Акционерное общество «Национальная компания «Казахстан инжиниринг»
ТОВАРИЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ
«RESEARCH&DEVELOPMENT ЦЕНТР «КАЗАХСТАН ИНЖИНИРИНГ»
(ТОО «R&D ЦЕНТР «КИ»)

Экз. №_____

СБОРНИК
Межведомственной научно-практической конференции «Разработка оборудования для создания национальной системы военной радиосвязи»

(в рамках грантового финансирования на 2022-2024 гг.)
ИРН AP 148029/0222

Астана 2024

АО «НК «Казахстан инжиниринг»
ТОО «R&D центр «Казахстан инжиниринг»

Экз. №_____

Разработка оборудования для создания национальной системы военной радиосвязи

Сборник Межведомственной научно-практической конференции

ИРН AP 148029/0222

Астана 2024

УДК 621.3(069)
ББК 33.2
С 32
ISBN 978-601-7026-43-1

Редакционная коллегия:
Редактор: Байбеков С.Н., доктор технических наук, профессор
Члены редакционной коллегии:
Жасузаков С.А., генерал-полковник, доктор философии (PhD).
Рыспаев А.Н., генерал-майор запаса, доктор философии (PhD), ассоциированный профессор (доцент).
Доля А.В., майор, докторант.
Секретарь редакционной коллегии:
Несипова С.С.

Рецензенты:
1. Б.С.Касимов – начальник кафедры основ военной радиотехники и электроники, доктор философии (PhD), полковник.
2. Д.Е.Абдрасилов – старший преподаватель цикла МКС кафедры ЗРВ, доктор философии (PhD), полковник.

Сборник материалов Межведомственной научно-практической конференции «Разработка оборудования для создания национальной системы военной радиосвязи»: – Астана, 2024. – 172 с. – русский.

Рекомендовано к изданию Ученым советом ТОО «R&D центр «Казахстан инжиниринг». Протокол №07 от 18 марта 2024 года.

В Сборник вошли доклады участников Межведомственной научно-практической конференции «Разработка оборудования для создания национальной системы военной радиосвязи», посвященной обсуждению разрабатываемого в рамках проекта грантового финансирования на 2022-2024 гг. (ИРН AP 148029/0222 «Разработка оборудования для создания национальной системы военной радиосвязи»).

Материалы сборника конференции объединяют научно-технические мысли широкого круга специалистов по развитию и совершенствованию научных исследований в области организации связи и управления, а также применение средств, родов и видов связи, производства, технического обслуживания и ремонта средств связи и коммутации.

ISBN 978-601-7026-43-1

УДК 621.3(069)
ББК 33.2
С 32

© ТОО «R&D центр «Казахстан инжиниринг», 2024

ПРИВЕТСТВЕННОЕ СЛОВО К УЧАСТНИКАМ КОНФЕРЕНЦИИ

Байсейтов Г.Н.
генеральный директор ТОО «R&D центр «Казахстан инжиниринг»

Құрметті конференцияға қатысушылар! Сіздерді ведомствоаралық ғылыми-практикалық конференциясында көргенімізге қуаныштымыз!

Уважаемые участники конференции! Мы рады приветствовать Вас на межведомственной научно-практической конференции.

Я хочу выразить благодарность всем присутствующим за понимание и активное участие в вопросе создания современной системы связи в Республике Казахстан.

Это еще раз подчеркивает актуальность темы и подтверждает, что у государственных органов есть единое понимание важности вопроса.

Проводимая межведомственная научно-практическая конференция призвана способствовать формированию реальных прогнозов в вопросах интеграции имеющихся средств радиосвязи силовых ведомств, создания отечественного радиооборудования, отвеючащего потребностям пользователей, а также определению общих очертаний перспективных научно-технических изысканий в этой области.

В условиях маневренного скоротечного современного боя с резкой сменой обстановки и при отсутствии сплошной линии соприкосновения войск гарантией устойчивого и гибкого управления войсками является надежная и качественная радиосвязь. Основным преимуществом радиосвязи является ее

мобильность, способность передавать информацию различного характера в движении.

При этом в настоящее время во всём мире в качестве радиосетей, предназначенных для обеспечения общественной безопасности, чаще используют узкополосные системы радиосвязи, основное преимущество которых – устойчивая работа. Но у них нет возможности высокоскоростной передачи данных, которая на современном этапе развития необходима для эффективного выполнения обязанностей сотрудниками служб общественной безопасности. Широкополосные системы связи обеспечивают обмен большими объемами данных, однако имеют небольшую зону покрытия и более дорогостоящи.

Наша совместная работа призвана способствовать обсуждению различных вопросов науки, методики и практики, и выработать рекомендаций по ***разработке национальной системы военной радиосвязи.***

Уважаемые коллеги!

Полагаю, что профессионализм состава участников Конференции будет способствовать выработке решений этих вопросов, а также дальнейшему совершенствованию взаимовыгодного сотрудничества между силовыми структурами, оборонно-промышленным комплексом в области научно-технической деятельности, а также развития вооружения и военной техники.

Выражаем надежду, что выводы конференции помогут в установлении облика основных перспективных направлений развития военной радиосвязи в Казахстане, перечня наиболее приоритетных прикладных, фундаментально-поисковых и экспериментальных работ, предшествующих полномасштабной разработке новых и перспективных изделий и материалов.

Надеюсь, что выработанные в ходе конференции предложения станут ориентиром для нашей дальнейшей совместной деятельности.

Құрметті қатысушылар!
Барлықтарыңызға шығармашылық табыс, қызықты да жемісті еңбектер тілеймін! Назарларыңызға рахмет!

УДК 629.783

О НЕКОТОРЫХ ВОПРОСАХ ПРИМЕНЕНИЯ БПЛА ПРИВЯЗНОГО ТИПА ДЛЯ РЕТРАНСЛЯЦИИ СВЯЗИ И КОНТРОЛЯ ОХРАНЯЕМОЙ ТЕРРИТОРИИ

СЕМЧЕНКО А.Г.[1], *полковник, докторант*
ТОЙБАЗАРОВ Д.О.[1], *полковник, доктор (PhD)*
БАЙСЕИТОВ Г.Н.[2], *полковник, кандидат технических наук*

[1]*Национальный университет обороны Республики Казахстан, г. Астана, Казахстан*
[2]*Генеральный директор ТОО «R&D центр «Казахстан инжиниринг», г. Астана, Казахстан*

Аннотация.

Статья разработана в рамках научного исследования по теме программы: ИРН BR21882279 «Разработка и изготовление малогабаритного ретранслятора связи на базе беспилотного летательного аппарата (БПЛА) для увеличения дальности и устойчивости радиосвязи».

Статья посвящена исследованию некоторых вопросов применения беспилотных летательных аппаратов (БПЛА) привязного типа для ретрансляции радиосвязи и контроля важных объектов, в том числе военных. В статье анализируются основные проблемы и вызовы, связанные с применением привязных БПЛА для ретрансляции связи, включая проблемы с безопасностью передачи данных, надежностью и техническими особенностями привязных дронов. Рассматриваются примеры использования БПЛА привязного типа в военной и гражданской сферах в целях ретрансляции связи, охраны территории и стратегических объектов.

В заключении статьи делается вывод о потенциале применения БПЛА привязного типа для ретрансляции связи и контроля объектов в различных сферах деятельности. Результаты обзора могут быть полезны для специалистов в области беспилотных систем и технологий связи, обороны и безопасности, а также для разработчиков и производителей БПЛА.

В рамках литературного обзора проанализированы научные статьи, публикации, отраженные в открытых источниках.

Ключевые слова: беспилотный летательный аппарат (БПЛА), БПЛА привязного типа; ретрансляция связи, контроль охраняемой территории.

В настоящее время БПЛА привлекают все большее внимание пользователей в различных сферах деятельности, включая оборону, безопасность объектов и телекоммуникации. Одной из ключевых функций, выполняемых БПЛА, является ретрансляция связи, что позволяет установить бесперебойный и эффективный обмен информацией между заинтересованными удаленными абонентами. Разведывательные возможности в режиме реального времени многих современных БПЛА также ни у кого не вызывают сомнений.

В данной статье будет рассмотрено применение БПЛА привязного типа для ретрансляции связи и контроля охраняемых территорий. Основное внимание будет уделено специфике применения БПЛА для ретрансляции связи в различных областях, таких как военные операции, чрезвычайные и аварийные ситуации, телекоммуникация и научные исследования. Будут рассмотрены преимущества и ограничения использования БПЛА в каждой из этих областей. В дополнение к техническим аспектам, также будет рассмотрен вопрос безопасности применения БПЛА привязного типа для ретрансляции связи и охраны территории.

Материалы этой статьи могут быть полезны специалистам в области телекоммуникаций, обороны и безопасности. Кроме того, данная информация может оказаться полезной при определении направлений развития применения БПЛА в военной и гражданской сферах.

Основная часть. Трудно в это поверить, но БПЛА находятся на службе у человека уже более ста лет.

С момента своего появления в 1916 году в виде радиоуправляемых монопланов, беспилотники очень видоизменились, а в последние два десятилетия стремительно вошли в нашу повседневную жизнь. Технологии, применяемые на современных беспилотных летательных аппаратах, значительно улучшились, усовершенствовались их конструкция и технические возможности. БПЛА превратились в универсальную воздушную платформу для самой широкой линейки полезной нагрузки.

Одним из последних достижений в данной сфере является использование в качестве воздушной платформы привязных беспилотных систем или привязных дронов. Рынок привязных дронов растет с каждым годом благодаря преимуществам, которые они предоставляют пользователям по своим возможностям и характеристикам. К примеру, рост этого рынка в 2019 году составил 53,54% и совокупный темп роста в период с 2019 по 2023 год ожидался более 70% [1].

Многие люди, знакомые с дронами в жизни и в быту, ничего не знают о привязных беспилотных системах, обо всех их преимуществах, которые они представляют как в гражданской, так и в военной сферах. Такие беспилотники могут «висеть» в воздухе долгие десятки часов без необходимости замены элементов питания, так как энергию для силовой установки дрона и для полезной нагрузки, они получают по длинному кабелю от наземной станции питания и управления. Управление такими беспилотниками в режиме 24/7 не требует высокой квалификации операторов, так как БПЛА в прямом смысле привязан к наземной станции и не совершает сложных маневров и эволюций в воздухе.

Дроны мультикоптеры обладают рядом преимуществ по сравнению с беспилотными летательными аппаратами, построенными по самолетной схеме. Они способны осуществлять вертикальный взлет и посадку, что делает их более удобными в использовании, так как им не требуется взлетно-посадочная полоса и дорогостоящее стартовое оборудование. Мультикоптеры также

предоставляют возможность ведения разведки и наблюдения, обнаружения и идентификации объектов в режиме реального времени, передачи данных на наземные станции управления, выдачи целеуказаний, мониторинга окружающей среды, фотовидеосъемки и ретрансляции радиосигналов.

Рисунок 1 – Состав оборудования БПЛА-привязного типа

Развитие класса привязных мультикоптеров, которые связаны с наземным пунктом управления с помощью кабеля-троса, обладающих небольшими размерами и потреблением энергии, считается наиболее перспективным направлением. Концепция использования привязных мультикоптеров особенно актуальна в случаях, когда требуется продолжительное нахождение в воздухе, на одной высоте, в заданной точке пространства. Основными особенностями таких авиационных платформ являются продолжительное время полета, быстрое развертывание и защищенность канала передачи данных.

Привязные авиационные платформы включают в себя стартовую платформу, базовую станцию, мультикоптер, полезную нагрузку, кабель-трос и наземный блок питания (пример представлен на рисунке 1). Полезная нагрузка может состоять из оптико-электронных приборов и различного радиоэлектронного оборудования [2].

Беспилотники такого типа находят своё широкое применение в военной сфере (рисунок 2).

Вот некоторые примеры основных направлений применения привязных БПЛА в военных целях:

1. Разведка объектов и местности. Беспилотники могут использоваться для получения информации в реальном масштабе времени о состоянии позиций противника, наличии подвижных объектов, маршрутах их передвижения. Такие БПЛА могут быть оснащены различными датчиками, сенсорами, тепловизорами, оптическими и радиолокационными системами.

Рисунок 2 – БПЛА-привязного типа в военной сфере

2. Связь. Привязные БПЛА могут использоваться для ретрансляции связи, особенно в труднодоступных или удаленных районах, где установка традиционных систем связи и управления может быть затруднена. Они могут быть оборудованы специализированной аппаратурой для усиления и передачи сигналов связи, что позволяет поддерживать надежную связь между различными военными объектами и органами военного управления.

3. Контроль и охрана Государственной границы и военных объектов. БПЛА могут быть оснащены датчиками, такими как радары и инфракрасные камеры, для обнаружения незаконного пересечения границы или других нарушений. Беспилотники могут использоваться для обеспечения безопасности военных баз и стратегических объектов военного и государственного управления. Дроны могут выполнять функции наблюдения и обнаружения активности по периметру охраняемых объектов, а также успешно использованы определения точного местоположения таких угроз.

Рисунок 3 – Применение БПЛА привязного типа для наблюдения в военной сфере

И это только некоторые примеры применения привязных БПЛА в военной сфере. Технология беспилотных летательных аппаратов постоянно развивается, и их возможности и применение продолжают расширяться.

Каждый тип БПЛА, отличающийся по своей конструкции, техническим характеристикам, имеет свои положительные и отрицательные стороны. Используя эти знания потребителям и разработчикам легче определить какой именно БПЛА для каких целей подходит и насколько будет эффективен в конкретных условиях обстановки.

Для примера, ниже приведены несколько основных преимуществ привязных БПЛА:

1) привязные дроны очень просты в использовании, все компоненты системы легко настраиваются, эксплуатируются и перемещаются в любую труднодоступную точку;

2) привязные дроны при необходимом обслуживании имеют практически неограниченный источник питания и время полета, так как подключаются к автономному источнику переменного тока, преобразующего его в постоянный ток, питание подается к БПЛА и его полезной нагрузке по кабелю;

3) информация по кабелю всегда защищена от радиоперехвата, все данные передаются через волоконно-оптический кабель, что повышает скорость передачи, защищает информацию от взлома, собранные беспилотником данные отправляются обратно на станцию также через кабель и передаются в базу (пункт управления) для сбора и анализа информации.

Также широкое применение БПЛА привязного типа нашли и в гражданской сфере.

К примеру, привязные дроны, такие как дрон Elistair, могут использоваться для ретрансляции мобильной связи. В будущем ожидается, что дроны-ретрансляторы связи станут неотъемлемой частью городского и сельского пространства, и одной из наиболее востребованной задачей их применения будет расширение охвата сети сотовой связи и интернета. Привязные дроны могут выступать в роли летающих станций связи, повышая эффективность и качество мобильных сетей, а также обеспечивая доступ в интернет в отдаленных районах.

В 2017 году компания AT&T продемонстрировала, как дроны с сотовыми приемопередатчиками могут быть использованы для быстрой замены неработоспособных базовых станций и восстановления мобильного покрытия сети сотовой связи после урагана Мария на Пуэрто-Рико [3].

После данного успешного опыта применения начали проводить исследования для определения оптимального расположения таких «мобильных летающих станций» в целях максимальной эффективности их применения.

В настоящее время стартап Spooky Action в США уже тестирует привязные дроны для предоставления интернет-соединения (рисунок 4) в удаленных районах Африки [3]. В сельской местности привязные дроны могут стать альтернативой дорогим вышкам сотовой связи, обеспечивая непрерывное подключение и доступ к интернету.

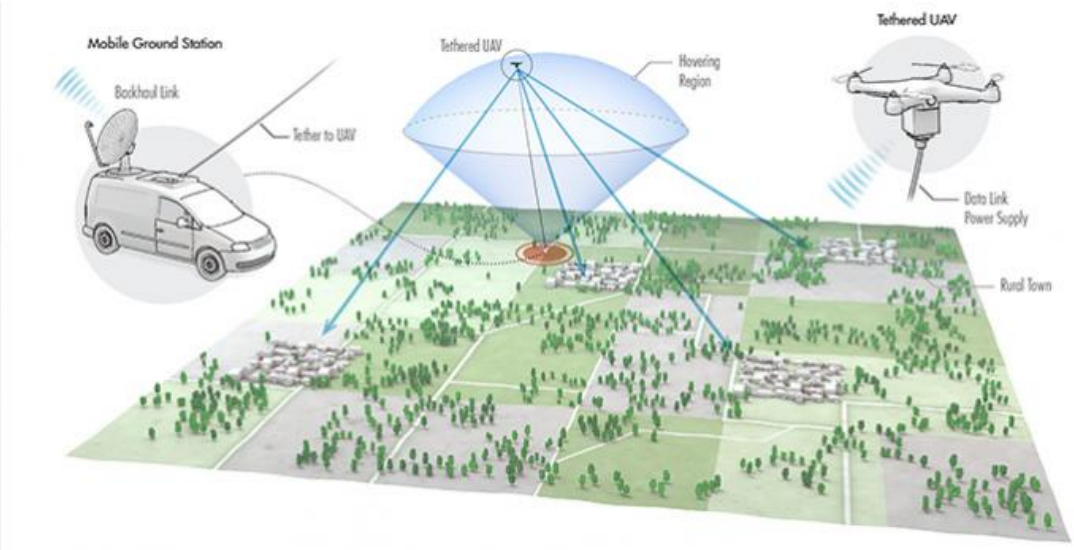


Рисунок 4 – Применение БПЛА привязного типа для ретрансляции связи в сельской местности

Привязные дроны при необходимых условиях способны находиться в воздухе до месяца или даже дольше, что является значительным преимуществом по сравнению с обычными дронами. Кроме того, они обеспечивают более стабильную передачу информации в основную сеть благодаря оптико-волоконному кабелю. Единственным недостатком привязных дронов является ограниченная мобильность, однако кабель, соединяющий их со станцией, может быть длиной до 150 метров.

Исследования, проведенные специалистами из KAUST, показали, что в будущем привязные дроны будут превосходить обычные дроны в решениях, связанных с сотовой связью. Это связано с тем, что оборудование 5G потребляет больше энергии и имеет больший вес по сравнению с 4G, что делает привязные дроны более привлекательными для данных целей. Кроме того, привязные дроны (рисунок 5) могут быть использованы в городской местности для дополнения стационарных станций сотовой связи, помогая снизить нагрузку на них и распределять трафик в пиковые часы.

Примеры конкретного использования БПЛА привязного типа для ретрансляции связи и наблюдения в военных и гражданских целях:

− использование БПЛА привязного типа в различных военных операциях для передачи информации и обеспечения связи между командными пунктами и боевыми подразделениями на поле боя. Это позволяет оперативно получать данные о ситуации на местности и координировать действия в режиме реального времени;

− БПЛА привязного типа могут использоваться для ретрансляции связи между поисковыми группами и командным центром в ходе проведения поисково-спасательных операций. Это поможет сократить время реагирования в сложной обстановке при спасении пострадавших, особенно при происшествиях или катастрофах в отдаленной или труднодоступной местности;

− БПЛА привязного типа могут выполнять функции плавучих станций связи, вышек связи в горной и пустынной местности, ретранслируя связь в отдаленных или труднодоступных районах, где установка обычной инфраструктуры связи представляет серьёзные экономические затраты.

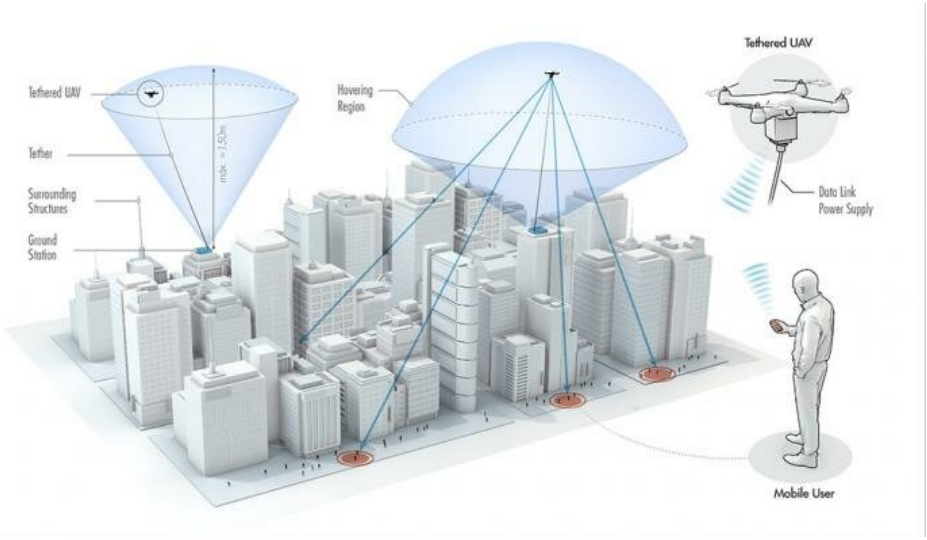


Рисунок 5 – Применение БПЛА привязного типа в качестве альтернативы вышкам сотовой связи

Выводы: В данной статье были рассмотрены некоторые вопросы применения беспилотных летательных аппаратов привязного типа для ретрансляции связи и контроля охраняемой территории. БПЛА привязного типа представляют собой эффективное средство для обеспечения связи в удаленных и труднодоступных районах, где прокладка проводной линии связи является нецелесообразной или невозможной.

Главными преимуществами таких БПЛА является их высокая мобильность и быстрое время развертывания. Они могут быть легко переброшены в необходимую точку местности, где оперативно настраиваются и успешно используются. Благодаря этому, БПЛА привязного типа позволяют в необходимые сроки обеспечить надежную и непрерывную связь и контроль пространства в зоне охраняемой территории. Благодаря своим техническим характеристикам, они могут осуществлять наблюдение контроль объектов на малых и предельно малых высотах, в том числе в сложных метеорологических условиях.

Однако, необходимо отметить, что применение БПЛА привязного типа в военной сфере имеет некоторые ограничения, связанные с вмешательством в его работу со стороны противника включая физическое уничтожение БПЛА.

Применение БПЛА привязного типа в настоящее время является одним из самых перспективных направлений, а расширение линейки полезной нагрузки станет новым импульсом к применению таких беспилотников как в военной, так и гражданской сферах. Таким образом, в целом, использование БПЛА привязного типа для ретрансляции связи и контроля охраняемой территории является эффективным решением.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1 KARNEEV SYSTEMS/Статьи/Применение привязных дронов в военной сфере/ URL:https://www.karneev.com/stati/primenenie-privyaznykh-dronov-v-voennoy-sfere-/(дата обращения 10.03.2024).

2 С. Семёнов, А. Полтавский, статья Зарубежные привязные авиационные платформы на базе мультикоптеров (2022)/ Fact Military/ Зарубежное военное обозрение. – 2022. – №4. – С.60-66/ URL: http://factmil.com/publ/strana/izrail/zarubezhnye _privjaznye_aviacionnye_platformy_na_baze_multikopterov_2022/36-1-0-1980/ (дата обращения 10.03.2024).

3 KARNEEV SYSTEMS/Статьи/Ретрансляция мобильной связи с привязного дрона Elistair/ URL:https://www.karneev.com/stati/retranslyatsiya-mobilnoy-svyazi-s-privyaznogo-drona-/(дата обращения 10.03.2024).

УДК 623.61

ПРОБЛЕМНЫЕ ВОПРОСЫ ОРГАНИЗАЦИИ ТАКТИЧЕСКОЙ РАДИОСВЯЗИ В УСЛОВИЯХ СОВРЕМЕННЫХ ВОЕННЫХ КОНФЛИКТОВ

ЖАНТЛЕСОВ А.У., *полковник*
ПРОСКУРА И.В., *подполковник*

Главное командование Национальной гвардии Республики Казахстан,
г. Астана, Республика Казахстан

Аннотация. В статье рассмотрены основные проблемные вопросы организации тактической УКВ радиосвязи в условиях ведения военных конфликтов с применением современных средств радиоразведки и радио подавления. Рассмотрены вопросы использования технологии ППРЧ, «битного» шифрования. Приведены практические приемы использования средств УКВ радиосвязи.

Данная научная статья опубликована в рамках выполнения научно-исследовательской работы ИРН AP148029/0222 «Разработка оборудования для создания национальной системы военной радиосвязи».

Ключевые слова: речевое кодирование, ППРЧ, стандарты DMR, APCO-25, TETRA.

Түйіндеме. Мақалада қазіргі заманғы радио барлау және радио басу құралдарын қолдана отырып, әскери қақтығыстар жағдайында радиобайланыстың тактикалық УҚТ ұйымдастырудың негізгі проблемалық мәселелері қарастырылған. ЖЖЖҚҚ технологиясын қолдану, «биттік» шифрлау мәселелері қарастырылды. УҚТ радиобайланыс құралдарын қолданудың практикалық әдістері келтірілген. Бұл ғылыми мақала ЖТН AP148029/0222 «Ұлттық әскери радиобайланыс жүйесін құруға арналған жабдықтарды әзірлеу» ғылыми-зерттеу жұмысын орындау шеңберінде жарияланды.

Түйін сөздер: сөйлеуді кодтау, ЖЖЖҚҚ, DMR, APCO-25, TETRA стандарты.

Abstract. The article considers the main problematic issues of the organization of tactical VHF radio communication in the context of military conflicts using modern means of radio intelligence and radio suppression. The issues of using the PTOF technology, «bit» encryption is considered. Practical methods of using VHF radio communication are given. This scientific article was published as part of the research work of IRN AP148029/0222 «Development of equipment for the creation of a national military radio communication system».

Key words: voice encoding, PTOF, DMR, APCO-25, TETRA standard.

Ведение современных военных конфликтов характеризуется использованием большого количества технических разнотипных средств и

систем радиосвязи военного и гражданского назначения, с широким применением технологических способов как приема и передачи различных видов информации, так и перехвата или подавления информационных потоков, причем в соответствующей литературе наиболее полному анализу данной проблематики подвергаются как правило вопросы организации связи в оперативном и стратегическом звеньях управления, тогда как анализ тактического звена управления представлен классическим пониманием организации связи в УКВ диапазоне, без учета особенностей ведения боевых действий в современных войнах.

Конфликты в Сирии, на Ближнем востоке, Украине показали, что на линии боевого соприкосновения противоборствующих сторон на относительно малых участках фронта сконцентрировано огромное количество радиоэлектронных средств связи, средств РЭР и РЭБ, беспилотной авиации различных протоколов, и частотных диапазонов, в связи с этим вопросы организации радиосвязи, мероприятия по ее защите от радио подавления, вскрытия тактических радиосетей, смена ключей шифрования, позывных, имеет критически важное значение при выполнении боевых задач, и пренебрежение такими, казалось бы, незначительными вопросами как смена ID-номеров корреспондентов, ставит под угрозу любые тактические действия подразделения.

Повсеместное внедрение беспилотной «карманной» авиации, позволяющей видеть в режиме онлайн каждый метр местности, на которой ведутся боевые действия, своевременная координация штурмовых и оборонительных действий вынуждает насыщать передний край портативными радиостанциями и доводить средства радиосвязи практически до каждого военнослужащего. Все это заставляет взглянуть под другим углом на практические вопросы эксплуатации радиостанций, их применение и варианты использования в тех или иных критических ситуациях, а также на некоторые вопросы организации радиосвязи на самом низовом уровне управления.

Выбор радиостанции.

Практическая эксплуатация в жестких условиях ведения боевых действий показывает, что предпочтение отдается радиостанциям с дисплеем и клавиатурой для возможности ручного ввода частоты и изменения основных настроек, так как требования по скрытому управлению войсками заставляют часто менять режимы работ и рабочие частоты и так проще унифицировать настройку и работать на средствах связи в полевых условиях. Наличие аккумуляторной батарей емкостью не менее 2000 мАч, класс защиты минимум IP67, а еще лучше – IP68 (защита от воды), мощность передатчика от 5 Вт, с возможностью регулировки, поддержка аналоговой и цифровой связи стандарта DMR. Для автомобильной радиостанции еще нужен и источник питания. Напряжение источника питания должно соответствовать напряжению бортовой сети, а мощность блока питания нужна выше минимум на 30%, чем максимальная потребляемая мощность автомобильной радиостанции. Кроме дополнительного АКБ и зарядного устройства, не будут лишними гарнитура,

выносная кнопка PTT, запасная антенна, кабель программирования, ларингофон для работы в шумных местах – в бронетехнике или вертолете.

Порядок ношения радиостанции военнослужащим.

Вариантов ношения радиостанции при ведении боевых действий достаточно много, каждый военнослужащий с максимальным удобством для себя размещает радиостанцию на своей экипировке, но практика использования портативной радиостанции на поле боя выработала определенные рекомендации, с учетом физических свойств распространения радиоволн. Эффективность использования радиостанции во много определяется максимально эффективным излучением радиосигнала ее антенной. Важно помнить, что антенне необходимо свободное пространство и не желательно напрямую контактировать с телом человека, стальной плитой бронежилета или стволом автомата. Одно из самых оптимальных мест – размещение радиостанции на груди на лямке разгрузки/бронежилета и антенна размещена вся над плечом вне соприкосновения с телом или металлическими деталями экипировки. Если предполагается падать на грудь, радиостанцию лучше держать выше на плечо, антенной градусов под 40-45 назад. Общая эффективность радиоизлучения при работе стоя упадёт, зато сохранится приемлемая работа в положении лёжа на груди. Если военнослужащий всё время действует с рюкзаком за спиной, можно расположить радиостанцию в верхней части рюкзака или боковом его кармане с тем, чтобы антенна располагалась как можно выше, на расстоянии от тела, лучше с небольшим наклоном назад, для этого потребуется выносная микротелефонная гарнитура с кнопкой PTT. В случае размещения радиостанции на бронежилете сзади - антенна должна быть над плечом и не затеняться стальными пластинами. Выполнение этих рекомендаций военнослужащими непосредственно на поле боя, повысит эффективность радиосвязи и увеличит дальность работы радиосредств [1].

Работа с антеннами

Анализируя опыт организации тактической УКВ радиосвязи при ведении боевых действий в современных военных конфликтах, полезно использовать антенны портативных радиостанций при проведении маневра по частотным диапазонам используемых радиосредств.

Для эффективного перекрытия всего диапазона радиостанций подойдут антенны в 1/4 длины волны, это 45-50 см для VHF (136-174 МГц – длина волны 2 м) и 14-15 см для UHF (400-500 МГц – длина волны 0,7м). Четвертьволновые антенны своего диапазона более эффективны (дальность связи существенно больше), чем сверхширокополосные антенны, которые обладают сверхширокополосностью в ущерб эффективности (в следствии неоптимальной длины, потери в резистивном элементе согласования).

Антенна длиной около 40 см при правильном её исполнении работает как 1/4 на VHF и как 3/4 или 5/8 на UHF. В этом случае она будет очень узкой по частоте в диапазоне UHF и потребуется подбирать такую антенну под требуемые частоты или подбирать частоты под имеющуюся антенну. Работа

вне эффективной полосы частот резко увеличивает риск поломки радиопередатчика и сильно снижает дальность связи.

Антенны длиннее 40 см, например антенна 70-120 см, перестают работать обычным образом в диапазоне UHF и начинают работать как антенна бегущей волны, затягивая основной лепесток сигнала вверх вдоль стержня антенны. И не важно, какого типа у вас радиостанция - работая на длинную антенну, вы светите конусом примерно под 45 градусов вверх. Этот недостаток можно перевести в достоинство, наклоняя такую длинную антенну в сторону корреспондента, усилив сигнал в его сторону и уменьшив во все остальные. Для диапазона VHF антенна длиной 100-120 см будет антенной 5/8 или 3/4 и в этом диапазоне с такой антенной вышеуказанный эффект может отсутствовать или проявляться незначительно [2-3].

Пеленгация с помощью радиостанции.

Практический опыт «грубой» пеленгации работающего на передачу средства радиосвязи широко применяется военнослужащими ряда воюющих государств.

При использовании на радиостанции антенны, например ленты длиной 100-120 см, при расположении радиостанции на бронежилете сзади, необходимо согнуть антенну вперёд буквой П, самый кончик антенны зафиксировать изолятором (верёвка, капроновая стяжка) на груди. Важно, чтобы антенна не касалась головы военнослужащего. При таком размещении наиболее сильное распространение радиосигнала будет вперёд, самое слабое – назад. Таким образом в условиях леса или темноты можно определить направление на вашего корреспондента или на радиста противника.

Если имеется четвертьволновая антенна (45 см VHF или 15 см UHF) и необходимо определить направление на источник радиопередачи, необходимо поставить радиостанцию горизонтально на уровне груди антенной горизонтально от себя. Затем вращаясь вокруг вертикальной оси, определить сторону, откуда идёт сигнал. Со спины передача приниматься не будет или будет сильно ослаблена. Медленно вращаясь влево-вправо, можно определить направление максимального затухания между двумя одинаковыми направлениями сильного приёма. В этом положении антенна указывает направление на источник сигнала [4-6].

Шифрование радиосигнала.

Ключевые требования к тактической системе военной связи – помехоустойчивость и скрытность связи. С развитием средств РЭР и РЭБ, а также с появлением в гражданском секторе многочисленных пеленгаторов, спектроанализаторов и других технических, относительно дешевых и простых в использовании средств, очень остро стоит вопрос о защите тактических УКВ радиосетей от вскрытия. Решением является использование радиостанций с технологией псевдослучайной перестройкой рабочей частоты и функцией «битного» шифрования.

Средства УКВ радиосвязи с реализованной функцией «битного» шифрования используются повсеместно, однако при выборе средства

радиосвязи нужно понимать, что имеющееся на многих УКВ радиостанциях 40, 64, 128 и 256-битное шифрование не указывает уровня криптостойкости шифрования. Количество бит, это разрядность ключа, указывающая на количество двоичных разрядов в ключе, каково количество возможных вариантов ключа – 2 в 40-й степени, в 64-ой, в 128-й, в 256-й.

Помимо битности шифрования, необходимо обращать внимание на алгоритм шифрования, который и определяет криптостойкость. Другими словами, сколько и каких математических операций производится при шифровании информации. Чем меньше операций и чем они проще - тем проще вскрывается шифр. Чем больше операций и чем они сложнее, тем мощнее нужен процессор радиостанции, чтобы успевать проворачивать процесс шифровки-дешифровки в реальном времени.

Для примера алгоритм шифрования XOR, даже с длинным ключом - вскрывается сравнительно просто, потому что не требует многого от процессора станции, а алгоритм шифрования AES, распространённый мировой стандарт, более требователен к процессору станции и, соответственно, труднее вскрывается.

Развитие средств цифровой радиосвязи заставляет обращать внимание на вопросы скрытого управления подразделениями с отхождением от «классического» понимания этого вопроса. Например радиостанции, работающие на основе стандартов радиосвязи DMR, APCO-25, TETRA используют уникальные идентификаторы (ID) для работы в своих радиосетях, тогда как многие средства РЭР способны определять данные идентификаторы, что позволяет в дальнейшем при не смене идентификаторов этих радиостанций в течении длительного времени, вскрывать систему управления, с обеспечением точной адресной привязки конкретных радиостанций к конкретным должностным лицам, командирам, расчетам и т.д. Таким образом, в комплекс мероприятий по скрытому управлению необходимо вносить вопросы периодичности смены ID- номеров УКВ радиостанций.

В ряде современных конфликтов наблюдались возможности технических средств РЭР многих государств вскрывать систему управления противника в тактической зоне ведения боевых действий, насыщенной УКВ радиостанциями с 64 бит шифрованием, также наблюдалась возможность удалённо ликвидировать радиостанции с 256-битным шифрованием. Нужно понимать, что «битное» шифрование не дает необходимый уровень помехозащищенности, данную проблему решает в какой-то степени технологи ППРЧ, но и тут имеются свои ньюансы.

Средства радиосвязи с функцией ППРЧ характеризуются скоростью скачков частоты в секунду (радиостанции фирм Harris и Aselsan – до 1 500 скачков с секунду, Азарт – до 20000 скачков в секунду), однако помехоустойчивость ППРЧ радиоканала определяется тем, как выполнена синхронизация. Если синхронизация нарушается, то система связи полностью выходит из строя. Синхронизация – самое уязвимое место ППРЧ радиосистем, поэтому методу синхронизации должно уделяться наиболее пристальное

внимание. Пакеты синхронизации отличаются от информационных пакетов, нарушают их псевдослучайный характер и становятся наиболее привлекательной мишенью для средств РЭП. Максимальная помехоустойчивость достигается при синхронизации по информационному сигналу без применения синхроимпульсов. Только в этом случае передаваемый поток данных является псевдослучайным, и все пакеты равноценны и равновероятны. Требование к псевдослучайному характеру ППРЧ сигнала имеет более важное значение, чем скорость скачкообразного изменения частоты в секунду [7-11].

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1 Оптимальное размещение и ношение средств радиосвязи [Электронный ресурс].URL: https://forum.guns.ru/forummessage/7/2218027.html (дата обращения 07.03.2024);

2 Антенны для радиостанций [Электронный ресурс].URL: https://kbberkut.ru/stati-o-racijah-i-radiosvjazi/ant.htmlЭлектронный ресурс: https://helpiks.org/4-94826.html (дата обращения 07.03.2024);

3 Факты о расстоянии: каков диапазон для радио [Электронный ресурс].URL: - http://m.ru.ecomeradio.com/info/the-facts-about-distance-what-s-the-range-for-65068457.html (дата обращения 07.03.2024);

4 [Электронный ресурс].URL: https://habr.com/ru/articles/397175/(дата обращения 07.03.2024);

5 [Электронный ресурс].URL: https://investim.guru/otvety/primery-pelengov-shemy-i-obyasneniya(дата обращения 07.03.2024);

6 [Электронныйресурс].URL:https://moluch.ru/archive/472/104408/(дата обращения 07.03.2024);

7 Шифрование и разведзащищенность https://combat-center.ru/blog/detail/SHIFR/;

8 Шифрование в радиостанциях [Электронный ресурс].URL: https://dzen.ru/a/ZRgfIHavM0Y2iLGd;

9 FHSS ППРЧ [Электронный ресурс].URL: https://wiki.rusmonitor.ru/FHSS_%D0%9F%D0%9F%D0%A0%D0%A7;

10 Помехоустойчивость приема сигналов с ППРЧ [Электронный ресурс].URL: https://conf-ntores.etu.ru/assets/files/2023/sbornik-23/155-157.pdf;

11 Военный ордена Жукова университет радиоэлектроники, материалы II Всероссийской научно-практической конференции «Проблемы и основные направления развития радиоэлектроники и образовательного процесса подготовки специалистов радиотехнических систем специального назначения» 7–8 ноября 2019 года. Из статьи М. Ю. Мамона «Направления развития линий связи с псевдослучайной перестройкой рабочей частоты».

УДК 623.61

КВ РАДИОСВЯЗЬ - КАК НЕОТЬЕМЛЕМАЯ СОСТАВЛЯЮЩАЯ СЕТИ РАДИОСВЯЗИ В СИСТЕМЕ СВЯЗИ

ЖАНТЛЕСОВ А.У., *полковник*
МАРКУС В.А., *подполковник*

Главное командование Национальной гвардии Республики Казахстан,
г. Астана, Республика Казахстан

Аннотация. В статье рассмотрена необходимость и значимость дальнейшего использования КВ радиосвязи при построении и развитии надежных и экономически эффективных систем военной связи, с учетом применения имеющихся на сегодняшний день современных способов и механизмов, повышающих ее качество и устойчивость.

Данная научная статья опубликована в рамках выполнения научно-исследовательской работы ИРН AP148029/0222 «Разработка оборудования для создания национальной системы военной радиосвязи».

Ключевые слова: сети подвижной радиосвязи, КВ радиосвязь, сети связи, ионизация атмосферы, резерв.

Түйіндеме. Мақалада әскери байланыстың сенімді және экономикалық тиімді жүйелерін құру және дамыту кезінде ҚТ радиобайланысын одан әрі пайдаланудың қажеттілігі мен маңыздылығы, оның сапасы мен тұрақтылығын арттыратын қазіргі заманғы әдістер мен механизмдерді қолдануды ескере отырып қарастырылады.

Бұл ғылыми мақала ЖТН AP148029/0222 «Ұлттық әскери радиобайланыс жүйесін құруға арналған жабдықтарды әзірлеу» ғылыми-зерттеу жұмысын орындау шеңберінде жарияланды.

Түйінді сөздер: жылжымалы радиобайланыс желілері, ҚТ радиобайланыс, байланыс желілері, атмосфераны иондау, резерв.

Abstract. The article considers the necessity and importance of further use of HF radio communications in the construction and development of reliable and cost-effective military communications systems, taking into account the use of modern methods and mechanisms available today that increase its quality and stability.

This scientific article was published as part of the research work of IRN AP148029/0222 «Development of equipment for the creation of a national military radio communication system».

Key words: mobile radio networks, HF radio communications, communication networks, atmospheric ionization, reserve.

Радиосвязь на сегодняшний день остается важнейшим средством управления войсками. В условиях современного маневренного скоротечного

боя с резкой сменой обстановки и при отсутствии сплошной линии соприкосновения войск надежная качественная радиосвязь является гарантией устойчивого и гибкого управления войсками. Основным преимуществом радиосвязи является ее мобильность, способность передавать информацию различного характера в движении, не ограничивая свободу действий платформ, на которых установлены радиостанции.

В настоящее время во многих странах мира ведутся работы по переоснащению систем связи ВС на цифровые системы передачи информации, в основе которых применяются современные информационные и телекоммуникационные технологии, что несомненно приводит к структурным, топологическим и технологическим изменениям в построении линейной и узловой составляющих интегрированной цифровой системы связи.

Для организации сетей связи требуется создание высокоскоростной интегрированной цифровой системы связи в составе транспортной сети и сетей доступа за счет цифровизации и внедрения современных телекоммуникационных технологий, позволяющих обеспечить своевременное и с надлежащим уровнем качества предоставление услуг служб электросвязи, определяемых современными технологиями управления. Немаловажная роль отводится сети подвижной радиосвязи (СПРС), которая предоставляет мобильным абонентам возможность непрерывного и устойчивого обмена информацией при их нахождении в подвижных объектах (КШМ, бронеобъектах, автомобилях) и при перемещении в пешем порядке. В отличии от традиционно применяемых для этих целей сетей прямой (командной) радиосвязи СПРС позволяет на комплексной основе использовать в интересах мобильных абонентов возможности стационарных и полевых вторичных сетей дальней связи, а также многоканальных радиорелейных, спутниковых, тропосферных и проводных средств первичной сети. Обладая качественно новыми способностями, СПРС предоставляет своим пользователям возможность непосредственного доступа к общему информационному пространству в любой точке обслуживаемой территории, которая формируется зонами электромагнитной доступности стационарных и подвижных базовых станций (БС). В современных условиях практически все представители силового блока, формируя научно-техническую политику, уделяют достаточно серьезное внимание вопросам обеспечения своих абонентов подвижной радиосвязью, полагаясь, как правило, на собственные возможности при ее практической реализации. Следствием такого подхода является создание разнотипных ведомственных систем, которые не обеспечивают возможности их совместной эксплуатации. Это затрудняет оперативное взаимодействие мобильных формирований силовых ведомств при совместном выполнении специальных мероприятий. Эксплуатируемые на сегодняшний день СПРС характеризуются низкой тактико-технико-экономической эффективностью, поскольку уже не в полной мере удовлетворяют предъявляемым к ним требованиям по перечню предоставляемых абонентам услуг, пропускной

способности, времени установления соединения и другим потребительским свойствам.

Анализ эксплуатационно-технических характеристик существующих отечественных СПРС военного назначения показывает, что на сегодняшний день они не позволяют в полной мере реализовать потенциальные возможности данного вида связи по целому ряду причин. Во-первых, стационарные и полевые компоненты СПРС не объединены в единую систему, что не позволяет устанавливать соединения с абонентами, местоположение которых априорно неизвестно. Во-вторых, в региональной системе ввиду недостаточной ее разветвленности чрезвычайно мал процент перекрытия зонами связи территории, в пределах которой функционируют ее потребители. В - третьих, ограниченные технические возможности и относительно большие массогабаритные характеристики возимых и переносных спутниковых средств не позволяют обеспечить требуемую непрерывность связи с мобильными абонентами, а также создают определенные трудности в их эксплуатации. В-четвертых, в настоящее время для доступа в различные вторичные сети используются разнотипные средства связи, что предопределяет необходимость наличия у абонентов нескольких терминальных устройств или ограничивает их возможности.

Наиболее существенными недостатками радиосвязи являются: возможность обнаружения сигнала работающей радиостанции и его подавления; ограниченность полосы пропускания; возникновение взаимных помех из-за высокой плотности радиостанций, работающих в одном диапазоне.

В современном мире для обеспечения достаточно уверенной передачи информации на больших территориях применяют различные системы и технические средства связи, обеспечивающие в совокупности достаточно высокую надежность информационных сетей связи страны. Несмотря на то, что в условиях быстрого развития высокоэффективных кабельных, радиорелейных и спутниковых линий связи удельный вес КВ радиосвязи снизился, сохраняется необходимость ее технического совершенствования. КВ радиосвязь играет важную роль, как средство ведомственной, межведомственной, магистральной внутренней и международной, зоновой, подвижной и производственно-диспетчерской связи общего пользования. Радиосвязь в КВ диапазоне обеспечивает следующие службы: магистральную, зоновою, и местную радиосвязь, сеть радиовещания, службу стандартных частот, служебные линии для земных станций спутниковой связи, авиационную связь, морскую связь, службу радиосвязи железнодорожного транспорта, военную связь, межсудовую связь в морском флоте, различные наземные подвижные радиослужбы, любительскую радиосвязь и другие. За долгие годы существования КВ радиосвязи неоднократно высказывалось мнение, что другие виды связи полностью ее вытеснят. Действительно, во многих странах автоматизированная сеть связи строится на основе высокоэффективных кабельных и радиорелейных магистралей. Развитие волоконно-оптических линий связи снимает многие ограничения в увеличении пропускной способности сетей связи. Проблемы

связи с малонаселёнными территориями, отдаленными от промышленных центров труднопроходимой местностью, смогут решать спутниковые системы связи. Быстро растет роль спутников и в сетях подвижной связи. В итоге в условиях развитой и нормально функционирующей ведомственной, межведомственной, общегосударственной и межгосударственной системы связи удельный вес КВ радиосвязи в общем объеме передачи информации уменьшается. Однако, вопрос о ликвидации в обозримом будущем, КВ радиосвязи не стоит практически ни в одной стране мира, напротив, наряду с тем, что последние годы характеризуются бурным развитием микроволновых средств дальней связи, увеличивается внимание к технической реконструкции КВ радиосвязи [1]. Основанием для этого является правильная оценка КВ радиосвязи, учитывающая ее технический потенциал и экономическую эффективность, а также ее стратегическую роль, как необходимого резерва. К тому же радиосвязь в КВ диапазоне, наряду со спутниковой остается одним из видов межрегиональной связи, как экономичный способ организации дальней связи. Системы связи в микроволновых диапазонах экономичны только при одновременной передаче нескольких сотен и тысяч телефонных каналов. В этом случае стоимость одного телефонного канала, определенная, как результат деления общих капитальных и эксплуатационных расходов, затраченных на систему связи, на число каналов, оказывается сравнительно небольшой. В многих случаях не требуется большого числа каналов. При этом КВ радиоаппаратура для передачи одного-двух телефонных разговоров или работы нескольких десятков терминалов передачи данных обходится сравнительно недорого. Оборудование автоматизированных центров можно размещать в защищенных, упрощённых и удешевлённых помещениях. Тем самым отпадает необходимость в жилых и подсобных помещениях. Однако, автоматизация и устранение обслуживающего персонала, требует высокой надежности и резервирования, как основного, так и дополнительного оборудования. Так же, несмотря на многочисленность радиостанций, сохраняется резерв в использовании пропускной способности КВ диапазона. Ряд свойств КВ радиосвязи делает ее в определённых условиях незаменимой. Например, повреждение отдельных промежуточных станций радиорелейных линий при массовых беспорядках, боевых действиях, стихийных бедствиях или по другим причинам, а также выход из строя спутника могут привести к большим трудностям в работе общегосударственной сети связи или к полному нарушению ее функционирования на значительных участках территории. В аналогичных же условиях радиосвязь может быть восстановлена в кротчайшие сроки при наименьших затратах. При катастрофическом возникновении сильной ионизации атмосферы КВ радиосвязь, нарушается не в большей мере, чем другие радиотехнической системы, адаптируется же и восстанавливается гораздо быстрее [2]. Следует иметь ввиду также то, что КВ радиосвязь играет определенную роль в обеспечении спутниковой связи наземными средствами: служебной, сигнализацией и синхронизацией. Учитывая, что КВ радиосвязь

широко применяется в ведомственных сетях связи, она остается важным звеном комплексной общегосударственной сети связи страны.

Связь в КВ диапазоне на больших расстояниях с помощью мобильных станций небольшой мощности во многих случаях имеет значительное экономическое и практическое преимущество перед проводной и радиорелейной связью. Однако, из-за замираний сигнала при ионосферной распространении и наличия «зон молчания» надежность канала КВ связи может быть недостаточно высокой, а в отдельных случаях и очень низкой. Если команды управления в большой региональной системе связи передавать только по КВ каналам, то потеря информации при передаче могут быть существенными. Именно поэтому КВ радиосвязь широко применяют в качестве резервной для более надежных систем связи. Роль ее существенно возрастает в условиях, когда не исключена возможность чрезвычайных ситуаций. Живучесть КВ связи в этих условиях намного выше, чем проводной и радиорелейной.

КВ радиосвязь отличается сложностью и нестационарностью условий распространения радиоволн и помеховых ситуаций. Для обеспечения устойчивой и качественной ионосферной радиосвязи в КВ диапазоне требуется применение сложных сигнально-кодовых конструкций, адаптивных устройств различного уровня и всех современных достижений цифровой обработки сигнала. Адаптация предполагает автоматическую смену используемых длин волн для перехода в диапазоны с лучшим распространением и минимальными помехами; регулирование мощности передатчиков для улучшения условий электромагнитной совместимости и экономии электроэнергии; применения антенн с автоматической регулировкой диаграммы направленности; повышение устойчивости приема; прием с различными видами разнесения; использование помехозащитного кодирования и информационной обратной связи; передачу по параллельным каналам и т.д.

Несмотря на широкое распространение высокоскоростных современных систем передачи информации радиосвязь в КВ диапазоне благодаря ряду уникальных свойств остается одним из важнейших видов связи, используемой многими ведомствами службами и организациями. Большое число работающих радиостанций, значительные по уровням и разнообразные по видам помехи, замирания сигналов, ограниченность диапазона затрудняют его использование. Тем не менее, имеется значительный ресурс пропускной способности КВ радиосвязи.

В последнее десятилетие КВ радиосвязь загружена передачей информации только на 10-15 %. Причин тут несколько. Одна из причин-увеличение объема передачи информации по другим каналам связи, в частности спутниковой. Однако расчеты и опыты показывают, что стоимость канала спутниковой связи на порядок дороже КВ связи. Вторая причина – устаревшее представление о низкой надежности ионосферной связи. Третья причина – распространившаяся мода на «престижные» быстродействующие

каналы связи, хотя для решения очень многих задач это быстродействие не требуется и только увеличивает затраты.

Таким образом современный этап развития КВ связи характеризуется совершенствованием ее технических средств, целью которого должно быть достижение максимальной степени автоматизации и адаптации к изменяющимся характеристикам каналов передачи информации [3]. Автоматическое управление радиосвязью потребовало разработки автоматизированных радиоприёмных и радиопередающих центров. Автоматизация радиоцентров повышает надежность радиосвязи, предотвращает или сокращает перерывы связи, сокращает время подготовки аппаратуры к работе, делает систему более экономичной, особенно при длительном отсутствии нагрузки и работе в ждущем режиме. Современная КВ радиосвязь должна быть полностью автоматизированной с адаптацией системы к изменяющимся характеристикам каналов передачи информации.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1 Селиванова С.П., Сомов В.Г. Анализ факторов, влияющих на качество радиосвязи при распространении радиоволн в нестационарной диспергирующей анизотропной среде. // Актуальные проблемы авиации и космонавтики, 2015. – Т.1. – С.247-249.

2 Селиванова С.П., Сомов В.Г. Повышение качества радиосвязи в КВ-диапазоне. // Актуальные проблемы авиации и космонавтики, 2015. – Т.1. – С. 250-252.

3 Коршунов Д.В., Васильев А.С., Лапшин Э.В. Анализ факторов, влияющих на качество радиосвязи в КВ-диапазоне. // Труды Международного симпозиума «Надежность и качество», 2018. – Т.2. – С.372-373.

УДК 621.396

ДИСТАНЦИОННОЕ УПРАВЛЕНИЕ РАДИОСТАНЦИЯМИ С ПОМОЩЬЮ ДОПОЛНИТЕЛЬНОГО ПОЛЕЗНОГО УСТРОЙСТВА

ИСТИМЕСОВ М.Б., *начальник цикла БПСВ, подполковник запаса*
КУЗМИТСКИЙ С.В.

Военная кафедра НАО «КарТУ имени Абылкаса Сагинова»,
город Караганда, Республика Казахстан

Аннотация. В статье рассмотрены принципы дистанционного управления радиостанцией. Рассмотрены преимущество использования дистанционного управления радиостанцией, работы приемо-передающего трактов, способы соединения при дистанционной управлении маломощной радиостанцией.

Ключевые слова: радиосвязь, дистанционное управления, радиостанция, антенна, сигнал.

В области радиосвязи происходят постоянные изменения по вопросу работы на технике радиосвязи, технологии идут вперед, изобретаются все новые и новые системы радиосвязи, которые в цене являются недоступными каждому радиолюбителю, кроме этого мало приобрести радиостанцию нужно к ней приобрести и аксессуары, для организации удобства при эксплуатации и выполнения определенных функций, либо для сопряжения с аксессуарами более старого парка, по причине работоспособности последних.

Поэтому предлагаем вашему вниманию рассмотреть полезное приспособление для организации дистанционного управления радиостанцией нового парка с помощью телефонного аппарата войскового образца типа ТА-57 (телефонный аппарат модификации 1957 года), который успешно эксплуатируется многими специалистами связи и состоит на вооружении многих армий мира.

Что понимается под дистанционным управлением радиостанцией?

