ТЕЛЕКОММУНИКАЦИИ и СВЯЗЬ

№2 (02) 2024

ТЕМА НОМЕРА:

ЗАЩИТА ИНФОРМАЦИОННЫХ РЕСУРСОВ СИСТЕМ УПРАВЛЕНИЯ РОБОТОТЕХНИЧЕСКИМИ КОМПЛЕКСАМИ

WWW.TELEMIL.RU

DOI: 10.24682/3034-4050

ТЕЛЕКОММУНИКАЦИИ И СВЯЗЬ

НАУЧНЫЙ РЕЦЕНЗИРУЕМЫЙ ЖУРНАЛ

№2 (02) 2024 г.

Выходит 6 раз в год

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

Журнал принимает к публикации статьи по специальностям перечня научных специальностей 6.0.0.

Учредитель и издатель

ФГБУ «16 Центральный научно-исследовательский испытательный институт Министерства Обороны РФ»

(Военно-научный комитет Главного управления связи Вооружённых Сил Российской Федерации)

Над номером работали:

Г. И. Макаренко – *шеф-редактор,* Н. В. Селезенев – *отв. секретарь,* В. А. Пестерева – *верстка,* А.М. Старков – *маркетинг и подписка*

Подписано к печати 20.10.2024 г.
Общий тираж 120 экз. Цена свободная

Адрес: 141006, г. Мытищи Московской обл., 1-й Русаковский пер, д. 1.
E-mail: editor@telemil.ru тел.: +7 (985) 939-75-01.

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

СОДЕРЖАНИЕ

Подписка на журнал осуществляется в 2024 году через редакцию журнала

DOI:10.24682/3034-4050-2024-2-1-1

АНАЛИЗ ТЕХНИЧЕСКИХ ВОЗМОЖНОСТЕЙ КОМПЛЕКСОВ РАДИОСВЯЗИ ШЕСТОГО ПОКОЛЕНИЯ ТАКТИЧЕСКОГО ЗВЕНА УПРАВЛЕНИЯ

Пшеничников А.В.[1], Бородулин Р.Ю.[2], Лященко С.А.[3]

DOI:10.24682/3034-4050-2024-2-2-5

Ключевые слова: *комплексы радиосвязи, тактического звена управления, сеть прямых связей, сеть радиодоступа, сеть распределенная, помехозащищенность, сеть радиосвязи.*

Аннотация. *В данной статье рассмотрены основные требования, предъявляемые к комплексам радиосвязи 6-го поколения и их технические возможности с точки зрения построения автоматизированных систем радиосвязи, требованиям по помехозащищенности и скрытности. Рассматривается интегрированная сеть радиосвязи тактического звена управления, исходя из следующих составляющих: организации сетей прямых связей, сетей радиодоступа и сетей распределения. Рассматриваются возможности и технические характеристики радиостанций «Азарт» и «Аксион».*

Цель работы: *состоит в анализе технических возможностей комплексов радиостанций 6-го поколения тактического звена управления с точки зрения предоставления спектра услуг, характерных для цифровой радиосвязи.*

Результаты *исследования: В статье проведен анализ режимов работы, используемых в средствах радиосвязи 6-го поколения для обеспечения требуемой помехозащищенности и разведзащищенности системы связи, а также, применяемых сетевых технологий. Были проанализированы радиосредства 6-го поколений, применяемые для построения радиосетей в зоне проведения специальной военной операции, а также режимы работы, применяемые в радиосредствах для обеспечения помехозащищенности и разведзащищенности системы связи, технологии по построению сетей радиосвязи. Выявлены достоинства и недостатки применения радиостанций для построения сетей радиосвязи. На основе проведенного анализа обоснованы перспективы развития радиосредств 6го поколения для построения автоматизированной сети радиосвязи, а также предложены направления развития средств радиосвязи для построения перспективной автоматизированной сети радиосвязи. В статье отражены актуальные вопросы опыта применения средств радиосвязи в зоне проведения специальной военной операции. Указаны положительные и отрицательные стороны использования радиостанций для построения сетей радиосвязи. По основным проблемным вопросам предложены возможные пути решения.*

Научная новизна: *впервые рассматривались комплексы радиосредств с точки зрения построения автоматизированных сетей радиосвязи, требований по помехозащищенности, по сетевым и радиотехнологиям.*

Современные средства радиосвязи тактического звена управления (ТЗУ), стоящие на снабжении ВС РФ и применяемые в зоне специальной военной операции (СВО), реализуют принципы построения, базирующиеся на совмещении передовых технологий в области радио и сетевых систем. Такой подход к построению средств радиосвязи предполагает их реализацию на платформе программно-определяемого радио. Следовательно, современные средства радиосвязи, кроме высоких характеристик радиотрактов, должны удовлетворять требованиям по построению автоматизированных сетей радиосвязи [1].

Другим аспектом, определяющим требования к современным средствам радиосвязи ТЗУ, является учет деструктивных воздействий противника. Необходимо учесть особенности построения современных систем воздействия, основанных на динамическом расширении спектра воздействий в зависимости от режимов функционирования радиосредств. Поэтому к средствам радиосвязи ТЗУ дополнительно должны предъявляться требования по помехозащищенности [2].

Опыт проведения СВО показал, что немаловажным требованием к средствам радиосвязи ТЗУ является их способность функционировать скрытно от радиоразведки противника [3]. Таким образом, определяются требования к радиосредствам ТЗУ по сетевым и радиотехнологиям, скрытности и помехозащищенности. Основываясь на вышеизложенном, в данной статье

[1]Пшеничников Александр Викторович, доктор технических наук, профессор, начальник кафедры радиосвязи Военной академии связи им. С.М. Буденного, г. Санкт-Петербург, Россия. E-mail: siracooz77@mail.ru

[2]Бородулин Роман Юрьевич, доктор технических наук, профессор, доцент кафедры радиосвязи Военной академии связи им. С.М. Буденного, г. Санкт-Петербург, Россия. E-mail: borodulkomon@yandex.ru

[3]Лященко Станислав Алексеевич, адъюнкт кафедры радиосвязи Военной академии связи им. С.М. Буденного, г. Санкт-Петербург, Россия. E-mail: parij61@mail.ru

проведем анализ технических возможностей комплексов радиосвязи ТЗУ 6-го поколения на соответствие сформулированным требованиям.

Интегрированная сеть радиосвязи ТЗУ, организованная на основе радиосредств 6-го поколения, включает в себя три относительно самостоятельные по принципам организации, но единые по технической основе, составляющие:

- сеть прямых связей (СПС);
- сеть радиодоступа (СРД);
- сеть распределенную (СР).

Сеть прямой связи представляет собой сеть, строящуюся на основе прямого взаимодействия узлов, находящихся в зоне радиовидимости. СПС применяется при отсутствии требуемой связности сети в зависимости от помеховой обстановки, условий расположения и движения корреспондентов на местности.

Сеть радиодоступа имеет архитектуру «абонентский терминал — базовая радиостанция». СРД строится на базе портативных и индивидуальных радиосредств, а также возимых радиостанций. Возимые радиостанции должны использоваться в качестве шлюзов для интеграции абонентов СРД в транспортную сеть распределенной сети. СРД обеспечивает организацию открытой или криптографически защищенной телефонной симплексной и дуплексной радиосвязи и передачи данных между несколькими корреспондентами одновременно с возможностью адресного вызова каждого из них.

СР организуется как децентрализованная, адаптивно-меняющаяся и самовосстанавливающаяся телекоммуникационная сеть произвольной топологии на основе пакетных технологий с коммутацией и маршрутизацией на канальном и сетевом уровнях. СР организуется в автоматическом режиме при появлении узлов сети в пределах радиовидимости друг друга. Ключевыми свойствами СР является динамическая маршрутизация и автоматическая ретрансляция — возможность передачи информации между двумя узлами, находящимися вне зоны доступности друг друга, через промежуточные узлы. При этом маршруты, по которым осуществляется ретрансляция информации между объектами СР, определяются автоматически, исходя из текущей топологии сети и качества связей между радиостанциями.

Средства радиосвязи 6-го поколения представлены комплексами «Азарт» и «Аксион». Общими принципами построения данных комплексов, были следующие:

- применение единой унифицированной платформы с возможностью программного управления конфигурацией радиостанций;
- возможность обеспечения радиосвязи в диапазонах частот от 1,5 до 2500 МГц;
- предоставление широкого спектра услуг, характерного для цифровой радиосвязи.

Таким образом, отличительной особенностью радиосредств 6-го поколения является технология программно-определяемого радио, обеспечивающая основные способы формирования и обработки радиосигналов. Такое построение определяет широкие возможности по внедрению в радиостанции различных видов радиосигналов и режимов функционирования.

Радиостанции комплекса «Азарт» учитывают воздействие современных систем деструктивных воздействий, в частности, скорость ППРЧ составляет 20 000 скачков в секунду, что физически исключает постановку наиболее эффективных помех «в след», затрудняет применение имитационных помех. Кроме того, реализация режима ППРЧ в комплексе 6-го поколения предполагает возможность работы в широкой полосе частот, что снижает эффективность воздействия преднамеренных помех. Однако, негативным следствием высоких показателей помехозащиты за счет увеличения широкополосности, является ухудшение характеристик радиотрактов, что определяет некоторое снижение дальности радиосвязи.

Для увеличения дальности радиосвязи в радиостанциях комплекса «Азарт» реализован режим многопролетной ретрансляции, а также подключение внешних усилителей мощности. Для создания обширной сети передачи голосовых и текстовых данных на значительных расстояниях применяют режим IP-ретрансляции.

Радиостанции комплекса «Азарт» обеспечивают взаимодействие с транкинговыми сетями профессиональной связи стандарта TETRA (TErrestrial Trunked RAdio) при наличии базовой и коммутационной инфраструктуры [4]. Данный стандарт предусматривает реализацию временного разделения каналов (для чего может выделяться 4 тайм-слота).

В таблице 1 представлены основные характеристики радиостанций комплекса «Азарт», принятых на снабжение ВС РФ.

Таблица 1.

Основные характеристики	Р-187-В				Р-187-П1	Р-187-П2
	ДКМВ	МВ	ДМВ1	ДМВ2	МВ-ДМВ1	МВ-ДМВ1
Диапазон рабочих частот, МГц	1,5…30	30…220	220…520	520…2500	27…520	27…1000
Мощность передатчика, Вт	100	40/100	40	10	4	4
Виды радиосетей	СПС	СПС, СРД,	СПС, СРД, СРД	СПС, СР	СПС, СРД	СПС, СРД
Скорость ППРЧ, ск/с	100	20000	СПС/СРД 20000	СР-500 СПС-20000	20000	20000
Скорость передачи данных, кбит/с	до 9,6	до 256	до 2048	до 32 786	до 320	до 320

Из представленных данных следует, что возимая радиостанция Р-187-В обеспечивает возможность построения сети радиосвязи, как единой интегрированной сети связи, включающей сеть прямых связей, сеть радиодоступа и распределенную сеть с ячеистой топологией.

Радиостанция обеспечивает:

- многоканальную связь;
- ретрансляцию аналоговых и цифровых сигналов, в том числе междиапазонную с временным разделением каналов;
- передачу речи в симплексном режиме ведения переговоров между несколькими абонентами;
- циркулярную связь;
- передачу речи в дуплексном режиме между несколькими абонентами одновременно (конференцсвязь);
- передачу высокоскоростных данных;
- передачу видеоизображения (видеоконференцсвязь в диапазонах ДМВ1 и ДМВ2);
- передачу коротких текстовых сообщений; файловый обмен;
- сопряжение с аппаратурой внутренней связи и коммутации объектов.
- Портативная радиостанция Р-187-П1 обеспечивает передачу речевой преобразованной в цифровую форму информации в МВ-ДМВ диапазонах;
- передачу данных со скоростью: в МВ диапазоне — до 64 кбит/с; в ДМВ1 диапазоне в узкополосном режиме — до 256 кбит/с, в широкополосном режиме — от 2048 до 8192 кбит/с.

Новая прошивка портативных и возимых радиостанций комплекса «Азарт» реализует режим «Аксион» для встречной работы с радиостанциями соответствующего комплекса.

Портативная радиостанция Р-187-П2 имеет расширенный диапазон частот (27-1000 МГц), позволяет организовать встречную работу со всеми имеющимися средствами радиосвязи, в том числе с радиостанциями Р-187-П1 и Р-187-В. Она обеспечивает ретрансляцию с временным разделением каналов; передачу речи в дуплексном режиме в стандарте TETRA; возможность маскирования речи; прием и передачу текстовых сообщений, навигационной информации.

В настоящее время на снабжение ВС РФ принят возимый вариант радиостанций комплекса «Аксион». Возимые радиостанции «Аксион-В» обеспечивают работу в командных сетях прямых связей, ячеистых распределенных сетях обмена данными (СР), сетях радиодоступа пеших абонентов в единую сеть связи (СРД), доступ в гражданские сотовые сети связи.

Основными возможностями радиостанций «Аксион-В» являются гибкая модульная конфигурация, высокие характеристики электромагнитной совместимости радиосредств, независимая работа в четырех радиосетях, встроенная ГЛОНАСС/GPS навигация с электронной картой; передача-прием текстовых сообщений и видео, дистанционное управление.

В таблице 2 представлены основные технические характеристики радиостанций комплекса «Аксион-В».

Таблица 2.

Основные характеристики	Аксион-В			
	ДКМВ	МВ	ДМВ1	ДМВ2
Диапазон рабочих частот, МГц	1,5…30	30…220	220…520	520…2500
Мощность приемопередатчика, Вт	100	40	40	10
Шаг сетки частот, Гц	0,7	1	1	1
Виды радиосетей	СПС	СПС, СРД	СПС, СРД, СР	СПС, СР
Число узлов в сети	—	—	до 256	до 256
Дальность связи, км	350	20	16	6
Скорость ППРЧ, $с^{-1}$	100	1200	1200	1200
Скорость передачи данных, кбит/с	до 9,6	до 256	до 2048	до 32 768
Чувствительность приемника, мкВ	0,7	1	1	1

Таким образом, технические решения, примененные в радиосредствах 6-го поколения, предоставляют возможность организовывать интегрированные сети радиосвязи. Сетевые решения при этом основаны на интеграции разнородных сетей посредством единой адресации и реализации протокола межканальной (межсетевой) маршрутизации.

Основные направления развития средств радиосвязи ТЗУ основываются на реализации свойств когнитивных радиосистем. При этом перспективные средства радиосвязи ТЗУ должны обладать системой управления выделенными ресурсами для обеспечения помехозащиты и скрытности функционирования радиолиний от сложных динамических систем деструктивных воздействий.

Альтернативным аспектом развития средств радиосвязи ТЗУ следует выделить построение полносвязных, динамически управляемых сетей радиосвязи. При этом целесообразно реализовать единый стандарт перспективных средств радиосвязи ТЗУ на основе современных технологий радиосвязи.

Литература

1. Пшеничников А.В. Модели и методы помехозащиты радиолиний: монография. – СПб.: ВАС, 2017. – 136 с.
2. Беккиев А.Ю., Борисов В.И. Базовые принципы создания помехозащищенных систем радиосвязи // Теория и техника радиосвязи. – 2014. №1. С. 5-18.
3. Манаенко С.С., Дворников С.В., Пшеничников А.В. Теоретические аспекты формирования сигнальных конструкций сложной структуры // Информатика и автоматизация. 2022. Т. 21. № 1. С. 68-94.
4. Лохвицкий М.С. Мобильная связь: стандарты, структуры, алгоритмы, планирование / М.С. Лохвицкий, А.С. Сорокин, О.А. Шорин. – Москва: Научно-техническое издательство «Горячая линия – Телеком», 2018. – 264 с.

ANALYZING THE TECHNICAL CAPABILITIES OF SIXTH-GENERATION TACTICAL COMMAND AND CONTROL RADIO COMMUNICATION COMPLEXES

Pshenichnikov A.V.[1], Borodulin R. Y.[2], Lyashchenko S. A.[3]

Keywords: *Radio communication complexes, tactical control link, direct link network, radio access network, distributed network, noise immunity, radio communication network.*

Abstract: *In this article the basic requirements for the 6th generation radio communication complexes and their technical capabilities from the point of view of building automated radio communication systems, requirements for interference protection and stealth are considered. The integrated radio communication network of tactical control link is considered, based on the following components: organization of direct communication networks, radio access networks and distribution networks. Possibilities and technical characteristics of radio stations «Azart» and «Aksion» are considered.*

[1]Alexander V. Pshenichnikov, Dr.Sc., Professor, Head of the Radio Communications Department, Budenniy Military Academy of Communications, Moscow, Russia. S.M. Budyonny Military Academy of Communications, St. Petersburg, Russia. St. Petersburg, Russia. E-mail: siracooz77@mail.ru

[2]Roman Yu. Borodulin, , Dr.Sc, Professor, Associate Professor of the Department of Radio Communications, S.M. Budyonny Military Academy of Communications, St. Petersburg, Russia. S.M. Budyonny Military Academy, St. Petersburg, Russia. St. Petersburg, Russia. E-mail: borodulkomon@yandex.ru

[3]Stanislav A. Lyashchenko, Associate Professor, Radio Communications Department, S.M. Budenniy Military Academy, St. Petersburg, Russia. S.M. Budyonny Military Academy, St. Petersburg, Russia. St. Petersburg, Russia. E-mail: parij61@mail.ru

ИССЛЕДОВАНИЕ ВОПРОСОВ ПРОИЗВОДИТЕЛЬНОСТИ МЕШ-СЕТЕЙ В СИСТЕМАХ СВЯЗИ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

Прядкин А. М.[1] , Гришанов И. С.[2]

DOI:10.24682/3034-4050-2024-2-6-12

Ключевые слова: *беспроводные технологии, пропускная способность, управление, меш-сеть, производительность, время реакции, протокол, расширяемость, масштабируемость.*

Цель исследования. *Разработать (обосновать) предложения, способствующие эффективному применению меш-сетей в системах специального назначения при, на основе технических решений в области управления и связи.*

Метод исследования. *Аналитический с привлечением математического аппарата для получения зависимости времени передачи сообщений различной длины от пропускной способности канала.*

Результатом *исследования является анализ основных сетевых характеристик производительности распределенных систем с целью разработки рекомендаций по повышению производительности функционирования mesh-сетей. В работе был произведен анализ зависимостей времени передачи сообщений различной длины от пропускной способности канала, времени загрузки файла от его размеров, а также сравнение различных сетевых технологий с точки зрения задержки передачи и джиттера, в результате которых были сделаны выводы об оптимальном размере длины пакета в mesh-сети, ее производительности и задержках передачи относительно различных вариантов Ethernet-технологии. Произведен анализ зарубежных и отечественных разработок в области маршрутизации пакетов в mesh-сетях, сформулированы основные требования к процессу маршрутизации, обеспечивающие производительную работу сети.*

Научная новизна *заключается в комплексном анализе и сравнении различных аспектов беспроводных пакетных технологий обмена данными для мобильных устройств, включая WiMAX и Wi-Fi Mesh, а также в детальном рассмотрении протокола 802.11s, который является передовым стандартом в области mesh-сетей.*

Введение

Беспроводные технологии доступа с пакетной коммутацией предназначены для обмена информацией между мобильными абонентами. Эта задача может быть реализована с использованием двух систем двух стандартов: Wi-Fi Mesh, и WiMAX. WiMAX является централизованной системой, основанной на создании базовых станций, которые концентрируют трафик с определенного сектора в одной точке. Технология меш позволяет полностью децентрализовать архитектуру сети и увеличить зону ее действия. Цель разработки стандарта IEEE 802.11s — обеспечение автоматической маршрутизации между узлами сети Wi-Fi, в которой каждый узел для передачи информации способен задействовать соседние, используя прыжковый механизм перераспределения трафика и не более 5% пропускной способности канала. Стандарт IEEE 802.11s регламентирует протоколы обнаружения, идентификации и установления соединения между соседними устройствами. Совокупность устройств, работающих в сети по стандарту IEEE 802.11s, образует меш-сеть.

Таким образом, реализуется концепция постепенного масштабирования сети. Начав развитие сети в одной точке, в идеале можно неограниченно увеличивать зону ее действия, просто добавляя новые устройства. Прокладки дополнительных коммуникаций не требуется.

Системы WiMAX и Wi-Fi Mesh имеют различный подход к построению городской сети — от глобального охвата до постепенного развития. Обычно они дополняют друг друга, а не конкурируют между собой. WiMAX предназначена обеспечивать передачу данных в районе сосредоточения абонентов, а Wi-Fi Mesh в движении и т. д.

Сетевые характеристики, влияющие на производительность mesh-сетей

Потенциально высокая производительность — это одно из основных свойств распределенных систем, к которым относятся меш-сети. Это свойство обеспечивается возможностью параллельной передачи трафика между несколькими узлами сети.

[1] Прядкин Андрей Михайлович, адъюнкт кафедры боевого применения войск связи Военной академии связи имени Маршала Советского Союза С.М. Буденного, Санкт-Петербург. E-mail: tbilnovspb28@mail.ru

[2] Гришанов Илья Сергеевич, аспирант кафедры «Электрическая связь» Петербургского государственного университета путей сообщения имени Александра I, Санкт-Петербург. E-mail: igrissh@zohomail.com

Существует несколько основных характеристик производительности сети:

- время реакции;
- пропускная способность;
- задержка передачи и вариация задержки передачи.

Пропускная способность отражает объем данных, переданных сетью или ее частью в единицу времени. Пропускная способность не является пользовательской характеристикой, так как она говорит о скорости выполнения внутренних операций сети — передачи пакетов данных между узлами сети через различные коммуникационные устройства. Зато она непосредственно характеризует качество выполнения основной функции сети — передачи сообщений и поэтому чаще используется при анализе производительности сети, чем время реакции.

Пропускная способность измеряется либо в битах в секунду, либо в пакетах в секунду. Пропускная способность может быть мгновенной, максимальной и средней.

Средняя пропускная способность вычисляется путем деления общего объема переданных данных на время их передачи, причем выбирается достаточно длительный промежуток времени — час, день или неделя.

Мгновенная пропускная способность отличается от средней тем, что для усреднения выбирается очень маленький промежуток времени — например, 10 мс или 1 с.

Максимальная пропускная способность — это наибольшая мгновенная пропускная способность, зафиксированная в течение периода наблюдения.

Чаще всего при проектировании, настройке и оптимизации сети используются такие показатели, как средняя и максимальная пропускные способности. Средняя пропускная способность отдельного элемента или всей сети позволяет оценить работу сети на большом промежутке времени, в течение которого в силу закона больших чисел пики и спады интенсивности трафика компенсируют друг друга. Максимальная пропускная способность позволяет оценить возможности сети справляться с пиковыми нагрузками, характерными для особых периодов работы сети, например утренних часов, когда сотрудники предприятия почти одновременно регистрируются в сети и обращаются к разделяемым файлам и базам данных.

Пропускную способность можно измерять между любыми двумя узлами или точками сети, например между узлом сети и сервером, между входным и выходным портами маршрутизатора. Для анализа и настройки сети важно знать данные о пропускной способности отдельных элементов сети.

Важно отметить, что из-за последовательного характера передачи пакетов различными элементами сети общая пропускная способность сети любого составного пути в сети будет равна минимальной из пропускных способностей составляющих элементов маршрута. Для повышения пропускной способности составного пути необходимо в первую очередь обратить внимание на самые медленные элементы. Следует подчеркнуть, что если передаваемый по составному пути трафик будет иметь среднюю интенсивность, превосходящую среднюю пропускную способность самого медленного элемента пути, то очередь пакетов к этому элементу будет расти теоретически до бесконечности, а практически — до тех пор, пока не заполниться его буферная память, а затем пакеты просто начнут отбрасываться и теряться.

Обычно при определении пропускной способности сегмента или устройства в передаваемых данных не выделяются пакеты какого-то определенного пользователя, приложения или компьютера — подсчитывается общий объем передаваемой информации. Тем не менее, для более точной оценки качества обслуживания такая детализации желательна, и в последнее время системы управления сетями все чаще позволяют ее выполнять.

Время реакции сети является интегральной характеристикой производительности сети с точки зрения пользователя. В общем случае время реакции определяется как интервал времени между возникновением запроса пользователя к какой-либо сетевой службе и получением ответа на этот запрос.

Очевидно, что значение этого показателя зависит от типа службы, к которой обращается пользователь, от того, какой пользователь и к какому серверу обращается, а также от текущего состояния элементов сети — загруженности сегментов, коммутаторов и маршрутизаторов, через которые проходит запрос, загруженности сервера и т. п.

Поэтому целесообразно использовать также и средневзвешенную оценку времени реакции сети, усредняя этот показатель по пользователям, серверам и времени дня (от которого в значительной степени зависит загрузка сети).

Время реакции сети обычно складывается из нескольких составляющих. В общем случае в него входит время подготовки запросов на клиентском компьютере, время передачи запросов между клиентом и сервером через сегменты сети

и промежуточное коммуникационное оборудование, время обработки запросов на сервере, время передачи ответов от сервера клиенту и время обработки получаемых от сервера ответов на клиентском компьютере.

Знание сетевых составляющих времени реакции дает возможность оценить производительность отдельных элементов сети, выявить узкие места и в случае необходимости выполнить модернизацию сети для повышения ее общей производительности.

Задержка передачи определяется как задержка между моментом поступления пакета на вход какого-либо сетевого устройства или части сети и моментом появления его на выходе этого устройства. Этот параметр производительности по смыслу близок ко времени реакции сети, но отличается тем, что всегда характеризует только сетевые этапы обработки данных, без задержек обработки компьютерами сети. Обычно качество сети характеризуют величинами максимальной задержки передачи и вариацией задержки. Не все типы трафика чувствительны к задержкам передачи, во всяком случае, к тем величинам задержек, которые характерны для компьютерных сетей, — обычно задержки не превышают сотен миллисекунд, реже — нескольких секунд. Такого порядка задержки пакетов, порождаемых файловой службой, службой электронной почты или службой печати, мало влияют на качество этих служб с точки зрения пользователя сети. С другой стороны, такие же задержки пакетов, переносящих голосовые данные или видеоизображение, могут приводить к значительному снижению качества предоставляемой пользователю информации — возникновению эффекта «эха», невозможности разобрать некоторые слова, дрожание изображения и т. п.

Пропускная способность и задержки передачи являются независимыми параметрами, так что сеть может обладать, например, высокой пропускной способностью, но вносить значительные задержки при передаче каждого пакета. Пример такой ситуации дает канал связи, образованный геостационарным спутником. Пропускная способность этого канала может быть высокой, например 2 Мбит/с, в то время как задержка передачи всегда составляет не менее 0,24 с, что определяется скоростью распространения сигнала (около 300 000 км/с) и длиной канала (72 000 км).

Стандарт IEEE 802.11s требует, чтобы все устройства в меш-сети поддерживали метрику **времени передачи в канале** (Airtime Link Metric). Эта обязательная метрика необходима для совместимости устройств.

Она задается формулой

$$t = (R + B / r) / (1 - e),$$

где R и B — константы, определенные стандартом для различных физических реализаций (802.11a, 802.11b): B — число битов в тестовом пакете (8192), R — накладные расходы доступа к каналу, которые включают в себя заголовки пакетов, кадры протоколов доступа и т. д.; r — скорость передачи данных в канале (Мбит/с); e — вероятность возникновения ошибки (измеряется экспериментально на пакетах длиной B). Эта метрика представляет собой оценку времени передачи (в секундах) пробного пакета длиной Bt с учетом возможных ретрансляций при потерях в канале. Способ определения параметров r и ef в стандарте не приводится, однако можно предположить, что для этого должна использоваться периодическая рассылка пробных пакетов длиной Bt = 8192 бит. Рассматривались скорости от 12 до 54 мбит/с. На рисунке 1 приведены графики зависимости времени передачи сообщения по каналу от его пропускной способности при передачи пробных сообщений различной длины.

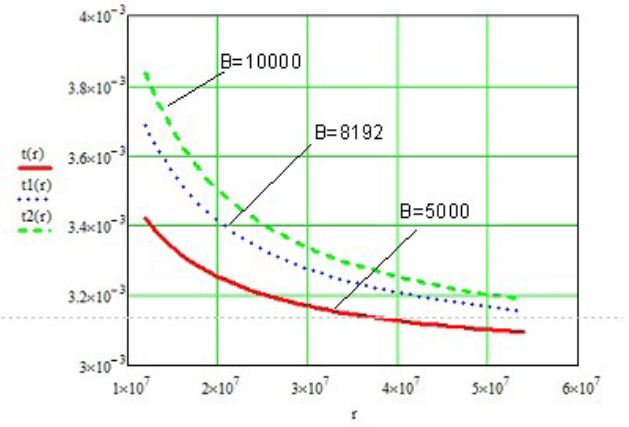

Рис.1.Графики зависимости времени передачи сообщения по каналу от его пропускной способности при передачи пробных сообщений различной длины

Как следует из приведенных графиков, время задержки при одной и той же пропускной способности канала может изменяться в значительных пределах. При этом наибольший разброс значений наблюдается при меньших значениях пропускной способности. Отсюда следует вывод о целесообразности передачи сообщений в меш-сетях пакетами небольшого размера.

В [4] приведены результаты измерений для проводного Ethernet и для 802.11n для случая, когда к точке доступа подключены 20 пользователей из которых 10 активны. На рисунке 2 приведены графики зависимости среднего времени загрузки файла от его размеров.

