* можно максимально точно аппроксимировать заданные в табличном виде модуль и фазу коэффициента отражения S_{11} СВЧ устройства.

Так как рассматриваемые модуль и фаза коэффициента отражения S_{11} являются комплексными, то для поиска функции, максимально точно описывающей транзистор с заданными параметрами, необходимо воспользоваться некоторыми свойствами комплексных чисел.

Как известно, модуль комплексного числа S_{11} можно представить в виде

$$S_{11} = |S_{11}| = \sqrt{A^2 + B^2}, \tag{5}$$

где A – действительная часть S_{11}, а B – мнимая часть. Тогда фаза коэффициента отражения S_{11} равна

$$\varphi = \arctan\frac{A}{B}. \tag{6}$$

Представим функцию (4) через четные и нечетные части ее числителя и знаменателя [1]:

$$f(s) = \frac{P(s)}{Q(s)} = \frac{(m_1 + n_1)}{(m_2 + n_2)}.$$

Умножим $P(s)$ и $Q(s)$ на $(m_2 + n_2) = Q(-s)$:

$$f(s) = \frac{P(s)}{Q(s)} = \frac{(m_1 + n_1)}{(m_2 + n_2)}\frac{m_2 - n_2}{m_2 - n_2} = \frac{(m_1 m_2 - n_1 n_2) + (n_1 m_2 - m_1 n_2)}{m_2^2 - n_2^2},$$

где

$m_1 = a_0 + a_2 s^2 + ... + a_{2n} s^{2n}$ - четная часть числителя функции $f(s)$;

$m_2 = b_0 + b_2 s^2 + ... + b_{2m} s^{2m}$ - четная часть знаменателя функции $f(s)$;

$n_1 = a_1 s + ... + a_{(2n+1)} s^{(2n+1)}$ - нечетная часть числителя функции $f(s)$;

$n_2 = b_1 s + ... + b_{(2m+1)} s^{(2m+1)}$ - нечетная часть знаменателя функции $f(s)$.

С помощью математического преобразования, выражение (4) можно представить в виде четной $Ev\ f(s)$ и нечетной $Od\ f(s)$ части от $f(s)$:

$$Ev\ f(s) = \frac{m_1 m_2 - n_1 n_2}{m_2^2 - n_2^2}; \qquad Od\ f(s) = \frac{n_1 m_2 - m_1 n_2}{m_2^2 - n_2^2};$$

При $s = i\omega$ имеем:

$$Ev\ f(s)\big|_{s=i\omega} = \mathrm{Re}\, f(i\omega); \qquad Od\ f(s)\big|_{s=i\omega} = i\,\mathrm{Im}\, f(i\omega).$$

Полученные выражения $\mathrm{Re}\, f(i\omega)$ и $\mathrm{Im}\, f(i\omega)$ предлагается использовать в качестве аппроксимирующих функций $\mathrm{Re}\, F(s)$ и $\mathrm{Im}\, F(s)$ передаточных и входных характеристик радиотехнических устройств.

Используя численный метод решения задачи приближения и, наложив на выражение (3) ограничения условий физической реализуемости и положительной вещественной функции, изложенные выше, получаем системы неравенств:

$$\begin{cases} |\mathrm{Re}\, F(\omega_{\min}) - \mathrm{Re}\, f(\omega_{\min})| \le \delta; \\ |\mathrm{Re}\, F(\omega_1) - \mathrm{Re}\, f(\omega_1)| \le \delta; \\ ..... \\ |\mathrm{Re}\, F(\omega_{\max}) - \mathrm{Re}\, f(\omega_{\max})| \le \delta. \end{cases} \tag{5}$$

$$\begin{cases} |\mathrm{Im}\, F(\omega_{\min}) - \mathrm{Im}\, f(\omega_{\min})| \le \delta; \\ |\mathrm{Im}\, F(\omega_1) - \mathrm{Im}\, f(\omega_1)| \le \delta; \\ ..... \\ |\mathrm{Im}\, F(\omega_{\max}) - \mathrm{Im}\, f(\omega_{\max})| \le \delta. \end{cases} \tag{6}$$

Где в качестве целевой функции выбран параметр δ, который минимизируется путем подбора коэффициентов a_0, a_1, a_2,... a_n и b_0, b_1, b_2,... b_m.

Список использованных источников:

1. *Карни, Ш., Теория цепей. Анализ и синтез. – М. «Связь», 1973. – 269с.*
2. *Белецкий, А.Ф. Теория линейных электрических цепей / А.Ф. Белецкий. – М.: Радио и связь, 1986. – 544.*

ИССЛЕДОВАТЕЛЬСКИЙ ПРОГРАММНЫЙ КОМПЛЕКС НА БАЗЕ UNITY ДЛЯ ОПРЕДЕЛЕНИЯ УЯЗВИМОСТЕЙ В БОЕВЫХ ПОРЯДКАХ ФОРМИРОВАНИЙ ПВО ПРИ ПРОТИВОДЕЙСТВИИ УДАРНЫМ БЕСПИЛОТНЫМ ЛЕТАТЕЛЬНЫМ АППАРАТАМ

Пальцев В.А.

Военная Академия Республики Беларусь г. Минск, Республика Беларусь

Шарак Д.С. – канд. техн. наук, доцент

Аннотация. В докладе рассматривается исследовательский программный комплекс на базе UNITY позволяющий определять уязвимости в боевых порядках формирований противовоздушной обороны. Приведены его отличия от существующих.

Вооруженные конфликты последних лет, а также происходящие в настоящее время, показали, что применение ударных беспилотных летательных аппаратов (БЛА) в противовоздушном бою становится одним из важных факторов оперативно-тактической обстановки, который должен в полной мере учитываться при автоматизации процесса оценки противника в комплексах средств автоматизации (КСА) управления формированиями противовоздушной обороны (ПВО) тактического уровня. Поэтому необходимо прогнозировать маршруты подлета не только пилотируемой авиации и крылатых ракет, но и ударных БЛА. Эта задача формализуется в виде задачи нахождения кратчайшего пути в графе, который построен на основе представления зоны действия БЛА в трехмерном виде и использовании координатной сетки. Веса вершин графа рассчитываются с учетом их попадания в области противодействия средств ПВО и радиоэлектронной борьбы (РЭБ) [1].

В докладе рассматривается исследовательский программный комплекс на базе UNITY позволяющий в трехмерном виде моделировать произвольный рельеф местности и зоны противодействия БЛА, задавать типы, способы применения и профили полета БЛА, формировать граф и рассчитывать веса его вершин, а также рассчитать кратчайший маршрут в соответствии с выбранным алгоритмом (модифицированные алгоритмы Дейкстры и A-star) и визуализировать его.

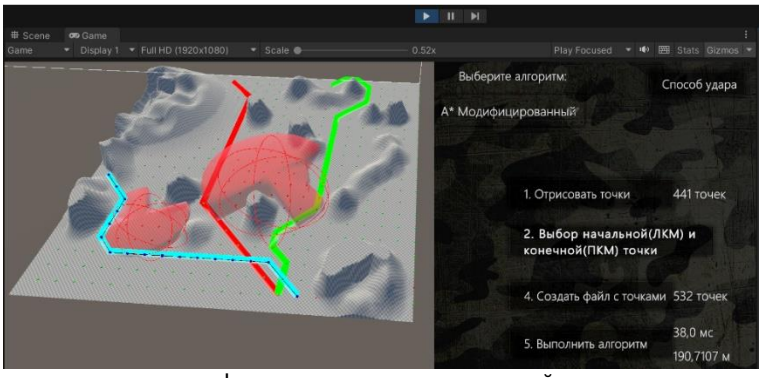

Рисунок 1 – Вид сформированных на рельефе местности зон противодействия, вершин графа и маршрутов

Отличия предлагаемого исследовательского программного комплекса для формирования маршрутов подлета ударных БЛА к объектам удара от существующих заключаются в следующем:

– используются реализуемые зоны обнаружения, поражения (а не зоны огня) и подавления РЭБ;

– используются разработанные модифицированные алгоритмы поиска кратчайшего пути в графе, в котором вес перехода в рассматриваемый узел координатной сетки может меняться в зависимости от пространственного направления перехода в него из соседних узлов;

– предусматриваются различные варианты реализации способов прорыва и преодоления системы ПВО, а также формирование параметров узлов сетки под соответствующий вариант.

Предлагаемый исследовательский программный комплекс может быть использован для разработки (совершенствования) специального математического обеспечения КСА управления формированиями ПВО, радиотехнических войск и РЭБ при решении задач прогнозирования действий воздушного противника, формирования исходной информации (ожидаемые маршруты ударных БЛА) для моделирования боевых действий этих формирований, а также определения эффективных боевых порядков.

Список использованных источников:

1. *Пальцев, В. А. Подход к решению задачи прогнозирования маршрутов полета беспилотных летательных аппаратов в комплексах средств автоматизации органов управления подразделениями противовоздушной обороны / В. А. Пальцев, А. А. Посудевский, Д. С. Шарак // Вестн. Воен. Акад. Респ. Беларусь. – 2024. – № 3 (84). – С. 75–82.*

ГЕНЕРАЦИЯ КРИПТОГРАФИЧЕСКИ СТОЙКОЙ ПСЕВДОСЛУЧАЙНОЙ ПОСЛЕДОВАТЕЛЬНОСТИ ДЛЯ АЛГОРИТМА ПСЕВДОСЛУЧАЙНОЙ ПЕРЕСТРОЙКИ РАБОЧЕЙ ЧАСТОТЫ В СИСТЕМАХ ЗАЩИТЫ КАНАЛА СВЯЗИ С БЕСПИЛОТНЫМ ЛЕТАТЕЛЬНЫМ АППАРАТОМ

Мойсюк-Дранько Я.А.