Дистанционным управлением называют такой режим работы радиостанции, при котором прием, передача, а также перевод ее с приема на передачу и обратно осуществляется с пункта управления, находящегося на некотором удалении от радиостанции. Этот вынесенный пункт может быть местом управления несколькими радиостанциями.

В каких случаях целесообразно использовать режим дистанционного управления радиостанцией?

Как известно, для повышения дальности и надежности связи антенну радиостанции (особенно УКВ радиостанции) желательно располагать на открытом возвышенном месте.

Пункты же управления обычно находятся в глубоких подвалах, блиндажах или в закрытых помещениях зданий, где непосредственное

расположение антенн радиостанций невозможно из-за большого затухания радиоволн.

Применение режима дистанционного управления позволяет места расположения радиостанции и пункта управления выбирать в зависимости от обстановки. Кроме того, при работе на пункте управления нескольких радиостанций желательно удалять их как одну от другой, так и от пункта управления.

Делают это для того, чтобы не демаскировать пункт управления и исключить взаимные помехи между радиостанциями, поскольку одновременно одни радиостанции могут работать на передачу, а другие на прием.

Возможны и другие случаи использования режима дистанционного управления радиостанциями.

При переводе радиостанций в режим дистанционного управления дальность их действия не уменьшается.

Принцип дистанционного управления. К системе дистанционного управления маломощной радиостанцией обычно предъявляются требования:

– пункт управления должен соединяться с радиостанцией кабелем с числом проводов не более двух;

– соединительным кабелем может быть обычный полевой кабель;

– в качестве устройства для дистанционного управления на пункте управления необходимо использовать обычный полевой телефонный аппарат с добавлением к нему несложной приставки.

При работе с вынесенного пункта по радиоприем корреспонденций может вестись на телефон микротелефонной трубки телефонного аппарата типа ТА-57, а передача – с помощью микрофона той же трубки. От телефонного аппарата производится также перевод радиостанции с приема на передачу и обратно при помощи посылок постоянного тока. Следовательно, по двухпроводной линии протекает одновременно постоянный ток и переменный ток звуковой частоты.

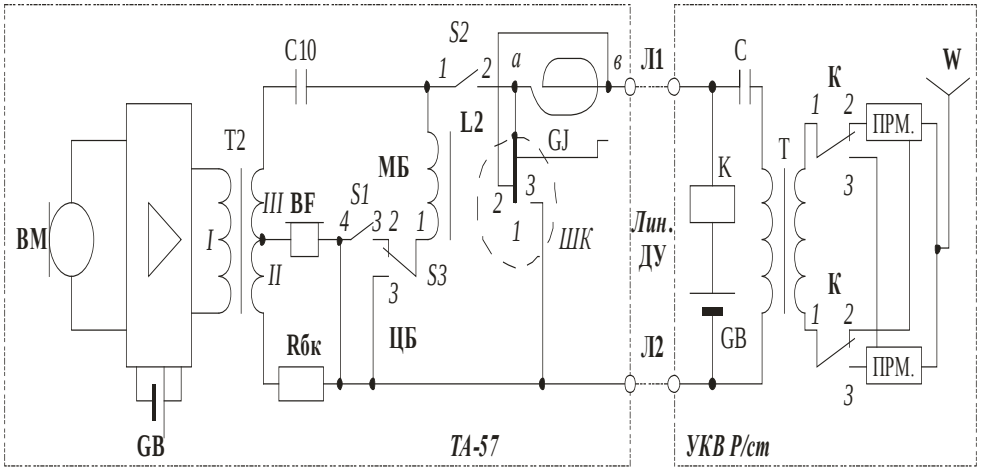


Рисунок 1 – Цепь дистанционного управления радиостанцией

Дистанционное управление радиостанцией обеспечивается разговорным клапаном S1 микротелефона. При этом переключатель S3 устанавливается в положение МБ. В радиостанции к проводам линии подключен источник питания GB и переключающее реле К. При нажатии разговорного клапана S1 его контактами 3-4 создается цепь срабатывания реле к радиостанции:

«Плюс» батареи GB радиостанции, обмотка реле К, провод «а» линии, клемма Л1, вывод индуктора GJ «а», контакты 2-1 переключателя S2, обмотка дросселя L2, контакты 1-2 переключателя S3, контакты 3-4 переключателя S1, клемма Л2, провод «в» линии, «минус» батареи GB радиостанции.

В результате радиостанция переключается в режим передачи.

При отжатом разговорном клапане S1 микротелефона разговорная цепь размыкается, и радиостанция переключается в режим приема. Разговор через радиостанцию ведется в симплексном режиме. Цепи передачи и приема разговора не отличаются от уже рассмотренных выше.

На всех радиостанциях при управлении происходит один и тот же физический процесс, при нажатии на переговорный клапан (тангенту) микротелефонной гарнитуры срабатывает пара управления, которая ставит радиостанцию на передачу и через микрофон модулируется сигнал и передается в эфир, при отпускании тангенты радиостанция переходит в режим приема, поэтому соответственно для работы радиостанции на прием и передачу необходимы пара, отвечающая за прием сигнала.

Пара, отвечающая за передачу сигнала и пара, отвечающая за управления радиостанцией, кроме этого, радиостанция может управятся по четырех проводной схеме, где управление радиостанцией происходит по одному проводу приема, по одному проводу передачи и одному проводу управления относительно корпусного провода часто такая схема управления встречается на большинство радиостанциях.

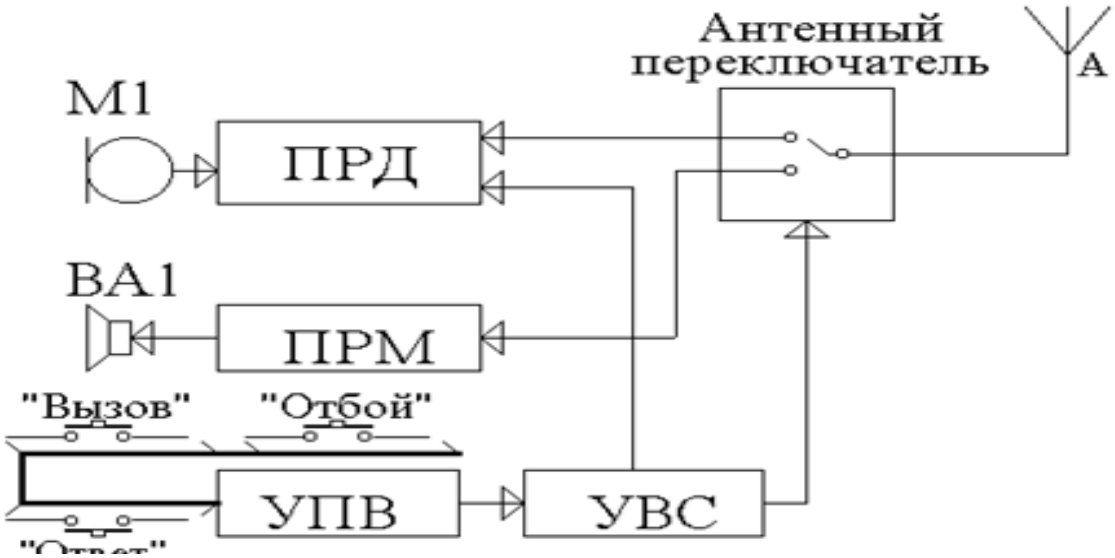


Рисунок 2 – Структурная схема радиостанции

Управление любой радиостанцией можно организовать без установки дополнительного оборудования, от выносного телефонного аппарата войскового образца ТА-57 с помощью изготовленного полезного приспособления блока управления радиостанцией, состоящего из доступных и дешевых элементов:

– Реле РЭС-22 паспорт РФ4500131-2шт (РФ4,525,023-00; РФ4,523,023-07)

– Емкость МБТО-2 1мкФ на 300В-2шт.

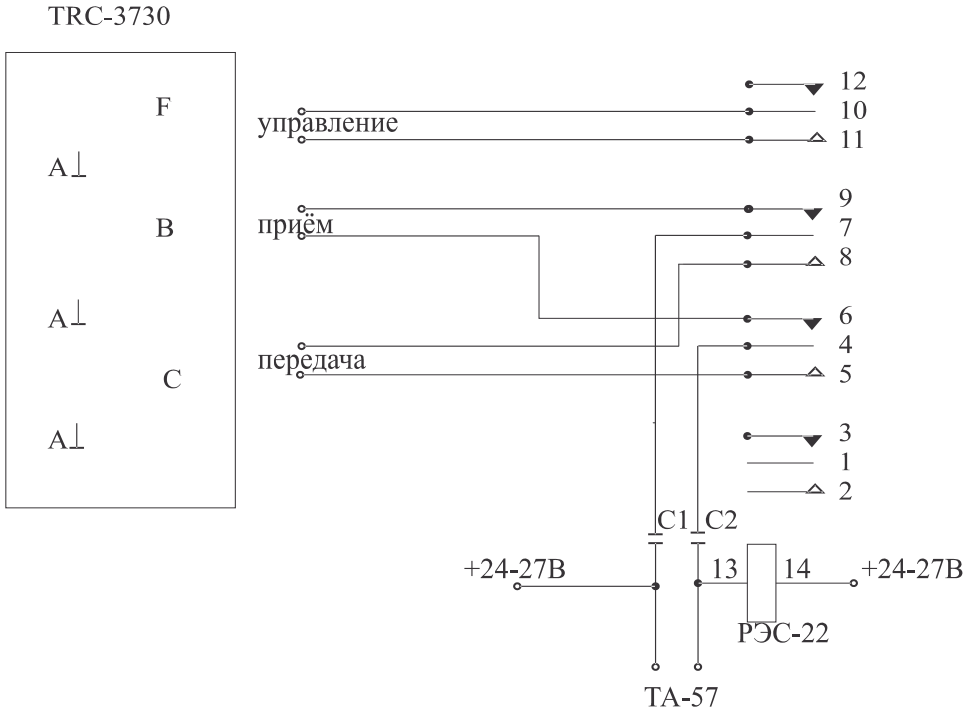


Рисунок 3 – Схема блока

Управление радиостанцией происходит по проводу «F» относительно корпусного провода «А», приём по проводу «В» относительно корпусного провода «А» и передача по проводу «С» относительно провода «А». Электрическое питание осуществляется от источника 24-27 В, при чем полярность значения не имеет.

Приемный тракт осуществляется следующим образом:

По цепи от разъема радиостанции по проводу «В» относительно корпусного провода «А» подается на контакты реле 6, 9 при отжатой тангенты на телефонном аппарате ТА-57 контакты постоянно замкнуты с контактами 7 и 4 реле.

Передающий тракт осуществляется следующим образом:

При нажатии тангенты на телефонном аппарате ТА-57 создается шлейф по которому питание подается на реле и происходит его работа при котором происходит соединение контактов 4 и 5, 8 и 7 тракта передачи и контактов 10 и 11 линии управления, радиостанция переходит из режима прием в режим передача.

Таким образом можно организовать дистанционное управления различными радиостанциями старого и нового парка, данная схема управления успешно эксплуатируется на нашей военной кафедре в частности нами был собран тренажер командно - штабной машины где вместо блока коммаутации проводной связи была использованна данная схема, для обучения наших слушателей работе на средствах связи.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

Техническое описание и инструкция по эксплуатации радиостанции КВ диапазона TRC – 3730.

УДК 621.394.6

СЕТЬ MPLS В СОЗДАВАЕМОЙ СИСТЕМЕ РАДИОСВЯЗИ СИЛОВЫХ ВЕДОМСТВ РЕСПУБЛИКИ КАЗАХСТАН

ЗВЕРЕВ Н.Н., *магистр, майор*

Войсковая часть 29990, г.Астана, Республика Казахстан

Аннотация. Данная статья посвящена сети MPLS и её интеграции в системе радиосвязи силовых ведомств Республики Казахстан. Рассмотрены преимущества сети MPLS и применение сетей в построении перспективный системы радиосвязи.

Ключевые слова. Система связи, телекоммуникация, коммутация, передача данных.

Анализ современных боевых действий и требуемой для их ведения системы управления предопределяет необходимость построения системы связи, которая должна обеспечить создание инфокоммуникационной инфраструктуры, которая объединит все органы и пункты управления и будет способна предоставить необходимые информационные ресурсы и сервисы должностным лицам — от командира подразделения до солдата и единицы техники.

Одним из возможных способов создания подобной сети связи является сеть радиосвязи на основе разрабатываемых программно-аппаратных комплексов радиосредств, как единой интегрированной сети связи, включающей сеть прямых связей, распределенную сеть с ячеистой топологией и сеть радиодоступа.

В современных условиях существенно возрастает роль системы связи при управлении группировками войск (сил) в условиях проведения боевых (специальных) операций. Система связи должна уметь быстро реагировать на изменения обстановки, динамично изменяя при этом свою структуру, а также совершенствовать способы построения и режимы работы, выполняя главную задачу — обеспечение информационного обмена в системе управления [1].

По мере разработки и оснащения органов управления, частей и подразделений силовых ведомств республики Казахстан перспективными цифровыми средствами связи, развитие системы связи должно быть направлено на построение сетевой инфраструктуры и сопряжение вновь принимаемых на вооружение средств радиосвязи с действующими комплексами и средствами радиосвязи.

Инфраструктурный подход к построению перспективной системы радиосвязи позволит развернуть многоуровневую эшелонированную инфокоммуникационную сеть и также сформировать единое информационное пространство всех силовых ведомств. При этом повысится управляемость, пропускная способность, устойчивость, доступность, разведзащищенность сети и непрерывность управления.

Для оптимального использования ресурсов такой сети связи необходимо использовать достаточно сложные механизмы межканальной маршрутизации и ретрансляции информации в единой сети с учетом доступного ресурса и специфики отдельных подсетей связи [2, 3], а также иерархическую систему адресации понятную для пользователей (должностных лиц) и обеспечивающую однозначное определение пути прохождения информации между абонентами [4].

При построении перспективной самоорганизующейся радиосети необходимо соблюдать требования к обеспечению качества услуг, предоставляемых должностным лицам различных звеньев управления, а также к обеспечению высокой степени надежности функционирования данной радиосети.

Для решения этих задач в создаваемой сети связи целесообразно использовать многопротокольную коммутацию по меткам **MPLS.**

MPLS (англ. *multiprotocol label switching* — многопротокольная коммутация по меткам) — механизм в высокопроизводительной телекоммуникационной сети, осуществляющий передачу данных от одного узла сети к другому с помощью меток.

MPLS является масштабируемым и независимым от каких-либо протоколов механизмом передачи данных. В сети, основанной на MPLS, пакетам данных присваиваются метки. Решение о дальнейшей передаче пакета данных другому узлу сети осуществляется только на основании значения присвоенной метки без необходимости изучения самого пакета данных. За счёт этого возможно создание сквозного виртуального канала, независимого от среды передачи и использующего любой протокол передачи данных [5].

История появления MPLS

В 1996 году группа инженеров из фирмы «Ipsilon Networks» разработала «Протокол управления потоком» (англ. Flow management protocol). Основанная на этом протоколе технология «коммутации IP-пакетов», работающая только поверх упрощенной сети, не получила коммерческого успеха.

Фирма «Cisco Systems» разработала похожую технологию «коммутации на основе тегов» (англ. ***t**ag **s**witching*), не ограниченную передачей поверх сети.

Данная технология, впоследствии переименованная в «коммутацию на основе меток» (англ. ***l**abel **s**witching*), была закрытой разработкой фирмы «Cisco». Позднее она была передана в специальную комиссию интернет-разработок (IETF) для открытой стандартизации [5].

Технология MPLS основана на обработке заголовка MPLS, добавляемого к каждому пакету данных. Заголовок MPLS может состоять из одной или нескольких «меток». Несколько записей (меток) в заголовке MPLS называются стеком меток.

Формат записи в стеке меток			
32 бита			
20 бит	3 бита	1 бит	8 бит
Label	TC	S	TTL

Каждая запись в стеке меток состоит из следующих четырёх полей:

- значение метки (англ. *label*); занимает 20 бит;
- поле «класс трафика» (англ. ***T**raffic **c**lass*); используется для реализации механизмов качества обслуживания (QoS) и явного уведомления о перегрузке, занимает 3 бита;
- флаг «дно стека» (англ. *bottom of stack*); если флаг установлен в 1, то это означает, что текущая метка последняя в стеке; занимает 1 бит;
- поле TTL (англ. ***T**ime **t**o **l**ive*); используется для предотвращения петель MPLS коммутации; занимает 8 бит.

Сети построенные с применением технологии MPLS является масштабируемым и независимым от каких-либо протоколов механизмов передачи данных. В сети, основанной на MPLS, пакетам данных присваиваются метки. Решение о дальнейшей передаче пакета данных другому узлу сети осуществляется только на основании значения присвоенной метки без необходимости изучения самого пакета данных. За счёт этого возможно создание сквозного виртуального канала, независимого от среды передачи и использующего любой протокол передачи данных.

Построенная по технологии MPLS сеть, является иерархической и представляет собой двухуровневую архитектуру. Иерархия состоит из первого уровня – опорной сети (ядра сети) с коммутирующими по меткам маршрутизаторами LSR (P) и второго уровня - периферийной или пограничной части сети провайдера, к которым подключаются сети пользователей транспортных услуг [6].

В MPLS-маршрутизаторе пакет с MPLS-меткой коммутируется на следующий порт после поиска метки в таблице коммутации вместо поиска по таблице маршрутизации. При разработке MPLS поиск меток и коммутация по меткам выполнялись быстрее, чем поиск по таблице маршрутизации или RIB (англ. ***R**outing **i**nformation **b**ase* — информационная база маршрутизации), так как коммутация может быть выполнена непосредственно на коммутационной фабрике вместо центрального процессора. Маршрутизаторы, расположенные на входе или выходе MPLS-сети, называются LER (англ. ***L**abel **e**dge **r**outer* – граничный маршрутизатор меток). LER на входе в MPLS-сеть добавляют метку MPLS к пакету данных, а LER на выходе из MPLS-сети удаляет метку MPLS из пакета данных. Маршрутизаторы, выполняющие маршрутизацию пакетов данных, основываясь только на значении метки, называются LSR (англ. ***L**abel **s**witching **r**outer* — коммутирующий метки маршрутизатор). В некоторых случаях пакет данных, поступивший на порт

LER, уже может содержать метку, тогда новый LER добавляет вторую метку в пакет данных. Метки между LER и LSR распределяются с помощью LDP (англ. ***L**abel **d**istribution **p**rotocol]]* – протокол распределения меток) Для того, чтобы получить полную картину MPLS-сети, LSR постоянно обмениваются метками и информацией о каждом соседнем узле, используя стандартную процедуру. Виртуальные каналы (туннели), называемые LSP (англ. ***L**abel **s**witch **p**ath* – пути коммутации меток), устанавливаются провайдерами для решения различных задач, например, для организации VPN или для передачи трафика через сеть MPLS по указанному туннелю.

Достоинства технологии MPLS

1. MPLS позволяет достаточно легко создавать виртуальные каналы между узлами сети;

2. Технология позволяет инкапсулировать различные протоколы передачи данных;

Инкапсуляция – *механизм, который объединяет данные и методы, манипулирующие этими данными, и защищает и то и другое от внешнего вмешательства или неправильного использования. Когда методы и данные объединяются таким способом, создается объект.*

3. Независимость от особенностей технологий канального уровня;

4. Отсутствие необходимости поддержания нескольких сетей второго уровня, необходимых для передачи различного рода трафика. По виду коммутации MPLS относится к сетям с коммутацией пакетов.

5. Технология MPLS была разработана для организации единого протокола передачи данных как для приложений с коммутацией каналов, так и приложений с коммутацией пакетов.

6. MPLS может быть использован для передачи различного вида трафика, включая IP-пакеты, ячейки ATM, фреймы SONET/SDH и кадры Ethernet.

Исходя из рассмотренных выше материалов следует, что в создаваемой сети радиосвязи, в основе которой лежит самоорганизующаяся архитектура с реализацией следующих возможностей:

– создание единого, охватывающего большую площадь, информационного пространства;

– возможность высокой масштабируемости;

– устойчивость самоорганизующейся сети связи к выходу из строя её отдельных элементов.

MPLS технологии являются наиболее подходящим направлением развития средств радиосвязи нового поколения, обеспечивающих предоставление пользователям (должностным лицам) широкого спектра мультисервисных услуг с требуемым качеством в условиях проведения боевых (специальных) операций.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1 Воробьев И.Г., Лисейкин Р.Е., Ткачев Д.Ф. Концептуальные подходы к построению региональной защищенной мультисервисной сети связи // Актуальные проблемы инфотелекоммуникаций в науке и образовании. III Международная научно-техническая и научно-методическая конференция: сборник научных статей. – СПб.: СПбГУТ, 2014 г.

2 Лящук М.З., Ткачев Д.Ф. Проактивный алгоритм динамической маршрутизации в мобильных распределенных перспективных сетях, построенных на радиосредствах нового поколения // Фундаментальные и прикладные исследования в современном мире, 2016. – №13-1.

3 Ткачев Д.Ф., Лящук М.З., Лисейкин Р.Е. Реактивный алгоритм динамической маршрутизации в перспективной мобильной сети, построенной на радиосредствах нового поколения // Молодой ученый. – 2016. – №11 (115).

4 Лящук М.З., Ткачев Д.Ф., Дворников А.С., Ткачев А.Ф. Предложение по адресованию пользователей перспективной сети радиосвязи специального назначения // T-Comm: Телекоммуникации и транспорт. – 2016. – Т.10. – № 5.

5 https://ru.wikipedia.org/wiki/MPLS.

6 https://teletype.in/@awakentrue.

УДК 355:34

СОВЕРШЕНСТОВОВАНИЕ ТЕХНИКИ ОБСЛУЖИВАНИЯ СРЕДСТВ СВЯЗИ

МУРТАЛИМОВ Ш.Р.[1], *преподаватель кафедры вооружения и стрельбы, магистр, подполковник*
ВОЛКОВ Б.В.[1], *старший преподаватель кафедры вооружения и стрельбы, магистр, полковник*

[1]*Академия Национальной гвардии, город Петропавловск, Республика Казахстан*

Аннотация: в статье рассматриваются ключевые направления и технологические инновации в области совершенствования техники обслуживания средств связи. Подчеркивается важность интеграции современных технологий в повышение эффективности, надежности и безопасности телекоммуникационных сетей. Особое внимание уделяется эволюции методов диагностики и мониторинга, автоматизации процессов обслуживания и развитию стандартов безопасности. Статья подчеркивает необходимость тесного сотрудничества между операторами связи, производителями оборудования, разработчиками программного обеспечения и регуляторными органами для разработки и внедрения общепризнанных стандартов и нормативов, что способствует совместимости различных систем и облегчает внедрение инноваций.

Ключевые слова: инновации, качество, эффективность, технологии, методы, сотрудничество

Современный мир невозможно представить без средств связи. От мобильных телефонов и интернета до спутниковой связи и радиоволн – все эти технологии требуют постоянного обслуживания и улучшения. Совершенствование техники обслуживания средств связи – это неотъемлемая часть развития телекоммуникационной отрасли, направленная на повышение качества и доступности связи. В этой статье мы рассмотрим ключевые аспекты и направления развития в этой области.

Инновации в оборудовании.

Первый и самый очевидный аспект совершенствования – это внедрение новых технологий в оборудование. Речь идет о таких направлениях, как:

− 5G и будущие стандарты связи. Внедрение 5G и исследования в области 6G обещают значительно увеличить скорость передачи данных, снизить задержку и повысить надежность связи [1].

− интернет вещей (IoT). Разработка устройств и инфраструктуры для поддержки миллиардов устройств IoT требует новых подходов к обслуживанию и управлению сетью.

− спутниковая связь нового поколения. Проекты типа Starlink от SpaceX стремятся предоставить высокоскоростной интернет в самых отдаленных

уголках планеты, что вызывает потребность в разработке нового оборудования и методик его обслуживания.

Автоматизация и ИИ.

Автоматизация процессов обслуживания и применение искусственного интеллекта (ИИ) могут радикально изменить подходы к поддержке средств связи:

− предиктивное обслуживание. Использование алгоритмов машинного обучения для анализа данных об оборудовании позволяет предсказывать неисправности до их возникновения, что снижает простои и эксплуатационные расходы.

− роботизированные системы обслуживания. Роботы и дроны могут использоваться для осмотра и ремонта труднодоступных или опасных участков инфраструктуры, например, вышек сотовой связи или подводных кабелей.

Устойчивое развитие.

Экологическая составляющая также играет важную роль в совершенствовании техники обслуживания. Развитие технологий в этом направлении включает:

− энергоэффективное оборудование. Снижение энергопотребления средств связи не только сокращает эксплуатационные расходы, но и уменьшает воздействие на окружающую среду.

− вторичное использование и рециклинг. Разработка методов и технологий для переработки старого оборудования помогает сократить отходы и способствует переходу на циркулярную экономику.

Интеграция современных технологий в обслуживание средств связи.

Продолжая тему совершенствования техники обслуживания средств связи, следует уделить внимание интеграции современных технологий, которые позволяют не только улучшить качество обслуживания, но и сделать его более эффективным и экономичным.

Цифровая трансформация.

Цифровизация процессов обслуживания позволяет значительно повысить их эффективность. Это достигается за счет внедрения систем управления базами данных, облачных технологий и платформ для удаленного мониторинга и управления сетями. Цифровая трансформация обеспечивает оперативный доступ к необходимой информации, упрощает процесс поиска и устранения неисправностей, а также способствует более глубокому анализу работы сетей связи [2].

Расширенная и виртуальная реальность.

Технологии расширенной (AR) и виртуальной реальности (VR) находят все большее применение в обслуживании и ремонте средств связи. С их помощью инженеры могут получать визуальную информацию о состоянии оборудования в реальном времени, просматривать схемы и инструкции непосредственно во время работы, а также проводить виртуальное обучение и симуляции для повышения квалификации без необходимости физического присутствия у оборудования.

Блокчейн.

Технология блокчейна может применяться в обслуживании средств связи для повышения безопасности, прозрачности и надежности операций. Например, использование блокчейна для учета и контроля за распределением ресурсов, таких как частоты радиосвязи, позволяет исключить несанкционированное использование и споры между операторами. Кроме того, блокчейн может использоваться для защиты данных пользователей и обеспечения конфиденциальности передачи информации [3].

Сотрудничество и стандартизация.

Усилия по совершенствованию техники обслуживания средств связи требуют не только внедрения новых технологий, но и тесного сотрудничества между операторами связи, производителями оборудования, разработчиками ПО, а также государственными и международными регуляторными органами. Разработка и внедрение общепризнанных стандартов и нормативов способствует совместимости различных систем и устройств, улучшает качество обслуживания и облегчает внедрение инноваций.

Эволюция методов диагностики и мониторинга.

Продолжая тему совершенствования техники обслуживания средств связи, стоит особо выделить прогресс в методах диагностики и мониторинга. Эти аспекты играют ключевую роль в обеспечении непрерывности и надежности связи. Современные технологические достижения позволяют переосмыслить традиционные подходы и внедрить новые решения, направленные на предотвращение сбоев и минимизацию времени реакции на инциденты.

Интеллектуальные системы мониторинга.

Разработка и внедрение систем мониторинга на основе искусственного интеллекта и машинного обучения значительно повышают эффективность обнаружения и диагностики проблем. Такие системы способны анализировать огромные объемы данных в реальном времени, выявляя аномалии и предсказывая потенциальные сбои до их возникновения. Это позволяет оперативно принимать меры по предотвращению отказов и сокращать время простоя.

Беспроводные технологии диагностики.

Использование беспроводных технологий и датчиков IoT для диагностики состояния оборудования обеспечивает более глубокий и всесторонний мониторинг. Беспроводные датчики могут быть установлены в труднодоступных или опасных для человека местах, обеспечивая непрерывный сбор данных о состоянии оборудования. Это способствует более точному и своевременному выявлению неисправностей.

Автоматизированные инструменты обслуживания.

Автоматизация процессов обслуживания с использованием программного обеспечения и робототехники позволяет не только ускорить выполнение рутинных задач, но и повысить их точность. Автоматизированные системы способны выполнять комплексную проверку оборудования, обновление

программного обеспечения и исправление некоторых типов неисправностей без вмешательства человека [4].

Развитие стандартов безопасности.

В условиях постоянно растущих киберугроз развитие и внедрение передовых стандартов безопасности становится приоритетной задачей для обеспечения надежности средств связи. Это включает в себя разработку новых методов шифрования, аутентификации и защиты данных, а также создание отказоустойчивых систем, способных противостоять атакам и обеспечивать бесперебойную работу связи даже в условиях кибератак.

Заключение

Совершенствование техники обслуживания средств связи — это комплексный процесс, требующий интеграции новейших технологических разработок, автоматизации процессов и учета экологических аспектов. Развитие в этих направлениях обеспечит не только повышение качества и доступности связи для конечных пользователей, но и способствует устойчивому развитию телекоммуникационной отрасли в целом.

Техника обслуживания средств связи продолжает развиваться, адаптируясь к новым вызовам и потребностям современного мира. Интеграция передовых технологий и методов в области ИИ, IoT, робототехники и кибербезопасности открывает новые горизонты для повышения эффективности, надежности и безопасности телекоммуникационных сетей. Эти инновации не только способствуют улучшению качества обслуживания, но и задают направление для будущего развития всей отрасли связи.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1 Ефанов В.А., Козлова Л.П. Перспективы развития и возможности 5G сетей. Труды учебных заведений связи. – 2016 г.

2 Богачев Ю.С., Бекулова С.Р. Цифровизация как способ повышения эффективности управления промышленностью. Национальная безопасность. – 2023 г.

3 Петров И.О., Дронин Я.С., Севостьянов В.Р., Манышев В.С., Щербаха Н.К. Использование блокчейна в беспроводной связи и сетях. Новые импульсы развития: вопросы научных исследований. – 2021 г.

4 Ковтун М.В. Робототехника и автоматическое управление. Теория и практика современной науки. – 2023 г.

УДК 621.396.2

ПЕРСПЕКТИВЫ РАЗВИТИЯ ВОЕННОЙ РАДИОСВЯЗИ В НАЦИОНАЛЬНОЙ ГВАРДИИ РЕСПУБЛИКИ КАЗАХСТАН

СУЛТАНБЕКОВ Ж.Г., *магистр, подполковник*
ЩЕРБАКОВ А.В., *подполковник*

Академия Национальной гвардии, Кафедра ТиОВД,
город Петропавловск, Республика Казахстан

Аннотация. В данной статье рассматриваются некоторые аспекты развития разработки оборудования для создания национальной системы военной радиосвязи в целях применения средств связи и автоматизированных систем в Национальной гвардии Республики Казахстан при выполнении возложенных служебно-боевых задач.

Ключевые слова: войсковой оперативный резерв, Региональное командование, Центр боевого управления, транкинговая радиосвязь, DMR, LTE-шлюз.

Анализ крупных протестных акций, проводимых в странах мира, таких как Китай, Франция, Беларусь, Кыргызстан показывает, что в целях успешного противодействия противоправным действиям граждан, участвующих в массовых беспорядках, мотивируемых разрешением различных социальных вопросов, формируется группировка войск, сводная тактическая группа, которая должна иметь упреждающую информацию состояния и управления своими силами. Поэтому все большее внимание уделяется совершенствованию системы управления и системы связи, средствам связи, роль которых за частую является определяющим в противоборстве. Поэтому сегодня, как никогда, завоевание превосходства в информационно-телекоммуникационном пространстве можно сопоставить по значимости с завоеванием превосходства в воздухе в годы Великой Отечественной войны.

Таким образом, выполнение задач по управлению силами и средствами, задействованных по пресечению массовых беспорядков традиционными способами при существующем комплексе сил и средств будет затруднено, а в ряде случаев и невозможно. Наиболее рациональным путем достижения высокой эффективности системы управления, отвечающей предъявляемым к ней требованиям, является построение такой ее структуры, которая могла бы адаптироваться к конкретным условиям тактической обстановки, при этом, необходимо учитывать обеспечение высокой доступности системы связи и ее элементов в процессе боевого применения, учет возможности попыток срыва управления и вывода из строя элементов телекоммуникационной инфраструктуры активными участниками массовых беспорядков.

Рассмотренные особенности организации управления в специальной операции указывают на ряд противоречий, решаемых при построении

технической основы системы управления. Для решения этих задач предполагается выработать основные направления развития средств отображения информации состояния и управления ВОРез (далее войсковой оперативный резерв), сводной тактической группой при проведении специальной операции.

В ходе проведения специальной операции, заместителю Министра внутренних дел – Главнокомандующему Национальной гвардией, командующему РгК (далее Региональное командование), для принятия адекватного решения необходима достоверная информация в реальном масштабе времени, отражающая сложившуюся обстановку. В связи с этим особую актуальность приобретает создание единого информационного пространства, объединяющего все уровни управления силами ВОРез, сводной тактической группы.

При этом необходимость существенного повышения требований по своевременности, видам и качеству услуг связи требует внедрения новейших технологий, видов связи и интеграции вторичных сетей. Кроме того, внедрение таких новых видов услуг связи, как передача видеоизображений и картографической информации, электронная почта и др., требует пропускной способности каналов в сотни и более Мбит/с., что в свою очередь предопределяет использование в системе связи Национальной гвардии цифровых телекоммуникационных технологий, позволяющих обеспечивать требуемую пропускную способность. В настоящее время в Национальной гвардии имеется возможность и практическая реализация вывода систем видеонаблюдения ЦОУ ДП (далее Центр оперативного управления Департамента полиции), акиматов городов Республики Казахстан в ЦУВ ГКНГ, а также в ПБУ (далее Пункт боевого управления) воинских частей Национальной гвардии (рисунок №1).

Рисунок 1 – Пункт боевого управления воинских частей Национальной гвардии

Управление силами и средствами, задействованными в специальной операции, осуществляется в развернутой сети транкинговой связи системы

связи Национальной гвардии. В этих целях созданы каналы и транкинговые группы управления и взаимодействия.

В целях контроля и профилактики предупреждения правонарушений на боевой службе, оперативного реагирования на правонарушения и уличные преступления, а также в рамках построения единой системы транкинговой УКВ радиосвязи Национальной гвардии, в 2018 году осуществлена установка базовых станций в г. Астана, Шымкент и Актобе. В ноябре и декабре 2020 года введены в эксплуатацию 9 базовых станций: в г. Актау, Атырау, Уральск, Караганда, Семей, Усть-Каменогорск, Тараз по одному комплекту и Алматы-2 комплекта.

Система транкинговой связи, совместно с системой диспетчеризации, позволяет существенно увеличить оперативность управления элементами боевых порядков ВОРез, сводной тактической группой, а также осуществлять онлайн-мониторинг местонахождения военнослужащих с рабочих мест диспетчера воинских частей и существенно расширить зону покрытия УКВ радиосвязи в условиях плотной городской застройки.

Система диспетчеризации позволяет при нажатии корреспондентом специальной кнопки на радиостанции, увидеть диспетчером на экране сигнал SOS от радиостанции (точное место нахождения корреспондента.) Также имеется возможность вызова корреспондента с внутреннего рабочего телефона на радиостанцию и обратно.

Диспетчерское место рассчитано на работу с любого компьютера воинской части, но не более двух диспетчеров одновременно с двух разных компьютеров.

Диспетчер имеет возможность наблюдать по карте местонахождение корреспондентов, вызвать их голосовой связью, отправить или получить SMS-сообщение, просмотреть историю передвижений по карте каждого выбранного им корреспондента, производить записи всех радиопереговоров и телефонных звонков.

Взаимоувязывание установленных базовых транкинговых станций в единую информационно – телекоммуникационную сеть Национальной гвардии позволяет управлять элементами ВОРез, сводной тактической группой, получать голосовую, текстовую и визуальную информацию о местонахождениях корреспондентов в зоне действия транкинговой связи с любого пункта управления (рисунок №2).

ВОЗМОЖНОСТИ СИСТЕМЫ ДИСПЕТЧЕРИЗАЦИИ С ИСПОЛЬЗОВАНИЕМ СЕТИ ТРАНКИНГОВОЙ СВЯЗИ НАЦИОНАЛЬНОЙ ГВАРДИИ

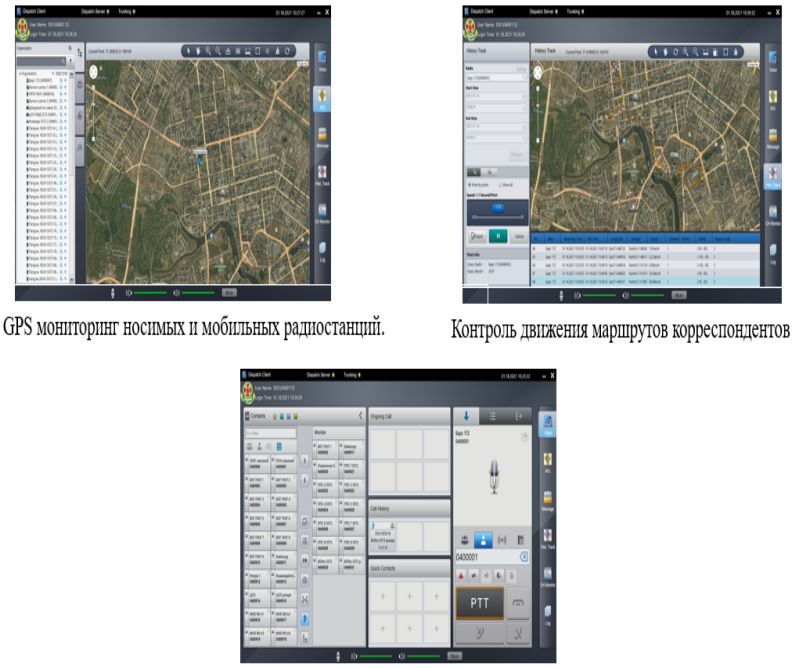


Рисунок 2 – Пункт управления корреспондентами

В целях сбора информации силами разведки в районе выполнения служебно-боевых задач при использовании мультирежимных терминалов Hytera PDC-760G с возможностью передачи видеофайлов, аудиосообщений, SMS-сообщений в ЦУВ ГКНГ, ПБУ воинских частей. Реализована функция загрузки информации в ЕИП через данные терминалы в зоне действия сотового оператора (рисунок №3). Развернута резервная беспроводная мобильная сеть на базе ретрансляторов E-Pack-100. Данные ретрансляторы имеют модуль GSM, что позволяет организовать более устойчивую связь между радиостанциями в сети, в том числе позволяет организовать радиоканал между корреспондентом радиостанции и пользователем мобильного телефона практически с любого места.

DMR-LTE СЕТЬ СБОРА ИНФОРМАЦИИ И РАЗВЕДКИ

Рисунок 3 – Функция загрузки информации в ЕИП

Функционирует мобильная сеть коротковолновой радиосвязи на базе тактических штабов спецподразделений, комплексных аппаратных связи РгК, воинских частей, с возможностью передачи голосовой информации от мобильного пункта управления с района выполнения задачи, до пункта постоянной дислокации при совершении марша. Ведется работа по практической реализации сети передачи данных в КВ радиосетях Национальной гвардии, что позволит в короткие сроки передавать текстовые файлы, радиограммы, копии документов с большим информативным содержанием в единицу времени (рисунок № 4).

Рисунок 4 – Передача данных в КВ радиосетях НГ РК

Перспективы передачи и получения различных видов информации при выполнении служебно-боевых задач.

Ведутся работы по развертыванию сети мобильного доступа КАС (КШМ) к транспортной среде ЕТСГО посредством оборудования мобильной спутниковой связи и LTE-шлюза сети мобильного оператора, что позволит получить еще один дополнительный транспортный канал передачи информации в полевых условиях, тем самым существенно повысив надежность связи.

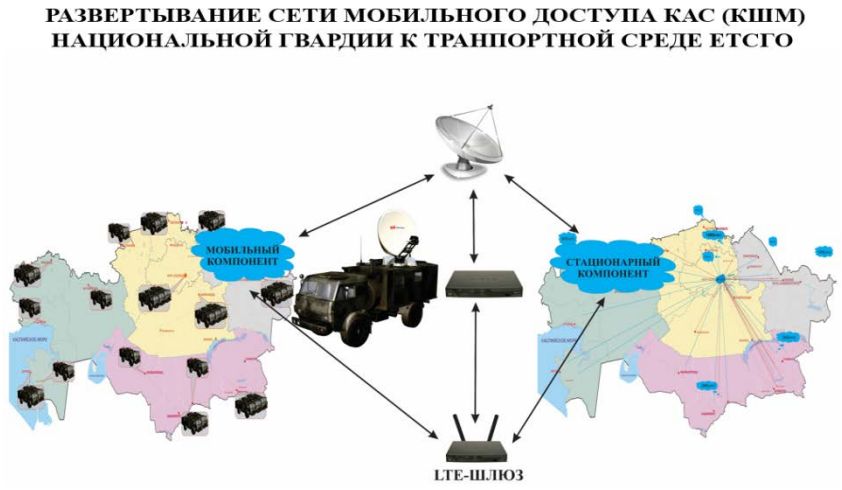


Рисунок 5 – Развертывание сети мобильного доступа КАС (КШМ)

Реализуется техническая возможность организации мобильного (беспроводного) VPN канала при несении службы по охране общественного порядка и при выполнении других служебно-боевых задач. Таким образом у оператора планшета появится возможность наблюдения войсковых нарядов в режиме онлайн, получения текстовой оперативной информации), выхода в телефонную сеть НГ и т.д.

Рисунок 6 – Схема реализации мобильной VPN системы

СПИСОК ИСПОЛЬЗУЕМОЙ ЛИТЕРАТУРЫ

1 Беккер А.В. Связь – техническая основа управления войсками. Учебное пособие. Петропавловск: Академия Национальной гвардии Республики Казахстан, 2023. – 84 с.

2 Учебное пособие: Жакубаев А.А. Учебное пособие Военная техника радиосвязи 2016, Петропавловск, ВИ НГ РК.

3 Учебное пособие: Рудаков А.Л. Жакубаев А.А. Учебное пособие Подготовка по связи 2014, Петропавловск, ВИ ВВ МВД РК.

4 Приказ Главнокомандующего Национальной гвардии Республики Казахстан №65 от 18 февраля 2015 года. «Руководство по радиосвязи Национальной гвардии Республики Казахстан (часть 2)». Астана. – 2015 г.

5 Учебное пособие: Учебное пособие по дисциплинам связи (часть 1): Учебное пособие/ А.В.Щербаков. – Академия НГ РК., 2022 г.

УДК 69

ВОЗМОЖНОСТЬ ПЕРЕДАЧИ СИГНАЛОВ АВТОМАТИЧЕСКОЙ ТЕЛЕФОННОЙ СТАНЦИИ ЧЕРЕЗ ВЫСОКОЧАСТОТНЫЕ АНАЛОГОВЫЕ КАНАЛЫ

ИСТИМЕСОВ М.Б., *начальник цикла БПСВ подполковник запаса*
КУЗМИЦКИЙ С.В.,
ЛЕПЕТУХИН Е.А.,
ШУКУРБАЕВ Б.Н.

Военная кафедра НАО КарТУ «имени Абылкаса Сагинова»,
город Караганда, Республика Казахстан

Аннотация. Данная статья посвящена описанию модернизацию аппаратуры первичного уплотнения П-303 ОБ блока дифференциальных систем ДСВ-3 под каналы автоматической телефонной станции.

Ключевые слова. Телефонная станция, многоканальная система связи, реле.

Одним и часто возникающих вопросов при организации многоканальной системы связи используя аналоговое оборудование это передача номеров автоматической телефонной станции по аппаратуре первичного уплотнения, если использовать современную технику связи через цифровой канал то с этим не возникает никакой проблемы, но если нет новой техники и ваша организация ограничена аппаратурой старого парка, то можно использовать вариант который мы хотим вам предложить, конкретно это передача от шести до двенадцати номеров автоматической телефонной станции по радиорелейной линии образуемой Р-409М в с использованием аппаратуры первичного уплотнения П-303 ОБ и переделанного блока дифференциальных систем (далее – ДСВ-3). В вооруженных силах постсоветского пространства в военной связи широкое применение находит радиорелейная станция Р-409, которая в своем составе имеет аппаратуру первичного уплотнения П-303 ОБ которая уплотняет 6 каналов тональной частоты. Радиорелейная станция Р-409М предназначена для организации самостоятельных радиорелейных или кабельных линий связи, а также для ответвления каналов от многоканальных линий связи. Кроме этого, станция может быть использована для обеспечения радиорелейного пере приёмного участка в кабельной линии связи аппаратуры П-303-ОБ. Аппаратура уплотнения П-303ОБ обеспечивает шесть высокочастотных телефонных каналов в полосе частот 4-32 кГц (или три канала в полосе 4-20 кГц) и один канал для служебной связи в полосе 0,3-1,8 кГц. Аппаратура П-303ОБ позволяет получить два «широких» канала с полосой эффективно передаваемых частот 12,3-23,4 кГц. Вызов по каналам производится на тональной частоте 2100 Гц с уровнем передачи на 0,7 Нп (6,7 дБ) ниже

измерительного уровня. По служебному каналу обеспечивается громкоговорящий прием вызова и посылка вызова голосом.

Сама высокочастотная стойка Р-409 организует групповой тракт для работы аппаратуры уплотнения П-303 ОБ в состав которой входит блок дифференциальных систем (далее – ДСВ-3) который и подвергнется переделки. Блок ДСВ-3. Блок содержит устройства дифсистем для трех телефонных каналов. На лицевой панели расположены гнезда с дужками для переключения режимов и для системы передачи вызова.

Переделка стандартного блока дифференциальных систем ДСВ-3 для работы в качестве псевдоавтоматической телефонной станции (далее – АТС) заключается в следующем:

В первую очередь необходимо блоки ДСВ-3 разделить на входящий компонент (сторона абонента далее ТФ) и исходящего компонента (сторона станции (далее – АТС).

Со станционной стороны (АТС) блок дифференциальной системы вызова на три канала подключают через разделительные конденсаторы номиналом 1.0 мкФ, далее работа ДСВ-3 работает в стандартном режиме, вызывной сигнал заставляет срабатывать блок посылок индукторного вызова (далее – ПНВ), который включает генератор в сторону корреспондента по каналу тональной частоты.

Со стороны входящего комплекта абонентской стороны (ТФ) блок ДСВ-3 включает блок генератора индукторного вызова (далее ГИВ) и вызывное напряжение поступает на абонентский телефонный аппарат.

При наборе номера абонент снимает трубку срабатывает реле «Р1-I», которое подключает конденсатор номиналом 4700 мкФ, напряжением16 вольт к реле «РЭС-9», РЭС-9 остается в положении включено пока через его обмотку разряжается конденсатор. В это время конденсатор реле РЭС-9 в канал тональной частоты подаётся от блока генератора тонального вызовы (далее ГТВ) импульс генератора, со стороны автоматической телефонной станции на ДСВ-3 этот импульс включает реле «Р2-I» далее реле своими контактами включает счётчик импульсов на микросхеме «NE 555» которая в свою очередь включает реле РЭС-10 которое подключает параллельное линии подающей номер от АТС резистор номиналом 560 Ом для удержании линии, затем абонент тонального набора соединяется с любым номером автоматической телефонной станции.

По завершению разговора абонент кладёт трубку и на ДСВ-3 со стороны абонента в реле «Р1-I» происходит её обесточивание, к реле РЭС-9 подключается другой конденсатор номиналом 4700 мкФ напряжением 16 вольт, который разрежается некоторое время через реле РЭС-9 в свою очередь на это время подключает генератор тонального вывода в сторону канала тональной частоты на ДСВ-3 станционную сторону.

На ДСВ-3 со станционной стороны срабатывает реле Р2-I на некоторое время. Этот импульс заставляет микросхему NE 555 обеспечит реле РЭС-10,

которая своими контактами отключает резистор удержания линий номиналом 560 Ом от канала. Система готова к следующему циклу работы.

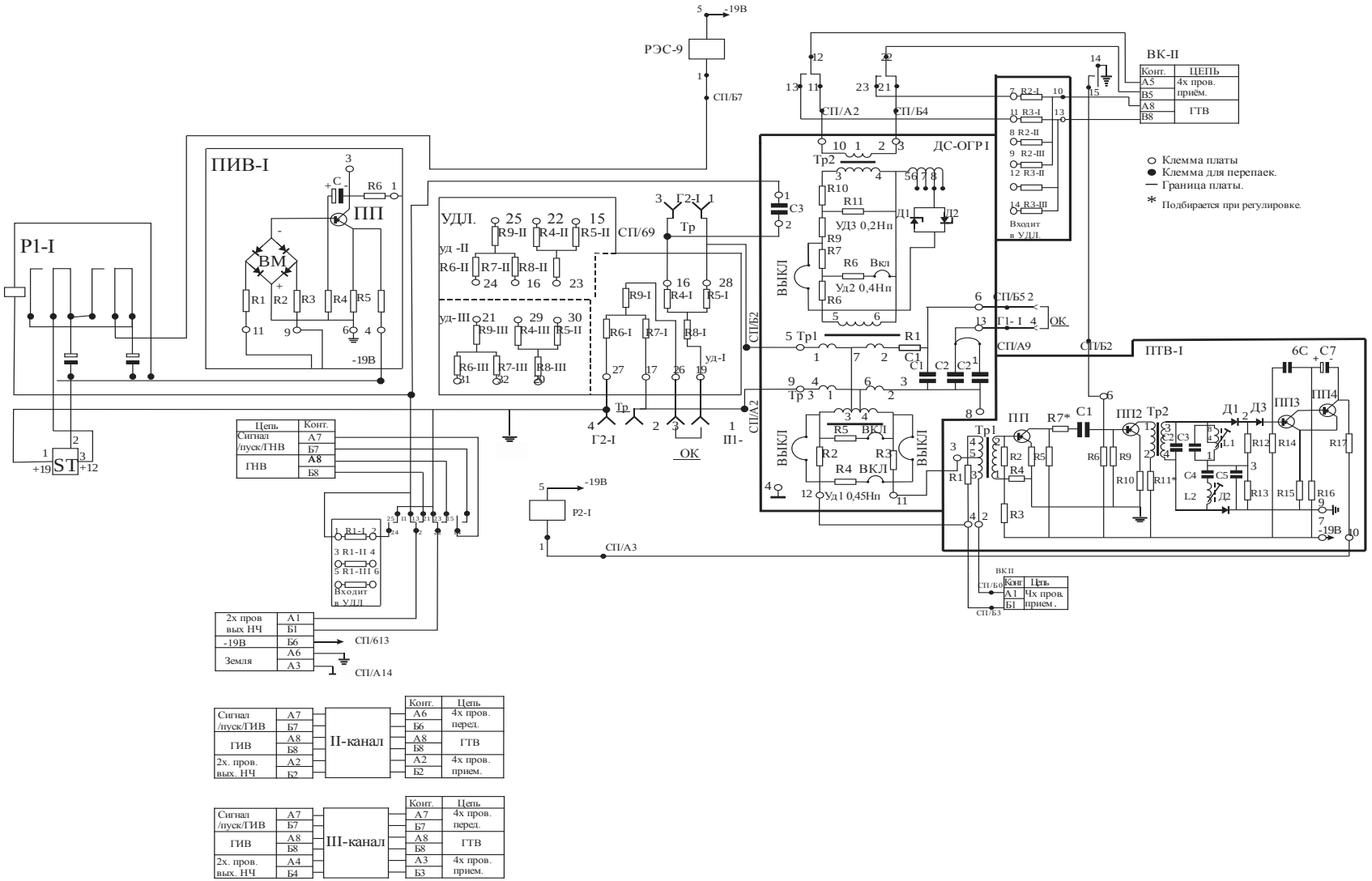


Рисунок 1 – Блок дифсистем и устройства вызова ДСВ-3 (ТФ)

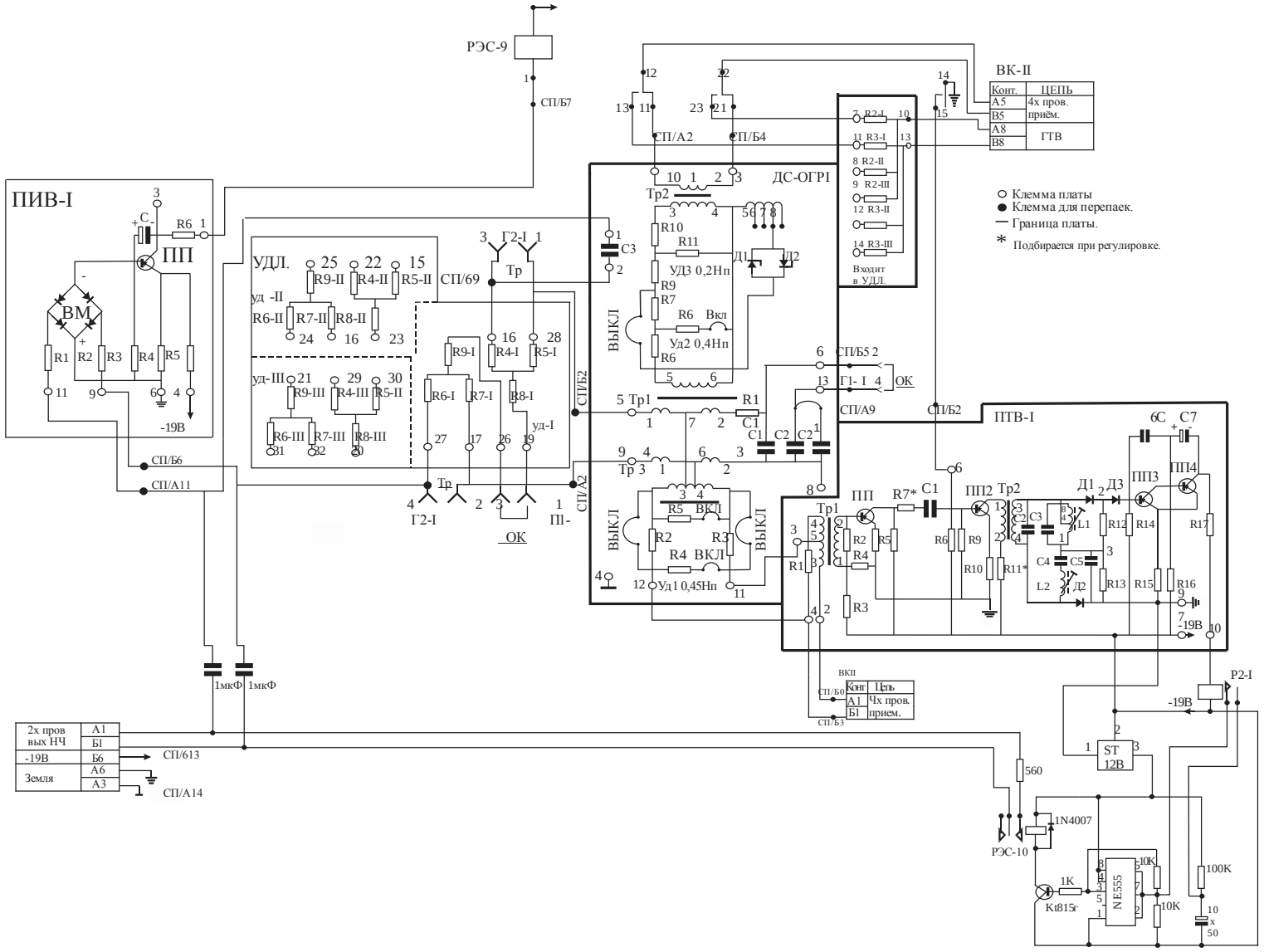


Рисунок 2 – Блок дифсистем и устройства вызова ДСВ-3 (АТС)

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1 Техническое описание и инструкция по эксплуатации аппаратуры уплотнения П-303 ОБ.