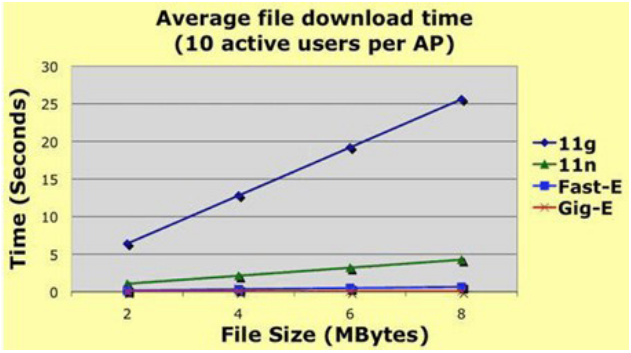

Рис. 2. Среднее время загрузки файла

Из графиков следует, что в зависимости от размеров файла происходит линейное нарастание времени загрузки, которое при размере файла в 8 Мбайт достигает 25 секунд при технологии 802.11g, что в несколько раз больше, чем при использовании технологий семейства Ethernet.

Для задач передачи трафика реального времени критическим параметром является время задержки. Согласно рекомендациям ITU задержка отклика не должна превышать 150 мсек. Результаты сравнения различных сетевых технологий с точки зрения задержки передачи представлено на рисунке 2.

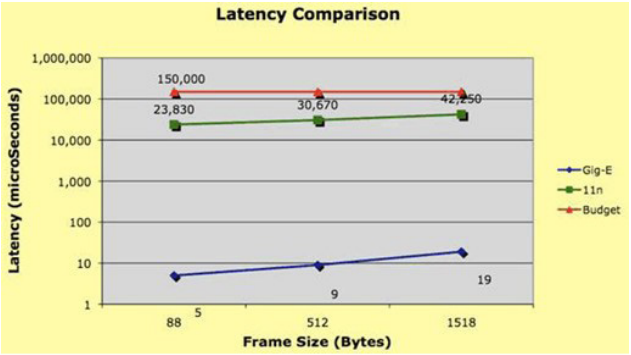

Рис.3. Сравнение задержек для Ethernet и 802.11

По данному параметру технология GigabitEthernet значительно превосходит стандарт 802.11n, что не удивительно с учетом пропускной способности обеих технологий.

Для мультимедийных приложений важным параметром является также вариация времени задержки (или джиттер), который не должен превышать 30мсек. Результаты сравнения разных технологий по временному разбросу представлены на рисунке 3.

Из графика следует, что несмотря на превосходство технологии GigabitEthernet, стандарт 802.11 так же может использоваться для передачи мультимедийных сообщений, поскольку вариация времени задержки не превышает 10 мс.

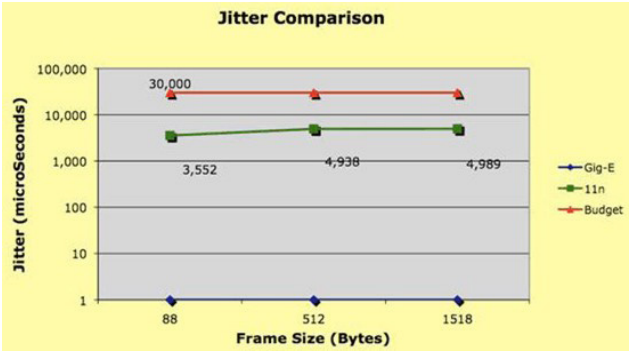

Рис. 4. Временной разброс отклика для Ethernet и 802.11

Термины **расширяемость и масштабируемость** иногда используют как синонимы, но это неверно — каждый из них имеет четко определенное самостоятельное значение.

Расширяемость (extensibility) означает возможность сравнительно легкого добавления отдельных элементов сети (пользователей, компьютеров, приложений, служб), наращивания длины сегментов сети и замены существующей аппаратуры более мощной. При этом принципиально важно, что легкость расширения системы иногда может обеспечиваться в некоторых весьма ограниченных пределах. Например, локальная сеть Ethernet, построенная на основе одного сегмента толстого коаксиального кабеля, обладает хорошей расширяемостью, в том смысле, что позволяет легко подключать новые станции. Однако такая сеть имеет ограничение на число станций — их число не должно превышать 30–40. Хотя сеть допускает физическое подключение к сегменту и большего числа станций (до 100), но при этом чаще всего резко снижается производительность сети. Наличие такого ограничения и является признаком плохой масштабируемости системы при хорошей расширяемости.

Масштабируемость (scalability) означает, что сеть позволяет наращивать количество узлов и протяженность связей в очень широких пределах, при этом производительность сети не ухудшается. Для обеспечения масштабируемости сети приходится применять дополнительное коммуникационное оборудование и специальным образом структурировать сеть. Например, хорошей масштабируемостью обладает многосегментная сеть, построенная с использованием коммутаторов и маршрутизаторов и имеющая иерархическую структуру связей. Такая сеть может включать несколько тысяч компьютеров и при этом обеспечивать каждому пользователю сети нужное качество обслуживания.

Анализ существующих протоколов маршрутизации меш-сетей

В связи с тем, что стандарт меш-сетей находится в стадии доработки, многие ведущие фирмы мира предлагают свои собственные протоколы маршрутизации. Известно довольно много различных разработок, в большинстве своем они лишь поверхностно описаны разработчиками. Так, в беспроводной платформе Cisco Aironet 1520 Series фирмы Cisco Systems используется проприетарный протокол маршрутизации Cisco's Adaptive Wireless Path Protocol (AWPP). Логика протокола скрыта, однако по косвенным данным можно предположить, что он базируются на одной из версий HWMP, работающего в проактивном режиме. Управление и мониторинг сети, т. е. функция корневого узла, реализует специальное устройство — контроллер беспроводной сети Cisco Wireless LAN Controller, компания рекомендует использовать в меш-сетях контроллеры серии 4400. Довольно много информации о маршрутизации в своих сетях представила корпорация Microsoft. Компания разработала реактивный протокол маршрутизации, основанный на алгоритме динамической маршрутизации источника DSR (Dynamic Source Routing). Он очень похож на протокол Ad Hoc On Demand Distance Vector (т. е. на HWMP), с той лишь разницей, что для маршрутизации от источника до адресата используется маршрутная таблица источника, а не промежуточных узлов. Компания Microsoft предложила и протокол маршрутизации источника по качеству канала (Link Quality Source Routing, LQSR), который является адаптацией DSR на виртуальный второй с половиной уровень эталонной сетевой модели взаимодействия открытых систем OSI. Введение промежуточного уровня предпринято компанией, чтобы сделать протокол прозрачным для более высокого уровня, но при этом обеспечить его корректную работу при переходе между проводной и беспроводной сетями. К предложенному протоколу прилагается пять различных метрик: количество шагов; время на получение ответа (Round Trip Time, RTT); время на посылку пробного пакета от источника до адресата и обратно (Packet Pair); ожидаемое время передачи (Expected Transmission Time, ETT) и взвешенное совокупное ожидаемое время передачи (Weighted Cumulative ETTs, WCETT). Помимо основного протокола LQSR, есть версия многоинтерфейсного LQSR (MR-LQSR — MultiRadio Link Quality Source Routing), которая, согласно экспериментам, дает существенный прирост производительности сети, узлы которой поддерживают несколько интерфейсов. Компания Tropos Networks также представила свое решение в области маршрутизации в меш-сетях. Яркий пример внедрения ее разработок — сеть Google WiFi, объединяющая свыше 400 маршрутизаторов в опорной сети, охватывающая более 12 квадратных миль и 15 тыс. домов для обслуживания 25 тыс. пользователей. Данного результата удалось достичь благодаря разработке и использованию протокола Predictive Wireless Routing Protocol (PWRP), способного работать в больших сетях без потери пропускной способности. PWRP является закрытым проприетарным протоколом, поэтому точных данных о его работе нет. Однако из официальных документов разработчика следует, что данный протокол — полностью распределенный и в первую очередь ориентирован на обеспечение связи клиент-сервер, которая динамически оптимизируется и с легкостью масштабируется при расширении сети. Про метрику, используемую в протоколе, известно лишь то, что она основана на измерении действительной производительности беспроводной сети. Группа OLPC team предложила упрощенную версию протокола HWMP. Неоспоримые преимущества этого решения — открытость проекта и исходных кодов и его поддержка крупными компаниями. Специально для меш-сетей в Голландском институте беспроводной и мобильной связи (Twente Institute for Wireless and Mobile Communications) разработан протокол Forwarding Layer for MEshing (FLAME). Он работает на виртуальном втором с половиной уровне модели OSI, аналогично протоколу LQSR. Это наделяет FLAME теми же преимуществами, что и LQSR, т е. прозрачностью с точки зрения протоколов верхних уровней и независимостью от среды передачи данных. Однако в отличие от LQSR протокол FLAME не использует никаких метрик (первый пришедший от узла пакет считается пришедшим по кратчайшему пути, который и используется в дальнейшем), — любой полученный пакет является основанием для обновления информации о его источнике. При этом в таблицу маршрутизации заносится интерфейс и соседний узел, через которые пролегает путь к источнику пакета. Для этого в сети под управлением FLAME ко всем передаваемым пакетам добавляется FLAME-заголовок.

В отечественном аппаратно-программном комплексе меш-сетей, разработанном коллективом под руководством профессора В. М. Вишневского на базе серийно выпускаемого комплекса РЭС «Рапира», в качестве базового протокола маршрутизации используется HWMP. Кроме того,

в ИППИ РАН разработан оригинальный протокол маршрутизации,

обеспечивающий полностью прозрачный переход между проводной сетью и беспроводной меш-сетью. Разработанный в ИППИ РАН протокол, так же, как и протоколы FLAME и LQSR, использует виртуальный «2,5 уровень» модели OSI, однако в остальном его алгоритмы отличаются от FLAME и LQSR.

В состав комплекса также входит специальная программа — контроллер сети, — которая занимается мониторингом беспроводной сети, а также обеспечивает удобство конфигурирования сети. Эта программа совмещает в себе функции ряда вспомогательных сервисов, таких как NTP- и DHCP-серверы, а также функции сервера безопасности сети. Разработанный отечественный аппаратно-программный комплекс беспроводных меш-сетей будет широко использован при построении распределенных беспроводных городских сетей (как альтернатива WiMAX), в промышленных сенсорных сетях и в других областях.

Во многом требования, предъявляемые к оборудованию меш-сетей, являются аналогичными требованиям к оборудованию других сетей доступа. Особенно это касается требований по противодействию внешним воздействующим факторам. Поскольку основные отличия меш-сетей заключаются в иной организации функций канального уровня и в использовании собственных протоколов маршрутизации, то особые требования предъявляются к протоколам маршрутизации.

В общем случае способ маршрутизации должен удовлетворять следующим основным требованиям [5]:

- гарантированно определять маршрут передачи сообщений, если он существует;
- обеспечивать маршрутизацию одноадресных, многоадресных и циркулярных сообщений;
- обеспечивать оптимизацию выбираемых маршрутов в соответствии с принятым критерием;
- устранить (не допускать) зацикливания сообщений;
- адаптироваться к возможным изменениям условий функционирования сети и изменениям параметров информационных потоков;
- требовать незначительного расходования сетевых ресурсов;
- иметь приемлемую сложность реализации и необходимое быстродействие.

Выводы

1. В результате исследования сформулированы ключевые различия между беспроводными пакетными технологиями обмена данными для мобильных устройств — WiMAX и Wi-Fi Mesh. Рассмотрены возможности протокола 802.11s, являющегося наиболее современным и поддерживаемым стандартом в сфере mesh-сетей.
2. Досконально проанализированы такие сетевые характеристики как: пропускная способность, время реакции, задержка передачи, расширяемость и масштабируемость сети. Также приведены сведения о метрике времени передачи в канале, обеспечивающей согласованность устройств в mesh-сети.
3. С помощью методов математического аппарата выявлена тенденция к росту диапазона значений времени задержки пакета данных при его передаче по низкоскоростному каналу, что демонстрирует необходимость применения в mesh-сетях пакетов небольшого размера.
4. Произведенное сравнение среднего времени загрузки файлов разного размера для стандартов 802.11g, 802.11n, Fast- и Gigabit-Ethernet выявило, что наиболее близок к стандартам Ethernet по производительности в ходе исследования оказался протокол 802.11n.
5. Графики 2 и 3 демонстрируют пригодность использования технологии 802.11n для передачи трафика реального времени и мультимедийных приложений, несмотря на значительное отставание по показателям среднего времени задержки и джиттера от технологии Gigabit-Ethernet.
6. Во второй части работы приведен анализ, сравнение и требования к зарубежным и отечественным протоколам маршрутизации распределенных сетей.

Литература

1. Татаринов В.И. Введение в самоорганизацию интеллектуально-определяемых сетей / В.И. Татаринов // Информация и Космос. — 2022. — № 2. — С. 119–124.
2. Гусс С.В. Самоорганизующиеся mesh-сети для частного использования / С.В. Гусс // Математические структуры и моделирование. 2016. №4(40). С. 102–115.
3. Чанцис Ф., Стаис И., Кальдерон П., Деирменцоглу Е., Вудс Б. Практический хакинг интернета вещей / пер. с англ. Л. Н. Акулич. — М.: ДМК Пресс, 2022–480 с.

4. Киреев С.А. Оптимизация передачи информации в самоорганизующихся сетях // Процессы управления и устойчивость. 2020 Т. 67, № 1. С.56–78.
5. Миклуш В.А. Оценка показателей качества обслуживания беспроводных сенсорных сетей / В.А. Миклуш, Т.М. Татарникова, С.В. Рудых // Информация и Космос. 2022. № 4. С.21-27.
6. Афанасьев А.Л. Многокритериальная многопутевая маршрутизация в mesh-сетях / А.Л. Афанасьев, А.В. Гармонов // (http://www.govvrn.ru).
7. Леонов. А.В. Экспериментальная оценка возможности использования алгоритма муравьиной колонии AntHocNet для решения задачи маршрутизации в FANET / Леонов А. В. // Научно-технические ведомости СПбГПУ. Информатика. Телекоммуникации. Управление. 2017.Том 10, № 1. С 7–26. DOI:10/18721/JCSTCS.10101
8. Гольдштейн, Б.С. Сети связи пост NGN / Б. С. Гольдштейн, А. Е. Кучерявый. — СПб.: БХВ Петербург, 2014.160 с.:

INVESTIGATION OF MESH NETWORK PERFORMANCE ISSUES IN SPECIAL-PURPOSE COMMUNICATION SYSTEMS

Pryadkin A. M.[1], Grishanov I. S.[2]

Keywords: *wireless technologies, bandwidth, management, mesh network, performance, response time, protocol, extensibility, scalability.*

Objective. *To develop (substantiate) proposals that contribute to the effective use of mesh networks in special-purpose systems in the field of, on the basis of, technical solutions in the field of control and communication.*

Research method. *Analytical with the use of mathematical apparatus to obtain the dependence of the time of transmission of messages of various lengths on the bandwidth of the channel.*

The result of *the study is the analysis of the main network characteristics of the performance of distributed systems in order to develop recommendations for improving the performance of mesh networks. In this work, the author analyzes the dependencies of the transmission time of messages of various lengths on the bandwidth of the channel, the file download time on its size, as well as a comparison of various network technologies in terms of transmission latency and jitter, as a result of which conclusions are drawn about the optimal size of the packet length in a mesh network, its performance and transmission delays relative to various variants of Ethernet technology. The analysis of foreign and domestic developments in the field of packet routing in mesh networks is carried out, the basic requirements for the routing process that ensure the performance of the network are formulated.*

The scientific novelty *lies in the comprehensive analysis and comparison of various aspects of wireless packet data exchange technologies for mobile devices, including WiMAX and Wi-Fi Mesh, as well as in the detailed consideration of the 802.11s protocol, which is the leading standard in the field of mesh networks.*

well as in a detailed examination of the 802.11s protocol, which is an advanced standard in the field of mesh networks.

References

1. Tatarinov V. I. Vvedenie v samoorganizaciju intellektual'no-opredeljaemyh setej / V.I. Tatarinov // Informacija i Kosmos. – 2022. – № 2. – C. 119–124.
2. Guss S.V. Samoorganizujushhiesja mesh-seti dlja chastnogo ispol'zovanija / S.V. Guss // Matematicheskie struktury i modelirovanie. 2016. №4(40). S. 102–115.
3. Chancis F., Stais I., Kal'deron P., Deirmencoglu E., Vuds B. Prakticheskij haking interneta veshhej / per. s angl. L. N. Akulich. – M.: DMK Press. 2022.–480 s.
4. Kireev S.A. Optimizacija peredachi informacii v samoorganizujushhihsja setjah // Processy upravlenija i ustojchivost'. 2020 T. 67, № 1. S.56–78.
5. Miklush V.A. Ocenka pokazatelej kachestva obsluzhivanija besprovodnyh sensornyh setej / V.A. Miklush, T.M. Tatarnikova, S.V. Rudyh // Informacija i Kosmos. 2022. № 4. S.21-27.
6. Afanas'ev A.L. Mnogokriterial'naja mnogoputevaja marshrutizacija v mesh-setjah / A.L. Afanas'ev, A.V. Garmonov // (Afanas'ev A.L., Garmonov A.V. - Mnogokriterial'naja mnogoputevaja marshrutizacija v mesh-setjah, data obrashhenija 30 sentjabrja 2024 g.).
7. Leonov A. V. Jeksperimental'naja ocenka vozmozhnosti ispol'zovanija algoritma murav'inoj kolonii AntHocNet dlja reshenija zadachi marshrutizacii v FANET / Leonov A. V. // Nauchno-tehnicheskie vedomosti SPbGPU. Informatika. Telekommunikacii. Upravlenie. 2017. Tom 10, № 1. S. 7–26. DOI:10.18721/JCSTCS.10101
8. Gol'dshtejn, B. S. Seti svjazi post NGN / B. S. Gol'dshtejn, A. E. Kucherjavyj. – SPb.: BHV Peterburg, 2014.160 s.

[1]Andrey M. Pryadkin, adjunct of the Department of Combat Use of Signal Troops of the Military Academy of Communications named after Marshal of the Soviet Union S.M. Budyonny, St. Petersburg. E-mail: tbilnovspb28@mail.ru

[2]Ilya S. Grishanov, postgraduate student of the Department of Electrical Communications, Alexander I St. Petersburg State University of Railway Engineering, St. Petersburg. E-mail: igrissh@zohomail.com

КАЧЕСТВО ОБСЛУЖИВАНИЯ ТРАФИКА РЕАЛЬНОГО ВРЕМЕНИ В МУЛЬТИСЕРВИСНОЙ СЕТИ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

Аникеев А.И.,[1] Репин Б.Г.,[2] Селезнев А.В.[3]

DOI:10.21682/3034-40-50-2024-2-13-20

Ключевые слова: *сеть с пакетной коммутацией, соглашение о качестве обслуживания, сетевой трафик, качество передачи, доступность услуг, приоритезация трафика, точки контроля, сеть доверенного оператора.*

Аннотация.

Цель статьи: *на основе анализа особенностей обеспечения качества обслуживания трафика реального времени в мультисервисной сети специального назначения разработать подходы к реализации механизмов контроля.*

Метод исследования: *при проведении исследования применялись методы теории телетрафика.*

Результат: *в работе проведен анализ механизмов маркировки и обработки трафика реального времени в мультисервисной сети специального назначения, которая является составной VPN MPLS сетью. Предложены подходы к реализации механизмов контроля качества. Сформулирована проблема обеспечения требуемого качества обслуживания трафика, связанная с особенностями маркировки, перемаркировки и настройки механизмов обработки трафика реального времени при продвижении его через составную сеть, поскольку именно туннелирование трафика в сети IP/MPLS порождает эту проблему. Определен метод корректировки ситуации, опирающийся на мутацию поля DSCP пакета, в частности, предлагается маркировать трафик классом EF, обеспечивающим сервис с низкой задержкой и сводящий к минимуму джиттер задержки.*

Практическая ценность *состоит в том, что в статье предложена реализация механизмов QoS с учетом существующей практики маркировки трафика реального времени на конечных узлах и перемаркировки трафика в сети IP/MPLS доверенного оператора. В частности, для маркировки исходного потока трафика реального времени предлагается использовать класс DSCP, обеспечивающий сохранение исходной кодировки при переходе из домена IP в домен MPLS. Процессы обработки трафика в сети доверенного оператора находятся вне зоны контроля системы управления связью мультисервисной сети специального назначения, поэтому в работе определены точки контроля качества, поскольку в случаях, когда сложно провести измерение, актуальным является анализ текущих характеристик качества обслуживания трафика.*

Введение

С точки зрения современных тенденций развития телекоммуникаций специального назначения актуальной задачей является построение конвергентной мультисервисной сети. Такая сеть должна обеспечивать неограниченный набор услуг, предоставлять гибкие возможности по управлению и созданию новых видов сервиса. Последнее требует реализации универсальной транспортной сети с распределенной коммутацией, где взаимодействие между устройствами и приложениями осуществляется с помощью создания виртуальных соединений, на управление которыми заметно влияют особенности стохастической динамики процессов пакетной коммутации [1].

Одной из наиболее актуальных проблем исследования вероятностно-временных характеристик сетей является адекватный учет особенностей сетевого трафика.

Традиционный трафик локальных и глобальных сетей состоит из передачи файлов приложений, не требующих принятия специальных мер или применения специальной обработки. Однако, при передаче голоса, видео и других приложений реального времени по сети с пакетной коммутацией, ситуация кардинально меняется и без реализации механизмов обеспечения качества обслуживания (Quality of Service, QoS) уже не обойтись [2].

Адекватно настроенные механизмы приоритезации и обработки трафика позволяют соответствующим образом распределить доступную

[1]Аникеев Александр Иванович, преподаватель кафедры «Сетей связи и систем коммутации» Военной академии связи, г. Санкт-Петербург, Россия. E-mail: aai1956@yandex.ru

[2]Репин Борис Григорьевич, кандидат военных наук, доцент, доцент кафедры «Сетей связи и систем коммутации» Военной академии связи, г. Санкт-Петербург, Россия. E-mail: rbg@inbox.ru

[3]Селезнев Андрей Васильевич, кандидат технических наук, научный сотрудник Военной академии связи, г. Санкт-Петербург, Россия. E-.mail: andrsel@mail.ru

пропускную способность канала и обеспечить требуемый уровень качества обслуживания разноприоритетного трафика. Здесь следует отметить, что приоритезация требуется в основном только в узких, загруженных местах, когда пропускной способности канала не хватает для передачи всех поступающих пакетов и нужно каким-то образом дифференцировать их обработку. Кроме того, приоритезация необходима для предотвращения влияния всплесков сетевой активности на чувствительный к задержкам трафик.

Современная мультисервисная сеть специального назначения представляет собой сеть VPN IP/MPLS. Следовательно, для обеспечения требуемого качества предоставляемых услуг необходимы соответствующие настройки маркировки туннелированного трафика и механизмов QoS для эффективной обработки туннелированного трафика. Туннелирование является важной особенностью обработки трафика в таких сетях, поскольку передача приоритезированного трафика осуществляется через виртуальные каналы или туннели для обеспечения конфиденциальности, целостности и безопасности передаваемой информации и гарантировать приемлемый уровень обслуживания для каждого приложения

Туннелирование трафика позволяет объединить удаленные сегменты в единую сеть, в которой могут использоваться различные технологии и ресурсы. В случае использования VPN IP/MPLS сети, основным преимуществом является возможность обеспечения требуемого уровня качества обслуживания (QoS), что особенно важно для приложений реального времени.

Исследование вопросов конфигурирования механизмов QoS является важным аспектом обеспечения оптимальной производительности и надежности такой сети. В данном контексте, разработка подходов к настройке параметров QoS, специально адаптированной для управления туннельным трафиком имеет большое значение и включает в себя определение оптимальных параметров, учитывающих специфику сетей специального назначения, а также обеспечение баланса между эффективностью и степенью защиты передаваемых данных.

Особенности обработки трафика реального времени

Для передачи трафика реального времени в сетях, не гарантирующих QoS, разработан и применяется протокол H.323, который предоставляет специальную поддержку, необходимую приложениям реального времени. Он состоит из множества спецификаций, определяющих, как мультимедийные приложения взаимодействуют друг с другом по сети, не гарантирующей QoS. Одним из таких протоколов является протокол передачи в реальном масштабе времени (Real-Time Transfer Protocol, RTP), используемый для доставки потокового аудио и видео по сетям с пакетной коммутацией. В качестве транспорта для сервисов реального времени RTP использует UDP и может дополняться протоколом управления трафиком реального времени (Real-Time Control Protocol, RTCP) для мониторинга уровня QoS и передачи сеансовой информации между участниками сеанса. Протокол RTP не способен повлиять на задержку в сети, но он сокращает дрожание изображения и звука при воспроизведении при наличии задержек. Он, в принципе, может установить факт потери пакетов (пакеты нумеруются на передаче), но мер для восстановления потерь не предпринимает, его задача — обеспечить комфортную для получателя транспортировку потока пакетов приложения реального времени.

Один из способов расширения возможностей RTP — использование его совместно с протоколом резервирования ресурсов — RSVP, который поддерживается многими приложениями реального времени [3,4,5].

При сопряжении различных сетей связи существуют определенные проблемы, связанные с обеспечением качества обслуживания при предоставлении услуг связи. Предпосылками для возникновения возможных проблем служат:

- число классов сервиса, используемое для предоставления услуг связи потребителям;
- уровень (канальный и/или сетевой), на котором обеспечивается качество обслуживания;
- используемая политика маркировки трафика при предоставлении различного вида услуг связи;
- политики управления трафиком: ограничения, фильтрация, формирование трафика на сетевых интерфейсах узлов;
- другие — например, использование защитных экранов (Firewall), глубокого анализа пакетов (DPI) в режиме реального времени, криптографических методов шифрования.

Часть проблем в плоскости обеспечения качества услуг при сопряжении может быть решена за счет разработки и применения эффективной схемы отображения (и перемаркировки) классов обслуживания, а также использования принципов иерархического QoS.

Отображение классов обслуживания может выполняться для каждой услуги как в пределах одного уровня (канального или сетевого), так и между уровнями (например, отображение значений приоритетов 802.1q/p или битов MPLS EXP в значения ToS или DSCP).

Контроль качества обслуживания трафика

Качество обслуживания определяется как мера производительности передающей системы, отражающая качество передачи и доступность услуг. Доступность услуг является важнейшим элементом QoS. Для успешного внедрения QoS необходимо обеспечить максимально высокую доступность сетевой инфраструктуры. (Конечной цели высокой доступности соответствует уровень 99,999 процентов, то есть только 5 минут простоя в год). Качество передачи сети определяется следующими факторами [4]:

Доступность — диапазон времени сетевой достижимости между входной и выходной точкой сети — это сетевая доступность.

Доступность сервиса — это диапазон времени, в течение которого этот сервис доступен между определенными входной и выходной точками с параметрами, оговоренными в соглашении об уровне обслуживании (SLA).

Потери — это отношение правильно принятых пакетов к общему количеству пакетов, которые были переданы по сети. Потери выражаются в процентах отброшенных пакетов, которые не были доставлены по назначению. Обычно, потери — это функция от доступности. Если сеть не загружена, то потери (во время отсутствия перегрузок) будут равны нулю. Во время перегрузок действующие механизмы QoS будут определять, какие пакеты могут быть сброшены.

Определяя требования QoS для VoIP трафика, рекомендуется придерживаться следующих правил [5,6]:

Голосовой трафик должен быть промаркирован как DSCP EF, в соответствии с «Базовыми Основами QoS» и RFC 3246.

Сигнализация должна быть промаркирована как CS3, в соответствии с «Базовыми Основами QoS» (во время миграции можно использовать AF31).

Потери пакетов в магистралях, спроектированных для предоставления VoIP сервиса высокого качества, не должны превышать 0.25 процентов.

Задержка — это время, которое требуется пакету для того, чтобы после передачи дойти до пункта назначения. В случае голоса, эта задержка определяется как время прохождения сигнала от говорящего к слушающему.

Колебания задержки (jitter) — это разница между сквозным временем задержки, которая возникает при передаче по сети разных пакетов. Так, например, если для передачи одного пакета по сети требуется 100 мсек, а для передачи следующего пакета — 125 мсек, то колебание задержки составит 25 мсек.

Односторонняя задержка не должна превышать 150ms, в соответствии со International Telecommunication Union (ITU) G.114.

Колебания задержки (jitter) должны быть менее 10 мсек. Максимальный jitter должен быть менее чем бюджет по задержке в сети минус минимальная сетевая задержка. Это типовое значение колебания задержки для VoIP обусловлено бюджетом по задержке, так называемым mouth-to-ear, в 100 мсек. (Это достаточно консервативный бюджет по сравнению с G.114, в котором рекомендуется jitter менее 150 мсек). Из этого значения мы вычитаем время распространения по магистрали (30 мсек) и задержку кодека (35 мсек), что дает нам бюджет для jitter в 35 мсек. Эти 35 мсек разбиваются на 30 мсек на доступе (15 мсек вход/выход) и 5 мсек на магистрали: то есть в худшем варианте, для адаптивных jitter-буферов, колебания задержки должны быть менее 10 мсек.

Для каждого разговора (в зависимости от частоты квантирования, кодека и заголовка второго уровня) требуется 21–106 kbps гарантированной приоритетной полосы пропускания.

Для трафика сигнализации требуется 150 bps (плюс заголовок второго уровня) гарантированной полосы пропускания.

На качество голосовой связи напрямую влияют три фактора качества QoS: потери пакетов, задержка и вариации задержки.

Потери пакетов вызывают кратковременные пробелы в разговоре. Потери двух и более последовательных 20 мсек сэмплов приведут к заметной деградации качества голоса. Предположив случайное распределение сбросов пакетов в одном речевом потоке, сброс 1-го процента в голосовом потоке привела бы в среднем к потере, которую нельзя было бы восстановить каждые 3 минуты. Аналогично, уровень сброса 0,25 процента привел бы в среднем к потере, которую нельзя было бы восстановить каждые 53 минуты.