Национальный детский технопарк г. Минск, Республика Беларусь

Дубовик И.А. – канд. техн. наук

Аннотация. В работе рассматривается проблема обеспечения защищённости радиоканала беспилотных летательных аппаратов посредством алгоритма псевдослучайной перестройки рабочей частоты (ППРЧ). Проведён сравнительный анализ генераторов псевдослучайных последовательностей: линейного конгруэнтного генератора, Mersenne Twister, XorShift и перемешанного конгруэнтного генератора (PCG) — по критериям периода, скорости генерации, прохождения статистических тестов BigCrush и наличия структурных паттернов в выходной последовательности. Замер вычислительной эффективности произведён на микроконтроллере ESP32-S3. Описан механизм формирования затравки генератора на пульте радиоуправления и её передачи на полётный контроллер посредством синхронизационного пакета. Показано, что PCG обеспечивает наилучшее сочетание статистической стойкости, периода генерации и вычислительной эффективности для применения в бортовых системах реального времени.

Современные беспилотные летательные аппараты функционируют в условиях интенсивного радиоэлектронного противодействия, что требует применения методов защиты радиоканала управления. Одним из ключевых является псевдослучайная перестройка рабочей частоты (ППРЧ, FHSS), при которой несущая частота изменяется по псевдослучайному закону, известному лишь легитимным участникам связи [1]. Качество алгоритма ППРЧ непосредственно определяется свойствами генератора псевдослучайной последовательности (ГПСП): он должен обеспечивать максимальный период, равномерное распределение, непредсказуемость выходных значений без знания внутреннего состояния и низкую вычислительную сложность.

Линейный конгруэнтный генератор (LCG) вычисляет последовательность по рекуррентному соотношению:

$$X_{n+1} = (a \cdot X_n + c)\ mod\ m \quad (1),$$

Алгоритм отличается простотой и высокой скоростью, однако имеет критический недостаток: младшие биты выходной последовательности обладают существенно меньшим периодом, а внутреннее состояние тривиально восстанавливается по нескольким наблюдаемым значениям [2], что делает LCG непригодным для криптографических применений.

Генератор Mersenne Twister (MT19937) основан на линейном регистре сдвига с обратной связью и обеспечивает период $2^{19937}-1$ [3]. Он проходит большинство стандартных статистических тестов, однако знание 624 последовательных 32-битных выходов позволяет полностью восстановить внутреннее состояние и предсказать всю дальнейшую последовательность [4]. Это является неприемлемым для задач защиты радиоканала.

Генератор XorShift основан на последовательном применении операций XOR и побитового сдвига к внутреннему состоянию:

$$X_{n+1} = X_n \oplus (X_n \ll a) \oplus (X_n \gg b) \quad (2),$$

где a и b — константы сдвига, подобранные для обеспечения максимального периода.

Генератор отличается исключительной простотой реализации и высокой скоростью работы, так как использует только операции, нативные для большинства процессорных архитектур. Тем не менее базовый XorShift не проходит ряд тестов пакета BigCrush, а его выходная последовательность уязвима к линейному криптоанализу [5]. Расширенные варианты — XorShift128+ и XorShift1024* — частично устраняют статистические недостатки, однако не решают проблему криптографической стойкости.

Перемешанный конгруэнтный генератор (PCG) устраняет указанные недостатки. Внутреннее состояние обновляется по схеме LCG, к которой затем применяются операции «перемешивания» (permutations/mixing) для маскировки линейных закономерностей [6]. Выходное значение формируется функцией пермутации PCG-XSH-RR, которая применяет операции XOR-сдвига и циклического сдвига для маскировки линейных закономерностей внутреннего состояния:

Для оценки вычислительной эффективности рассматриваемых алгоритмов был разработан тестовая программа, реализующая последовательную генерацию 10^6 псевдослучайных чисел для каждого из генераторов. Замер времени выполнения производился на микроконтроллере ESP32-S3 с тактовой частотой 240 МГц, представляющем типичную аппаратную платформу для бортовых систем управления БЛА. Результаты измерений подтвердили, что PCG и XorShift демонстрируют сопоставимую скорость генерации, существенно превосходя Mersenne Twister ввиду значительно меньшего размера внутреннего состояния и отсутствия операций с большими массивами данных. Исход сравнения приведён в таблице 1.

Таблица 1 – Сравнение генераторов псевдослучайных последовательностей

Характеристика	LCG	Mersenne Twister	XorShift	PCG
Период	2^{64}	2^{19937}-1	2^{64}-1	2^{64}
Скорость генерации (чисел/секунду)	7.949.125	2.977.431	7.951.021	4.467.077
Прохождение тестов BigCrush	нет	частично	частично	да
Обнаружение паттерна	да	нет	да	нет

В алгоритме ППРЧ текущая частота на k интервале определяется как:

$$f_k = f_{min} + (PCG(S_k) \bmod N) \cdot \Delta f \quad (3),$$

где N — число рабочих частот, $f_{\min}$ — минимальная частота сетки, Δf — шаг.

Для обнаружения паттернов возникаемых у отражает результат визуального и автокорреляционного анализа выходной последовательности: для каждого генератора строилась двумерная диаграмма рассеяния пар последовательных значений (X_n, X_{n+1}), на которой структурные закономерности проявляются в виде выраженных линий или плоскостей — так называемая гиперплоскостная структура, характерная для генераторов с линейным внутренним преобразованием. У LCG и XorShift такие паттерны были визуально обнаружены, что соответствует теореме Марсальи. PCG и Mersenne Twister паттернов в двумерной проекции не обнаружили, однако MT уязвим к восстановлению состояния, тогда как PCG устойчив как к визуальному, так и к алгебраическому анализу.

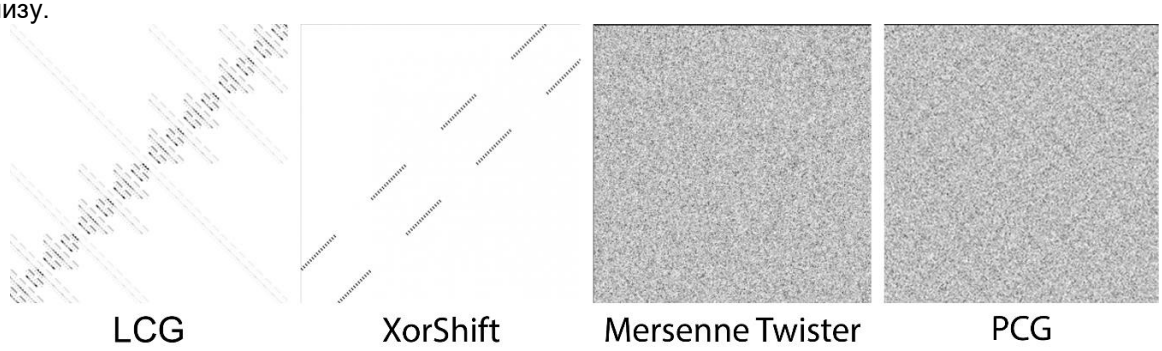

Рисунок 1 – Диаграммы обнаружения паттернов генераторов псевдослучайных чисел

На пульте радиоуправления начальное значение генератора (seed, затравка) формируется путём объединения секретного ключа K, прошитого в оба устройства на этапе производства, с текущей временной меткой T и одноразовым числом N_{once}, генерируемым при каждом включении:

$$S_0 = H(K \mid T \mid N_{once}) \quad (4),$$

где H — криптографическая хэш-функция. Сформированная затравка передаётся на полётный контроллер в составе синхронизационного пакета по защищённому каналу до начала сеанса связи, после чего оба устройства независимо инициализируют генератор PCG одним и тем же значением S_0 и воспроизводят идентичную псевдослучайную последовательность частот. Поскольку состояние генератора детерминировано начальным значением, пульт и полётный контроллер в каждый момент времени переходят на одну и ту же частоту синхронно, не обмениваясь дополнительными данными в ходе полёта; перехват синхронизационного пакета без знания ключа K не позволяет противнику восстановить затравку ввиду односторонности хэш-функции.

Таким образом, XorShift превосходит LCG по качеству выходной последовательности и сопоставим с ним по скорости, однако уязвим к алгебраическим атакам ввиду линейной структуры преобразования. PCG превосходит все рассмотренные алгоритмы по совокупности криптографических и вычислительных характеристик, что делает его оптимальным выбором в качестве ядра генератора ПСП для систем ППРЧ беспилотных летательных аппаратов.

Список использованных источников

1. Скляр, Б. Цифровая связь. Теоретические основы и практическое применение / Б. Скляр. — 2-е изд. — М. : Вильямс, 2007. — 1104 с.

2. Кнут, Д. Э. Искусство программирования. Т. 2 : Получисленные алгоритмы / Д. Э. Кнут. — 3-е изд. — М. : Вильямс, 2007. — 832 с.

3. Matsumoto, M. Mersenne Twister: A 623-dimensionally equidistributed uniform pseudo-random number generator / M. Matsumoto, T. Nishimura // ACM Transactions on Modeling and Computer Simulation. — 1998. — Vol. 8, № 1. — P. 3–30.