2 Техническое описание и инструкция по эксплуатации радиорелейной станции Р-409М.

УДК 621.391

САМООРГАНИЗУЮЩИЕСЯ СЕТИ

ХАЛИКОВ Д.Р., *майор*

Департамент связи ГШ ВС РК Министерства обороны Республики Казахстан, город Астана

Развитие и применение технологии интернета вещей (IoT – Internet of Things) обуславливает необходимость использования беспроводных сетей, позволяющих значительно упростить сбор и обработку данных, одним из таких решений являются самоорганизующиеся сети с высокой надежностью и децентрализованным управлением [1].

Самоорганизующаяся сеть позволяет решать множество задач, например, быстрое развертывание беспроводных сетей с высокой пропускной способностью, не требующих строительства инфраструктуры, организацию беспроводного обмена с датчиками в коммунальной сфере – приборами учета воды, газа, тепла, электроэнергии, обмен информацией между датчиками и устройствами в системе умный дом и др. Пользователи точек доступа и сами точки могут находиться высоко в воздухе или постоянно перемещаться (если, например, установлены в патрульных машинах или в квадрокоптерах, доставляющих товары, заказанные в интернет-магазине).

Организованную таким образом сеть невозможно настроить статически, её топология меняется, а устройства подключаются и отключаются, причём как пользовательские, так и промежуточные сетевые, составляющие основу построения сети. В этой связи автоматизация, оптимизация настроек и маршрута сети является актуальной.

Одно из определений самоорганизующейся сети – сеть, не имеющая определенной структуры, меняющаяся и распределяющая функции между узлами при подключении нового устройства или изменении характера трафика и т.д [2].

Для самоорганизующейся сети характерны следующие свойства:

1. Беспроводная. Можно использовать существующие протоколы, стандарты и технологии беспроводной связи, такие, как, например, IEEE 802.11 Wi-Fi (для локальных и городских сетей), IEEE 802.15.1 Bluetooth (для бытовых устройств), IEEE 802.15.4 Zigbee (для датчиков).

2. Динамическая. Сеть настраивается сама, в автоматическом режиме, без участия человека. Требует обмена управляющей, а в некоторых случаях и статистической информацией между узлами, участвующими в организации сети приёма и передачи данных (например, для балансирования нагрузки и отправки сведений об изменении топологии сети).

3. Децентрализованная. В таких сетях нет единого управляющего центра. Каждое устройство сети (абонент) — активный участник процесса организации приёма и передачи данных между сетевыми узлами.

4. Мобильная. Узлы, составляющие сеть, могут перемещаться в пространстве, выбывать из сети, а новые устройства, в свою очередь, присоединяться к сети и участвовать в её организации.

В целом история создания современных самоорганизующихся сетей берет свое начало с 1970-х годов с момента создания PRNET (Packet Radio Networks), финансированные Министерством обороны США. Цель создания самоорганизующихся сетей заключалась в возможности работать в сети, получать доступ к сети Интернет в любом месте, даже находясь в движении, не полагаясь на инфраструктуру фиксированной сети связи.

С развитием всепроникающих беспроводных сетей возникла необходимость в использовании нового типа сетей, без устойчивой структуры и способной адаптироваться к меняющимся характеристикам каналов связи. Такие сети стали называть самоорганизующимися.

Типы самоорганизующихся сетей

Ad hoc сети – радиосети со случайными стационарными абонентами, реализующие полностью децентрализованное управление при отсутствии базовых станций или опорных узлов. Топология – фиксированная со случайным соединением узлов.

MANET (Mobile Ad hoc NETworks) сети – радиосети со случайными мобильными абонентами, реализующие полностью децентрализованное управление при отсутствии базовых станций или опорных узлов. Топология – быстро меняющаяся со случайным соединением узлов [3].

Mesh сети – радиосети ячеистой структуры, состоящие из беспроводных стационарных маршрутизаторов, которые создают беспроводную магистраль и зону обслуживания абонентов (мобильных, стационарных), имеющих доступ (в пределах зоны покрытия) к одному из маршрутизаторов. Топология – звезда, со случайным соединением опорных узлов.

Для самоорганизующейся сети свойственны следующие характеристики:

1. Самоконфигурация – распознавание и регистрирование в сети новых подключенных устройств. При этом соседние автоматически корректируют свои технические параметры (например, мощность излучения и т.д.).

2. Самооптимизация – адаптация параметров устройств при изменении параметров сети таких как, количество пользователей, уровня сигнала, уровня внешних помех и др.

3. Самовосстановление – автоматическое обнаружение и устранение сбоев, перераспределение функций между устройствами при выходе из строя каких-либо узлов сети для повышения отказоустойчивости сети в целом.

Подробно остановимся на одном типе самоорганизующихся сетей – **mesh-сети.**

Определение Mesh-сетей

Mesh в переводе с английского языка означает «ячейка», т.о. mesh-сеть (ячеистая сеть).

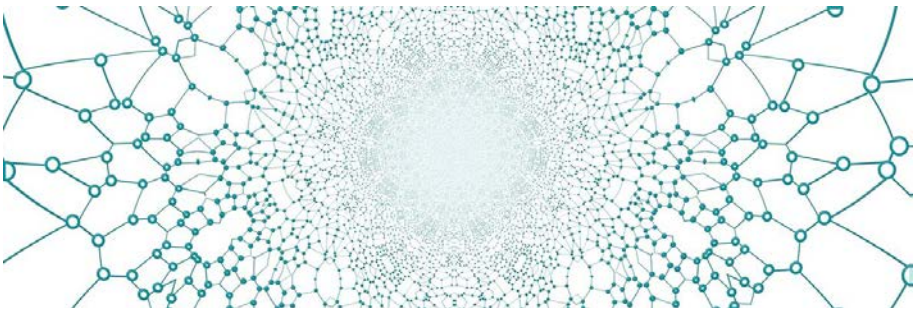


Рисунок 1 – Топология mesh-сети

Ячеистая топология (*mesh-сеть*) — сетевая топология, построенная на принципе ячеек, в которой каждое устройство (абонент) сети соединяются друг с другом и способны принимать на себя роль маршрутизатора для остальных участников [4].

Рассмотрим еще одно определение mesh-сети — это одноранговые (P2P, peer-to-peer) распределенные сети, в которых каждое устройство (абонент) соединяется со своими ближайшими соседями (устройствами) и может принимать на себя функцию маршрутизатора. Каждое устройство в mesh-сети называется узлом, и они создают децентрализованную сеть, где каждый узел может связаться с любым другим узлом в пределах своей беспроводной области покрытия [5].

Подобные сети способны реализовать высокую отказоустойчивость и поэтому нашли широкое применение в таких областях, как военная связь, интеллектуальные транспортные системы, локальные беспроводные сети, беспроводные сенсорные сети, кроме того, могут быть использованы в бизнесе, в сфере образовании, промышленности и в других областях.

Первые упоминания о mesh-сети для решения задач передачи информации следует искать в военных приложениях. На базе технологии Mesh созданы системы для организации мобильной связи с единичными объектами в зоне военных действий. Подобные системы обеспечивают высокоскоростную передачу цифровой информации, видео- и речевую связь, а также определяют местоположение объектов.

Сети подобного класса применяются военными ведомствами разных стран для организации оперативной связи в тактических целях, например во время проведения антитеррористических операций, в зонах локальных военных конфликтов.

Основные возможности mesh-сети:

1) создание зон сплошного информационного покрытия большой площади;

2) масштабируемость сети (увеличение площади зоны покрытия и плотности информационного обеспечения) в режиме самоорганизации;

3) использование беспроводных транспортных каналов (backhaul) для связи точек доступа в режиме «каждый с каждым»;

4) устойчивость сети к потере отдельных элементов [6].

В таких одноранговых сетях (P2P) каждый узел может соединяться с ближайшими устройствами и принимать функции маршрутизатора (ретранслятора), что обусловлено большими зонами покрытия сети с взаимозаменяемыми узлами и возможностью автоматического масштабирования.

Mesh-сети (multi-hop) – сетевая топология, в которой беспроводные устройства объединены многочисленными, зачастую избыточными соединениями, которые вводят по стратегическим соображениям.

Это определение достаточно хорошо соответствует функциям развертываемых сетей такого класса. Идея самоорганизующейся сети, имеющей децентрализованное управление и обладающей высокой степенью надежности, была предложена давно, но эффективная реализация подобной технологии стала возможной в результате быстрого развития беспроводных технологий [7].

Mesh-сети интегрируют в себя различные сетевые и радиотехнологии. Самый распространенный на сегодняшний день стандарт беспроводного соединения – Wi-Fi, поэтому и сами mesh-сети строятся в основном на этой технологии.

Такие сети предоставляют наиболее интересные решения, интегрирующие различные технологии беспроводного доступа. Операторы связи, которые разворачивают сети в мегаполисах с помощью технологий самоорганизующихся сетей, таких как Mesh топологии локальных LAN и городских MAN, могут легко интегрировать их в глобальные сети WAN.

Особая актуальность mesh-сетей определяется развитием микроэлектроники, появлением различных устройств, способных работать автономно долгое время, имеющих особенность многократной смены режима работы (online или offline) и нуждающихся в обмене информацией со своим окружением, а также с управляющим (информационным) центром.

Примерами технологий, построенных на базе mesh-сетей являются, например, Z-Wave, ZigBee и др. Они нашли широкое применение так называемых «умных домах», где каждое устройство является одновременно и приемником, и передатчиком, таких устройств в одной сети может быть несколько десятков (различные датчики движения, освещения, протечки, присутствия, температуры и влажности и другие, выключатели, розетки, управляемые лампочки, электроприводы штор, управление гаражными воротами и другие).

Основное преимущество mesh-сетей – это независимость. Можно создать свою сеть передачи данных, которую никто не контролирует и все время оставаться на связи. Чем больше устройств, тем надежнее сеть, т.о. можно всегда оставаться на связи в местах, где отсутствует сетевая инфраструктура. Это может быть особо актуально в районах повышенного риска (проведение спасательной операции, геологоразведка и др.) и удаленных населенных пунктах.

Рисунок 2 – Архитектура Mesh-сети

Рассмотрим строение mesh-сети. Эта сеть покрывает территорию, разделенную на кластерные зоны, число которых теоретически не ограничено, совокупностью которых и является mesh-сеть. В одном кластере размещается от 8 до 16 точек доступа. Одна из таких точек является узловой (gateway) и для подключения к магистральному каналу связи узловая точка присоединяется с помощью кабеля (оптического или электрического) либо радиоканала с использованием систем широкополосного доступа. Все точки доступа (узловые и простые) в кластере соединяются между собой с помощью радиосвязи. Они могут работать в двух режимах. Первый режим обеспечивает одну - единственную функцию ретранслятора, второй – две одновременно работающие функции: абонентской точки доступа и ретранслятора. Процедура расширения сети в пределах кластера ограничивается установкой новых точек доступа, интеграция которых в существующую сеть происходит автоматически.

Недостаток подобных сетей заключается в том, что они используют промежуточные пункты для передачи данных; это может вызвать задержку при пересылке информации и, как следствие, снизить качество трафика реального времени (например, речи или видео). В связи с этим существуют ограничения на количество точек доступа в одном кластере.

Топология Mesh основана на децентрализованной схеме организации сети, в отличие от типовых сетей 802.11, которые создаются по централизованному принципу. Точки доступа, работающие в mesh-сетях, не только предоставляют услуги абонентского доступа, но и выполняют функции маршрутизаторов/ретрансляторов для других точек доступа той же сети. Благодаря этому появляется возможность создания самоустанавливающегося и самовосстанавливающегося сегмента широкополосной сети.

Протоколы маршрутизации

Маршрутизация в mesh-сети может быть как простой, так и сложной, в зависимости от алгоритмов маршрутизации. В mesh-сети каждое устройство может быть подключено к каждому другому устройству в сети, создавая таким образом сеть, обладающую высокой отказоустойчивостью и распределенной архитектурой.

Главной особенностью mesh-сети является использование специальных протоколов, которые предоставляют возможность каждой точке в сети создавать мини-базу для контроля динамической маршрутизации трафика и

отслеживания состояния транспортного канала, что необходимо для поиска оптимального маршрута в сети. Если вдруг одна из точек отключается, то происходит автоматическое перераспределение трафика по альтернативному маршруту. Тем самым гарантируется доставка трафика адресату за минимальное время. Важно отметить, что при резком увеличении трафика сеть способна к самовосстановлению и адаптации [8].

В беспроводных сетях протоколы маршрутизации обеспечивают поиск оптимального пути для IP-трафика, так как топология в данной сети является переменной. Выбор оптимального пути трафика основан на критериях длины и надежности пути и задержки, пропускной способности, загрузки канала связи.

Следует принимать следующие классы маршрутизации:

1. Проактивная. Каждый узел сети при определенном условии или через определенное время рассылает служебные сообщения. На основе этой информации каждый узел сети строит таблицу маршрутизации. Эта информация потребуется при необходимости передачи сообщения другому узлу. Примеры протоколов: Optimized Link-State Routing (OLSR), Destination-Sequenced Distance Vector (DSDV).

2. Реактивная. При необходимости отправки сообщения узел-отправитель передает широковещательное сообщение узлу-получателю, который подтверждает полученное сообщение ответом с указанием его маршрута. Затем узел-отправитель сохраняет маршрут в таблице маршрутизации. Примеры: Dynamic Source Routing (DSR), Ad Hoc On Demand Distance-Vector (AODV).

3. Гибридная. Сеть может быть разделена на некоторое количество подсетей, внутри которых взаимодействие между элементами сети выполняется с помощью проактивных протоколов, а реактивные протоколы обслуживают коммуникацию подсетей между собой, т.о. при гибридной маршрутизации уменьшаются не только размеры таблиц маршрутизации элементов подсети, но также и объем служебной информации, так как отдельно формируются маршруты между подсетями и отдельно внутри подсетей. Примеры: Zone Routing Protocol (ZRP), Landmark Routing Protocol (LANMAR), Hybrid Wireless Mesh Protocol (HWMP).

В отличие от сетей с постоянной топологией, где применяются протоколы маршрутизации – вектора расстояния и состояния канала (с метрикой маршрутов), для сетей особого назначения актуален выбор правильной метрической системы. Современный рынок предлагает универсальное программное обеспечение ZigBee, IrDA, Bluetooth, Wi-Fi, необходимое для построения надежной и безопасной mesh связи. Для обмена информацией, подключенных устройств и топологии необходима определенная продолжительность работы аккумуляторов пользовательских устройств. Для такой среды требуется протокол, адаптирующийся под ресурсоемкость устройств.

В mesh-сети присутствуют особые устройства, отличающие ее архитектуру – узлы Mesh Point (MP), взаимодействующие с такими же узлами и поддерживающие характерные для mesh-сети службы. Если в топологии сети

такие узлы совмещены с точками доступа AP, они называются точками доступа mesh-сети Mesh Access Point (MAP). Соединение с внешними сетями происходит с помощью порталов mesh-сети, Mesh Point Portal (MPP). По сравнению с протоколами более высокого уровня и другими устройствами функции mesh-сети аналогичны широковещательной Ethernet сети, у которой все узлы соединены на канальном уровне.

«Живучесть» такой сети в условиях чрезвычайных ситуаций достаточно велика за счет динамической переконфигурации и перемаршрутизации трафика, а также вследствие наличия большого количества обходных и резервных путей (маршрутов) для трафика внутри сети. Как правило, каждый узел такой сети имеет связность, равную двум и более, что позволяет повысить отказоустойчивость структуры сети в целом и оперативно решать поставленные задачи».

Возможно использование – вместе и по отдельности – реактивного и проактивного режимов в гибридном протоколе HWMP (Hybrid Wireless Mesh Protocol). В сети с проактивным режимом какой-либо узел может использовать Метод выбора пути по запросу установить прямое соединение. Поэтому протокол HWMP является более эффективным.

Появление интенсивно развивающейся технологии mesh-сетей воплощает мечту о глобальном информационном пространстве уже сегодня. Mesh-сети способны быстро и без вложения больших средств объединять в единую среду целые предприятия и даже города. В то время как традиционный подход в организации больших сетей предполагает установку множества опорных точек доступа, новая технология позволяет устройствам «договариваться» друг с другом о взаимной передаче данных по всей территории их размещения без строительства базовых станций [9].

Достаточно подключить всего одно устройство к внешней сети или Интернет, чтобы доступ к ним получил весь кластер близкорасположенных устройств (абонентов), который в свою очередь распространит подключение на следующий кластер и т.д. Любое устройства в сети может взять на себя функцию точки доступа-маршрутизатора или репитера для других устройств (абонентов).

Благодаря способности автоматической перестройки сети при любых изменениях в ее составе или конфигурации достигаются серьёзные преимущества по сравнению с обычными сетями:

− простота развертывания – нет необходимости протягивать кабель к отдельной точке доступа индивидуально;

− расширяемость – точки автоматически настраиваются в сети;

− высокая надежность – ввиду высокой избыточности потеря одной точки приводит к реорганизации маршрутизации с минимальным ухудшением сервиса у абонентов. Технология поддерживает высокоскоростной обмен данными в тяжелой электромагнитной обстановке, автоматическое обнаружение перегрузок и отказов в канале;

− возможность связи при отсутствии прямой видимости — конфигурация mesh-сетей не требует наличия между точками прямой видимости и может обеспечивать связь, как при ограниченной, так и при отсутствии прямой видимости;

− спектральная продуктивность;

− низкое потребление энергии.

Mesh-сети строятся просто и быстро**, работают надежно и продуктивно, расширяются гибко и легко. Автоматически образуют инфраструктуру для передачи данных в условиях высокой плотности абонентов и сложных рельефов.** Такие возможности делает технологию Mesh основным решением при построении современных сетей передачи данных с высокой надежностью и пропускной способностью, как в гражданской, так и в военной сферах.

А в условиях современных военных конфликтов, когда меняются принципы и подходы ведения боевых действий, в условиях постоянной радиоэлектронной разведки противника, построение надежных беспроводных сетей передачи данных является особенно актуальным. Ведь для проведения успешной военной операции необходима устойчивая и надежная связь, как между людьми, так и различными устройствами, будь то беспилотные летательные аппараты, различные сенсоры и др.

Применение mesh-сетей в Вооруженных Силах Республики Казахстан

Развитие телекоммуникационного рынка ежегодно вносит новые предложения и направления по совершенствованию системы связи Вооруженных сил ведущих государств на мировой арене.

На сегодняшний день имеются новые системы связи с возможностью построения высокопроизводительных, беспроводных сетей на тактическом уровне и в комплексе с применением средств видеонаблюдения, передачи данных и телефонии создают полную осведомленность и контроль действий своих подразделений командованию при выполнении ими задач в специальных операциях.

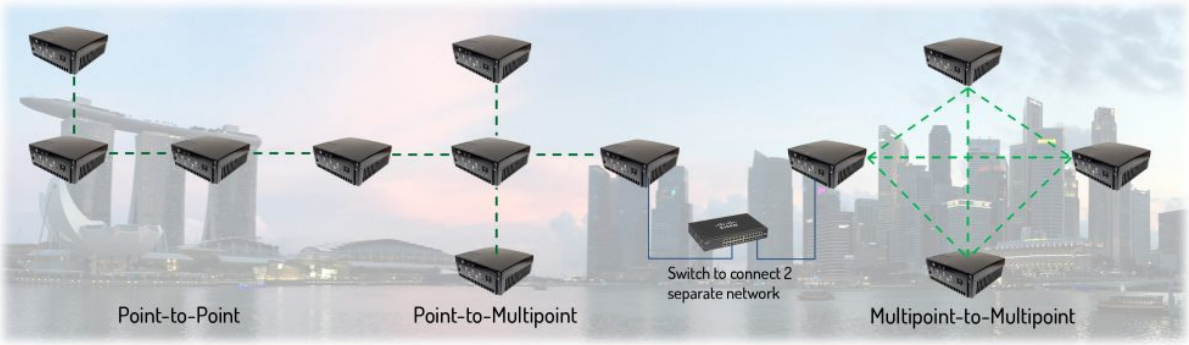
В 2023 году Вооруженными Силами Республики Казахстан был приобретен комплект оборудования m**MESH, работоспособность которого, была продемонстрирована на учебном полигоне «Берег» в рамках тактических учений «Батыл тойтарыс – 2023».**

В состав, приобретенной системы m**MESH входит большое количество аксессуаров, каждый**

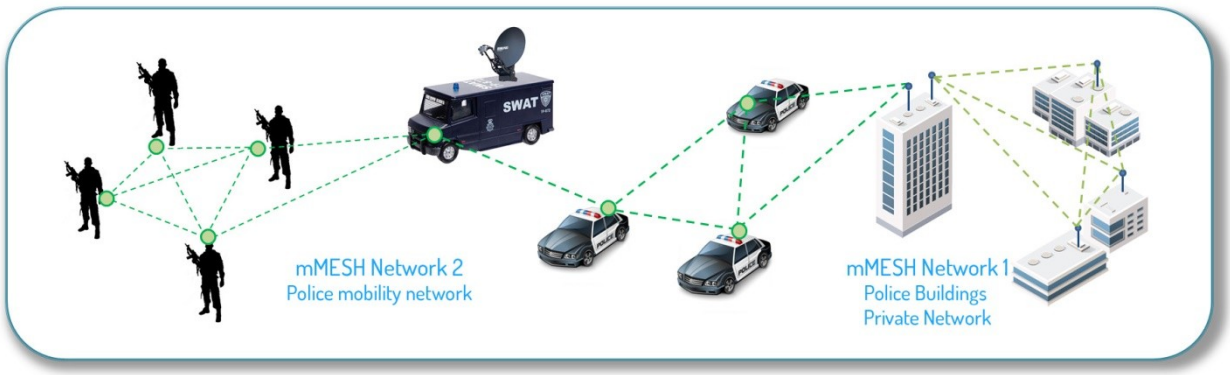
из которых является носителем различной информации, с возможностью вывода ее на пункты управления различного звена и взаимного информирования на поле боя.

Данное оборудование произведено Сингапурской компанией ACE6 Technology и представляет собой беспроводное решение высокой пропускной способности на базе IP, которое обеспечивает связь между людьми, транспортными средствами и командными центрами в самых неблагоприятных и нестабильных сценариях. Оборудование mMESH, использует радиочастотную технологию COFDM для формирования надежных сетей за считанные минуты, даже в ситуациях отсутствия прямой видимости [10].

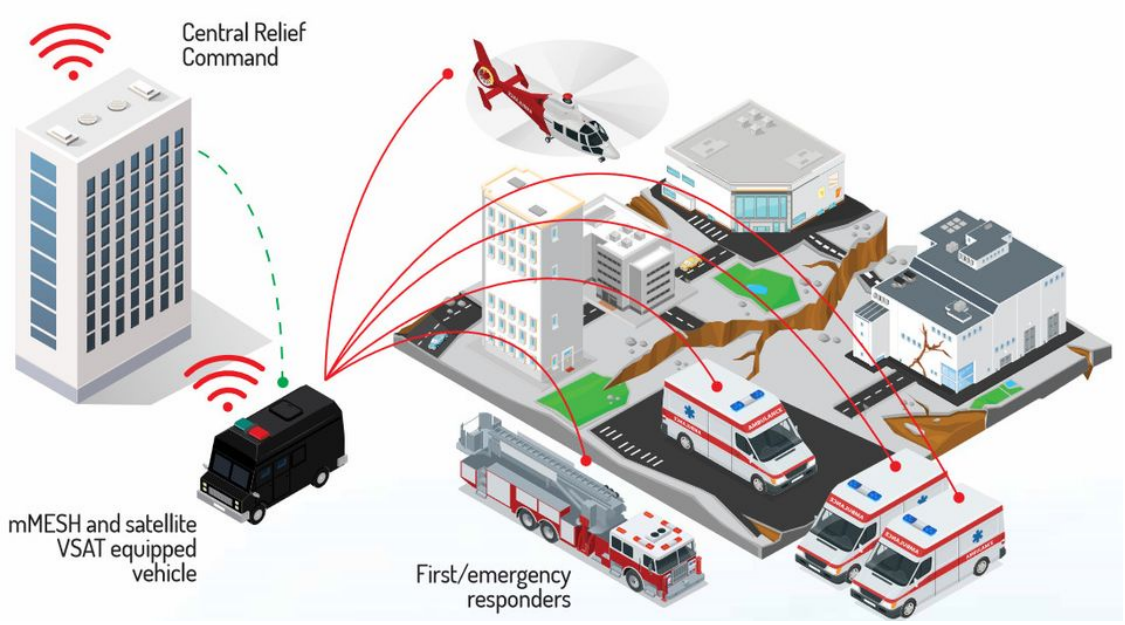
Никакого сложного программирования не требуется, и каждый узел mMESH может работать как ретранслятор, обеспечивая расширенный диапазон покрытия в соответствии с вашими потребностями.



Самоформирующийся, самовосстанавливающийся и автономный mMESH позволяет передавать аудиовизуальные данные в любой конфигурации в многоточечной сети для наиболее эффективной и надежной связи. Используя mMESH, возможно быстро подключить до 64 радиостанций на одной частоте, даже используя устаревшие технологии, такие как спутниковые IP-сети. В сочетании с традиционными технологиями спутниковой связи или другими типами стратегических коммуникационных технологий дальнего действия mMESH является идеальным решением для подключения на последней миле для операций на передовой, снабжая командные центры высококачественной аудиовизуальной информацией в реальном времени.



Продукты mMESH полностью поддерживают мобильность, позволяя командам общаться где угодно и когда угодно. Они были успешно использованы для управления беспилотными летательными аппаратами, движением конвоев, антитеррористическими тактическими подразделениями, пожарными подразделениями и многими другими сценариями, где безопасная, быстро развертываемая частная сеть имеет решающее значение. mMESH помог бесчисленным командам освоить работу в экстремальных условиях, обеспечив улучшенную осведомленность о ситуации в реальном времени для более эффективного и действенного принятия решений.



Подводя итог, можно сделать вывод, что использование современного оборудования позволяет увеличить боевой потенциал войск за счет совершенствования системы управления.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1 http://msm.omsu.ru/jrns/jrn40/GussMesh2016.pdf;
2 https://iot.ru/wiki/samoorganizuyushchiesya-seti;
3 https://crossgroup.su/solutions/data_transfer/adhoc_nets.html;
4 https://ru.wikipedia.org/wiki/%D0%AF%D1%87%D0%B5%D0%B8%D1%81%D1%82%D0%B0%D1%8F_%D1%82%D0%BE%D0%BF%D0%BE%D0%BB%D0%BE%D0%B3%D0%B8%D1%8F;
5 https://cyberleninka.ru/article/n/samoorganizuyuschiesya-mesh-seti-dlya-chastnogo-ispolzovaniya/viewer;
6 https://cyberleninka.ru/article/n/mesh-seti-perspektivy-razvitiya-vozmozhnye-primeneniya;
7 https://lib.tssonline.ru/articles2/fix-op/mesh_seti_techn_prilozh_oborud;
8 https://ntk.kubstu.ru/data/mc/0085/4317.pdf;

9 https://www.skneman.ru/solutions/texnologicheskie-resheniya/peredacha-dannyx-c-podvizhnyx-obektov/;
10 https://www.ace6tech.com/products/.

УДК 355:34

БЕЗОПАСНОСТЬ СИСТЕМ ВОЕННОЙ СВЯЗИ

КИБАЕВ Е.И.[1], *сотрудник*
ЖАНБАБАЕВ Е.А.[1], *сотрудник*

Академия Комитета Национальной безопасности Республики Казахстан, город Алматы

Аннотация. В условиях современного информационного пространства обеспечение безопасности военных коммуникаций является ключевым фактором обороноспособности страны. В статье рассматриваются технические, организационные и стратегические аспекты создания безопасных систем военной связи с учетом современных вызовов и угроз. Предлагаются практические рекомендации и стратегии для создания устойчивой и надежной системы военной связи.

Ключевые слова: безопасность военных коммуникаций, конфиденциальность, технологии, шифрования, угрозы.

Аннотация. Бұл мақала әскери радио желісінің ақпараттық-қауіпсіз инфрақұрылымын дамытуға арналған. Заманауи ақпараттық кеңістікте әскери коммуникациялардың қауіпсіздігін қамтамасыз ету ұлттық қорғаныс қабілетінің негізгі факторы болып табылады. Зерттеу заманауи сын-қатерлер мен қауіптерді ескере отырып, мұндай инфрақұрылымды құрудың техникалық, ұйымдастырушылық және стратегиялық аспектілерін зерттейді. Ұлттық ақпараттық қауіпсіздік мүдделерін тиімді қорғау үшін инженерлік шешімдерді саяси қолдау және стратегиялық көзқараспен біріктіру қажеттілігіне баса назар аударылады. Жүргізілген жұмыстардың нәтижесінде ұлттық әскери радио желісі үшін тұрақты және сенімді ақпараттық қауіпсіздік инфрақұрылымын құру бойынша практикалық ұсыныстар мен стратегиялар ұсынылды.

Тірек сөздер: әскери коммуникациялардың қауіпсіздігі, құпиялылық, технология, қауіптер.

Abstract. This article is devoted to the development of an information-secure infrastructure for a national military radio network. In the modern information space, ensuring the security of military communications is a key factor in national defense capability. The study examines the technical, organizational and strategic aspects of creating such an infrastructure, taking into account modern challenges and threats. Emphasis is placed on the need to integrate engineering solutions with political support and strategic vision to effectively protect national information security

interests. As a result of the work, practical recommendations and strategies are proposed for creating a sustainable and reliable information security infrastructure for the national military radio network.

Key words: security of national military communications, confidentiality, technology, threats.

Современные технологии, включая криптографию, беспроводные сети и цифровые протоколы, создают новые возможности как для защиты, так и для атак на системы связи. Кибератаки могут быть направлены на взлом шифрования, перехват передаваемых данных, или даже на управление военными системами издалека. Кроме того, также присутствуют физические угрозы, такие как вандализм или вторжение на объекты связи. Все эти факторы делают необходимым разработку комплексных мер и систем для обеспечения информационной безопасности военных коммуникаций [1].

Чтобы гарантировать эффективную систему безопасности связи, требуется разработать инфраструктуры, которые будут способны оперативно обнаруживать и предотвращать кибератаки, обеспечивать защиту от несанкционированного доступа к данным, а также обеспечивать непрерывную доступность коммуникационных средств даже в условиях враждебных действий или технических сбоев. Это подразумевает использование передовых технологий зашиты информации криптографии, механизмов аутентификации и авторизации, а также физических мер защиты, таких как биометрические системы доступа и защитные экранированные объекты.

В рамках разработки информационно-безопасной инфраструктуры для военных систем связи крайне важно изучить передовой опыт зарубежных военных организаций. Некоторые из подходов и технологий, которые они применяют, могут быть весьма полезными и применимыми и в контексте национальных проектов по обеспечению информационной безопасности.

Один из ключевых аспектов, который стоит выделить, это концепция «оборонительной глубины» (defense in depth), активно используемая в таких странах, как США и другие члены НАТО [2]. Эта концепция предполагает создание нескольких уровней защиты для обеспечения надежной защиты информационной инфраструктуры. Она включает в себя не только защиту периметра, но и внутренние уровни защиты, такие как мониторинг и обнаружение инцидентов, системы контроля доступа и аутентификации, а также меры защиты на уровне приложений и данных.

Ниже приведены уровни защиты, отражающие концепцию «Оборонительной глубины» рисунок 1.

Рисунок 1 – Уровни оборонительной глубины

Кроме того, важно обратить внимание на развитие кибервоенной деятельности в других странах. Многие из них активно развивают и применяют методы и технологии кибербезопасности, включая разработку специализированных алгоритмов шифрования и обнаружения атак, а также использование искусственного интеллекта для анализа и предотвращения кибератак.

Использование передового опыта иностранных военных организаций может существенно улучшить эффективность и надежность систем военной связи. Однако при этом необходимо учитывать особенности и требования собственной концепции информационной безопасности. Адаптация и применение этих методов должны быть сориентированы на конкретные потребности и условия страны.

Для наглядного представления процесса разработки информационно-безопасной инфраструктуры для систем военной связи можно использовать следующую схему (рисунок 2):

Рисунок 2 – Основные этапы разработки информационно-безопасной инфраструктуры

Для успешной разработки информационно-безопасной инфраструктуры систем военной связи важно провести всесторонний анализ существующих уязвимостей и потенциальных угроз, с которыми может столкнуться система. Этот анализ включает в себя оценку различных сценариев атак, которые могут представлять угрозу для информационной безопасности. К примеру, среди таких угроз могут быть кибератаки различных типов, такие как атаки типа «Man-in-the-Middle» (MITM), перехват трафика или дешифровка передаваемых данных.

Анализ уязвимостей и угроз позволяет идентифицировать основные риски, с которыми может столкнуться система, и выявить уязвимые точки, которые могут быть использованы злоумышленниками для нарушения информационной безопасности. Такой подход позволяет эффективно адаптировать стратегии защиты и разработать соответствующие меры для предотвращения и минимизации потенциальных угроз.

В результате анализа уязвимостей и угроз формируется комплексное представление о текущем состоянии информационной безопасности системы и определяются приоритеты для последующих шагов по защите. Это позволяет разработчикам уделить особое внимание наиболее критическим областям и улучшить общую степень защиты информационной инфраструктуры систем военной связи [3].

После проведения анализа уязвимостей и угроз следующим логическим шагом является проектирование защитных механизмов и технологий, которые обеспечат надежную защиту информационной инфраструктуры военной связи. Этот этап включает в себя разработку комплексной системы безопасности, которая будет эффективно противодействовать потенциальным угрозам.

Одним из основных компонентов защиты является система шифрования. Защита передаваемой информации осуществляется путем применения современных криптографических алгоритмов в том числе отечественных систем шифрования страны разработчика, которые обеспечивают конфиденциальность данных. Это позволяет предотвратить несанкционированный доступ к информации, даже в случае перехвата или прослушивания трафика. Кроме того, важно уделить внимание не только самому алгоритму шифрования, но и его правильной реализации в программном обеспечении, чтобы исключить возможные уязвимости.

Дополнительно к системе шифрования, в проектировании защитных механизмов важное место занимают механизмы аутентификации и контроля доступа. Механизмы аутентификации обеспечивают проверку подлинности пользователей и устройств, что предотвращает несанкционированный доступ к системе. Контроль доступа позволяет управлять правами доступа пользователей и устройств к различным ресурсам и функциям системы, обеспечивая принцип минимальных привилегий и предотвращая несанкционированные действия.

При проектировании защитных механизмов также важно учитывать программное обеспечение (ПО), используемое в рамках инфраструктуры. Это

включает в себя разработку безопасного программного кода, регулярные аудиты безопасности, использование защищенных архитектур и фреймворков, а также обеспечение быстрой реакции на обнаруженные уязвимости и регулярное обновление программного обеспечения. Также, важно обеспечить безопасность прикладных программ, баз данных, операционных систем и других компонентов инфраструктуры для полной защиты от потенциальных атак.

После разработки и внедрения защитных механизмов необходимо провести комплексное тестирование и адаптацию инфраструктуры для обеспечения ее надежной работы. Этот процесс включает в себя несколько видов тестирования, каждый из которых направлен на проверку определенных аспектов функционирования системы.

Модульное тестирование: на этом этапе проводится тестирование отдельных модулей или компонентов информационной инфраструктуры. Целью модульного тестирования является проверка корректности работы каждого модуля в изоляции от остальных частей системы. Это позволяет выявить и исправить возможные ошибки в коде или конфигурации до интеграции компонентов.

Интеграционное тестирование: на этом этапе проводится проверка взаимодействия между различными модулями и компонентами системы. Целью интеграционного тестирования является обеспечение корректной работы системы в целом, а не только отдельных ее частей. В процессе интеграционного тестирования проверяется передача данных между компонентами, обработка ошибок и другие аспекты, связанные с взаимодействием модулей.

Системное тестирование: на этом этапе проводится тестирование всей информационной инфраструктуры в целом. Целью системного тестирования является проверка работы системы в реальных условиях и с использованием реальных данных. В процессе системного тестирования проверяется функциональность системы, ее производительность, надежность и другие характеристики.

Приемочное тестирование: на этом этапе проводится окончательное тестирование системы перед ее внедрением в эксплуатацию. Целью приемочного тестирования является проверка соответствия системы требованиям заказчика и обеспечение ее готовности к использованию. В процессе приемочного тестирования система проверяется на соответствие функциональным и нефункциональным требованиям, а также на удовлетворение потребностей пользователей.

Каждый вид тестирования играет важную роль в обеспечении качества информационной инфраструктуры и позволяет выявить и устранить возможные проблемы и несоответствия в работе системы перед ее внедрением в эксплуатацию [4].

Окончание разработки и внедрения информационно-безопасной инфраструктуры является лишь одним из этапов в обеспечении безопасности систем военной связи. Важным аспектом является постоянная поддержка и

обновление системы, чтобы эффективно реагировать на новые угрозы и изменения в технологическом окружении.

Регулярное обновление защитных механизмов является необходимым для поддержания высокого уровня защиты информационной инфраструктуры. Это включает в себя установку последних обновлений и патчей безопасности, а также внедрение новых методов и технологий защиты, разработанных в ответ на появляющиеся угрозы. Регулярные обновления позволяют минимизировать риски и обеспечивают актуальность системы в условиях постоянно меняющейся среды безопасности.

Одновременно с обновлением защитных механизмов важно обеспечить непрерывное обучение персонала. Обучение персонала позволяет повысить осведомленность о существующих угрозах, обучить персоналу правильным методам работы с защищенной информацией и реагирования на инциденты безопасности. Это помогает укрепить человеческий фактор как важный элемент в общей системе защиты информации.

Проведение аудитов безопасности также играет важную роль в обеспечении безопасности информационной инфраструктуры. Аудиты позволяют выявить потенциальные уязвимости и недостатки в системе, оценить ее с точки зрения соответствия стандартам безопасности и законодательству, а также предложить рекомендации по улучшению системы. Проведение регулярных аудитов обеспечивает контроль за состоянием безопасности и помогает предотвращать возможные инциденты.

Таким образом, постоянная поддержка и обновление информационно-безопасной инфраструктуры являются неотъемлемой частью процесса обеспечения безопасности и гарантируют ее эффективную работу в условиях постоянно меняющейся среды рисков.

Разработка информационно-безопасной инфраструктуры для систем военной связи представляет собой сложный и многоэтапный процесс, требующий не только высокой технической компетенции, но и глубокого понимания современных угроз информационной безопасности. Этот процесс должен быть основан на комплексном подходе, включающем в себя анализ уязвимостей, разработку защитных механизмов, их внедрение, тестирование и постоянное обновление.

Защита коммуникаций военных структур имеет критическое значение для обеспечения национальной безопасности. Успешная реализация информационно-безопасной инфраструктуры не только обеспечивает конфиденциальность, целостность и доступность передаваемой информации, но и способствует эффективному функционированию военных и правительственных органов.

Однако следует отметить, что технологии и методы защиты постоянно эволюционируют, а угрозы информационной безопасности становятся все более сложными и изощренными. Создание надежной инфраструктуры важно, но и обеспечение её непрерывной адаптации и улучшения в соответствии с меняющейся обстановкой безопасности не менее важно.

В заключении отметим, что разработка информационно-безопасной инфраструктуры для систем военной связи является одним из стратегических приоритетов в обеспечении национальной безопасности. Этот процесс требует не только технических решений, но и политической поддержки, а также стратегического видения, чтобы гарантировать эффективную защиту национальных интересов в информационной среде.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1 Браун А. и Джонсон Р. «Протоколы безопасной связи для военных радиостанций» // Обзор оборонных технологий. – 2019. – С.112-125.

2 Смит, Дж. «Меры кибербезопасности для военных систем связи» // Журнал военных технологий, 2020. – С.45–56.

3 Национальный институт стандартов и технологий. «Руководство по обеспечению безопасности систем радиосвязи» // Специальная публикация NIST, 2022. – С.800-204.

4 Грэм Д. и Фьюстер М. «Опыт автоматизации тестирования: примеры автоматизации тестирования программного обеспечения» // Аддисон-Уэсли, 2012. – С.88-100.

УДК 621.391

LORAWAN ЖЕЛІСІ АРҚЫЛЫ АЛЫС ҚАШЫҚТЫҚПЕН ХАБАРЛАМА АЛМАСУ

ОТАРБЕК Н.А., *қызметкер*

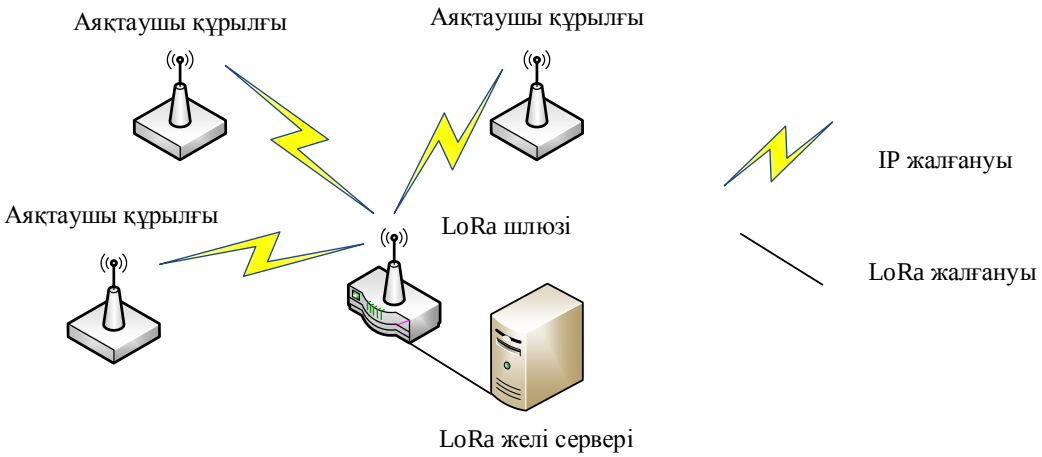
Қазақстан Республикасы Ұлттық қауіпсіздік комитетінің Академиясы, Алматы қаласы

Мақалының өзектілігі қазіргі уақытта жоғары сенімді ведомстволық радиобайланысты жүзеге асыру қажеттілігімен анықталады. Жоғары сенімділікке кепіл беретін қазіргі уақытта радиобайланыстың тұрақтылығын, сондай-ақ сигнал көзін анықтау және басу қиындығын білдіреді. Байланыс технологиясында қолданылатын Chirp (сызықты жиілік модуляциясы) және FHSS – (ағыл. frequency-hopping spread spectrum – жиілікті секіргіш таралу спектрі) сияқты тарату спектрінің технологияларын пайдаланатын сигналдардың шуылға төзімділігі өте жоғары екенін атап өтуге болады, нәтижесінде олардың қолданылуы жыл сайын артып келеді. Тәжірибеде ведомстволық радиобайланыста тек жиілікті секіргіш таралу спектрі технологиясы қолданылады, ол өз кезегінде радиобарлау құралдарымен өте оңай анықталады. Бұл баяндамада LoraWAN стандартында енгізілген сызықты жиілік модуляция спектрін кеңейтумен балама технологияны пайдалану мүмкіндігі талқыланады. Баяндама авторы бұл технологияны ведомстволық радиобайланыс стандартын енгізу үшін пайдалануды ұсынады.

LoRa – интернет заттары үшін инфрақұрылымдық шешім ретінде алға шығарылған ауқымы жағынан ұзақ қашықтықты алатын, аз қуатпен жұмыс жасайтын, бит жылдамдығы төмен, сымсыз телекоммуникация жүйесі. SEMTECH әзірлеген LoRa физикалық деңгейі ұзақ қашықтыққа, төмен қуат пен төмен өткізу қабілеттілігімен байланысты қамтамасыз етеді. LoRa орналастырылған аймаққа байланысты ISM 433, 868 немесе 915 МГц диапазонында жұмыс істейді. Әрбір берілістің пайдалы жүктемесі 2-ден 255 октетке дейін болуы мүмкін, ал арна агрегациясын пайдаланған кезде деректер жылдамдығы 50 Кбит/с дейін жетуі мүмкіндігі бар. Модуляция әдісі – SEMTECH компаниясының петенттелген меншікті технологиясы [1].

LoRaWAN – көптеген аяқтаушы құрылғылар LoRa модуляциясын қолдана отырып, шлюздармен өзара әрекеттесуге мүмкіндік беретін ортаға қол жеткізуді басқаратын механизмін ұсына алады. LoRa модуляциясы патенттелген болса да, LoRaWAN-LoRa Alliance әзірлеген ашық стандарт болып табылады.

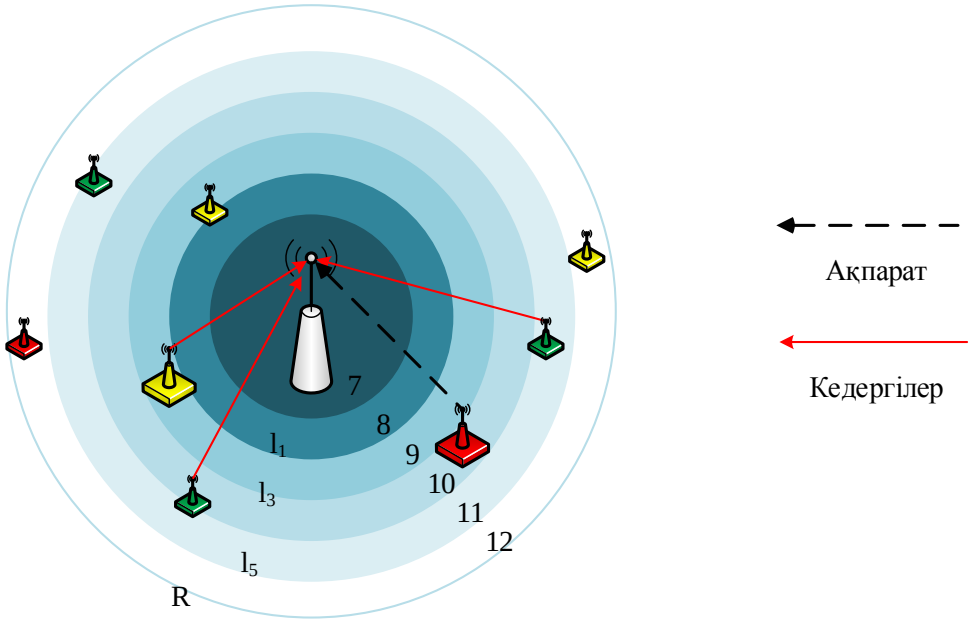
Әдеттегі LoRa желісі 1-суретте көрсетілгендей «жұлдыз» топологиясымен үш түрлі құрылғы түрін қамти алады.



Сурет 1 – LoRa желі архитектурасы

LoRaWAN желісінің негізгі архитектурасы келесідей: аяқтаушы құрылғылар LoRaWAN желісімен және LoRa көмегімен шлюздермен байланыса алады. 1 суретте көрсетілгендей, аяқтаушы құрылғылар шлюздермен LoRa жалғануы арқылы байланысып LoRaWAN желілік серверіне жоғары өткізу қабілеттілігі бар транзиттік интерфейс яғни қолданыстағы Ethernet немесе 3G арқылы жалғанады. Шлюздер тек екі бағытты қайталағыштар немесе протокол түрлендіргіштері бола алады, желілік сервер құрылғылар жіберген пакеттерді декодтауға және құрылғыларға қайта жіберілуі керек пакеттерді жасауға жауап береді. LoRa аяқтаушы құрылғыларының үш класы бар, олар тек төменгі сызықты жоспарлаумен ерекшеленеді.

Келесі мәселе байланыс аймағы, яғни LoRa шлюзі мен аяқтаушы құрылғылардың арасындағы арақашықты есептеу үшін осы мақалада [2] көрсетілген есептеулерді қарастырайық.



Сурет 2 – Бір ғана шлюзден және R км радиуста біркелкі орналасқан бірнеше бір мезгілде жіберетін аяқтаушы құрылғылардан тұратын жоғары байланыстағы жүйені орнату

1 суретте қарастырылғандай, негізгі аяқтаушы құрылғымыз ақпаратты LoRa шлюзіне жіберу сәтінде, басқа аяқтаушы құрылғылардың кедергілеріне қарамай алыс қашықтықтан ақпаратты ала алады, оның ақпарат жіберу жылдамдығы 1 кестеде көрсетілген.

Кесте 1 – Өткізу қабілеттілігі BW=125 КГц үшін 25 байтты хабардың LoRa сипаттамасы [2]

Тарату факторы	Битрейт, Кб/с	Жеткізу уақыты, мс	Сағатына жібереді	Қабылдағыш сезімталдығы	Арақашықтық, км
7	5.47	36.6	98	-123	l_0–l_1
8	3.13	64	56	-126	l_1–l_2
9	1.76	113	31	-129	l_2–l_3
10	0.98	204	17	-132	l_3–l_4
11	0.54	372	9	-134.5	l_4–l_5
12	0.29	682	5	-137	> l_5

1 кестені талдайтын болсақ, ең алыс қашықтықта оның битрейт жылдамдығы 0,29 кбит/с болады, бұл дегеніміз сағатына шамамен 125 байт ақпаратты алыс қашықтыққа жібере алатының көреміз.

Дыбыстық байланыс үшін ең аз битрейт 700 бит/с арқылы ашық бастапқы Codec2 сөйлеу кодекімен пайдалануға болады. Одан жоғары 800 бит/с – FS-1015 мамандандырылған сөйлеу кодектерінде қолданылатын сөзді тану үшін қажетті ең төменгі деңгей. Одан соң 2,15 кбит/с – ашық бастапқы Speex кодекінің минималды бит жылдамдығы болады. Жібере алатын 6 кбит/с – ашық бастапқы Opus кодекінің ең аз бит жылдамдығы болады. Осы мәліметтерге сүйене отырып дыбыстық ақпарат алмасуға қол жеткізе аламыз.

LoRa стандартының шуға төзімділігі [3,4] сипатталған. Атап айтқанда, радиосигналдың деңгейі кедергі шу деңгейінен 20 есе төмен болуы мүмкін, бұл радиобайланыстың құпиялылығын қамтамасыз ете алады. Атап айтқанда, LoRa сигналдарына электрондық радиотаратқыш аппаратураны басуды қолдану өте қиын міндет екенін атап өтуге болады. Жоғарыда сипатталған LoRa артықшылықтары осы стандартты ведомстволық радиобайланыста қолдану сенімділіктің жоғары деңгейін, құпиялылықты және электрондық радиотаратқыш аппаратураны басу мүмкін еместігін қамтамасыз етеді деген қорытынды жасауға мүмкіндік береді.

Қорытындылай келе LoRa желісі бұл тұрақты түрде аз шығын жұмсау арқылы алыс аймақты бірнеше сымсыз шифрланған үздіксіз телефондық байланыспен қамтамасыз ете алатын жаңа телекоммуникация жүйесі [5]. LoRa модуляциясының таралу спектрінің модуляциясына және қабылдағыштың жоғары сезімталдығына байланысты жақсы кедергі иммунитетті қамтамасыз ететінін көрсетеді. LoRa қала маңындағы тығыз ауданда 3 км-ге дейін желіні қанағаттанарлық қамтуды қамтамасыз ете алатынын көрсетеді. Далалық сынақтарда бұл көрсеткіш едәуір жақсырақ болады. LoRa желісі және аяқтаушы

құрылғылардың көмегімен алыс қашықты оңай әрі ұзақ уақытқа бір-бірімен ақпарат байланыстыра аламыз.

ПАЙДАЛАНЫЛҒАН ӘДЕБИЕТТЕР ТІЗІМІ

1. Aloÿs Augustin, Jiazi Yi, Thomas Clausen and William Mark Townsley, A Study of LoRa: Long Range & Low Power Networks for the Internet of Things // licensee MDPI, Basel, Switzerland – 2016.
2. Orestis Georgiou and Usman Raza, Low Power Wide Area Network Analysis: Can LoRa Scale? // IEEE Wireless Communications Letters - 2017.
3. Матаева А.Б., Косяков И.О., Оценка эффективности применения линейно частотной модуляции в сетях LoRa // Вестник КазАТК – 2017 – №100, с 185-189.
4. Косяков И.О. Радиочастотное подавление сигналов с ЛЧМ // Информатика и прикладная математика: Мат. VI Межд. науч. конф. (29 сентября -2 октября 2021 г.). Алматы, 2021. – с. 447-450
5. Emekcan Aras, Gowri Sankar Ramachandran, Piers Lawrence and Danny Hughes: Exploring The Security Vulnerabilities of LoRa // iMinds-DistriNet, KU Leuven, 3001 Leuven, Belgium - 2017.