Задержка более 200 мсек может вызвать деградацию качества голосовой связи. Если общая задержка в канале становится слишком большой, разговор по телефону начинает напоминать переговоры по спутниковому каналу связи или по симплексному радиоканалу. В стандарте Международного Союза Электросвязи для технологии VoIP (G.114) говорится, что задержка величиной в 150 мсек в одном направлении является приемлемой для качество голосовой связи. Было продемонстрировано, что разница в каче-

стве голоса между сетями с задержкой в 150 мсек и 200 мсек является незначительной и практически незаметной для пользователя. В [5,6] предлагается ориентироваться на ITU стандарт 150 мсек, но если существуют ограничения не позволяющие добиться такого бюджета, то размер задержки может быть увеличен до 200 мсек без значительной деградации качества связи.

Для выравнивания вариации задержки в IP-телефонии используются адаптивные джиттер-буферы. Они частично решают проблему, однако могут компенсировать отклонение задержки лишь в пределах от 20 до 50 мсек.

При передаче трафика интерактивного видео также есть особенности. Так как видео конференция включает аудио кодек G.711 для речи, то у нее и соответствующие голосовому трафику требования к потерям, задержке и колебаниям задержки. Однако трафик видео конференции радикально отличается от трафика голоса. Например, трафик видео конференций использует переменные размеры пакетов и переменные скорости передачи пакетов. Скорость видео конференции — это скорость сэмплирования видео потока, но не реальная полоса пропускания, которую требует видео вызов. Иными словами, полезная нагрузка пакетов видео конференции заполняется 384 kbps потока видео сэмплов. IP, UDP и RTP заголовки (40 байт на пакет) должны быть дополнительно включены в требования по полосе пропускания (так же как и заголовки второго уровня). Так как используются переменные размеры пакетов и скорости генерации пакетов, то достаточно трудно точно подсчитать абсолютное значение накладных расходов. Тестирование, однако, показало, что для расчета можно использовать скорость видео конференции плюс 20 процентов

Оценка качества обслуживания трафика реального времени (TPB) должна давать реальную картину происходящих процессов, поэтому при создании сценария для интервалов оценки обслуживания TPB необходимо учитывать следующие требования [5]:

- интервал оценки должен быть достаточно длительным, чтобы содержать необходимое количество пакетов нужного потока;
- интервал оценки должен быть достаточно длительным, чтобы был отражен период характерного использования (время существования потока) или оценка пользователя;
- интервал оценки должен быть достаточно коротким для обеспечения баланса применяемых рабочих характеристик на протяжении каждого интервала (интервалы плохих рабочих характеристик не должны быть скрыты в слишком длинном оценочном интервале, они должны быть идентифицированы);
- интервал оценки должен быть достаточно коротким для обращения к фактическим аспектам измерения.

Для выполнения оценок, связанных с TPB, минимальный интервал должен быть порядка 10–20 секунд с характерной скоростью передачи пакетов (от 50 до 100 пакетов в секунду), также интервал должен иметь верхнее ограничение в пределах нескольких минут.

Эффективным решением может являться организация взаимодействия системы управления сетью и подсистемы мониторинга показателей QoS. При таком взаимодействии система управления сетью, получая информацию о деградации системы связи, информирует оператора, который может запросить подробную информацию с сервер-менеджера и принять решение о реконфигурации сети для эффективного распределения ресурсов.

Точки контроля могут располагаться как на интерфейсе UNI, так и на местах сопряжения различных сетей, т. е. можно контролировать как end-to-end QoS, так и Segment QoS [7]. Пример расположения точек контроля показан на рис. 1 [9].

Рис 1. Расположение точек контроля

Существует более простой способ контроля показателей качества обслуживания в сетях, который зачастую используется операторами связи. Многие операторы и пользователи телекоммуникационных услуг используют для контроля показателей QoS простые методы, например ICMP PING или трассировка. При использовании данных методов можно измерить только задержку при передаче сигнала в IP-сети в прямом и обратном направлениях (IPRTD), а задержка при передаче сигнала в одном направлении для пакетной сети, конечно же, не равна точно половине IPRTD. Существуют также другие проблемы, связанные с PING: 1 — на маршрутизаторах PING иногда отключается для уменьшения вероятности проникновения хакера и воздействий, вызывающих отказ в обслуживании законных пользователей; 2 — PING имеет наименьший приоритет при обработке пакетов на маршрутизаторе. Следовательно, задержка, измеренная при помощи PING, не является точной мерой задержки трафика пользователя [6].

Другим важным аспектом контроля качества сетевых параметров является управление пропускной способностью. Для этого следует применять методы управления трафиком, такие как Traffic Engineering (TE). Эти методы позволяют контролировать и приоритезировать различные типы трафика в сети, что позволяет гарантировать необходимое качество обслуживания для приложений в режиме реального времени.

Для обнаружения и устранения возможных проблем с качеством обслуживания также полезно использовать системы мониторинга сетевого трафика, такие как сетевые анализаторы или системы пакетного анализа. Эти системы позволяют анализировать сетевой трафик и идентифицировать возможные проблемы.

В целом, контроль качества сетевых параметров трафика в мультисервисных сетях специального назначения требует применения различных методов и инструментов. Он должен быть основан на комбинации протоколов уровня приложения, управления трафиком и систем мониторинга, чтобы обеспечить стабильное и надежное функционирование сети.

Заключение

В современных мультисервисных сетях широкое применение получило туннелирование трафика. Туннелирование трафика обеспечивает управление потоками данных за счёт построения сети на 2(3) уровне модели OSI, позволяет связывать удаленные узлы в единую сеть с общими ресурсами, упрощает администрирование сети за счёт разделения на уровень инфраструктуры и уровень пользователей и обеспечивает построение единых сетей на базе различных сетевых технологий.

Туннелирование трафика ориентировано на построение сети и обеспечение надежной передачи данных, в то же время, вопросы обеспечения качества обслуживания при транспортировке инкапсулированного трафика требуют дополнительного рассмотрения.

Контроль качества предоставления услуг и контроль качества обслуживания трафика в сети передачи данных являются важными составляющими процесса эксплуатации сети. Поскольку существенная доля сетевой инфраструктуры мультисервисной сети специального назначения являются арендованными ресурсами доверенного оператора, важную роль в обеспечении требуемого качества обслуживания трафика играет соглашение между оператором и заказчиком.

На сегодняшний день самый распространенный способ согласования требований заказчика и возможностей оператора — заключение соглашений об уровне сервиса (Service Level Agreement, SLA), т. е. контрактов, где четко указано, какого уровня доступность, сервисы и цены ожидает получить заказчик. В таком соглашении доверенный оператор должен гарантировать срок бессбойной работы и длительность задержки в конкретное время суток для конкретных видов приложений. Соглашение также может содержать информацию о доступности пользовательского соединения [8,9].

Кроме того, должно быть определено, какие сервисы и гарантии обслуживания предлагаются для каждого класса трафика, пропускная способность (скорость, с которой пакеты передаются по сети), задержка (время между отправкой и приемом пакетов на конечных станциях), процент потерянных пакетов (максимально возможное число удаленных при передаче пакетов) и вариация задержки (разницу во времени доставки пакетов из одного потока).

Поскольку, как правило, в сети оператора существует собственная политика в области QoS, важной проблемой является обеспечение единого понимания механизмов дифференциации трафика в сетях заказчика и доверенного оператора [10].

Доверенный оператор использует атрибуты маркирования третьего уровня (IPP или DSCP) для определения какому операторскому классу сервиса следует назначить этот пакет. Следовательно, заказчики для достижения соответствующего уровня сервиса должны маркировать/перемаркировать трафик в соответствии политикой операторской сети. Дополнительно, оператор

может перемаркировать трафик вне контракта в пределах своего облака, что может повлиять на пользовательский трафик и требует последовательной политики сквозной маркировки. Следующие вопросы должны быть учтены при определении стратегии маркировки/перемаркировки на границе клиент-оператор.

Общее правило маркировки в корпоративных сетях заключается в маркировке трафика и установке границ доверия как можно ближе к источнику, насколько это возможно административно и технически. В [10] рекомендуется не доверять маркировке, установленной на хостах пользователей (так как здесь возможны злоупотребления). Определенные типы трафика, возможно, нужно перемаркировывать еще до передачи на пограничные устройства оператора для получения доступа к определенному классу. Если требуется такая перемаркировка, то рекомендуется производить ее на граничном маршрутизаторе узла. Это связано с тем, что набор предлагаемых оператором сервисов может измениться или расшириться со временем, а производить перенастройку проще, если она производится только на границе пользовательской сети. Могут существовать классы, где множество типов трафика требуется пометить одинаковыми значениями для получения доступа к определенным очередям. Например, на высокоскоростных каналах может потребоваться передавать голос, интерактивное видео и сигнализацию в операторском классе реального времени. Если в операторский класс реального времени направляются только пакеты, промаркированные DSCP EF и CS5, то это означает, что три этих приложения должны использовать один и тот же код приоритета DSCP. Однако, полосу пропускания, выделенную для EF, следует ограничивать, чтобы другие классы трафика могли быть обработаны, поскольку возможна ситуация, что всю полосу пропускания займет трафик EF. В то же время, очередь, выделенная для EF должна иметь наивысший приоритет, чтобы предназначенный для нее трафик проходил быстро и не вызывал значительных задержек.

Качество обслуживания трафика реального времени обычно контролируется процедурами без обратной связи, основанными на понятии SLA — соглашении между пользователем услуг и администрацией сети относительно параметров передаваемого трафика и качества его обслуживания.

При организации межсетевого взаимодействия в этом случае критичными аспектами являются:

- разграничение зон ответственности служб технической эксплуатации;
- выбор размещения точек контроля показателей качества функционирования сети и качества предоставления услуг связи.

Контроль показателей QoS с использованием рассмотренных в работе способов может эффективно использоваться в процессе эксплуатации сетей, в том числе для контроля SLA, что позволит существенно повысить качество предоставляемых телекоммуникационных услуг.

Литература

1. Ясинский С.А., Репин Б.Г., Григорчук А.Н., Аникеев А.И. О моделировании трафика в мультисервисной сети специального назначения // Труды ЦНИИС. Санкт-Петербургский филиал. 2022. Т. 1. № 13. С. 96–105.
2. Ясинский С.А., Одоевский С.М., Рафальская М.И. Анализ сложности решения обратных оптимизационных задач при обосновании сетевых механизмов обеспечения качества обслуживания мультимедийного трафика // Информация и космос. 2023. №2., с.54-63.
3. Елисеев Д.И., Никитин И.С., Оранский С.В., Репин Б.Г. Управление механизмами QoS с помощью политик. //В сборнике: Современное состояние и перспективы развития инфокоммуникационных сетей связи специального назначения. Материалы научно-практической конференции. Санкт-Петербург, 2024. С. 104–108.
4. Аникеев А.И., Григорчук А.Н., Оранский С.В., Репин Б.Г. Исследование свойств туннелированного голосового трафика в VPN сети специального назначения. //В сборнике: Современное состояние и перспективы развития инфокоммуникационных сетей связи специального назначения. Сборник материалов научно-практической конференции. Санкт-Петербург, 2023. С. 105–112.
5. Григорчук А.Н., Оранский С.В., Репин Б.Г. Проблема использования маркировки при туннелировании маркированного трафика. Труды ЦНИИС. Санкт-Петербургский филиал. 2022. Т. 1. № 13. С. 146–160.
6. Аникеев А.И., Григорчук А.Н., Оранский С.В., Репин Б.Г. Особенности передачи мультимедийного трафика в мультисервисной сети специального назначения. //В сборнике: Современное состояние и перспективы развития инфокоммуникационных сетей связи специального назначения. Сборник материалов научно-практической конференции. Санкт-Петербург, 2023. С. 113–118.
7. Оранский С.В., Репин Б.Г., Селезнев А.В., Ясинский С.А. О влиянии туннелирования на величину задержки пакетов в мультисервисной сети специального назначения. //В сборнике: Современные тенденции инженерного образования. Сборник материалов Научно-практической конференции. Санкт-Петербург, 2023. С. 258–263.

8. Ибрагимов Б.Г., Гасанов А.Г. Исследование и оценка эффективности мультисервисных сетей NGN/ IMS при передаче мультимедийных трафиков // T-Comm: Телекоммуникации и транспорт. 2017. Том 11. №2. С. 15–18.
9. Смирнов П.И. Способы оценки показателей качества обслуживания в мультисервисных сетях // НИИ Масштаб — научно-исследовательский институт, разработчик сложных систем и средств телекоммуникаций, защиты информации, автоматизированного управления. https://mashtab.org/company/massmedia/articles/qos/
10. Принципы построения мультисервисной сети ПАО «Ростелеком» С.Л. Гавлиевский, В.Г. Карташевский, Д.В. Проскура, Д.С. Сахарчук, М.Ю. Сподобаев // Горячая линия — Телеком, 2019. 228 с., ил.

QUALITY OF SERVICE OF REAL TRAFFIC TIME IN A MULTI-SERVICE NETWORK SPECIAL PURPOSE

Anikeev A.I.[1], Repin B.G.[2], Seleznev A.V.[3]

Keywords: *packet-switched network, quality of service agreement, network traffic, transmission quality, service availability, traffic prioritization, control points, trusted operator network.*

The purpose of the article is to *develop approaches to the implementation of control mechanisms based on the analysis of the features of ensuring the quality of service of real-time traffic in a special-purpose multiservice network.*

Research method: *the methods of the teletraffic theory were applied.*

Result: *the paper analyzes the mechanisms of marking and processing real-time traffic in a special-purpose multiservice network, which is a composite VPN MPLS network. Approaches to the implementation of quality control mechanisms are proposed. The problem of ensuring the required quality of traffic service is formulated, associated with the features of marking, relabeling and setting up mechanisms for processing real-time traffic when moving it through a composite network, since it is the tunneling of traffic in the IP/MPLS network that generates this problem. A method for correcting the situation based on the mutation of the DSCP field of the packet is determined, in particular, it is proposed to mark traffic with the EF class, which provides a service with low latency and minimizes jitter latency.*

The practical value *lies in the fact that the article proposes the implementation of QoS mechanisms, taking into account the existing practice of marking real-time traffic at end nodes and remarking traffic in the IP/MPLS network of the trusted operator. In particular, it is proposed to use the DSCP class to mark the initial flow of real-time traffic, which ensures the preservation of the original encoding when moving from the IP domain to the MPLS domain. Traffic Processing Processes in the Network of the Trusted Operator are beyond the control of the communication management system of a special-purpose multiservice network, so quality control points are determined in the work, since in cases where it is difficult to measure, the analysis of the current characteristics of the quality of traffic service is relevant.*

References

1. Jasinskij S.A., Repin B.G., Grigorchuk A.N., Anikeev A.I. O modelirovanii trafika v mul'tiservisnoj seti special'nogo naznachenija // Trudy CNIIS. Sankt-Peterburgskij filial. 2022. T. 1. № 13. S. 96–105.
2. Jasinskij S.A., Odoevskij S.M., Rafal'skaja M.I. Analiz slozhnosti reshenija obratnyh optimizacionnyh zadach pri obosnovanii setevyh mehanizmov obespechenija kachestva obsluzhivanija mul'timedijnogo trafika // Informacija i kosmos. 2023. №2., s.54-63.
3. Eliseev D.I., Nikitin I.S., Oranskij S.V., Repin B.G. Upravlenie mehanizmami QoS s pomoshh'ju politik. //V sbornike: Sovremennoe sostojanie i perspektivy razvitija infokommunikacionnyh setej svjazi special'nogo naznachenija. Materialy nauchno-prakticheskoj konferencii. Sankt-Peterburg, 2024. S. 104–108.
4. Anikeev A.I., Grigorchuk A.N., Oranskij S.V., Repin B.G. Issledovanie svojstv tunnelirovannogo golosovogo trafika v VPN seti special'nogo naznachenija. //V sbornike: Sovremennoe sostojanie i perspektivy razvitija infokommunikacionnyh setej svjazi special'nogo naznachenija. Sbornik materialov nauchno-prakticheskoj konferencii. Sankt-Peterburg, 2023. S. 105–112.
5. Grigorchuk A.N., Oranskij S.V., Repin B.G. Problema ispol'zovanija markirovki pri tunnelirovanii markirovannogo trafika. Trudy CNIIS. Sankt-Peterburgskij filial. 2022. T. 1. № 13. S. 146–160.

[1]Alexander I. Anikeev, Lecturer, Department of Communication Networks and Switching Systems, Military Academy of Communications, St. Petersburg, Russia. E-mail: aai1956@yandex.ru
[2]Boris G. Repin, Ph.D., Associate Professor, Associate Professor of the Department of Communication Networks and Switching Systems, Military Academy of Communications, St. Petersburg, Russia. E mail: rbg@inbox.ru
[3]Andrey V. Seleznev, Ph.D., Researcher of the Military Academy of Communications, St. Petersburg, Russia. E-.mail: andrsel@mail.ru

6. Anikeev A.I., Grigorchuk A.N., Oranskij S.V., Repin B.G. Osobennosti peredachi mul'timedijnogo trafika v mul'tiservisnoj seti special'nogo naznachenija. //V sbornike: Sovremennoe sostojanie i perspektivy razvitija infokommunikacionnyh setej svjazi special'nogo naznachenija. Sbornik materialov nauchno-prakticheskoj konferencii. Sankt-Peterburg, 2023. S. 113–118.
7. Oranskij S.V., Repin B.G., Seleznev A.V., Jasinskij S.A. O vlijanii tunnelirovanija na velichinu zaderzhki paketov v mul'tiservisnoj seti special'nogo naznachenija. //V sbornike: Sovremennye tendencii inzhenernogo obrazovanija. Sbornik materialov Nauchno-prakticheskoj konferencii. Sankt-Peterburg, 2023. S. 258–263.
8. Ibragimov B.G., Gasanov A.G. Issledovanie i ocenka jeffektivnosti mul'tiservisnyh setej NGN/ IMS pri peredache mul'timedijnyh trafikov // T-Comm: Telekommunikacii i transport. 2017. Tom 11. №2. S. 15–18.
9. Smirnov P.I.. Sposoby ocenki pokazatelej kachestva obsluzhivanija v mul'tiservisnyh setjah // NII Masshtab — nauchno-issledovatel'skij institut, razrabotchik slozhnyh sistem i sredstv telekommunikacij, zashhity informacii, avtomatizirovannogo upravlenija. https://mashtab.org/company/massmedia/articles/qos/
10. Principy postroenija mul'tiservisnoj seti PAO «Rostelekom» S.L. Gavlievskij, V.G. Kartashevskij, D.V. Proskura, D.S. Saharchuk, M.Ju. Spodobaev // Gorjachaja linija — Telekom, 2019. 228 s., il.

РАЗВИТИЕ СОВРЕМЕННОЙ МИКРОЭЛЕКТРОННИКИ В ОБОРОННОЙ ПРОМЫШЛЕННОСТИ РОССИИ

Базир Г.И.[1], Кузина Е.И.[2], Константинова А.А.[3]

DOI:10.21682/3034-40-50-2024-2-21-24

Ключевые слова: *микроэлектроника, микроэлектронное производство, автоматизация, новые технологии, полупроводниковые материалы*

Цель работы: *изучение особенностей современного производства изделий микроэлектро-ники в сфере оборонной промышленности. Рассмотрение потенциала и роли микроэлектронной индустрии в современном технологическом укладе, актуальных проблем, которые возникают при проектировании и производстве изделий микроэлектроники*

Метод исследования*: использованы аналитический, синтетический, индуктивный и де-дуктивный методы обработки тематических исследований, научных публикаций и релевантных литературных источников.*

Результаты: *проведен сравнительный анализ тенденций развития современной микро-электроники и ее внедрения в оборонную промышленность Российской Федерации (РФ) с учетом опыта специальной военной операции.*

Практическая ценность: *на основе сравнительного анализа определены перспективные направления развития микроэлектроники в оборонной промышленности РФ.*

Введение

Электронная промышленность является наиважнейшей для современных систем связи и навигации отраслью. Она обеспечивает компонентной базой области деятельности подразделений министерства обороны (МО) РФ как в мирное время, так и, в случае возникновения ситуаций военных конфликтов, где присутствует техническая коммуникация.

Аппаратура на основе изделий микроэлектроники широко используется в совре-менных военных операциях, в связи с этим она выступает мощным индикатором технологического развития ВС РФ [1]. Изделия микроэлектроники позволяют проектировать и производить в промышленных масштабах функционально сложное оборудование. Микроэлектронное производство стремится к размерному масштабированию до топологий 14, 10 и 7 нм и менее и развитию элементной базы в направлениях функционального усложнения, увеличения надёжности, сокращения размеров, массы, потребляемой энергии стоимости

Актуальность проблемы

В настоящее время процесс масштабирования высокоточных микроэлектронных изделий вошёл в фазу «замедления», совершенствования текущего производственного процесса и развития методов 2,5D- и 3D-интеграции [2]. В микроэлектронном производ-стве возникла тенденция к сокращению компонентных издержек и увеличению уровня интеграции при параллельном продолжении использования 28-нм технологического уровня. Инновационное развитие микроэлектроники определяют факторы увеличения плотности расположения элементов и площади кристалла, интеллектуальности приборов и эффективности производства, обеспечиваемой за счёт использования новейшего техно-логического оборудования.

Микроэлектроника определяет производительность любого современного высоко-точного оборудования и ориентируется на выпуск продуктов с высокой добавленной стоимостью, доля интеллектуальной составляющей в которых достигает 80% [3]. Это опре-деляет роль микроэлектронной индустрии в современном технологическом укладе и актуализирует необходимость увеличения темпов её развития. В настоящее время в Российской микроэлектронике преобладает продукция военного назначения — на неё приходится порядка 80% производимых изделий. Для гражданского использования в стране производятся интегральные микросхемы и основные электронные компоненты.

[1]Базир Геннадий Иванович, кандидат физико-математических наук, доцент, доцент 2 кафедры Военной академии связи, г. Санкт-Петербург, Россия. E-mail: gennadiy.bazir@gmail.com

[2]Кузина Екатерина Ивановна, преподаватель 2 кафедры Военной академии связи, г. Санкт-Петербург, Россия. E-mail: 78_kuzik@mail.ru

[3]Константинова Анна Алексеевна, кандидат технических наук, старший преподаватель 2 кафедры Воен-ной академии связи, г. Санкт-Петербург, Россия. E-mail: konstantinova.a.a@mail.ru

Рис. 1. Автоматизированные системы связи и навигации

Такое положение не всегда положительно сказывается на развитии отрасли, по-этому руководство страны поставило перед предприятиями оборонно-промышленного комплекса задачу наращивания также и доли гражданской продукции [4]. Однако для предприятий, в структуре производства которых доля гражданской продукции не превышает 10%, самостоятельный выход на рынок высокотехнологичной гражданской продук-ции проблематичен в силу неготовности производственных мощностей к выпуску таких изделий и отсутствия конструкторских, административно-управленческих и маркетинго-вых компетенций по организации производства и выводу товаров на гражданский рынок.

Переход на выпуск изделий двойного и гражданского применения позволит обеспечить загрузку производственных мощностей, однако для этого предприятиям необходимо оптимизировать производственный цикл, разработав и освоив комплексную автоматизированную линию сборки полупроводниковых приборов и интегральных микросхем двойного применения в металлопластмассовых корпусах. При этом остальные этапы производства — разработка электронной компонентной базы, создание фотошаблонов, производство кристаллов, сборка, измерения и все виды испытаний — не требуют изменений.

Помимо переориентации предприятий оборонно-промышленного комплекса, к первоочередным задачам развития отечественных микроэлектронных производств относятся [5]:

- запуск на имеющихся производствах новых технологий, таких как BCD, FRAM (MRAM), микроболометры, SiGe, DRAM и EEPROM;
- развитие на существующих микроэлектронных производствах технологий и правил проектирования для создания высоковольтных и аналоговых микросхем, Flip Chip кристаллов и специальных ПЛИС;
- запуск полномасштабного производства пластин по технологиям кремния на изоляторе и объёмного кремния;
- запуск производства 300-мм пластин по технологии 28 нм и менее;
- расширение существенного производства фотошаблонов и запуск производства фотошаблонов уровнем технологии 90 нм и менее;
- освоение серийного производства кремниевых пластин и пластин кремния на изоляторе диаметром 200 мм.

Повысить эффективность микроэлектронного производства возможно путём авто-матизации и механизации процессов на всех фазах производственного цикла [6]:

1. Заготовительная. Включает изготовление и разрезание слитков на пластины, подготовку оснастки и инструментов и производство корпусов.
2. Обрабатывающая. Предназначена для получения интегральных структур в полупроводниковом материале либо на его поверхности.
3. Сборочно-контрольная. Включает разделение пластин на кристаллы, сборку схем в корпус, герметизацию, контроль качества изделий и различные испытания.

Основные характеристики изделий микроэлектроники формируются в обрабатывающей фазе, поэтому в ней предъявляются наиболее высокие требования к стабильности, точности и условиям выполнения технологических процессов. Для их обеспечения современное оборудование микроэлектронных производств полностью компьютеризируется, что позволяет практически полностью исключить вероятность ошибок операторов и снизить влияние человеческого фактора [7]. Программа технологического процесса включает всю необходимую последовательность манипуляций по обработке подложек. При этом в программу можно вносить изменения, адаптируя производство под конкретные заказы.

Однако автоматизации и механизации процессов недостаточно для развития кон-курентного микроэлектронного производства: для обеспечения глубоких качественных изменений в производительных силах, создания принципиально новых видов продукции и технологий требуется интенсивное расширение и развитие исследований в области естественных и технических наук [8]. В частности, исследователям необходимо решить ряд проблем, возникающих при проектировании и производстве изделий микроэлектроники:

- проблема межсоединений, заключающаяся

в необходимости обеспечения коммутации между огромным количеством элементов микросхемы;
- проблема теплоотвода, заключающаяся в увеличении удельной мощности, рассеиваемой единицей поверхности подложки, при уменьшении размеров элементов и расстояния между ними;
- проблема уменьшения размеров элементов интегральных схем и увеличения площади обрабатываемых подложек;
- проблема дефектов подложки, возникающих при интеграции кристаллов больших размеров;
- проблема контроля параметров компонентов.

Другая актуальная проблема микроэлектроники — это возрастающая потребность в поиске и применении новых полупроводниковых материалов, превосходящих домини-рующий в настоящее время кремний по ряду электрофизических свойств [9]. Наиболее перспективными полупроводниковыми материалами являются карбид кремния (SiC), нитрид галлия (GaN), оксид галлия (Ga2O3), алмаз и нитрид алюминия (AlN).

Значимой проблемой в контексте импортозамещения микроэлектронного производства является обеспечение безопасности продукции [10]. Поскольку практически на любом этапе создания в микросхемы, возможно, внедрить аппаратный «троян» — вирус, могущий выполнять несанкционированные и скрытые от наблюдателя функции.

Одним из ключевых направлений развития отечественного производства изделий микроэлектроники должно являться обеспечение безопасности и качества производимых изделий, что требует внедрения комплекса нормативно-технических мероприятий по противодействию возможным угрозам.

Заключение

Таким образом, новейшая микроэлектроника в интересах оборонно-промышленного комплекса является одной из наиболее динамично развивающихся обла-стей промышленности, следующий этап развития которой сопряжён с использованием квантовых эффектов. Для их применения технологическое оборудование микроэлектронного производства должно основываться на передовых научно-технических достижениях в первую очередь в военных научно-исследовательских центрах и институтах, быть автоматизированным и работать в составе адаптивных робототехнических комплексов. Ключевое значение для производства изделий микроэлектроники имеет качество выпускае-мой продукции, повышение которого напрямую связано с экономическим благополучием отечественных предприятий и обороноспособностью нашего государства в условиях современного мира.

Литература:

1. Малькова Н.Ю., Петрова М.Д., Кирьянова М.Н. Условия труда и функциональное состояние органа зрения работающих в современном производстве изделий микроэлектроники // Гигиена и санитария. 2020. № 99 (6). – С. 591–596.
2. Инновационные технологии и оборудование субмикронной электроники / А.П. До-станко [и др.]; под ред. акад. НАН Беларуси А.П. Достанко. – Минск: Белорусская наука, 2020. – 263 с. ISBN: 978-985-08-2521-6
3. Сиротин Д.В. Состояние и возможности развития российской микроэлектронной отрасли // Экономическое возрождение России. – 2021. – № 3 (69). – С. 105–122.
4. Белоусова Н.Н., Плис Н.И. Проблемы диверсификации производства на предприятиях оборонно-промышленного комплекса Российской Федерации: на примере микроэлектроники // Экономические и социально-гуманитарные исследования. – 2019. – № 3 (23). – С. 14–21.
5. Эннс В. Меры по развитию отечественной микроэлектроники в современных условиях // Электроника: Наука, технология, бизнес. – 2022. – № 6 (217). – С. 86–93. – DOI: 10.22184/1992-4178.2022.217.6.86.92
6. Алмаметов В.Б. Современные проблемы развития микроэлектроники / В.Б. Алмаме-тов // Труды международного симпозиума «Надёжность и качество». – 2020. – Т. 1. – С. 17–19.
7. Демидов А.А., Рыбалка С.Б. Современные и перспективные полупроводниковые материалы для микроэлектроники следующего десятилетия (2020-2030 гг.) // Прикладная математика 2021. № 53 – С. 53–72.
8. Белоус А., Солодуха В. Основные тенденции развития, проблемы и угрозы современной микроэлектроники // Компоненты и технологии. 2029. № 10. С. 6–14.
9. Болсынов М.Ы. Особенности современного производства изделий микроэлектроники // Аллея науки. 2023. Т. 1. № 7 (82). С. 546–551.
10. Кирпичников А.П., Васильев С.Н. Особенности современной микроэлектроники и вопросы построения систем управления высокой надежности и безопасности // Надежность. 2017. Т. 17. № 3 (62). С. 10–16.