4. Шахтарин, Б. И. Генераторы псевдослучайных сигналов / Б. И. Шахтарин, В. А. Ковригин. — М. : Горячая линия–Телеком, 2010. — 192 с.

5. Marsaglia, G. Xorshift RNGs / G. Marsaglia // Journal of Statistical Software. — 2003. — Vol. 8, № 14. — P. 1–6.

6. O'Neill, M. E. PCG: A Family of Simple Fast Space-Efficient Statistically Good Algorithms for Random Number Generation / M. E. O'Neill // Harvey Mudd College Technical Report. — 2014. — HMC-CS-2014-0905. — 65 p.

НАХОЖДЕНИЕ АППРОКСИМИРУЮЩИХ ФУНКЦИЙ ЧИСЛЕННЫМ МЕТОДОМ ДЛЯ УВЕЛИЧЕНИЯ РАВНОМЕРНОСТИ ФАЗАЧАСТОТНОЙ ХАРАКТЕРИСТИКИ ШИРОКОПОЛОСНЫХ СОГЛАСУЮЩИХ УСТРОЙСТВ И ФИЛЬТРОВ

Полещук М.И.

Военная академия Республики Беларусь г. Минск, Республика Беларусь

Бойкачев П.В. – доктор техн. наук, доцент

Аннотация. Показана возможность снижения фазовых искажений спектров сигналов во входных трактах на этапе аппроксимации.

Заметный прогресс в технологиях спутниковой и мобильной систем телекоммуникации, а также в радиолокационных системах, в значительной степени связан с применением широкополосных и сверхширокополосных сигналов. Для обработки таких сигналов, к входным трактам радиоприемных устройств предъявляются некоторые требования (например, избирательность и внесение минимальных искажений амплитудного и фазового спектров сигнала). В традиционной схемотехнике неискажающее устройством – устройство, которое имеет равномерную амплитудно-частотную характеристику. Однако стоит отметить, что неравномерность фазочастотной характеристики (ФЧХ) может оказать более серьезные проблемы на этапе обработки сигналов.

Для обеспечения вышеизложенных требований в последние годы стали применять фильтры с модифицированными функциями (МФ) передачи [1, 2]. В сравнении с классическими аппроксимирующими функциями (АФ), модифицированные функции передачи имеют следующие недостатки:

− большая неравномерность в полосе фильтрации;
− меньшее затухание в полосе заграждения;
− отсутствие свойства квадратной симметрии;
− большая нелинейность ФЧХ [**Ошибка! Источник ссылки не найден.**].

Предлагается находить АФ численным методом. Следовательно, аналитическое выражение для прототипа функции передачи (ФП) имеет следующий вид:

$$K_m\left(-s^2\right)=\frac{a_0+a_1s+a_2s^2+\ldots+a_ns^n}{b_0+b_1s+b_2s^2+\ldots+b_ms^m}, \quad (1)$$

где $K_m\left(-s^2\right)$ – АФ описывающая функцию передачи мощности в синтезируемых цепях; $s=\sigma+j\omega$ – комплексная частота; a_0 – коэффициенты числителя полинома аппроксимирующей функции, b_0 – коэффициенты знаменателя полинома аппроксимирующей функции, n − порядок числителя (число вещественных частот, на которых функция принимает нулевое значение; m − порядок знаменателя.

Аппроксимирующая функция (1) отличается от классической функции тем, что, определенным образом, в нее добавляются нули передачи (числитель выражения (1)). Данные нули образованы комплексно-сопряженными парами, расположенными на комплексной плоскости *s*-переменной. Корни числителя и знаменателя (1) должны подчиняться квадрантной симметрии, благодаря чему коэффициенты полинома Гурвица будут являться действительными. В этом случае цепи согласования и фильтрации, с выбранной ФП, будут иметь физическую реализуемость.

В работах [3, 4] нули передачи МФ располагаются только на мнимой оси комплексной плоскости *s*-переменной, что обеспечивает максимальный уровень спада и равномерность в полосе согласования и фильтрации амплитудно-частотной характеристики, но ухудшает линейность фазочастотной характеристики. Для коррекции фазы, а именно улучшения ее линейности в полосе согласования и фильтрации предлагается модифицировать классические АФ таким образом, чтобы нули образовывали комплексно-сопряженную четверку на всей *s*- плоскости, а не только на мнимой оси.

Линейность фазочастотной характеристики нагляднее описывает групповое время запаздывания (ГВЗ). Чем больше величина разброса ГВЗ между минимальным и максимальным значением, тем нелинейность фазы больше. На рисунке 1 приведена зависимость разброса ГВЗ от расположения нулей функции передачи для МФ Чебышева пятого порядка.

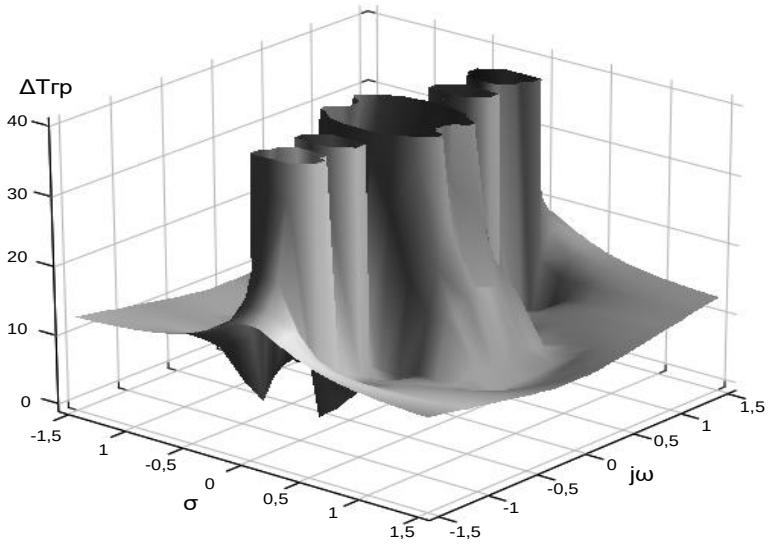

Рисунок 1 – Зависимость разброса ГВЗ от расположения нулей ФП для МФ Чебышева пятого порядка

Зависимость разброса ГВЗ от расположения нулей ФП для МФ Чебышева пятого порядка, представленная на рисунке 1, позволяет определить область расположения вводимых нулей передачи, в которой разброс ГВЗ минимальный. Видимая на рисунке пара нулей расположена в районе σ=±0,035 и jω= ±0,96.

На рисунке 2 представлена зависимость коэффициента передачи по мощности (*а*) и ГВЗ (*б*) от частоты функции (1) (сплошная линия), в сравнении с классической функцией Чебышева пятого порядка (пунктирная линия), для одинаковых начальных условий.

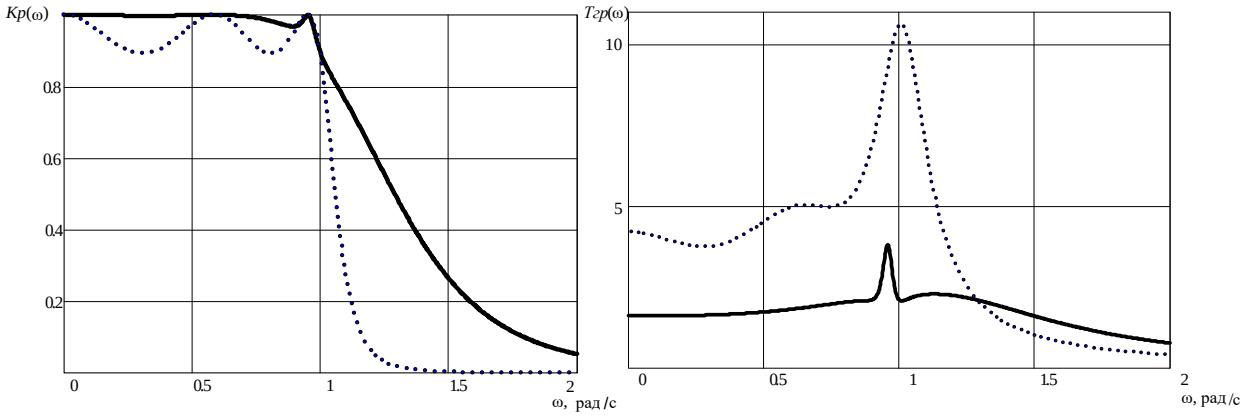

Рисунок 2 – Коэффициент передачи по мощности (а) и ГВЗ (б) от частоты функции (1) пятого порядка (сплошная линия) в сравнении с классической функцией Чебышева пятого порядка (пунктирная линия)

Анализ приведенных зависимостей показывает, что функция (1) уступает классической функции передачи в избирательности, но имеет большую равномерность в полосе фильтрации (согласования) коэффициента передачи и более равномерное и меньшее ГВЗ.

Следует отметить, что функция (1) может использоваться для конструирования широкого класса полиномиальных фильтров и широкополосных согласующих цепей по различным критериям, таким как минимизация искажения сигнала, как по фазе, так и по амплитуде, минимизация чувствительности на тот или иной элемент схемы, минимизация вероятности ошибки приема сигнала.