УДК 355/359

ОТКРЫТЫЙ ЕВРОПЕЙСКИЙ СТАНДАРТ ЦИФРОВОЙ РАДИОСВЯЗИ DMR

ДУЙСЕМБЕКОВ О.А., *к.т.н., подполковник*
ШАНДРОНОВ Д.Н., *доктор PhD, полковник*

Военно-инженерный институт радиоэлектроники и связи,
г. Алматы, Республика Казахстан

Аннотация. В данной статье рассматривается вывод и распространение стандарта DMR (Digital Mobile Radio), проведен краткий анализ технологий цифровой радиосвязи, указаны преимущества технологии DMR в сравнении с аналогичными или похожими технологиями. Описаны механизмы частотного и временного разделения каналов, дуплексного разноса частот, раскрыта организация и работа логических каналов Технология DMR предоставляет повышенную эффективность использования радиочастотного ресурса, а также позволяет сократить количество оборудования. Использование технологии DMR позволяет значительно сэкономить средства на внедрение и эксплуатацию. Расширенная зона действия оборудования обеспечит более долгий срок автономной работы радиостанции, дополнительные функции передачи помогают пользователю работать более эффективно и результативно.

Ключевые слова: стандарт DMR, передача данных, канал, радиосвязь, радиостанция, диапазон, конвенциональная радиосвязь, транкинговая радиосвязь, индивидуальный вызов, групповой вызов, логический канал связи, акустические помехи, цифровая обработка сигнала.

Ассоциация DMR (DMR Association). Эта структура, основанная девятью компаниями – производителями и поставщиками абонентских устройств и сетевого оборудования в сфере цифровой радиосвязи (Motorola, CML Microcircuits, Funkwerk Koelleda, Fylde Micro, Icom, Kenwood, SELEX Communications (Finmeccaninca), Tait Radio Communications и Vertex Standard), продолжила дело своего предшественника – DMR MOU. Целью новой организации заявлен вывод стандарта DMR (Digital Mobile Radio) «на новый уровень, что обеспечивает в его рамках совместимость различного оборудования и стимулирующий развитие новых сервисов и устройств. Данный стандарт должен постепенно стать приоритетным для профессиональных пользователей конвенциональной и транкинговой цифровой радиосвязи».

В основу технологии DMR составляют TDMA (Time Division Multiple Access – многостанционный доступ с временным разделением каналов), что позволяет разместить два временных интервала (независимых логических канала) на одной частотной несущей с сеткой частот 12,5 кГц. Тип модуляции – 4FSK (четырехуровневая частотная манипуляция). Гибкость, заложенная в рамках стандарта DMR, позволяет реализовывать решения не только в

классических диапазонах 136-174 МГц и 403-470 МГц, но во всем спектре частот от 50 до 999 МГц. Причем дуплексный разнос для решений с применением точки ретрансляции допускается любым, в том числе классической частотой 4,6 МГц для диапазона 160 МГц и 45 МГц для диапазона 900 МГц. Дуплексный разнос определяется 15-битной сигнальной последовательностью в структуре цифрового кода стандарта DMR [1].

Как известно, в последнее время мало представляются открытых цифровых решений для диапазонов частот ниже 400 МГц. Суррогатные схемы с интеграцией модулей оцифровки в аналоговые радиостанции не позволяли реализовать преимущества работы, заложенные в рамках стандарта DMR. Теперь же решения с применением технологии DMR станут актуальны в условиях сложной электромагнитной обстановки и многолучевого распространения сигнала.

В соответствии с технологией временного уплотнения на одном частотном канале организуются 2 логических канала. Важным условием с точки зрения планирования конвенциональной сети радиосвязи является то, что в режиме прямой связи (без использования ретранслятора) в настоящее время задействуется лишь один логический канал из двух доступных. Это характерное обстоятельство объясняется отсутствием точки синхронизации для одновременной передачи двумя абонентскими терминалами (радиостанциями). В этом случае преимущества прямого режима по отношению к аналоговому режиму в части увеличения канальной емкости не будет.

Длительность временного интервала, организующего 1 логический канал, составляет 30 мс. Из них 27,5 мс отведены под полезную нагрузку, составляющую 216 битов, и под 48 сигнальных битов. Защитный межинтервальный разнос – 2,5 мс. Таким образом, канальная скорость передачи данных 2160 бит/с. В случае передачи пакетных данных следует учитывать, что в зависимости от длины IP-пакетов процент полезных данных будет снижаться за счет заголовков IP-пакетов [2].

Существует три разновидности, или уровня (tier), стандарта DMR.

DMR Tier I – простейший вариант технологии, ориентированный на работу в нелицензируемом диапазоне 446 МГц, полоса 12,5 кГц, доступ FDMA. Устройства DMR Tier I (как и dPMR 446, который тоже относится к Tier I) предназначены для работы в режиме peer-to-peer, т.е. без сетевой инфраструктуры. Максимальная мощность пользовательского оборудования - 0,5 Вт. Технология может применяться в комбинации с аналоговой PMR 446. Ввиду отсутствия ретранслятора удвоение спектральной эффективности в данном варианте недостижимо. Оборудование DMR Tier I ориентировано на частных пользователей и малые предприятия, которым не требуются большая зона покрытия и расширенные возможности радиосвязи. Количество каналов на этом уровне ограничено, не используются ретрансляторы и недоступны сетевые возможности.

DMR Tier II – стандарт конвенциональной связи, охватывающий лицензируемые частоты от 66 до 960 МГц. Оборудование этого стандарта

предназначено для тех пользователей, которым необходимы качественная передача голоса, интегрированная возможность передачи данных и более эффективное использование спектра, а также для профессиональных портативных, автомобильных радио и ретрансляторов. Для DMR Tier II определена двухслотовая технология TDMA, используется полоса 12,5 кГц.

DMR Tier III описывает транкинговую связь в диапазонах 66-960 МГц. Здесь также используется двухслотовая TDMA в канале 12,5 кГц. DMR Tier III призван заменить стандарт аналоговой транкинговой связи MPT-1327, добавив к его возможностям более эффективное использование спектра, на этом уровне реализуются все возможности DMR работа с ретрансляторами и внешними антеннами, передача данных всех типов, в том числе по протоколам IPv4 и IPv6 [3].

В настоящее время общедоступным является оборудование DMR Tier II, и сам стандарт DMR чаще всего упоминается как стандарт конвенциональной связи.

Важным, с точки зрения регулирующих органов, является то обстоятельство, что существующая сетка частот 12,5 кГц сохраняет свою целостность при внедрении решений стандарта DMR, что, в свою очередь, позволит пользователям осуществить плавную миграцию собственных средств связи от аналоговых технологий к цифровым, увеличивая канальную емкость в 2 раза.

В данное время основными производителями средств профессиональной радиосвязи стандарта DMR являются компании Motorola и Hytera Communications Co., Ltd.

Цифровой стандарт передачи DMR гарантирует стабильное качество речи на всей дистанции связи между корреспондентами за счет перевода звукового сигнала в цифровой код. Более того, использование специальных аудио кодеков позволяет исключить из эфира акустические шумы и сделать речь приятной для восприятия. Современные математические механизмы работы с кодом исправляют ошибки в пакетах на грани зоны радиопокрытия, что позволяет увеличить расстояние устойчивой связи. Помимо улучшения качества радиосвязи связи, в два раза увеличилось время автономной работы портативных радиостанций, использующих стандарт DMR.

Качество передачи речи. Вокодер с алгоритмом ACELP (линейное предсказание с возбуждением от алгебраической кодовой книги) особенно подходит для использования в условиях сильных акустических помех. Для обнаружения ошибок при передаче в канале радиосвязи и их исправления при канальном кодировании применяется технология Forward Error Correction (FEC) и механизмы CRC (Cyclic Redundancy Code) [4].

Стандарт защищает от прослушивания. Открытость каналов аналоговой связи доставляла известные неудобства при работе в канале, особенно в тех случаях, когда инструменту оперативной радиосвязи отводится ключевая роль в процессах работы. Повсеместное использование гражданами и организациями радиостанций с широким диапазоном частот приводило к возможности

прослушивания рабочих каналов и помехам в работе. Переход на цифровой стандарт позволяет исключить прослушивание эфира аналоговыми радиостанциями, а учитывая возможность шифрования цифрового сигнала штатными средствами рации, практически сводит к нулю возможность прослушивания и постановки помех другими участниками эфира.

Говоря о дальности связи, стоит упомянуть, что достигаемые результаты зависят не только от наличия естественных природных преград, но и от окружающей электромагнитной обстановки.

Основные возможности DMR. Стандарт DMR постоянно совершенствуется, реализуя функциональный набор, ранее нехарактерный для сектора средств конвенциональной радиосвязи.

К основным функциональным возможностям цифрового стандарта DMR следует отнести:

− цифровую обработку сигнала;

− управление аккумуляторной батареей;

− приоритетный аварийный вызов;

− удаленный контроль;

− опциональное шифрование;

− одновременную передачу голоса и данных (в том числе пакетных);

− работу в аналоговом режиме, что особенно актуально при постепенной миграции аналоговых конвенциональных систем.

Типы вызовов, реализуемых в рамках стандарта DMR:

− индивидуальный вызов «радиостанция – радиостанция»;

− групповой вызов «радиостанции – группа радиостанций»;

− групповой вызов «радиостанция – все радиостанции»;

− передача пакетных данных с канальной скоростью 2 кбит/с.

Стандарт DMR отличает быстрое установление вызова (до 200 мс) и поддержка режима «поздний вход» для групповых вызовов [5].

Цифровой стандарт радиосвязи DMR взяла на вооружение крупнейшими производителями связного оборудования. На сегодняшний день не встретим среди модельного ряда абонентских радиостанций Motorola, Icom, Kenwood аналоговых устройств и этому есть ряд причин. Помимо улучшения качества радиосвязи, в два раз увеличилось время автономной работы портативных радиостанций, использующих стандарт DMR.

Вот лишь некоторые аргументы в пользу стандарта DMR:

− конфиденциальность - защита сеанса связи от прослушивания, включая шифрование на уровне 256 бит;

− устойчивость к акустическим помехам за счет высокого качества и разборчивости речи;

− передача данных, включая сообщения, GPS координаты, изображения и т.д.;

− эффективное использование частот – два канала связи DMR вместо одного в аналоговом режиме;

− значительное увеличение времени работы от аккумуляторных батарей;

− широкие возможности и низкая стоимость оборудования при построении радиосетей;

− интеграция с различными сторонними системами для наращивания функционала.

В настоящее время существуют две серии оборудования стандарта DMR – на диапазоны 136...174 МГц и 403...470 МГц. Полевые испытания оборудования показали существенный выигрыш по отношению к аналоговым сетям при использовании радиостанций в городских условиях и многолучевом распространения сигнала:

− улучшенный режим «свободные руки»;

− встроенный приемник GPS сигналов для реализации приложений по контролю местоположения;

− дуплексный вызов (в проекте).

Новый европейский стандарт используется достаточно большой популярностью у пользователей, со временем требования к возможностям профессиональной радиосвязи повышались, и соответственно сервисы улучшилось.

Подводя итог можно выделить следующие преимущества DMR:

− временное разделение канала на два тайм-слота ведет к двойной экономии частотного ресурса и заряда аккумуляторов;

− улучшенное качество связи по всей зоне покрытия;

− большие возможности, заложенные в технологии, потенциал для реализации нестандартных решений.

Новый стандарт цифровой радиосвязи обеспечивает лучшие характеристики и большую функциональность систем профессиональной радиосвязи.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1 Названов А.И. Технология цифровой мобильной связи DMR. – М.: Omoled.ru, 2016. – 6 с.

2 Петренко В.И., Рачков В.Е., Иванов Ю.В. Системы и средства подвижной радиосвязи:. Учебное пособие / Под ред. В.И. Петренко. – Ставрополь: СВИС РВ, 2010. – 231 с.

3 Дмитриев В.И. Стандарты и технология подвижной радиосвязи и беспроводной передачи данных. СПБ, ВАС, 2016. – 328 с.

4 Берлин А.Н. Телекоммуникационные сети и устройства. Учебное пособие. Москва, издательство: Бином. 2012. – 319 с.

5 Петренко В.И. Рачков В.Е. Иванов Ю.В. Системы и средства подвижной радиосвязи. Учеб. пособие. Ставрополь: СВИС РВ, 2010. – 231 с.

УДК 007/52

РАДИОБАЙЛАНЫСТА ҚАЙТАЛАҒЫШ ҚҰРЫЛҒЫСЫН ҚОЛДАНУ

ДУЙСЕМБЕКОВ О.А., *т.ғ.к., подполковник,*
ЖАНБУЛАТОВ Д.М., *т.ғ.м., подполковник*

Радиоэлектроника және байланыс әскери инженерлік институты,
Алматы қаласы, Қазақстан Республикасы

Түйіндеме. Бұл мақалада радиобайланыстағы екі станция арасындағы кедергілерге байланысты немесе қашықтықта тікелей байланыс мүмкін болмаған жағдайда хабарлама беру үшін маңызды элемент болып табылады қайталағыш құрылғысы тұралы мәліметтер кеңінен қарастырылған.

Мақала барысында қазіргі кездегі радиобайланыста кеңінен қолданыс тапқан қайталағыштың тарату қуаты, жиілік диапазоны және күшейту сияқты негізгі сипаттамалары ашып көрсетілген. Жәнеде радиобайланыстағы қайталағыштың жұмыс принциптері, сипаттамалары және негізгі қолданылу аясы тұралы мағлұматтар берілген.

Қайталағыш құрылғысының сигналдарды ұзақ қашықтыққа жіберуге арналған антенналары, сигнал күшін арттыруға арналған күшейткіші және жиілікті түрлендіруге арналған араластырғыш сияқты негізгі құрамының жұмысы ашып көрсетілген.

Түйін сөздер: қайталағыш, радиобайланыс, радиотехникалық құрылғы, радиостанция, күшейткіш, түрлендіргіш, жиілік диапазоны, байланыс ауқымы, қамту аймағы, хабарлама.

Реле (қайталағыш) – дегеніміз латын тілінен аударғанда жаңартуды, әрекеттің қайталануын және аудармашы, сөзбе-сөз тасымалдаушы дегенді білдіреді, ол радиотехникалық құрылғы, жасанды электр өткізгіш орта немесе радио желісінің аралық нүктесі ретінде (радиорелелік, ғарыштық байланыс) пайдаланылатын аспан денесі болып табылады.

Радиобайланыстағы қайталағыш кедергілерге немесе қашықтыққа байланысты екі станция арасындағы тікелей байланыс мүмкін болмаған жағдайда хабарлама беру үшін маңызды элемент болып табылады. Мұндай жүйе радио сигналдарды бір станциядан екіншісіне беруге мүмкіндік береді жәнеде оларды беру жүйесінде күшейтеді.

Қайталағыштың жұмыс негізі бірінші станцияда сигналды қабылдау, оны күшейту және сигналды қалпына келтіруге және одан әрі беруге болатын басқа станцияға жіберу болып табылады. Бұл ұзын сымдарды немесе басқа физикалық құралдарды қажет етпестен радиобайланыста ұзақ мерзімді байланысқа мүмкіндік береді.

Радиобайланыстағы қайталағыштың негізгі сипаттамаларына тарату қуаты, жиілік диапазоны және күшейту кіреді. Тарату қуаты сигналдың қаншалықты берілетінін анықтайды, ал жиілік диапазоны қайталағышты қандай шектерде қолдануға болатындығын анықтайды. Күшейту сигналдың берілу кезінде қаншалықты артыратынын көрсетеді.

Радиобайланыстағы қайталағыштар сигналмен нашар қамтылған жерлерде, мысалы, таулы аймақтарда немесе теңіз кеңістігінде белсенді қолданылады. Олар сондай-ақ әртүрлі радиобайланыстарда, соның ішінде әскери салалардың шұғыл коммуникацияларында маңызды рөл атқарады. Қайталағыштардың арқасында радиобайланыстағы байланыс сенімдірек және пайдаланушылардың кең ауқымы үшін қолжетімді болады [1].

Радиобайланыстағы қайталағыш – бұл сигналды таратқыштан қабылдағышқа қайта жіберу арқылы радио сигналдарды ұзақ қашықтыққа жіберуге мүмкіндік беретін құрылғы. Ол алыс қашықтықта және кедергі кезінде байланыс орнатуда шешуші рөл атқарады.

Қайталағыштың негізгі жұмыс принципі – таратқыштан сигнал қабылдау, оны күшейту және қабылдағышқа басқа жиілікке беру. Қайталағыштар әртүрлі жиілік диапазондарында, соның ішінде қысқа толқынды, ультрақысқа толқынды диапазондарда жұмыс істей алады.

Қайталағыш қабылдағыш таратқыштан сигнал алады және оны электр сигналына айналдырады. Содан кейін сигнал қажетсіз кедергілерді жою және сигнал күшін арттыру үшін сүзгілер мен күшейткіштер арқылы өтеді.

Әрі қарай, сигнал қайталағыштың таратқыш бөлігіне түседі, онда оны басқа жиілікке модуляциялау жүреді. Модуляция байланыс жүйесінің түріне байланысты аналогтық немесе сандық болуы мүмкін [2].

Модуляциядан кейін сигнал қайталағыш антеннаға беріледі, ол оны ауаға шығарып таратады. Антенна радиобайланыста маңызды рөл атқарады, өйткені ол алыс қашықтыққа сигнал беруді қамтамасыз етеді.

Байланыстың екінші жағында қабылдағыш орнатылады, ол қайталағыштан сигнал алады. Қабылдағыш сигналды қайтадан электрге айналдырады және демодуляция және декодтау сияқты одан әрі өңдеуді жүзеге асырады.

Қайталағыштарды телекоммуникация, азаматтық және әскери радиобайланыс сияқты әртүрлі салаларда қолдануға болады. Олар байланыс сапасын жақсартуға, қамту аймағын кеңейтуге және ұзақ қашықтыққа сенімді сигнал беруді қамтамасыз етуге мүмкіндік береді.

Радиобайланыстағы қайталағыштың жұмыс принципі

Радиобайланыстағы қайталағыш – бұл сигналды басқа жиілікке ауыстыру арқылы радио сигналдарды алыс қашықтыққа беру үшін қолданылатын құрылғы. Ол сигналдың нашар қамтылған аймақтарында немесе шалғай аудандар арасында байланыс орнатуда маңызды рөл атқарады.

Қайталағыштың негізгі жұмыс принципі – ол радио сигналдарды бір жиілікте қабылдайды, оларды күшейтеді және алыс қашықтыққа беру үшін басқа жиілікке аударады. Сигналды бір жиіліктен екіншісіне ауыстырудың бұл процесі жиілікті түрлендіру деп аталады.

Қайталағыш бірнеше негізгі компоненттерден тұрады, соның ішінде сигналдарды қабылдауға және беруге арналған антенналар, сигнал күшін арттыруға арналған күшейткіш және жиілікті түрлендіруге арналған араластырғыш. Антенналар сигналдарды белгілі бір жиілікте қабылдау және

беру үшін қолданылады, ал күшейткіш сигналдың қуатын арттырады, осылайша ол байланыс жолындағы кедергілерді жеңе алады. Араластырғыш сигналдың жиілігін басқа жиілікке ауыстыру арқылы түрлендіреді, осылайша оны ұзақ қашықтыққа жіберуге болады [3].

Радиобайланыстағы қайталағыштар алыс қашықтыққа байланыс орнату үшін коммерциялық және мемлекеттік ұйымдарда кеңінен қолданылады. Олар нашар қабылдау аймақтарында сигналмен қамтуды жақсартуға және шалғай аудандар арасындағы байланысты қамтамасыз етуге мүмкіндік береді. Радиобайланыста қайталағыштың жұмыс істеу принципі сигнал жиілігін түрлендіруге негізделген, бұл сигналды ұзақ қашықтыққа жіберуге және сенімді байланыс орнатуға мүмкіндік береді.

Радиобайланыстағы қайталағыштың негізгі сипаттамалары.

Радиобайланыстағы қайталағыш – бұл радио сигналдарды бір жиілікте қабылдайтын және оларды осы немесе басқа жиілікте жіберетін құрылғы. Қайталағыштың негізгі функциясы – радиоқабылдағыштарды қайталау және күшейту, бұл радиобайланысты қамту аймағын ұлғайтуға және байланыс сапасын арттыруға мүмкіндік береді.

Алайда, негізгі функциядан басқа, қайталағыштар осы құрылғыларды таңдау және пайдалану кезінде ескеру қажет бірқатар маңызды сипаттамаларға ие:

Жиілік диапазоны: қайталағыштарды белгілі бір жиілік диапазонында жұмыс істеу үшін арнайы ұйымдастыруға болады. Қайталағышты таңдағанда, оның жиілік диапазоны пайдаланылатын радиобайланыс диапазонына сәйкес келетініне көз жеткізу керек.

Таратқыштың қуаты: қайталағыш таратқыштың қуаты байланыс ауқымы мен сапасын анықтайды. Таратқыштың қуаты неғұрлым жоғары болса, қамту аймағы соғұрлым кең болады және байланыс сапасы жақсарады. Алайда, жоғары қуат кедергілерге әкелуі мүмкін, сондықтан таратқыштың қуатын пайдалану бойынша бекітілген ұсыныстарды сақтау қажет [4].

Қабылдағыштың сезімталдығы: қайталағыш қабылдағыштың сезімталдығы оның әлсіз радио сигналдарын қабылдау және оларды басқа жиілікке беру қабілетін анықтайды. Қабылдағыштың сезімталдығы неғұрлым жоғары болса, байланыс сапасы соғұрлым жақсы және қамту аймағы кеңірек болады.

Шу деңгейі: қайталағыштың шу деңгейі, қабылдағыштың сезімталдығы сияқты байланыс сапасына әсер етеді. Шу деңгейі неғұрлым төмен болса, байланыс сапасы соғұрлым жақсы болады және сигналға кедергі аз болады.

Жұмыс режимі: қайталағыштар әртүрлі режимдерде жұмыс істей алады олар – қарапайым немесе дуплексті болып келеді. Қарапайым режимде қайталағыш тек радио сигналдарды басқа жиілікте қайталайды, ал дуплексті режимде ол радио сигналдарды бір уақытта қабылдап, таратып жібере алады.

Қайталағышты дұрыс орнату және пайдалану ерекше маңызды. Жиілік диапазонын, таратқыш қуатын және басқа өнімділікті пайдалану талаптарын орындамау радиобайланыстың бұзылуына және кедергілердің пайда болуына

әкелуі мүмкін. Сондықтан, қайталағышты қолданар алдында оның нұсқауларымен және орнату және пайдалану бойынша ұсыныстарымен танысу қажет.

Радиобайланыстағы қайталағыштың маңызына тоқталсақ, Қайталағыш – бұл радиобайланыста маңызды рөл атқаратын құрылғы екені баршамызға мәлім. Ол таратқыштан қабылдағышқа берілетін радио сигналды күшейтуге және қайталауға мүмкіндік береді. Қайталағыштар радиобайланыстың әртүрлі салаларында, соның ішінде ұялы байланыс, көлік жүйелері, радиожиілікті зерттеу кезінде қолданылады.

Қайталағыштың негізгі қызметі – радиобайланыстың сапасы мен ауқымын жақсарту. Бұл сигналдарға кедергілерді жеңуге, тарату ауқымын арттыруға және сенімді байланыс орнатуға мүмкіндік береді. Қайталағыштардың қолдана отырып сигналдарды алыс қашықтыққа жіберуге болады, тікелей байланыс мүмкін емес алыс жерлерде сонымен қатар қол жетімді жақын аймақтарға байланыс орнатуға болады [5].

Радиобайланыста қайталағыштар сигналды күшейту және оны сапаны жоғалтпай айтарлықтай қашықтыққа беру қажет болған жағдайларда кеңінен қолданылады. Бұл, әсіресе, қауіпсіздік жүйелері, шұғыл операциялар немесе коммерциялық коммуникациялар сияқты үздіксіз байланыс қажет болған жағдайларда қолданылады.

Қайталағыштар әлсіз сигнал мәселелерін, кедергілерді және тарату жолындағы кедергілерді жою арқылы радиобайланыстың тиімділігін арттырады. Олар кез-келген жағдайда тұрақты және сенімді байланыс орната отырып, сөйлеу және деректер сапасын жақсартуға мүмкіндік береді.

Сонымен қатар, қайталағыштар радио желісін қамтуды арттыруға және шалғай немесе қол жетімсіз жерлерде байланыс орнатуға мүмкіндік береді. Олар мұнаралар, ғимараттар немесе таулар сияқты биік жерлерге орнатылып, сигналды алыс қашықтыққа жібереді. Осының көмегімен қайталағыштар шалғайдағы ауылдық жерлерде, терең аңғарларда немесе нашар қамтылған жерлерде байланыс орнатады.

Радиобайланыстағы қайталағыштың маңыздылығын асыра бағаламау қиын. Ол радио желілерінің инфрақұрылымының ажырамас бөлігі болып табылады және тұрақты, сапалы және сенімді байланысты қамтамасыз етеді. Қайталағыштардың арқасында сигналдар кедергілерді жеңе отырып ұзақ қашықтыққа жіберіледі, бұл оларды заманауи радиобайланыста таптырмас құрылғы болып табылады [6].

Радиобайланыста қайталағышты қолдану.

Қайталағыштар радиосигналмен қамту аймағын кеңейту үшін радиобайланыста кеңінен қолданылатынын айтып өттік. Олар сигналды алыс қашықтыққа жіберуге немесе таулар, ғимараттар, ормандар және басқа кедергілер сияқты кедергілерді жеңуге мүмкіндік береді.

Қайталағыштың негізгі міндеті – әлсіз кіріс радио сигналын күшейту және оны үлкен қашықтыққа немесе жетуі қиын жерлерге беру. Қайталағыштар радиосигналды таратуды қажет ететін әртүрлі салаларда, соның ішінде таулы

аудандарда, биік ғимараттары бар қалаларда, ауылдық жерлерде және т. б. қолданылады.

Радиобайланыста қайталағыштардың негізгі қолданылуы.

Ұялы байланыс: қайталағыштарды ұялы байланыс операторлары сигналды күшейту және базалық станциялардан қашықтығына қарамастан сенімді қамтуды қамтамасыз ету үшін пайдаланады. Қайталағыштардың арқасында таулы шатқалдардың тереңдігінде, шалғай аудандарда және басқа да нашар қамтылған жерлерде байланыс қамтамасыз етіледі [7].

Радиолокация: қайталағыштар радарлар сияқты радиолокациялық жүйелердің қамту аймағын кеңейту үшін қолданылады. Олар объектілерді ұзақ қашықтыққа, сондай-ақ қатты кедергілер мен физикалық кедергілер жағдайында анықтауға және бақылауға мүмкіндік береді.

Авиациялық байланыс: авиацияда қайталағыштар ұшу кезінде ұшақтармен байланысты қамтамасыз ету үшін қолданылады. Олар байланыс сапасын жақсартуға әсіресе шалғай аудандар мен әуе кеңістігінде үлкен мүмкіндіктер береді.

Спутниктік байланыс: қайталағыштар жерсеріктік станциядан жердегі антенналарға радио сигналын күшейту және беру үшін қолданылады. Олар рельефтің қиын жағдайында немесе ауа-райының қолайсыздығында спутникпен тұрақты байланыс орнатады.

Радиобайланыста қайталағыштарды қолдану ұзақ қашықтықта және қатты кедергі жағдайында тұрақты және сапалы байланысты қамтамасыз етуде маңызды рөл атқарады. Олар радиосигналмен қамту аймағын кеңейтуге және қол жетпейтін жерлерде байланыс орнатуға мүмкіндік береді, бұл байланыс көптеген қызмет салаларында маңызды рөл атқаратын қазіргі әлемде ерекше маңызды [8].

Қорытындылай атқанда қайталағыш – бұл бірнеше бірнеше рөлдерді атқаратын және оның тиімділігі мен функционалдығын анықтайтын бірқатар негізгі сипаттамаларға ие радиобайланыстағы маңызды құрылғы. Атап айтқанда:

Сигналды күшейту.

Радиобайланыстағы қайталағыштың негізгі рөлдерінің бірі – әлсіз немесе нашар қабылданатын сигналдардың күшеюі. Бұл әсіресе қабылдау сапасы төмен жерлерде, мысалы, шалғай аудандарда немесе радиотолқындардың өткізгіштігі нашар ғимараттардың ішінде өте маңызды. Қайталағыш әлсіз сигналды қабылдайды және оны күшейтеді, бұл байланыс сапасын жақсартуға мүмкіндік беретіні сөзсіз.

Сигналды қайталау.

Қайталағыштың екінші рөлі – сигналды қайталау. Егер әлсіз немесе сапасыз сигналды қолайлы деңгейге дейін күшейту мүмкін болмаса, қайталағыш оны қабылдап алып, алыс қашықтыққа, тау жоталары немесе ғимараттар сияқты кедергілер арқылы қайталай алады.

Қамту аймағын кеңейту.

Қайталағыш радиобайланыс аймағын кеңейте алады, ол қол жетімді емес немесе шектеулі жерлерде байланыс орнатады. Сигналды күшейту және қайталау арқылы қайталағыш шу мен сигналдың жоғалуын азайтуға, байланыс ауқымын арттыруға және сапалы қосылымды қамтамасыз етуге мүмкіндік береді.

Байланыс сапасын жақсарту.

Қайталағыш байланыс сапасын жақсартуға да ықпал етеді. Күшейткіш сигналды қайталаушы рөлінің арқасында, таратқыштан қабылдағышқа берілетін сигналдағы кедергілер мен бұрмалануларды жоя алады. Бұл маңызы әсіресе электромагниттік кедергі деңгейі жоғары немесе радиобайланысты көп пайдаланатын жерлерде көптеп сезініледі.

Қайталағыштар бейне хабар тарату, ұялы байланыс, спутниктік байланыс және жалпы радиобайланыс сияқты салаларда кеңінен қолданылады. Олардың сигналды күшейту және қайталау сияқты функциялары байланыс сапасын едәуір жақсартады және қамту аймағын кеңейтеді, бұл оларды қазіргі радиобайланыстың ажырамас бөлігі етеді.

ПАЙДАЛАНЫЛҒАН ӘДЕБИЕТТЕР ТІЗІМІ:

1 Петренко В.И., Рачков В.Е., Иванов Ю.В. Системы и средства подвижной радиосвязи:. Учебное пособие / Под ред. В.И. Петренко. – Ставрополь: СВИС РВ, 2010. – 231 с.

2 Дмитриев В. И. Стандарты и технология подвижной радиосвязи и беспроводной передачи данных. СПБ, ВАС, 2016. – 328 с.

3 Рекомендация МСЭ-RP.530-15 (09/2013) Данные о распространении радиоволн и методы прогнозирования, требующиеся для проектирования наземных систем прямой видимости.

4 Берлин А.Н. Телекоммуникационные сети и устройства. Учебное пособие. Москва, издательство: Бином. 2012. – 319 с.

5 Берлин А.Н. Телекоммуникационные сети и устройства. Учебное пособие. М.: Бином. – 2012. – 319 с.

6 Дуйсембеков О.А., Дмитриев В.И., Мустафин С.К., Пылаев Н.А. Расчет радиуса зоны покрытия мобильного комплекса технических средств ВПА - фидерной системы ПВ «Старт-1Р». 71-я Всероссийская научно-техническая конференция, посвящённая Дню радио. – СПб. СПбГЭТУ «ЛЕТИ». – 2016. – 213 с.

7 URL: https://stud.kz/referat/show/68664

8 URL: https://www.yaneuch.ru/cat_34/azrg-zamany-jelektrlk-ajlanys/488771.3197059.page5.html#

ӘОЖ 004.9

QAMAL БЛОКТЫҚ СИММЕТРИЯЛЫҚ ШИФРЛАУ ЖҮЙЕСІ АРҚЫЛЫ ӘСКЕРИ РАДИОБАЙЛАНЫС ЖҮЙЕСІН ҚОРҒАУ

ТЕМИРБЕКОВА Ж.Е., *қызметкер*
АРЫН Ғ.Б., *қызметкер*

ҚР ҰҚК академиясы, Қазақстан Республикасы, Алматы қаласы

Аңдатпа. Әскери радиобайланыс әскери операцияларда қауіпсіздік пен тиімділікті қамтамасыз етудің маңызды аспектісі. Киберқауіпсіздікке және үнемі дамып келе жатқан кибершабуыл қаупіне назар аудара отырып, жіберілетін ақпаратты қорғау деректердің құпиялылығы мен тұтастығын сақтаудың негізгі міндеті. Радиобайланыстағы қауіпсіздікті қамтамасыз етудің ең тиімді әдістерінің бірі – блоктық симметриялы шифрлауды қолдану. Зерттеу жұмысында әскери радиобайланыс жүйесін қорғау контекстінде блоктық симметриялық шифрлауды, атап айтқанда QAMAL алгоритмін пайдалану зерттелінді. Әзірленген QAMAL алгоритмі берілген деректердің құпиялылығын, тұтастығын және аутентификациясын қамтамасыз ететін қауіпсіздік пен тиімділіктің жоғары дәрежесіне ие. Мақалада QAMAL алгоритмінің құрылымы, кілттерді генерациялау процедуралары, S-box ауыстыру, Mixer1 және Mixer2 егжей-тегжейлі қарастырылды. QAMAL алгоритмін әскери радиобайланыс контекстінде қолданудың артықшылықтары, мысалы, шабуылдарға жоғары қарсылығы, қауіпсіздік параметрлерін конфигурациялаудағы икемділік, шифрлау мен кері шифрлаудың жоғары жылдамдығы зерттелінді.

Түйін сөздер: QAMAL алгоритмі, блоктық симметриялық шифрлау, биттік кілттер, криптографиялық операциялар, массив, раундтық кілттер.

Кіріспе.

Блоктық симметриялық шифрлау – бұл деректерді белгілі бір өлшемдегі бекітілген блоктарға бөлетін шифрлау әдісі. Әрбір деректер блогы басқа блоктардан тәуелсіз шифрланады, бұл деректердің қауіпсіздігі мен тұтастығының жоғары деңгейін қамтамасыз етеді. Әскери радиобайланыс жіберілетін деректерді қорғауға ерекше назар аударуды қажет етеді, өйткені оларда құпия ақпарат пен стратегиялық маңызды командалық хабарламалар болуы мүмкін. Блоктық симметриялық шифрлауды қолдану әскери радиобайланыстың қауіпсіздігін қамтамасыз ету үшін төмендегідей артықшылықтары бар:

– Деректердің құпиялылығы: блоктық симметриялық шифрлау деректердің құпиялылығының жоғары деңгейін қамтамасыз етеді, өйткені әрбір ақпарат блогы тек байланыс мүшелеріне белгілі құпия кілт арқылы шифрланады.

– Интеграцияланған аутентификация: кейбір блоктық шифрларды шифрлау процесіне аутентификацияны қосу үшін конфигурациялауға болады, бұл деректерді бұрмалаудан және шабуылдардан қорғауды қамтамасыз етеді.

– Тиімділік және өнімділік: оңтайландырылған криптографиялық түрлендірулердің арқасында QAMAL алгоритмі жоғары жұмыс жылдамдығына және төмен есептеу құнына ие.

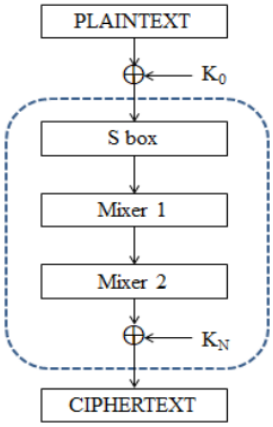
– Іске асырудың қарапайымдылығы: QALQAN, QAMAL, AES (Advanced Encryption Standard) сияқты блоктық симметриялы шифрлар кең таралған және оңай жүзеге асырылады [1].

Қазіргі әскери радиобайланыс жіберілетін ақпаратты рұқсатсыз алудан және өзгертуден қорғаудың жоғары деңгейін талап етеді. Блоктық симметриялық шифрлау мұндай орталарда деректердің құпиялылығын қамтамасыз етудің ең тиімді әдістерінің бірі болып табылады. QAMAL алгоритмі шабуылдарға жоғары қарсылық пен тамаша өнімділікке ие блоктық симметриялық шифрлау саласындағы соңғы жетістіктердің бірі болып табылады. QAMAL алгоритмі әртүрлі криптографиялық түрлендірулерді қолдануға негізделген, мысалы, кілттерді қабаттастыру, S-box ауыстыру және деректерді араластыру процедуралары. Ол әртүрлі кілттер мен блок ұзындықтарын қолдайды, бұл нақты жүйенің талаптарына байланысты қауіпсіздік деңгейін реттеуге мүмкіндік береді. Сонымен қатар, QAMAL алгоритмі жоғары жұмыс жылдамдығына және төмен есептеу құнына ие, бұл оны әскери радио қолданбалары үшін тамаша таңдау.

Материалдар мен әдістер

«Qamal» шифрлау алгоритмі

Әзірленген шифрлау алгоритмінің құрылымдық схемасы 1-суретте көрсетілген. Алгоритм 128, 192 және 256 биттік блоктар мен кілттердің ұзындығын қолдайды. Шифрлау раундтарының саны блок пен кілттің ұзындығына байланысты. Ұзындығы 128, 192 және 256 биттік k кілттері 8, 10, 12 шифрлау раундтарының сандарына сәйкес келеді. Барлық раундтар 2-модульді дөңгелек кілтпен қосу операциясымен аяқталады [2].



Сурет 1 – Qamal шифрлау алгоритмінің құрылымдық схемасы

Шифрлау алгоритмі биттік қосу (XOR) операциясы, s-ауыстыру блогы, Mixer1 және Mixer2 араластыру процедуралары арқылы жасалған кілтті қабаттастыру процедураларын қамтиды:

– Бірінші процедура ашық мәтін блогына 2-Модуль (XOR операциясы) бойынша кілтті қабаттастыру (жинақтау) операциясын орындайды.

– Екінші процедура-ауыстыру кестесінің S1-блогы (S1-box). Сызықтық емес байт түрлендіруі орындалатын жерде: әр байтқа сызықтық емес биективті алмастыру қолданылады. Қолданылатын S-блок 1-кестеде көрсетілген.

1-кесте. S1-блок ауыстыру кестесі

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	C9	34	F0	18	55	86	21	6B	87	D2	6E	99	BD	31	98	89
1	29	73	83	8B	1A	19	E1	E4	F3	5B	72	3F	A6	F9	2E	A3
2	7E	10	94	07	EC	AD	2F	26	20	93	66	3D	DD	64	5F	C1
3	13	E0	80	25	D3	08	75	6A	B9	2D	D1	CC	FD	CA	3B	FC
4	D5	DA	E2	CE	A0	7F	AE	C8	9C	09	3C	95	BA	35	3E	7B
5	FA	8D	23	AB	D9	E8	74	2A	C3	A8	D8	52	45	B5	0A	0C
6	A4	61	9A	FB	AA	F6	78	84	C4	E9	EE	54	50	81	DF	90
7	36	B4	BB	44	C5	96	4B	28	14	E6	8F	FF	B0	1F	53	47
8	00	4C	40	2C	9B	9F	4A	01	7D	AF	92	56	7A	DB	8E	16
9	63	24	A9	1D	33	4D	E7	1C	70	69	B7	C6	32	E5	57	03
A	97	A5	EB	D4	BC	5D	F8	85	06	F2	59	F4	17	22	38	DC
B	0B	FE	BE	CD	41	82	04	0E	48	71	30	AC	EF	C7	2B	CB
C	B8	8C	5A	42	A7	4E	D0	46	BF	B3	91	E3	11	7C	6F	DE
D	88	58	1E	5C	9D	60	C0	62	05	79	ED	76	C2	02	65	D7
E	F1	8A	77	F7	37	B1	0F	67	CF	0D	A1	6C	4F	3A	39	1B
F	27	B6	5E	F5	EA	6D	15	9E	B2	12	A2	68	43	51	49	D6

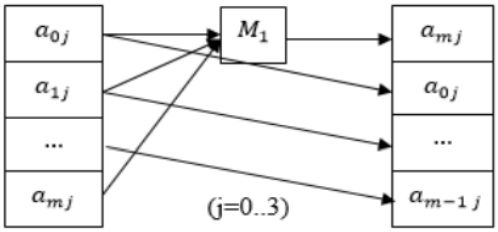
– Үшінші процедура-Mixer1 түрлендіру. Блоктың байттары $m = 4$ өлшеміндегі екі өлшемді A массиві ретінде ұсынылады, мұндағы m бастапқы блоктың өлшеміне байланысты 4, 6 және 8 мәнін алады.

$$A = \begin{bmatrix} a_{00} & a_{01} & a_{02} & a_{03} \\ a_{10} & a_{11} & a_{12} & a_{13} \\ \cdots & \cdots & \cdots & \cdots \\ a_{m0} & a_{m1} & a_{m2} & a_{m3} \end{bmatrix}$$

Әр бағанның байттары 256 модуліне сәйкес қосылады:

$$M_1(b_{ij}) = \sum_{i=0}^{m} a_{ij} mod 256, j = \overline{0,3},$$

содан кейін алынған бірінші бағанның жаңа байты жоғарғы a_{00} байт орнына қойылады, ал қалған байттар бір позицияға жылжиды. Бұл операция m рет қайталанады. Нәтижесінде бірінші бағандағы m байттарының жаңа жиынтығы пайда болады. Содан кейін бұл процесс қалған үш баған үшін орындалады (2-сурет).



Сурет 2 – Mixer 1 блогының құрылымдық схемасы

– Төртінші процедура: Mixer 2 түрлендіру. Mixer 1 блогын қалыптастыру нәтижесінде $m = 4$ өлшемді Жаңа B массиві алынады, мұндағы m блоктың өлшеміне байланысты 4, 6 немесе 8 мәндерін алады:

$$B = \begin{bmatrix} b_{00} & b_{01} & b_{02} & b_{03} \\ b_{10} & b_{11} & b_{12} & b_{13} \\ \cdots & \cdots & \cdots & \cdots \\ b_{m0} & b_{m1} & b_{m2} & b_{m3} \end{bmatrix}.$$

Массивтің әр жолы $GF(2^8)$ ақырлы өрісіне жататын коэффициенттері бар үшінші дәрежелі көпмүше түрінде ұсынылады [3]. Бұл көпмүшелер келесідей түрленеді:

$$b_i(x) = b_{i0}x^3 + b_{i1}x^2 + b_{i2}x + b_{i3}, i = 0, \dots, 3\,.$$

Әрбір $b_i(x)$ көпмүшесі $p(x)$модулі бойынша бекітілген (бұрын таңдалған) $m_i(x)$ көпмүшелеріне көбейтіледі:

$$\begin{gathered} m_0(x) = 168x^3 + 34x^2 + 187x + 186, \\ m_1(x) = 210x^3 + 53x^2 + 210x + 101, \\ m_2(x) = 218x^3 + 25x^2 + 250x + 210, \\ m_3(x) = 144x^3 + 75x^2 + 158x + 27, \\ m_4(x) = 163x^3 + 4x^2 + 111x + 106, \\ m_5(x) = 150x^3 + 237x^2 + 13x + 53, \\ m_6(x) = 99x^3 + 59x^2 + 104x + 205, \\ m_7(x) = 167x^3 + 49x^2 + 241x + 154, \\ p(x) = x^4 + x + 55. \end{gathered}$$

$m_i(x)$ көпмүшелері келесідей қолданылады. 128 биттік ашық блоктың ұзындығы $m_0(x)$, $m_1(x)$, $m_2(x)$, $m_3(x)$ алғашқы төрт көпмүшені пайдаланады. Блок ұзындығы 192 бит үшін алғашқы алты көпмүше $m_0(x)$, $m_1(x)$, $m_2(x)$, $m_3(x)$, $m_4(x)$, $m_5(x)$ блоктың үшінші мүмкін ұзындығы үшін барлық сегіз көпмүшелер қолданылады [4].

«Qamal» шифрын кері ашу алгоритмі

Шифр мәтінін кері ашу үшін шифрлау кезінде қолданылатын барлық криптографиялық түрлендірулер инверцияланып, кері ашу алгоритмінде кері тәртіпте қолданылады. Раундтық кілттер де кері тәртіпте қолданылады. Кері ашу кезінде көрсетілген блок ұзындықтарының әрқайсысы үшін сәйкесінше 6, 8 және 10 раунд орындалады, олардың әрқайсысында InvS, InvMixer1 және InvMixer2 инверсиялық операциялары орындалады [5].

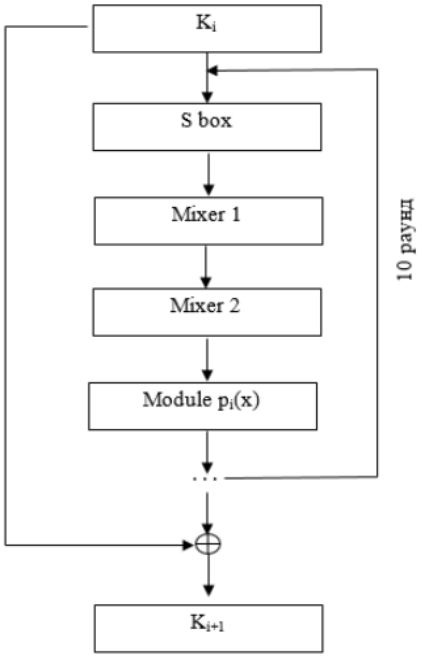
InvS операциясы S-box блогындағы элементтерді қалыптастыру үшін қолданылатын операцияға кері әсер етеді. S - box массивінің байттары кері ауыстыру арқылы алынған жаңа байттармен ауыстырылады, нәтижесінде инверттелген S-box пайда болады.

InvMixer операциясы M_1 (b_{ij}) түрлендіруіне кері операция InvMixer2 операциясы Mixer2 блогын алу процедурасына кері әрекет болып табылады. Mixer2-ге кері блокты алу үшін массивтің әрбір жолы $GF(2^8)$ өрісіндегі төртмүшелі көпмүше ретінде қарастырылады. Бұл көпмүшені $p(x)$ көпмүшесінің модулі бойынша бекітілген көпмүшеліктерге көбейтеді:

$$m_0^{-1}, m_1^{-1}, m_2^{-1}, m_3^{-1}\ m_4^{-1}, m_5^{-1}, m_6^{-1}, m_7^{-1}.$$

Раундтық кілттерді құру алгоритмі

K_i раундтық кілттерін генерациялау алгоритмі K_0 бастапқы шифрлық кілтіне негізделген кілтті кеңейту процедурасы арқылы жүзеге асырылады. Бұл процедура раундтық кілттердің массивін жасайды, олардың ішінен қажетті рауднтық кілт кейін таңдалады. Раундтық кілттерді алу схемасы 3-суретте көрсетілген.Раундтық кілттерді құру процедурасы ауыстыру кестесін өзгертуді және жаңа $Module\ p_i(x)$ түрлендіруін қоспағанда, шифрлау процесінде қолданылатын барлық түрлендірулерді қамтиды[5].



Сурет 3 – K_i кілтті кеңейту схемасы, мұндағы $i = 0,1, \ldots, 6(8,10)$

$Module\ p_i(x)$ көпмүшесі $P(x) = p_1(x), p_2(x), \dots, p_s(x)$ мұндағы – $p_1(x), p_2(x), \dots, p_s(x)$ жұмыс негіздері ретінде қолданылатын екілік коэффициенттері бар төмендетілмейтін көпмүшелер болып табылады. $N = m_1 + m_2 + \cdots + m_S$ деп белгіленген $P(x)$ көпмүшесінің дәрежесі блоктың ұзындығына сәйкес келеді (яғни 128, 192, 256). Mixer2 блогынан шығатын мәліметтер $N(x)$ көпмүшесі ретінде екілік коэффициенттермен ұсынылады $k_1(x), k_2(x), \dots, k_s(x)$, бұл $N(x)$ көпмүшесінің тиісті жұмыс негіздеріне бөлінуінен қалған қалдықтарды білдіреді. $p_i(x), i = 1, \dots, s$, мұндағы $p_i(x), i = 1, \dots, s$ кілтті кеңейту процедурасының құпия элементтері [6].

Осылайша, Qamal шифрлау алгоритміндегі дөңгелек кілттерді қалыптастыру алгоритмі K_0 шифрының бастапқы кілтінен K_i кілттер массивін кеңейту және құру процедурасы болып табылады. Бұл кілттер массиві процестің қауіпсіздігі мен сенімділігін қамтамасыз ету үшін шифрлаудың келесі кезеңдерінде қолданылады. Кілтті кеңейту процедурасы берілмейтін көпмүшелер мен ауыстыру кестелерін қолдануға негізделген түрлендірулерді қамтиды, бұл жіберілетін деректердің құпиялылығын тиімді қорғауды қамтамасыз етеді.

Нәтижелер.

AES және QAMAL алгоритмдері әскери радиобайланыс жүйелерін қорғау үшін қолданылатын тиімді блоктық симметриялық шифрлау әдістері болып табылады. Дегенмен, олардың арасында бірнеше негізгі айырмашылықтар бар:

– Шабуылдарға төзімділік: AES өнеркәсіпте кеңінен қолданылады және кең криптографиялық бағалауға ие, бұл оны әртүрлі шабуылдарға төзімді етеді. Екінші жағынан, QAMAL шифрлаудың кейбір инновациялық әдістерін ұсынса да, оның кең ауқымды жұмыс жағдайларында, соның ішінде әскери сценарийлерде сенімділігін дәлелдеу үшін оның криптографиялық күшін егжей-тегжейлі талдауды талап етеді.

– Өнімділік: AES жоғары шифрлау және шифрды шешу жылдамдығымен жиі танылады, бұл оны деректердің үлкен көлемін нақты уақытта өңдеуді қажет ететін жүйелерде пайдалану үшін тартымды етеді. QAMAL жоғары өнімділікті қамтамасыз ете алатынымен, оның осыған байланысты тиімділігі қосымша зерттеуді қажет етеді.

– Икемділік: AES арнайы жүйе талаптарына қауіпсіздік деңгейін реттеуге мүмкіндік беретін бірнеше кілт ұзындығы опцияларын (128, 192 және 256 бит) ұсынады. QAMAL сондай-ақ теңдеудің ұқсас деңгейіне мүмкіндік беретін кілт пен блок ұзындықтарында икемділікті ұсынады.

– Криптографиялық бағалау және қолдану: AES әртүрлі салаларда, соның ішінде әскери, қаржылық және коммерциялық салаларда кеңінен қолданылады және оның стандарты көптеген криптографиялық хаттамалар мен стандарттардың бөлігі болып табылады. QAMAL, керісінше, зерттеудің бастапқы сатысында және оны әртүрлі салаларда кеңінен қолдану үшін одан әрі криптографиялық бағалау мен қолдануды қажет етеді.

Тұтастай алғанда, AES ұзақ және табысты пайдалану тарихы бар және жақсы зерттелгенімен, QAMAL оның тиімділігі мен қауіпсіздігін, әсіресе әскери радиобайланыс контекстінде одан әрі зерттеуді және бағалауды қажет ететін ықтимал қызықты балама болып табылады.

Қорытынды

Бұл жұмыста «Qamal» блоктық симметриялық шифрлауды қолдана отырып, әскери радиобайланыс жүйесін қорғау әдісіне егжей-тегжейлі шолу және әзірлеу жасалды. Әзірленген алгоритм әскери коммуникациялық жүйелердегі ақпараттың құпиялылығы мен тұтастығын қамтамасыз етудің маңызды құралы болып табылады. Осы зерттеудің негізгі нәтижелері мен қорытындылары мыналарды қамтиды:

– Тиімділігі мен сенімділігі: «Qamal» блоктық симметриялы шифрлау қуатты криптографиялық түрлендірулер мен қосымша қауіпсіздік қабаттарын қолдану арқылы деректерді қорғаудың жоғары деңгейін ұсынады.

– Әр түрлі кілттер мен блоктардың ұзындығын қолдау: Алгоритм әр түрлі кілттер мен блоктардың ұзындығын қолдайды, бұл белгілі бір әскери байланыс жүйесінің талаптарына сәйкес қауіпсіздік деңгейін реттеуге мүмкіндік береді.

– Шабуылға төзімділік: әртүрлі кілттерді қолдану процедураларын, s-ауыстыру блоктарын және араластыру процедураларын қолдану әскери қақтығыстар кезінде жүйенің сенімділігін арттыратын криптоаналитикалық шабуылдардың әртүрлі түрлеріне төзімділікті қамтамасыз етеді.

– Практикалық маңыздылығы: әзірленген алгоритм кибершабуылдар мен тыңшылық қаупі жоғары жағдайларда да берілетін ақпаратты қорғауды қамтамасыз ете отырып, нақты әскери коммуникациялық жүйелерде қолдану үшін кең әлеуетке ие.

– Зерттеудің келесі бағыттары: болашақта «Qamal» алгоритмінің қауіпсіздігі мен өнімділігін әртүрлі пайдалану сценарийлерінде талдау, сондай-ақ жоғары тиімділік пен жұмыс жылдамдығын қамтамасыз ету үшін оны оңтайландыру бойынша қосымша зерттеулер жүргізу жоспарлануда.

Осылайша, ұсынылған «Qamal» блоктық симметриялық шифрлау алгоритмі әскери радиобайланыс жүйесін қорғаудың маңызды құралы болып табылады және нақты әскери жағдайларда сәтті қолдану мүмкіндігіне ие.

Блоктық симметриялық шифрлау әскери радиобайланыстың қауіпсіздігі мен құпиялылығын қамтамасыз ететін қуатты құрал болып табылады. Оның тиімділігі, жоғары жылдамдығы және іске асырудың қарапайымдылығы оны осы маңызды салада берілген ақпаратты қорғау үшін тамаша таңдау жасайды. Дегенмен, шифрлау параметрлерін дұрыс конфигурациялау және деректерді барынша қорғау үшін құпия кілттерді қауіпсіз басқаруды қамтамасыз ету маңызды.

ПАЙДАЛАНЫЛҒАН ӘДЕБИЕТТЕР ТІЗІМІ

1 D. Coppersmith, C. Holloway, S. Matyas and N. Zunic, “The Data Encryption Standard,” Information Security Technical Report, vol. 2, no 2, 1997, pp. 22-24.

2 Kunbolat T.A., Biyashev R.G. “Differential Cryptanalysis of New Qamal Encryption Algorithm” . International Journal of Electronics and Telecommunications November 2020, 66(4):647-653, DOI: 10.24425/ijet.2020.134023.

3 Kunbolat T.A., Biyashev R.G. “Encryption algorithm "QAMAL NPNS" based on a nonpositional polynomial notation”. International Journal of Electronics and Telecommunications, 2020, DOI: 10.26577/JMMCS.2020.v105.i1.17.