MODERN DEVELOPMENT MICROELECTRONICS IN DEFENSIVE INDUSTRY OF RUSSIA

Bazir G.I.[1], Kuzina E.I.[2], Konstantinova A.A.[3]

Keywords: *microelectronics, microelectronics manufacturing, automation, new technologies, sem-iconductor materials.*

Abstract:

Objective: *to study the peculiarities of modern production of microelectronics products in the sphere of defense industry. To achieve it, analytical, synthetic, inductive and deductive methods of pro-cessing case studies, scientific publications and relevant literary sources were used.*

Research method: *analysis of the peculiarities of modern production of microelectronics products at the enterprises of the defense-industrial complex and identification of the direction of microelectronics development in the Russian Federation. Consideration of the potential and role of the microelectronics industry in the modern technological mode, actual problems that arise in the design and manufacture of microelectronics products.*

Results: *a comparative analysis of trends in the development of modern microelectronics and its implementation in the defense industry of the Russian Federation (RF) was carried out, taking into ac-count the experience of a special military operation*

Practical value: *on the basis of comparative analysis the perspective directions of microelectron-ics development in the defense industry of the Russian Federation are determined.*

References

1. Mal'kova N.Ju., Petrova M.D., Kir'janova M.N. Uslovija truda i funkcional'-noe sos-tojanie organa zrenija rabotajushhih v sovremennom proizvodstve izdelij mikrojelek-troniki // Gigiena i sanitarija. 2020. № 99 (6). – S. 591–596.
2. Innovacionnye tehnologii i oborudovanie submikronnoj jelektroniki / A.P. Dostanko [i dr.]; pod red. akad. NAN Belarusi A.P. Dostanko. – Minsk: Belorusskaja nauka, 2020. – 263 s. ISBN: 978-985-08-2521-6
3. Sirotin D.V. Sostojanie i vozmozhnosti razvitija rossijskoj mikrojelektron-noj otrasli // Jekonomicheskoe vozrozhdenie Rossii. – 2021. – № 3 (69). – S. 105–122.
4. Belousova N.N., Plis N.I. Problemy diversifikacii proizvodstva na pred-prijatijah obo-ronno-promyshlennogo kompleksa Rossijskoj Federacii: na primere mikro-jelektroniki // Jekonomiches-kie i social'no-gumanitarnye issledovanija. – 2019. – № 3 (23). – S. 14–21.
5. Jenns V. Mery po razvitiju otechestvennoj mikrojelektroniki v sovremennyh uslovijah // Jelektronika: Nauka, tehnologija, biznes. – 2022. – № 6 (217). – S. 86–93. – DOI: 10.22184/1992-4178.2022.217.6.86.92
6. Almametov V.B. Sovremennye problemy razvitija mikrojelektroniki / V.B. Almametov // Trudy mezhdunarodnogo simpoziuma «Nadjozhnost' i kachestvo». – 2020. – T. 1. – S. 17–19.
7. Demidov A.A., Rybalka S.B. Sovremennye i perspektivnye poluprovodniko-vye materi-aly dlja mikrojelektroniki sledujushhego desjatiletija (2020-2030 gg.) // Prikladnaja matematika 2021. № 53 – S. 53–72.
8. Belous A., Soloduha V. Osnovnye tendencii razvitija, problemy i ugrozy so-vremennoj mikrojelektroniki // Komponenty i tehnologii. 2029. № 10. S. 6–14.
9. Bolsynov M.Y. Osobennosti sovremennogo proizvodstva izdelij mikrojelek-troniki // Al-leja nauki. 2023. T. 1. № 7 (82). S. 546–551.
10. Kirpichnikov A.P., Vasil'ev S.N. Osobennosti sovremennoj mikrojelektroni-ki i voprosy postroenija sistem upravlenija vysokoj nadezhnosti i bezopasnosti // Nadezh-nost'. 2017. T. 17. № 3 (62). S. 10–16.

[1]Gennady I. Bazir, Ph.D. (in Math.), Associate Professor, Associate Professor of the 2nd Department of the Mil-itary Academy of Communications, St. Petersburg, Russia. E-mail: gennadiy.bazir@gmail.com
[2]Ekaterina I. Kuzina, Lecturer of the 2nd Department of the Military Academy of Communications, St. Peters-burg, Russia. E-mail: 78_kuzik@mail.ru
[3]Anna A. Konstantinova, Candidate of Technical Sciences, Senior Lecturer of the 2nd Department of the Mili-tary Academy of Communications, St. Petersburg, Russia. E-mail: konstantinova.a.a@mail.ru

ВИРТУАЛЬНАЯ РЕАЛЬНОСТЬ В МОДЕЛИРОВАНИИ БОЕВЫХ ДЕЙСТВИЙ И ПОДГОТОВКЕ ПЕРСОНАЛА

Яровой Р.В.[1], Изотов Д.Ю.[2], Лукашенок В.И.[3]

DOI:10.24682/3034-40-50-2024-2-25-36

Ключевые слова: *виртуальные тренировки, психологическая реабилитация, посттравматическое стрессовое расстройство, командная работа, индивидуализированное обучение, когнитивные навыки, боевая готовность, адаптация технологий, экспозиционная терапия, стрессоустойчивость, симуляционные сценарии.*

Аннотация

Цель *работы: проанализировать возможности виртуальной реальности для повышения эффективности военной подготовки, а также оценить его потенциал в психологической реабилитации военнослужащих.*

Метод *исследования: анализ существующих технологий виртуальной реальности, их применение в рамках тренировочных программ.*

Результаты *исследования: использование виртуальной реальности значительно улучшает подготовку военнослужащих, позволяя им отрабатывать сложные сценарии в безопасных условиях. Научные предложения включают рекомендации по дальнейшему совершенствованию технологий виртуальной реальности для адаптации их к специфическим задачам различных подразделений, а также интеграции виртуальной реальности в программы профессиональной подготовки и психологической поддержки. Технология предлагает значительные перспективы для создания индивидуализированных программ обучения, которые могут повысить боеготовность и психологическую устойчивость военнослужащих.*

Научная новизна: *заключается в предложении новых подходов к синхронизации виртуальных сценариев с реальными боевыми условиями, что способствует улучшению когнитивных и тактических навыков военнослужащих.*

Введение

Современные военные технологии стремительно развиваются, открывая новые возможности для повышения эффективности подготовки военного персонала и моделирования боевых действий. Одним из наиболее перспективных инструментов в этой области является виртуальная реальность (*VR*). Виртуальные симуляции позволяют воспроизводить боевые сценарии с высокой степенью реализма, предоставляя военнослужащим возможность тренироваться в условиях, максимально приближенных к реальным. Это особенно важно в современных условиях, когда быстрота реакции, точность действий и адаптивность к меняющимся обстоятельствам могут стать решающими факторами успеха на поле боя.

Использование *VR* для подготовки военнослужащих и моделирования боевых действий значительно расширяет возможности традиционных методов обучения, позволяя избежать высоких затрат, связанных с проведением полевых учений, и минимизировать риски для участников. Кроме того, технологии виртуальной реальности позволяют многократно воспроизводить сложные и опасные боевые ситуации, обеспечивая персоналу многогранную подготовку и отработку навыков в различных условиях [1].

История развития VR-технологий

Технологии виртуальной реальности (*VR*) имеют долгую историю развития, начиная с простейших симуляторов и заканчивая современными высокотехнологичными системами, способными воспроизводить сложные и реалистичные сценарии. Первые упоминания о *VR* связаны с разработкой пилотных тренажеров в середине XX века, которые использовались для обучения пилотов без необходимости реальных полетов. С тех пор *VR*-технологии значительно эволюционировали, и сегодня их применение охватывает не только авиацию, но и другие виды военной подготовки, включая моделирование боевых действий, обучение тактическим операциям и взаимодействию в сложных боевых условиях.

[1]Яровой Роберт Владимирович, научный сотрудник научно-исследовательского центра Военной академии связи, г. Санкт-Петербург, Россия. E mail: Nadzar@yandex.ru

[2]Изотов Даниил Юрьевич, младший научный сотрудник научно-исследовательского центра Военной академии связи, г. Санкт-Петербург, Россия. E mail: daniil.izotov.1999@mail.ru

[3]Лукашенок Василий Ильич, младший научный сотрудник научно-исследовательского центра Военной академии связи, г. Санкт-Петербург, Россия. E mail: lukasenokvasilij@gmail.com

Современные исследования показывают, что использование виртуальной реальности позволяет существенно повысить уровень подготовки персонала за счет более глубокого погружения в обучающие сценарии и многократного повторения сложных операций. Работы таких авторов, как [2], демонстрируют преимущества *VR* для тренировки военнослужащих, включая снижение стресса при реальных боевых операциях и улучшение навыков принятия решений в критических ситуациях. Другие исследования [3] подчеркивают важность использования *VR* для моделирования сложных и опасных ситуаций, что позволяет безопасно отрабатывать сценарии взаимодействия в условиях боя.

Помимо этого, значительное внимание уделяется разработке специализированных программных платформ и симуляторов, которые могут быть интегрированы с системами управления и анализа данных. Такие технологии, как симуляционные комплексы *VBS3* и *Bohemia Interactive Simulations*, уже активно применяются военными структурами различных стран для моделирования как тактических операций, так и стратегического планирования. Эти платформы позволяют создавать масштабные сценарии, имитирующие поведение войск, техники и объектов в реальном времени.

Таким образом, обзор существующей литературы свидетельствует о высоком потенциале виртуальной реальности в военной подготовке и моделировании боевых действий. Однако, несмотря на значительные достижения, остается ряд нерешенных вопросов, связанных с техническими ограничениями, интеграцией *VR* с другими технологиями и экономической эффективностью подобных систем.

Технологические аспекты виртуальной реальности

Виртуальная реальность (*VR*) представляет собой комплекс технологий, включающий в себя аппаратные и программные компоненты, которые совместно создают интерактивную и иммерсивную среду, воспроизводящую реалистичные сценарии. В этом разделе будут рассмотрены ключевые технологические аспекты *VR*, используемые для моделирования боевых действий и подготовки персонала, включая аппаратное обеспечение, программное обеспечение и возможности интеграции *VR* с другими современными технологиями [4].

Аппаратное обеспечение

Основными элементами аппаратного обеспечения виртуальной реальности являются *VR*-шлемы, контроллеры и различные датчики. Современные *VR*-шлемы, такие как *Oculus Rift, HTC Vive*, и более специализированные устройства для военных нужд, обеспечивают пользователю полное погружение в виртуальное пространство благодаря высокому разрешению экранов, широкому полю зрения и точному отслеживанию движений головы. Контроллеры позволяют взаимодействовать с виртуальной средой, обеспечивая естественные жесты и манипуляции. В некоторых системах используются тактильные перчатки, которые добавляют осязательные ощущения, что повышает уровень реализма тренировок.

Дополнительно могут использоваться трекеры движений тела, платформы для ходьбы (например, *Virtuix Omni*), которые позволяют пользователю перемещаться по виртуальной среде естественным образом. Эти устройства особенно важны в контексте военной подготовки, где точное воспроизведение движений и взаимодействия с окружением имеет критическое значение.

Программное обеспечение и симуляционные платформы

Программное обеспечение для виртуальной реальности включает в себя как готовые симуляционные платформы, так и инструменты для создания специализированных сценариев. Одной из наиболее популярных платформ для военных нужд является *VBS3* (*Virtual Battlespace 3*), разработанная *Bohemia Interactive Simulations*. Эта платформа позволяет создавать детализированные сценарии боевых действий, включая различные виды местности, погодные условия, поведение войск и техники.

Другие программные решения, такие как *Unity3D* и *Unreal Engine*, широко используются для разработки кастомизированных симуляторов, которые могут быть адаптированы под конкретные требования военных структур. Эти движки позволяют создавать высоко реалистичные виртуальные среды с поддержкой физики, освещения и искусственного интеллекта, что делает их идеальными для моделирования сложных тактических операций[4].

Интеграция VR с другими технологиями

Одним из важных направлений развития *VR* является интеграция с другими современными технологиями, такими как искусственный интеллект (*ИИ*), машинное обучение и анализ больших данных. Искусственный интеллект позволяет создать более реалистичное поведение виртуальных противников и союзников, делая симуляции динамичными и непредсказуемыми. Машинное обучение, в свою очередь, может быть использовано для адаптации сценариев под уро-

[4]URL: https://vr-perm.ru/edu_content (Дата обращения: 02.09.2024)

вень подготовки конкретных военнослужащих, предлагая индивидуализированные тренировки и оценки.

Кроме того, интеграция *VR* с системами анализа больших данных позволяет собирать и обрабатывать огромные массивы информации, получаемой во время тренировок. Это дает возможность командованию проводить детальный анализ действий персонала, выявлять ошибки и предлагать пути их исправления. Такие системы уже начинают применяться в передовых армиях мира, повышая эффективность подготовки и оперативности принятия решений.

Таким образом, технологическая инфраструктура виртуальной реальности в военной сфере включает в себя как аппаратные средства для создания иммерсивной среды, так и программные решения, обеспечивающие реалистичность и адаптивность сценариев. Интеграция с другими технологиями, такими как ИИ и большие данные, позволяет значительно расширить возможности *VR*, делая её незаменимым инструментом для подготовки и моделирования в современных вооружённых силах.

Социально-культурные аспекты внедрения VR в военные структуры

Технологии виртуальной реальности (*VR*) постепенно становятся важной частью военной подготовки, однако их внедрение не ограничивается только техническими аспектами. Важную роль играют социальные и культурные последствия использования *VR*, которые затрагивают как традиционные методы обучения, так и внутренние процессы военных структур. Этот раздел исследует, как использование *VR* влияет на военную культуру, социальные аспекты взаимодействия военнослужащих и их профессиональное развитие.

Влияние на военную культуру и традиции

Военные структуры традиционно опираются на устоявшиеся методы подготовки, многие из которых веками передавались от одного поколения солдат к другому. Такие методы включают практическую тренировку в полевых условиях, физическое взаимодействие с реальной техникой и соблюдение строгой дисциплины. Внедрение *VR* нарушает эти традиции, предоставляя новый, цифровой подход к обучению. Это может вызвать сопротивление со стороны более консервативных элементов военных организаций, которые привыкли к физическим, реальным условиям обучения.

Тем не менее, *VR* не отменяет военные традиции, а предлагает более гибкие и современные методы подготовки, которые могут дополнять классические подходы. Например, вместо полевых учений, которые могут быть редкими и дорогостоящими, *VR* позволяет военнослужащим часто повторять сценарии, отрабатывать действия в сложных ситуациях и улучшать навыки взаимодействия в группе. Это не только сохраняет дисциплинарные и тактические основы обучения, но и усиливает их за счет технологических возможностей.

Социальные последствия для военнослужащих

Одной из важных сторон внедрения *VR* в военную подготовку является влияние на межличностное взаимодействие среди военнослужащих. Традиционные методы обучения предполагают тесное физическое взаимодействие, что способствует созданию духа товарищества и командной работы. Виртуальная реальность может уменьшить эти аспекты, поскольку тренировки проходят в цифровой среде, где непосредственный контакт между людьми минимален. Это может привести к снижению уровня социальной сплоченности, что особенно важно в боевых ситуациях, когда доверие и взаимодействие внутри команды играют ключевую роль.

С другой стороны, *VR* позволяет имитировать коллективные действия и командные сценарии, где солдаты учатся взаимодействовать друг с другом в виртуальной среде, что также способствует развитию навыков работы в команде. Более того, виртуальная реальность может облегчить тренировки военнослужащих, находящихся в разных географических точках, что особенно важно для международных коалиций или подразделений, выполняющих задачи за рубежом. Это позволяет наладить взаимодействие между военнослужащими, которые в реальной жизни могут не пересекаться до момента совместного выполнения боевых задач [5].

Профессиональное развитие и карьерный рост

Использование *VR* в военной подготовке также открывает новые возможности для профессионального роста военнослужащих. С одной стороны, *VR* предлагает персонализированные программы обучения, которые можно адаптировать под конкретные нужды и слабые стороны каждого солдата. Это позволяет улучшить индивидуальные навыки, что в свою очередь способствует ускорению продвижения по службе.

Кроме того, внедрение *VR* требует от военных структур создания новых должностей и специализаций, связанных с разработкой, управлением и поддержкой *VR*-систем. Появляются

такие профессии, как операторы виртуальных тренажеров, разработчики сценариев боевых действий в виртуальной реальности, технические специалисты по *VR* и инструкторы по использованию новых технологий. Это создает дополнительные возможности для профессионального роста в новых направлениях, повышая конкурентоспособность военнослужащих на рынке труда как внутри, так и за пределами военной службы.

Внедрение виртуальной реальности в военные структуры имеет глубокие социально-культурные последствия. С одной стороны, оно меняет традиционные методы подготовки, требуя адаптации устоявшихся процессов и норм. С другой стороны, оно открывает новые возможности для профессионального развития, межличностного взаимодействия и модернизации военной культуры. *VR*-технологии помогают создавать более гибкую и современную военную систему, которая может быстрее адаптироваться к вызовам современного мира, сохраняя при этом ключевые элементы командной работы и дисциплины.

Применение VR в моделировании боевых действий

Виртуальная реальность (*VR*) открывает новые горизонты в моделировании боевых действий, предоставляя возможности для создания детализированных и реалистичных сценариев, которые можно использовать как для тренировки военнослужащих, так и для анализа тактических решений. В этом разделе будут рассмотрены основные аспекты применения *VR* в моделировании боевых действий, включая сценарии симуляций, преимущества использования *VR* и сравнение с традиционными методами моделирования.

Сценарии и типы симуляций

Одним из ключевых преимуществ *VR* является возможность создания широкого спектра сценариев боевых действий, от тактических операций до масштабных сражений. Симуляции могут включать различные типы местности, погодные условия, время суток и другие факторы, влияющие на ход боевых действий. Такие сценарии позволяют моделировать действия как на уровне небольших подразделений, так и на уровне крупных военных формирований.

Примеры симуляций включают:

- **тренировка пехотных подразделений:** симуляция городских боевых действий, зачистка зданий, взаимодействие с союзниками и противодействие скрытым угрозам;
- **бронетанковые операции:** управление танками и бронетехникой в условиях открытой местности, взаимодействие с артиллерией и авиацией;
- **воздушные операции:** симуляции боевых вылетов, воздушных боев и операций по поддержке наземных сил;
- **морские операции:** моделирование действий флота, включая противолодочные операции и высадку десанта.

Каждый из этих сценариев может быть адаптирован в реальном времени, что позволяет создавать динамичные и непредсказуемые условия, требующие от военнослужащих быстрой адаптации и принятия решений.

Преимущества использования VR для моделирования

Виртуальная реальность предоставляет ряд значительных преимуществ перед традиционными методами моделирования боевых действий:

- **реалистичность:** *VR* позволяет создать иммерсивную среду, в которой военнослужащие могут полностью погрузиться в сценарий боевых действий. Это улучшает восприятие и усвоение навыков, которые впоследствии могут быть использованы в реальных условиях;
- **безопасность:** виртуальные симуляции позволяют отрабатывать сложные и опасные операции без риска для жизни и здоровья военнослужащих. Это особенно важно при подготовке к операциям в экстремальных условиях;
- **повторяемость:** в отличие от полевых учений, *VR*-сценарии могут быть многократно воспроизведены, что позволяет тренировать определенные навыки до тех пор, пока они не будут отработаны до совершенства;
- **гибкость и адаптивность:** сценарии могут быть быстро изменены или адаптированы в зависимости от целей тренировки, что делает *VR* идеальным инструментом для подготовки различных категорий военнослужащих.

Сравнение VR-симуляций с традиционными методами

Хотя традиционные методы моделирования, такие как полевые учения и настольные игры, по-прежнему занимают важное место в военной подготовке, виртуальная реальность предлагает уникальные возможности, которые невозможно достичь с помощью других средств:

- **полевые учения:** учения дают реальное физическое ощущение условий боя, но они требуют больших ресурсов, времени и финансовых затрат. *VR*-симуляции, напротив, более экономичны и могут проводиться в любое время и в любом месте;

- **настольные игры и компьютерные симуляторы:** хотя они позволяют моделировать стратегические и тактические операции, они ограничены двухмерным представлением и отсутствием полного погружения. *VR* предлагает 360-градусную перспективу, повышая уровень погружения и восприятия;
- **киберучения:** упражнения нацелены на кибербезопасность и защиту информационных систем. Хотя они важны, *VR* может дополнить их, моделируя последствия кибератак в физическом пространстве боевых действий.

Использование виртуальной реальности в моделировании боевых действий предоставляет уникальные преимущества, которые могут существенно повысить уровень подготовки военнослужащих и улучшить стратегическое планирование. Благодаря возможностям *VR*, военные структуры могут проводить тренировки в условиях, максимально приближенных к реальным, что значительно повышает боеготовность и оперативные способности[5].

Подготовка персонала с использованием VR

Виртуальная реальность (*VR*) становится неотъемлемой частью подготовки военного персонала, предоставляя уникальные возможности для обучения, тренировки и оценки навыков в условиях, максимально приближенных к реальным боевым действиям. В этом разделе будут рассмотрены ключевые аспекты использования *VR* для подготовки персонала, включая методы обучения, психологические и физиологические аспекты, а также примеры успешного применения *VR* в военных учебных центрах.

Обучение и тренировки

VR предоставляет военнослужащим возможность отрабатывать широкий спектр навыков — от базовых до сложных, связанных с конкретными военными операциями. Основные направления применения *VR* в обучении и тренировках включают:

- **тактические тренировки:** симуляция боевых действий в различных условиях, включая городской бой, лесистую местность или пустыню. Виртуальная среда позволяет военнослужащим отрабатывать тактические маневры, взаимодействие в команде и принятие решений под давлением;
- **обучение эксплуатации техники:** *VR* позволяет военнослужащим изучать и тренироваться в управлении сложной техникой, такой как танки, самолеты или корабли, без риска повреждения оборудования и в условиях, недоступных в реальной жизни;
- **отработка действий в чрезвычайных ситуациях:** моделирование сценариев аварийных ситуаций, таких как утечка химикатов, пожар или атака с использованием оружия массового поражения. Это позволяет военнослужащим подготовиться к быстрому реагированию и минимизации последствий таких инцидентов;
- **психологическая подготовка:** виртуальные сценарии, моделирующие стрессовые или экстремальные ситуации, помогают военнослужащим развивать устойчивость к стрессу и улучшать свои навыки принятия решений в критических условиях.

Психологические и физиологические аспекты

Одним из ключевых преимуществ использования VR в военной подготовке является возможность воспроизведения реалистичных сценариев, которые вызывают эмоциональные и физиологические реакции, сходные с теми, которые могут возникнуть в реальных боевых условиях. Это включает:

- **управление стрессом:** регулярные тренировки в виртуальной среде, имитирующей боевые условия, помогают военнослужащим развить психологическую устойчивость, уменьшая уровень стресса и повышая их способность к концентрации и контролю эмоций в экстремальных ситуациях;
- **физическая активность:** в некоторых VR-тренировках используется оборудование, которое требует активного передвижения, что способствует физическому развитию и поддержанию формы военнослужащих;
- **эффект присутствия:** виртуальная реальность создает сильное ощущение присутствия в боевой обстановке, что позволяет военнослужащим более глубоко погружаться в тренировочные сценарии и получать более реалистичный опыт.

Кейс-стади: Примеры успешного применения VR в военных учебных центрах

Применение *VR* в военной подготовке уже доказало свою эффективность в ряде вооруженных сил по всему миру. Вот несколько примеров:

- **армия США:** в США широко используются *VR*-тренажеры для подготовки солдат, особенно в таких областях, как пилотирование беспилотных летательных аппаратов, пехотные маневры и действия в условиях городского боя. Вирту-

[5]URL: https://vr-app.ru/blog/primenenie-vr-texnologii-v-armii-i-voennoi-podgotovke/ (Дата обращения: 04.09.2024)

альные полигоны позволяют военнослужащим отрабатывать действия в различных сценариях, включая борьбу с повстанческими группировками и участие в миротворческих операциях;

- **Британская армия:** в Великобритании активно используют *VR* для обучения тактическим действиям, в том числе в сложных условиях, таких как действия в горной местности или под водой. Британские военные учебные центры также применяют *VR* для подготовки операторов танков и бронетехники;
- **Израильские вооруженные силы:** Израиль использует *VR* для подготовки военнослужащих к операциям в условиях городских боев, что особенно актуально для страны, где значительная часть боевых действий происходит в плотнозаселенных районах. Виртуальные симуляции позволяют солдатам отрабатывать действия по зачистке зданий, взаимодействию с гражданским населением и противодействию террористическим угрозам.

Эти примеры демонстрируют, что виртуальная реальность стала важным инструментом военной подготовки, обеспечивая более безопасные, экономически эффективные и гибкие возможности для обучения. Благодаря *VR*, военнослужащие могут получить необходимый опыт и развить навыки, которые позволят им более уверенно действовать в реальных боевых условиях[6].

Проблемы и вызовы внедрения VR в военную подготовку

Несмотря на очевидные преимущества виртуальной реальности (*VR*) в военной подготовке, её внедрение сталкивается с рядом проблем и вызовов, которые необходимо преодолеть для максимально эффективного использования технологий. Далее будут рассмотрены основные трудности, связанные с внедрением *VR*, включая технические ограничения, затраты, адаптацию и обучение персонала, а также вопросы безопасности и этики.

Технические ограничения

Одним из основных технических вызовов является высокая потребность *VR* в вычислительных мощностях. Для создания реалистичных и детализированных симуляций требуется значительное количество ресурсов, включая мощные графические процессоры и специализированное оборудование. Кроме того, современные *VR*-системы могут столкнуться с проблемами производительности при одновременном обучении большого количества военнослужащих или моделировании сложных сценариев, включающих множество участников и объектов.

Другой важной технической проблемой является ограниченная физическая свобода движения. Хотя существуют решения, такие как платформы для ходьбы и трекеры движений, они все еще не могут полностью заменить реальные физические ощущения, особенно при обучении в сложных условиях, таких как пересеченная местность или подводные операции.

Высокие затраты на внедрение

Разработка, приобретение и обслуживание *VR*-систем связаны с высокими затратами, что может стать значительным барьером для их широкого внедрения. Военным структурам необходимо инвестировать не только в оборудование, но и в программное обеспечение, а также в обучение персонала, что требует значительных финансовых ресурсов. Кроме того, обновление и модернизация *VR*-систем могут быть сложными и затратными, особенно с учетом быстрого развития технологий.

Адаптация и обучение персонала

Успешное внедрение *VR* требует адаптации учебных программ и обучения персонала использованию новых технологий. Это может быть сложной задачей, особенно для тех, кто не имеет опыта работы с *VR* или компьютерными технологиями в целом. Военные структуры должны разработать новые методики обучения и тренировок, которые будут учитывать особенности виртуальной среды, а также обучать инструкторов и технический персонал для поддержки этих программ.

Вопросы безопасности и этики

Использование *VR* в военной подготовке также поднимает вопросы безопасности и этики. Одним из основных аспектов является безопасность данных и защита информации. *VR*-системы могут собирать и хранить большое количество данных о пользователях и сценариях тренировок, что делает их потенциальными целями для кибератак. Военным структурам необходимо обеспечивать надежную защиту данных и разрабатывать протоколы безопасности для предотвращения утечек информации.

Кроме того, этические вопросы возникают в связи с возможным воздействием виртуальных симуляций на психику военнослужащих. Постоянное погружение в боевые сценарии и стрессовые ситуации может вызывать психологические

[6]URL: https://www.ixbt.com/news/2017/05/09/garnitury-virtualnoj-realnosti-pomogajut-izrailskim-voennym-gotovitsja-k-boevym-dejstvijam-v-tunneljah-.html (Дата обращения: 04.09.2024)

проблемы, такие как посттравматическое стрессовое расстройство (ПТСР). Необходимо учитывать эти риски и разрабатывать стратегии поддержки военнослужащих, проходящих обучение в *VR*-среде.

Проблемы совместимости и стандартизации

Еще одной важной проблемой является совместимость различных *VR*-систем и необходимость стандартизации. Военные структуры часто используют разные программные и аппаратные решения, которые могут быть несовместимы друг с другом. Это создает сложности при интеграции *VR*-систем с существующими тренажерами, симуляторами и системами управления. Разработка общих стандартов и протоколов взаимодействия может стать важным шагом на пути к решению этой проблемы [6].

Перспективы и будущее развитие VR в военной подготовке

Виртуальная реальность (*VR*) стремительно развивается, и её потенциал в военной подготовке далеко не исчерпан. В этом разделе будут рассмотрены перспективы дальнейшего развития *VR*-технологий, возможные направления их совершенствования, а также роль *VR* в будущих концепциях военного обучения и боевой готовности.

Интеграция с искусственным интеллектом и машинным обучением

Одним из ключевых направлений развития *VR* в военной сфере является интеграция с искусственным интеллектом (ИИ) и машинным обучением. Использование ИИ позволяет создавать более сложные и адаптивные сценарии, где поведение противников, союзников и гражданских лиц может динамически изменяться в зависимости от действий пользователя. Это делает тренировки более реалистичными и полезными для развития навыков принятия решений в условиях неопределенности.

Машинное обучение может быть использовано для анализа действий военнослужащих в виртуальной среде, выявления их сильных и слабых сторон, а также для адаптации тренировок под индивидуальные потребности каждого пользователя. В будущем это может привести к созданию полностью персонализированных программ подготовки, которые будут учитывать уровень подготовки, психологические особенности и физические возможности каждого военнослужащего [7].

Расширенная и смешанная реальность

Расширенная (AR) и смешанная реальность (MR) являются естественным продолжением развития *VR*-технологий и также находят своё применение в военной подготовке. AR позволяет накладывать виртуальные элементы на реальный мир, что может быть полезно при тренировках на реальных полигонах или в условиях, приближенных к боевым. MR, в свою очередь, объединяет элементы реального и виртуального миров, создавая более сложные и интерактивные среды для обучения.