Список использованных источников:

1. *Cameron, R. J. Advanced Filter Synthesis / R. J. Cameron // Microwave magazine IEEE. – 2011. –Vol. 12. – P. 42–43.*
2. *Cameron, R. J. Generation of Transfer and Reflection Polynomials / R. J. Cameron // Microwave magazine IEEE– 2011. – Vol. 12. – P. 46–47.*
3. *Бойкачев П.В., Филиппович Г.А., Метод модификации аппроксимирующих функций для синтеза фильтров и согласующих цепей / «Вестник» ВАРБ. – №3(36). – 2012.*
4. *Бойкачев П.В., Филиппович Г.А. Широкополосный синтез согласующих устройств на основе модифицированной аппроксимации функции передачи / «Вестник БелГУТ». – №2(25). – 2013.*

СИСТЕМА РАСПОЗНАВАНИЯ НАЗЕМНЫХ ОБЪЕКТОВ ДЛЯ БПЛА НА ОСНОВЕ НЕЙРОННОЙ СЕТИ YOLOv8m

Горев Е.В

Учреждение образования «Национальный детский технопарк»

Дубовик И.А кандидат технических наук, доцент

Аннотация. Разработана система автоматического обнаружения и классификации наземных и воздушных объектов по видеопотоку с БПЛА на базе нейронной сети YOLOv8m. Система обеспечивает распознавание 13 классов объектов с mAP@0.5 = 0,901 в реальном времени при задержке 97–183 мс и скорости 18–22 кадра/с.

Современные БПЛА широко применяются в задачах разведки, мониторинга территорий и охраны объектов. Ключевым компонентом таких систем является модуль автоматического распознавания объектов, позволяющий идентифицировать цели без участия оператора. Существующие системы ограничены 5–10 классами и не обеспечивают mAP выше 0,88 при работе в реальном времени [1, 2, 3]. Двухпроходные детекторы (Faster R-CNN, Mask R-CNN) точны, однако не соответствуют требованиям реального времени; лёгкие архитектуры для встроенных платформ быстры, но существенно уступают по точности. Задача одновременного достижения широкого охвата классов, высокой точности и малой задержки остаётся актуальной.

Разработанная система распознаёт 13 классов: наземную технику (легковые автомобили, бронетехника, артиллерия), личный состав, стрелковое оружие, суда, авиатехнику (самолёты, вертолёты, БПЛА), объекты инфраструктуры. Для обучения сформирован датасет из 104503 аэро и сухопутных снимков на основе открытых коллекций VisDrone 2021, DOTA v2.0, MO-UAV и собственной аэросъёмки с высот 50–500 м при различных условиях освещения. Разметка выполнялась двумя операторами с перекрёстной верификацией. Применялись аугментации Mosaic, случайные геометрические трансформации и изменение яркостных характеристик изображений.

Система построена на основе YOLOv8m — anchor-free однопроходного детектора с backbone CSPDarknet и агрегацией признаков PANet на трёх масштабных уровнях (128×128, 64×64, 32×32) [4]. Количество параметров модели составляет 25,9 млн. Обучение проводилось с применением оптимизатора AdamW на предобученных весах COCO 2017 в течение 200 эпох (ранняя остановка). Наилучший результат достигнут на 106-й эпохе: Precision = 0,900, Recall = 0,851, mAP@0.5 = 0,901 при скорости 18–22 кадра/с и разрешении 1024×1024 пикс. [4, 5]. Подробные результаты по классам приведены в таблице 1.

Таблица 1 — Результаты распознавания по основным классам

Класс объекта	Precision	Recall	mAP@0.5
Бронетехника	0,912	0,876	0,908
Авиатехника	0,920	0,871	0,911
Человек	0,867	0,812	0,856
Оружие	0,823	0,764	0,814
Наземные сооружения	0,879	0,828	0,869
Среднее по всем	0,900	0,851	0,901

Система реализована в виде веб-приложения на основе Flask: видеосигнал с БПЛА принимается по протоколу RTSP/UDP, обрабатывается нейронной сетью и транслируется оператору в формате MJPEG. Суммарная задержка обработки кадра составляет 97–183 мс (инференс 45–82 мс, постобработка NMS 8–15 мс, передача 32–68 мс), что соответствует требованию реального времени. Интерфейс позволяет настраивать пороги уверенности, выбирать отображаемые классы и вести запись аннотированного видеопотока. В сравнении с аналогами (MO-UAV: mAP = 0,831, 7 классов; DOTA YOLOv5: mAP = 0,758) разработанная система обеспечивает наилучшее сочетание точности, охвата классов и задержки обработки [3, 4].

Таким образом, разработанная система на основе YOLOv8m обеспечивает распознавание 13 классов объектов с mAP@0.5 = 0,901 при задержке 97–183 мс, превосходя существующие аналоги по совокупности показателей. Дальнейшее развитие планируется в направлениях: интеграция алгоритмов трекинга (ByteTrack), адаптация модели под бортовые вычислительные модули NVIDIA Jetson Orin, а также расширение датасета за счёт синтетических данных Unreal Engine.

Список использованных источников:

1. Zhu P. et al. Detection and Tracking Meet Drones Challenge // IEEE TPAMI. — 2021. — Vol. 44, No. 11. — P. 7380–7399.
2. Xia G.-S. et al. DOTA: A Large-Scale Dataset for Object Detection in Aerial Images // CVPR. — 2018. — P. 3974–3983.
3. Mandal M. et al. MO-UAV: Multi-Object Detection in UAV Images // SPCOM. — 2021.
4. Jocher G. et al. Ultralytics YOLOv8. — 2023. — DOI: 10.5281/zenodo.8347048.
5. Loshchilov I., Hutter F. Decoupled Weight Decay Regularization // ICLR. — 2019.

МЕТОДИКА ОБОСНОВАНИЯ ТЕХНИЧЕСКИХ ТРЕБОВАНИЙ К КООРДИНАТНОМУ БЛОКУ ЦЕЛИ ИСТРЕБИТЕЛЬНОГО БЕСПИЛОТНОГО ЛЕТАТЕЛЬНОГО АППАРАТА

Шорец-Пашковский В.В., Мороз А.Н., Бухтиаров Д.В.

Военная академия Республики Беларусь г. Минск, Республика Беларусь

Мороз А.Н. – канд. техн. наук, доцент

Аннотация. В докладе описана методика, позволяющая предъявить требования к величине поля зрения и дальности обнаружения пассивного оптического бортового координатного блока цели истребительного беспилотного летательного аппарата, при получении целеуказания с наземного технического средства разведки. Задача решена применительно к средствам радиолокационной разведки ЗРК «Тор-М2».

Низкая эффективность использования «классических» средств борьбы с МБПЛА приводит к необходимости поиска новых эффективных и совершенствования существующих средств борьбы с ними. В качестве новых средств борьбы с МБПЛА можно выделить комплексы лазерного и СВЧ воздействия, шрапнельные боеприпасы к стрелковому оружию и зенитным артиллерийским комплексам, а также истребительные БПЛА (ИБПЛА).

Задачей ИБПЛА является поражение воздушной цели. ИБПЛА имеет на своем борту оптический пассивный КБЦ. Информацию о координатах и параметрах движения цели ИБПЛА получает от наземного измерительного устройства, в качестве которого используются станция обнаружения целей и станция наведения ЗРК «Тор-М2». Задача состоит в определении технических характеристик (величина поля зрения и соответствующая этому значению дальность обнаружения конкретной цели с заданными габаритами), которые позволят решить задачу прицеливания и обнаружения бортовым КБЦ ИБПЛА с заданной вероятностью без последующего допоиска. Считается, что бортовой КБЦ может осуществлять слежение за целью только по угловым координатам.

Рассмотрим решение задачи в вертикальной плоскости земной системы координат (рисунок 1).