4 Kunbolat T.A., Biyashev R.G., Kapalova N. “Investigation of the different implementations for the new cipher Qamal” International Journal of Electronics and Telecommunication, 2019, DOI: 10.1145/3357613.3357622.

5 Kunbolat T.A., Biyashev R.G., Kapalova N. “Development and analysis of the new hashing algorithm based on block cipher”, Eastern-European Journal of Enterprise Technologies April 2022, 2(9 (116)) 182-186, DOI: 10.15587/1729-4061.2022.25206.

6 Kunbolat T.A., Biyashev R.G. “Development and Study of an Encryption Algorithm” November 2022, Computation 10(11):198, DOI: 10.3390/computation10110198.

7 B. Shnier, “Chapter 12 – Data Encryption Standard (DES),” in Applied Cryptography: Protocols, Algorithms, and Source Code in C, Hoboken, NJ, USA: John Wiley & Sons, 1996, pp. 370-421.

ӘОЖ 004.9

РАДИОБАЙЛАНЫСТЫ ҚОРҒАУ ҮШІН ГОМОМОРФТЫ ШИФРЛАУДЫ ҚОЛДАНУ

ТЕМИРБЕКОВА Ж.Е., *PhD докторы*
КЕНЕСОВ Ә.Ж., *қызметкер*

ҚР ҰҚК академиясы, Қазақстан Республикасы, Алматы қаласы

Аңдатпа. Радиобайланыс жүйесі қазіргі байланыс әлемінде маңызды рөл атқарады. Криптографияның қарқынды дамуы деректердің құпиялылығын қамтамасыз етудің жаңа әдістеріне әкеледі және осындай әдістердің бірі гомоморфты шифрлау. Мақалада радиобайланыс жүйесін қорғау үшін гомоморфты шифрлау процесін қолдану қарастырылды. Радиобайланыс жүйесінде жіберілген хабарламалардың құпиялылығын қамтамасыз ету және деректерді рұқсатсыз кіруден қорғау өте маңызды. Гомоморфты шифрлауды радиобайланыста қолдану деректерді қорғауды күшейтіп қана қоймайды, сонымен қатар криптография мен ақпараттық қауіпсіздікте жаңа тәсілдерді құруға ықпал етеді. Неғұрлым тиімді және қол жетімді шешімдердің пайда болуымен гомоморфты шифрлау жаңа деңгейде өңделетін деректердің құпиялылығы мен тұтастығына кепілдік береді, болашақта қорғалған радиобайланыс жүйелерін жүзеге асырудың кілті бола алады.

Түйін сөздер: гомоморфты шифрлау, радиобайланыс, радиобайланыс жүйесі, Пэйе криптожүйесі.

Кіріспе.

Гомоморфты шифрлау – арифметикалық және логикалық операцияларды шифрланған деректерге алдын-ала шифрлауды қажет етпестен тікелей жүргізуге мүмкіндік беретін шифрлау технологиясы және де деректерді құпиялылықты сақтай отырып өңдеуге мүмкіндік береді. Бұлтты есептеу, медициналық зерттеулер, қаржылық қызметтер және жеке деректерді өңдеу және радиобайланысты қорғау сияқты ақпаратты қорғаудың жоғары дәрежесін қажет ететін салалар үшін революциялық үлгі болып табылады.Тарихи тұрғыдан алғанда, гомоморфты шифрлау тұжырымдамасы алғаш рет 1978 жылы ұсынылды, бірақ ұзақ уақыт бойы ол айтарлықтай есептеу шектеулеріне байланысты теориялық болып қала берді. Саладағы алғашқы жетістік 2009 жылы Крейг Гентри криптографияда осы бағыттың белсенді дамуына түрткі болған тамаша идеяларына негізделген толық гомоморфты шифрлау схемасын енгізген кезде болды [1]. Гомоморфты шифрлау 2 негізгі түрге бөлінеді: жартылай гомоморфты және толық гомоморфты. Жартылай гомоморфты шифрлау шифрланған деректерге операциялардың тек бір түрін (қосу немесе көбейту) орындауды қолдайды. Толық гомоморфты шифрлау, ең қуатты форма, шифрды шешуді қажет етпестен шифрланған деректердегі кез-келген операциялардың шексіз санын қолдайды және құпия деректерді өңдеуді қажет

ететін әртүрлі салаларда қолданылады. Мысалы, медициналық деректерді ашпай-ақ талдау үшін пайдаланылуы мүмкін. Қаржы секторында деректерді бұзу қаупінсіз қауіпсіз транзакциялар жүргізуге және қаржылық ақпаратты талдауға көмектесе алады.Бұлтты есептеулерде, радиобайланыс бастапқы ақпаратты ашпай-ақ үшінші тарап серверлеріндегі деректерді өңдеу үшін белсенді қолданылады.Гомоморфты шифрлаудың артықшылықтары айқын ол пайдаланушылар мен ұйымдарға шифрланған деректердегі есептеу операцияларын деректердің өзін ашу қаупінсіз үшінші тараптарға беруге мүмкіндік беретін қауіпсіздік пен құпиялылықтың жоғары деңгейін қамтамасыз етеді. Электрондық дауыс беру, қауіпсіз қаржылық жазбалар және деректерді құпия талдау сияқты салаларда маңызды ақпаратты қауіпсіз өңдеуге жаңа мүмкіндіктер ашады. Гомоморфты шифрлау техникалық және практикалық қиындықтарға тап болады, соның ішінде жоғары есептеу шығындары және бар жүйелерге интеграциялану қиындықтары болды. Осы кедергілерге қарамастан, саладағы үздіксіз зерттеулер мен әзірлемелер гомоморфты шифрлаудың тиімділігі мен ыңғайлылығын жақсартуға бағытталған, оны болашақ цифрлық қауіпсіздікті қамтамасыз етудің перспективалы құралы етеді. Гомоморфты шифрлауды қолданудың артықшылықтары қарастырылды, мысалы, шифрланған деректерде қауіпсіз есептеу және радиоарнаны тарату кезінде ақпаратты қорғау және деректерді қорғауды, хабарламалардың құпиялылығын талап ететін әртүрлі сценарийлерде радиобайланыс қауіпсіздігін қамтамасыз етудің перспективалық әдісін ұсынылды.

Радиобайланыста гомоморфты шифрлауды қолдану

Радиобайланыс саласында деректердің құпиялылығы өте маңызды. Жіберілген деректерді рұқсатсыз кіруден және тыңдаудан қорғауды қамтамасыз ету маңызды. Гомоморфты шифрлау радиобайланыс процесінде деректерді қорғаудың бірегей мүмкіндігін ұсынады. Радиобайланыста гомоморфты шифрлауды қолдану қазіргі байланыс желілерінде берілетін деректердің қауіпсіздігі мен құпиялылығын қамтамасыз етудегі маңызды қадам болып табылады. Гомоморфты шифрлау шифрланған деректердің шифрын ашпай-ақ кең ауқымды операцияларды орындауға мүмкіндік береді, радиобайланыстағы ақпаратты қорғаудың жаңа перспективаларын ашады [2].

Біріншіден, радиоарна арқылы ақпарат беру кезінде деректердің құпиялылығын қорғау негізгі міндет болып табылады. Гомоморфты шифрлау құпиялылықтың жоғары деңгейін қамтамасыз етеді, өйткені шифрланған деректерді ұстап алған жағдайда да, шабуылдаушы олардың мазмұнына тиісті кілтсіз қол жеткізе алмайды.

Екіншіден, гомоморфты шифрлау шифрланған деректерде қауіпсіз есептеулерді қамтамасыз етеді. Әсіресе қашықтағы құрылғыларда одан әрі өңдеу үшін деректерді тасымалдау жағдайында пайдалы. Гомоморфты шифрлауды қолданған кезде есептеулер құпия ақпараттың ағып кету қаупін азайта отырып, шифрланған деректерде жүргізілуі мүмкін.

Сонымен қатар, гомоморфты шифрлау оларды радиоарна арқылы беру кезінде деректерге шабуылдан қорғауды қамтамасыз етеді. Шифрланған

деректер шабуылдаушылар үшін түсініксіз болып қалады, тіпті егер олар ұсталса да, байланыс желісінің жалпы қауіпсіздігін арттырады. Ақырында, таратылған байланыс желілерінде гомоморфты шифрлау әртүрлі құрылғылар немесе желі түйіндері арасындағы деректерді қауіпсіз өңдеуді қамтамасыз етеді, берілетін ақпараттың жалпы қауіпсіздігі мен құпиялылығын жақсартады. Гомоморфты шифрлаудың берілетін деректердің құпиялылығы мен қауіпсіздігін қамтамасыз ету сияқты бірқатар артықшылықтары болғанымен, оның есептеу талаптары мен мүмкін болатын өнімділік шектеулерін, әсіресе радио контекстінде ескеру қажет. Технологияның дамуы берілетін ақпаратты сенімді қорғауды қамтамасыз ете отырып, қауіпсіз және тиімді байланыс жүйелерін құруға ықпал етуі мүмкін.

Қолданатын әдіс.

Пэйе криптожүйесімен гомоморфты шифрлау радиобайланыста қауіпсіздік пен құпиялылықты қамтамасыз етудің маңызды құралы болып табылады. Оның заманауи технологиялар мен ақпараттық қауіпсіздік контекстіндегі маңыздылығын түсіну оның беретін артықшылықтары мен мүмкіндіктерін түсінуге көмектеседі.Деректерді беру ашық байланыс арналары арқылы жүзеге асырылатын радиобайланыс саласында құпиялылықты қорғау басым міндетке айналады [3]. Гомоморфты шифрлау, әсіресе Пэйе криптожүйесін қолдана отырып, деректерді үшінші тұлғалардың тыңдауы мен талдауы үшін қол жетімді болмайтындай етіп шифрлау құралын ұсынады. Пэйе криптожүйесі гомоморфты қосу қасиетіне ие, шифрланған деректердің шифрын ашпай-ақ операцияларды орындауға мүмкіндік береді. Хабарламаны алушы бастапқы ақпараттың мазмұнын ашпай-ақ деректерді жинақтау, орташалау немесе біріктіру сияқты әртүрлі операцияларды орындай алатынын білдіреді. Пэйе криптожүйесімен гомоморфты шифрлауды қолданудың артықшылықтарының бірі деректерді ұстауға байланысты шабуылдардан қорғау. Шифрланған деректер байланыс арнасы бұзылған жағдайда да қорғалған болып қалады, өйткені оларды шифрлау үшін кері шифрлау кілтіне кіру қажет. Пэйе криптожүйесімен гомоморфты шифрлау қашықтағы серверлерде немесе бұлтты орталарда олардың мазмұнын ашпай-ақ деректерді өңдеу мүмкіндігін береді. Оны үшінші тарап платформаларында немесе құрылғыларында құпия ақпаратты өңдеуді қажет ететін сценарийлер үшін тамаша шешім етеді.Сондай-ақ, Пэйе криптожүйесімен гомоморфты шифрлауды қолдану ұйымдарға деректерді қорғау заңнамасының талаптарын сақтауға және пайдаланушылардың жеке ақпаратының қауіпсіздігін қамтамасыз етуге көмектесетінін атап өткен жөн. Этикалық тұрғыдан да, белгіленген стандарттар мен ережелер тұрғысынан да маңызды.

Осылайша, Пэйе криптожүйесімен гомоморфты шифрлау ашық байланыс арналарында деректерді қорғау мен ақпаратты өңдеудің тиімді құралдарын ұсына отырып, радиобайланыста қауіпсіздік пен құпиялылықты қамтамасыз етуде шешуші рөл атқарады.

Мысалы:

Бізде екі әскери штабтың орналасқан жері туралы келесі мәліметтер бар:

– А штабының координаттары $(X_a, Y_a) = (10, 15)$
– Б штабының координаттары $(X_b, Y_b) = (20, 30)$
Параметрлерді Пэйе криптожүйесімен шифрлау қолданылды:
– Ашық кілт: $(n, g) = (91, 16)$
– Құпия кілт: ($\lambda = 60$)
Шифрлау қадамдары:
1. А штабының орналасқан жерін шифрлау:

$$C_1 = 16^{10} * {r_1}^{91} \, mod \, 91^2$$

2. Б штабының орналасқан жерін шифрлау:

$$C_2 = 16^{20} * {r_2}^{91} \, mod \, 91^2$$

Шифрлаудан кейін келесі шифрланған деректер алдынды:

$$C_1 = 28677$$
$$C_2 = 83326$$

Осы шифрланған деректерді алады және құпия кілтін пайдаланып кері ширлау қолданады.
Кері шифрлауға арналған формула:

$$locA' = L({c_1}^{\lambda} \, mod \, 91^2) * \mu \, mod \, 91$$
$$locA' = L({c_2}^{\lambda} \, mod \, 91^2) * \mu \, mod \, 91$$

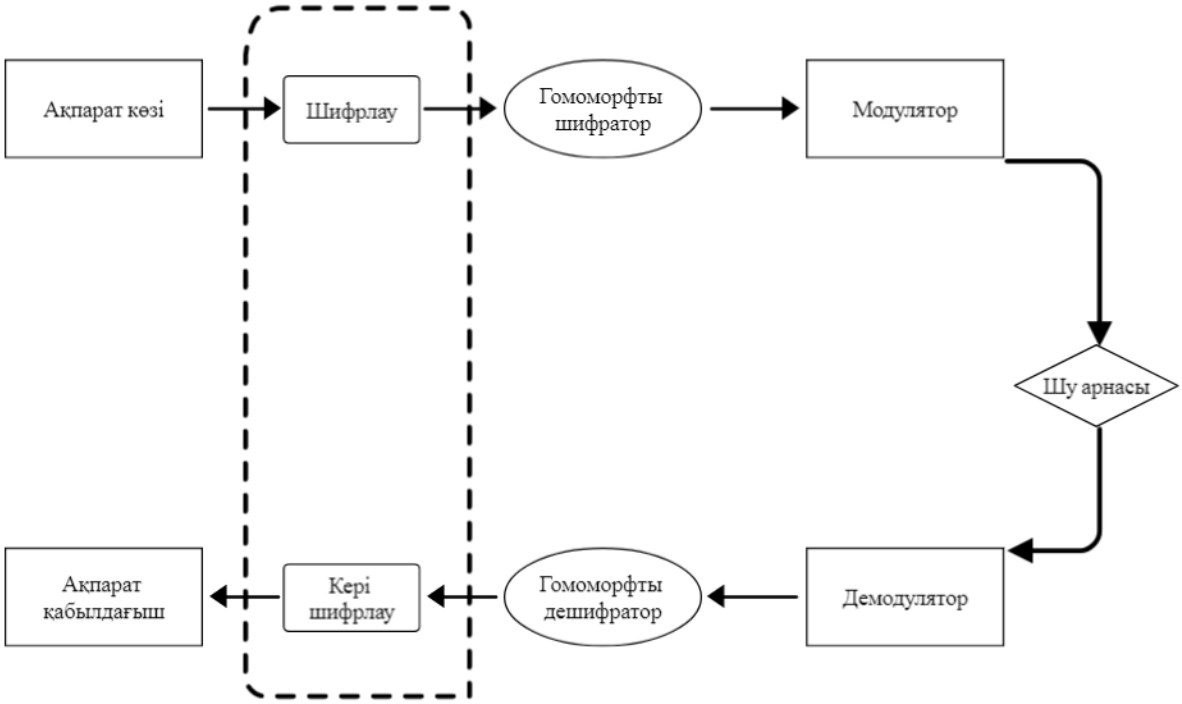
Құпия деректерді кері шифрлағаннан кейін келесі мәндер алынады:

$$locA' = 10$$
$$locB' = 20$$

Екі штабтың жиынтық орнын табу үшін Б штабы алынған координаттарды жай ғана қосылады:

$$Total\_location = locA' + locB' = 10 + 20 = 30$$

Осылайша, штаб Б шифрланған деректерді шифрлап, қосқаннан кейін екі штабтың жалпы орны $(x, y) = (30, 35)$ екенін біле алады.
Радиобайланыс жүйесіне гомоморфты шифрлауды енгізу берілетін ақпараттың қауіпсіздігі мен құпиялылығының жоғары деңгейін қамтамасыз етеді. Мұндай жүйенің құрылымдық сызбасы 1-суретте көрсетілген. Әртүрлі тарату кезеңдерінде деректерді шифрлау және өңдеу үшін қосымша компоненттерді қамтиды.



1 сурет – Сандық радиобайланыс жүйесінің құрылымдық схемасы

Құрылымдық сызбасы:

1. Ақпарат көзі: ақпарат жіберу үшін бастапқы деректерді жасайды.
2. Гомоморфты шифратор: сандық деректерге гомоморфты шифрлауды қолданады, оларды шифрсыз өңдеуге болатын шифрланған түрге айналдырады.
3. Модулятор: шифрланған деректерді радиоарна арқылы беру үшін түрлендіреді, оны таратушы ортаның сипаттамаларына бейімдейді.
4. Демодулятор: қабылданған сигналды қайтадан сандық түрге түрлендіреді.
5. Гомоморфты дешифратор: қосымшаға байланысты деректерді шифрланған түрде қосымша өңдеуге болады. Егер бастапқы деректермен жұмыс қажет болса, транскрипция жасалады.
6. Ақпарат қабылдағыш: берілген ақпаратты пайдаланатын соңғы пайдаланушы немесе құрылғы.

Ерекшеліктері:

– Гомоморфты шифрлау шифрланған деректердің үстінен есептеулер жүргізуге мүмкіндік береді, оның нәтижесі шифрды шешкеннен кейін бастапқы деректердің үстіндегі операциялармен бірдей болады.

– Мүмкіндікті бұлтты есептеулерде, сенімсіз байланыс арналары арқылы берілгенде немесе деректерді өңдеу деректерге қол жеткізбестен жүргізілуі керек жағдайларда деректердің қауіпсіздігін қамтамасыз ету үшін пайдалануға болады.

– Пайдалану сценарийіне байланысты, гомоморфты дешифраторды қабылдағыштың жағына оларды декодтауға дейін нақты өңдеу тапсырмаларын

орындау үшін орналастыруға болады немесе егер деректерді өңдеу шифрланған түрде жүргізілсе, оның болуы талап етілмеуі мүмкін.

Мұндай радиобайланыс жүйесі берілетін ақпараттың құпиялылығы маңызды салаларда, мысалы, әскери қосымшаларда, деректерді қорғау және жеке байланыс жүйелерінде қолданылады[4].

Нәтиже.

Ақпараттық қауіпсіздік барған сайын өзекті мәселеге айналатын әлемде, әсіресе маңызды салаларда радиобайланысты қорғау шешуші рөл атқарады. Гомоморфты шифрлау, Пэйе криптожүйесімен бірге, берілетін деректердің қауіпсіздігі мен құпиялылығын қамтамасыз етудің қуатты құралы болып табылады[5].Пэйе криптожүйесі радиобайланыста деректердің құпиялылығы мен тұтастығын қамтамасыз ету әдісі болып табылады. Хаттама ақпаратты рұқсатсыз кіруден және араласудан қорғау үшін қолданылады. Гомоморфты шифрлаумен бірге Пэйе криптожүйесі радиобайланысты қорғаудың қуатты механизмін жасайды. Пэйе криптожүйесі арқылы радиобайланыста гомоморфты шифрлауды қолданудың бірқатар артықшылықтары бар:

Деректердің құпиялылығы мен тұтастығы: шифрланған деректерді радиоарна арқылы оларды ашу қаупінсіз беруге болады. Деректерді ұстап алған жағдайда да, шабуылдаушы бастапқы ақпаратқа оның шифрлануына байланысты қол жеткізе алмайды.Пэйе криптожүйесі деректердің тұтастығын тексеруді қамтамасыз етеді, яғни алушы алынған ақпараттың тасымалдау процесінде араласпағанына немесе өзгермегеніне сенімді бола алады.

Шабуылға төзімділік және тиімділігі: гомоморфты шифрлау криптоаналитикалық шабуылдардың әртүрлі түрлеріне төзімді, мысалы, шамадан тыс шабуылдар және уақыт шабуылдары. Киберқауіпсіздік қаупінің жоғарылауы жағдайында радиобайланысты қорғау әдісін сенімдірек етеді. Гомоморфты шифрлау шифрланған деректердің шифрын ашпай-ақ операцияларды орындауға мүмкіндік беретіндіктен, берілетін ақпарат көлемін айтарлықтай азайтуға болады. Желідегі жүктемені азайтады және деректерді беру тиімділігін арттырады.

Пэйе криптожүйесі гомоморфты шифрлауды радиобайланыста қолдану арнайы техникалық шешімдер мен ойластырылған инфрақұрылымды қажет етеді. Дегенмен, оның деректердің қауіпсіздігі мен құпиялылығындағы артықшылықтары оны әскери коммуникациялар, медициналық бақылау және басқару жүйелері, сондай-ақ корпоративтік желілер сияқты көптеген қолданбалар үшін өте маңызды етеді.Деректер барған сайын құнды ресурсқа айналған қазіргі әлемде олардың радиоарналар арқылы берілуін қорғау маңызды міндетке айналуда. Пэйе криптожүйесі гомоморфты шифрлауды қолдану радиобайланыс қауіпсіздігін қамтамасыз етудегі ең перспективалы шешімдердің бірі болып табылады.

Қорытынды.

Радиобайланыс саласына гомоморфты шифрлауды енгізу киберқауіптердің өсуі және деректер алмасудың үнемі өсіп келе жатқан көлемі жағдайында берілетін ақпараттың қауіпсіздігін қамтамасыз ету жолындағы перспективалық

қадам болып табылады. Тәсілдің ерекшелігі-ақпаратты қорғаудың жаңа деңгейін қамтамасыз ететін шифрланған деректердің үстінен оларды алдын-ала декодтаусыз есептеулер жүргізу мүмкіндігі. Қолданыстағы радиобайланыс жүйелерінде олардың үйлесімділігі мен қауіпсіз өзара әрекеттесуін қамтамасыз ету үшін гомоморфты шифрлау әдістерін стандарттау қажеттілігі маңызды аспект болып табылады. Қиындықтарды жеңу криптография мамандарының, аппараттық өндірушілердің, бағдарламалық жасақтама жасаушылардың және реттеуші органдардың келісілген күш-жігерін қажет етеді. Гомоморфты шифрлау процестерін оңтайландыруға бағытталған қарқынды зерттеулер мен әзірлемелер есептеу шығындарын едәуір төмендетіп, осы технологияны қолданыстағы жүйелерге біріктіруді жеңілдетеді.Көбінесе тек әскери және арнайы қызметтерге арналады. Гомоморфты шифрлау қашықтағы құрылғылардағы немесе бұлттық ортадағы деректерді олардың мазмұнын ашпай өңдеуге мүмкіндік береді,әсіресе жоғары құпиялылықты қажет ететін қолданбалар үшін маңызды.Радиобайланыста гомоморфты шифрлауды қолдану берілетін ақпараттың қауіпсіздігі мен құпиялылығын қамтамасыз етудегі маңызды қадам болып табылады.Оны қолдану берілетін ақпаратты радиоарна арқылы беру процесінде рұқсатсыз қол жеткізуден және шабуылдардан қорғау үшін жаңа перспективалар ашады. Дұрыс іске асырылған және интеграцияланған кезде ол ақпаратты қорғаудың және болашақта радиобайланыста қауіпсіздікті қамтамасыз етудің тиімді құралы бола алады.

ПАЙДАЛАНЫЛҒАН ӘДЕБИЕТТЕР ТІЗІМІ

1 Smith, J., & Johnson, R. (2020). «Advancements in Homomorphic Encryption: Implications for Modern Security». Journal of Cybersecurity and Digital Forensics, 8(2), 45-59.

2 Green, M., & Baker, T. (2022). «A Comparative Analysis of Homomorphic Encryption Schemes for Wireless Networks». Wireless Networks, 28(2), 619-632.

3 Zhang, Y., & Lee, W. (2022). «Secure and Efficient Homomorphic Encryption Protocols for Cloud-Based Radio Access Networks». IEEE Access, 10, 58472-58485.

4 Брусенцов, А.П., Ватолин, Р.А., Иванов, И.Е. (2022) «Применение гомоморфного шифрования для защиты информации в системах радиосвязи», Журнал «Радиотехника», № 4, стр. 56-63.

5 Иванов С.А., Петров В.Б. «Анализ методов гомоморфного шифрования в системах защиты информации на базе радиосвязи», Журнал «Проблемы защиты информации», 2023, № 2, стр. 45-53.

УДК 004.9

ИССЛЕДОВАНИЕ АЛГОРИТМА AES ДЛЯ ЗАЩИТЫ СИСТЕМЫ ВОЕННОЙ РАДИОСВЯЗИ

ТЕМИРБЕКОВА Ж.Е., *доктор PhD*
МЫРЗАҒАЛИ И.Н., *сотрудник*

Академия КНБ Республики Казахстан, город Алматы

Аннотация. В современном мире защита конфиденциальности данных военной радиосвязи становится все более актуальной задачей. Информация является наиболее важной в компьютеризированном мире. Поскольку это форма обработки данных, обеспечение ее безопасности является обязательным. Система обороны страны является главной заботой нации. Защита конфиденциальных военных данных от несанкционированного доступа, раскрытия или модификации – это то, что должно быть обеспечено соответствующими сторонами. Лучший вариант, который можно предложить, - это стандарты шифрования и расшифрования AES. В рамках нашей работы мы сосредоточились на методах шифрования спутниковых изображений, которые используются в военной связи, прототипе системы для безопасного обмена сообщениями в режиме реального времени и механизмах шифрования изображений. Поток будет содержать подробные факты, касающиеся основных аспектов, упомянутых выше, вместе с заключением, чтобы подкрепить наше объяснение.

Ключевые слова: AES, защищенный обмен сообщениями, шифрование, режимы AES, расширение ключа AES, шифрование изображений.

Введение.

Вооруженные силы часто в значительной степени полагаются на безопасную передачу сообщений, подобно другим организациям, которые заботятся о безопасности обмена данными. Для вооруженных сил безопасность данных является серьезной проблемой, и сотрудники сил безопасности активно следуют передовым практикам, чтобы гарантировать защиту данных и их целостность. Для обеспечения защиты совместно используемых данных через сеть используется несколько методов, среди которых шифрование, аутентификация, цифровая подпись. Защита методов передачи данных - это методология защиты информации от несанкционированных разрушителей при доступе к системам связи понятным образом при отправке сообщений получателям. Криптографические методы помогают обеспечить конфиденциальность данных. Вооруженные силы и правительственные учреждения используют криптографические технологии для защиты своих секретных данных. Во время боя это также полезно на поле боя, поскольку не

позволяет информации стать достоянием противников. В механизмах хранения и передачи данных для защиты данных используется шифрование.

Такие алгоритмы, как DES, 3DES, Blowfish, RSA могут использоваться для шифрования и защиты конфиденциальных данных. Алгоритм Advanced Encryption Standards (AES) используется в военных целях из-за его безопасности и скорости. В военных действиях безопасность видеозвонков и изображений действительно важна. AES может использоваться для шифрования сохраненных изображений и изображений, которые передаются. Благодаря универсальности, простоте исполнения, простота AES может быть принята в качестве общего стандарта шифрования. Причина использования методов AES заключается в том, что AES трудно взломать по сравнению с DES [1]. В этой статье упоминалось о расширении ключа для шифрования изображений и изменениях для обеспечения качественного процесса.

Материалы и методы

Исследование распространения сбоев в Шифровании спутниковых изображений с использованием AES

Наблюдение Земли (НЗ), другими словами, спутниковые изображения играет большую роль в качестве бесценного ресурса для задач обороны и безопасности. Когда военные хотят развертывать миссии и планировать операции удаленно, ценность этих изображений огромна. Терминалы – это распространенное оборудование, которое позволяет получать изображения с высокой скоростью и высоким разрешением на военно-тактическом уровне. При определении уровня производительности этих спутников большую роль играют точность, надежность и полезность изображений в режиме реального времени. Спутники НЗ получают изображения с помощью камер высокого разрешения. При передаче данных, полученных с этих спутников, на наземную станцию стратегии защиты были оснащены встроенным шифрованием. К сожалению, современный мир использует устаревшие алгоритмы, такие как стандарт шифрования данных (DES) [2].

То AES считается стандартом шифрования с наиболее широким спектром применения из-за гибкости, легкости внедрения, простоты и желаемого результата. Данные, полученные с помощью спутников, могут быть ошибочными по двум основным причинам. Первый тип в основном фокусируется на ошибках, возникающих во время шифрования, а второй тип содержит ошибки, возникающие во время передачи.

Эти спутники всегда многократно запускают операции в нестабильных средах, поэтому в большинстве случаев электронное оборудование, вызванное процессами шифрования, может быть повреждено из-за этих условий окружающей среды. Обычно эти ошибки называются сбоями в работе с одним битом, называемыми сбоями в работе с одним событием (SEU). Более того, шум в канале передачи также является источником этих сбоев являются перебросы отдельных битов SEU. Более того, шум в канале передачи также является источником этих сбоев [3].

Режимы работы использовались для шифрования данных более чем из одного блока в блочном шифре AES. Если говорить о методологиях, AES содержит пять основных режимов: изменение блока шифрования (CBC), обратная связь на выходе режим (OFB), режим обратной связи с шифром (CFB), электронная книга кодов (ECB) и режим счетчика (CTR). Эти режимы могут быть классифицированы как режимы обратной связи и без обратной связи. В разделе обратная связь у нас есть: CBC, CFB, OFB, тогда как в разделе без обратной связи у нас есть ECB и CTR. Кроме того, ECB и CBC рассматриваются как блочные шифры, в то время как OFB, CFB и CTR называются потоковыми шифрами. Специально созданный программное обеспечение, написанное с использованием языка программирования Java для реализации шифрования и расшифрования спутниковых мультиспектральных изображений. Разработка AES состоит из двух частей. Одна – это основные модули, а другая - модули обратной связи. SubBytes, ShiftRows, соответствующие обратные модули и MixColumns для расшифрования включены в основные модули. С другой стороны, модули обратной связи состоят из процедур шифрования и расшифрования в режимах ECB, CBC, CFB, OFB и CTR. Начнем с того, что ECB является базовым режимом, на основе которого были созданы все остальные режимы. Но при анализе основная проблема, связанная с этим режимом, заключается в том, что одни и те же результаты ввода простых данных публикуются в одном и том же выводе зашифрованных данных на этапе шифрования. В результате перехватчик может выявить закономерности. По этой причине этот режим считался небезопасным во многих приложениях. Для предотвращения шаблонов зашифрованных данных используются режимы обратной связи. При использовании режимов обратной связи режим CBC скрывает цифры данных в зашифрованном тексте, который был идентифицирован как более безопасный, чем ECB. Наиболее важным фактором, касающимся режима CTR, является то, что они не содержат какую-либо обратную связь или цепочку. Таким образом, AES был улучшен для параллельного выполнения нескольких шифров. Что привело к созданию высокопроизводительных приложений [4].

Прототип криптоалгоритма AES и его усовершенствования. Схема управления ключами

Представлено исследование, целью которого является создание прототипа системы для безопасного обмена сообщениями в режиме реального времени для военных организаций между пользователями рабочих станций, подключенных к одной и той же сети TCP/IP. Передача данных, основанная на симметричных алгоритмах шифрования для обеспечения безопасности, а именно AES, экономит время. Точнее, пользователю приложения предоставляется персональный ключ для раскрытия общего сетевого приложения сертифицированным пользователям того же приложения.

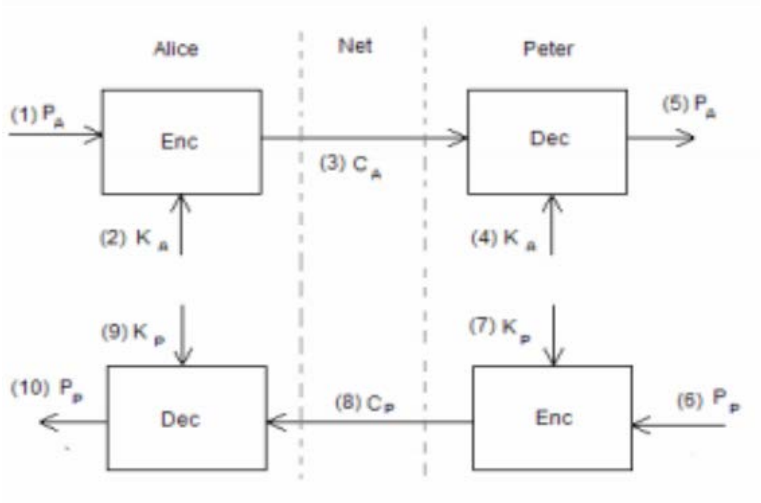


Рисунок 1 – Схема работы дуплексной связи в системе

Также стандартной практикой является использование одной и той же службы системы доменных имен с разрешением имени хоста и IP-адреса (DHCP) (DNS) в качестве одного и того же разрешения имени хоста и IP-адреса для всех приложений. И один и тот же интерфейс (ODBC, JDBC) для доступа к конкретным системами управления реляционными базами данных (RDBMS). Симметричное основное управление, поэтому емкость также необходимо абстрагировать. Приложения должна быть доступна только услуга управления ключами. Это стандартизированная отдельная инфраструктура. Шифрование и расшифрование также возможны для обеспечения единообразного решения Качество защиты и соответствующий объем. Инновационная платформа для автоматизированного контроля скрытых ключей шифрования для систем безопасности и жизненного цикла хранимых данных.

Эти функции выражены в безопасной работе с сообщениями, система обмена которыми также перечислена ниже:

– регистрация пользователя;
– инициализация пользователя;
– генератор ключей;
– установка ключа;
– регистрация ключа;
– обновление ключа;
– резервное копирование ключа.

Шифрование изображений на основе расширения ключа AES Цифровое изображение состоит из элементов, называемых пикселями, которые организованы в упорядоченный двумерный прямоугольный массив. Каждый из этих пикселей имеет свое значение интенсивности и адрес местоположения [2].

Безопасность конфиденциальных видеоконференций и баз данных изображений очень важны в военных операциях. Все это требовало эффективного и быстрого метода шифрования изображений, которые сохраняются, а также передаются. Этот алгоритм шифрует набор пикселей изображения на основе расширения ключа AES с использованием ключа

длиной 128 бит. Для каждого набора пикселей ключ будет меняться. Вместо совместного использования всех ключей между двумя сторонами, исходный ключ будет общим для того, чтобы генерировать ключи у обеих сторон независимо, используя процесс расширения ключа AES.

Результат

Механизм расширения ключа AES

Процесс расширения ключа генерирует слово за словом круглые ключи, где кластер из 4 байт, известный как слово, и процесс генерирует $4x\ (Nr + 1)$ слова. Где Nr рассматривается как количество раундов.

```
KeyExpansion (byte key[16], word w[44])
{
    word temp
    for (i = 0; i < 4; i++)    w[i] = (key[4*i], key[4*i+1],
                                       key[4*i+2],
                                       key[4*i+3]);
    for (i = 4; i < 44; i++)
    {
     temp = w[i - 1];
     if (i mod 4 = 0)    temp = SubWord (RotWord (temp))
                                ⊕ Rcon[i/4];
     w[i] = w[i-4] ⊕ temp
    }
}
```

Рисунок 2 – Генерация расширенного ключа

На рисунке 2 значение S-образного поля для слова Rcon - круглая константа. Rot Word – поворот слова (круговой сдвиг влево на 8 бит).

Модификации расширения ключа AES

Для повышения качества шифрования в процесс расширения ключа были внесены следующие изменения:

– расширение исходного ключа выполняется с учетом количества пикселей в выбранном изображении, а не 10 раундов;

– значение rcon создается из исходного ключа вместо постоянного значения –улучшает эффект лавина образности;

– в процессе расширения ключа используются как s-box, так и обратный s-box–улучшает качество шифрования;

–некоторый круговой сдвиг выполняется в s-образном блоке и обратном s-образном блоке на основе начальной клавиши – улучшает чувствительность ключевых.

Процесс: выбор ключа: Отправляющая и принимающая стороны должны согласовать ключ длиной 128 бит, который представлен в виде блоков, где каждый блок состоит из 8 бит. Этот ключ является симметричным ключом, и он будет использоваться для шифрования и расшифрования. Следовательно, им необходимо безопасно делиться.

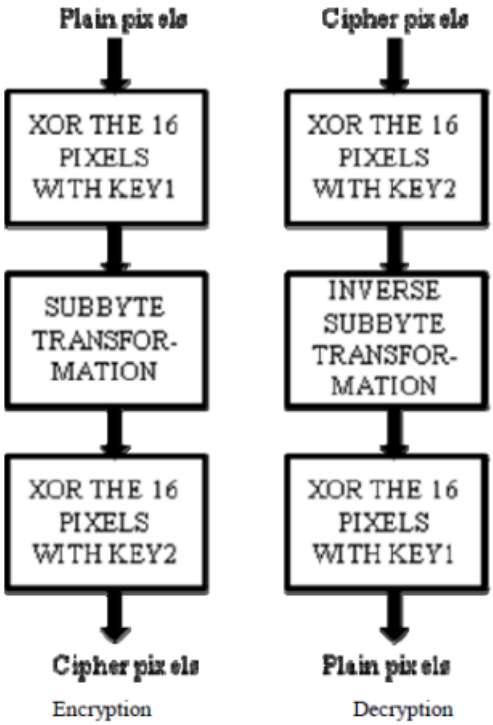


Рисунок 3 – Процесс шифрования и расшифрования

Генерация ключей: как отправляющая, так и принимающая стороны могут независимо генерировать ключи, используя описанный выше модифицированный метод расширения ключа AES. Этот процесс выполняется только один раз, пока обе стороны не решат изменить исходный ключ [7].

Шифрование выполняется в 16 пикселях, содержащих span. Каждый набор пикселей проходит две операции XOR с использованием расширенных ключей и преобразования SubBytes. Это гарантирует, что извлечение ключа из зашифрованного изображения и обычного изображения невозможно.

Для расшифровки используется обратное преобразование SubBytes. Кроме того, порядок операций XOR меняется на противоположный.

Заключение

В данной статье описываются три метода, такие как шифрование спутниковых изображений с использованием режимов ECB, CBC, CFB, OFB и CTR алгоритма AES, прототип системы для безопасного обмена сообщениями в режиме реального времени между рабочими станциями, подключенными к одной и той же сети TCP/IP, и механизм шифрования изображений с использованием расширение ключа AES. Неисправности, возникающие из-за шума в канале передачи, называются SEA, и это наиболее распространенный тип неисправности. Рекомендуемый метод шифрования спутниковых изображений - режим CTR. Расширенная схема управления ключами используется для хранения, извлечения секретных ключей, необходимых для шифрования и дешифрования, и управления ими. Модифицированное расширение ключа AES используется для генерации набора ключей, которые не являются нелинейными, для шифрования и расшифрования изображения. Этот метод обеспечивает высококачественное шифрование при низких требованиях

к памяти. Вышеупомянутые методы делают военную связь более безопасной и надежной.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1 Subramanyan, V.M. Chabria and T.G.S. Babu, «Image Encryption Based on AES Key Expansion», 2011 Second International Conference on Emerging Applications of Information Technology, Kolkata, 2011, pp. 217-220, doi: 10.1109/EAIT.2011.60.

2 AES Key Expansion, Accessed on: March 4, 2024 [Online]. Available: http://www.brainkart.com/article/AES-KeyExpansion_8410/

3 M.Alrammahi and U.Kaur, «Development of advanced encryption standard (AES) cryptography algorithm for wifi security protocol», International Journal of Advanced Research in Computer Science, vol. 5, no. 3, pp. 62-67, 2014. doi: 10.13140/RG.2.2.20993.97124.

4 A.M.Abdullah, «Advanced encryption standard (AES) algorithm to encrypt and decrypt data», Cryptography and Network Security, vol. 16, pp. 1-11, 2017.

5 N.Kashyap, A.Aggarwal and T.Choudhury, «Security techniques using Enhancement of AES Encryption», 2018 International Conference on Computational Techniques, Electronics and Mechanical Systems (CTEMS), Belgaum, India, 2018, pp. 468-472, doi: 10.1109/CTEMS.2018.8769278.

6 E.S.I.Harba, «Secure data encryption through a combination of AES, RSA, and HMAC», Engineering, Technology & Applied Science Research, vol. 7, no. 4, pp. 1781–1785, Aug. 2017, doi: 10.48084/etasr.1272

7 M.Z.Gunduz and R.Das, «Cyber-security on smart grid: threats and potential solutions», Computer Networks, vol. 169, 2020, doi: 10.1016/j.comnet.2019.107094.

8 R.Banu and T.Vladimirova, «Investigation of Fault Propagation in Encryption of Satellite Images Using the AES Algorithm», MILCOM 2006 – 2006 IEEE Military Communications conference, Washington, DC, 2006, pp. 1-6, doi: 10.1109/MILCOM.2006.302064.

9 P.Patil, P.Narayankar, D.G.Narayan, and S.M.Meena, «A comprehensive evaluation of cryptographic algorithms: DES, 3DES, AES, RSA and Blowfish», Procedia Computer Science, vol. 78, pp. 617–624, 2016, doi: 10.1016/j.procs.2016.02.108.

ӘОЖ 004.9

ЭЛЬ-ГАМАЛЬ АЛГОРИТМІ АРҚЫЛЫ РАДИОБАЙЛАНЫС ЖҮЙЕСІНІҢ ҚАУІПСІЗДІГІН АРТТЫРУ

ТЕМИРБЕКОВА Ж.Е., *PhD докторы*
МЫРЗАҚҰЛ Ж.Н., *қызметкер*

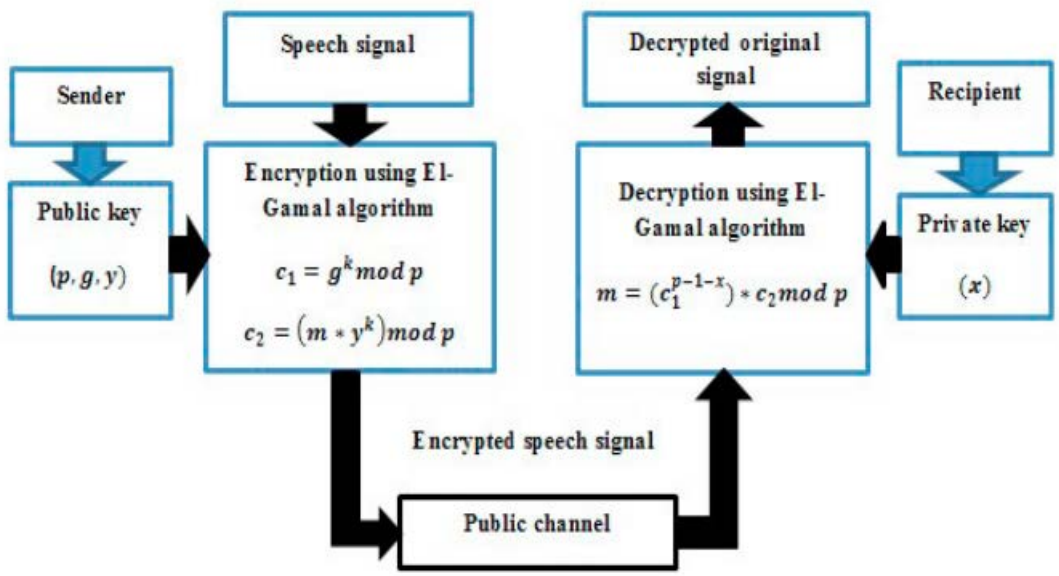
ҚР ҰҚК академиясы, Қазақстан Республикасы, Алматы қаласы

Аңдатпа. Радиобайланыс жүйелері әртүрлі салаларда, соның ішінде әскери операцияларда, төтенше жағдайларда және коммерциялық байланыста маңызды рөл атқарады. Дегенмен, радиоарна арқылы берілетін ақпаратты қорғау, әсіресе киберқауіпсіздік қауіпінің артуы жағдайында өте маңызды. Радиобайланыс жүйесінің қауіпсіздігін жақсарту үшін дискретті логарифмге негізделген Эль-Гамаль алгоритмін сөйлеу сигналдарына қолдануы қарастырылды. Эль-Гамаль ашық кілтті криптожүйесі модульдік дәреже мен дискретті логарифмдердің қасиеттерін қолдана отырып, қауіпсіз байланыс үшін сенімді шешім ұсынады. Бастапқы сигналда минималды бұрмалануды қамтамасыз ете отырып, сөйлеу сигналдарын шифрлау үшін қолайлы сандық көріністерге түрлендіру процестері талқыланып, криптографиялық операциялармен байланысты есептеу күрделілігін ескере отырып, нақты уақыт режимінде сөйлеу сигналдарын шифрлау және кері шифрлау мәселелері де шешіліп, салыстырулар жүргізілді.

Түйін сөздер: Эль-Гамаль алгоритмі, сөйлеу сигналын шифрлау, нақты уақыттағы өңдеу, криптографиялық операциялар, қауіпсіздік, байланыс жүйелері.

Эль-Гамаль алгоритмі – кілттерді бөлісуге және деректерді шифрлауға арналған криптографиялық алгоритм. Ол күрделі математикалық амалдарға, атап айтқанда дискретті логарифмге негізделген [1]. Эль-Гамаль алгоритмі күрделі құрылымымен және күшті математикалық принциптерді қолданумен қауіпсіздіктің жоғары деңгейін қамтамасыз етеді. Эль-Гамаль алгоритмі криптографияның әртүрлі салаларында, негізінен құпиялылық пен аутентификация үшін қолданылады [2]. Эль-Гамаль алгоритмін қолдануға болатын бірнеше аймақтар: Деректерді шифрлау. Эль-Гамаль алгоритмін хабарлар мен деректерді шифрлау үшін пайдалануға болады. Бұл әсіресе тасымалданатын ақпараттың құпиялылығы маңызды сценарийлерде пайдалы. Негізгі алмасу протоколдары: Эль-Гамаль алгоритмі екі тарап арасында ортақ құпия кілтті орнату үшін кілт алмасу протоколдарында жиі пайдаланылады [3]. Мысалы, оны Диффи-Хеллман протоколында қолдануға болады. Электрондық қолтаңба: Эль-Гамаль алгоритмі аутентификация мен деректердің тұтастығын қамтамасыз ететін электрондық қолтаңбаларды жасау үшін пайдаланылуы мүмкін [4]. Бұл хабарламалардың авторлығы мен түпнұсқалығын тексеру қажет жүйелерде маңызды. Аутентификация хаттамалары: Эль-Гамаль

аутентификация хаттамаларында қолданылуы мүмкін, мұнда тараптар өздерінің жеке басын растай алады және жалғандық мүмкіндігін болдырмайтын жолмен деректер алмасуы мүмкін. Торға негізделген криптография: Эль-Гамаль алгоритмін торға негізделген криптографияда қолдануға да бейімдеуге болады, бұл криптожүйелерді қорғаудың заманауи тәсілдерінің бірі болып табылады. Тұтастай алғанда, Эль-Гамаль алгоритмі күшті криптографиялық құралдарды қамтамасыз етеді және оны қолдану белгілі бір тапсырманың немесе жүйенің нақты талаптары мен сипаттамаларына байланысты. Эль-Гамаль алгоритмі RSA алгоритмінен ерекшеленеді, өйткені RSA-да қауіпсіздік үлкен бүтін факторларды табудың күрделілігіне негізделген, ал Эль-Гамаль алгоритмінде қауіпсіздік үлкен қарапайым модульдің дискретті логикасын есептеудің күрделілігіне негізделген. Эль-Гамаль криптожүйесінің тағы бір артықшылығы бір хабарламаны немесе қарапайым мәтінді әр шифрлау әр түрлі шифрланған мәтіндер жұбын шығарады [5]. Эль-Гамаль алгоритмінің жұмысын үш кезең түрінде ұсынуға болады, атап айтқанда: кілтті құру кезеңі, шифрлау және шифрды ашу кезеңдері. Әр кезең келесідей қысқаша 1-суретте көрсетілген.



Сурет 1 – Іске асырылған криптожүйенің құрылымдық схемасы

Материалдар мен әдістер

Ашық және құпия кілттерді генерациялау:

1. Кездейсоқ жай сан p таңдалады.
2. g бүтін сан таңдалады .
3. x кездейсоқ бүтін сан таңдалады $1 < x < p - 1$.
4. $y = g^x \bmod p$ есептеледі.
5. Ашық кілт (y, g, p), құпия кілт – x саны.

Шифрлау

M хабарламасы p санынан аз болуы керек. Хабарлама келесідей шифрланады:

1. Сеанс кілті таңдалады - кездейсоқ бүтін сан, k бұл $1 < k < p - 1$.
2. $C_1 = g^k mod p$ және $C_2 = y^k mod p$ сандары есептелінеді.
3. (C_1, C_2) сандар жұбы шифр мәтіні болып табылады.

Кері шифрлау

Құпия кілт x біле отырып, бастапқы хабарламаны формула бойынша (C_1, C_2) шифр мәтінінен есептеуге болады:

$$M \equiv C_2 * (C_1^x)^{-1} mod p.$$

$gcd(s, p) = 1$ шарты s мәні үшін әрқашан p модулі бойынша кері элемент бар екенін көрсетеді.

Эль-Гамаль алгоритмін радиобайланыс жүйесінде қолдану артықшылықтары 1-кестеде көрсетілген.

Кесте 1 – Эль-Гамаль алгоритмінің артықшылықтары

Артықшылығы	Сипаттамасы
Құпиялылық	Эль-Гамаль алгоритмін қолдана отырып, хабарламаларды шифрлау жіберілетін ақпараттың құпиялылығын қамтамасыз етеді, өйткені хабарламаны тек алушы өзінің жеке кілтімен шеше алады.
Кілттерді қауіпсіз бөлісу	Эль-Гамаль алгоритмін құрылғылар арасында кілттерді қауіпсіз бөлісу үшін пайдалануға болады, бұл хабарламаларды кейінірек шифрлау және шифрын ашу үшін ортақ құпия кілттерді сәйкестендіруге мүмкіндік береді.
Сандық қолтаңба	Сандық қолтаңбаларды құру және тексеру үшін Эль-Гамаль алгоритмін қолдану жіберушінің түпнұсқалығын және жіберілген деректердің тұтастығын қамтамасыз етеді.
Ұстаудан қорғау	Эль-Гамаль алгоритмі арқылы деректерді шифрлау оларды ұстауға және рұқсатсыз қол жеткізуге төзімді етеді, өйткені тіпті ұсталған деректер де шифрланған күйінде қалады.
Икемділік және масштабтау	Эль-Гамаль алгоритмі икемділік пен масштабталуға ие, бұл оны әртүрлі радиобайланыс сценарийлерінде, соның ішінде шифрлау, аутентификация және кілттермен алмасудың әртүрлі аспектілерінде қолдануға мүмкіндік береді.

Енгізілген криптожүйеге 1-кестедегі мәліметтер бойынша екі негізгі бөлік қатысады: сөйлеуді шифрлау және Эль-Гамаль алгоритмі негізінде сөйлеуді кері шифрлау. Біріншіден, ашық және жеке кілттер ашық кілт жіберуші тарапынан алынған сөйлеу үлгілерін шифрлау үшін пайдаланылған кезде жасалады. Екіншіден, шифрланған немесе кері шифрланған сөйлеу үлгілері қауіпсіз арна арқылы қабылдағышқа дәйекті түрде жіберіледі. Үшіншіден, шифрланған сөйлеу үлгілері бастапқы сөйлеу сигналын қалпына келтіру үшін алушы жағындағы жеке кілтке сәйкес шифрланады.

Нәтижелер

Төменде Эль-Гамаль шифрлау алгоритміне мысал көрсетілген:

$p = 179$ жай санын таңдау;

$g = 47, 1 < g < p$ таңдау;

формула бойынша $y = 4779(Mod\ 179) = 56$;

Аннаға ашық кілт $(y, g, p), (179;\ 47;\ 56)$ жібереді.

Анна келесі қадамдарды орындайды:

$p-1$- мен өзара жай санды таңдайды $x = 29, 1 < x < p - 1$;

формула бойынша a=4729(Mod 179)=110 есептейді;

Келесі қаадам әрбір символды шифрлайды:

$$Ш - 23, b = 5629 \bullet 23(Mod\ 179) = 176;$$
$$И - 8 = b = 5629 \bullet 8(Mod\ 179) = 69;$$
$$Ф - 19 = b = 5629 \bullet 19(Mod\ 179) = 52;$$
$$Р - 15 = b = 5629 \bullet 15(Mod\ 179) = 107;$$

(a, b) Бобқа жібереді.

Боб құпия кілтті және (3) формуланы қолдану арқылы кері шифрлау жасайды:

Шифрланған символдардың реттік номерін анықтайды:

$$176 \bullet 110179 - 79 - 1(Mod\ 179) = 23;$$
$$69 \bullet 110179 - 79 - 1(Mod\ 179) = 8;$$
$$52 \bullet 110179 - 79 - 1(Mod\ 179) = 19;$$
$$107 \bullet 110179 - 79 - 1(Mod\ 179) = 15;$$

Кілттердің генерациялау уақытын, шифрлау уақытын, кері шифрлау уақытын криптожүйенің әртүрлі деректер ұзындығы бойынша тестілеу үшін әр түрлі ұзындықтағы мәліметтер жиынтығын жасалынды. Ол үшін 1000, 2000, 3000, 4000, 5000 символды деректер файлы құрылды. Криптожүйе үшін кілттерді генерациялау процесі жасалынды. Генерацияланған кілттерді пайдаланып деректер жиынындағы әрбір файл шифрланды. Генерацияланған кілттерді пайдаланып әрбір шифрланған файлдың кері шифрлау процесі жүзеге асырылды. Әртүрлі кілт ұзындығы мен мәліметтер жиынтығы үшін 3-5 қадамдарды қайталанады. Кілттерді генерациялау, символдардық ұзындығы бойынша шифрлау, шифрланған деректердің ұзіндығы негізіндегі кері шифрлау уақыттары 2-кестеде көрсетілген.