Эти технологии открывают новые возможности для интеграции виртуальных сценариев с реальными условиями, что позволяет военнослужащим тренироваться в максимально приближенных к боевым ситуациям, сохраняя при этом возможность анализа и корректировки действий в реальном времени.

Развитие тактильной обратной связи и физических симуляторов

Одной из перспективных областей развития *VR* является усовершенствование тактильной обратной связи, которая позволит пользователям более полно ощущать взаимодействие с виртуальной средой. Развитие технологий, таких как тактильные перчатки, костюмы с датчиками и платформы для ходьбы, сделает тренировки в *VR* еще более реалистичными, позволяя пользователям чувствовать вес объектов, сопротивление, текстуры и другие физические характеристики.

В сочетании с *VR* это может привести к созданию новых типов симуляторов, которые не только визуально, но и физически воспроизводят условия боевых действий. Такие системы могут быть особенно полезны для подготовки к сложным операциям, требующим высокой степени точности и координации движений [8].

Виртуальные тренажеры и дистанционное обучение

Развитие *VR* также открывает новые возможности для дистанционного обучения и использования виртуальных тренажеров. Военные структуры могут создавать централизованные виртуальные учебные центры, к которым военнослужащие смогут подключаться из любой точки мира. Это позволит проводить тренировки и оценку навыков без необходимости физического присутствия в учебных центрах, что особенно актуально в условиях необходимости сокращения расходов и повышения оперативности подготовки.

Виртуальные тренажеры могут быть использованы для отработки как индивидуальных, так и групповых навыков, включая взаимодействие в команде, управление техникой и выполнение сложных тактических маневров. Такие

тренажеры могут стать важным элементом подготовки в условиях постоянного изменения боевых условий и появления новых угроз.

Поддержка принятия решений и стратегическое планирование

В будущем *VR* может сыграть важную роль в поддержке принятия решений и стратегическом планировании. Использование виртуальных симуляций для моделирования различных сценариев боевых действий, анализа их последствий и оценки эффективности стратегий может значительно повысить качество планирования операций. Командование сможет проводить виртуальные военные игры, отрабатывая различные варианты развития событий и готовя персонал к реагированию на неожиданные ситуации.

Влияние на междисциплинарное взаимодействие

VR также может способствовать развитию междисциплинарного взаимодействия, объединяя военных специалистов, ученых, инженеров и стратегов в рамках совместных проектов и тренировок. Это позволит интегрировать различные аспекты военной науки и техники, создавая более комплексные и эффективные системы подготовки и управления.

Перспективы использования виртуальной реальности в военной подготовке весьма многообещающие. В ближайшие годы мы можем ожидать значительных улучшений в технологиях *VR*, что приведет к созданию более реалистичных, адаптивных и эффективных систем подготовки. Интеграция *VR* с ИИ, машинным обучением и другими современными технологиями сделает военные тренировки еще более эффективными, помогая военнослужащим готовиться к будущим вызовам на высоком уровне.

VR как средство психологической реабилитации военнослужащих

Психологическая реабилитация военнослужащих после участия в боевых действиях или выполнения сложных и стрессовых задач становится одной из важных задач современных вооруженных сил. Виртуальная реальность (*VR*) все чаще рассматривается как эффективный инструмент в работе с посттравматическим стрессовым расстройством (ПТСР), а также другими психоэмоциональными нарушениями, возникающими у военнослужащих. В этом разделе будут рассмотрены возможности *VR* в реабилитации, основные направления ее применения, а также примеры успешного использования технологии для восстановления после психологических травм.

Посттравматическое стрессовое расстройство (ПТСР)

Посттравматическое стрессовое расстройство является одной из наиболее распространенных психологических проблем среди военнослужащих, особенно тех, кто участвовал в боевых действиях. Симптомы ПТСР включают ночные кошмары, флешбеки, чувство постоянной тревожности, раздражительность и проблемы с памятью. Эти симптомы могут серьезно повлиять на качество жизни человека и его способность функционировать в обществе.

Традиционные методы лечения ПТСР включают психотерапию, когнитивно-поведенческую терапию и медикаментозное лечение. Однако *VR* предоставляет новую перспективу для работы с ПТСР, позволяя создавать контролируемые, безопасные виртуальные сценарии, которые воспроизводят травматические события, но в управляемой и контролируемой среде. Это помогает пациентам постепенно преодолевать свои страхи и восстанавливать контроль над эмоциями через метод десенсибилизации. *VR* также позволяет повторять терапевтические сессии без необходимости перемещаться в реальные условия, что значительно улучшает доступность лечения [9].

Виртуальная экспозиционная терапия

Одной из наиболее эффективных методик лечения ПТСР с использованием виртуальной реальности является экспозиционная терапия (*VRET — Virtual Reality Exposure Therap*y). В рамках этой терапии пациенты погружаются в виртуальные сценарии, которые имитируют ситуации, вызывающие у них стрессовые реакции. В отличие от традиционной экспозиционной терапии, где воспоминания и травматические события проигрываются только в воображении пациента, *VR* позволяет создать детализированные и реалистичные обстановки, максимально приближенные к реальным боевым ситуациям.

Под контролем психотерапевта пациент постепенно сталкивается с травмирующими событиями и учится управлять своими эмоциями. Использование *VR* в этой терапии позволяет точно контролировать интенсивность и сложность сценариев, начиная с простых ситуаций и постепенно увеличивая их сложность. Это помогает пациентам проходить процесс реабилитации на более глубоком уровне и в более безопасных условиях, что ускоряет процесс выздоровления.

Реабилитационные программы для восстановления боевых навыков

Кроме работы с ПТСР, *VR* может быть полезна для восстановления боевых навыков и психологической устойчивости военнослужащих после тяжелых ранений или длительных перерывов в службе. С помощью виртуальной реальности можно создавать тренировки, которые помогут военнослужащим вернуться к активной службе после физической или эмоциональной травмы. Виртуальные симуляторы позволяют военнослужащим постепенно адаптироваться к условиям, которые могут быть стрессовыми или вызывать дискомфорт в реальной жизни, без риска повторных травм.

Эти реабилитационные программы могут включать сценарии тренировок, где военнослужащий постепенно восстанавливает свою уверенность в сложных ситуациях. Виртуальные симуляции позволяют улучшить не только психологическое состояние, но и физическую координацию, навыки владения оружием и тактическое мышление, что может помочь военнослужащим вернуться к своим обязанностям в армии.

Психологическая поддержка для ветеранов

Важным аспектом использования *VR* в реабилитации является помощь ветеранам, которые возвращаются к гражданской жизни после военной службы. Многие ветераны сталкиваются с проблемами адаптации в обществе, особенно если они страдают от ПТСР или других психоэмоциональных расстройств. *VR* может быть использована как часть программ интеграции, где ветераны участвуют в виртуальных сценариях, которые помогают им плавно адаптироваться к мирной жизни, справляться с социальными трудностями и восстанавливать социальные связи.

Сценарии могут включать различные аспекты гражданской жизни: от поиска работы до общения с семьей и друзьями. Виртуальная среда позволяет ветеранам отрабатывать различные жизненные ситуации без риска столкновения с реальными последствиями, что помогает им адаптироваться к новым условиям жизни на безопасной и поддерживающей платформе.

Преимущества использования VR в реабилитации

- **безопасная среда:** *VR* позволяет создать контролируемые условия, где пациенты могут работать с травматическими событиями, не подвергаясь риску повторного травмирования;
- **персонализация лечения:** программы *VR* могут быть адаптированы под конкретные потребности каждого пациента, что делает процесс реабилитации более целенаправленным и эффективным;
- **доступность и удобство:** использование *VR* исключает необходимость физического присутствия в определенных локациях для проведения терапии, что значительно облегчает доступ к лечению;
- **интерактивность и вовлеченность:** *VR* создает более интерактивную среду по сравнению с традиционными методами лечения, что помогает пациентам лучше вовлекаться в процесс восстановления.

Использование виртуальной реальности для психологической реабилитации военнослужащих становится важным направлением в медицинских и психологических программах вооруженных сил. *VR* не только помогает лечить ПТСР и другие психоэмоциональные расстройства, но и способствует восстановлению боевых навыков, социальной адаптации и интеграции ветеранов в гражданскую жизнь. В будущем эта технология может стать ключевым элементом комплексных программ реабилитации, предлагая военнослужащим и ветеранам эффективные и безопасные методы лечения и поддержки [10].

Обратная связь и оценка эффективности VR-тренировок

Эффективность внедрения виртуальной реальности (*VR*) в военную подготовку и реабилитацию напрямую зависит от того, насколько качественно и объективно можно оценить результаты использования этой технологии. Оценка эффективности *VR*-тренировок включает различные подходы к анализу их влияния на боевую готовность, развитие навыков, психологическое состояние военнослужащих и другие аспекты. Этот раздел посвящен методам оценки эффективности *VR*-тренировок, а также значению обратной связи от военнослужащих для улучшения и адаптации этих систем.

Методы оценки эффективности VR-тренировок

Оценка эффективности *VR*-тренировок требует комплексного подхода, который включает как количественные, так и качественные методы анализа. Существует несколько ключевых аспектов, которые можно учитывать при оценке эффективности:

1. Оценка боевой готовности и навыков:

- **тестирование навыков до и после тренировки:** один из простейших способов измерить влияние *VR*-тренировок — сравнить уровень навыков военнослужащего до и после участия в виртуальных симуляциях. Это могут быть как физические, так и тактические навыки, например, точность стрельбы, скорость принятия решений, умение взаимодействовать в команде;
- **реальные боевые учения:** сравнение результатов тренировок в виртуальной среде с результатами полевых учений также позволяет оценить, насколько *VR* помогает улучшить готовность к реальным боевым действиям.

2. Когнитивные и психологические показатели:

- **измерение уровня стресса и психоэмоциональной устойчивости:** с помощью биометрических данных (например, частоты сердечных сокращений, уровня кортизола) можно оценить влияние *VR* на стрессоустойчивость военнослужащих в стрессовых сценариях;
- **оценка когнитивных способностей:** тестирование памяти, концентрации внимания и скорости реакции в ходе *VR*-симуляций помогает оценить когнитивные аспекты обучения.

3. Анализ взаимодействия в команде:

- **оценка командной работы:** *VR* позволяет проводить групповые тренировки, где можно анализировать, насколько эффективно члены команды взаимодействуют между собой в виртуальной среде. Это помогает выявлять слабые места в коммуникации и стратегии, что может быть полезно для улучшения совместных действий в реальных боевых ситуациях;
- **роль лидеров и распределение обязанностей:** оценка лидерских качеств и умения распределять задачи внутри команды также может быть частью анализа эффективности *VR*-тренировок.

4. Продолжительность сохранения навыков:

- **долгосрочные результаты:** важно не только оценивать мгновенные улучшения после *VR*-тренировок, но и следить за тем, насколько устойчиво сохраняются полученные навыки и знания в долгосрочной перспективе. Это может быть сделано с помощью повторных тестирований через определенный промежуток времени.

Роль обратной связи от пользователей

Обратная связь от военнослужащих, участвующих в *VR*-тренировках, является важным источником данных для улучшения этих систем и адаптации их под реальные нужды. Военнослужащие, активно использующие *VR* в обучении, могут предоставить информацию о том, насколько удобными, реалистичными и полезными являются виртуальные симуляции. Важные аспекты обратной связи включают:

- **реалистичность сценариев:** военнослужащие могут оценить, насколько точно виртуальные симуляции передают реальные боевые условия, что помогает разработчикам улучшать детали и создавать более правдоподобные сценарии. Например, сценарии могут требовать улучшения по уровню детализации, динамике событий или взаимодействию с виртуальными противниками.
- **пользовательский опыт (UX):** оценка удобства использования *VR*-оборудования и интерфейсов также является важным аспектом обратной связи. Пользователи могут дать рекомендации по улучшению навигации, управления и взаимодействия с виртуальной средой, что сделает тренировки более эффективными и комфортными;
- **психологическое восприятие:** некоторые военнослужащие могут испытывать дискомфорт или стресс вовремя *VR*-тренировок, особенно если они напоминают реальные боевые ситуации. Обратная связь в этом аспекте помогает учитывать психологические границы пользователей и адаптировать сценарии, чтобы они были максимально полезными, но при этом не вызывали излишнего стресса;
- **индивидуализация тренировок:** обратная связь позволяет создать персонализированные программы обучения, которые учитывают индивидуальные особенности и слабые стороны каждого военнослужащего. Например, если определенные навыки требуют больше времени для освоения, тренировочные программы могут быть адаптированы под конкретного солдата;
- **предложения по улучшению технологий:** военнослужащие могут вносить предложения по модернизации *VR*-технологий, таких как улучшение тактильной обратной связи, графики или добавление новых сценариев, что поможет увеличить реалистичность и разнообразие тренировок.

Использование аналитики и данных для улучшения VR-тренировок

Современные *VR*-системы могут собирать большие объемы данных, включая биометрические показатели (сердечный ритм, движения глаз), данные о действиях пользователя (скорость реакции, точность выполнения задач) и другие параметры. Эти данные могут быть про$_{\text{анали-}}$

зированы с помощью алгоритмов машинного обучения и искусственного интеллекта для выявления паттернов и тенденций. Такой подход помогает автоматически адаптировать тренировки, предоставляя каждому пользователю уникальный опыт, основанный на его уровне навыков и психологических особенностях.

Аналитические инструменты также могут помочь в разработке новых тренировочных сценариев, которые будут направлены на устранение слабых мест, выявленных на основе собранных данных. Таким образом, *VR*-системы могут постоянно эволюционировать и становиться более точными и эффективными.

Оценка эффективности *VR*-тренировок и использование обратной связи от военнослужащих играют ключевую роль в развитии и совершенствовании этой технологии. С помощью комплексного анализа данных и обратной связи можно улучшать реалистичность симуляций, адаптировать программы под индивидуальные нужды и повысить общую боевую готовность военнослужащих. *VR* становится не просто инструментом обучения, но и гибкой платформой, способной постоянно улучшаться на основе собранных данных и отзывов пользователей, обеспечивая тем самым эффективную и точную подготовку к боевым действиям.

Заключение

Несмотря на многочисленные вызовы, виртуальная реальность представляет собой мощный инструмент для военной подготовки. Однако для достижения максимальной эффективности требуется преодоление технических, финансовых и организационных барьеров. Важно учитывать вопросы безопасности и этики, а также работать над созданием совместимых и стандартизированных решений, чтобы *VR* могла стать полноценной частью военной подготовки в будущем.

Литература

1. Спицын П. А., Бавула А. А. Новый уровень обучения перспективные формы обучения курсантов с использованием средств виртуальной реальности // Вестник военного образования. 2021. №4. С. 99–103.
2. Полевода И.И., Иваницкий А.Г., Миканович А.С., Пастухов С.М., Грачулин А.В., Рябцев В.Н., Навроцкий О.Д., Лихоманов А.О., Винярский Г.В., Гусаров И.С. Технологии виртуальной и дополненной реальности в образовательном процессе // Вестник университета гражданской защиты МЧС Белоруссии. 2022. Том 6. №1. С.119-142. DOI: 10.33408/2519-237X.2022.6-1.119
3. Иванов В.Е. Зарубин В.П. Вокуев Д.Н. Технология виртуальной реальности при моделировании ЧС / Пожарная безопасность: проблемы и перспективы. 2016. С. 249–251.
4. Волынов М.М., Китов А.А., Горячкин Б.С. Виртуальная реальность: виды, структура, особенности, перспективы развития // E-Scio. 2020. №5. С.795-812. eLIBRARY ID: 42989000
5. Уварина Н. В., Полковников А. В. Анализ и перспективы применения иммерсивных технологий в системе подготовки офицеров российской армии / Современная высшая школа: инновационный аспект №4, 2020. С. 10-19.
6. Дремлюга Р. И. Виртуальная реальность: проблемы правового регулирования // Актуальные проблемы российского права. 2020. №9. С 39–49.
7. Бурцева Д.Я., Менделеев Е.А., Хонин И.Л., Докучаев К.О., Петров Р.В. Разработка VR. Особенности совместимости с нейротехнологиями // Вестник Новгородского государственного университета им. Ярослава Мудрого. 2021.№4. С. 10–14.
8. Воловик М.Г., Борзиков В. В., Полякова А. Г. Технологии виртуальной реальности в комплексной медицинской реабилитации пациентов с ограниченными возможностями (обзор) // Published 12 July 2020 Medicine. DOI:10.20538/1682-0363-2020-2-142-152
9. Воловик М.Г., Белова А.Н., Кузнецов А.Н., Полевая А.В., Воробьева О.В., Халак М.Е. Технологии виртуальной реальности в реабилитации участников боевых действий с посттравматическим стрессовым расстройством (обзор) // СТМ. 2023. №1. С. 74–86.
10. Аксенова Е. И., Горбатов С. Ю.. Технологии виртуальной и дополненной реальности в здравоохранении / М.: ГБУ «НИИОЗММ ДЗМ», 2021. – 40 с.

VIRTUAL REALITY IN COMBAT SIMULATION AND PERSONNEL TRAINING

Yarovoy R.V.[1], Izotov D.Yu.[2], Lukashenok V.I.[3]

Keywords: *virtual training, psychological rehabilitation, post-traumatic stress disorder, teamwork, individualized training, cognitive skills, combat readiness, technology adaptation, exposure therapy, stress resistance, simulation scenarios.*

Abstract

The purpose of the *work: to analyze the possibilities of virtual reality to increase the effectiveness of military training, as well as to assess its potential in the psychological rehabilitation of military personnel.*

Research method: *analysis of existing virtual reality technologies, their application within the framework of training programs.*

Results of the study: *the use of virtual reality significantly improves the training of military personnel, allowing them to practice complex scenarios in a safe environment. Scientific proposals include recommendations for further improvement of virtual reality technologies to adapt them to the specific tasks of various units, as well as the integration of virtual reality into professional training and psychological support programs. significant prospects for the creation of individualized training programs that can increase the combat readiness and psychological resilience of military personnel.*

Scientific novelty *consists in the proposal of new approaches to the synchronization of virtual scenarios with real combat conditions, which contributes to the improvement of cognitive and tactical skills of military personnel·*

References

1. Spicyn P. A., Bavula A. A. Novyj uroven' obuchenija perspektivnye formy obuchenija kursantov s ispol'zovaniem sredstv virtual'noj real'nosti // Vestnik voennogo obrazovanija. 2021. №4. S. 99–103.
2. Polevoda I.I., Ivanickij A.G., Mikanovich A.S., Pastuhov S.M., Grachulin A.V., Rjabcev V.N., Navrockij O.D., Lihomanov A.O., Vinjarskij G.V., Gusarov I.S. Tehnologii virtual'noj i dopolnennoj real'nosti v obrazovatel'nom processe // Vestnik universiteta grazhdanskoj zashhity MChS Belorussii. 2022. Tom 6. №1. S.119-142. DOI: 10.33408/2519-237X.2022.6-1.119
3. Ivanov V.E. Zarubin V.P. Vokuev D.N. Tehnologija virtual'noj real'nosti pri modelirovanii ChS / Pozharnaja bezopasnost': problemy i perspektivy. 2016. S. 249–251.
4. Volynov M.M., Kitov A.A., Gorjachkin B.S. Virtual'naja real'nost': vidy, struktura, osobennosti, perspektivy razvitija // E-Scio. 2020. №5. S.795-812. eLIBRARY ID: 42989000
5. Uvarina N. V., Polkovnikov A. V. Analiz i perspektivy primenenija immersivnyh tehnologij v sisteme podgotovki oficerov rossijskoj armii / Sovremennaja vysshaja shkola: innovacionnyj aspekt №4, 2020. S. 10-19.
6. Dremljuga R. I. Virtual'naja real'nost': problemy pravovogo regulirovanija // Aktual'nye problemy rossijskogo prava. 2020. №9. S 39–49.
7. Burceva D.Ja., Mendeleev E.A., Honin I.L., Dokuchaev K.O., Petrov R.V. Razrabotka VR. Osobennosti sovmestimosti s nejrotehnologijami // Vestnik Novgorodskogo gosudarstvennogo universiteta im. Jaroslava Mudrogo. 2021.№4. S. 10–14.
8. Volovik M.G., Borzikov V. V., Poljakova A. G. Tehnologii virtual'noj real'nosti v kompleksnoj medicinskoj reabilitacii pacientov s ogranichennymi vozmozhnostjami (obzor) // Published 12 July 2020 Medicine. DOI:10.20538/1682-0363-2020-2-142-152
9. Volovik M.G., Belova A.N., Kuznecov A.N., Polevaja A.V., Vorob'eva O.V., Halak M.E. Tehnologii virtual'noj real'nosti v reabilitacii uchastnikov boevyh dejstvij s posttravmaticheskim stressovym rasstrojstvom (obzor) // STM. 2023. №1. S. 74–86.
10. Aksenova E. I., Gorbatov S. Ju.. Tehnologii virtual'noj i dopolnennoj real'nosti v zdravoohranenii / M.: GBU «NIIOZMM DZM», 2021. – 40 s.

[1]Robert V. Yarovoy, Researcher, Research Center, Military Academy of Communications, St. Petersburg, Russia. E mail: Nadzar@yandex.ru

[2]Daniil Yu.Izotov, Junior Researcher, Research Center, Military Academy of Communications, St. Petersburg, Russia. E mail: daniil.izotov.1999@mail.ru

[3]Vasily I. Lukashenok, Junior Researcher, Research Center, Military Academy of Communications, St. Petersburg, Russia. E mail: lukasenokvasilij@gmail.com

ПОВЫШЕНИЕ ПРОПУСКНОЙ СПОСОБНОСТИ РЕТРАНСЛЯТОРА СВЯЗИ ПРИ РАБОТЕ ЗЕМНЫМИ СТАНЦИЯМИ С ПАРЦИАЛЬНЫМИ КАНАЛАМИ

Бурлаков С.О.[1], Драгунов М.Ю.[2]

DOI:10.24682/3034-4050-2024-2-37-42

Ключевые слова: *коэффициент использования частотного ресурса, спутниковая радиолиния, распределение частотного ресурса; скорость передачи канала; помехозащищенность канала; задача о заполнении рюкзака.*

Аннотация

Цель: *рассмотреть особенности распределения частотного ресурса ствола с прямой ретрансляцией для нужд военных потребителей.*

Метод исследования: *рассматриваемый вопрос сводится к решению задачи упаковки частотного ресурса ретранслятора сигналами земных станций с парциальными каналами с учетом требований к качеству канала связи и скорости передачи земных станций. При решении научной задачи использовались методы полного перебора всех подмножеств с дополнительным ограничением.*

Результат: *предложена методика распределения частот ретранслятора связи для работы земных станций с парциальными каналами. Методика позволяет повысить коэффициент использования ресурса ретранслятора и помехоустойчивость радиолиний спутниковой связи при дублировании передаваемой информации в парциальных каналах, а также организовывать сети спутниковой связи, используя парциальные каналы в качестве отдельных направлений связи. Отличие применяемой методики от известных заключается в распределении парциальных каналов одной земной станции по всему стволу ретранслятора связи с учетом помеховой обстановки.*

Научная новизна: *предлагаемая методика распределения частот ретранслятора связи дает возможность перераспределять частотный ресурс не только внутри своей сети, но и между сетями, работающими в одном стволе ретранслятора, с учетом доступного ресурса, помеховой обстановки и требований, предъявляемых к качеству связи.*

Введение

В статье [1, 2] предложена земная станция (ЗС) с возможностью изменения количества трактов передачи и приема. Входной абонентский дискретный поток делится на парциальные каналы (ПК), каждый из которых обрабатывается в своем тракте. В указанной статье представлены структурные схемы трактов передачи и приема ЗС с ПК, подход к делению входного потока при передаче и объединении парциальных каналов при приеме.

Достоинством ЗС с ПК являются: увеличение коэффициента использования частотного ресурса ретранслятора, благодаря использованию его незанятых полос; возможность организовывать сети в стволе с прямой ретрансляцией без использования центральной ЗС; повышение помехозащищенности радиолиний спутниковой связи (СС) путем дублирования передаваемой информации или распределения трактов передачи и приема парциальных каналов по неподавленным частотам; повышение разведзащищенности радиолиний за счет распределения трактов передачи и приема по всей частотной полосе ствола.

Недостатками ЗС с ПК являются: усложнение аппаратуры, которое устраняется использованием цифровой обработки сигналов; усложнение процесса установления и ведения связи, которое должно минимизироваться путем автоматизации указанных процессов; необходимостью реализации в ЗС с ПК подсистемы мониторинга наличия сигналов и помех в стволе ретранслятора.

Постановка задачи распределения частотного ресурса ретранслятора

В полосе частот ствола ретранслятора $\Delta f_{\text{ств}}$ работают ЗС, между соседними сигналами которых имеются M незанятых частотных полос (рис. 1). Каждая i-я частотная полоса ($i = 1…M$) характеризуется набором параметров (f_{i}, Δf_{i}, $p_{\text{ші}}$), где f_{i} — центральная частота; Δf_{i} — частотная ширина; $p_{\text{ші}}$ — мощность шума.

[1]Бурлаков Сергей Олегович, доктор технических наук, профессор, профессор кафедры военных систем космической, радиорелейной, тропосферной связи и навигации Военной академии связи, г. Санкт-Петербург, Россия. E-mail: soburlakov@yandex.ru

[2]Драгунов Михаил Юрьевич, адъюнкт кафедры военных систем космической, радиорелейной, тропосферной связи и навигации Военной академии связи, г. Санкт-Петербург, Россия. E-mail: dragunov1992@mail.ru

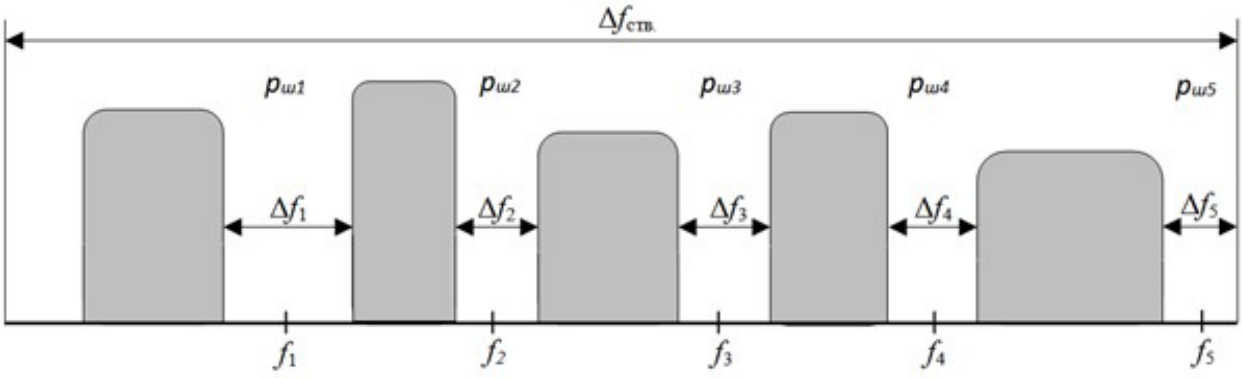

Рис 1. Загрузка ствола ретранслятора связи

Между N ЗС с ПК требуется организовать дуплексные направления спутниковой связи (НСС). Каждая пара ЗС формирует одно НСС, в котором требуемую и реализуемую скорости передачи данных от i-й ЗС обозначим как V_i^* и V_i соответственно. В НСС скорости передачи и приема данных могут как совпадать, так и не совпадать. Поэтому для корреспондирующих i-й и j-й ЗС возможны две ситуации: $V_i^* = V_j^*$, $V_i^* \neq V_j^*$ (рис. 2).

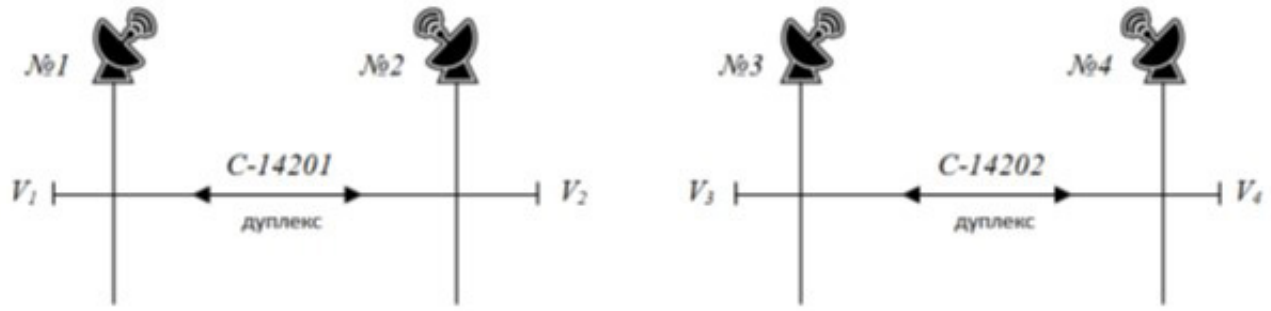

Рис. 2. Вариант схемы спутниковой связи

В соответствии с логикой работы ЗС с ПК каждое НСС реализуется несколькими парциальными каналами, каждый из которых имеет свой тракт передачи и приема (рис. 3) и характеризуется набором параметров ($V_{i,j}$, $f_{i,j}$, $P_{i,j}$, $Mod_{i,j}$, $\mathrm{Kod}_{i,j}$), где i — номер ЗС ($i = 1…N$), L_i — количество парциальных каналов i-й ЗС; j — номер парциального канала ($j = 1…L_i$): $V_{i,j}$ — входная абонентская скорость передачи парциального канала; $f_{i,j}$ — частота несущей радиосигнала; $P_{i,j}$ — мощность радиосигнала; $Mod_{i,j}$ — модуляция радиосигнала; $Kod_{i,j}$ — вид и параметры помехоустойчивого кодирования.