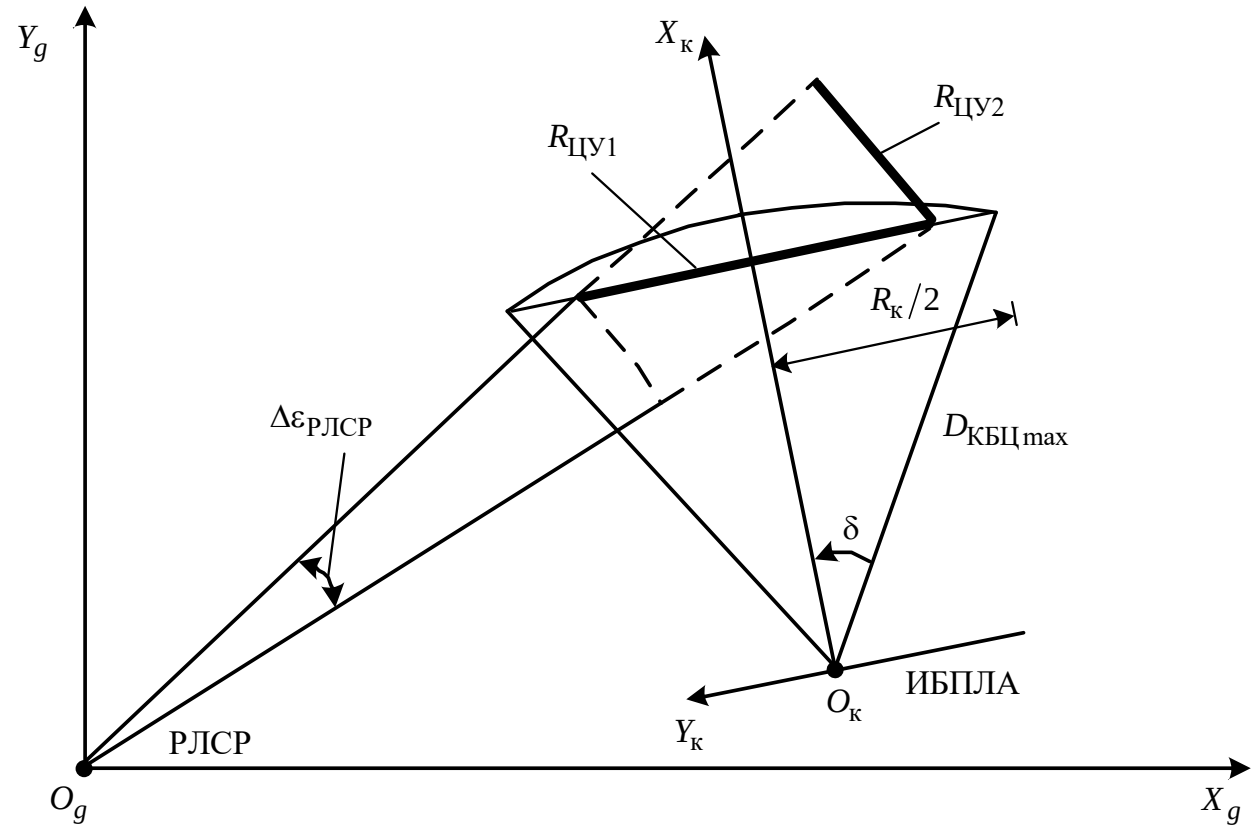

Рисунок 1 – Соотношение угла поля зрения и дальности обнаружение КБЦ ИБПЛА с формой и максимальным габаритным размером строба ЦУ

Алгоритм методики обоснования технических требований представлен на рисунке 2.

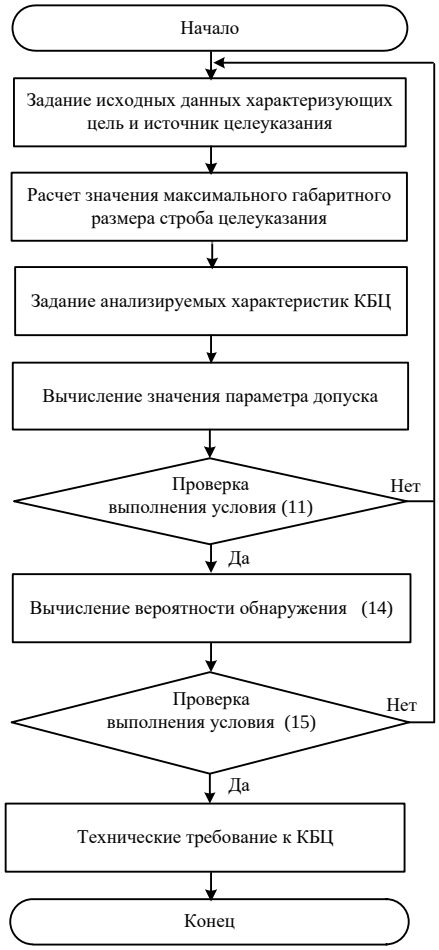

Рисунок 2 –Алгоритм методики обоснования технических требований к КБЦ ИБПЛА

Используя данную методику получены дальность обнаружения и угол поля зрения КБЦ ИБПЛА (таблица 1). Задача решена применительно к видеокамере 2Мп M-920V2.

Таблица 1 – Технические характеристики КБЦ и граничные значения параметра допуска

Тип источника ЦУ	Величина максимального габарита ЦУ, м	Величина параметра допуска, $P_{ДОП}$, м	Дальность обнаружения КБЦ $D_{КБЦ\ max}$, м	Угол поля зрения КБЦ δ , град
СН ЗРК ТОР М2	161	550	900	21,5

Список использованных источников:

1. Thermal behavior of the YAG precursor prepared by sol–gel combustion process / F. Qiu [et al.] // Ceramics International, 2005. – P. 663-665.

2. Третьяков, Ю.Д. Введение в химию твердофазных материалов : учеб. пособие / Ю.Д. Третьяков, В.И. Путляев. – М. : Изд-во Моск. ун-та : Наука, 2006. – 400 с.

3. Цитраты алюминия (III) / В.В. Чевела [и др.] // Ученые записки казанского университета: Естественные науки, 2011. – С.61-69 .

3. Обоснование облика модульной системы противодействия малогабаритным беспилотным летательным аппаратам (шифр «Дербник - 2022»): отчет о НИР / Воен. акад. Респ. Беларусь; рук. темы А.С. Солонар. – Минск.

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

5. Косачев, И.М. Перспективы создания зенитного ракетного комплекса ближнего действия пятого поколения / И.М. Косачев, К.Н. Чугай // Наука и военная безопасность. – 2021. – № 1 (67). – С. 2–6.

6. Мороз, А.Н. Требование к точности информации целеуказания с борта воздушного носителя для прицеливания наземных измерительных устройств зенитного ракетного комплекса / А. Н. Мороз, С. А. Шабан // Сб. науч. ст. Воен. акад. Респ. Беларусь. – 2011. – № 20. – С. 57–62.

7. Драгун, В.Р. Пособие по изучению правил стрельбы на зенитном ракетном комплексе 9К331МК / В.Р. Драгун [и др.]. - Минск: Командование ВВС и войск ПВО, 2018. 183 с.

8.Охрименко, А.Е. Основы радиолокации. Часть I. / А.Е. Охрименко [и др.]. - Москва: Министерство обороны СССР, 1983. 285 с.

ВЗАИМОДЕЙСТВИЕ ТАНКОВЫХ ПОДРАЗДЕЛЕНИЙ С ГРУППАМИ ОПЕРАТОРОВ БПЛА ПРИ ВЕДЕНИИ ОГНЯ С ЗАКРЫТЫХ ОГНЕВЫХ ПОЗИЦИЙ: СОВРЕМЕННОЕ СОСТОЯНИЕ И ПЕРСПЕКТИВЫ РАЗВИТИЯ

Павелко В.С., Кулешова В.Р.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Ли А.Е. – магистр управления

Аннотация. В статье рассматривается способ боевого применения танковых подразделений в условиях массового использования беспилотных летательных аппаратов.

Современный общевойсковой бой характеризуется высокой динамичностью и насыщенностью применения высокоточных средств поражения. Опыт последних конфликтов, особенно Специальной военной операции, свидетельствует о том, что танк, традиционно считавшийся «королем полей», утратил свою былую неуязвимость в связи с массовым применением FPV-дронов и барражирующих боеприпасов.

Как отмечается в аналитическом обзоре, посвященном деятельности Центра «Рубикон», «танк в условиях господства ударных беспилотников стремительно теряет свое значение».

Статистические данные, приведенные в открытых источниках, подтверждают данное утверждение. Так, по данным объективного контроля до 77 % уничтоженных танков приходится на долю ударных беспилотных летательных аппаратов (далее – БЛА).

В этих условиях выживаемость танковых подразделений напрямую зависит от их способности вести огонь, не входя в зону прямого поражения высокоточным оружием и дронами-камикадзе противника [1].

С учетом этого актуальным является возвращение к практике применения танков как орудия поддержки с закрытых огневых позиций (далее - ЗОП), что стало вынужденной, но оправданной мерой. В данных условиях танк способен вести огонь осколочно-фугасными снарядами на дистанции до 9–10 км, работая из-за укрытий и складок местности [2]. Следует отметить, что данный подход не является основным способом применения танков в ходе огневого поражения. Однако, с учетом складывающейся обстановки, в интересах минимизации потерь, указанный способ применения является наиболее обоснованным [3].

Суть тактики заключается в отказе от выхода на прямую наводку там, где это не обусловлено сиюминутной необходимостью прорыва обороны. В этом случае применение танковых подразделений (танков) осуществляется при поддержке БПЛА ведением огня с закрытых позиций с большой дистанции, но «предельно точно», разбирая укрепления противника «до основания».

В ряде источников приводится метод «танковых качелей», суть которого заключатся в том, что пара танков выходит на указанный огневой рубеж, осуществляет огневое поражение по указанным целям, «уходит» на перезарядку и смену направления. В этом случае противник не успевает прицелиться. При таком способе применения одна машина накрывает сектор огнем из глубины, вторая работает на переднем крае, при этом корректировка ведется исключительно операторами БПЛА.

Следует обратить внимание, что при этом существенно возрастает роль групп операторов БПЛА, осуществляющих наводку и корректировку огня танков. По сути происходит интеграция в тактическое звено «танк (танковая пара) – расчет БПЛА».

Ключевым элементом указанного тактического звена является сокращение времени цикла управления огнем. Если ранее информация от разведывательного органа до танкистов проходила длинную «цепочку системы управления», то сейчас ситуация изменилась коренным образом: информация поступает от расчета БПЛА напрямую танковому подразделению. [4]

Это подтверждается военным экспертом Ю.Ляминым, который в интервью газете «Известия» подчеркивает, что «Информация танкистам будет поступать непосредственно от операторов БПЛА. Раньше частенько эта цепочка была длиннее. Теперь цели будут уничтожаться практически тут же». Это становится возможным благодаря техническому оснащению: «Картинка с беспилотника

поступает на планшеты командиров танковых взводов. И танковые экипажи в реальном времени могут видеть результаты своей боевой работы с «полупрямой наводки» [4].