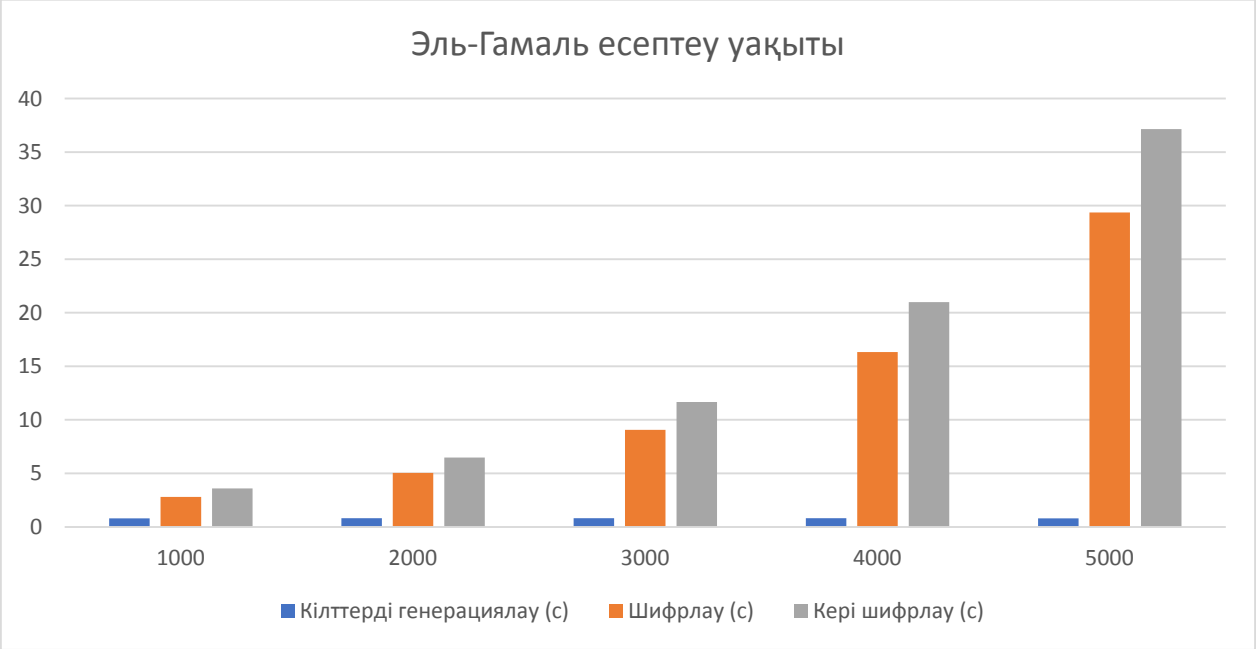
Кесте 2 – Эль-Гамаль криптожүйесінде әртүрлі кілттерді генерациялау, шифрлау, кері шифрлау нәтижесі

Символ саны	Кілттерді генерациялау (с)	Шифрлау (с)	Кері шифрлау (с)
1000	0,8	2,8	3,6
2000	0,81	5,04	6,48
3000	0,81	9,072	11,664
4000	0,81	16,3296	20,9954
5000	0,8	29,3638	37,1452

Эль-Гамаль криптожүйесінде 1000 символды деректердің кілттерді генерациялау процесі 0,8с, шифрлау уақыты 2,8с, кері шифрлау уақыты 3,6с құрады. Ал 2000 символды деректердің кілттерді генерациялау процесі 0,81с, шифрлау уақыты 5,04с, кері шифрлау уақыты 6,48с құрады. 3000 символды

деректердің кілттерді генерациялау процесі 0,81с, шифрлау уақыты 9,072с, кері шифрлау уақыты 11,464с құрады. 4000 символды деректердің кілттерді генерациялау процесі 0,81с, шифрлау уақыты 16,329с, кері шифрлау уақыты 20,995с құрады. 5000 символды деректердің кілттерді генерациялау процесі 0,8с, шифрлау уақыты 29,363с, кері шифрлау уақыты 37,142с құрады. Нәтижесінде бағдарламалық модульді практикалық тұрғыдан қолдануға болатынын көруге болады.

Сынақ нәтижелерін талдау барысында әртүрлі кілт ұзындығы мен деректер жиыны үшін кілттерді генерациялау, шифрлау және кері шифрлау уақытын салыстырамыз. Жалпы процесс 2-суретте көрсетілген.



Сурет 2 – Эль-Гамаль криптожүйесінде кілттерді генерациялау, шифрлау және кері шифрлау уақытын әртүрлі деректер ұзындығы бойынша тестілеу нәтижесі

Сынақ нәтижелеріне сүйене отырып қорытынды және қолданба үшін оңтайлы кілт ұзындығын анықтау нәтижесінде сәйкесінше, 1000 символды деректер файлы кілттерді генерациялау, шифрлау, кері шифрлау процесінде жылдам уақыт көрсеткішіне ие болды, деректер файлында символдардың өсуімен уақыт көрсеткіші өсе береді. Диаграммадан шифрлау алгоритмінің деректер саны өскен сайын уақыт сызықты өсетінін байқауға болады. Осыған байланысты бағдарламалық жасақтаманың алгоритм күрделігі: $O(n)$ құрады.

Эль-Гамаль криптожүйесінде кілттің оңтайлы ұзындығын анықтау үшін әр түрлі мәліметтер ұзындығында кілттерді генерациялау, шифрлау және кері шифрлау уақытын тексеруге болады. Тестілеу нәтижелері бойынша жасалуы мүмкін бірнеше тұжырымдар келесідей:

– кілт ұзындығы неғұрлым үлкенірек болса, криптожүйенің қауіпсіздік деңгейі соғұрлым жоғары болады, сонымен қатар кілттерді генерациялауға, шифрлауға және кері шифрлауға салыстырмалы түрде жоғарылау уақыт кетеді.

Кілт ұзындығын таңдағанда, шифрланатын хабарламалардың ұзындығына шектеулерді ескеру қажет. Мұндай жағдайда келесідей тұжырымдама жасауға болады: егер шифрланатын деректердің ұзындығы көп болса, онда сәйкесінше кілттің ұзындығын 24-40 бит көлемінде ал шифрланатын деректердің ұзындығы аса көп емес жағдайда кілттің ұзындығын 512 бит алуға болады;

– Эль-Гамаль криптожүйесінде кілт ұзындығы өнімділікке әсер етеді, өйткені хабарламаларды шифрлау және кері шифрлау үшін үлкен сандармен операцияларды орындау қажет. Қауіпсіздік маңызды болып табылатын көптеген қосымшалар үшін Эль-Гамаль криптожүйесінде кілт ұзындығын кемінде 2048 бит пайдалану ұсынылады. Егер өнімділік маңызды фактор болса, онда қысқа кілттерді қолдануға болады, бірақ кем дегенде 1024 бит.

Ұсынылған криптожүйенің өнімділігіне қол жеткізу үшін келесі жалпы өлшемдер қолданылады: сигнал шу коэффициенті (SNR), сегменттік сигналдың шуылға қатынасы (SNRseg) және журнал ықтималдығының коэффициенті (LLR). Бұл өлшемдердің қысқаша сипаттамасы төменде келтірілген.

Сигналдың шуылға қатынасы (SNR): сигнал қуатының сигналда бар фондық шу қуатына қатынасын сандық түрде анықтау үшін сигналды өңдеуде қолданылатын өлшем. Ол әдетте децибелмен (дб) өрнектеледі және сигналдың сапасын бағалау үшін қолданылады. Жоғары SNR мәндері шу деңгейіне қатысты сигналдың жақсырақ сапасын көрсетеді [6].

Сегменттік сигналдың шуылға қатынасы (SNRseg): бүкіл сигналға емес, сигналдың белгілі бір сегменттеріне немесе бөліктеріне бағытталған SNR вариациясы. Ол SNR-ге ұқсас есептеледі, бірақ әртүрлі бөліктердегі сапаның өзгеруін бағалау үшін сигналдың әртүрлі сегменттеріне қолданылуы мүмкін.

Журнал ықтималдығының коэффициенті (LLR): LLR-бұл әртүрлі салаларда, соның ішінде байланыс және ақпарат теориясында қолданылатын статистикалық өлшем. Бұл екі ықтимал гипотезаны немесе шешімді ескере отырып, белгілі бір сигналды байқау ықтималдығының арақатынасының логарифмі. Байланыс жүйелерінде LLR декодтау процестерінде жиі қолданылады, мысалы, қателерді түзету үшін арналарды декодтау, мұнда ол қабылданған сигналдар негізінде ең ықтимал жіберілетін хабарды анықтауға көмектеседі.

Шифрланған сөйлеу сигналының сапасы: шифрлау сапасының көрсеткіштері кез-келген сөйлеу криптожүйесінде екі мақсат үшін өте маңызды: сөйлеу криптожүйесінің бұрмалану дәрежесін, сөйлеу криптожүйесінің жақсы өнімділігін, сондай-ақ бұрмалану мөлшерін көрсету және сөйлеуді шифрлау әдісінің иммунитетін тыңдау құрылғыларының шабуылдарына анықтау. Қазіргі криптожүйеде қолданылатын шифрлау сапасының көрсеткіштері: сигнал/шу қатынасы (SNR), сегменттік сигнал/шу қатынасы (SNRseg) және логарифмдік ықтималдық қатынасы (LLR) арқылы шифрланған сөйлеу сигналының жоғары сапасына SNR және SNRseg мәндері төмендегенде және LLR мәні жоғарылағанда қол жеткізіледі. Ұсынылған әдістің нәтижелері 3-кестеде келтірілген.

Кесте 3 – Шифрлау процесі үшін қалдық талдау нәтижелері

Файл атауы	SNR (dB)	SNRseg(dB)	LLR
Signal 1	-35.0224	-38.0201	2.1145
Signal 2	-37.1918	-39.2972	2.1588
Signal 3	-35.0895	-43.9929	1.0794
Signal 4	-37.2481	-35.0016	1.4616

3-кестеден SNR және SNRseg мәндері төмен екені анық, ал LLR мәні жоғары, бұл төмен қалдық түсінікті көрсетеді. Бірақ ұсынылған әдіспен берілген шифрлау сапасы жоғары екенін білдіреді. Енгізілген криптожүйенің тиімділігіне шудың әсері қарастыруға тұрарлық маңызды мәселе болып табылады. Енгізілген әдіс өнімділігі әртүрлі қуат деңгейлеріндегі Гаусс шуымен сыналған. Бұл жұмыста SNR, SNRseg және LLR болып табылатын бірдей сапа көрсеткіштері шифрланған сөйлеу сигналы үшін (5дб-ден 50дб-ға дейін) шудың әртүрлі SNR мәндері болған кезде есептеледі. Нәтижелерден SNR және SNRseg өнімділік көрсеткіштерінің мәндері шудың мәніне сәйкес жоғарылайды, ал сигнал мәні кіріс SNR шу мәндерінің жоғарылауымен төмендейді. Осылайша, ұсынылған алгоритм жоғары SNR кезінде жоғары тиімділікпен шу әсеріне қарсы тұра алады.

Қорытынды

Аппараттық құралдардың дамуы қазіргі заманғы криптографиялық есептеулердің өнімділігін едәуір жақсартты. Дегенмен, криптографиялық алгоритмдерге хакерлердің шабуылдары да жоғары қарқынмен жасалуда. Бұл тұрғыда кілтті басқарудың ең жақсы шешімі ашық кілтті криптография болып табылады. Ашық кілт криптографиясында әрбір пайдаланушы өзінің құпия кілтін қорғауға жауапты. Бұл ерекше қасиет симметриялы алгоритмдерде жоқ болғандықтан, асимметриялық криптография желілер арқылы пайдаланушылардың деректерін қауіпсіз бөлісудің негізі болып табылады. Ұсынылған криптожүйе сөйлеу сигналдарын шифрлау мен кері шифрын ашу үшін қолданылатын ашық кілт технологиясының ерекше түрі. Эль-Гамаль криптожүйесін бұзу x құпия кілтін алу және C_1 табу үшін дискретті логарифм мәселесін шешуге негізделген. x және C_1 құпия кілттерін болжау тек x - ты болжаудан әлдеқайда қиын. Осы екі санның барлық ықтимал шешімдерін табу шабуылдаушы үшін мыңдаған жылдарға созылады. Сондықтан, бұл криптожүйе маңызды ақпараттың құпиялылығы мен қауіпсіздігін қамтамасыз ету үшін сөйлеу сигналдарының қауіпсіздігін қарастырады. Ұсынылған криптожүйенің өнімділігін әртүрлі шифрлау және кері шифрлау сапасының шаралары тұрғысынан талдау бастапқы сигналмен салыстырғанда қалпына келтірілген сөйлеу сигналының жақсы сапасын сақтай отырып, қауіпсіздіктің қанағаттанарлық деңгейін көрсетеді. Сонымен қатар, бұл криптожүйе әртүрлі қарқындылықтағы Гаусс шуына жақсы төзімділікке ие, бұл оның сөйлеу деректерін шифрлау мен кері шифрлаудағы тиімділігін растайды. Бұл

криптожүйені хаотикалық жүйелер немесе кодтау алгоритмдері сияқты қауіпсіздіктің басқа деңгейін қосу арқылы одан әрі жақсартуға болады. Ұсынылған криптожүйенің криптографиялық беріктігі, кілттермен алмасу механизмі және деректердің аутентификациясы мен тұтастығын қамтамасыз ету мүмкіндігі, радиоарна арқылы берілетін ақпаратты қорғау үшін тиімді екені көрсетілді. Бұл алгоритмді енгізу, әртүрлі қолданбаларда радиобайланыс жүйесінің қауіпсіздігі мен сенімділігін арттыруға өз үлесін тигізеді.

ПАЙДАЛАНЫЛҒАН ӘДЕБИЕТТЕР ТІЗІМІ

1 Ian F. Blake and Theo Garefalakis. On the complexity of the discrete logarithm and diffie-hellman problems. J. Complex., 20(2-3):148-170, 2004.

2 Dan Boneh. The decision Diffie-Hellman problem. Lecture Notes in Computer Science, 1423:48-63, 1998.

3 Dan Boneh, Antoine Joux, and Phong Q. Nguyen. Why textbook elgamal and rsa encryption are insecure. In ASIACRYPT ’00: Proceedings of the 6th International Conference on the Theory and Application of Cryptology and Information Security, pages 30–43, London, UK, 2000. Springer-Verlag.

4 Trepacheva A. V., Babenko L. K. Formal cryptanalysis of fully homomorphic systems using the problem of factorization of numbers // Information counteraction to terrorism threats. – 2015. No. 24. – P. 283-286.

5 Sonia Rani, and Harpreet Kaur. (2017) «Technical Review on Symmetric and Asymmetric Cryptography Algorithms» International Journal of Advanced Research in Computer Science 8 (4): 182-186.

6 Tin Zar New, and Su Wai Phyo. (2015). «Performance Analysis of RSA and ElGamal for Audio Security» International Journal of Software Engineering and Technology Informatics 1 (1): 0031-0035.

УДК 004.621.39

АТМОСФЕРНЫЕ ОПТИЧЕСКИЕ ЛИНИИ СВЯЗИ - НОВАЯ АЛЬТЕРНАТИВА ПРОВОДАМ

ЛЕВИНА Ю.Д., *м.п.н., подполковник*

Военно-инженерный институт радиоэлектроники и связи,
г.Алматы, Республика Казахстан

Аннотация. В статье рассмотрены вопросы разработки атмосферных оптических линий связи (АОЛС), одна из главных причин популярности АОЛС – сложность обнаружения самого факта связи, невозможность перехвата сообщений и, главное, невозможность подавления связи средствами радиоэлектронной борьбы (РЭБ).

Ключевые слова: атмосферные оптические линии связь, инфракрасное излучение, оптическая система, беспроводная связь, фотодиод.

Түйіндеме. Мақалада атмосфералық оптикалық байланыс линиясын (АОБЛ) жасау сұрақтары қарастырылған, АОБЛ белгілілігінің негізгі себептері болып – байланыс фактісінің қиындығын табу, мәліметті және, негізгі, радиоэлектронды күрес (РЭК) құралдарымен байланысты бақылауға алдын алу мүмкіндігін жою.

Негізгі сөздер: атмосфералықоптикалық линиялық байланыс, инфрақызыл сәулесі, оптикалық жүйесі, желісіз байланыс, фотодиод.

Abstract: the article deals with the development of atmospheric optical communication lines (FSO Free Space Optics), one of the main reasons for the popularity of FSO – the complexity of the detection of the fact of communication, the inability to intercept messages and, most importantly, the inability to suppress communication means electronic warfare (EW).

Keywords: atmospheric optical communication lines, infrared radiation, optical system, wireless communication, photodiode.

Сегодня на практике все еще применяются традиционные решения связи – это проводные каналы (медный кабель, волоконно-оптические линии связи), беспроводные радиолинии. Но прогресс не стоит на месте, особенно в наш век информатизации.

В начале XXI века все большую популярность набирают атмосферные оптические линии связи (*далее – АОЛС)* (FSO технология), которые делают возможной передачу данных через атмосферу по лазерному лучу. Звучит фантастически, но в свое время и беспроводные радиосоединения казались чем-то нереальным.

Так что же такое АОЛС и в чем их преимущество перед «традиционными» линиями связи. Идея использования света для передачи информации вовсе не новая. В 1880 году Александр Белл запатентовал

фототелефон, в котором солнечный луч, отраженный от зеркальца, модулировался голосом, передавался через атмосферное пространство и поступал на твердотельный детектор. Так, задолго до изобретения лазера, оптического волокна и даже радио, появился прототип современных атмосферных оптических линий связи.

В СССР первая АОЛС была создана в Москве в 1965 году – была пущена телефонная линия между зданием МГУ на Ленинских горах и Зубовской площадью протяженностью около 5 км.

После этого в СССР было построено еще несколько АОЛС: в Ереване, Красногорске, Куйбышеве, Клайпеде. В целом, испытания прошли успешно, но на тот момент технология АОЛС была признана неперспективной, и первые системы на базе лазеров так и не прижились. Для лазерных лучей требовалась прямая и хорошая видимость: малейшее колебание здания под напором ветра или из-за проехавшего мимо машина могло сбить луч с курса [1].

Решить эти проблемы удалось в 1990-х годах за счет использования сложных систем автотрекинга. Наряду с применением современной элементной базы, это позволило лишь в XXI веке создать высокоэффективные АОЛС.

Чтобы отличить новые лазерные системы от их предшественников, технологии присвоили новое название Free Space Optics (FSO, буквально – «оптика в свободном пространстве»).

FSO технология: Технология FSO, атмосферная оптическая связь, АОЛС, АОЛП, беспроводный оптический канал связи (БОКС) – это способ беспроводной передачи информации в коротковолновой части электромагнитного спектра. В ее основе лежит принцип передачи цифрового сигнала через атмосферу (или космическое пространство) путем модуляции излучения в нелицензируемом диапазоне длин волн (инфракрасном или видимом) и его последующим детектированием оптическим фотоприемным устройством. Импульс светового излучения при прохождении в атмосфере практически не испытывает дисперсионных искажений фронтов, характерных для любых оптических волокон. Это принципиально позволяет передавать поток данных со скоростями до террабит в секунду. К основным преимуществам такого способа передачи информации можно отнести: высокие скорости передачи (которые невозможно достичь при использовании любых других беспроводных технологий), простота инсталляции, а также отсутствие необходимости платить за использование частотного диапазона. В настоящее время технология обеспечивает передачу цифровых потоков до 10 Гбит/с, что позволяет:

− решать проблемы «последней мили» при высокой защищенности канала связи,

− развивать городские сети передачи данных и голоса (MAN),

− развивать решения WDM (волновое мультиплексирование) для сетей SONET/SDH.

Современное состояние FSO технологии (беспроводной оптической связи) позволяет создавать надежные каналы связи на расстояниях от 100 до

1500-2000 м в условиях атмосферы и до 100 000 км в открытом космосе, например, для связи между спутниками. Являясь альтернативным решением по отношению к оптоволокну, атмосферные оптические линии передачи данных (АОЛП) позволяют сверхоперативно сформировать беспроводный оптический канал связи (мобильные системы с автонаведением обеспечивают установление связи за 10-15 минут) при значительно меньших затратах [2].

Сегодня данная технология является одной из новейших в телекоммуникационной отрасли, она стала доступна широкому кругу пользователей. Потребность в лазерной связи возросла, так как стали стремительно развиваться информационные технологии. Резко увеличивается число абонентов, развиваются Интернет, IP-телефония, кабельное телевидение с большим числом каналов, компьютерные сети и т.д.

В основе беспроводных оптических систем лежат технологии организации высокоскоростных каналов связи посредством инфракрасного излучения. Это делает возможной передачу данных (текстовые, звуковые, графические данные) через атмосферное пространство, предоставляя оптическое соединение без использования стекловолокна.

Лазерная связь: Передатчиком служит мощный полупроводниковый лазерный диод. Входной электрический сигнал поступает в приемопередающий модуль, в котором кодируется различными помехоустойчивыми кодами, модулируется оптическим лазерным излучателем, фокусируется оптической системой передатчика в узкий коллимированный лазерный луч и передается в атмосферу.

На принимающей стороне оптическая система фокусирует оптический сигнал на высокочувствительный фотодиод, который преобразует оптический пучок в электрический сигнал. Далее сигнал демодулируется и преобразуется в сигналы выходного интерфейса.

Скорость передачи информации, достигаемая в беспроводном оптическом канале, сравнима с оптоволоконным. Некоторые модели позволяют построить соединение с пропускной способностью 100/200 Мбит/с. В настоящий момент также есть модель со скоростью 10 Гбит/с в полнодуплексном режиме. Эта единственная представленная на мировом рынке беспроводная система связи, осуществляющая передачу данных на такой скорости, произведена на предприятии – Государственном Рязанском приборном заводе (ГРПЗ) [3].

Преимущества: АОЛС без труда преодолевают водные и транспортные магистрали, железнодорожные пути, непроходимые местности, где прокладка кабельных соединений невозможна или затруднена. Они вне конкуренции в случае сжатых сроков, так как запуск канала занимает всего несколько часов.

Системы могут применяться только на соединениях типа «точка – точка» и оперируют очень узкой диаграммой направленности излучения, поэтому можно создать почти неограниченное количество каналов в непосредственной близости друг от друга.

Как известно, безопасность имеет особое значение во всех системах беспроводной связи. Поскольку радиочастотные системы излучают сигналы во

всех направлениях, то сигналы можно просто и легко перехватить или подавить средствами радиоэлектронной борьбы (РЭБ). Поэтому для повышения безопасности радиочастотных сетей обычно применяют кодирование и различные средства защиты передаваемой информации.

Однонаправленный луч света атмосферной оптической линии связи перехватить трудно. АОЛС-системы нечувствительны к электромагнитному шуму, не производят его. У них лучшая, чем у радио, защищенность. Именно поэтому эти системы активно используются в силовых ведомствах для организации временных линий связи, беспроводных высокоскоростных защищенных каналов связи на дистанциях от 50 м до 7 км, где прокладка кабельных соединений невозможна или затруднена. При этом АОЛС Artolink производства ГРПЗ – единственное на рынке подобное оборудование, обеспечивающее дальность связи до 7 км.

Атмосферную оптическую линию связи Artolink демонстрировали в Москве на выставке Interpolitex 2014.

Оборудование Artolink эксплуатируется в России, в странах СНГ и дальнем зарубежье: США, Индии, Сирии, Южной Корее, странах Евросоюза и других.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1 Вишневский В.М. Широкополосные беспроводные сети передачи информации. – М.: Техносфера, 2005. – С.52-58.

2 Елисеев И.В. Доверие к беспроводной оптике // Военно-теоретический журнал. Москва 2021. – С.47.

3 Аппаратура атмосферной оптической линии связи Artolink. [Электронный ресурс]. – URL:https://dzen/ru (дата обращения 06.03.24)

4 Атмосферные оптические линии связи. [Электронный ресурс]. – URL:https://as.kz (дата обращения 24.02.24).

УДК 623.6

ИСПОЛЬЗОВАНИЕ ТЕХНОЛОГИЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В СИСТЕМЕ УПРАВЛЕНИЯ БЕСПИЛОТНЫМ ЛЕТАТЕЛЬНЫМ АППАРАТОМ

ШАНДРОНОВ Д.Н., *доктор PhD, полковник,*
ДУЙСЕМБЕКОВ О.А., *к.т.н. подполковник,*
ЖАНБУЛАТОВ Д.М., *подполковник*

Военно-инженерный институт радиоэлектроники и связи,
город Алматы, Республика Казахстан

Аннотация. В статье представлена структурная схема комплекса с беспилотным летательным аппаратом, обозначена необходимость использование автономной системы управления. Приведена структурно-функциональная схема систем навигации и управления беспилотным летательным аппаратом, которые позволят обеспечить требуемый уровень автономности. Для построения автономной системы управления акцент сделан на использовании оптико-электронных средств, методов и алгоритмов компьютерного зрения, технологий искусственного интеллекта.

Данная научная статья опубликована в рамках выполнения научно-исследовательской работы ИРН BR21882279 «Разработка и изготовление малогабаритного ретранслятора связи на базе беспилотного летательного аппарата (БПЛА) для увеличения дальности и устойчивости радиосвязи».

Ключевые слова: беспилотный летательный аппарат, автономная система управления, инерциальная навигационная система, компьютерное зрение, искусственный интеллект.

Аннотация. Мақалада ұшқышсыз ұшу аппараты бар кешеннің құрылымдық сызбасы келтіріліп, автономды басқару жүйесін қолдану қажеттілігі көрсетілген. Автономияның қажетті деңгейін қамтамасыз етуге мүмкіндік беретін ұшқышсыз ұшу аппаратын навигациялау және басқару жүйелерінің құрылымдық-функционалдық сызбасы келтірілген. Автономды басқару жүйесін құру үшін оптикалық-электронды құралдарды, компьютерлік көру әдістері мен алгоритмдерін, жасанды интеллект технологияларын қолдануға баса назар аударылады.

Бұл ғылыми мақала ЖТН BR21882279 «Радиобайланыстың қашықтығы мен тұрақтылығын арттыру үшін ұшқышсыз ұшу аппараты (ҰҰА) базасында шағын габаритті байланыс ретрансляторын әзірлеу және дайындау» ғылыми-зерттеу жұмысын орындау шеңберінде жарияланған.

Түйін сөздер: ұшқышсыз ұшу аппараты, автономды басқару жүйесі, инерциялық навигация жүйесі, компьютерлік көру, жасанды интеллект.

Одним из трендов развития научно-производственных направлений в наши дни является проектирование и разработка беспилотных летательных аппаратов (далее БПЛА), предназначенных для использования в различных сферах жизнедеятельности человека, в том числе в государственных силовых структурах. Основанием для данного утверждения послужили следующие предпосылки:

во-первых, стремительно возрастающая роль применения БПЛА в военных конфликтах, как для ударных действий, так и для обеспечивающих;

во-вторых, расширение круга задач, возлагаемых на беспилотные летательные аппараты, которые стали использоваться как в интересах силовых государственных органов, так и в других ведомствах, деятельность которых во многом облегчается использованием беспилотных летательных аппаратов.

Данное обстоятельство требует постоянного развития и совершенствования БПЛА различного назначения, как в технической реализации, так и в способах их применения.

Актуальность и необходимость применения БПЛА для обеспечения боевых действий Сухопутных войск указана в [1-6]. Основное преимущество использования БПЛА в военных целях – минимизация потерь личного состава при выполнении опасных задач, низкие затраты на содержание и применения, минимальная вероятность обнаружения во время полета, а также передача необходимой информации в режиме реального времени.

По мнению военных экспертов БПЛА в настоящее время значительно изменили тактику ведения боевых действий, поэтому в ближайшем будущем количество БПЛА в войсках, а также круг решаемых ими задач будут неуклонно возрастать. Для дальнейшего развития теоретических положений и повышения эффективности боевых действий Сухопутных войск, Сил специальных операций, разведывательных сил необходимо совершенствование применения БПЛА.

Как правило, подавляющее большинство известных БПЛА так или иначе задействуют наземный пункт управления. Поэтому имеет смысл рассматривать комплекс с беспилотным летательным аппаратом. Состав и структурная схема такого комплекса, представлена на рисунке 1 [7].

Рассматриваемый комплекс с БПЛА включает в себя две подсистемы: бортовую и стационарную (размещенную на наземном пункте управления) подсистемы.

Бортовая подсистема включает в свой состав три основных системы: управления, связи и навигации. Стационарная подсистема включает в свой состав системы связи, отображения и управления.

Системы связи (бортовая и стационарная) обеспечивают помехоустойчивый приём и передачу данных между БПЛА и пунктом управления.

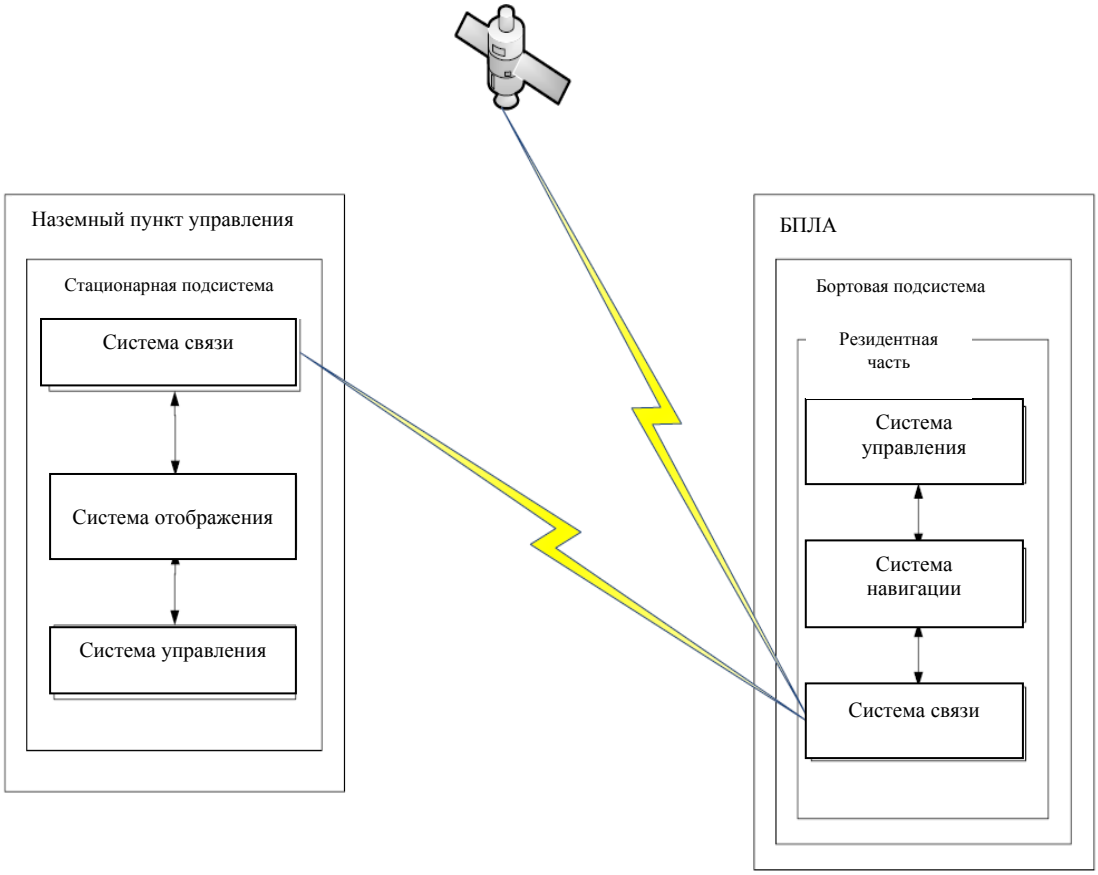


Рисунок 1 – Структурная схема комплекса с беспилотным летательным аппаратом

Стационарная система отображения предназначена для обеспечения интерфейса оператора при управлении, контроле БПЛА, а также получении информации от бортовых средств.

Бортовая система навигации состоит из инерциальной и спутниковой подсистемы и предназначена для обеспечения формирования навигационной информации для управления БПЛА.

Бортовая и стационарная управляющие системы обеспечивают обработку получаемой информации, формирование команд управления полётом и режимами работы БПЛА, контроль функционирования аппаратуры.

Одной из проблем в настоящее время является недостаток существующего способа управления беспилотными летательными аппаратами в системе оператор-БПЛА, которое осуществляется в зоне прямой радиовидимости. Его невозможно использовать при значительном увеличении дальности полета и вне условий прямой радиовидимости [8, 9]. Кроме того, передача команд управления осуществляется через широкополосную система радиосвязи, для которой характерны низкие помехозащищенность и помехоустойчивость [10, 11], что может способствовать, в условиях радиоэлектронного противодействия, перехвату канала управления БПЛА или его подавлению. В таких случаях не исключается прекращение выполнения боевой задачи или потеря БПЛА.

Данные обстоятельства вызывают острую необходимость проведения

теоретических и практических поисков в направлении обеспечения устойчивого непрерывного управления БПЛА, в том числе без привязки к спутниковым системам [12].

В зависимости от используемой системы управления БПЛА подразделяются на три класса [13]: с автоматизированным (радиокомандным), с автономным (программным) и ручным управлением. Подавляющее большинство созданных и применяемых БПЛА имеют автоматизированную, ручную или комбинированную системы управления, что повышает вероятность потери аппарата в результате ошибки оператора или потери сигналов управления и навигации. В связи с этим построение БПЛА с автономным управлением является наиболее приоритетным направлением развития беспилотной техники.

Вышесказанное проявляются в существующих тенденциях развития аппаратной составляющей БПЛА. Устройства, разрабатываемые в последние годы, обеспечивают технические возможности для создания БПЛА с высоким уровнем автономности. Известно 5 основных уровней автономности БПЛА [14], которые представлены в таблице 1.

Таблица 1 – Уровни автономности БПЛА

Уровень автономности	Уровень 0	Уровень 1	Уровень 2	Уровень 3	Уровень 4	Уровень 5
Степень автоматизации	Нет	Низкая	Частичная	Условная	Высокая	Полная
Описание	Управление 100% ручное	Пилот несет ответственность за управление дроном. Дрон способен выполнять минимум 1 важную функцию	Пилот несёт ответственность за безопасности операций. Дрон способен поддержи-вать высоту в определён-ных условиях, а также регулирует направление	Пилот работает в аварийном режиме. Дрон способен выполнять все функции самостоя-тельно, но «при заданных определён-ных условиях»	Пилот не принимает никакого участия в цикле управления. Дрон оснащен несколькими аварийными системами, так что в случаях сбоя одной из систем дрон продолжит работать	Дрон использует систему ИИ при планировании полета
Уклонение от препятствий	Нет	Обнаружение и уведомление		Обнаружение и уклонение	Обнаружение и самостоятельное уклонение	

Примечание – таблица составлена по материалам [14].

Анализ существующих БПЛА позволил заключить, что в настоящее время известны примеры дронов 4-го уровня автономности, к которым можно отнести модели: Skydio R1 копании NVIDIA, построенный на основе чипа Jetson TX1; DJI Mavic 2, использующий систему обнаружения препятствий в нескольких направлениях FlightAutonomy. Системы управления и навигации, реализующие известные технологии, как правило, состоят из достаточно большого набора различных компонентов, а также используют спутниковую подсистему местоопределения БПЛА (задействуют данные полученные от бортовой

системы связи). Так, например, система «FlightAutonomy», состоит из 7 компонентов, включая 5 камер (датчики двойного видения, прямого и нижнего, и главную камеру), двухдиапазонное позиционирование спутников (GPS и GLONASS), 2 ультразвуковых дальномера, резервные датчики и группу из 24 мощных специализированных вычислительных ядер.

Не вызывает сомнений, что в случае отсутствия или потери доступа к каналам связи или спутникового позиционирования известные виды БПЛА будут иметь затруднения для продолжения работы в штатном режиме. Следовательно, для повышения уровня автономности необходимо доработать бортовую систему управления, представленную на рисунке 1, таким образом, чтобы в случае отсутствия доступа к каналам связи БПЛА имел возможность использовать для обеспечения автономности полёта данные инерциальной подсистемы и информацию мониторинга территории и объектов. Решение данной задачи видится в разработке ряда специализированных методов и алгоритмов компьютерного зрения, представленных в работе [12, 15]. Данные методы и алгоритмы возможно реализовать с использованием специального вычислителя, размещённого на борту БПЛА, в составе системы обработки и распознавания изображений. Задачей данной системы будет являться добывание данных для системы управления беспилотным летательным аппаратом, которая должна обеспечить автоматический взлёт и посадку БПЛА, выход в район выполнения задачи, определение препятствий по ходу движения, обеспечивая высокий уровень его автономности.

Структурно-функциональная схема автономной системы наведения, демонстрирующая принцип работы БПЛА в режиме использования инерциальной системы навигации, может иметь вид, представленный на рисунке 2, где синим цветом отмечены блоки, в которых могут найти место технологии искусственного интеллекта, получившие в настоящее время активное развитие.

В представленной схеме системы наведения БПЛА важную роль выполняет система обработки и распознавания изображений, на вход которой будет поступать информация от инерциальной навигационной системы с эталонным изображением местности и датчика изображений. На выходе будут выдаваться координаты новой точки целеуказания. В основе принципа работы системы обработки и распознавания изображений лежат задачи предобработки, обнаружения, распознавания и целеуказания. Рассмотрим подробнее каждую задачу.

Задача предобработки состоит в снижении влияния шума и улучшения качества исходного изображения. Необходимо отметить, что подавление погодных помех в системах компьютерного зрения по-прежнему остаётся трудно решаемой задачей. В связи с этим актуальным видится проведение исследований, направленных на разработку алгоритмов фильтрации для подавления статических и динамических погодных помех.

Для решения задач обнаружения и распознавания изображений существует большое число различных подходов, среди которых наиболее перспективным

видится использование методов машинного обучения, включая искусственные нейронные сети, машины опорных векторов, алгоритмы бустинга и другие [16]. Наибольшую эффективность в решении задач распознавания образов, включая задачи классификации изображений, показывают глубокие нейронные сети, в том числе сверточные нейронные сети. Их преимуществом является автоматический выбор признаков [16].

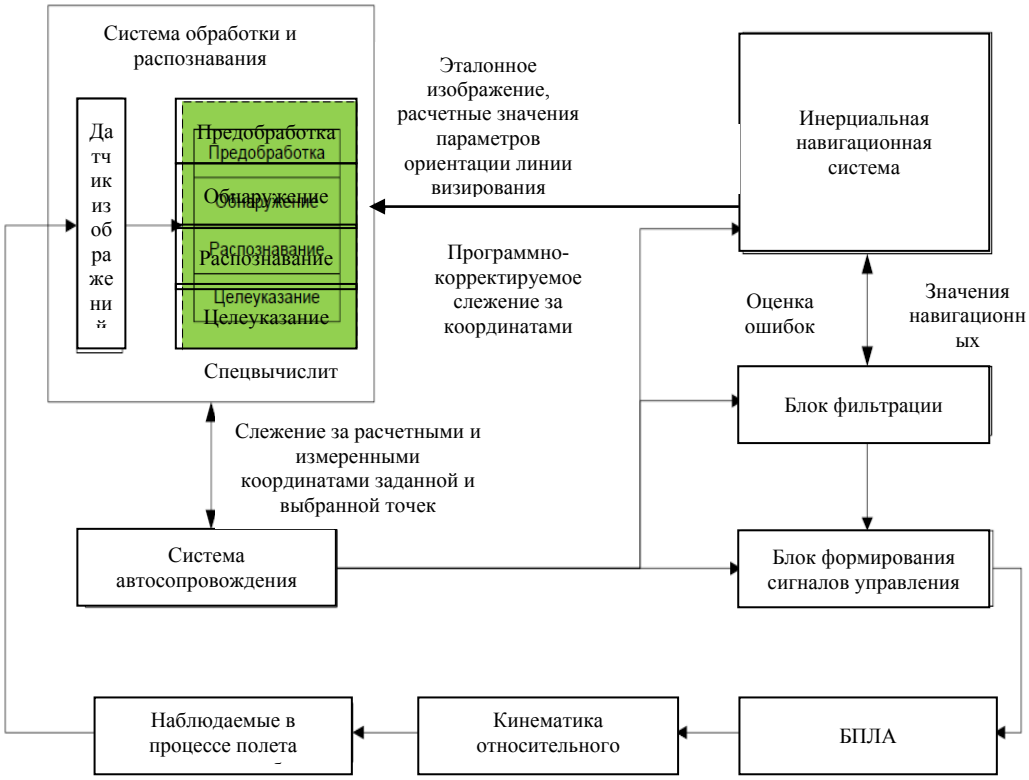


Рисунок – 2 Структурно-функциональная схема автономной системы наведения БПЛА

Задача целеуказания в общем случае сводится к расчёту на основе данных, полученных в результате обнаружения и распознавания на изображении различных объектов, траектории БПЛА.

Несомненно, можно сделать БПЛА полностью автономным, который будет решать задачи в автоматическом режиме. Но запрограммировать все возможные ситуации (обучить нейронную сеть на множествах различных обучающих выборок) представляет собой достаточно сложную задачу. Исходя из этого видится необходимым построение адаптивной системы управления. Даная система управления должна обеспечивать перераспределение функций между бортовой и стационарной системами управления, а также включать в свой состав экспертную систему принятия решений, предназначенную для формирования рекомендаций оператору БПЛА по наиболее целесообразным действиям в текущей обстановке. В свою очередь, бортовые устройства должны обеспечивать систему управления всей необходимой информацией об изменениях условий полёта, а система связи – безопасную и помехоустойчивую передачу этих данных оператору [17].

Таким образом, можно сделать следующие выводы:

– в условиях высокой вероятности радиоэлектронного подавления каналов управления и навигации БПЛА возникает необходимость иметь автономную бортовую систему управления;

– важную роль в создании системы автономного управление БПЛА должны играть оптико-электронные системы, совершенствование которых в настоящее время позволяет осуществлять подробный мониторинг местности;

– в связи с разработкой и активным внедрением специализированных графических процессоров, позволяющих эффективно решать задачи компьютерного зрения с использованием методов машинного обучения, в том числе на борту БПЛА, видится необходимость проведения исследований в данном направлении.

Решение данных задач позволит в конечном итоге, используя современную аппаратную базу, осуществить разработку комплекса с БПЛА, который можно применять в режиме автономности высокого уровня.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1 Шандронов Д.Н. Вероятный характер будущих военных конфликтов // Научные труды ВИИРЭиС. – №3. – 2020. – С.135-145.

2 Темірбекұлы А. Применение беспилотных авиационных комплексов в специальной войсковой операции // Современное состояние и перспективы развития БПЛА в Республике Казахстан. Материалы Международной научно-теоретической конференции: Сборник статей и докладов, каталог БПЛА мировых производителей – Нур-Султан. – 2020. – С.82-85.

3 Темірбекұлы А. Изменение тактики действий незаконных вооруженных формирований по опыту войны в Сирии // Военно-теоретический журнал Бағдар Национального университета обороны – Астана. – 2018. - №1. – С.56-58.

4 Семченко А.Г. Краткий обзор и анализ боевого применения БПЛА в современных вооруженных конфликтах / Бекетов Б.Ш., Семченко А.Г. // Хабаршысы НУО – 2021. – № 4.– С. 54-58.

5 Яцук К.В., Стафее М.С., Казаринов С.В. Применение беспилотных летательных аппаратов в локальных конфликтах и войнах // Молодой ученый. – 2016. - №5. – С.107-111.

6 Бодрова А.С. Сборник докладов и статей по материалам II научно-практической конференции «Перспективы развития и применения комплексов с беспилотными летательными аппаратами» / Под. общ. ред. А.С. Бодрова, С.И. Безденежных. - Коломна: ГЦ БпА МО РФ, 2017. – 337 с.

7 Ищук В.И., Мочалов С.А. Принцип построения радиоэлектронного оборудования комплексов с беспилотными летательными аппаратами ВМФ // Доклады и статьи ежегодной научно-практической конференции «Перспективы развития и применения комплексов с беспилотными летательными аппаратами». Коломна: ГЦ БпА МО РФ, 2016. – С. 95–100.

8 Долуханов, М. Распространение радиоволн / М. П. Долуханов. – М.: Связь, 1972. – 336 с.

9 Фомин А.Н., Копылов В.А., Филонов А.А., Андронов А.В. Общая теория радиолокации и радионавигации. Распространение радиоволн: учебник / под общ. ред. А.Н. Фомина. – Красноярск: Сиб. федер. ун-т, 2017. – 318 с.

10 Жанбулатов Д.М. Криптографическая защита радиопереговоров в коротковолновых каналах связи // Научные труды ВИИРЭиС. – №2(52). – 2023 г. – С.95-100.

11 Красильников М. Н., Современные информационные технологии в задачах навигации и наведения беспилотных летательных аппаратов, Москва: ФИЗ-МАТЛИТ. – 2009. – С.1-36.

12 Буянов И.А. Автономная система ориентирования беспилотного летательного аппарата: состав и схема функционирования в формате 3D // Молодой учёный. 2017. №50 (184). С. 24-30.

13 Замятин П.А. Системы управления беспилотными летательными аппаратами. // Инновационная наука. – 2020. - №4. – С.37-42.

14 Radovic *M.* Tech Talk: Untangling The 5 Levels of Drone Autonomy [Электронный ресурс] URL: https://www.droneii.com/drone-autonomy (дата обращения: 27.02.2024).

15 Красильщиков М.Н., Себрякова Г.Г. Управление и наведение беспилотных маневренных летательных аппаратов на основе современных информационных технологий: учеб. пособие. М.: ФИЗМАТЛИТ, 2003. 280 с.

16 Гареев М.Ш., Котляр А.В., Кулеев Р.Ф., Янин Д.М. Методы автоматического обнаружения и сопровождения объектов по изображениям, полученным с БЛА // Сборник докладов и статей по материалам II научно-практической конференции «Перспективы развития и применения комплексов с беспилотными летательными аппаратами» / Под. общ. ред. А.С. Бодрова, С.И. Безденежных. - Коломна: ГЦ БпА МО РФ, 2017. – С. 48-51.

17 Тутубалин П.И., Кирпичников А.П. Обеспечения информационной безопасности функционирования комплексов беспилотной разведки // Вестник технологического университета. 2017. Т. 20. № 21. С. 86-92.

УДК 355:34

ТЕХНИЧЕСКОЕ ОБСЛУЖИВАНИЕ ОБОРУДОВАНИЯ СВЯЗИ

КАРАТАЕВ Б.С., *преподаватель, майор запаса*

Казахский национальный исследовательский технический университет имени К.И.Сатпаева, Институт военного дела город Алматы, Республика Казахстан

Аннотация. Для оценки качества эксплуатации аппаратуры связи в подразделениях ГПС периодически проводятся технические осмотры и проверки. Объем и периодичность выполнения мероприятий по техническому обслуживанию определяются специальными инструкциями по техническому обслуживанию (эксплуатационная и ремонтная документация). Техническое обслуживание средств связи проводится по планово-предупредительной схеме, которая предусматривает следующую периодичность технического обслуживания: ТО № 1 (ежедневное); ТО № 2 (еженедельное); ТО № 3 (квартальное); ТО № 4 (сезонное).Планирование эксплуатации, технического обслуживания и ремонта средств связи осуществляется начальником службы связи гарнизона и отражается в годовом плане эксплуатации средств связи, утверждаемом начальником.

Ключевые слова: Оборудование связи, регламент работы, эксплуатация цифровых телефонных станций.

Оборудование связи – это целый комплекс технически сложной аппаратуры, которая обеспечивает возможность регулярного обмена различными данными между основными пользователями на определенных расстояниях. Примеров и разновидностей такого оборудования очень много – начиная от портативных любительских радиостанций и заканчивая сложной системой спутниковой связи.

Вне зависимости от типа оборудования, при его регулярном использовании происходят различные процессы:

- естественная выработка ресурса (износ);
- выход из строя отдельных компонентов или всего устройства в целом;
- поломки, возникающие по причине неправильной эксплуатации.

Чтобы избежать преждевременного выхода из строя аппаратуры, необходимо проводить регулярное техническое обслуживание оборудования связи. Это комплекс мероприятий, который имеет циклическую периодичность и включает в себя целый ряд работ, которые гарантирует стабильное функционирование комплекта аппаратуры.

Основные виды операций для обслуживания оборудования связи

Обслуживание оборудования связи предусматривает проведения целого ряда операций:

- контрольно-проверочные мероприятия. В ходе работ проверяются основные технические характеристики аппаратуры, путем проведения соответствующих замеров и сравнивая результаты с эталонными показателями. Также на этой стадии могут быть выявлены различные дефекты, которые трудно обнаружить при штатном использовании оборудования;

- регулировка и настройка. В случае выявления отклонений от заданных рабочих показателей и отсутствие поломок, производят настройку, регулировку или калибровку аппаратуры согласно нормативным рабочим показателям;

- профилактика и ремонт. Основная цель профилактических работ заключается в выявлении различных дефектов, которые могут повлиять на работоспособность всего оборудования или конкретного узла. В случае необходимости для устранения существенных неисправностей проводят ремонтные работы.

Стадии технического обслуживания

Регулярная профилактика гарантирует отсутствие серьезных поломок оборудования и существенно увеличивает его работоспособность и продолжительность эксплуатации. Техническое обслуживание производится исходя из периодичности и в зависимости от типа аппаратуры.

Все мероприятия разделяются на четыре основные группы:

- ежедневная профилактика. Обязательное условие для оборудования, которое работает в круглосуточном режиме или с перерывом не более 24 часов. В комплекс работ входит внешний осмотр, удаление загрязнений с аппаратуры без вскрытия защитного кожуха, общий мониторинг оборудования связи (проверка фактической работоспособности в заданном диапазоне настроек);

- Еженедельный осмотр. Действия проводятся над аппаратурой, которая работает в непрерывном режиме или с прерыванием более 24 часов. В комплекс работ не только входят все действия из предыдущего пункта, но и целый ряд дополнительных процедур – осмотр и чистка контактов, проверка аппаратуры на работоспособность во всех режимах при помощи специальной контрольно-измерительной аппаратуры;

- Квартальное обслуживание. Обязательная процедура для всех устройств связи вне зависимости от режима их функционирования и длительности непрерывной работы. Кроме проведения регламентного еженедельного ТО проводится полная проверка оборудования связи на работоспособность во всех диапазонах, проверка антенн, контактов и соединительных узлов. Дополнительно производится чистка аппаратуры и замена вышедших из строя элементов, которые обнаружены в ходе проверки;

- Сезонные мероприятия. Выполнение регламентных работ касается всего оборудования, включая резервные системы и аппаратуру, которая хранится на складе. В комплекс мероприятий входят не только работы, описанные в предыдущем пункте, но и дополнительные процедуры – замена неисправных элементов, проверка резервных цепей связи, доукомплектация складского оборудования, контроль над ведением отчетной документации.

Все регламентные работы обязательно заносятся в специальный журнал (бланк) с указанием вида ТО и данных лиц, ответственных за проведение регулярных профилактических работ.

В случае обнаружения неисправности, уполномоченные специалисты производят ремонтные или восстановительные работы.

Оборудование для ремонта аппаратов связи – это специальный инструмент и контрольно-проверочная аппаратура, которая позволяет производить полный комплекс профильных работ любого уровня сложности.

Правильный монтаж и обслуживание оборудования связи – гарантия безопасной и стабильной работы.

Чтобы свести к минимуму возникновение поломок в оборудовании связи, необходимо учесть несколько критериев:

- сертификация оборудования связи. Перед покупкой аппаратуры убедитесь, что она соответствует всем указанным требованиям и прошла обязательную проверку согласно нормативным документам;
- эксплуатация в соответствии с регламентом;
- регулярное проведение технического обслуживания;
- правильная установка аппаратуры.

Монтаж оборудования связи является технически сложным процессом, который выполняют специалисты. Вне зависимости от объема работ, необходимо не только правильно расположить и соединить все блоки, произвести заземление оборудования связи и подготовить всю систему к пробному запуску.

Чтобы узнать больше о регламентах технической проверки, монтажных и ремонтных работах, техническом обслуживании оборудовании для связи, а также увидеть новейшие технологические отраслевые достижения и современные системы связи, достаточно посетить профильную выставку «Связь». Масштабная экспозиция будет располагаться на территории ЦВК «Экспоцентр».

Техническая эксплуатация станций представляет собой комплекс организационных и технических мероприятий по поддержанию аппаратно-программного комплекса станции в состоянии, при котором обеспечивается обслуживание вызовов с заданным качеством при передаче любых видов сообщений, для которых данная станция предназначена.

Основными задачами технической эксплуатации телефонных станций являются:

- обеспечение бесперебойной, эффективной и высококачественной работы телефонных станций;
- поддержание в норме электрических характеристик оборудования коммутации;
- поддержание в норме электрических характеристик каналов;
- поддержание безошибочной работы программного обеспечения телефонной станции;

- организация эффективной работы технического персонала, отвечающего за техническую эксплуатацию станции; проведение мероприятий по развитию и модернизации станций.

Техническая эксплуатация цифровых телефонных станций включает:

- техническое обслуживание и ремонт оборудования телефонных станций;
- контроль за нагрузкой и качеством работы оборудования телефонных станций и включенных в них каналов и линий;
- техническое обслуживание и поддержку программного обеспечения (ПО) телефонных станций;
- работы по развитию телефонных станций и их модернизации;
- техническое оснащение телефонных станций;
- поддержку телефонных станций со стороны поставщика или сервисных центров технического обслуживания;
- организацию работы технического персонала;
- ведение документации, учет и порядок отчетности;
- содержание технических помещений;
- соблюдение правил техники безопасности и охраны труда.

Основным документом, определяющим принципы организации технической эксплуатации цифровых телефонных станций, выполнение которых является обязательным для технического персонала, обслуживающего данные станции - являются «Правила Технической эксплуатации цифровых телефонных станций сети электросвязи».

Для нормальной работы цифровой коммутационной системы с программным управлением должны быть обеспечены надлежащая эксплуатация и высококачественное техническое обслуживание, что в основном включает в себя следующее.

Ежедневные операции по обработке услуг: добавление, удаление и изменение записей об абонентах; регистрация и удаление таких данных, как предоставление дополнительных услуг и полномочий на прямой набор номера, тестирование и диагностика совместно с консолью измерения; периодический сбор и анализ статистики трафика; периодический вывод тарификационных таблиц и счетов; составление отчетов и анализ данных о работе оборудования.

Регламентное техобслуживание и техобслуживание системного уровня, включая работы по приведению оборудования в порядок, регламентное и профилактическое тестирование.