Частотный ресурс ретранслятора между ЗС с ПК должен распределяться с учетом требований к качеству канала связи и скорости передачи ЗС.

Требования к качеству каналов связи определяются вероятностью битовой ошибки

на его выходе и формализуются системой из ($N \cdot L_N$) неравенств:

$$P_{\text{ош } i,j} \geq P^*_{\text{ош}}, \; i=1…N, j=1…L_i \qquad (1)$$

Требования к скорости передачи ЗС задаются системой из N неравенств:

$$\sum_{j=1}^{L_i} V_{i,j} = V_i^*, \; L_i \leq L_i^* \quad i=1…N \qquad (2)$$

где L_i^* максимально допустимое количество парциальных каналов i-й ЗС.

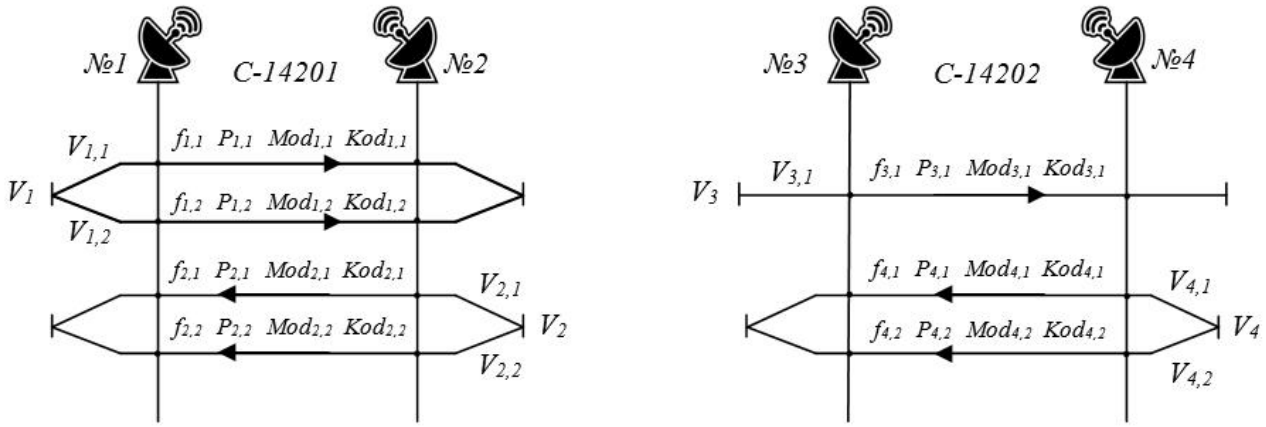

Рис. 3. Вариант реализации схемы спутниковой связи ЗС с ПК

При распределении частотного ресурса необходимо как можно плотнее упаковывать имеющийся частотный ресурс ретранслятора сигналами ЗС с ПК, что формализуется целевой функцией:

$$\left[\sum_{i=1}^{M}\Delta f_i - \sum_{i=1}^{N}\sum_{j=1}^{L_i}\Delta f_{i,j}\right] \xrightarrow{f_{i,j},\,\Delta f_{i,j}} \max \qquad (3)$$

Зависимости $P_{\text{ош i,j}}$ и $\Delta f_{\text{i,j}}$ от ($V_{\text{i,j}}$, $f_{\text{i,}}$ $P_{\text{i,j}}$, $Mod_{\text{i,j}}$, $Kod_{\text{i,j}}$) определяется известными выражениями [3].

В изложенной постановке задача имеет много переменных. Поэтому, исходя

из режимов работы ЗС специального назначения, целесообразно зафиксировать некоторые параметры парциальных радиолиний: модуляция — фазовая двухпозиционная (ФМ-2); кодирование — сверточное (R=1/2, K=5) или (R=3/4, K=7), парциальная мощность на выходе усилителя зависит от распределения абонентских скоростей каналов [4]:

$$P_{\text{вых}\,i,j} = P_{\text{УМ}\,i}\frac{V_{i,j}}{\sum_{j=1}^{L_i}V_{i,j}} \qquad (4)$$

где $P_{\text{ум}_\text{i}}$ мощность усилителя мощности i- й ЗС.

Для каждого парциального радиоканала достижение минимального значения вероятности битовой ошибки возможно за счет обеспечения максимума мощности передатчика [5, 6].

При изменении $V_{\text{i,j}}$ меняется $\Delta f_{\text{i,j}}$. При этом спектральная плотность мощности излучаемого сигнала согласно (4) не меняется, что при одинаковом $p_{\text{ші}}$ не меняет h^2_{ij} на входе парциального приемника. Таким образом, качество парциального канала можно менять только выбором параметров кодирования, что, в свою очередь, также меняет $\Delta f_{\text{i,j}}$.

Методика распределения частот ретранслятора связи для работы земными станциями с парциальными каналами как задача заполнения «Рюкзака»

Рассматриваемая задача сводится к решению задачи упаковки частотного ресурса ретранслятора сигналами ЗС с ПК, с учетом требований к качеству канала связи и скорости передачи ЗС, т. е. распределению $N\,L_{\text{i}}$ сигналов по М незанятым частотным полосам при условии:

$$\sum_{i=1}^{M}\Delta f_i \geq N\cdot L_i\cdot\Delta f_{i,j} \qquad (5)$$

Одним из способов решения этой задачи является полный перебор всех подмножеств из n элементов, которых будет 2^n и выбор среди них наилучшего подмножества, удовлетворяющего условиям задачи. Для каждого значения Δf_{i} будет храниться информация по наилучшему его решению, т. е. наиболее выгодное заполнение частотного интервала для всех возможных $\sum_{i=1}^{M}\Delta f_i$.

Есть две возможности распределения сигналов по частотным полосам, используя первые i сигналов — взять его или нет. Если не брать, то в этом случае:

$$F(i,\sum_{i=1}^{M}\Delta f_i) = F(i-1,\sum_{i=1}^{M}\Delta f_i) \qquad (6)$$

Если брать (при условии выполнения (5)), то останется свободная вместимость $\Delta f_{\text{i}} - \Delta f_{\text{i,j}}$,

которую можно будет заполнить первыми i-1 сигналами, следовательно:

$$F(i,\sum_{i=1}^{M}\Delta f_i) = F(i-1,\sum_{i=1}^{M}\Delta f_i - \Delta f_{i,j}) \qquad (7)$$

Из двух возможных вариантов нужно выбрать вариант, удовлетворяющий условию (3).

Выполняя вышеприведенный алгоритм, получится множество вариантов распределения, оценка которых осуществляется в соответствии с целевой функцией (3) [7, 8].

При планировании распределения частотного ресурса ретранслятора могут вводиться дополнительные ограничения для парциальных каналов, что повлияет на конечное распределение. В этом случае стоит рассмотреть способ решения задачи о распределении частотного ресурса с дополнительным ограничением на типы предметов, где под типом предмета понимается свойство, ограничивающее распределение парциальных каналов по М незанятым частотным полосам.

Рассмотрим свободные частотные полосы М, которые выступают в качестве «рюкзака», с ограничением b^* на возможный максимальный «вес» предметов в нём и множество предметов n. Добавим ограничение: в «рюкзак» можно поместить только d^* типы предметов из n возможных, $d^* \le n$. Каждый i-й тип предметов (i = 1, 2, . . . , n) характеризуется своими характеристиками: a_i, c_i и x_i. Требуется получить «рюкзак» при выполнении ограничений и условия (3).

Для формализации постановки задачи введём в рассмотрение набор булевых переменных $\tilde{x}_i$, $i = 1, 2, \ldots, n$: $\tilde{x}_i = 1$, если хотя бы один предмет i-го типа помещён в «рюкзак», и $\tilde{x}_i = 0$, если ни одного предмета i-го типа в «рюкзаке» нет. Число возможных типов предметов в «рюкзаке» ограничено условием:

$$\sum_{i=1}^{n}\tilde{x}_i \le d^*. \qquad (8)$$

Необходимо максимизировать стоимость предметов в «рюкзаке»:

$$c_1x_1 + c_2x_2 + \ldots + c_nx_n \to \max, \qquad (9)$$

при ограничении:

$$a_1x_1 + a_2x_2 + \ldots + a_nx_n \le b^*. \qquad (10)$$

Используя идеи динамического программирования, рассмотрим множество задач типа (8)–(10).

При d = 1 решается задача отыскания максимума (9) при использовании только предметов одного типа i, $1 \le i \le n$, для заполнения виртуальных «рюкзаков» с максимальными суммарными весами предметов b ($0 \le b \le b^*$):

$$f_1(b) = \max(c_ix_i), \qquad (11)$$

при ограничениях для каждого выбираемого значения x_i и b, удовлетворяющих условиям

$$a_ix_i \le b. \qquad (12)$$

Найденные значения максимумов $f_1(b)$ обозначим для дальнейшего использования как $f1(\Delta b)$, где $\Delta b = b$, $0 \le b \le b^*$, $0 \le \Delta b \le b^*$. Для получения максимума (9) при наполнении «рюкзака» не более чем двумя типами предметов, т. е. при d = 2, будем считать, что часть вместимости «рюкзака» Δb будет выделяться для наполнения вторым типом предметов. Конкретный номер типа предмета будут определяться для каждого виртуального«рюкзака» вместимостью b из выражения:

$$f_2(b) = \max(c_ix_i + f_1(b-\Delta b)) = \max(c_ix_i) + f_1(b-\Delta b), \qquad (13)$$

при ограничениях:

$$1 \le i \le n,\ 0 \le \Delta b \le b,\ 0 \le b \le b^*,\ a_i x_i \le \Delta b. \qquad (14)$$

В (13) $f_1(b-\Delta b)$ представляет собой уже найденное на первом шаге алгоритма максимальное значение стоимости «рюкзака» вместимостью $b-\Delta b$ при его наполнении экземплярами только одного типа предметов при выполнении (11) и (12). Это максимальное значение складывается со значением с, где тип предмета i выбирается из множества {1, 2, . . . , n}, и количество экземпляров этого типа определяется для каждой вместимости «рюкзака» Δb, где $0 \le \Delta b \le b$ при выполнении ограничений (14).

Для получения максимума двух слагаемых, одно из которых имеет фиксированное значение, нужно выбрать предмет типа i, который даёт максимальное значение cixi при вместимости виртуального «рюкзака» Δb и $a_ix_i \le \Delta b$. На первом шаге алгоритма такое значение уже было определено и обозначено как $f_1(\Delta b)$. Следовательно, выражение (13) можно записать так:

$$f_2(b) = \max(f_1(\Delta b) + = \max(c_ix_i) + f_1(b-\Delta b), \qquad (15)$$

при $0 \le \Delta b \le b$, $0 \le b \le b^*$.

Продолжая процесс, получим рекуррентное уравнение относительно числа типов предметов, используемых при заполнении гипотетических «рюкзаков»:

$$f_d(b) = \max(f_1(\Delta b) + f_{d-1}(b-\Delta b), \qquad (16)$$

для всех $0 \le \Delta b \le b$, $0 \le b \le b^*$, d = 2, 3, . . . , d^* [9, 10]. Повышение помехозащищенности радиолиний СС достигается путем дублирования передаваемой информации по незанятым частотным полосам или распределения трактов передачи и

приема парциальных каналов по неподавленным частотам, что планируется в ходе выделения M частотных полос.

Выводы

В статье рассмотрена постановка задачи распределения частотного ресурса ретранслятора связи, вариант реализации схемы спутниковой связи ЗС с ПК, предложена методика распределения частот ретранслятора при работе ЗС с парциальными каналами.

Приведенная методика кроме повышения коэффициента использования частотного ресурса ретранслятора, позволит повысить помехоустойчивость радиолиний в случае дублирования передаваемой информации в парциальных каналах, а также организовывать сети спутниковой связи, используя парциальные каналы в качестве отдельных направлений связи.

Литература

1. Цветков К.Ю., Бурлаков С.О., Климов И.С. Распределение частот ретранслятора связи при работе земных станций с парциальными каналами // Труды Военно-космической академии имени А. Ф. Можайского. 2020. № 672. С. 88–91.
2. Бурлаков С.О., Смирнов А.А., Цветков К.Ю. Научно-технические предложения по реализации методики распределения частотно-энергетического ресурса земных станций и бортовых радиотехнических комплексов высокоскоростных систем спутниковой связи // Труды Военно-космической академии имени А. Ф. Можайского. 2020. № 673. С. 68–78.
3. Немировский М.С., Локшин Б.А., Аронов Д.А. Основы построения систем спутниковой связи / Под ред. М.С. Немировского. – М.: Горячая линия – Телеком, 2018.
4. Бурлаков С.О., Веркин С.С., Егрушев В.Е., Антонов В.В. Методика оценки требуемой мощности передатчика земной станции // Инновации. Наука. Образование. 2020. № 23. С. 728-734.
5. Махов Д.С. Метод оптимизации энергетических параметров системы передачи информации в парциальных радиоканалах малоразмерных подвижных объектов на основе аппарата теории нечетких множеств // Системы управления, связи и безопасности. 2019. № 4. С. 27–49.
6. Якушенко С.А., Шабуня В.В., Лукашев А.В., Егрушев В.Е., Веркин С.С., Лаута О.С., Сатдинов А.И., Селезнев А.В. Спутниковые системы передачи специального назначения / Под ред. С.А. Якушенко. – СПб.: ВАС, 2024.
7. Массобрио Р., Дорронзоро Диаз В., Несмачнов Кановас С.Е. Виртуальный Эрудит для решения задачи о рюкзаке: обучение автоматическому распределению ресурсов // Тр. Ин-та системного Программирования РАН. 2019. Т31, №2. С. 21–32.
8. Топка В.В. Многомерная задача о рюкзаке: эффективный метод решения и возможные приложения // Труды Института системного анализа Российской академии наук. 2019. Т. 69. №2. С. 54–64.
9. Офицеров В.П., Смирнов С.В. Метод решения задачи о рюкзаке с дополнительным ограничением на число типов предметов // Челябинский физико-математический журнал. 2022. Т.7. С. 267–276.
10. Савельев В.П. Задача о рюкзаке, условия оптимальности // Евразийское Научное Объединение. 2019. № 4-1 (50). С. 31–34.

INCREASING THE THROUGHPUT OF THE COMMUNICATION REPEATER WHEN WORKING WITH EARTH STATIONS WITH PARTIAL CHANNELS

Burlakov S.O.[1], Dragunov M.Yu.[2]

Keywords: *frequency resource utilization factor, satellite radio link, frequency resource allocation; channel transmission rate; channel noise immunity; backpack filling problem.*

Abstact

Objective: *to consider the features of the distribution of the frequency resource of the barrel with direct relay for the needs of military consumers.*

Research method: *the issue under consideration is reduced to solving the problem of packing the frequency*

[1]Sergey O. Burlakov, Dr.Sc., Professor, Professor of the Department of Military Systems of Space, Radio Relay, Tropospheric Communication and Navigation, Military Academy of Communications, St. Petersburg, Russia. E-mail: soburlakov@yandex.ru

[2]Mikhail Yu. Dragunov, Adjunct of the Department of Military Systems of Space, Radio Relay, Tropospheric Communication and Navigation, Military Academy of Communications, St. Petersburg, Russia. E-mail: dragunov1992@mail.ru

resource of the repeater with signals from earth stations with partial channels, taking into account the requirements for the quality of the communication channel and the transmission rate of earth stations. In solving the scientific problem, methods of complete enumeration of all subsets with an additional limitation were used.

Result: *a method for allocating communication repeater frequencies for the operation of earth stations with partial channels is proposed. The method allows to increase the coefficient of transponder resource utilization and interference immunity of satellite communication radio links when duplicating transmitted information in partial channels, as well as to organize satellite communication networks using partial channels as separate communication directions distribution of partial channels of one earth station throughout the trunk of the communication repeater, taking into account the interference situation.*

Scientific novelty: *the proposed method of frequency distribution of the communication repeater makes it possible to redistribute the frequency resource not only within the network, but also between the networks operating in the same trunk of the repeater, taking into account the available resource, interference situation and requirements for the quality of communication.*

References

1. Cvetkov K.Ju., Burlakov S.O., Klimov I.S. Raspredelenie chastot retransljatora svjazi pri rabote zemnyh stancij s parcial'nymi kanalami // Trudy Voenno-kosmicheskoj akademii imeni A. F. Mozhajskogo. 2020. № 672. S. 88–91.
2. Burlakov S.O., Smirnov A.A., Cvetkov K.Ju. Nauchno-tehnicheskie predlozhenija po realizacii metodiki raspredelenija chastotno-jenergeticheskogo resursa zemnyh stancij i bortovyh radiotehnicheskih kompleksov vysokoskorostnyh sistem sputnikovoj svjazi // Trudy Voenno-kosmicheskoj akademii imeni A. F. Mozhajskogo. 2020. № 673. S. 68–78.
3. Nemirovskij M.S., Lokshin B.A., Aronov D.A. Osnovy postroenija sistem sputnikovoj svjazi / Pod red. M.S. Nemirovskogo. – M.: Gorjachaja linija – Telekom, 2018.
4. Burlakov S.O., Verkin S.S., Egrushev V.E., Antonov V.V. Metodika ocenki trebuemoj moshhnosti peredatchika zemnoj stancii // Innovacii. Nauka. Obrazovanie. 2020. № 23. S. 728-734.
5. Mahov D.S. Metod optimizacii jenergeticheskih parametrov sistemy peredachi informacii v parcial'nyh radiokanalah malorazmernyh podvizhnyh ob#ektov na osnove apparata teorii nechetkih mnozhestv // Sistemy upravlenija, svjazi i bezopasnosti. 2019. № 4. S. 27–49.
6. Jakushenko S.A., Shabunja V.V., Lukashev A.V., Egrushev V.E., Verkin S.S., Lauta O.S., Satdinov A.I., Seleznev A.V. Sputnikovye sistemy peredachi special'nogo naznachenija / Pod red. S.A. Jakushenko. – SPb.: VAS, 2024.
7. Massobrio R., Dorronzoro Diaz V., Nesmachnov Kanovas S.E. Virtual'nyj Jerudit dlja reshenija zadachi o rjukzake: obuchenie avtomaticheskomu raspredeleniju resursov // Tr. In-ta sistemnogo Programmirovanija RAN. 2019. T31, №2. S. 21–32.
8. Topka V.V. Mnogomernaja zadacha o rjukzake: jeffektivnyj metod reshenija i vozmozhnye prilozhenija // Trudy Instituta sistemnogo analiza Rossijskoj akademii nauk. 2019. T. 69. №2. S. 54–64.
9. Oficerov V.P., Smirnov S.V. Metod reshenija zadachi o rjukzake s dopolnitel'nym ogranicheniem na chislo tipov predmetov // Cheljabinskij fiziko-matematicheskij zhurnal. 2022. T.7. S. 267–276.
10. Savel'ev V.P. Zadacha o rjukzake, uslovija optimal'nosti // Evrazijskoe Nauchnoe Ob#edinenie. 2019. № 4-1 (50). S. 31–34.

ОСОБЕННОСТИ ЗАЩИТЫ ИНФОРМАЦИОННЫХ РЕСУРСОВ СИСТЕМ УПРАВЛЕНИЯ РОБОТОТЕХНИЧЕСКИМИ КОМПЛЕКСАМИ

Стародубцев Ю.И.[1], Лаута О.С.[2], Худайназаров Ю.К.[3]

DOI:10/24682/3034-4050-2024-2-43-52

Ключевые слова: *информационно-управляющая система, защищаемые информационные ресурсы, угрозы информационной безопасности, комплексный подход.*

Аннотация

Цель: *предложить решение задачи анализа особенностей защиты информационных ресурсов (ИР) системы управления робототехническими комплексами (РТК).*

Метод: *использован системный подход для анализа состава, функций, роли и места информационно-управляющей системы в системе управления современных и перспективных РТК. Методом аналитического моделирования представлены основные противоречия в теории управления РТК военного назначения (ВН).*

Результат: *приведены результаты анализа защищаемых информационных ресурсов в информационно-управляющей системе робототехнического комплекса: информации, носителей информации и информационных процессов. Выявлены основные особенности применяемых протоколов информационного взаимодействия в соответствии с эталонной моделью OSI.*

Представлены результаты анализа угроз информационной безопасности и функциональные составляющие комплексной системы защиты информационных ресурсов системы управления робототехническими комплексами.

Научная новизна: *заключается в формализации объективных противоречий в свойствах процесса управления РТК ВН между непрерывностью и скрытностью, а также между свойствами системы управления РТК: ограниченность ресурсов (вычислительных, сетевых и памяти) для реализации функций безопасности; высокая динамика структурных, информационных и функциональных характеристик защищаемых ресурсов Следствием указанных противоречий является необходимость комплексирования разнородных методов и средств защиты, а также управления в реальном масштабе времени задачами и информационными ресурсами информационно-управляющей системы (ИУС) РТК ВН.*

Известные в настоящее время методы и технологии не позволяют учесть все особенности ИР системы управления РТК как объекта защиты и обеспечить адекватность системы защиты угрозам и состоянию защищаемых ресурсов при их высокой динамичности.

Введение

В современных условиях перехода к массовому применению робототехнических комплексов военного назначения, проблемной областью является отсутствие методологии оптимального управления РТК ВН при выполнении задач вне контролируемой зоны в условиях деструктивных внешних воздействий.

Одной из проблем в данной области является защита информационных ресурсов системы управления РТК ВН.

Под робототехническим комплексом (РТК) понимается[4] комплекс, состоящий из одного или нескольких роботов, их рабочих органов и любых механизмов, оборудования, приборов или датчиков, обеспечивающих выполнение роботом функционального назначения (задания).

Система управления (СУ) РТК представляет собой совокупность управляющей логики и силовых функций, позволяющих контролировать и управлять механической конструкцией робота, а также осуществлять взаимосвязь с внешней средой (оборудованием и пользователями). СУ РТК ВН относится к специальным системам управления оружием, в частности к информационно-техническим системам реального времени, которые используют ресурс специальных (выделенных) направлений и сетей связи.

Оператор — лицо, уполномоченное запускать,

[1]Стародубцев Юрий Иванович, доктор военных наук, профессор, профессор кафедры Безопасности инфокоммуникационных систем специального назначения Военной академии связи им. Маршала Советского Союза С.М. Буденного, г. Санкт-Петербург, Россия. E-mail: starodub@mail.ru

[2]Лаута Олег Сергеевич, доктор технических наук, профессор кафедры Государственного университета морского и речного флота имени адмирала С.О. Макарова, г. Санкт-Петербург, Россия. E-mail: laos-82@yandex.ru

[3]Худайназаров Юрий Кахрамонович, кандидат технических наук, докторант кафедры Безопасности инфокоммуникационных систем специального назначения Военной академии связи им. Маршала Советского Союза С.М. Буденного, г. Санкт-Петербург, Россия. E-mail: yu-78@ya.ru

[4]ГОСТ Р 60.0.0.4 — 2019/ИСО 8373:2012 Роботы и робототехнические устройства. Термины и определения.

контролировать и останавливать выполнение заданной операции роботом или робототехническим комплексом.

Информационные ресурсы РТК ВН включают в себя: оперативные данные, которые хранятся, передаются и обрабатываются в системе управления СУ РТК; данные, которые обеспечивают функционирование элементов СУ РТК (программные коды микроконтроллеров, программные агенты, операционная система, используемые протоколы информационного обмена (форматы сообщений, идентификаторов, алгоритмы обработки данных), структура и параметры используемых сигналов).

Ключевое значение в координации и управлении группой РТК имеет информационно-управляющая система (ИУС). Рассмотрим основные особенности информационно-управляющей системы группы РТК.

Информационно-управляющая система (ИУС) группы РТК представляет собой высокоуровневую систему, которая позволяет координировать и управлять действиями нескольких робототехнических устройств, работающих совместно. Такие системы могут использоваться в различных контекстах, например, в промышленной автоматизации, военной технике, логистике и многих других областях. Основные элементы такой системы следующие.

1. Центральный управляющий узел (центральный контроллер), выполняет функции: планирования, мониторинга и координации действий всей группы роботов; управления общими задачами и распределения задач между роботами; обработки данных, поступающих от всех роботов, с целью принятия решений.
2. Индивидуальные контроллеры роботов выполняют функции: локального управления и контроля каждого робота; реализации задач, полученных от центрального управляющего узла; обратной связи с центральным узлом, включая отчеты о выполнении задач и состояние робота.
3. Средства связи включают в себя: беспроводные или проводные каналы связи для обмена данными между центральным узлом и индивидуальными роботами; средства синхронизации и координации действий между роботами.
4. Сенсорные системы включают в себя: датчики и сенсоры, установленные на роботах для сбора информации о внешней среде и собственном состоянии (например, камеры, лидары, GPS, датчики положения и движения); средства обработки и передачи сенсорных данных для принятия решений и выполнения задач.
5. Аналитические модули могут включать в себя: модули для обработки данных и анализа информации (например, модуль машинного зрения, модуль распознавания образов, алгоритмы машинного обучения); средства оптимизации маршрутов, прогнозирование ситуаций и принятие решений на основе анализа данных [1].
6. Интерфейсы пользователя включают в себя: консоли управления для операторов, где можно задавать задачи, мониторить состояние системы, получать отчеты и управлять отдельными роботами; графические интерфейсы, панели управления и системы визуализации.
7. Подсистемы обеспечения безопасности могут включать: механизмы для предотвращения коллизий между роботами и с окружающей средой; средства аутентификации и защиты от несанкционированного доступа.
8. Энергетическая подсистема: источники питания для роботов и централизованных систем; механизмы управления энергопотреблением и резервирования энергии для надежной работы всей системы.

Основные функции ИУС включают:

1. Сбор информации. ИУС собирает данные от различных сенсоров и устройств, установленных на роботах, а также от внешних источников, таких как камеры наблюдения, GPS и т. д.
2. Анализ данных. ИУС обрабатывает и анализирует собранные данные для принятия решений. Этот анализ может включать обнаружение препятствий, определение оптимальных маршрутов движения и т.д.
3. Планирование задач. ИУС распределяет задачи между роботами на основе алгоритмов, которые могут учитывать текущие состояния роботов, их расположение, и другие релевантные данные.
4. Обмен информацией. ИУС обеспечивает быстрое и надежное взаимодействие между всеми членами группы роботов, что позволяет координировать их действия и предотвращать конфликты.
5. Безопасность и защита. ИУС включает меры по защите информации и предотвращению несанкционированного доступа. В области информационной безопасности это особенно важно для предотвращения кибератак и обеспечения целостности данных.
6. Мониторинг и контроль. ИУС непрерывно отслеживает состояние и выполнение задач каждым роботом, а также может вмешиваться в случае возникновения проблем.

Таким образом, информационно-управляющая система является центральной частью системы управления робототехнических комплексов, обеспечивая синхронизацию, координацию и выполнение задач в соответствии с заданными параметрами и условиями.

В соответствии с моделью OSI (Open Systems Interconnection) ИУС группы РТК, можно рассмотреть на каждом из семи уровней. Для обеспечения

информационного взаимодействия робототехнических комплексов на каждом уровне в рамках модели OSI выполняются функции с использованием соответствующих протоколов информационного обмена (табл. 1).

1. Физический уровень (Physical Layer): обеспечивается функция физического соединения между устройствами. Параметры физического уровня включают электрические и механические характеристики интерфейсов и среды передачи. Реализация в составе ИУС группы РТК предполагает использование разнообразных физических сред, таких как радиочастоты (Wi-Fi, Zigbee), оптоволокно или другие беспроводные технологии для соединения роботов друг с другом.
2. Канальный уровень (Data Link Layer): обеспечивается функция надёжной передачи данных через физические соединения. Обнаружение и исправление ошибок на уровне кадра. Реализация в составе ИУС группы РТК предполагает использование протоколов MAC (Media Access Control) для управления доступом к общей среде передачи. Применяются технологий, такие как Bluetooth или Zigbee, которые включают функции ARQ (Automatic Repeat reQuest) для коррекции ошибок.
3. Сетевой уровень (Network Layer): реализуется функция определения маршрутов данных между устройствами. Управление логическими адресами и маршрутизацией пакетов. В составе ИУС группы РТК может обеспечиваться использованием протоколов маршрутизации, таких как OLSR (Optimized Link State Routing) или RPL (Routing Protocol for Low-power and Lossy Networks), чтобы обеспечить эффективную маршрутизацию данных между роботами в динамическом окружающем пространстве.
4. Транспортный уровень (Transport Layer): реализуется функция надёжной передачи данных между хостами. Установление, поддержание и завершение соединений, контроль перегрузок и восстановление данных при ошибках. В составе ИУС группой РТК может обеспечиваться применением UDP (User Datagram Protocol) для приложений, требующих минимальной задержки, или TCP (Transmission Control Protocol) для приложений, где требуется надёжность.
5. Сеансовый уровень (Session Layer): реализуется функция управления сеансами связи, установления, координации и завершения сеансов между взаимодействующими устройствами. В составе ИУС группой РТК данная функция может обеспечиваться с использованием протоколов для установления и управления сессиями данных, например, с помощью WebSocket для сессионных взаимодействий между группами роботов.
6. Представительный уровень (Presentation Layer): реализуется интерпретация данных между различными формами данных, кодирование, дешифрование и сжатие данных. В составе ИУС группы РТК функция может обеспечиваться с помощью кодирования сообщений данных с использованием стандартов, таких как JSON или XML, для унифицированного формата обмена данными между различными подсистемами РТК.
7. Прикладной уровень (Application Layer): реализуется поддержка специфических сетевых приложений, таких как удалённое управление, коммуникация и совместная работа. В составе ИУС группы РТК может обеспечиваться с использованием протоколов приложения, таких как MQTT (Message Queuing Telemetry Transport) для обмена телеметрической информацией между роботами, или RESTful API для взаимодействия с внешними системами.