С учетом возрастания роли расчетов операторов БПЛА функции оператора в интересах обеспечения информацией танков для ведения огня с ЗОП включают в себя:

- поиск и идентификацию целей – обнаружение замаскированных опорных пунктов, бронетехники в «лесах» и лесополосах;
- целеуказание и пристрелка – выдача точных координат танковым подразделениям в интересах огневого поражения и переноса огня в случае необходимости;
- корректировка и оценка поражения – объективный контроль результатов стрельбы для немедленного переноса огня или прекращения обстрела [4].

Работа танков с ЗОП в связке с БПЛА требует не просто высокого взаимодействия, но и их слаженности. Командир танка получает на планшет данные о цели и наносит огневое поражение с закрытой позиции.

После выполнения огневой задачи, принципиально важным, является немедленная смена огневой позиции в целях исключения ответного огня артиллерии противника или атаки дронами-камикадзе».

Сокращение времени нахождения боевых машин на позиции напрямую зависит от полученных разведывательных данных и корректировки огня расчетами БПЛА и влияет на эффективность их применения и живучесть в ходе ведения боевых действий.

Для защиты от контрбатарейной борьбы и вражеских FPV-дронов применяются комплексы радиоэлектронной борьбыи «антидроновые козырьки». При этом, операторы БПЛА выполняют функцию воздушного прикрытия, предупреждая танкистов о появлении угроз воздушного нападения.

Следует обратить внимание, что тактика совместного применения танковых подразделений и расчетов БПЛА привела к изменению организационно-штатной структуры. Так в 2025–2026 годах в Вооруженных Силах Российской Федерации начался процесс включения в состав танковых батальонов штатных рот БПЛА [5].

Принятое решение по сути исключает эпизодическое приданное усиление танковых подразделений расчетами БПЛА и переход к штатной интеграции. Речь идет о повышении эффективности применения в бою за счет слаженности их работы в период подготовки к боевому применению.

Анализ применения танковых подразделений в современных конфликтах позволяет сделать следующие выводы:

- стрельба с закрытых огневых позиций перестала быть вспомогательной функцией танка, став основным способом его применения в интересах огневого поражения, а также возможностью по сохранению живучести на поле боя, насыщенном FPV-дронами;
- эффективность огня танков с ЗОП находится в прямой зависимости от качества работы операторов БПЛА, действующих в едином информационном контуре за счет передачи необходимых данных в интересах огневого поражения;
- совместное применение танковых подразделений и расчетов БПЛА приводит к существенному сокращению цикла управления и эффективности их применения. Это в итоге привело к необходимости изменений организационно-штатной структуры танковых подразделений (батальонов) и включения в штат расчетов БПЛА. Данный подход позволил перейти от взаимодействия в ходе ведения боевых действий к совместному применению, обеспечивая тактическую самостоятельность подразделений.

В заключение хотелось бы отметить, что применение танковых подразделений совместно с расчетами БПЛА при решении задачи по ведению огня с закрытых огневых позиций становится не просто выходом их сложившейся ситуации, а тактической инновацией, оказывающей существенное влияние на эффективность ведения боевых действий.

Список использованных источников:

1. Танки больше не короли: Силы беспилотных Систем и Центр «Рубикон» меняют логику войны // Военная платформа. — 2025. — 22 декабря.

2. Минобороны раскрыло детали новой тактики танкистов ВС РФ при прорывах обороны // Российская газета. — 2025. — 21 декабря.

3. Танкисты уничтожили позиции и технику ВСУ на Харьковском направлении // Телеканал «Звезда». — 2025. — 14 октября 2. Степовой Б., Федоров А. Высота нападения: танковые подразделения Российской армии усиливаются БПЛА // Известия. — 2026. — 22 января.

4. Танкисты и артиллеристы стали видеть цели в Красноармейске, как на ладони // Комсомольская правда. — 2025. — 20 ноября.

5. Российские танки усилят беспилотниками // Lenta.ru (со ссылкой на Известия). — 2026. — 22 января.

ОГЛАВЛЕНИЕ

ТАКТИКА ПСИХОЛОГИЧЕСКОГО ВОЗДЕЙСТВИЯ В УСЛОВИЯХ СПЕЦИАЛЬНОЙ ВОЕННОЙ ОПЕРАЦИИ
(Бурштын Е.А., научный руководитель – Вербицкий Г.И.) **3**
ВЛИЯНИЕ АКЦЕНТУАЦИИ ХАРАКТЕРА ЛИЧНОСТИ НА ДЕЯТЕЛЬНОСТЬ ВОЕННОСЛУЖАЩЕГО
(Ковалевский А.И., научный руководитель – Вербицкий Г.И.) **6**
ТАКТИКА НАСТУПАТЕЛЬНОГО БОЯ В УСЛОВИЯХ СПЕЦИАЛЬНОЙ ВОЕННОЙ ОПЕРАЦИИ
(Соловей М.М., научный руководитель – Иволгина О.И.) **8**
ТАКТИКА ОБОРОНИТЕЛЬНОГО БОЯ В РЕАЛИЯХ СПЕЦИАЛЬНОЙ ВОЕННОЙ ОПЕРАЦИИ
(Зарецкий Г.В., научный руководитель – Лялихов К.А.) **11**
ПРИМЕНЕНИЕ БЕСПИЛОТНЫХ ЛЕТАТЕЛЬНЫХ АППАРАТОВ В НАЧАЛЬНОЙ ФАЗЕ СПЕЦИАЛЬНОЙ ВОЕННОЙ ОПЕРАЦИИ
(Грошев Е.С., научный руководитель – Сименков Е.Л.) **14**
АКТУАЛЬНОСТЬ ПРОВЕДЕНИЯ ПРАКТИЧЕСКИХ ТРЕНИРОВОК СПЕЦИАЛИСТОВ ПО КИБЕРБЕЗОПАСНОСТИ: РАЗРАБОТКА ВЕБ-ПРИЛОЖЕНИЯ ДЛЯ ВООРУЖЕННЫХ СИЛ РЕСПУБЛИКИ БЕЛАРУСЬ
(Пучков Е.С., научный руководитель – Савицкий А.Ю.) **17**
ПРИМЕНЕНИЕ ТЕХНОЛОГИЙ OSINT ДЛЯ ВЫЯВЛЕНИЯ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
(Лукашевич Е.А., научный руководитель – Супрун Ф.Н.) **18**
АВТОМАТИЗАЦИЯ УПРАВЛЕНИЯ ФИЗИЧЕСКОЙ ПОДГОТОВКОЙ КУРСАНТОВ: РАЗРАБОТКА СЕРВЕРНОГО ПРОГРАММНОГО СРЕДСТВА
(Лазовский И.А., научный руководитель – Томильчик Ю.В.) **19**
ВАЖНОСТЬ АТВТОМАТИЗАЦИИ ПРОЦЕССА ТЕСТИРОВАНИЯ ВОЕННОСЛУЖЕЩИХ ВООРУЖЕННЫХ СИЛ РЕСПУБЛИКИ БЕЛАРУСЬ (Пучков Е.С., научный руководитель – Стогначев Р.В.) **20**
ВЛИЯНИЕ СПОРТИВНЫХ ИГР НА СПЛОЧЕНИЕ ВОИНСКОГО КОЛЛЕКТИВА
(Рысев А.Д., Сиваков В.Л., Янович А.В., научный руководитель – Хомчик Д.Н.) **21**
УСТРОЙСТВО ДИАГНОСТИКИ СОСТОЯНИЯ АККУМУЛЯТОРНЫХ БАТАРЕЙ НОСИМЫХ РАДИОСТАНЦИЙ
(Алексеенко А.Д., научный руководитель – Федоренко В.А.) **22**
ПОРТАТИВНОЕ УСТРОЙСТВО ДЛЯ ОБНАРУЖЕНИЯ РАДИОЧАСТОТНОЙ АКТИВНОСТИ
(Бузинчик Е.В., научный руководитель – Дудак М.Н.) **23**
ПРОГРАММНЫЙ КОМПЛЕКС ВИЗУАЛИЗАЦИИ И КОНТРОЛЯ ЗНАНИЙ ПРИ ИЗУЧЕНИИ РРС Р-409МБ1
(Мисько А.А, научный руководитель – Викторович М.А.) **24**
ВИРТУАЛЬНАЯ ЭКСКУРСИЯ ПО ЦИФРОВОЙ ТРОПОСФЕРНОЙ СТАНЦИИ Р-432 КАК ЭЛЕМЕНТ ФОРМИРОВАНИЯ ПРОСТРАНСТВЕННОГО ПРЕДСТАВЛЕНИЯ ОБ ОБОРУДОВАНИИ **25**