Анализ аварийных сигналов и отказов, диагностика и устранение неисправностей, замена плат.

Управление данными, в том числе: резервирование, отладка и корректировка абонентских данных, станционных данных, тарификационных данных, промежуточных данных и программ.

Расширение системы, установление новых маршрутов и модификация в соответствии с требованиями, возникающими при развитии услуг связи, изменении структуры сети и местных условий.

Использование потенциальных возможностей оборудования и программного обеспечения прикладного уровня, реализация дополнительных услуг, обновление аппаратных средств для обеспечения научно обоснованных, современных методов управления оборудованием SPC.

Средства и оборудование технического обслуживания и эксплуатации

Существуют три метода выполнения операций технического обслуживания и эксплуатации:

• Аппаратный метод;

• Комбирированный аппаратно-программный метод;

• Программный метод;

Средства технического обслуживания и эксплуатации:

• Интеллектуальные платы;

• Специальные тестовые платы;

• Оборудование аварийной сигнализации (например, блок аварийной сигнализации);

• Программные средства техобслуживания и эксплуатации, включая систему мониторинга и систему управления данными;

• Терминал и программное обеспечение техобслуживания и эксплуатации.

Общая процедура техобслуживания и эксплуатации

Все устройства в цифровой коммутационной системе с программным управлением C&C08 можно разделить на пять категорий: оборудование управления, оборудование сигнализации, сетевое оборудование, терминальное оборудование и оборудование техобслуживания. Для техобслуживания вышеупомянутого оборудования существуют различные методы и процессы, описание которых приводится ниже.

Оборудование управления

Все оборудование управления функционирует в режиме «активный/резервный», при котором осуществляется точный поиск неисправностей средствами диагностики, после чего происходит переключение с активного оборудования на резервное и перераспределение нагрузки.

Общий процесс технического обслуживания оборудования выглядит следующим образом:

Когда программа обработки неисправностей обнаруживает отказ оборудования, резервное устройство автоматически переводится в активное состояние, после чего выполняется переключение «активный/резервный» и перераспределение нагрузки, а также производится плавное переключение процессов обработки.

Автономные сообщения и другая информация об авариях передаются на терминал и в другие устройства аварийной сигнализации. Результат диагностики и информация о местоположении неисправной платы в случае необходимости могут распечатаны.

Персонал технического обслуживания заменяет неисправное устройство новым и проверяет правильность работы оборудования.

Отчеты о рабочем состоянии оборудования и автономные сообщения просматриваются и документируются.

Неисправный блок посылается в центр технического обслуживания или изготовителю.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1 Бакаева Н.В., Чикулаева В.В. Технологическое оборудование для технического обслуживания автомобилей: Учебное пособие. - Орёл: Изд. Орёл, 2007.

2 Пескин, А.Е. Бытовая радиоэлектронная аппаратура. Устройство, техническое обслуживание, ремонт / А.Е. Пескин, Г.С. Гендин и др. - М.: Горячая линия-Телеком , 2014.

ӘӨЖ 355.583

COMMON ALERT PROTOCOL ЖАЛПЫ ҚҰЛАҚТАНДЫРУ ХАТТАМАСЫН ІСКЕ АСЫРУ ЖӨНІНДЕГІ ХАЛЫҚАРАЛЫҚ ТӘЖІРИБЕ

САҒЫМБАЙ А.С., *оқытушы, аға лейтенант*

ҚР ТЖМ М. Ғабдуллин атындағы Азаматтық қорғау академиясы,
Қазақстан Республикасы, Көкшетау қаласы

Аннотация: мақала халықты төтенше жағдайлар туралы құлақтандыру мәселелерін қарастыруға, қауіпті ескертулердің барлық түрлерін автоматты түрде жинау және қайта таратудың стандартты әдісін әзірлеуге арналған. Автормен жұмыста жалпы құлақтандыру хаттамасын құру және іске асыру тарихы талданды.

Түйін сөздер: төтенше жағдай; құлақтандыру жүйесі; құлақтандырудың техникалық құралы; құлақтандыру жүйелерін біріктіру; ақпарат алмасу хаттамалары; Common Alert Protocol жалпы құлақтандыру хаттамасы; төтенше жағдайлар туралы алдын ала құлақтандыру.

Табиғи және техногендік сипаттағы төтенше жағдайлар туындаған кезде апатқа тиімді қарсы тұруға, халықтың жаппай қаза болуын мен инфекциялық індеттерді жұқтырмауына жол бермеудің маңызды шарты, апат аймағындағы мемлекеттік органдарды, халықты және ұйымдарды уақытылы ақпараттандыру және хабардар ету болып табылады. Адами және материалдық шығындарды азайту бойынша шұғыл шараларды қамтамасыз етуге қабілетті құрал - төтенше жағдайлар қаупі төнген және туындаған кезде жақсы ұйымдастырылған орталықтандырылған мемлекеттік құлақтандыру жүйесінің болуы. Қазақстан Республикасында мемлекеттік және облыстық деңгейдегі құлақтандыру жүйесі қазіргі күйінде өткен ғасырдың 70-жылдарында пайдалануға берілді. Ол сымды байланыс арналары арқылы жұмыс істейтін аналогтық аппаратура негізінде салынған. Соңғы жаңғырту 90-шы жылдардың басында жүргізілді, оның барысында блоктар мен тораптар ішінара ауыстырылды [1]. Бастапқыда бейбіт және соғыс уақытында ірі қалалар мен өнеркәсіп объектілеріне қызмет көрсетуге арналған қолданыстағы құлақтандыру жүйесі ауылдық елді мекендердің басым көпшілігін қамтымайды. Объективті себептерге байланысты қолданыстағы құлақтандыру жүйесінің функционалдық мүмкіндіктері уақыт өте келе қысқарады. Мысалы, бұрын халықты құлақтандыру жүйесінің негізін құрайтын сымды радиохабар тарату жүйелері қазіргі уақытта жұмыс істемейді. Қазақстан Республикасы ТЖМ телефон және телеграф арналарының қолданыстағы аналогтық беру жүйелері мен коммутацияланатын құрылғылары ақпаратты цифрлық өңдеу және беру технологиясы пайдаланылатын республикалық байланыс желілері бойынша деректерді берудің талап етілетін параметрлерін қамтамасыз ете алмайды.

Басқару органдары мен халықты хабардар етудің қолданыстағы жүйесі тарихи тұрғыдан ескіргені, бейбіт және соғыс уақытында төтенше жағдайлардың алдын алу жөніндегі іс-шараларды одан әрі жетілдіруге кедергі болғаны анық.

Әлемде қазіргі заманғы технологиялар негізінде халықты құлақтандыру жүйелерін құрудың елеулі тәжірибесі жинақталған, оның бағыттарының бірі ұялы телефон байланыс желілері бойынша циркулярлық хабар тарату технологиясына негізделген құлақтандыру жүйелерін салуға кешенді көзқарас болып табылады

Бұл мәселені толық түсіну үшін, әлемнің көптеген елдерінде қабылданған бірыңғай құлақтандыру хаттамасын іске асырудың халықаралық тәжірибесін қарастырамыз.

Құлақтандыруға бірыңғай көзқарастың қажеттілігі туралы алғаш рет 2000 жылдың қарашасында АҚШ Ұлттық ғылыми-техникалық кеңесі (NSTC) шығарған «Апаттар туралы тиімді құлақтандыру» есебінде айтылды. Баяндамада жергілікті, аймақтық және Ұлттық деңгейлердегі қауіп кезіндегі құлақтандыру мен есептердің барлық түрлерін жедел және автоматты түрде жинау және қайта тарату үшін стандартты әдісті әзірлеу қажеттілігі туралы ұсыныс жасалды. Осылайша жалпы құлақтандыру хаттамасын құру міндеті пайда болды – Common Alerting Protocol (бұдан әрі – CAP хаттамасы) [2].

Бірқатар халықаралық құлақтандыру жүйелерін қамтитын коммерциялық CAP хаттамасы сынақтан өтті және оны NSTC ұсыныстарын ескере отырып одан әрі жетілдіруі жүргізілді және оны 2004 жылы қауіпсіздік стандарттарын, соның ішінде төтенше жағдайларды (OASIS) одан әрі ресімдеу үшін әзірлейтін құрылымдық ақпарат стандарттарын ілгерілету ұйымымен қабылданды [3].

Жалпы CAP хаттамасы – бұл әртүрлі алдын ала ескерту технологиялары арасында қоғамдық төтенше жағдай туралы ескертулерді бөлісуге арналған XML спецификациясының деректер форматы. Бұл табиғи немесе техногендік сипаттағы төтенше жағдайдың туындау мүмкіндігі немесе орын алуы туралы ескертетін хабарламаны ауа-райы және қауіпсіздік туралы ескерту сайты (Google Public Alerts) және ұялы хабар тарату (Cell Broadcast) сияқты көптеген ескерту жүйелерінде бір уақытта дәйекті түрде таратуға мүмкіндік береді. Стандартталған ескерту ақпаратының форматтары төтенше жағдайлардың ықтимал көздері туралы деректерді алуға және олардың пайда болу қаупіне жауап беру үшін қолданбаларды теңшеуге мүмкіндік береді. Осылайша, ескерту ақпаратын Ұлттық қауіпсіздік департаментінен, Америка Құрама Штаттарының геологиялық қызметінен, Ішкі істер департаментінен, Ұлттық мұхиттық және атмосфералық зерттеу басқармасынан (NOAA) және АҚШ Сауда министрлігінен, сондай-ақ мемлекеттік және жергілікті мемлекеттік органдардан бірдей форматта алуға болады. Мысалы, алынған бір ақпарат негізінде әртүрлі дабыл сигналдарын беруге болады, бұл ескертуге шешім қабылдайтын жауапты тұлғалар үшін хабардар ету тапсырмасын жеңілдетеді және азаматтардың құлақтандырылуына кепілдік береді.

Хабарландыру деректерін қауіптер, юрисдикциялар және құлақтандыру жүйелері бойынша жіктеу арқылы CAP төтенше жағдайларды анықтау үшін пайдаланылуы мүмкін. Процедуралық тұрғыдан CAP арнайы ескерту хабарламаларын жасайды.

Америка Құрама Штаттарының ауа-райы радиостанцияларының тәулік бойы жұмыс істейтін желісі ауа-райы туралы ақпаратты жақын маңдағы ұлттық ауа райы қызметінің кеңсесінен (NOAA Weather Radio) тікелей жібереді. Бұл желі АҚШ-тың автоматтандырылған төтенше жағдай туралы құлақтандыру жүйесінде қолданылады. Ол сандық радиостанциялар желісінде салынған және ұялы телефон түріндегі мобильді құрылғыларға (Wireless Emergency Alerts, WEA) апаттық ескертулерді таратуға арналған. NOAA Weather Radio жүйесінің артықшылығы – ендік/бойлық «қораптарды» және басқа геокеңістіктікті көріністерді үш өлшемде қолдана отырып, икемді географиялық мақсат қою. Жүйе аудио және бейне сандық кескіндерді, цифрлық шифрлауды және қолтаңбаны жіберуге мүмкіндік береді; хабарламаларды жаңарту мен жоюдың кеңейтілген көп тілді және көп тапсырмалы мүмкіндіктерімен толық және тиімді ескерту хабарламаларын жасауға арналған шаблондарды қолдайды.

CAP деректер құрылымы NOAA Weather Radio жүйесінің хабарлама форматтарымен, соның ішінде төтенше жағдай туындауы мүмкін белгілі бір аумаққа кодтаумен үйлесімді. Сондықтан CAP хаттамасы WEA-да алғашқылардың бірі болып кеңінен қолданылды.

CAP 1.0 протоколының бірінші нұсқасын OASIS 2004 жылдың сәуірінде мақұлдады. CAP 1.0 пайдалану тәжірибесіне сүйене отырып, 2005 жылдың қазан айында OASIS төтенше жағдайларды басқару техникалық комитеті CAP 1.1 жаңа нұсқасын қабылдады. 2006 жылдың қазан айында Женевада өткен жиналыста Cap 1.1 хаттамасын халықаралық электробайланыс Одағының стандарттау секторы жалпы құлақтандыру хаттамасы ретінде қабылдау үшін қарастырылдыды.

2007 жылы Халықаралық электробайланыс Одағының стандарттау секторы ASN Модулінің аудармасын қамтитын қосымшасы бар CAP хаттамасын қабылдады.1 XML CAP схемалары, бүкіл әлемде қолдануға ұсынылған.

Осылайша, 2008 жылдан бастап халықты төтенше жағдайлар туралы алдын ала ескертуге арналған мемлекеттік және қоғамдық ұйымдар өздерінің юрисдикцияларында Cap жалпы ескерту хаттамасын енгізе бастады. АҚШ. 2010 жылдың 30 қыркүйегінде Федералды Төтенше жағдайлар агенттігі (FEMA) [4] ұзақ тестілеуден, келісуден және талқылаудан кейін CAP әр түрлі платформалар, соның ішінде тарату құралдары, сымсыз байланыс құрылғылары арқылы апаттық хабарламаларды таратуға арналған жаңа интеграцияланған халыққты хабардар ету және құлақтандыру жүйесінің (IPAWS) хаттамасы ретінде ресми түрде қабылданды.

Австралия. CAP негізінде Австралия үкіметі өзінің құлақтандыру стандартын жасады (CAP o-std 2012). Австралияның Төтенше жағдайлар департаменті федералды басқару органдарын, сондай-ақ ауыл шаруашылығы,

балық шаруашылығы және орман шаруашылығы департаментін, Денсаулық сақтау департаментін, Метеорология, жер туралы ғылымдар бюросын қамтитын бірқатар мемлекеттік органдар мен төтенше жағдайлар қызметтерінен тұратын топ құрды [5].

Канада. Канадада CAP-CP жалпы құлақтандыру хаттамасының нұсқасын жұмыс тобы әзірледі, оның құрамына қоғамдық хабарлау мамандары, сондай-ақ мемлекеттік органдардың өкілдері кірді. Канадалық нұсқаның негізі CAP болды, бірақ ол канадалық қоғамдық құлақтандыру талаптарына сәйкес келтірілді. Атап айтқанда, екі тілділік, геокодтау, басқарылатын орындар мен оқиғалар тізімдері енгізілді. Нәтижесінде 2015 жылдың наурыз айында CAP-CP-ге негізделген Alert Ready ұлттық қоғамдық құлақтандыру жүйесі ресми түрде іске қосылды. Ұлттық құлақтандыру жүйесіне елдің барлық хабар таратушылары мен телевизиялық провайдерлері қатысады. Сонымен қатар, Канаданың халықаралық даму ғылыми орталығы «HazInfo» жобасының құрамдас бөлігі болған жергілікті деңгейдегі қауіп туралы ақпараттық жүйені іске асыру үшін CAP қолданды [6].

Германия. 1992 жылы Федералды үкімет пен жер үкіметтері халықты орнатылған 100000-ге жуық сиреналармен емес, телерадиохабарлаумен ескертуге келісті.

2001 жылы АҚШ-пен бір мезгілде Германияның азаматтарды қорғау және апаттар кезінде қолдау Федералды басқармасы (BBK) Cap 1.2 жалпы құлақтандыру хаттамасы негізінде Ұлттық модульдік құлақтандыру жүйесін құра бастады, бұл Германия тұрғындарын төтенше жағдайлар туралы ескерту және азаматтық қорғау шараларын қабылдау үшін BBK ақпаратына интернет арқылы қол жеткізуге мүмкіндік береді. Бұл жүйе федералды Штаттарға апаттар туралы алдын ала ескерту үшін де қол жетімді. Жаңа құлақтандыру жүйесін қолдана отырып, BBK, Германияның федералды және штаттық билігі хабарламалар құрып, оларды бұқаралық ақпарат құралдары арқылы халыққа жеткізе алады.

Бұл жүйе спутниктік хабар тарату желісін қолдана отырып жұмыс істейді және 150-ден астам мемлекеттік және медиа құрылымдарға төтенше жағдайлар туралы ақпарат береді. Бірақ халыққа жақын жерде хабар тарату қабылдағыштары болмаған жағдайда, оның тиімділігі айтарлықтай шектеледі, өйткені көптеген сиреналар бұл жүйеге қосылмаған немесе қызмет көрсетілмеген. Ұлттық модульдік төтенше жағдайлар кезінде құлақтандыру жүйесіндегі CAP мүмкіндіктерін кеңейту барлық ықтимал құлақтандыру құралдарын, соның ішінде сиреналарды қосу мәселесін шешуге ықпал етуі керек.

Италия. Италияның Ішкі істер министрлігінің өрт сөндірушілер, қоғамдық құтқарушылар және азаматтық қорғаныс департаменті 2008 және 2011 жылдардағы екі министрлік Жарлығымен CAP хаттамасын қабылдады [6]. Жарлықтарға сәйкес, ауқымды төтенше жағдайлар немесе құтқару жұмыстары кезінде өрт сөндіру корпусымен байланысқысы келетін Италиядағы кез келген төтенше жағдайға қатысушы CAP хаттамасын қабылдауы керек.

CAP хаттамасы алғаш рет 2009 жылы Орталық Италияның жер сілкінісінен кейін іске қосылды. Содан кейін төтенше жағдайлар департаменттерінің қызметкерлері ескерткіштер мен тарихи ғимараттарды қорғау бойынша уақытша шараларды әзірлеу және жүзеге асыру кезінде Мәдени мұра министрлігімен үйлестірді. Бүгінгі күні осы хаттаманы қолданатын жүйе күн сайын нақты уақыт режимінде жұмыс істейді. Ұлттық басқару орталығы, провинциялық және аймақтық диспетчерлік қызметтер төтенше жағдайлардың алдын алу мен жоюға, сондай-ақ құтқару жұмыстарын жүргізуге қатысты мыңдаған хабарламалар жібереді [7].

Тайвань. АҚШ пен Жапонияның тәжірибесіне сүйене отырып, Тайваньдағы төтенше жағдай туралы құлақтандыру жүйесі АҚШ-тағы IPAWS-пен бірдей CAP хаттамасының нұсқасын қабылдады, бірақ сонымен бірге Тайваньда негізінен, Жапонияда халықты төтенше жағдайдың алдын алу туралы хабардар ету үшін қолданылғанға ұқсас, бірнеше ұялы телефон пайдаланушыларына хабарлама жіберу әдісі қолданылады (Cell Broadcast Entity) [8].

Тайвань Үкіметі елдегі халықты ескерту саясатын жүзеге асыру үшін апаттардың алдын алу жөніндегі орталық кеңсені және ден қою кеңсесін (CDPR) анықтағанымен, қазіргі уақытта апаттар туралы ескертулерді шығаруға жауапты жеті орталық агенттік бар.

2016 жылдың мамырынан бастап Тайваньның Орталық ауа-райы бюросы аралда және оның айналасында 4,5-тен астам жер сілкінісі туралы ескертулер шығара бастады. Алайда, халық шұғыл хабарламаларды жеткізуге байланысты мәселелерге шағымданады, олар тым кеш келуі немесе мүлдем келмеуі мүмкін. Тұтастай алғанда, Тайвань соңғы жылдары халықты шұғыл ескерту үшін ұялы хабар тарату қызметтерін (CBS) дамытуда біраз жетістіктерге жетті, бірақ ұйымдастырушылық және техникалық сипаттағы көптеген кемшіліктер бар. Тайваньдағы төтенше жағдай туралы ақпартаттандыру ауа-райы туралы хабарламалармен шектеледі, ал АҚШ-тағы IPAWS халықты табиғи және техногендік сипаттағы кез-келген төтенше жағдайлар туралы ескертеді.

Қорытындылай келе, қазіргі уақытта CAP жалпы құлақтандыру хаттамасы кең таралған және әлемнің көптеген елдерінде кеңінен қолданылады. Алайда, жағымды жақтарын зерттей отырып, оны қолдану тәжірибесімен белгіленген кемшіліктерге назар аудару қажет. Ескерту ақпаратын көптеген мемлекеттік органдар, министрліктер мен ведомстволар, өкілетті ұйымдар енгізе алады, көбінесе оны алу көздерінің дұрыстығын тексерусіз, бұл халықтың дүрбелеңі мен жағымсыз көңіл-күйін тудыруы мүмкін. Әлемнің көптеген елдерінде АҚШ-қа ұқсас халықты құлақтандыруды ұйымдастыруға көзқарас бар; CAP хаттамасы әртүрлі министрліктер, ведомстволар мен ұйымдардың әртүрлі ескерту орталықтары мен пункттерінен басқарылатын ықтимал немесе туындаған төтенше жағдайлар туралы алдын ала ескертудің әртүрлі ақпарат ағындарын біріктіреді.

Біздің елімізде халықты хабардар ету жүйелері орталықтандырылған, ақпараттық алмасудың бірыңғай хаттамасын әзірлеу шын мәнінде қажет, бірақ

оның мақсаты – Қазақстан Республикасының аумағында халықты хабардар етудің қолданыстағы жүйелерінің бірыңғай ақпараттық кеңістікте жұмыс істеуін ұйымдастыруды қамтамасыз ету және оларды орталықтандырылған басқаруды жүзеге асыру. Халықты құлақтандырудың техникалық құралдарын ақпараттық алмасудың бірыңғай хаттамасын енгізу құлақтандырудың техникалық құралдарының бәсекеге қабілеттілігін арттыруға мүмкіндік береді.

ПАЙДАЛАНЫЛҒАН ӘДЕБИЕТТЕР ТІЗІМІ

1 Божко В.К. ТЖ Министірінің Қазақстан Республикасы Үкіметінің отырысында сөйлеген сөзі, 11 қыркүйек 2012 жыл.

2 Common alerting protocol (CAP 1.1) [Электрондық ресурс] // URL: https://www.dhs.gov/sites/default/files/publications/AlertProtocol-TG_0215–508.pdf.

3 OASIS [Электрондық ресурс] // URL: http://www.oasis-open.org/ committees/download.php/14759/emergency-CAPv1.1.pdf.

4 FEMA EASY Cap стандарты үшін сандық хабарлама форматын қабылдайды [Электрондық ресурс] // URL: https://www.fema.gov.

5 CAP-AU-STD v.3.0 Specification documents, and... [Электрондық ресурс] // Сайт Australian Government. URL: https://data.gov.au/ data/dataset/cap-au-std/resource/5f96bf8e-b167-4258-9127- 4f0206f3f223.

6 Соңғы мильдегі қауіп туралы ақпараттың таралуын бағалау (HazInfo) [Электрондық ресурс] // URL: http:// www.lirneasia.net/projects/current-projects/evaluating-last-milehazard-information-dissemination-hazinfo.

7 Өрт сөндірушілер, қоғамдық құтқарушылар және азаматтық қорғаныс департаменті (Dipartimento dei Vigili del Fuoco, del Soccorso Pubblico e della Difesa Civile) [Электрондық ресурс] // URL: http://www.vigilfuoco.it/aspx/home.aspx.

8 Ssu-Ming Chang. Disaster Public Warning System in Taiwan [Электрондық ресурс] // URL: https://www.aspanet.org/ ASPADocs/Annual%20Conference/2018/Papers/ChangSsuMing. Pdf.

УДК 623.61

ОПРЕДЕЛЕНИЕ ПОЗИЦИИ С ПОМОЩЬЮ СИГНАЛОВ WI-FI

КАЛИАСКАРОВ Н.Б., *доктор PhD, заведующий кафедрой ТСС*
ГАВРИЛОВА М.А., *магистр, старший преподаватель*
ЖАНТУГАНОВА Т.С., *магистр, ассистент*
БАКИРОВ Э.В., *студент группы РЭТ-21-2*

НАО Карагандинский технический университет имени Абылкаса Сагинова,
г. Караганда, Республика Казахстан

Аннотация: В современных условиях технологического развития военные структуры всегда ищут новые подходы и технологии для обеспечения безопасности и эффективности военных операций. Одной из ключевых областей, требующей постоянного развития и совершенствования, является компьютерное зрение, которое находит применение в различных сферах, включая наблюдение, распознавание действий и игровые технологии. Оценка человеческой позы играет важную роль в этой области, определяя положение суставов и ключевых точек на туловище и голове. Однако, как и в любой задаче распознавания на основе камеры, проблемой остается возможность окклюзии, особенно в военных сценариях, где обнаружение и отслеживание целей могут затрудняться из-за стен, препятствий или других видов маскировки.

Ключевые слова: радиочастотные сигналы, Wi-Fi, RF-Pose, радио, радиочастотные отражения, дальность сигнала.

В данной работе представлен фундаментально новый подход к решению проблемы окклюзии в оценке позы человека с использованием радиочастотных (RF) сигналов. В отличие от видимого света, который может быть заблокирован стенами и непрозрачными объектами, радиочастотные сигналы в диапазоне Wi-Fi могут преодолевать такие преграды и даже отражаться от человеческого тела, что открывает возможности для отслеживания людей сквозь стены. Последние достижения в области беспроводных систем использовали эти свойства для обнаружения людей и отслеживания их скорости ходьбы сквозь окклюзии. Однако существующие системы ограничены: либо отслеживают только одну конечность в любой момент времени, либо создают статическое и грубое описание тела, где части тела, наблюдаемые в разные моменты времени, схлопываются в один кадр [1,2].

Представленный в тезисе подход, названный RF-Pose, основан на нейронных сетях, которые анализируют беспроводные сигналы и извлекают точные двумерные позы человека, даже когда они находятся за стеной или полностью скрыты от визуального наблюдения. RF-Pose передает сигналы с низкой мощностью (в 1000 раз меньше, чем у Wi-Fi) и наблюдает их отражения от окружающей среды. Используя только радиоотражения в качестве входных

данных, он оценивает скелет человека. Этот подход позволяет отслеживать человека даже в тех случаях, когда он полностью скрыт за стеной.

Система оценки позы на основе радиочастот использует передачу слабого радиочастотного сигнала и прием его отражений. Для разделения радиочастотных отражений от различных объектов обычно используются техники, такие как FMCW (Frequency Modulated Continuous Wave) и антенные решетки [3]. FMCW разделяет радиочастотные отражения на основе расстояния отражающего объекта, в то время как антенные решетки разделяют отражения на основе их пространственного направления. В данной работе обозревается радио, которое генерирует сигнал FMCW и имеет две антенные решетки: вертикальную и горизонтальную (другие радио также доступны). Таким образом, входные данные имеют форму двумерных изображений тепловых карт, одну для каждой из горизонтальной и вертикальной антенных решеток. Как показано на рисунке 1, горизонтальная тепловая карта является проекцией отражений сигнала на плоскость параллельную земле, в то время как вертикальная тепловая карта является проекцией отраженных сигналов на плоскость перпендикулярную земле (красный цвет соответствует большим значениям, а синий - малым значениям).

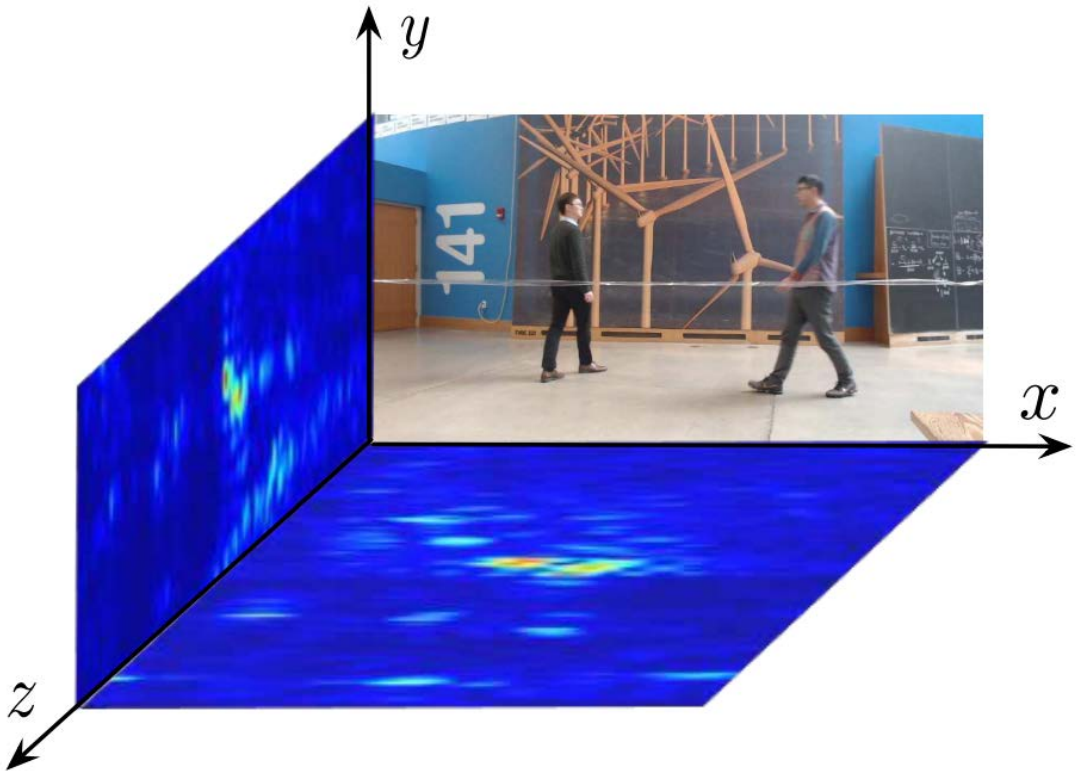


Рисунок 1 – Тепловая карта и фото

Следует отметить, что поскольку радиочастотные сигналы являются комплексными числами, каждый пиксель на этой карте имеет действительную и мнимую компоненты. Используемое радио генерирует 30 пар тепловых карт в секунду.

Важно отметить, что радиочастотные сигналы обладают внутренне

различными свойствами по сравнению с визуальными данными, то есть пикселями камеры.

Во-первых, радиочастотные сигналы в частотах, которые проникают сквозь стены, имеют низкое пространственное разрешение, гораздо ниже, чем у визуальных данных. Разрешение обычно составляет десятки сантиметров, и определяется шириной полосы пропускания сигнала FMCW и апертурой антенной решетки. В частности, данное радио имеет разрешение глубины около 10 см, и его антенные решетки имеют вертикальное и горизонтальное угловое разрешение 15 градусов.

Во-вторых, человеческое тело является зеркальным при частотах, которые проникают сквозь стены. Радиочастотная зеркальность – это физическое явление, которое проявляется, когда длина волны больше шероховатости поверхности. В этом случае объект действует как отражатель, а не как рассеиватель. Длина волны радио составляет около 5 см, поэтому люди действуют как отражатели. В зависимости от ориентации поверхности каждой конечности сигнал может отражаться к датчику или от него. Таким образом, в отличие от систем камер, где любой снимок показывает все незакрытые ключевые точки, в радиосистемах один снимок содержит информацию о подмножестве конечностей и упущенных конечностях и частях тела, чья ориентация в данный момент отклоняет сигнал от датчика.

В-третьих, беспроводные данные имеют другое представление (комплексные числа) и разные перспективы (горизонтальные и вертикальные проекции) относительно камеры.

Эти свойства имеют значение для оценки позы и должны быть учтены при разработке нейронной сети для извлечения поз из радиочастотных сигналов.

Модель, изображенная на рисунке 2, реализует подход "учитель-ученик". В верхнем конвейере на рисунке показана сеть-учитель, которая обеспечивает перекрестное модальное обучение; в нижнем конвейере показана сеть-ученик, которая выполняет оценку позы на основе радиочастот [4].

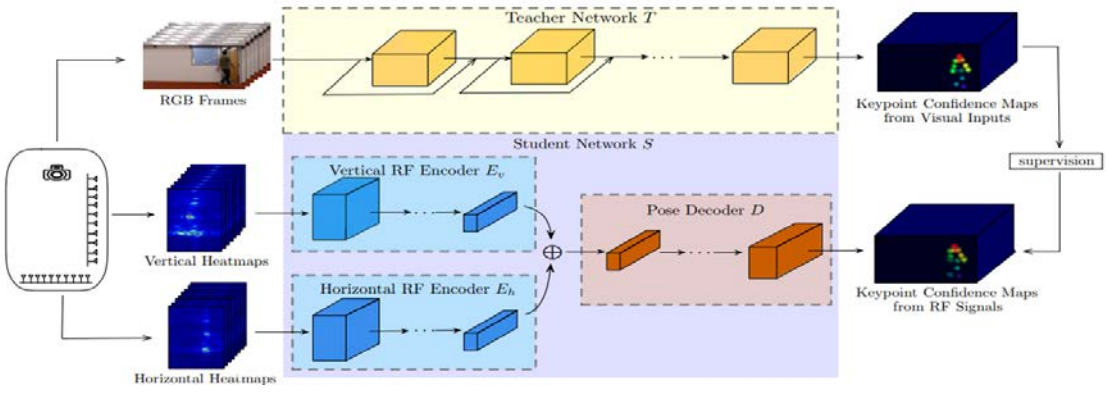


Рисунок 2 – Модель сети «учитель-ученик», используемая в RF-Pose. В верхнем конвейере осуществляется обучение с учителем, в то время как нижний конвейер обучается извлекать позу человека, используя только тепловые карты радиочастот

RF-Pose использует радиочастотные сигналы для вывода позы человека сквозь окклюзии. Однако радиочастотные сигналы и решение, которое мы представляем здесь, имеют некоторые ограничения: во-первых, человеческое тело непрозрачно на интересующих нас частотах - то есть на частотах, которые проникают сквозь стены. Следовательно, окклюзия между людьми является ограничением текущей системы. Во-вторых, рабочее расстояние радио зависит от его мощности передачи. Радио, которое используется в этой статье, работает на расстояние до 40 футов. Наконец, продемонстрировано, что извлеченная поза захватывает идентифицирующие особенности человеческого тела. Однако эксперименты, проведенные по идентификации, рассматривают только одну активность: ходьбу. Исследование более сложных моделей и идентификация людей в естественной среде во время выполнения повседневных действий, кроме ходьбы, остается на будущее.

Однако эта технология хоть и имеет невероятный потенциал, нуждается в ряде улучшений. Таких как:

- увеличение дальности действия: Расширение рабочего расстояния радио может быть критически важным для военных операций. Это может быть достигнуто увеличением мощности передатчика, улучшением антенных систем или использованием более эффективных алгоритмов обработки сигналов.
- повышение точности и разрешения: Увеличение точности и пространственного разрешения технологии поможет лучше обнаруживать и отслеживать цели, особенно в условиях ограниченной видимости или при наличии маскировки.
- диверсификация действий: Расширение спектра действий, которые могут быть идентифицированы и отслежены с использованием этой технологии, включая не только ходьбу, но и другие важные военные действия, такие как бег, ползание, переноска грузов и использование оружия.
- преодоление окклюзии: Разработка методов преодоления окклюзии между людьми и другими объектами, например, путем анализа отраженных сигналов с различных ракурсов или использования более сложных алгоритмов обработки данных.
- улучшение безопасности и конфиденциальности: Разработка методов защиты данных от перехвата или вмешательства вражеской стороной, а также обеспечение безопасного и конфиденциального обмена информацией между различными узлами системы.
- интеграция с другими сенсорами: Использование данных от радиочастотных сенсоров в комбинации с данными от других типов сенсоров, таких как оптические, инфракрасные или акустические, может повысить общую эффективность и надежность системы наблюдения и обнаружения военных целей.
- адаптация к различным условиям боевых действий: Учет разнообразных условий боевых действий, включая разные типы местности, погодные условия и характеристики противника, для разработки адаптивных алгоритмов и стратегий использования технологии.

В заключение, можно отметить, что технология оценки позы на основе радиочастотных сигналов, хотя и демонстрирует значительные потенциальные преимущества для использования в военных целях, все еще находится в стадии развития и требует дальнейших исследований и разработок. Несмотря на ограничения, такие как ограниченное рабочее расстояние, низкое пространственное разрешение и ограничения в идентификации действий, эта технология имеет огромный потенциал для применения в армии.

Дальнейшие усилия в области исследований и разработок должны быть направлены на улучшение точности, дальности действия и функциональности системы, а также на адаптацию её к различным условиям военных действий. Необходимо также разработать стратегии по преодолению ограничений, таких как окклюзия и ограничения в идентификации действий, чтобы обеспечить более полное и надежное использование технологии на поле боя.

В целом, несмотря на текущие ограничения, технология оценки позы на основе радиочастотных сигналов обещает стать важным инструментом для улучшения военной безопасности, обнаружения и отслеживания целей, и она заслуживает дальнейшего внимания и инвестиций со стороны военных и исследовательских организаций.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1 T. Pfister, J. Charles, and A. Zisserman. Flowing convnets for human pose estimation in videos. In Proceedings of the IEEE International Conference on Computer Vision, ICCV, 2015.

2 A. Newell and J. Deng. Associative embedding: End-toend learning for joint detection and grouping. arXiv preprint arXiv:1611.05424, 2016.

3 F. Adib, C.-Y. Hsu, H. Mao, D. Katabi, and F. Durand. Capturing the human figure through a wall. ACM Transactions on Graphics, 34(6):219, November 2015.

4 M. Andriluka, L. Pishchulin, P. Gehler, and B. Schiele. 2D human pose estimation: New benchmark and state of the art analysis. In Proceedings of the IEEE Conference on computer Vision and Pattern Recognition, 2014.

5 «Through-Wall Human Pose Estimation Using Radio Signals» Mingmin Zhao, Tianhong Li, Mohammad Abu Alsheikh, Yonglong Tian, Hang Zhao, Antonio Torralba, Dina Katabi.

УДК 621.396

УДАЛЕННЫЙ МОНИТОРИНГ ТЕХНИЧЕСКОГО СОСТОЯНИЯ ВОЕННЫХ ОБЪЕКТОВ С ИСПОЛЬЗОВАНИЕМ ВОЗМОЖНОСТЕЙ НАЦИОНАЛЬНОЙ СИСТЕМЫ ВОЕННОЙ РАДИОСВЯЗИ

КАЛИАСКАРОВ Н.Б., *доктор PhD, заведующий кафедрой,*
БОЛАТБЕКОВА Д.Н., *студентка группы РЭТ-2-2,*
САКЕНОВА С.Ж., *магистр, старший преподаватель,*
ЕСЕНЖОЛОВ У.С., *магистр, старший преподаватель,*
АЛДОШИНА О.В., *старший преподаватель.*

КарТУ имени Абылкаса Сагинова,
город Караганда, Республика Казахстан

Аннотация. Развитие коммуникационных и интеллектуальных систем, автоматизация и телекоммуникации, улучшение электроники и измерительных систем, а также создание национальной системы военной связи открывают новые возможности для мониторинга военных и стратегически важных объектов. Исследование, основанное на разработке распределенной системы Wi-Fi, позволило собирать и передавать данные о различных параметрах таких объектов, таких как расстояние между трещинами, магнитные поля и положение объектов. Эти данные могут использоваться для прогнозирования технического состояния объектов и выявления проблем.

Ключевые слова: беспроводная связь, удаленный мониторинг, гироскоп, акселерометр, датчик расстояния.

Улучшение автономных систем технической диагностики строительных объектов и мостов связано с применением новых измерительных датчиков и устройств беспроводной передачи данных, обладающих высокой точностью, помехозащищенностью и низким энергопотреблением. Непрерывный мониторинг является ключевым элементом в системах диагностики, включающих измерение напряженно-деформационных параметров и передачу данных в центр управления. Системы мониторинга позволяют адаптироваться к изменениям требований, включая функциональные, отказоустойчивые и масштабные требования.

Именно разработка беспроводной системы Wi-Fi отвечает требованиям непрерывного мониторинга технического состояния мостов, военных зданий и сооружений. Низкая стоимость устройств и их легкость в программировании не влияют на надежность системы, что делает её привлекательной [1].

Датчики MPU-6050 и MPU-9250 – это компактные устройства, включающие гироскопы, термометры и акселерометры. Оба измеряют данные по осям X, Y и Z, но MPU-9250 также имеет магнитометр для измерения магнитных данных. Для передачи данных используется Wi-Fi модуль NodeMCU V3. Сайт https://thingspeak.com/ используется в качестве сервера для

настройки. Датчик MPU-6050 отличается от MPU-9250 наличием дополнительных контактов XCL и XDA для подключения внешнего магнитометра. Оба датчика применяются для измерения данных по осям X, Y и Z в беспроводной системе. Результаты передаются на сервер каждые 15 секунд через Wi-Fi. Для измерения расстояния используется ультразвуковой датчик HC-SR04, интегрированный в систему с Wi-Fi модулем NodeMCU V3.

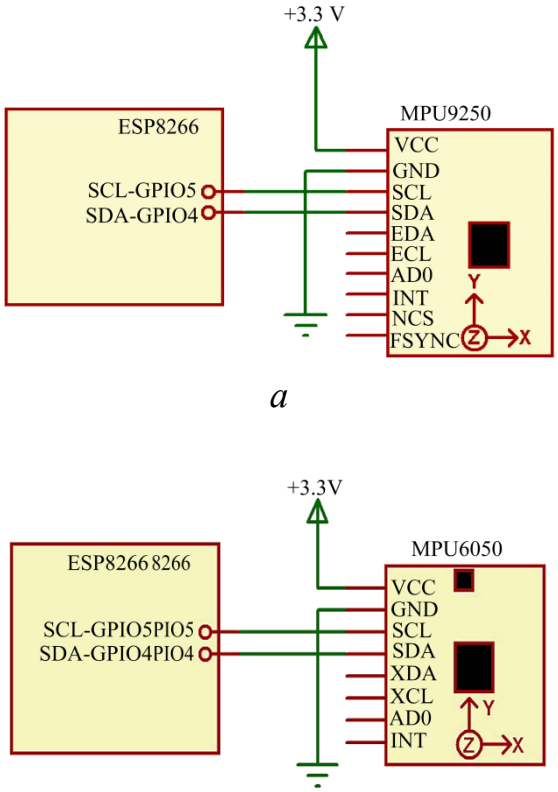


Рисунок 1 – Схема подключения выводов датчиков к Wi-Fi модулю семейства Esp8266: *а* – датчика MPU-9250; *б* – датчика MPU-6050

Кроме измерения угла наклона и ориентации объектов или сооружений, важным параметром для проведения удаленного мониторинга является возможность определения расстояния до трещин или стыков. Для этой цели используется специальное устройство. Оно работает следующим образом: при расширении контролируемой трещины увеличивается расстояние между отражающей панелью и приемником. Это происходит потому, что оптический датчик расположен с одной стороны трещины, а отражающая панель – с другой. Сигнал, пропорциональный ширине трещины, передается с приемника на усилитель, а затем на аналого-цифровой преобразователь (АЦП). Оцифрованный сигнал передается на микроконтроллер для обработки в соответствии с заданным алгоритмом. После этого информация передается по Wi-Fi на компьютер для окончательной обработки. Кроме передачи информационного сигнала, микроконтроллер формирует сигнал для включения

таймера, который периодически отключает источник питания для экономии электроэнергии [2].

Выбор беспроводного модуля обусловлен тем, что Wi-Fi модуль NodeMCU обладает различными методами для снижения энергопотребления [3]. Он компактен, обладает множеством функций с различными режимами, включая спящий режим, доступный через модификации аппаратного и программного обеспечения.

После подключения устройств к беспроводной системе передачи данных начинается процесс подготовки Wi-Fi модуля, включающий разработку уникального программного кода (скетча), в котором указываются данные сети Wi-Fi, параметры сервера, условия подключения к сети, привязка к элементам каналов для приема данных с датчиков, настройка отображаемого текста на мониторе порта при подключении устройства с датчиком, и другие программные настройки для определения угла наклона и ориентации в пространстве (рисунок 2-4).

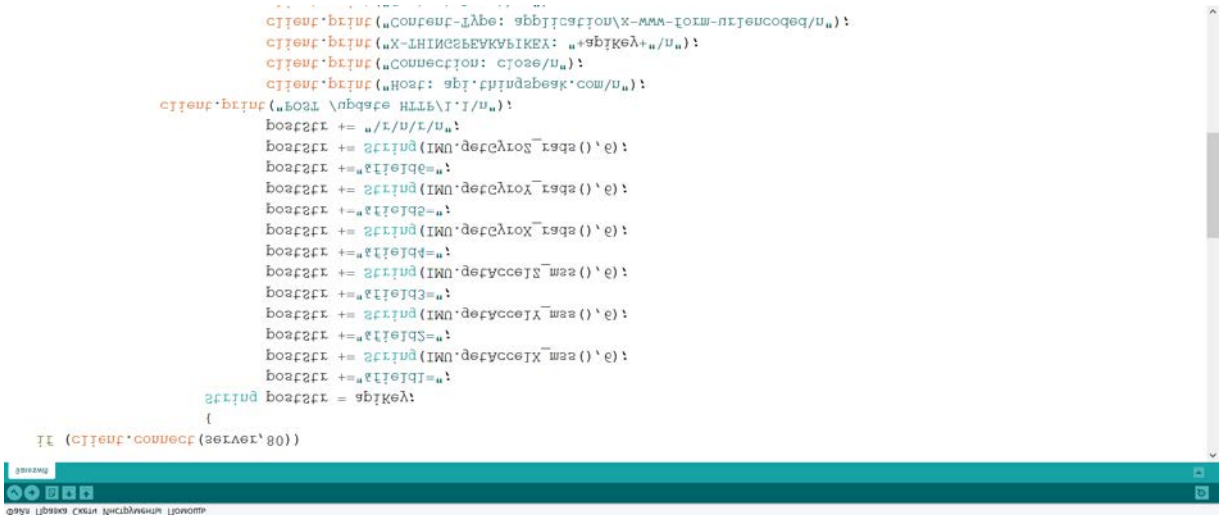


Рисунок 2 – Часть программного скетча, предназначенного для считывания измеряемых данных гироскопа и акселерометра и их передачи на сервер по Wi-Fi

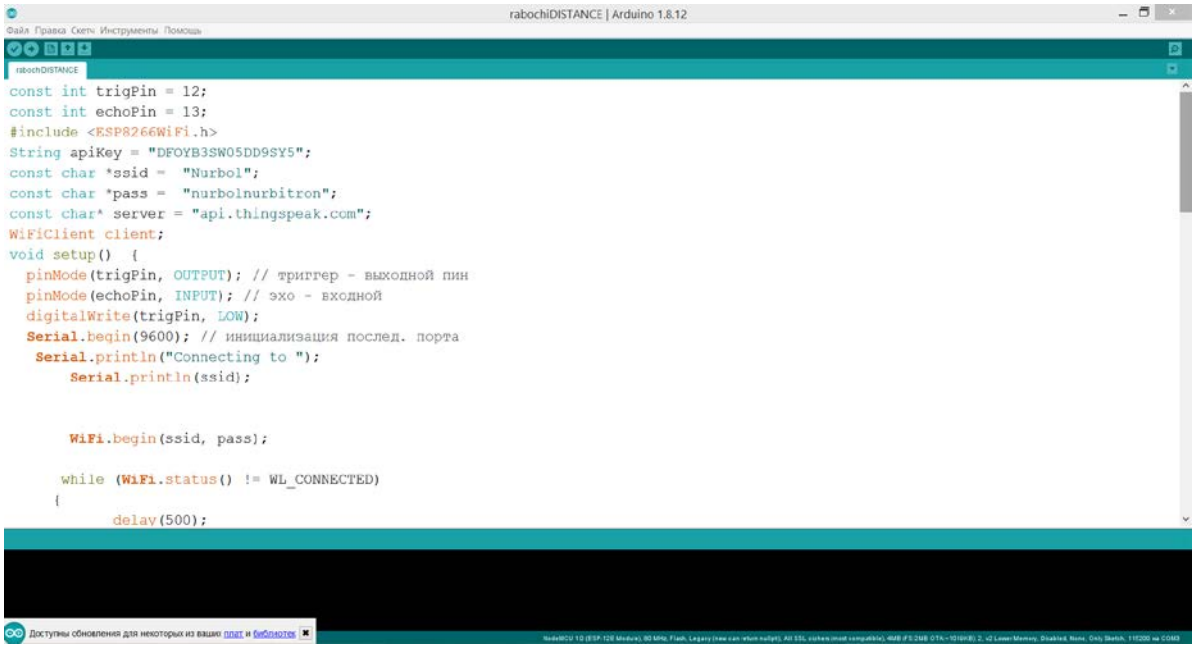
```
                        client.print("Connection: close\n");
                        client.print("X-THINGSPEAKAPIKEY: "+apiKey+"\n");
                        client.print("Content-Type: application/x-www-form-urlencoded\n");
                        client.print("Content-Length: ");
                        client.print(postStr.length());
                        client.print("\n\n");
                        client.print(postStr);

                        Serial.print("AccelX: ");
                        Serial.print(IMU.getMagX_uT(),6);
                        Serial.print("AccelY: ");
                        Serial.print(IMU.getMagY_uT(),6);
                        Serial.print("AccelZ: ");
                        Serial.print(IMU.getMagZ_uT(),6);

Serial.println("%. Send to Server.");
                    }
         client.stop();
          Serial.println("Waiting...");

 delay(15000);
}
```

Рисунок 3 – Часть программного скетча, предназначенного для считывания измеряемых данных магнитометра и их передачи на сервер по Wi-Fi



```
rabochiDISTANCE | Arduino 1.8.12
Файл Правка Скетч Инструменты Помощь
rabochiDISTANCE
const int trigPin = 12;
const int echoPin = 13;
#include <ESP8266WiFi.h>
String apiKey = "DFOYB3SW05DD9SY5";
const char *ssid =  "Nurbol";
const char *pass =  "nurbolnurbitron";
const char* server = "api.thingspeak.com";
WiFiClient client;
void setup()  {
  pinMode(trigPin, OUTPUT); // триггер - выходной пин
  pinMode(echoPin, INPUT); // эхо - входной
  digitalWrite(trigPin, LOW);
  Serial.begin(9600); // инициализация послед. порта
   Serial.println("Connecting to ");
       Serial.println(ssid);


       WiFi.begin(ssid, pass);

      while (WiFi.status() != WL_CONNECTED)
     {
           delay(500);
Доступны обновления для некоторых из ваших плат и библиотек
```

Рисунок 4 – Часть программного скетча для передачи данных с датчика расстояния по Wi-Fi модулю и настройки платы для подключения к серверу

Для соединения Wi-Fi модуля и датчика расстояния необходимо написать новый уникальный код, состоящий из множества строк на языке программирования в Arduino IDE (рис. 5). Этот код гарантирует правильное считывание, передачу и прием результатов на сервере. Также предусмотрено отображение данных измерений на мониторе порта. Важно отметить, что после настройки и прошивки платы все данные могут передаваться на сервер без прямого подключения к компьютеру, при наличии источника питания. Этот скетч позволяет отправлять данные на монитор порта в Arduino IDE для

проверки работоспособности датчиков (рис. 6, 8), а также на личный канал сервера через Wi-Fi.

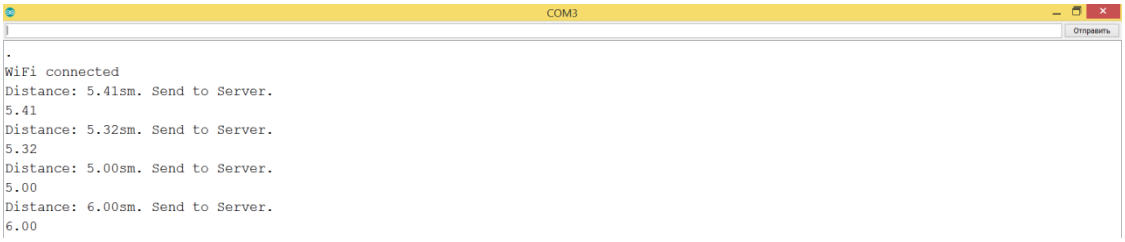


Рисунок 5 – Вывод измеряемых данных расстояний на монитор порта среды Arduino Ide

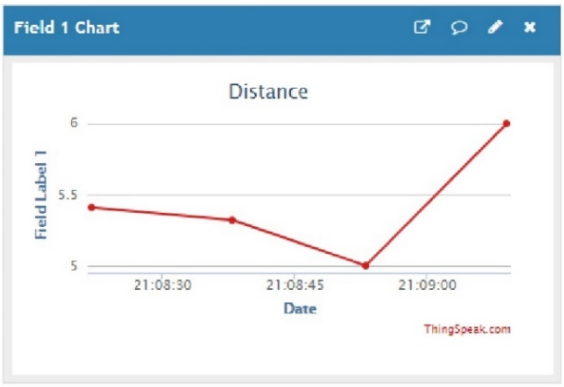


Рисунок 6 – График измеряемых данных о расстояниях на сервере

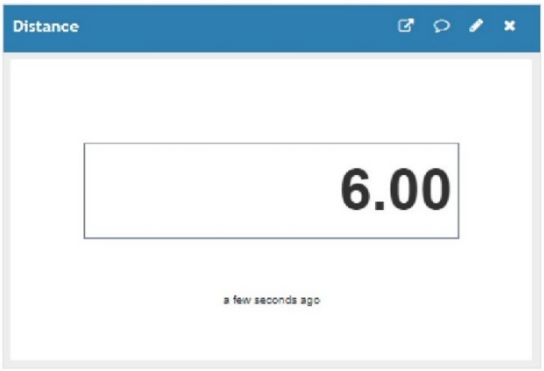


Рисунок 7 – Отображение последнего измерения расстояния на сервере

Работа датчика измерения расстояния основана на триангуляционном методе, где датчик, размещенный на удаленном объекте, определяет расстояние до объекта. В соответствии с описанной структурной и функциональной схемой, датчик подключается к Wi-Fi модулю. Этот модуль периодически принимает измерения расстояния, которые пользователь может настраивать, и передает полученные данные через роутер на сервер. Техническое описание датчика и Wi-Fi модуля подтверждает их совместимость и возможность работы

в единой системе. Процедуры сбора и передачи данных о расстоянии аналогичны процедурам передачи данных от других датчиков, таких как MPU-6050 и MPU-9250, различия заключаются лишь в уникальных программах скетчей.

На рис. 8 показан пример подключения датчика расстояния к Wi-Fi модулю.