Таблица 1.

Эталонная модель информационного взаимодействия элементов РТК

Уровень по OSI	***Выполняемые функции***	***Технологии, стандарты и протоколы***
Прикладной уровень	Поддержка специфических сетевых приложений, таких как удалённое управление, коммуникация и совместная работа	MQTT (Message Queuing Telemetry Transport), RESTful API
Представительный уровень	Интерпретация данных между различными формами данных, кодирование, дешифрование и сжатие данных	JSON или XML
Сеансовый уровень	Управление сеансами связи, установления, координации и завершения сеансов между взаимодействующими устройствами	WebSocket
Транспортный уровень	Надёжная передача данных между хостами. Установление, поддержание и завершение соединений, контроль перегрузок и восстановление данных при ошибках	UDP (User Datagram Protocol) или TCP (Transmission Control Protocol)

Уровень по OSI	*Выполняемые функции*	*Технологии, стандарты и протоколы*
Сетевой уровень	Определение маршрутов данных между устройствами, управление логическими адресами и маршрутизацией пакетов	OLSR (Optimized Link State Routing) или RPL (Routing Protocol for Low-power and Lossy Networks)
Канальный уровень	Надёжная передача данных через физические соединения. Обнаружение и исправление ошибок на уровне кадра	MAC (Media Access Control), технологий, такие как Bluetooth или Zigbee, которые включают функции ARQ (Automatic Repeat reQuest) для коррекции ошибок
Физический уровень	Физическое соединение между устройствами. Параметры физического уровня включают электрические и механические характеристики интерфейсов и среды передачи	Wi-Fi, Zigbee

Рассматривая взаимодействие РТК в составе группы, важно учитывать, что успешная работа на каждом из уровней OSI зависит от корректного функционирования и координации между этими уровнями. Современные подходы в кибернетике и робототехнике часто интегрируют решения, обеспечивающие надёжную и эффективную коммуникацию на каждом уровне модели OSI.

Первым этапом построения системы защиты является определение защищаемых информационных ресурсов ИУС группы РТК. Они могут быть классифицированы следующим образом:

1. Данные сенсоров и датчиков: данные позиционирования (GPS, LIDAR, камеры, инерциальные измерительные единицы (IMU)); данные окружающей среды (от сенсоров температуры, давления, освещения, влажности и других); тактические и стратегические данные (от сенсоров, которые обеспечивают понимание текущей ситуации в рабочей зоне).
2. Коммуникационные каналы: каналы прямой связи (беспроводные сети (Wi-Fi, LTE, радиосвязь), проводные сети (Ethernet и другие)); ретрансляторы и хабы (беспилотные летательные аппараты (БЛА), действующие как ретрансляторы сигналов);
3. Средства обработки данных и вычислительные ресурсы: серверы и облачные вычисления (обеспечение высокопроизводительных вычислений, анализа данных, машинного обучения); локальные вычислительные мощности (встроенные процессоры, ПЛИС и микроконтроллеры, выполняющие локальные вычисления на уровне каждого РТК);
1. Командные и управляющие системы: программное обеспечение для управления (алгоритмы и программы для сценарного управления, маршрутизации, координации действий); интерфейсы управления (системы ЧМИ (человеко-машинного интерфейса) для операторов);
2. Подсистема технического контроля: информационные базы данных о состоянии РТК (оперативная информация о текущем состоянии, результатах диагностики и техническом обслуживании).
3. Подсистема информационной безопасности: средства и функции шифрования и аутентификации (защита передаваемых и обрабатываемых данных от несанкционированного доступа); системы обнаружения вторжений (анализ сетевого трафика и активности для выявления аномалий и потенциальных угроз); другие подсистемы, реализующие политику безопасности и процедуры (набор правил и процедур для защиты информационных ресурсов).

Для формализации свойств указанных защищаемых ресурсов целесообразно их систематизировать в соответствии с тремя обобщенными категориями свойств информационно-управляющей системы:

- информационная (оперативная и служебная информация, математические модели, информационно-алгоритмическое обеспечение);
- структурная (вычислительные и сетевые (коммуникационные) ресурсы, память);
- функциональная (цель, задачи, процессы, действия).

Каждая из этих категорий информационных ресурсов имеет свою составляющую в общей эффективности и безопасности системы управления группой РТК, определяя выполнимость задач в разнообразных оперативных ситуациях и условиях.

Рассмотрим основные угрозы безопасности информационным ресурсам СУ группой РТК. Для СУ группой РТК существуют различные угрозы безопасности информационным ресурсам. Важно учитывать как внешние, так и внутренние угрозы:

1. Кибератаки (специальные программные воздействия): Malware, Ransomware (программное обеспечение, которое может скомпрометировать данные или нарушить функционирование робототехнических комплексов); фишинг (попытки обманом получить конфиденциальную информацию, такую как учетные данные или ключи доступа); DDoS (распределенные атаки отказа в обслуживании) (перегрузка сетевой инфраструктуры системы управления, приводящая к исчерпанию ресурсов);
2. Компрометация сетевой безопасности: снифинг трафика (сбор данных, передаваемых по сети, который может позволить злоумышленникам получить доступ к конфиденциальной информации); Man-in-the-Middle (атака «человек посередине») (перехват и изменение трафика между компонентами системы); беспроводные угрозы (использование незащищенных беспроводных соединений, что может позволить противнику получить доступ к управлению роботами);
3. Компрометация устройств и сенсоров: физический доступ (незаконное проникновение и физическая манипуляция устройствами или сенсорами); внедрение фальшивых сенсоров (введение ложных данных через сенсоры для дезориентации системы управления);
4. Уязвимости программного обеспечения: ошибки в коде (уязвимости из-за ошибок в программном обеспечении, которое управляет роботами); уязвимости программного обеспечения (использование устаревшего программного обеспечения с известными уязвимостями); недостаточная аутентификация и авторизация (неадекватные меры контроля доступа могут позволить неавторизованным пользователям получить доступ к системе управления);
5. Человеческий фактор: внутренние угрозы (обслуживающий персонал или операторы системы, которые могут преднамеренно или случайно скомпрометировать безопасность); неправильная конфигурация (ошибки в настройке системы, которые могут оставить уязвимости);
6. Социальная инженерия: (использование методов психологического влияния на обслуживающий персонал или на операторов РТК для получения доступа к конфиденциальной информации или системам).

Для защиты информационных ресурсов СУ группой РТК необходимо комплексно использовать методы и средства по следующим направлениям защиты:

1. Обеспечение сетевой безопасности (использование шифрования для защиты данных при передаче, установка межсетевых экранов и систем обнаружения вторжений (IDS));
2. Обеспечение программно-алгоритмической безопасности (кибербезопасности): регулярное обновление программного обеспечения, применение антивирусного ПО и брандмауэров, а также регулярные проверки на наличие уязвимостей (Penetration Testing);
3. Обеспечение защиты от несанкционированного физического доступа (ограничение доступа к устройствам, защита сенсоров от несанкционированного воздействия);
4. Обучение персонала: обучение операторов методам распознавания фишинговых атак, способам управления безопасностью данных и мероприятиям при нарушении безопасности;
5. Контроль и управление доступом (использование многофакторной аутентификации (MFA) и роли доступа (RBAC) для ограничения доступов к системам управления) [2];
6. Мониторинг и логирование: постоянный мониторинг систем и анализ логов для своевременного обнаружения аномалий и инцидентов безопасности [3].

Основные научно-теоретические проблемы разработки методологии защиты информационных ресурсов связаны с построением сетецентрической системы управления РТК ВН, позволяющей оперативно реагировать на изменения обстановки и перераспределять задачи и ресурсы.

Отличительными особенностями сетецентрического подхода, по сравнению с традиционным, являются:

- возможность согласованного испольвания географически распределенных сил и средств;

самосинхронизация сил, участвующих в операции (боевых действиях);

- высокая динамичность, активность и результативность всех процессов управления и самих боевых действий;
- изменение формы военных действий, которая от последовательных боев и операций с соответствующими промежутками (паузами) между ними, приобретает форму непрерывных высокоскоростных действий (операций, акций) с решительными целями;
- наличие сети связи между системами и средствами управления войсками и оружием, что дает возможность на обширном географическом пространстве проводить совместные действия, а также динамически наилучшим образом распределять ответственность и объем задач между различными подразделениями применительно к текущей обстановке.

Основная суть сетецентричекого подхода в возможности оперативного обмена информацией и многоуровневой самоорганизации для гарантированного выполнения поставленных задач в заданные сроки.

Новый облик ВС РФ предусматривает многоуровневую систему управления боевыми действиями в регионе конфликта. Поэтому для формирования структуры и требований к элементам сетецентрической системы управления необходимо определение принципа разграничения полномочий между различными иерархическими уровнями.

Основными недостатками в практике создания сетецентрических систем управления являются следующие [5].

1. Сетецентрические системы управления предполагают сбор и интеграцию различных средств и систем разведки, работающих на различных физических принципах в различных диапазонах длин волн в единую интегрированную базу данных. В то же время в научно-методическом плане не существует проверенных на практике и эффективных методов и способов идентификации целей, объединения и отождествления разнородных данных, обеспечивающих высокую вероятность обнаружения и идентификации целей.
2. Методы многомерной многофакторной оптимизации разработаны для крайне ограниченных и простых условий и функций и, как правило, не пригодны для сложных нелинейных функций с ярко выраженными корреляционными связями между основными параметрами этих функций. Поэтому требуется разработка методов синтеза сложных сетецентрических систем управления.
3. Проблема опознавания «свой-чужой» не имеет надежных методов и технических средств для распознавания своих сил и средств на поле боя. Требуется постановка комплекса поисковых и прикладных исследований для определения путей решения данной проблемы.

Построение защищенной сетецентрической СУ РТК позволит значительно повысить устойчивость управления группой РТК в конфликтных условиях. Обеспечение защиты информационных ресурсов СУ группой РТК основывается на анализе и формализации процессов информационного обмена в группе РТК, моделировании угроз информационной безопасности и определении комплекса защитных мер. Необходимо учесть особенности различных сценариев применения РТК военного назначения (ВН) [4], применяемых в составе группы.

К СУ РТК ВН предъявляются требования по следующим свойствам [5]:

1. Боевая готовность (способность системы и ее элементов переходить из одного состояния в другое за время, не превышающее допустимое);
2. Устойчивость (способность обеспечивать управление с требуемой эффективностью при воздействии неблагоприятных факторов);
3. Мобильность (способность в установленные строки развертываться, свертываться и перемещать свои элементы, а также изменять свою структуру в соответствии с обстановкой);
4. Производительность (способность преобразовывать требуемые объемы информации в установленные сроки);
5. Безопасность (способность противостоять всем видам разведки, вводу ложной информации и несанкционированному доступу к информации);
6. Качество используемых моделей, методик и алгоритмов управления (способность обеспечить необходимую адекватность управления на основе использования применяемых для выработки управляющих воздействий моделей, методик, алгоритмов);
7. Управляемость (способность изменять свое состояние в необходимых пределах и сохранять требуемые значения показателей существенных свойств при переходе из одного состояния в другое);

8. Ресурсопотребление (характеризует численность привлекаемых к управлению должностных лиц, номенклатуру и количество необходимых технических, программных и других средств).

При выполнении требований к сетецентрической системе управления [6], [7] возникает объективное противоречие между свойствами безопасности и производительности. Наглядным является графическое представление указанного противоречия при обеспечении выполнения требований к СУ РТК ВН (рис. 1).

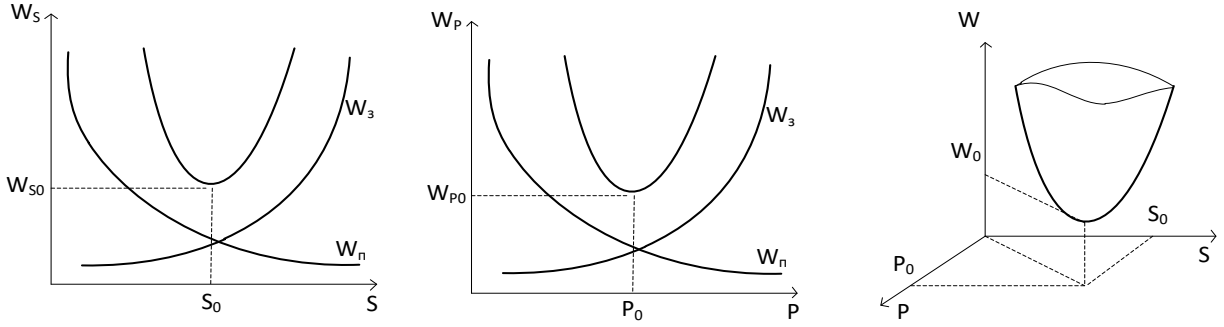

Рис. 1. Условия оптимальности управления РТК ВН

Проблема защиты ИР СУ РТК обусловлена объективными противоречиями при обеспечении выполнения требований к системе управления военного назначения: обеспечение безопасности ИУС РТК при заданных требованиях по производительности ИУС.

Пусть P — производительность ИУС РТК;

S — безопасность ИУС РТК;

$W_п(S)$ — потери при нарушении безопасности ИУС РТК;

$W_з(S)$ — затраты на обеспечение безопасности ИУС РТК.

Тогда условие оптимальности для безопасности ИУС РТК:

$$W_{S0}=min\ (W_п(S)+W_з(S)) \text{ при } P=const \quad (1)$$

Пусть $W_п(P)$ — потери, обусловленные недостаточной производительностью ИУС РТК;

$W_з(P)$ — затраты на обеспечение производительности ИУС РТК;

Тогда условие оптимальности для обеспечения производительности ИУС РТК:

$$W_{P0}=min\,(W_п(P)+W_з(P)) \text{ при } S=const \quad (2)$$

При функционировании ИУС должны выполняться оба условия оптимальности (безопасности и производительности) ИУС РТК:

$$W_{02}=min\,(W_{S0}+W_{P0}) \quad (3)$$

Концептуально проблема реализации комплексного подхода к защите ИР СУ РТК имеет два основных аспекта, обусловленные объективными противоречиями при реализации требований к процессу управления и к системе управления:

- обеспечение скрытности управления РТК при заданных требованиях непрерывности управления;
- обеспечение имитозащищенности ИУС РТК при заданных ограничениях по производительности ИУС.

Интероперабельность может быть своевременным дополнением существующего перечня требований к СУВН.

Интероперабельность[5] — способность двух и более информационных систем к обмену информацией и к использованию информации, полученной в результате обмена. Это свойство играет ключевую роль при создании, развитии и объединении информационных систем различных типов и назначения.

Другим актуальным требованием к системе управления военного назначения при возрастании степени ее интеллектуальности является «доверие» к искусственному интеллекту (ИИ).

Для РТК ВН особенностью применения обусловлено требование доверия к ИИ (объяснимость работы ИИ и процесса достижения им результатов).

Доверие[6] к системе искусственного интеллекта — уверенность потребителя, и при необходимости, организаций, ответственных за регулирование вопросов создания и применения систем искусственного интеллекта, и иных заинтересованных сторон в том, что система способна выполнять возложенные на нее задачи с требуемым качеством.

[5]ГОСТ Р 59796 — 2021 Информационные технологии. Интероперабельность. Термины и определения.

[6]ГОСТ Р 59276 — 2020 Системы искусственного интеллекта. Способы обеспечения доверия. Общие положения.

Доверенная система искусственного интеллекта — система искусственного интеллекта, в отношении которой потребитель и, при необходимости, организации, ответственные за регулирование вопросов создания и применения систем искусственного интеллекта, проявляют доверие.

Требуется поиск новых подходов для обеспечения скрытности и непрерывности управления, разработка новых методов и технологий для защиты ИР СУ РТК, позволяющие при ограниченных вычислительных, транспортных возможностях и памяти контролировать параметры целостности (имитозащищенность) разнородных информационных ресурсов в режиме реального времени.

Для разрешения указанных противоречий в теории и практике управления РТК ВН требуется проведение междисциплинарных исследований, разработка соответствующей методологии на основе новых подходов к моделированию современных информационно-телекоммуникационных систем в условиях информационного конфликта[8], исследование теоретических основ интеллектуализации ИУС РТК на основе современных методов и технологий управления сложными организационно-техническими системами в режиме реального времени [9], исследование методов и технологий формализации свойств и моделирования сложных систем [10], разработка новых методов и технологий управления сетевой безопасностью в информационно-телекоммуникационных сетях [11], а также мониторинга состояния информационно-телекоммуникационных сетей [12].

Выводы

Управление группами РТК (или роями роботов) является одной из наиболее сложных проблем в робототехнике и искусственном интеллекте. Основные аспекты данной проблемы следующие:

1. Самоорганизация и координация РТК в группе предполагают решение двух задач на оперативном и тактическом уровнях управления, связанных с особенностями сценариев применения РТК в составе группы: целеполагание (обеспечение синхронных и согласованных действий роботов с минимальными задержками и энергетическими затратами для решения групповой задачи) и целераспределение (эффективное распределение частных задач между роботами, чтобы максимизировать продуктивность и минимизировать дублирование усилий).
2. Коммуникация (применение технологий, обеспечивающих своевременность и достоверность связи между роботами в условиях, где могут быть помехи или ограничения по частоте, применение протоколов связи, которые могут масштабироваться для больших групп роботов);
3. Децентрализованное управление (создание алгоритмов, где каждый робот может принимать решения на основе ограниченной локальной информации; сокращение этапов и эпизодов функционирования группы РТК с необходимостью центрального управляющего узла, который может стать уязвимым из-за одного точечного отказа);
4. Работа в неизвестной и изменяющейся среде (разработка алгоритмов обеспечивающих способность группы робототехнических комплексов адаптироваться к непредсказуемым изменениям в окружающей среде, а также для исследования и картографирования неизвестных территорий);
5. Энергоэффективность (разработка стратегий для минимизации энергозатрат в процессе выполнения задач, создание систем для автономного подзаряда или распределения энергии среди роботов или оптимального распределения задач);
6. Обнаружение и разрешение внутренних конфликтов (создание алгоритмов, которые позволяют роботам избегать столкновений друг с другом и с окружающими объектами, эффективное разрешение конфликтов между роботами при доступе к ограниченным ресурсам);
7. Информационная безопасность и устойчивость к сбоям (защита группы роботов от информационно-технических воздействий, обеспечение устойчивости группы (роя или стаи) при выходе из строя одного или нескольких роботов).

Исследование этих проблемных аспектов требуют междисциплинарного подхода, включающего методы из области искусственного интеллекта, теории управления, коммуникаций.

Литература

1. Юмашева Е.С., Ныркова А.П. Применение алгоритмов машинного обучения для обнаружения аномального поведения в сетях критической информационной инфраструктуры // В сборнике: Региональная информатика и информационная безопасность. Сборник трудов Санкт-Петербургской международной конференции. Санкт-Петербург, 2023. С. 247–251.

2. Ныpков А.П., Соколов С.С., Алимов О.М., Черный С.Г., Доровской В.А. Оптимальная идентификация объектов в задачах распознавания необитаемыми подводными аппаратами // Проблемы информационной безопасности. Компьютерные системы. 2020. № 2. С. 58–64.
3. Мартынов В.Л., Ныpков А.П., Шиманская М.С., Кречетова Э.В., Шиманская Г.С. Гидроакустические коммуникации в вопросах противодействия подводным роботам // Информатизация и связь. 2024. № 2. С. 51–55.
4. Пшихопов В. Х., Гонтарь Д. Н., Мартьянов О. В. Концептуальные подходы к формированию сценариев боевого применения групп робототехнических комплексов // Системы управления, связи и безопасности. 2022. № 3. С. 138–182. DOI: 10.24412/2410-9916-2022-3-138-182
5. Боговик А.В., Игнатов В.В. Теория управления в системах военного управления: Учебн. – СПб.: ВАС, 2008. – 460 с.
6. Чижевский Я.А. Реализация концепции сетецентрических боевых действий в вооруженных силах США // Военная мысль. 2019. № 3, С. 116–137.
7. Попов А.А, Филатов В.И. Модели информационно-управляющей системы обеспечения взаимодействия разновидовых пунктов управления // Стратегическая стабильность. 2020. № 4, С. 19-23.
8. Макаренко С.И. Модели системы связи в условиях преднамеренных дестабилизирующих воздействий и ведения разведки. Монография. – СПб.: Наукоемкие технологии, 2020. – 337 с.
9. Макаренко С.И. Интероперабельность человеко-машинных интерфейсов. Монография. – СПб.: Наукоемкие технологии, 2023. – 185 с.
10. Можаева И.А., Струков А.В., Поленин В.И., Сущенков Д.А. Моделирование байесовских сетей доверия с применением ОЛВМ // В сборнике: Актуальные проблемы защиты и безопасности. Сборник трудов Санкт-Петербургской Всероссийской научно-практической конференции РАРАН. Санкт-Петербург, 2019. С. 430–442.
11. Милославская Н.Г. Построение центров управления сетевой безопасностью в информационно-телекоммуникационных сетях. Дис. …доктора технических наук: 05.13.19. –М.: Федеральный исследовательский центр «Информатика и управление» Российской академии наук, 2020. – 461 с.
12. Будко Н.П., Васильев Н.В., Обзор графо-аналитических подходов к мониторингу информационно-телекоммуникационных сетей и их применение для выявления аномальных состояний // Системы управления, связи и безопасности. 2021. №6. С. 53-75.

FEATURES OF PROTECTION OF INFORMATION RESOURCES OF CONTROL SYSTEMS OF ROBOTIC COMPLEXES

Starodubtsev Yu.I.[1], Lauta O.S.[2], Khudainazarov Yu.K.[3]

Keywords: *information management system, protected information resources, threats to information security, integrated approach.*

Abstract

Objective: *in the article to propose a solution to the problem of analyzing the features of the protection of information resources (IR) of the control system of robotic complexes (RTS).*

Method: *on the basis of a system approach, to analyze the composition, functions, role and place of the information and control system in the control system of modern and future RTCs. The method of analytical modeling presents the main contradictions in the theory of control of military RTCs (HG).*

Result: *the results of the analysis of protected information resources in the information management system of the robotic complex are presented: information, data carriers and information processes. The main features of the applied protocols of information interaction in accordance with the OSI reference model are revealed.*

The results of the analysis of information security threats and the functional components of the integrated system for the protection of information resources of the control system of robotic complexes are presented.

The scientific novelty consists *in the formalization of objective contradictions in the properties of the control process of the RTS HV between continuity and secrecy, as well as between the properties of the RTS control system: limited resources (computational, network and memory) for the implementation of security functions; high dynamics of structural, informational and functional characteristics of the protected resources The consequence of these contradictions is the need to integrate heterogeneous methods and protection tools, as well as real-time management of*

[1]Yuri I. Starodubtsev, Dr.Sc. (of Military), Professor, Professor of the Department of Security of Special Purpose Information and Communication Systems, Marshal of the Soviet Union S.M. Budyonny Military Academy of Communications, St. Petersburg, Russia. E mail: starodub@mail.ru

[2]Oleg S. Lauta, Dr.Sc. (of tech.), Professor of the Department of the State University of Maritime and Inland Shipping named after Admiral S.O. Makarov, St. Petersburg, Russia.Email: laos-82@yandex.ru

[3]Yuriy K. Khudainazarov, Ph.D., Doctoral Student of the Department of Security of Special Purpose Information and Communication Systems of the Military Academy of Communications named after Marshal of the Soviet Union S.M. Budyonny, St. Petersburg, Russia. E-mail: yu-78@ya.ru

tasks and information resources of the information management system (ICS) of the HV RTS.

Currently known methods and technologies do not allow to take into account all the features of the R&D system of the RTS control system as an object of protection and to ensure the adequacy of the protection system to threats and the state of protected resources with their high dynamics.

References

1. Jumasheva E.S., Nyrkov A.P. Primenenie algoritmov mashinnogo obuchenija dlja obnaruzhenija anomal'nogo povedenija v setjah kriticheskoj informacionnoj infrastruktury // V sbornike: Regional'naja informatika i informacionnaja bezopasnost'. Sbornik trudov Sankt-Peterburgskoj mezhdunarodnoj konferencii. Sankt-Peterburg, 2023. S. 247–251.
2. Nyrkov A.P., Sokolov S.S., Alimov O.M., Chernyj S.G., Dorovskoj V.A. Optimal'naja identifikacija ob#ektov v zadachah raspoznavanija neobitaemymi podvodnymi apparatami // Problemy informacionnoj bezopasnosti. Komp'juternye sistemy. 2020. № 2. S. 58–64.
3. Martynov V.L., Nyrkov A.P., Shimanskaja M.S., Krechetova Je.V., Shimanskaja G.S. Gidroakusticheskie kommunikacii v voprosah protivodejstvija podvodnym robotam // Informatizacija i svjaz'. 2024. № 2. S. 51–55.
4. Pshihopov V. H., Gontar' D. N., Mart'janov O. V. Konceptual'nye podhody k formirovaniju scenariev boevogo primenenija grupp robototehnicheskih kompleksov // Sistemy upravlenija, svjazi i bezopasnosti. 2022. № 3. S. 138–182. DOI: 10.24412/2410-9916-2022-3-138-182
5. Rahmanov A.A. Setecentricheskie sistemy upravlenija zakonomernye tendencii, problemnye voprosy i puti ih reshenija // Voennaja mysl' .2011. № 3, S. 41–50.
6. Bogovik A.V., Ignatov V.V. Teorija upravlenija v sistemah voennogo upravlenija: Uchebn. – SPb.: VAS, 2008. – 460 s.
7. Makarenko S.I. Modeli sistemy svjazi v uslovijah prednamerennyh destabilizirujushhih vozdejstvij i vedenija razvedki. Monografija. – SPb.: Naukoemkie tehnologii, 2020. – 337 s.
8. Lepeshkin O.M. Sintez modeli processa upravlenija social'nymi i jekonomicheskimi sistemami na osnove teorii radikalov: avtoreferat dis. …doktora tehnicheskih nauk : 05.13.10 / Lepeshkin Oleg Mhajlovich. – Sankt-Peterburg, 2014. – 33 s.
9. Polenin V.I., I.A. Rjabinin, S.K. Svirin, I.A. Gladkova Primenenie obshhego logiko-verojatnostnogo metoda dlja analiza tehnicheskih, voennyh organizacionno-funkcional'nyh sistem i vooruzhennogo protivoborstva // Pod red. A.S. Mozhaeva / Rossijskaja akademija estestvennyh nauk. – SPb: SPb-regional'noe otdelenie RAEN, 2011. – 416 s., ill.
10. Zatuliveter Ju. S., Fishhenko E. A. Problemy programmiruemosti, bezopasnosti i nadezhnosti raspredelennyh vychislenij i setecentricheskogo upravlenija. Ch. 1. Analiz problematiki // Problemy upravlenija. 2016. vypusk 3, s. 49–57.
11. V.V. Golenkov, N.A. Guljakina Gra92–101micheskie associativnye modeli i sredstva parallel'noj obrabotki informacii v sistemah iskusstvennogo intellekta // Doklady BGUIR №1. 2004 g. s. 92-101.

БОРЬБА С МАЛОРАЗМЕРНЫМИ БЕСПИЛОТНЫМИ ЛЕТАТЕЛЬНЫМИ АППАРАТАМИ СРЕДСТВАМИ РАДИОЭЛЕКТРОННОЙ БОРЬБЫ

Ануфриев А.А.[1], Чиркин П.М.[2], Шипунов В.А.[3]

DOI: 10.24682/3034-40-50-2024-2-53-61

Ключевые слова: *беспилотный летательный аппарат, противовоздушная оборона, радиоэлектронная борьба, сборный пункт поврежденных машин, маскировка, обнаружение, оповещение, противодействие.*

Аннотация

Цель работы *заключается в разработке рекомендаций по борьбе с малоразмерными беспилотными летательными аппаратами при их интенсивном и массовом применении противоборствующими сторонами в боевых действиях в ходе восстановления поврежденного вооружения, военной и специальной техники.*

Метод: *на основе анализа задач восстановления поврежденного вооружения, военной и специальной техники в ходе боевых действий, сравнения характеристик и возможностей применяемых беспилотными летательными аппаратами различного назначения, имеющихся сведений о состоянии борьбы с беспилотными летательными аппаратами средствами разведки, противовоздушной обороны, радиоэлектронной борьбы, способами противодействия техническим средствам разведки противника разработать комплект средств радиоэлектронной борьбы с применяемыми беспилотными летательными аппаратами и способы их боевого применения в ходе восстановления вооружения, военной и специальной техники на этапе эвакуации.*

Результаты: *определены основные особенности задач восстановления вооружения, военной и специальной техники, характеристики беспилотных летательных аппаратов, существенные в ходе решения задач борьбы с ними на этапе эвакуации вооружения, военной и специальной техники при ее восстановлении; разработаны требования к комплекту средств борьбы с беспилотными летательными аппаратами и определены их количественные значения; определены основные характеристики средств радиоэлектронной борьбы, существенные с точки зрения борьбы с беспилотными летательными аппаратами; определен комплект средств радиоэлектронной борьбы и разработаны способы его боевого применения.*

Практическая ценность *заключается в разработанных практических рекомендациях подразделениям технического обеспечения по борьбе с беспилотными летательными аппаратами в ходе эвакуации вооружения, военной и специальной техники.*

Постановка задачи

Одним из видов всестороннего обеспечения является техническое обеспечение, основу которого составляет восстановление вооружения, военной и специальной техники (далее – ВВСТ). Восстановление включает: техническую разведку, эвакуацию, ремонт и возвращение в строй отремонтированных (эвакуированных), а также передачу невосстанавливаемых в соединении (части) изделий силами и средствами старшего начальника. Восстановление ВВСТ является основным источником восполнения потерь в ходе боевых действий.