(Зелинский И.А., научный руководитель – Игнатенко А.А.)
МОДЕЛИРОВАНИЕ ОПЕРАТОРСКИХ ПРОЦЕДУР ТРОПОСФЕРНОЙ СТАНЦИИ Р 412МБ В КОМПЬЮТЕРНОМ ТРЕНАЖЁРЕ
(Бегаль Д.С., научный руководитель – Сидоров С.В.) **28**
КОНЦЕПТУАЛЬНЫЕ НАПРАВЛЕНИЯ МОДЕРНИЗАЦИИ ИНФОКОММУНИКАЦИОННОЙ ИНФРАСТРУКТУРЫ ВОЙСК СВЯЗИ В УСЛОВИЯХ ТРАНСФОРМАЦИИ ФОРМ И СПОСОБОВ ВЕДЕНИЯ ВООРУЖЕННОЙ БОРЬБЫ
(Лабан К.А., научный руководитель – Дудак М.Н.) **29**
ПОДВИЖНЫЕ КОМПЛЕКСЫ Р-443О: ВОЗМОЖНОСТИ И ПЕРСПЕКТИВЫ
(Ковалевская А.О., научный руководитель – Ермоленко Д.М.) **30**
УСТРОЙСТВО ДЛЯ СОЗДАНИЯ ИСКУССТВЕННЫХ ПОМЕХ НА ЦИФРОВЫХ И АНАЛОГОВЫХ ПРОВОДНЫХ ЛИНИЯХ СВЯЗИ
(Нестерович М.П., научный руководитель – Томильчик Ю.В.) **31**
СЕТЕВОЙ ТРЕНАЖЕР ПО РАБОТЕ НА РАДИОСТАНЦИИ Р-181-5НУ
(Шевчук А.А., научный руководитель – Латушко М.М.) **32**
СЕТЕВОЙ ТРЕНАЖЕР ПО РАДИОСТАНЦИИ Р-188
(Ивашкевич А.Ю., научный руководитель – Латушко М.М.) **33**
ЭЛЕКТРОННЫЙ ПРОГРАММНЫЙ КОМПЛЕКС «РАДИОСТАНЦИИ ТАКТИЧЕСКОГО ЗВЕНА УПРАВЛЕНИЯ»
(Носков Н.П., научный руководитель – Латушко М.М.) **34**
РЕФЛЕКСИЯ ПЛЕНА В ВОСПОМИНАНИЯХ УЧАСТНИКОВ ОБОРОНЫ БРЕСТСКОЙ КРЕПОСТИ 1941 Г.
(Бурштын Е.А., научный руководитель – Голубев В.Ю.) **35**
ЭЛЕКТРОННЫЙ ТРЕНАЖЁР ПО РАБОТЕ НА П-320 IP МАРШРУТИЗАТОРЕ
(Николаев А.В., научный руководитель – Бондарев П.И.) **36**
ОБОСНОВАНИЕ ЦЕЛЕСООБРАЗНОСТИ РАЗРАБОТКИ СРЕДСТВА МОНИТОРИНГА СОСТОЯНИЯ ОПТОВОЛОКОННЫХ ИНТЕРВАЛОВ В ТОПС
(Масло М.Ю., научный руководитель – Томильчик Ю.В.) **37**
КОМПЬЮТЕРНОЕ ПРИЛОЖЕНИЕ ДЛЯ КОНТРОЛЯ СВЯЗИ НА УЗЛАХ СВЯЗИ ПУНКТОВ УПРАВЛЕНИЯ
(Святун К.М., научный руководитель – Викторович М.А.) **38**
АКТУАЛЬНОСТЬ СЕТЕВОГО ТРЕНАЖЕРА ДЛЯ РАБОТЫ НА РАДИОСТАНЦИИ Р-180
(Ясюкович Н.В., научный руководитель – Дудак М.Н.) **39**
АВТОМАТИЗИРОВАННАЯ СИСТЕМА КОНТРОЛЯ СОСТОЯНИЯ ВВСТ В ПОДРАЗДЕЛЕНИЯХ ВООРУЖЕННЫХ СИЛ РЕСПУБЛИКИ БЕЛАРУСЬ
(Фирсов А.А., научный руководитель – Герасимов А.С.) **41**
ПРИМЕНЕНИЕ СОВРЕМЕННЫХ МЕТОДОВ ДИАГНОСТИКИ ПСИХОЛОГИЧЕСКОГО СОСТОЯНИЯ ВОЕННОСЛУЖАЩИХ
(Никитенко Р.А., научный руководитель – Герасимов А.С.) **44**
НЕОБХОДИМОСТЬ АВТОМАТИЗАЦИИ ПРОЦЕССА УЧЕТА МАТЕРИАЛЬНЫХ СРЕДСТВ
(Чернявский В.К., научный руководитель – Герасимов А.С.) **45**
ИСТОРИЯ РАЗВИТИЯ СЕТЕЙ DMR РАДИОСВЯЗИ **47**

(Запариванный А.В., научный руководитель – Герасимов А.С.)
IP-ТЕЛЕФОНИЯ: ЭВОЛЮЦИЯ И ПРОБЛЕМЫ ВНЕДРЕНИЯ В СИСТЕМАХ ВОЕННОГО УПРАВЛЕНИЯ
(Барковский В.Д., научный руководитель – Викторович М.А.) **49**
БАЗОВЫЕ ПРИНЦИПЫ ПОСТРОЕНИЯ БЕСПРОВОДНЫХ СЕНСОРНЫХ СЕТЕЙ
(Рац Р.А., научный руководитель – Аскерко А.В.) **52**
РОЛЬ КОМПЬЮТЕРНЫХ ПРОГРАММ В ИЗУЧЕНИИ СЛОЖНЫХ КОМПЛЕКСОВ СВЯЗИ: СРАВНИТЕЛЬНЫЙ АНАЛИЗ ТРАДИЦИОННЫХ И ИНТЕРАКТИВНЫХ МЕТОДОВ
(Высоцкий Д.М., научный руководитель – Викторович М.А.) **56**
РОЛЬ КОМПЬЮТЕРНОЙ ФОРЕНЗИКИ В ОБЕСПЕЧЕНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В УСЛОВИЯХ ЦИФРОВОЙ ТРАНСФОРМАЦИИ
(Шутко А.П., научный руководитель – Герасимов А.С.) **57**
ПОВЫШЕНИЕ ЭФФЕКТИВНОСТИ УПРАВЛЕНИЯ ПОДРАЗДЕЛЕНИЯМИ НА ОСНОВЕ ВНЕДРЕНИЯ ПРОГРАММНЫХ СРЕДСТВ ВИЗУАЛИЗАЦИИ ЗАДАЧ С УЧЕТОМ СОВРЕМЕННЫХ ТЕНДЕНЦИЙ РАЗВИТИЯ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ
(Волков П.А., Франковский В.В., научный руководитель – Гусаков П.Б.) **59**
ВНЕДРЕНИЕ RAG-СИСТЕМЫ В УЧЕБНЫЙ ПРОЦЕСС ПОДГОТОВКИ ИНЖЕНЕРОВ ПО ТЕЛЕКОММУНИКАЦИЯМ
(Бардашевич А.В., научный руководитель – Федоренко В.А.) **61**
СОВРЕМЕННЫЕ ВОЕННЫЕ ИННОВАЦИИ
(Жолудь В.А., научный руководитель – Борисовец А.В.) **63**
ПРИМЕНЕНИЕ РЕКТЕНН В РАДИОТЕХНИЧЕСКИХ ВОЙСКАХ
(Никончук Ю.А., научный руководитель – Янцевич М.А.) **64**
РАЗРАБОТКА КОМПЛЕКСА НАГЛЯДНО-ОБУЧАЮЩИХ ПРОГРАММ ДЛЯ ПРОФЕССИОНАЛЬНОЙ ПОДГОТОВКИ СПЕЦИАЛИСТОВ ПО РАДИОЭЛЕКТРОННОМУ ОБОРУДОВАНИЮ
(Маликов А.С., научный руководитель – Боровой А.Г.) **65**
ВЛИЯНИЕ СРЕДСТВ РАЗВЕДКИ И ОГНЕВОГО ПОРАЖЕНИЯ НА БАЗЕ БЕСПИЛОТНЫХ ЛЕТАТЕЛЬНЫХ АППАРАТОВ НА ЭЛЕМЕНТЫ ТАКТИЧЕСКОЙ ПОДГОТОВКИ ПОДРАЗДЕЛЕНИЯ
(Волков П.А., Франковский В.В., научный руководитель – Коношенко А.В.) **67**
БОЙ В ГОРОДЕ ПРИ НАСЫЩЕНИИ ПРОТИВНИКОМ БПЛА
(Некрашевич А.А., научный руководитель – Алисевич С.А.) **69**
РОЛЬ ЦИФРОВЫХ ТЕХНОЛОГИЙ В ПОДГОТОВКЕ КОМАНДИРОВ К ВЕДЕНИЮ ОБЩЕВОЙСКОВОГО БОЯ
(Дрозд А.А., научный руководитель – Усов Е.С.) **70**
ПСИХОЛОГИЧЕСКАЯ УСТОЙЧИВОСТЬ ВОЕННОСЛУЖАЩИХ В УСЛОВИЯХ СПЕЦИАЛЬНЫХ БОЕВЫХ ДЕЙСТВИЙ
(Ведерников В.Д., научный руководитель – Лепесий И.А.) **71**
ПРИМЕНЕНИЕ ПРОТИВОТАНКОВЫХ УПРАВЛЯЕМЫХ РАКЕТ В СОВРЕМЕННОМ ОБЩЕВОЙСКОВОМ БОЮ
(Мороговский А.А., научный руководитель – Степанец Е.В.) **74**
ТАКТИКА ПРИМЕНЕНИЯ ДРОНОВ В УСЛОВИЯХ **76**