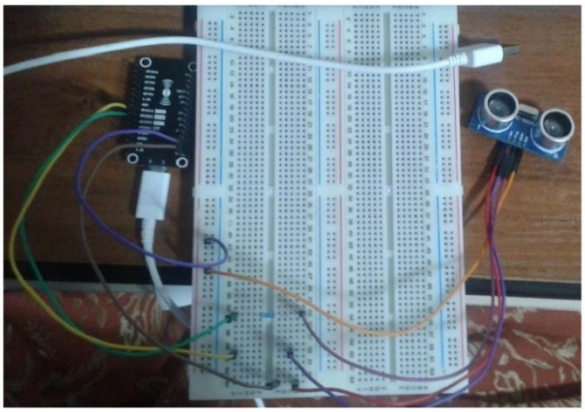
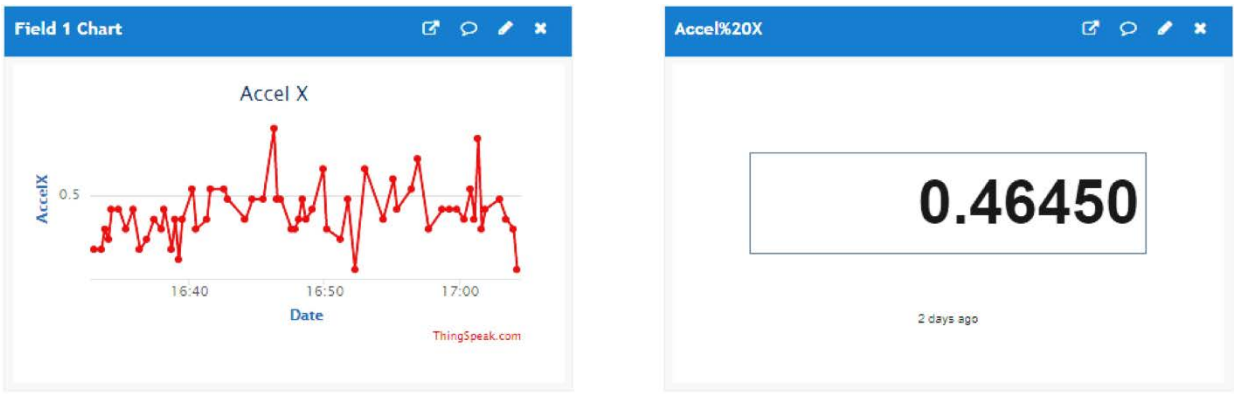


Рисунок 8 – Подключение датчика расстояния к Wi-Fi модулю в разрабатываемой распределенной беспроводной системе

Все данные передаются на сервер. Удобством и преимуществом сервера является то, что можно узнать время и дату приема того или иного значения. По полученным данным пользователь может сделать выводы, каким образом изменяются значения в ходе мониторинга за удаленным объектом.

На рис. 9-11 показаны результаты экспериментов при измерении датчиками MPU-9250. В ходе экспериментальной работы, в лаборатории каждые 15 секунд меняли положение макета, имитирующего военное сооружение или стратегически важный объект. Изменение угла наклона и ориентации в пространстве измерено по трем осям и результаты измерения отправлены при помощи Wi-Fi сети с датчиков на сервер.

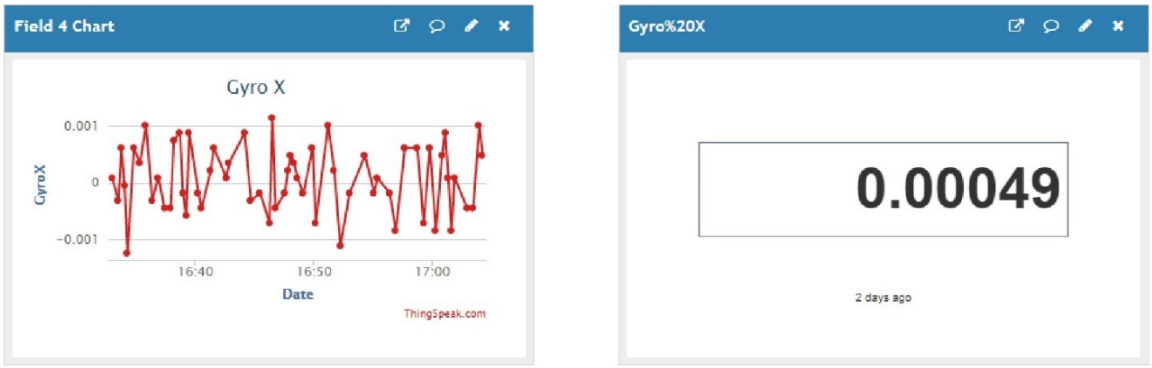


а

б

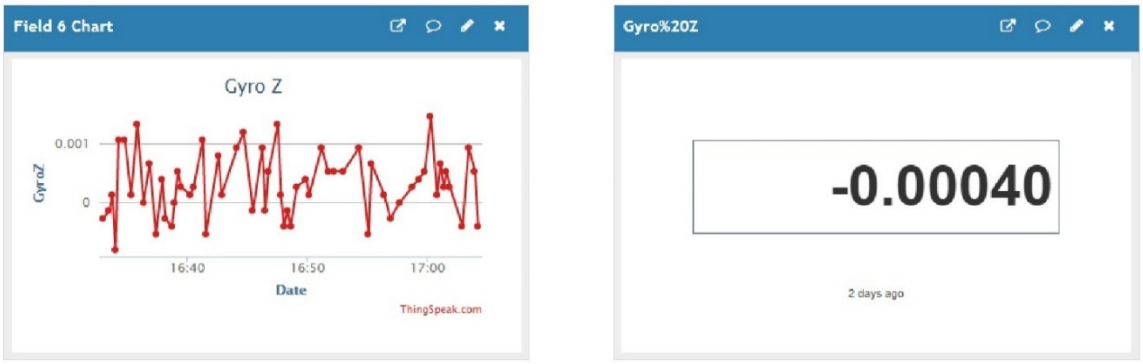
в

Рисунок 9 – Показания акселерометра в течении времени: *а* – по оси *X*; *б* – по оси *Y*; *в* – по оси *Z*



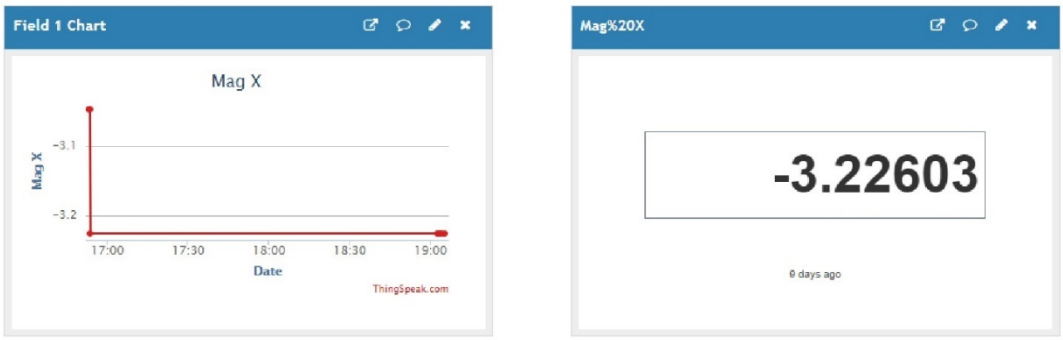
а

б

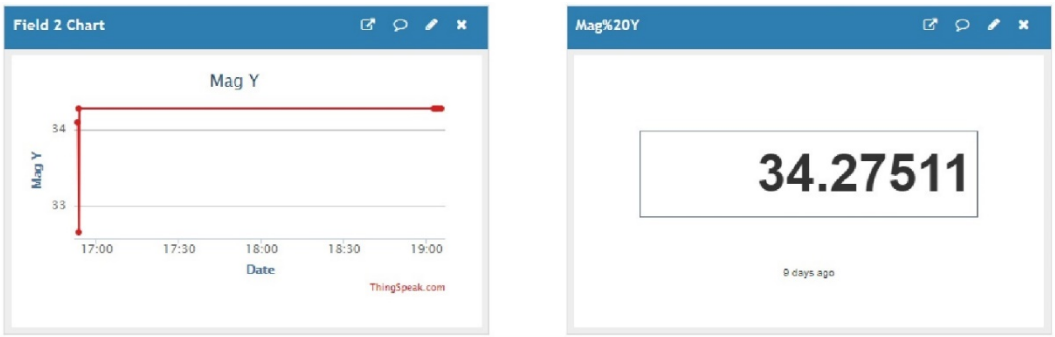


в

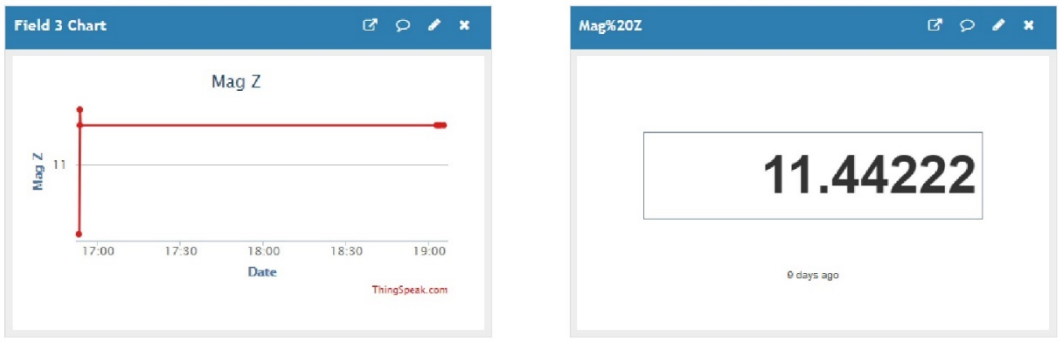
Рисунок 10 – Показания гироскопа в течении времени*:* *а* – по оси *X*; *б* – по оси *Y*; *в* – по оси *Z*



а



б



в

Рисунок 11 – Показания магнитометра в течении времени: *а* – по оси *X*; *б* – по оси *Y*; *в* – по оси *Z*

Полученные измерения позволяют пользователю на приемной стороне видеть в виде графиков все отклонения, скачки и возможные ошибки при построении сети. Обработка данных измерений позволила исправить все неточности и ошибки, возникающие в сети. Проведенная настройка и успешная апробация датчиков и устройств, входящих в беспроводную распределенную сеть, а также построение беспроводной сети, позволяет установить данные датчики на любом объекте военной сферы или мостовом сооружении.

Правильный выбор Wi-Fi модуля с четырьмя режимами энергопотребления помог сократить его энергопотребление. Режим глубокого сна был настроен для уменьшения потребления энергии, позволяя устройству выполнять задачи и переходить в спящий режим на определенное время. Небольшие размеры используемых устройств (Wi-Fi модуля и датчиков) позволяют системе функционировать на удаленных объектах, обеспечивая автономность. Полученные данные могут быть просмотрены онлайн с помощью устройства, имеющего доступ в сеть военной радиосвязи.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1 Фролова М.В. Применение Веб-технологий при разработке распределенных систем мониторинга // Известия ЮФУ. Технические науки. – Таганрог, 2011. – Тематический выпуск. Раздел I. Системы и сети. – С.41-47.

2 Ивель В.П., Разинкин В.П., Калиаскаров Н.Б. (2019). Разработка беспроводного устройства мониторинга состояния трещин и стыков зданий и сооружений, и его преимущества. «Вестник КазАТК», 2, 10-17. https://vestnik.alt.edu.kz/index.php/journal/issue/view/9/9

3 Kaliaskarov N.B., Ivel V.P., Yugay V.V., Gerasimova Y.V., Moldakhmetov S.S. Development of a distributed wireless Wi-Fi system for monitoring the technical condition of remote objects // Eastern-European Journal of Enterprise Technologies. – 2020, Vol.5 №9 (107). – P. 36–48. doi: https://doi.org/10.15587/1729-4061.2020.212301

УДК 654.16

ОБЗОР И АНАЛИЗ ТЕХНИЧЕСКИХ РЕШЕНИЙ ИНТЕГРАЦИИ РАЗЛИЧНЫХ СИСТЕМ РАДИОСВЯЗИ

ДОЛЯ А.В., *майор, докторант*

Национальный университет обороны Республики Казахстан, г.Астана

Аннотация. Целью данной статьи является систематизация существующих технических решений в области интеграции систем радиосвязи, анализ их функциональных возможностей, а также определение перспективных направлений развития в этой сфере. В статье используется комплексный подход, включающий в себя анализ научной литературы, технической документации, а также опыт реализации интеграционных систем в различных странах.

Ключевые слова: интеграция, функциональная совместимость, системы радиосвязи, интеграционный шлюз, VoIP, RoIP-шлюз.

В современном мире, характеризующемся стремительным развитием информационных технологий и неуклонным ростом объема предаваемых данных, становится критически важным обеспечение эффективного взаимодействия и интеграции различных систем радиосвязи [1]. Проблематика интеграции систем радиосвязи обусловлена не только разнообразием используемых стандартов, протоколов и технологий [2], но и необходимостью обеспечения высокого уровня совместимости, безопасности и надежности передачи данных.

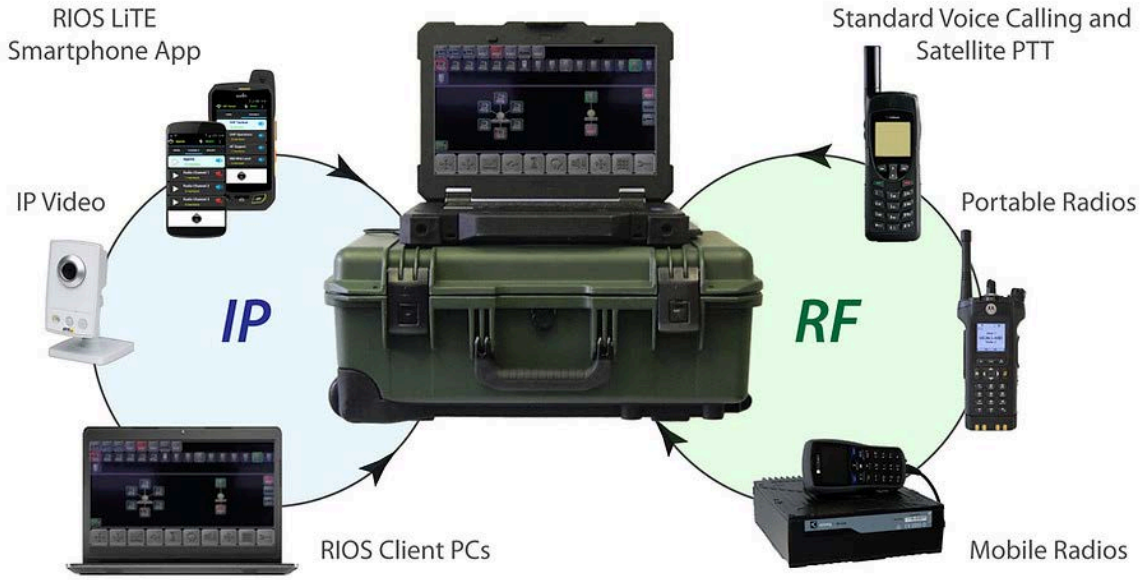
На сегодняшний день в мире существует несколько способов интеграции различных систем радиосвязи, которые подразумевают под собой использование шлюза (шлюзов). При этом, интеграционный шлюз может осуществлять сопряжение как различных систем радиосвязи в целом, так называемая межсистемная интеграция (использование VoIP, RoIP-шлюзов), так и непосредственно коммутацию аудиосигналов подключённых к нему различных систем радиосвязи. Более того, у некоторых предлагаемых технических решений могут одновременно присутствовать оба способа интеграции.

Таким образом, в данной статье рассмотрим технические решения в виде интеграционных шлюзов от различных зарубежных производителей, спроектированных как на основе IP-технологий, так и в виде программно-аппаратных комплексов, предназначенных для коммутации аудиосигналов между различными системами радиосвязи.

1. Интеграционный шлюз взаимодействия тактической радиосвязи RIOS TAC2 компании SyTech Corporation позволяет органам общественной безопасности, экстренным службам и военным организациям оперативно соединять радиосредства различных диапазонов частот (HF/VHF/UHF и

700/800 МГц). Радиосовместимость между разнородными устройствами достигается путем преобразования сопряженного сигнала в стандарт с открытым исходным кодом.

Применение современных технологий в RIOS TAC2 расширяет традиционную совместимость радиосвязи, включая интерфейсы для клиентских компьютеров RIOS, RIOS LiTE для Android и iPhone, а также опции для спутниковых телефонов, устройств VoIP, видеовходов и многого другого (рисунок 1) [3].



подключение через локальную сеть, Wi-Fi или сотовую связь

подключение через интерфейсный кабель RIOS

Рисунок 1 – Возможности подключения радиосредств и других устройств к интеграционному шлюзу RIOS TAC2 [3]

Модуль ввода-вывода RIOS TAC2 на задней панели имеет восемь интерфейсных портов, совместимых с радиостанциями Motorola, Harris, Codan, Kenwood, iCOM и других производителей (рисунок 2). IP-устройства подключаются через встроенный маршрутизатор с поддержкой локальной сети, Wi-Fi и возможностью обратной связи по сотовой связи с USB-устройством передачи данных пользователя. Управление осуществляется через программный графический интерфейс пользователя (удаленный клиент).

Рисунок 2 – Внешний вид интеграционного шлюза RIOS TAC2 [3]

Интеграционный шлюз RIOS TAC2 весит около 18 килограмм, включая батарею и контроллер. Он легко помещается в стандартный багажный отсек и соответствует требованиям FAA для перевозки ручной клади.

Встроенное управление питанием обеспечивает непрерывное питание контроллера шлюза, модуля ввода-вывода и маршрутизатора. RIOS TAC2 включает в себя источник питания переменного/постоянного тока с принудительной блокировкой, а также встроенный литий-ионный аккумулятор и бортовое оборудование. Интеграционный шлюз позволяет работать при полной зарядке батареи примерно 6-8 часов или более, в зависимости от заряда контроллера и других факторов.

RIOS TAC2 обеспечивает подключение к IP-сети через встроенный четырехпортовый маршрутизатор с поддержкой Wi-Fi/3G/4G. Варианты сети включают спутниковую связь или сотовую связь 3G/4G с предоставлением клиентом сотового USB-устройства. Имеется возможность подключения несколько узлов RIOS к различным типам беспроводных сетей с помощью программного модуля RIOS Multi-Site. Благодаря такому расположению удаленные узлы RIOS могут передавать и принимать голос, видео и текст в рамках единой платформы, расположенной в любом месте, где есть IP-подключение.

2. Серия Omnitronics IPR (IP Radio) представляет собой решения IP-интеграции, разработанные компанией Omnitronics для обеспечения взаимодействия и интеграции различных типов радиостанций (включая цифровые и аналоговые) в единую сеть радиосвязи [4]. Данное техническое решение позволяет осуществлять интеграцию систем радиосвязи различных стандартов, таких как DMR, NXDN, APCO-25, TETRA и другие, и позволяет обмениваться информацией и голосовыми данными между ними. Omnitronics IPR предлагает гибкие настройки, что позволяет настраивать и масштабировать ее под конкретные потребности (рисунок 3). Также, такая система обладает функциями управления трафиком и сетевыми возможностями для

эффективного распределения данных и контроля потока информации между различными радиостанциями.

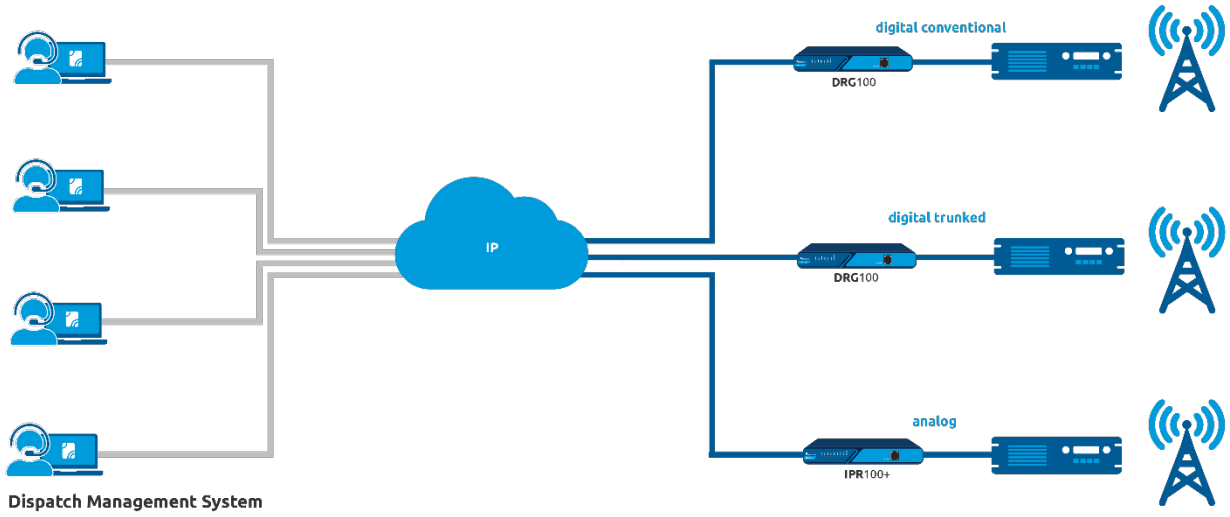


Рисунок 3 – Подключение радиосредств через интернет-протокол (RoIP) с применением оборудования серии Omnitronics IPR [4]

Модель IPR400 S2 компании Omnitronics (рисунок 4) представляет собой гибкий многоканальный радиоинтерфейс VoIP с программным обеспечением шлюза RoIP. Он сочетает в себе расширения передачи голоса по IP для аналогового радиооборудования и функциональную совместимость между разрозненными радиосистемами.

Рисунок 4 – RoIP шлюз IPR400 S2 [4]

4 порта IPR400 S2 могут быть связаны между собой внутри IPR400 S2 или с VoIP множеством комбинаций, что делает устройство эффективным для подключения ретрансляторов. Шлюз также поддерживает SIP-подключение для использования с диспетчерскими консолями, такими как RediTALK-Flex и решениями радиодиспетчерской серии omnicore. Когда IPR100 недостаточно, IPR400 S2 предлагает изолированные 4-проводные интерфейсы E&M, многоадресную рассылку, обнаружение голосовой активности, сжатие голоса, сигнализацию SELCALL и DTMF, шифрование и туннелирование данных RS-232.

Чтобы упростить настройку, IPR400 S2 включает в себя программно-настраиваемые сигналы E&M. Поддерживается PTT через сотовую связь (PTToC), а также удаленное управление по IP.

3. Интеграционный шлюз JPS Interoperability Solutions ACU-T (Advanced Communication Unit - Transceiver) (рисунок 5) обеспечивает интеграцию и взаимодействие между различными цифровыми и аналоговыми радиостанциями стандартов APCO-25, DMR, NXDN и другими, телефонными линиями, а также радио через интернет-протокол (RoIP) [5].

Рисунок 5 – Интеграционный шлюз JPS Interoperability Solutions ACU-T [5]

Интеграционный шлюз ACU-T обладает гибкими настройками, что позволяет пользователям настраивать ее для работы с различными стандартами и типами радиостанций в зависимости от потребностей. Шесть устройств, подключенных к ACU-T, могут быть соединены между собой в любой комбинации: от трех сетей с двумя пользователями до одной сети, в которой все шесть пользователей соединены вместе.

Основным средством управления является программный графический интерфейс пользователя (GUI). ACU-T также можно управлять с помощью встроенного контроллера клавиатуры и светодиодного дисплея состояния подключения системы.

Интеграционный шлюз ACU-T работает от входной мощности переменного/постоянного тока. Данная система часто предоставляется в компактном и портативном исполнении, что делает ее удобной для различных сценариев использования. ACU-T обеспечивает соответствие стандартам безопасности и надежности для обмена информацией между различными радиостанциями, соблюдая требования к защите передаваемых данных.

4. ICRI Radio Interoperability Gateway/Bridge – серия различных интеграционных устройств (аудиошлюзов), которые могут применятся для создания небольшой временной сети, созданной для конкретной операции [6].

Аудиошлюзы серии ICRI доступны в широком диапазоне различных конфигураций, которые позволяют настраивать их в соответствии с потребностями органов общественной безопасности, служб быстрого реагирования и вооруженных сил.

Так, например аудиошлюз ICRI 2TG (рисунок 6) может использоваться для соединения и объединения в единую радиосеть радиостанций различных диапазонов частот (HF/VHF/UHF и 700-900 МГц), различных стандартов (TETRA, APCO-25), а также стационарных/спутниковых телефонов, VoIP-устройств, сотовых телефонов, в течение нескольких минут после развертывания.

Рисунок 6 – Интеграционный аудиошлюз ICRI 2TG [6]

Габаритные размеры аудиошлюза ICRI 2TG составляют 9 см. в высоту, 26 см. в ширину и 16,5 см. в глубину. Пользовательское управление осуществляется с помощью встроенных переключателей разговорной группы; регулировка времени/задержки осуществляется внутри устройства.

В серии ICRI имеется также и полевой военный аудиошлюз ICRI-E, выполненный в переносном ударопрочном и водонепроницаемом кейсе (рисунок 7).

Рисунок 7 – Интеграционный аудиошлюз ICRI-E [6]

Отличительной особенностью данного устройства является возможность его автономного применения за счет использования аккумуляторных батарей, устанавливаемых в корпусе (рабочий цикл более 24 часов).

5. Infinimode Systems предлагает интеграционную платформу (аудиошлюз) InfiniMUX G4 как в стандартном исполнении (рисунок 8а), так и в

переносном корпусе (рисунок 8б). Данная платформа построена по модульному принципу и обеспечивает взаимное соединение различных систем голосовой связи, включая транкинговые радиосистемы, телефонные линии, а также мобильные и портативные голосовые радиостанции различных типов [7]. Также данная платформа может поддерживать другие типы систем связи, в том числе сотовую связь, спутниковые системы и IP-сети (VoIP).

(а) (б)

Рисунок 8 – Интеграционная платформа InfiniMUX G4 [7]

Интеграционная платформа InfiniMUX G4 обладает следующими основными функциями:

– простота настройки и эксплуатации;

– прочная и надежная конструкция для работы в полевых условиях;

– низкое энергопотребление (менее 6 Вт);

– возможность одновременного подключения до 28 радиоканалов или до 24 радиостанций и 4 телефонных линий;

– отдельные каналы могут быть сгруппированы в до 128 независимых сетей;

– отдельные модули могут быть заменены в «горячем режиме», что позволяет быстро заменить модуль, не влияя на связь по другим каналам;

– возможность управления двумя способами: через встроенный контроллер клавиатуры или через программный графический интерфейс пользователя;

– содержит светодиодную систему для отображения его рабочего состояния и состояния подключения.

6. Радиошлюз SafetyNet RadioBridge System компании Aegis Assessments, представляет собой автономный кейс, предназначенный для организации небольшой временной сети создаваемой для конкретного инцидента на месте чрезвычайной ситуации (рисунок 9) [8]. SafetyNet RadioBridge позволяет всем подключенным радиостанциям иметь бесперебойную связь без необходимости предварительной настройки.

Прочный, защищенный от атмосферных воздействий корпус радиошлюза содержит встроенную батарею, обеспечивающую работу на 48 часов со всеми радиоинтерфейсами. Ручка управления для каждого радиоинтерфейса

позволяет пользователю выбирать между 4 отдельными группами или группой общего вызова. Для оператора доступно подключение гарнитуры.

Рисунок 9 – Радиошлюз SafetyNet RadioBridge System [8]

Цены на вышеприведенные интеграционные системы могут значительно варьироваться в зависимости от множества факторов, включая регион, объем заказа, комплектацию, условия поставки, наличие дополнительных функций и другие индивидуальные требования.

Каждый из представленных интеграционных шлюзов имеет свои особенности, возможности и сферы применения. Выбор определенного шлюза может зависеть от требований конкретного проекта, а также от совместимости с радиосредствами, которые необходимо интегрировать.

Вместе с тем, задачи адаптации зарубежных систем к локальным условиям и оборудованию, применяемому в Вооруженных Силах, других войсках и воинских формированиях Республики Казахстан, остаются нерешенными и требуют дополнительных затрат, также существует и не менее важный вопрос информационной безопасности использования зарубежных систем при создании межведомственной интегрированной абонентской сети. При этом, опыт приобретения телекоммуникационного оборудования показывает высокую стоимость закупаемых систем за рубежом, а также дорогостоящее гарантийное обслуживание и закрытый характер технологии разработки, тактико-технических характеристик элементов (составных частей) и тактики применения комплексов в целом. Остается открытым вопрос и возможности приобретения данных систем в условиях геополитических изменений последних лет.

Таким образом, создание отечественного интеграционного шлюза систем радиосвязи может иметь несколько преимуществ по сравнению с покупкой иностранных образцов:

– локализация и адаптация: отечественный образец может быть разработан с учетом особенностей и конкретных потребностей страны,

законодательства и специфики систем связи, что может обеспечить более точную локализацию и адаптацию к местным условиям радиосвязи;

– техническая поддержка и обслуживание: локальные компании могут предоставлять более доступную техническую поддержку, обслуживание и обновление, а также быстрее реагировать на запросы пользователей, что в целом облегчает процесс эксплуатации сложных технических систем;

– развитие местной промышленности и компетенций: создание отечественного образца способствует развитию отечественной промышленности и компетенций в области разработки и производства интеграционных систем для радиосвязи, что может оказать положительное влияние на экономику и технологические навыки в стране;

– сокращение затрат: при правильном развитии и поддержке создание собственного оборудования может быть более экономичным, чем постоянная покупка иностранного оборудования;

– снижение зависимости от иностранных поставщиков: разработка и производство отечественного оборудования может снизить зависимость от иностранных поставщиков, что может быть критически важным в случае изменения политических, экономических или технологических обстоятельств;

– более гибкие решения и возможность кастомизации: при создании интеграционного шлюза внутри страны, компании могут лучше адаптировать решение к уникальным потребностям и требованиям клиентов, а также предоставить более гибкие решения и возможности кастомизации.

Однако стоит учитывать, что создание отечественного образца требует времени, ресурсов и финансирования на исследования, разработку, тестирование и внедрение. Поэтому решение о создании отечественного образца должно быть оценено исходя из специфики ситуации, требований к системе связи и возможностей местных предприятий и научно-исследовательских лабораторий.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1 Доля А.В. К вопросу создания интегрированной абонентской сети радиосвязи // Основные тенденции обеспечения региональной безопасности в условиях глобализации. Сборник материалов V международной научно-теоретической конференции. 29 ноября 2023 г. – Ташкент: Академия ВС РУ, 2023. – С. 277-281.

2 Доля А.В. Обзор и анализ современного состояния и технических особенностей проектирования транкинговой системы радиосвязи // «Современное состояние перспективы развития средств связи и телекоммуникации» (21 ноября 2023 г.) Мат-лы междунар. науч.- практ. конф. – Алматы, Военно-инженерный институт радиоэлектроники и связи, Республика Казахстан, 2023. – С. 52-56.

3 TAC2 Interoperability Gateway. – URL: https://www.sytechcorp.com/rios-tac2-interop-gateway (дата обращения – 20.01.2024).

4 RoIP Gateways. – URL: https://www.omnitronicsworld.com/ru/radio-over-ip-roip-solutions/ (дата обращения – 21.01.2024).

5 ACU-T Tactical Interoperability. – URL: https://www.psicompany.com/man-prod-info/Raytheon-JPS/Control-Equipment/ACU-T/ACU-T-Datasheet.pdf (дата обращения – 23.01.2024).

6 ICRI Radio Interoperability Gateway/Bridge. – URL: https://www.c-at.com/products/icri-radio-interoperability-gateway/ (дата обращения – 23.01.2024).

7 InfiniMUX G4 Communications Controller. – URL: https://web.archive.org/web/20040214201052/http://www.infinimode.com:80/UM1200-01.pdf (дата обращения – 24.01.2024).

8 Audio Gateway Handbook. – URL: https://taccomms.org/wp-content/uploads/2019/Interop/Audio-Gateway-Handbook_320_Final.pdf (дата обращения – 25.01.2024).

УДК 355/359.07

ОРГАНИЗАЦИЯ СВЯЗИ В СПЕЦИАЛЬНОЙ ТАКТИЧЕСКОЙ ГРУППЕ КАК ОСНОВА НАЦИОНАЛЬНОЙ СИСТЕМЫ ВОЕННОЙ РАДИОСВЯЗИ

КОЖЕКОВ Е.Т., *старший преподаватель, полковник запаса*
БОЙКОВ А.В., *к.в.н., PhD, начальник цикла, полковник запаса*

Аннотация. В данной статье рассмотрены некоторые вопросы комплексного подхода к организации связи в специальной тактической группе с точки зрения создания основы национальной системы военной радиосвязи.

Ключевые слова: специальная тактическая группа, мультиконвергентная система связи, цифровая связь, территориальная оборона, автоматизированная система управления.

Не будем подробно останавливаться на истории образования нового термина, нового подразделения тактического (оперативно-тактического) уровня – тактическая группа или специальная тактическая группа (СТГр). Несомненно, это произошло в результате развития боевой техники и вооружений, с последовавшим изменением не только тактики их применения, но и оперативного искусства в целом.

В разных армиях мира появились батальонные тактические группы (БТГ). Пионерами в их создании можно считать Армию Соединенных Штатов Америки (США), в соответствии с определением в энциклопедическом словаре, «батальонная тактическая группа – временное формирование, создаваемое в армии США на базе батальона для ведения боя» [1].

В технически оснащенных Армиях (Вооруженных силах (ВС)) государств создаются и эволюционируют под различными терминами тактические подразделения (группы) для выполнения специфических задач с «разнородовым» составом внутри. Терминология названия, задачи и состав таких тактических подразделений (групп) рассматривались неоднократно (в том числе и на II Ежегодной Международной научно-практической конференции «Цифровые средства связи: Вопросы их внедрения» ВИИРЭиС, ноябрь 2022 г. [2].

В ВС Республики Казахстан (РК) за последние десятилетие в ходе проведения учений, отработке задач по планам боевой подготовки применялась тактическая группа, основу которой составляло подразделение численностью до роты личного состава. На этапе становления ВС государства, при проведении ротных тактических учений (РТУ) действовала «ротная тактическая группа в составе мотострелковых, аэромобильных и артиллерийских подразделений при поддержке армейской авиации» [3]. При участии в учении «Мирная миссия-2021» «… ротная тактическая группа

регионального командования «Запад», … на бронетранспортерах, была переброшена разведывательно-штурмовая рота, усиленная танками и расчетом БПЛА. К маневрам привлечены самолеты Су-25 Военно-воздушных сил Казахстана» [4]. На сегодняшний день «… слаживание ротных тактических групп. Внедряются новые способы применения подразделений, в том числе для обороны населенных пунктов и участия в антитеррористических операциях» [5].

Необходимо отметить, что опыт вооруженных конфликтов современности подтверждает актуальность развития концепции применения ротных и батальонных тактических групп, обладающих возможностью действовать самостоятельно, в отрыве от главных сил [5].

Научно-исследовательские работы, проводимые при Министерстве обороны Республики Казахстан, в этой области в последние годы показывают, что: «тактические группы и отряды создаются для проведения разведывательно-поисковых, рейдовых, блокирующих, штурмовых действий; совершения обходов опорных пунктов противоборствующей стороны; охраны важных государственных объектов; выставления заслонов; сторожевых застав (блокпостов); устройства засад; боевого сопровождения колонн. Для борьбы с мобильными группами незаконных вооруженных формирований (НВФ) в составе мотострелковых подразделений создаются тактические подгруппы – «боевые двойки», «боевые тройки» и т.п.

Основу отрядов и групп составляют мотострелковые батальоны и роты, усиливаемые танками, артиллерией, инженерными и огнеметными подразделениями» [6, с.40].

Как правило, для ведения специальных войсковых действий на основе мотострелкового батальона (роты) создается батальонная (ротная) тактическая группа – сводное вооруженное формирование, предназначенное для ведения самостоятельных действий по поиску, блокированию и ликвидации НВФ.

Батальонная (ротная) тактическая группа состоит из мотострелкового батальона (роты), усиленного танковыми, артиллерийскими и инженерными подразделениями, под единым командованием. В ходе ведения боевых действий в состав батальонной (ротной) тактической группы для выполнения специальных задач могут входить подразделения специального назначения, а также Национальной гвардии и территориальной обороны [6, с. 41].

В продолжение сказанного в вооруженных конфликтах современности, в особенности настоящего времени, существенно видоизменяется состав БТГ своим наполнением, в том числе не только представителями силовых и других ведомств (таких как МВД, КНБ, МЧС, аналогичные им и другие), но и «административно-территориальных единиц в зонах боевых действий и территориальной обороны в интересах вооруженной защиты Республики Казахстан» [7, Глава 5, Параграф 4, п. 49].

Безусловно, основу СТГр, её «силовых и огневых» структурных подразделений для выполнения боевых задач, будут составлять ***мотострелковая рота (батальон), разведывательно-штурмовая рота***

(взвод) и т.п., но формирование этой СТГр должно проходить в порядке последовательного определения и реализации основных пунктов:

− военная (военно-политическая) цель действий;

− частные задачи для достижения цели действий;

− расчет необходимого состава сил и средств для решения частных задач;

− определение организационного (руководящего) ядра и пункта (или нескольких пунктов) временной дислокации (ПВД) СТГр для выполнения частных задач и достижения цели действий;

− организация связи СТГр, в том числе как внутренней, так и внешней.

Причем пункт «организация связи СТГр» на сегодняшний день становится краеугольным камнем создания национальной системы военной радиосвязи (НСВР).

Существует множество подходов к реализации НСВР, многие из них имеют рациональное зерно и право на существование. Так в одном из научных журналов рассматривается теория и практика построения существующих систем связи военного назначения на основе создания **мультиконвергентной системы связи** [8, с. 66-78].

По мнению авторов, основные усилия в развитии системы управления должны быть сосредоточены на обеспечении гарантированного сокращения цикла управления и повышении эффективности управления межвидовыми, разно ведомственными и коалиционными группировками войск (сил) в интересах обеспечения наиболее полного применения их боевых потенциалов при выполнении поставленных задач.

Для этого должно быть предусмотрено развитие объединенной автоматизированной цифровой системы связи в целях обеспечения предоставления полного перечня современных услуг связи органам военного управления; совместимость и модернизацию действующих, (что подразумевает интеграцию существующего сегодня «парка системы связи», включающего в себя аналоговые элементы, в «систему передачи данных»), создание перспективных автоматизированных систем управления (комплексов средств автоматизации – КСА) всех звеньев управления в интересах наращивания их функциональных возможностей; создание современных информационно-управляющих систем в целях оснащения ими перспективных образцов вооружения, военной и специальной техники (беспилотная авиация, роботизированные боевые комплексы и системы военного назначения), создание перспективных подвижных пунктов управления, обладающих высокой разведзащищенностью и живучестью, максимальной автономностью, большой мобильностью, минимальных по своему составу и обеспечивающих надежное управление войсками (силами).

Значимая роль в управлении войсками отводится внедрению качественно новых сетевых цифровых технологий, создающих принципиально иной базис как в структуре управления, так и в решении всей совокупности задач управления в режиме реального времени. Для этого необходимо создание системы программно-аппаратных средств, которые должны представлять собой

совокупность территориально разнесенных и взаимоувязанных подсистем, функционирующих на основе единой системы протоколов информационного взаимодействия в единой интегрированной системе обмена данными вооруженных сил.

Таким образом имеется необходимость в разработке и создании такой системы связи, которая по своим потенциальным характеристикам удовлетворяла бы динамично возрастающим требованиям устойчивого управления войсками в сложных условиях современных операций.

Применение современных сетевых цифровых технологий позволяет структурно и функционально обосновать построение перспективной системы связи СТГр как **мультиконвергентной.**

Под **мультиконвергентной системой связи СТГр** понимается совокупность территориально распределенных сетей связи, зональных узлов связи, развернутых в различных сферах (наземной, воздушной, кибер-, в перспективе космической), на основе унифицированных технических средств связи и соединенных физическими каналами связи для обеспечения управления войсками.

Основой мультиконвергентной системы связи является **мультисферная сеть связи** с пространственно-распределенной архитектурой, функционирующей на основе IP-технологии.

Для минимизации проблем совместимости и упрощения управления конвергентные решения позволяют объединить сетевые, вычислительные ресурсы, системы хранения и программное обеспечение в сконфигурированный единый «пакет», который работает и управляется как единая конвергентная система, обеспечивающая потребности системы управления в предоставлении современных услуг связи.

Опыт современных локальных конфликтов показывает, что при организации связи можно использовать глобальное киберпространство, находясь не только в границах своей страны, но и за её пределами. Быстрое развертывание сетей интернет, как стационарных, так и мобильных, почти всеми странами мира и широкая конвергенция данных сетей позволяют активно использовать их в том числе и в военной сфере. Следовательно, имеющиеся в настоящее время ресурсы глобального информационного и телекоммуникационного пространства будут формировать один из ключевых элементов мультисферной сети связи – **киберсферу**, под которой понимается масштабируемая, неоднородная искусственная система, состоящая из взаимосвязанных информационных и телекоммуникационных сетей.

Обязательным **элементом мультиконвергентной системы связи СТГр** являются средства доступа – комплекс носимых, возимых и автономных средств связи, обеспечивающих доступ потребителей (пунктов управления, должностных лиц, роботизированных систем, средств РУК и др.) к ресурсам мультисферной системы связи и образование унифицированных каналов и трактов связи для передачи сообщений всех видов в системе управления войсками.

Средства доступа в системе разделены на персональные и коллективные. Персональные средства доступа – это носимые мобильные средства связи, которые закрепляются за конкретными пользователями (должностными лицами пункта управления), коллективные – это средства, размещенные в командно-штабных машинах, в комплексных аппаратных связи и обеспечивающие доступ как персональных средств, так и собственных к ресурсу мультисферной сети связи, а также обеспечивающие предоставление основных услуг связи (передача голоса, передача данных, обмен короткими сообщениями, электронной почты и видео).

Мультиконвергентная система связи должна строиться с использованием единых принципов в соответствии со стандартами, разработанными в рамках эталонной модели взаимодействия открытых систем. При этом сети связи, входящие в состав вооруженных сил, войск и формирований других ведомств, должны являться составными частями данной системы, наращивая возможности сетей старшей инстанции в системе управления войсками и, в свою очередь, резервировались бы за счет ресурсов последней.

В мультиконвергентной системе связи должны широко применяться интернет-технологии, главным преимуществом которых является то, что они позволяют предоставить весь спектр услуг связи через единственную точку абонентского доступа, а многодиапазонные многосистемные терминалы радиосвязи могут функционировать в системах связи, использующих разные стандарты. Протоколы интернет-сети должны использоваться для передачи информации во всех звеньях управления, начиная с тактического звена.

Осуществляемые в настоящее время действия по повышению разведзащищенности и устойчивости функционирования пунктов управления привели к развитию модульных подвижных пунктов управления и созданию единого информационного пространства, что объективно подтверждают верность направления по созданию мультиконвергентной системы связи, которая будет являться базовым элементом технической основы системы управления.

Создание мультиконвергентной системы связи направлено на повышение устойчивости и непрерывности управления СТГр при кардинальном переходе к новой, более совершенной форме организации сетей (систем), создаваемых на основе интенсивного развития и широкого применения новых военных сетевых технологий при разработке систем и комплексов вооружений нового поколения [8, с. 66-78].

Внедрение соответствующих технологий должно привести к всесторонней технологизации процессов всех сфер военных и боевых действий и видов деятельности органов военного управления объединений, соединений и частей.

В целях минимизации финансовых затрат, реализации проекта создания национальной системы военной радиосвязи считаем целесообразным применить подход, основанный на синтезе теории **таксономии Сэмюэла Блума** [9, 10, 11, 12] применительно к созданию НСВР низшего уровня, от

тактического к стратегическому и метода дедукции (от простого к сложному) для практической реализации как отдельных уровней системы, так и создания её (системы) в целом.

Вкратце можно отметить, что модель, появившаяся в 1956 году, претерпела ряд изменений, учёные разработали новые квалификации, затем была пересмотрена другой группой учёных 2001 году. Пересмотренная (усовершенствованная) таксономия Блума выглядит следующим образом, (рисунок 1) Иерархию целей (и первую, и вторую) обычно изображают как пирамиду. В основании которой самые базовые цели, а на пике – сложные и многокомпонентные.

Считается, что каждый новый уровень как бы продолжает следующий. То есть, чтобы перейти к целям высшего порядка, сначала нужно разобраться с низшими.

Рисунок 1 – Один из вариантов модернизированной Таксономии Блума

В итоге, применение **таксономии** поможет равномерно и правильно определить (или/и распределить) цели и задачи создания каждого уровня национальной системы военной радиосвязи, причём речь здесь идёт именно о результатах, а не о деятельности, которая к этим результатам приводит (Рисунок 2).

Рисунок 2 – Вариант Таксономии Блума для создания НСВР

В связи с вышеизложенным, практическая реализация создания (построения) НСВР возможна начиная с низшего уровня и с минимальными затратами, путем создания системы связи СТГр, как низшего неделимого элемента системы.

В качестве основы формирования такой тактической группы предлагается задействовать подразделения территориальной обороны без отвлечения действующих сил силовых структур.

Другими словами, речь идет о создании системы связи в подразделении территориальной обороны, на которое предлагается возложить роль основного подразделения СТГр.

Постоянно меняющаяся геополитическая обстановка, характер военных угроз, опыт современных военных конфликтов выдвигают на особую роль значение территориальной обороны государства. Что в полной мере отражено в ВД РК: «62. Основными мерами по совершенствованию территориальной обороны являются:

1) **развитие системы управления территориальной обороной;**

2) совершенствование законодательства в сфере территориальной обороны;

3) **усиление боевого потенциала территориальных войск и повышение их боевых возможностей;**

4) **обеспечение оперативной совместимости для ведения совместной деятельности Вооруженных Сил, территориальных войск, других войск и воинских формирований, центральных и местных исполнительных органов, специальных государственных и правоохранительных органов при введении и обеспечении режимов чрезвычайного или военного положения».** [8, Глава 6, Параграф 1, п. 62]

В этой связи, видится целесообразным не ограничиваться существующей терминологией: «батальонная тактическая группа» или «ротная тактическая группа», а ввести новый термин: «специальная тактическая группа (СТГр)», как сводное вооруженное формирование, предназначенное для ведения самостоятельных действий по выполнению какой-то конкретной задачи (или задач) по предназначению, для достижения поставленной военной (военно-политической) цели.

Рассмотрим штатную ситуацию: СТГр выполняет задачу вдали от пункта постоянной дислокации (ППД), которая обеспечена связью со своим штабом в ППД, с взаимодействующими органами и местным штабом управления силами и средствами. В данной системе связи особых проблем нет, структурные подразделения группы обеспечены средствами для решения подобной задачи. Связь со взаимодействующими группами (подразделениями, частями вооруженных сил), внутри группы, оперативная связь с должностными лицами вышестоящего органа управления на территории пункта временной дислокации (ПВД) – все это организуется структурным подразделением связи самой СТГр путем создания сетей и направлений радио/телефонной связи и т.п. [9]

Для рассматрения каждого пункта теории построения ПСВР по значимости и содержанию необходимо проведение более углубленных не тольког теоретических, но и практических исследований. В том числе рассмотрение вопросов перехода к применению цифровых средств связи и интеграции их в единую автоматизированную систему управления войсками (АСУ В) вида вооруженных сил (далее Вооруженными силами и государства в целом). Так в обновленной Военной Доктрине нашего государства, указано: «п.11 Среди особенностей современных военных конфликтов отмечаются их активность, скоротечность, расширение масштабов, сфер ведения военных действий (в космическое и информационное пространство), а также высокое напряжение сил и ресурсов государства в вооруженной борьбе» [7, Глава 2, п.11].

В последующем на базе КСА СТГр возможно построение более крупных подразделений оперативно-тактического и оперативного уровня войск, которое может стать прототипом АСУ ВС в целом, и последующей её интеграции в систему управления военной организацией государства. Которое позволит реализовать основные меры по развитию системы управления военной организацией государства, к которым относятся:

1) **совершенствование деятельности Национального центра управления обороной и оснащение современными средствами связи и автоматизированными системами управления**;

2) **развертывание автоматизированных систем управления войсками,** оружием, ресурсами и обеспечение интеграции систем с информационными системами государственных органов и организаций, **входящих в состав военной организации государства**;

3) **поддержание эффективной работы** информационных ресурсов и систем, **инфраструктуры связи, сетей телекоммуникаций специального назначения для недопущения изоляции Верховного Главнокомандующего Вооруженными Силами и органов государственного управления**, а также **обеспечение их бесперебойной и устойчивой эксплуатации**;

4) внедрение отечественных технических и программных средств для информационных ресурсов и систем военного назначения [8, Глава 6, п.56].

Таким образом, более эффективная практическая реализация положений Военной доктрины Республики Казахстан на оперативном (оперативно-тактическом) уровнях требует внедрения цифровых средств связи и комплексов средств автоматизации, которые позволят максимально эффективно реализовать управление на всех уровнях вертикали силовых структур вплоть до уровня Национального центра управления обороной и повысят эффективность взаимодействия между ними.

Таким образом, организация связи в специальной тактической группе, которая может рассматриваться в качестве основы национальной системы военной радиосвязи требует проведения НИР, а практическая реализация - НИОКР. Объединить усилия этих двух направлений на начальном этапе

возможно через реализацию заявки на грантовое финансирование (программно-целевое финансирование).

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1 Военный энциклопедический словарь / М-во обороны Российской Федерации; [ред. комис. А. Э. Сердюков (пред.) и др.]. М. : Воениздат, 2007. 831 с.

2 А.В. Бойков, Е.Т. Кожеков, Некоторые аспекты связи в тактической группе, Сборник трудов Международной научно-практической конференции кафедры связи, с.37-42, 25 ноября 2022 г., https://www.viires.kz/ru/science/1548-sbornik_trudov_mezhdunarodnoj_nauchno_prakticheskoj_konferencii/

3 Министр обороны РК А. Джаксыбеков контролировал ход подведения итогов деятельности Сухопутных войск. https://online.zakon.kz/Document/?doc_id=31077984&pos=23;55#pos=23;55

4 Военнослужащие Казахстана участвуют в учении "Мирная миссия-2021", https://www.gov.kz/memleket/entities/mod/press/news/details/258602?lang=ru

5 Соединения и части Вооруженных сил приступили к подготовке ротных тактических групп, https://dknews.kz/ru/v-strane/245551-soedineniya-i-chasti-vooruzhennyh-sil-pristupili-k

6 Н.Ж. Асылов, Р.С. Садуев, В.В. Портнов, К.Ж. Койчыкулов, Т.А. Жубатов, Е.Р. Абдуллаев, Отчет о НИР, Научное обоснование форм и методов вооруженной борьбы с НВФ и разработка новых методов управления подразделениями в ходе подготовки и ведения боевых действий с НВФ, (промежуточный), Отчет 59 с., 1 ч., Алматы 2019, УДК 355/359, https://www.ncste.kz/assets/report_files/2019/AP05130810-OT-19/ru_55111__276483_1572455087.docx

7 Военная доктрина Республики Казахстан, https://www.akorda.kz/ru/security_council/national_security/voennuyu-doktrinu-respubliki-kazahstan

8 В.Г. Иванов, В.Н. Лукьянчик, Об эволюции теории и практики построения существующих систем связи военного назначения на основе создания мультиконвергентной системы связи группировки войск (сил) на театре военных действий, статья ВОЕННАЯ МЫСЛЬ 2021, №1, с. 66-78

9 https://skillbox.ru/media/education/taksonomiya-bluma-chto-eto-takoe-i-zachem-ona-pedagogam-i-metodistam/

10 https://4brain.ru/blog/taksonomija-chto-eto-takoe-primery-i-principy/

11 https://www.google.com/imgres?imgurl=http://linoit.com/entry/image/26457498&tbnid=Blw3kcpNho18DM&vet=1&imgrefurl=http://linoit.com/users/azejnelova/canvase

s/%25D0%25A2%25D0%25B0%25D0%25BA%25D1%2581%25D0%25BE%25D0%25BD%25D0%25BE%25D0%25BC%25D0%25B8%25D1%258F%2520%25D0%2591%25D0%25BB%25D1%2583%25D0%25BC%25D0%25B0&docid=hF45Xe1jFB9FfM&w=500&h=375&source=sh/x/im/m1/1&kgs=dff33a9c35adf3c8&shem=trie

ЗАКЛЮЧИТЕЛЬНОЕ СЛОВО

А.У.Жантлесов
полковник, соруководитель
научного проекта

Уважаемые участники
Межведомственной научно-практической конференции!

Подходит к завершению наша совместная работа на Межведомственной научно-практической конференции «Разработка оборудования для создания национальной системы военной радиосвязи».

Благодарю всех участников конференции за плодотворное взаимодействие нашего научного сообщества и обсуждение перспектив его развития в дальнейшем.

Уверен, что обсуждение актуальных вопросов реализации государственной политики в области радиосвязи, обеспечения перспективного развития отрасли, а также координаций усилий по разработке и производству радиостанций в Республике Казахстан внесет существенный вклад не только в повышение эффективности современного облика вооруженных сил, но и в дальнейшее развитие научных исследований.

Нам необходимо принять резолюцию по итогам проведения конференции, в которую предлагается включить следующие пункты:

– отметить актуальность и ценность выполненных исследований в рамках грантового финансирования на 2022-2024 годы по теме ИРН AP 148029/0222 «Разработка оборудования для создания национальной системы военной радиосвязи»;

– редакционной коллегией подготовить к изданию сборник статей с докладами участников конференции.

Предлагаю данный проект резолюции утвердить общим собранием участников конференции.

В завершении хочу пожелать всем участникам конференции дальнейших научных достижений и творческих успехов.

Всем спасибо за дружную и плодотворную работу на межведомственной научно-практической конференции!

До новых встреч!

СОДЕРЖАНИЕ

РАЗРАБОТКА ОБОРУДОВАНИЯ ДЛЯ СОЗДАНИЯ НАЦИОНАЛЬНОЙ СИСТЕМЫ ВОЕННОЙ РАДИОСВЯЗИ

Сборник межведомственной научно-практической конференции
(в рамках грантового финансирования на 2022-2024 гг.)
ИРН AP 148029/0222

Редакционно-издательское отделение
ТОО «R&D центр «Казахстан инжиниринг»

Отп. __ экз.
Исп. Жантлесов А.У.
Отп. Несипова С.С.
Тел 8 (7172) 32 21 39