ПРОТИВОДЕЙСТВИЯ РЭБ И ПВО
(Недбайлик С.В., научный руководитель – Бабич В.Н.)
ПРИМЕНЕНИЕ ИСКУСТВЕННОГО ИНТЕЛЛЕКТА В ВОЕННОМ ДЕЛЕ
(Соколов Д.С., Павелко В.С., научный руководитель – Коношенко А.В.) **78**
АППАРАТНО-ПРОГРАММНЫЙ ШЛЮЗ С АППАРАТНОЙ ИЗОЛЯЦИЕЙ КАНАЛОВ
(Бабич Н.В., научный руководитель – Дудак М.Н.) **80**
РАЗРАБОТКА МОБИЛЬНОГО ПРИЛОЖЕНИЯ ДЛЯ ПРОВЕРКИ ДОКУМЕНТОВ И ИДЕНТИФИКАЦИИ ЛИЧНОСТИ
(Некраш М.А., научный руководитель – Савицкий А.Ю.) **84**
ОНТОЛОГИЧЕСКАЯ МОДЕЛЬ АНАЛИЗА СООБЩЕНИЙ О ПРОИСШЕСТВИЯХ ДЛЯ ЗАДАЧ ИНФОРМАЦИОННОЙ ПОДДЕРЖКИ ДЕЖУРНЫХ СЛУЖБ МВД
(Мысько Н.А., научный руководитель – Савицкий А.Ю.) **85**
ПЕРСПЕКТИВЫ ПРИМЕНЕНИЯ И ИНТЕГРАЦИИ РОБОТИЗИРОВАННЫХ КОМПЛЕКСОВ СВЯЗИ В СУЩЕСТВУЮЩУЮ ИНФРАСТРУКТУРУ ВОЙСК ВС РБ
(Мастибродский В.В., научный руководитель – Сидоров С. В.) **87**
ИНТЕГРАЦИЯ БЕСПИЛОТНЫХ И РАДИОЭЛЕКТРОННЫХ СИСТЕМ В ОБЕСПЕЧЕНИИ БЕЗОПАСНОСТИ ВОЗДУШНОГО ПРОСТРАНСТВА ГОСУДАРСТВА
(Бондарович А.С., научный руководитель – Беккеров Д.Э.) **88**
СОВРЕМЕННЫЕ ПОДХОДЫ К ПРОТИВОВОЗДУШНОЙ ОБОРОНЕ В УСЛОВИЯХ ГИБРИДНЫХ УГРОЗ
(Возный П.С., научный руководитель – Хожевец О.А.) **89**
РАЗВИТИЕ БЕСПИЛОТНОЙ АВИАЦИИ В СИСТЕМЕ ПРОТИВОВОЗДУШНОЙ ОБОРОНЫ БЕЛАРУСИ
(Пеунов Т.А., научный руководитель – Лавринчик Н.Н.) **90**
ВЗАИМОДЕЙСТВИЕ ДЕЖУРНЫХ СИЛ ПВО С ВОЙСКАМИ ТЕРРИТОРИАЛЬНОЙ ОБОРОНЫ ПРИ ОХРАНЕ КРИТИЧЕСКИ ВАЖНЫХ ОБЪЕКТОВ
(Ревенко С.А., научный руководитель – Беккеров Д.Э.) **91**
ПЕРСПЕКТИВЫ РАЗВИТИЯ СИСТЕМ РАДИОЛОКАЦИОННОГО КОНТРОЛЯ МАЛЫХ ВЫСОТ В ВВС И ВОЙСКАХ ПВО ВООРУЖЕННЫХ СИЛ РЕСПУБЛИКИ БЕЛАРУСЬ
(Якубовский А.С., научный руководитель – Маргель А.Б.) **92**
ИСПОЛЬЗОВАНИЕ МЕТОДА ОПОРНЫХ ВЕКТОРОВ ДЛЯ ФОРМИРОВАНИЯ ОДНОМЕРНОЙ РЕШАЮЩЕЙ СТАТИСТИКИ ПРИ РАСПОЗНАВАНИИ МАЛОРАЗМЕРНЫХ БЕСПИЛОТНЫХ ЛЕТАТЕЛЬНЫХ АППАРАТОВ И ПТИЦ
(Чигряй В.Г., научный руководитель – Храменков А.С.) **93**
АНАЛИЗ СУЩЕСТВУЮЩИХ АЛГОРИТМОВ ОРИЕНТАЦИИ В БИНС
(Тищенко Т.А., Маликов А.С., научный руководитель – Боровой А.Г.) **95**
ИСПОЛЬЗОВАНИЕ ДЕМОНСТРАЦИОННОГО СТЕНДА «ОПТОЭЛЕКТРОННЫЙ ЛОГИЧЕСКИЙ ЭЛЕМЕНТ *ИЛИ-НЕ*» В ОБРАЗОВАТЕЛЬНОМ ПРОЦЕССЕ УЧРЕЖДЕНИЯ ОБРАЗОВАНИЯ «ВОЕННАЯ АКАДЕМИЯ РЕСПУБЛИКИ БЕЛАРУСЬ»
(Медушевская Н.В., научный руководитель – Мацкевич А.Н.) **96**
ОБЗОР ТЕХНИЧЕСКИХ ОСОБЕННОСТЕЙ ПРИ СОВМЕСТНОМ **98**

ИСПОЛЬЗОВАНИИ ТЕПЛОВИЗИОННОГО И ТЕЛЕВИЗИОННОГО КАНАЛОВ ОБНАРУЖЕНИЯ ЦЕЛИ
(Гуцев П.А., научный руководитель – Казарин А.В.)
ЧИСЛЕННО-АНАЛИТИЧЕСКИЕ МЕТОДЫ АППРОКСИМАЦИИ ПРИ ИЗУЧЕНИИ СВЧ ХАРАКТЕРИСТИК РАДИОЭЛЕКТРОННЫХ СИСТЕМ
(Швец В.С., Исаев В.О., Бойкачев П.В.) **99**
ИССЛЕДОВАТЕЛЬСКИЙ ПРОГРАММНЫЙ КОМПЛЕКС НА БАЗЕ UNITY ДЛЯ ОПРЕДЕЛЕНИЯ УЯЗВИМОСТЕЙ В БОЕВЫХ ПОРЯДКАХ ФОРМИРОВАНИЙ ПВО ПРИ ПРОТИВОДЕЙСТВИИ УДАРНЫМ БЕСПИЛОТНЫМ ЛЕТАТЕЛЬНЫМ АППАРАТАМ
(Пальцев В.А., научный руководитель – Шарак Д.С.) **101**
ГЕНЕРАЦИЯ КРИПТОГРАФИЧЕСКИ СТОЙКОЙ ПСЕВДОСЛУЧАЙНОЙ ПОСЛЕДОВАТЕЛЬНОСТИ ДЛЯ АЛГОРИТМА ПСЕВДОСЛУЧАЙНОЙ ПЕРЕСТРОЙКИ РАБОЧЕЙ ЧАСТОТЫ В СИСТЕМАХ ЗАЩИТЫ КАНАЛА СВЯЗИ С БЕСПИЛОТНЫМ ЛЕТАТЕЛЬНЫМ АППАРАТОМ
(Мойсюк-Дранько Я.А., научный руководитель – Дубовик И.А.) **102**
НАХОЖДЕНИЕ АППРОКСИМИРУЮЩИХ ФУНКЦИЙ ЧИСЛЕННЫМ МЕТОДОМ ДЛЯ УВЕЛИЧЕНИЯ РАВНОМЕРНОСТИ ФАЗАЧАСТОТНОЙ ХАРАКТЕРИСТИКИ ШИРОКОПОЛОСНЫХ СОГЛАСУЮЩИХ УСТРОЙСТВ И ФИЛЬТРОВ
(Полещук М.И., научный руководитель – Бойкачев П.В.) **104**
СИСТЕМА РАСПОЗНАВАНИЯ НАЗЕМНЫХ ОБЪЕКТОВ ДЛЯ БПЛА НА ОСНОВЕ НЕЙРОННОЙ СЕТИ YOLOv8m
(Горев Е.В., научный руководитель – Дубовик И.А.) **106**
МЕТОДИКА ОБОСНОВАНИЯ ТЕХНИЧЕСКИХ ТРЕБОВАНИЙ К КООРДИНАТНОМУ БЛОКУ ЦЕЛИ ИСТРЕБИТЕЛЬНОГО БЕСПИЛОТНОГО ЛЕТАТЕЛЬНОГО АППАРАТА
(Шорец-Пашковский В.В., Мороз А.Н., Бухтиаров Д.В., научный руководитель – Мороз А.Н.) **107**
ВЗАИМОДЕЙСТВИЕ ТАНКОВЫХ ПОДРАЗДЕЛЕНИЙ С ГРУППАМИ ОПЕРАТОРОВ БПЛА ПРИ ВЕДЕНИИ ОГНЯ С ЗАКРЫТЫХ ОГНЕВЫХ ПОЗИЦИЙ: СОВРЕМЕННОЕ СОСТОЯНИЕ И ПЕРСПЕКТИВЫ РАЗВИТИЯ
(Павелко В.С., Кулешова В.Р., научный руководитель – Ли А.Е.) **109**

Научное издание

Электронный сборник тезисов (докладов) 62-й научной конференции аспирантов, магистрантов и студентов учреждения образования «Белорусский государственный университет информатики и радиоэлектроники»

ИННОВАЦИОННЫЕ ТЕХНОЛОГИИ В ОБРАЗОВАТЕЛЬНОМ ПРОЦЕССЕ

(Минск, 15 апреля 2026 года)

В авторской редакции

Компьютерная верстка С.В.Романовский