Кроме того, многие ВВСТ, стоящие на вооружении, имеют характеристики, параметры, внешний вид, обуславливающие их высокую эффективность боевого применения, могут содержать конфиденциальную информацию. Такие образцы ВВСТ в целях обеспечения защиты государственной тайны должны быть немедленно эвакуированы с поля боя. Противник широко применяет свои образцы ВВСТ, которые также представляют интерес для отечественной военной науки.

Наиболее сложным этапом с точки зрения обеспечения скрытности, быстроты выполнения и защиты от поражения противником является этап эвакуации ВВСТ с поля боя.

Противник постарается всеми способами препятствовать проведению необходимых мероприятий. В районах расположения поврежденной техники будет барражировать его разведывательная беспилотная авиация с целью получения

[1]Ануфриев Алексей Александрович, кандидат технических наук, доцент, профессор кафедры радиоэлектронной борьбы Военной академии связи, г. Санкт-Петербург, Россия. E-mail: irbis453@mail.ru

[2]Чиркин Павел Михайлович, преподаватель кафедры радиоэлектронной борьбы Военной академии связи, г. Санкт-Петербург, Россия. E-mail: 67-ссср@mail.ru

[3]Шипунов Владимир Алексеевич, кандидат военных наук, доцент, профессор кафедры радиоэлектронной борьбы Военной академии связи, г. Санкт-Петербург, Россия. E-mail: colonel53@mail.ru

разведывательных данных о возможности добывания конфиденциальной информации о наших образцах ВВСТ или информации о возможности эвакуации своей поврежденной техники [1]. При обнаружении сил технической разведки и (или) средств эвакуации будут применяться ударные беспилотные летательные аппараты (БпЛА). Наиболее эффективными средствами разведки и поражения в этих условиях будут применяемые противником малоразмерные БпЛА на основе DJI и FPV-дронов.

Широкое разнообразие БпЛА, применение их для ведения разведки и поражения требует принятия соответствующих мер борьбы с ними и разработки соответствующих средств и способов борьбы. Борьба с БпЛА носит комплексный характер. Одной из ее составляющих является радиоэлектронная борьба (РЭБ). Номенклатура средств РЭБ с БпЛА в настоящее время достаточно многообразна. Необходимо правильно выбрать требуемые средства для решения конкретных задач в конкретных условиях, разработать способы их боевого применения. Существует реальная необходимость в методике количественной оценки состава средств РЭБ и способов их боевого применения при решении задач в ходе борьбы с малоразмерными БпЛА при эвакуации ВВСТ и на ее основе разработке рекомендаций по выбору средств и способов борьбы с ними.

Решение задачи

Борьба с малоразмерными БпЛА противника предполагает комплексное применение средств и способов обнаружения, оповещения, противовоздушной обороны (далее — ПВО), противодействия техническим средствам разведки противника (далее — ПД ТСР), организацию управления и взаимодействия, и подразделяется на три основные составляющие: о***бнаружение, оповещение и противодействие***. Способы борьбы с ними могут быть активными и пассивными [2].

Обнаружение должно осуществляться постоянно. Чем раньше будет вскрыт факт применения противником БпЛА, тем более эффективной будет борьба с ними.

Обнаружение осуществляется способами визуального наблюдения и с использованием технических средств. Для этого назначаются посты воздушного наблюдения (ПВН).

Визуальное наблюдение может осуществляться как непосредственно из района эвакуации, так и со специальных постов наблюдения, оборудуемых на некотором удалении от него.

Основными требованиями к ним являются:

- скрытность;
- отсутствие в непосредственной близости источников шума, тепла и света;
- соблюдение визуальной видимости с районом эвакуации.

При постановке задач на наблюдение указываются:

- содержание задачи;
- сектор наблюдения;
- возможные действия противника;
- вероятное направление подлета БпЛА;
- порядок оповещения при обнаружении БпЛА.

Для повышения эффективности обнаружения БпЛА используются различные оптические и оптико-электронные приборы (бинокли, приборы ночного видения, тепловизоры и др.).

В отсутствие визуального контакта с БпЛА их наличие обнаруживается также по звуку работы двигателей.

Основным демаскирующим признаком применения БпЛА является наличие радиоизлучения на частотах передачи видеоизображения и управления.

Оповещение базируется на заблаговременно создаваемую систему оповещения, включающую систему связи, средства оповещения (сирена, ракетница и др.), голосом и т. д. Сигналы должны быть понятны всем членам группы эвакуации.

Противодействие может осуществляться активными и пассивными способами.

К активным способам противодействия относятся:

- огневое поражение пунктов управления БпЛА противника.

К пассивным способам борьбы относятся:

- передвижение в условиях ограниченной видимости;
- оборудование фортификационных сооружений;
- создание ложных позиций;
- маскировка своих позиций;
- использование теплоизоляционных накидок для личного состава и ВВСТ [4];
- применение защитных сетей и металлических конструкций для защиты средств и объектов.

Борьба с БпЛА при эвакуации техники и ее ремонте имеет ряд особенностей.

На этапе эвакуации осуществляется буксировка или транспортирование поврежденных (технически неисправных) ВВСТ из-под огня противника из мест, которым угрожает захват противником, из районов радиационного, химического, биологического заражения в укрытия, к местам ремонта или передачи, а также выта-

скивание застрявших (затонувших) ВВСТ. Этот этап характеризуется рядом особенностей, являющихся демаскирующими признаками деятельности групп эвакуации. Наиболее информативными из них для иностранной технической разведки являются:

- активизация деятельности средств эвакуации на маршрутах передвижения и в районах расположения поврежденной техники;
- интенсивная работа средств связи;
- локализация личного состава и техники в местах расположения поврежденной техники;
- постоянно работающие двигатели средств эвакуации.

По этим демаскирующим признакам [5], особенно при отсутствии средств маскировки, противник может легко вскрыть маршруты перемещения и районы расположения эвакуационных средств.

На этапе эвакуации, учитывая его маневренный характер, в полном объеме применить перечисленные выше способы борьбы невозможно. Борьбу с БпЛА на этом этапе целесообразно организовать следующим образом.

Все средства эвакуации должны быть оборудованы защитными сетями, металлическими конструкциями для защиты от поражения FPV-дронов, средствами радиоэлектронного подавления [6]. Передвижение на маршрутах выдвижения и эвакуации осуществлять по возможности в условиях ограниченной видимости, в сопровождении средств РЭБ, предназначенных для создания помех радиоуправляемым минно-взрывным устройствам (далее — РУМВУ). При ведении переговоров по средствам связи строго соблюдать меры противодействия средствам радиоэлектронной разведки противника.

Для *обнаружения* атак необходимо сформировать ПВН с указанием задачи, сектора наблюдения, возможных действий противника, вероятного направления подлета БпЛА, порядка оповещения при их обнаружении. Посты должны быть оснащены необходимыми средствами видеонаблюдения, техническими средствами разведки и связи. С учетом малой численности группы эвакуации пост наблюдения может быть в составе одного наблюдателя. Целесообразное размещение наблюдателей — вкруговую вокруг объекта эвакуации на удалении, обеспечивающем принятие мер противодействия после оповещения. Для мобильности наблюдателя целесообразно применение мобильных средств передвижения, например, квадроцикл.

Противодействие целесообразно организовывать непосредственно на объекте эвакуации. Для этого формируется пост противодействия (ПП) аналогичный ПВН. Посту также указываются задачи, сектор наблюдения, возможные действия противника, вероятное направление подлета БпЛА, порядок взаимодействия с постами наблюдения, порядок оповещения. Посты оснащаются необходимыми средствами противодействия: средствами технической разведки и обнаружения, стрелковым вооружением, средствами РЭБ, средствами связи. Высокие результаты показывает гладкоствольное оружие, стреляющее дробью, создавая облако поражающих элементов, воздействующее на цель.

Наиболее эффективным, но не достаточным способом является применение средств РЭБ [7]. При этом надо учитывать, что противодействие БпЛА средствами РЭБ является всего лишь элементом общей системы ротиводействия и должно применяться в комплексе с другими мерами: скрытностью передвижения, маскировкой, применением защитных сетей и т. д. в соответствии с другими рекомендациями, инструкциями и распоряжениями.

Проведенный анализ типовых малоразмерных БпЛА показал (таблица 1), что с точки зрения РЭБ радиоподавление их каналов управления существующими средствами РЭБ вполне возможно. Вместе с тем в силу разработки комплексов различными фирмами функционирование каналов управления осуществляется в дискретных диапазонах. Имеются участки диапазона, в которых комплексы не работают. Этот факт создает возможность освоения при необходимости незанятых участков диапазона.

Таблица 1.

Типовые характеристики БпЛА

№ п/п	Название БпЛА	Предназначение	Диапазоны работ
1	«Mugin-5 Pro Китай»	Поиск и уничтожение стационарных и подвижных наземных целей	силу и фортификационные сооружения КУ прием: 5,800 МГц КУ передача: 2,400 МГц ТЛМ прием: 1420-1470 МГц ТЛМ передача: 902-928 МГц GPS, ГЛОНАСС, Galileo, BeiDou
2	Mugin-5 Pro 5000 мм с 8 моторными креплениями Китай	Поиск и уничтожение стационарных наземных целей, включая живую силу	КУ прием: 5,800 МГц КУ передача: 2,400 МГц ТЛМ прием: 1420-1470 МГц ТЛМ передача: 902-928 МГц GPS, ГЛОНАСС, Galileo, BeiDou
3	ACS-3M (Raybird-3), Украина	Ведение аэрофотосъемки и передача видеосигнала в дневное и ночное время по наземным и водным объектам, картографирование и корректировки огня артиллерии	КУ прием: 461-469 МГц (ППРЧ) КУ передача: 910-929 МГц (ППРЧ), GPS
4	Orlik PGZ-19R Польша	Ведение видовой разведки в бригадном звене управления	КУ прием: 450-460 МГц (ППРЧ) КУ передача: 450-460 МГц (ППРЧ), GPS
5	Народный (PD-1) Украина	Ведение воздушной разведки, поиска объектов на местности и определения их координат	КУ прием: 450-460 МГц (ППРЧ) КУ передача: 450-460 МГц (ППРЧ) ТЛМ прием: 310–390 МГц (ППРЧ) ТЛМ передача: 310–390 МГц (ППРЧ), GPS
6	Фурия Украина	Ведение воздушной разведки при неблагоприятных погодных условиях, в ночное время и в условиях плохой видимости корректировка огня артиллерии	КУ прием: 433-447 МГц КУ передача: 433-447 МГц ТЛМ прием: 917-928 МГц (ППРЧ) ТЛМ передача: 917-928 МГц (ППРЧ), GPS
7	Флай ай Польша	Обнаружение и уничтожение живой силы противника (осколочно-фугасная головная часть GO-1, радиус поражения — 10 м)	КУ прием: 4-5 ГГц, ширина 5,5 МГц КУ передача: 4-5 ГГц, GPS
8	Лелека-100 Украина	Аэроразведка, патрулирование, картографирование местности и получение точных географических координат в режиме реального времени	КУ прием: 438-448 МГц КУ передача: 438-448 МГц ТЛМ прием: 410-480 МГц ТЛМ передача: 410-480 МГц, 900-930 МГц, GPS
9	Supervisor SM 2 Украина	Поиск и уничтожение стационарных и подвижных наземных целей, включая живую силу и фортификационные сооружения	КУ прием: 433-439 Мгц, 915-930 Мгц, 2,4 ГГц; КУ передача: 433-439 Мгц, 915-930 Мгц, 2,4 ГГц; ТЛМ прием: 371,8-395,1 МГц; ТЛМ передача: 371,8-395,1 МГц; GPS
10	DJI «Mavic» Китай	Ведение аэрофотосъемки и картографирования, решения задач видеонаблюдения за обстановкой в режиме реального времени	КУ прием: 2,4-2,48 ГГц КУ передача: 2,4-2,48 ГГц ТЛМ прием: 5,525-5,850 ГГц ТЛМ передача: 5,525-5,850 ГГц GPS, ГЛОНАСС, BeiDou

Управление БпЛА в полете осуществляется на определенных частотах каналов управления (далее — КУ). От БпЛА передается на пункт управления видеоизображение. Кроме того, летательный аппарат в полете пользуется навигационными системами, подавление которых также дает положительный эффект [8]. Канал видеоизображения и канал навигационных систем объединены в канал телеметрии (далее — ТЛМ).

При этом необходимо правильно подобрать мощностные характеристики средств радиоподавления и обеспечить частотное совпадение передатчиков средств РЭБ с частотами, на которых осуществляется управление БпЛА.

Для определения мощностных характеристик средств РЭБ и правильного выбора дистанций радиоподавления необходимо провести расчеты, учитывающие условия применения как БпЛА, так и средств РЭБ. Для этого разработана методика оценки возможностей средств РЭБ по радиоподавлению каналов управления, передачи видеоизображения и навигации БпЛА [9].

Суть методики сводится к определению дальности радиоподавления каналов управления, навигации и передачи видеоизображения при известных исходных данных.

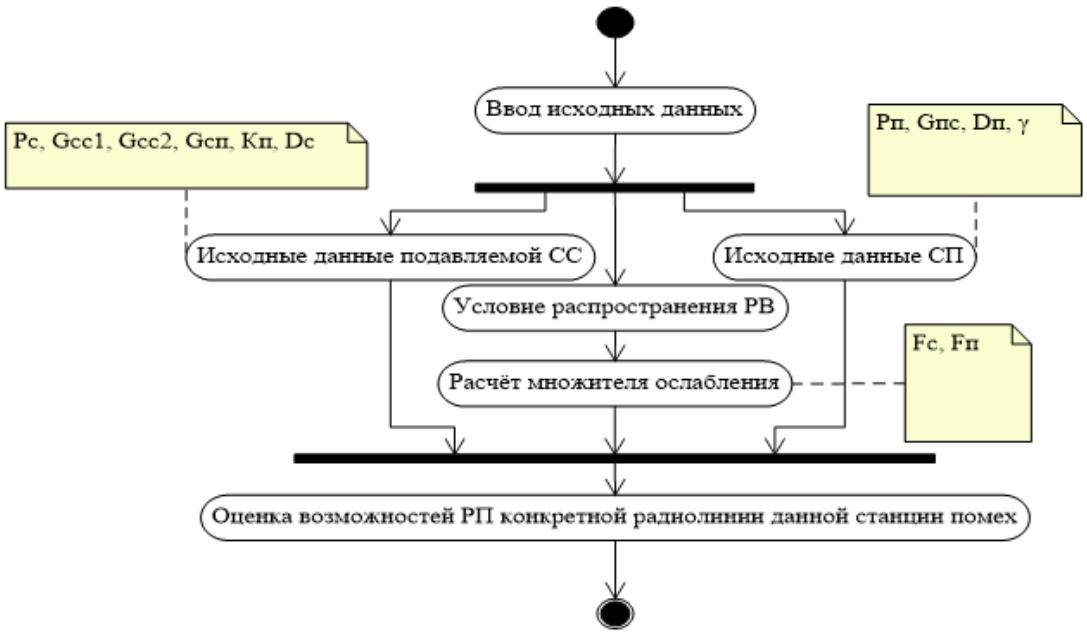

Рис.1. Методика оценки возможностей средств РЭБ по радиоподавлению

Анализ типовых средств РЭБ (таблица 2) показал, что их частотные диапазоны, как правило, совпадают с частотными диапазонами БпЛА. Это позволяет создавать помехи КУ и каналам ТЛМ. Вместе с тем, каждое конкретное средство РЭБ не имеет возможности создавать помехи во всем потенциальном диапазоне частот БпЛА. Чтобы подавить любой БпЛА, необходимо перекрыть весь их потенциальный частотный диапазон. Для этого необходимо формировать комплект средств РЭБ, обеспечивающий подавление во всем частотном диапазоне БпЛА.

Вместе с тем, необходимо иметь в виду, что средство РЭБ излучает электромагнитные волны и определение его координат вполне решаемая задача. Этот факт накладывает ограничения на выбор позиционного района для его развертывания. Средства РЭБ большой дальности целесообразно развертывать на удалении от прикрываемого объекта, а малой дальности — непосредственно на прикрываемом объекте. Исключение составляют средства РЭБ, предназначенные для защиты автомобильной и бронированной техники на марше путем установки специальных средств радиоэлектронного подавления, предназначенных для создания помех радиоуправляемым минно-взрывным устройствам.

Таблица 1.

Типовые характеристики БпЛА

№ п/п	Предназначение	Объекты воздействия	Частотный диапазон (МГц)
1	Для радиоподавления аппаратуры потребителей глобальных навигационных спутниковых систем беспилотных летательных аппаратов	Современные навигационные приемники БпЛА типа Novatel OEM719 и Ublox ZED-F9P	1168-1178, 1194-1212, 1221-1249, 1270-1283, 1556-1576, 1593-1604
2	Для интеллектуальной подмены координат путем искажения навигационных сигналов в АП ГНСС БпЛА	Современные навигационные приемники БпЛА типа Novatel OEM719 и Ublox ZED-F9P	1575,42
3	Для радиоподавления каналов управления беспилотных летательных аппаратов и их навигационных приемников	Коммерческие БпЛА ближнего действия	Каналы управления, СРНС, Wi-Fi
4	Для радиоподавления каналов управления БпЛА квадрокоптерного типа и их навигационных приемников	DJI Mavic Pro (FCC+), DJI Mini 2 (FCC), Ublox ZED-F9P, Mavic 3T (NeoBoost).	1100-1610, 700-2650, 2600-6000
5	Для радиоподавления каналов управления беспилотных летательных аппаратов и их навигационных приемников	Navic Pro (FCC+), DJI Mini 2 (FCC), Mavic 3 (FCC), Autel Evo 2 v3, БпЛА FPV-типа Crossfire TBS Tango2.	859-947, 1168-1287, 1555-1612, 2389-2495, 5715-5860
6	Для обнаружения каналов управления и радиоподавления каналов управления БпЛА и их навигационных приемников	DJI Mavic Pro (FCC+), DJI Mini 2 (FCC), Mavic 3 (FCC), Mavic 3T (NeoBoost), Autel Evo 2, аппаратура управления Crossfire TBS Tango2	430-436,863-870, 902-928, 1166-1279, 1559-1610, 2400-2484, 5150-5350, 5725-5875
7	Для радиоподавления каналов управления БпЛА квадрокоптерного типа и их навигационных приемников	Современные навигационные приемники БпЛА	433, 868, 900,1500, 2400, 5200, 5800
8	Для радиоподавления аппаратуры потребителей глобальных навигационных спутниковых систем	Современные навигационные приемники БпЛА	1150÷1300; 1550÷1610, GPS, ГЛОНАСС, Beidou, Galileo

В ходе эвакуации целесообразно, по возможности, устанавливать взаимодействие с частями и подразделениями ПВО, радиоэлектронной разведки (РЭР) и РЭБ. Средства ПВО и РЭР в дополнение к средствам постов наблюдения обеспечат своевременное оповещение об атаке. Средства РЭБ обеспечат радиоподавление атакующих БпЛА, что позволит не включать свои средства РЭБ, затруднив тем самым разведке противника определение координат объекта эвакуации.

На вооружении ПП целесообразно иметь средства РЭБ двух типов: средства большой дальности, обеспечивающие воздействие на дальностях, превышающих визуальный контакт, и средства малой дальности, обеспечивающие воздействие при визуальном контакте 10]. Такие средства приняты на снабжение Вооруженных Сил Российской Федерации, поставляются ведомством по линии Министерства обороны Российской Федерации и различными волонтерскими организациями.

Дальность подавления таких средств варьируется от нескольких десятков метров до десятков километров, обеспечивая подавление каналов навигации и управления БпЛА, а также передачи видеоизображения с борта БпЛА на наземный пункт управления. В группе эвакуации достаточно иметь средства большой дальности с возможностью подавления 2-3 км, функционирующие в автоматическом режиме. Однако при выборе конкретного образца средства РЭБ необходимо учитывать значительное влияние на эффективность их работы рельефа местности и местных предметов (здания, лесополосы), что значительно снижает дальность подавления.

Средства малой дальности известны под названием «антидроновое ружье» и применяются при визуальном наблюдении БпЛА на расстоянии от нескольких десятков до нескольких сотен метров. Их допускается размещать непосредственно на объекте эвакуации путем объединения ПВН, противодействия и огневого поражения.

Средства большой дальности целесообразно размещать на некотором удалении от объекта эвакуации на расстоянии их возможностей по дальности подавления. Для снижения возможностей противника по обнаружению и идентификации этих средств целесообразно развертывание 2–3 ложных позиций средств РЭБ. Развертывание и маскировку всех средств целесообразно организовать заблаговременно. Наиболее приемлемый способ прикрытия — вкруговую. При лимите времени развертывание средств противодействия осуществляется одновременно с эвакуацией с упреждением на время развертывания.

Вариант боевого применения показан на рисунке 2.

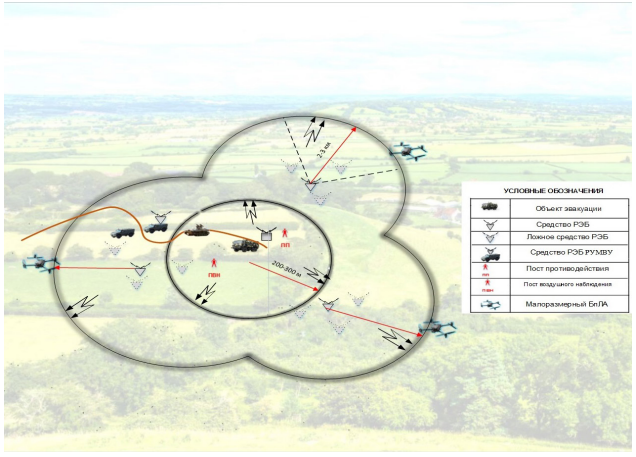

Рис.2. Боевой порядок средств РЭБ (вариант)

Выводы

При эвакуации ВВСТ в целях эффективной борьбы с БпЛА различного назначения, в том числе ударных, необходимо создавать систему противодействия БпЛА в составе подсистем оповещения, ПВО, РЭБ. Основными требованиями к ней могут быть:

- наличие в составе группы эвакуации, совершающей марш, средств ПВО, а также средств РЭБ, предназначенных для создания помех радиоуправляемым минно-взрывным устройствам;
- оборудование средств эвакуации защитными сетями, металлическими конструкциями, средствами индивидуального радиоэлектронного подавления для защиты от поражения FPV-дронов;
- наличие в группе эвакуации специально подготовленной группы борьбы с БпЛА в составе ПВН и ПП, которые могут быть, при необходимости, объединены в один пост;
- организация управления и взаимодействия в группе эвакуации по вопросам борьбы с БпЛА;
- оснащение ПВН техническими средствами наблюдения: визуальными и оптико-электронными средствами наблюдения, средствами связи и передачи разведывательных сведений, тепловизором, прожектором, приемником, модулем акустической разведки, спектроанализатором, лазерной указкой и др.;
- оснащение ПП средствами РЭБ большой (до 2–3 км) и малой, типа «антидроновое ружье» (сотни метров), дальности;
- комплектование ПП средствами РЭБ, перекрывающими потенциальный частотный диапазон БпЛА;
- развертывание в целях противодействия техническим средствам разведки противника вблизи реальных позиций средств РЭБ ложных позиций;
- развертывание на объекте эвакуации совмещенного ПВН, огневого поражения воздушных целей и противодействия, оснащенных «электронными ружьями».
- организация взаимодействия с частями ПВО, РЭР и РЭБ.

Литература

1. Андросов В.В., Рахмонбердиев Ф.А., Шипунов В.А. Система управления незаконных вооруженных формирований // Инновационная деятельность в Вооруженных Силах Российской Федерации. Труды всеармейской научно-практической конференции. Санкт-Петербург, 1921. С.271–273.
2. Михайлов Р.Л. Радиоэлектронная борьба в Вооруженных силах США: военно-теоретический труд. – СПб.: Наукоемкие технологии, 2018. – 131 с.
3. Ануфриев А.А., Чиркин П.М., Шипунов В.А. Задачи и направления совершенствования комплексов радиоэлектронного подавления в современных условиях // В сборнике: Инновационная деятельность в вооруженных силах Российской Федерации. Труды всеармейской научно-практической конференции. Санкт-Петербург, 2022. С. 75–79
4. Ануфриев А.А., Беляев Д.П., Чиркин П.М., Шипунов В.А. Защита от технической разведки образцов изделий на стадии их эксплуатации в локальных войнах и вооруженных конфликтах // В сборнике: Технологии. Инновации. Связь. Материалы научно-практической конференции. Санкт-Петербург, 2023. С. 84–88.
5. Меньшаков Ю.К. Основы защиты от технических разведок. – М.: Изд-во МГТУ им. Н.Э. Баумана, 2011. – 478 с.
6. Ануфриев А.А., Чиркин П.М., Шипунов В.А. Радиоэлектронная борьба в урбанизированной деятельности // В сборнике: Инновационная деятельность в вооруженных силах Российской Федерации. Труды всеармейской научно-практической конференции. Санкт-Петербург, 2022. С. 55–59.
7. Макаренко С. И. Анализ средств и способов противодействия беспилотным летательным аппаратам. Часть 3. Радиоэлектронное подавление систем навигации и радиосвязи // Системы управления, связи и безопасности. 2020. № 2. С. 101–175.
8. Ануфриев А.А., Чиркин П.М., Шипунов В.А. Анализ помехоустойчивости системы навигационно-временного обеспечения «Навстар» // В сборнике: Инновационная деятельность в вооруженных силах Российской Федерации. Труды всеармейской научно-практической конференции. Санкт-Петербург, 2022. С. 42-51.
9. А.А. Ануфриев, В.В. Панасюк, П.М. Чиркин, В.А. Шипунов. Оценка вероятности энергетической доступности подавляемых линий радиосвязи // В сборнике: Инновационная деятельность в Вооруженных Силах Российской Федерации. Труды всеармейской научно- практической конференции. Санкт-Петербург, 2023. С. 94–01.
10. Макаренко С.И. Противодействие беспилотным летательным аппаратам. Монография. – СПб.: Наукоемкие технологии. 2020. –204 с.

COUNTERING SMALL UNMANNED AERIAL VEHICLES WITH ELECTRONIC WARFARE

Anufriev A.A.[1], Chirkin P.M.[2], Shipunov V.A.[3]

Keywords: *air defense, assembly point of damaged vehicles, camouflage, detection, warning, counteraction.*

Abstract

The purpose *of the work is to develop recommendations for combating small-sized unmanned aerial vehicles during their intensive and massive use by the warring parties in combat operations during the restoration of damaged weapons, military and special equipment.*

Method: *on the basis of the analysis of the tasks of restoring damaged weapons, military and special equipment in the course of hostilities, comparing the characteristics and capabilities of unmanned aerial vehicles used for various purposes, the available information on the state of combating unmanned aerial vehicles by reconnaissance, air defense, electronic warfare, methods of countering enemy reconnaissance equipment, to develop a set of means electronic warfare against unmanned aerial vehicles used and methods of their combat use during the restoration of weapons, military and special equipment at the evacuation stage.*

Results: *the main features of the tasks of restoring weapons, military and special equipment, the characteristics of unmanned aerial vehicles that are essential in the course of solving the problems of combating them at the stage of evacuation of weapons, military and special equipment during its restoration have been determined; the requirements for the set of means of combating unmanned aerial vehicles have been developed and their quantitative values were determined; the main characteristics of electronic warfare means that are essential from the point of view of combating unmanned aerial vehicles have been determined; a set of electronic warfare equipment has been determined and methods of its combat use have been developed.*

The practical value *lies in the developed practical recommendations for technical support units to combat unmanned aerial vehicles during the evacuation of weapons, military and special equipment.*

[1]Alexey A. Anufriev, Ph.D., Associate Professor, Professor of the Department of Electronic Warfare of the Military Academy of Communications, St. Petersburg, Russia. E-mail: irbis453@mail.ru

[2]Pavel M. Chirkin, Lecturer, Department of Electronic Warfare, Military Academy of Communications, St. Petersburg, Russia. E-mail: 67-cccp@mail.ru

[3]Vladimir A. Shipunov, Ph.D, Associate Professor, Professor of the Department of Electronic Warfare of the Military Academy of Communications, St. Petersburg, Russia. E-mail: colonel53@mail.ru

References

1. Androsov V.V., Rahmonberdiev F.A., Shipunov V.A. Sistema upravlenija nezakonnyh vooruzhennyh formirovanij // Innovacionnaja dejatel'nost' v Vooruzhennyh Silah Rossijskoj Federacii. Trudy vsearmejskoj nauchno-prakticheskoj konferencii. Sankt-Peterburg, 1921. C.271–273.
2. Mihajlov R.L. Radiojelektronnaja bor'ba v Vooruzhennyh silah SShA: voenno-teoreticheskij trud. – SPb.: Naukoemkie tehnologii, 2018. – 131 s.
3. Anufriev A.A., Chirkin P.M., Shipunov V.A. Zadachi i napravlenija sovershenstvovanija kompleksov radiojelektronnogo podavlenija v sovremennyh uslovijah // V sbornike: Innovacionnaja dejatel'nost' v vooruzhennyh silah Rossijskoj Federacii. Trudy vsearmejskoj nauchno-prakticheskoj konferencii. Sankt-Peterburg, 2022. S. 75–79
4. Anufriev A.A., Beljaev D.P., Chirkin P.M., Shipunov V.A. Zashhita ot tehnicheskoj razvedki obrazcov izdelij na stadii ih jekspluatacii v lokal'nyh vojnah i vooruzhennyh konfliktah // V sbornike: Tehnologii. Innovacii. Svjaz'. Materialy nauchno-prakticheskoj konferencii. Sankt-Peterburg, 2023. S. 84–88.
5. Men'shakov Ju.K. Osnovy zashhity ot tehnicheskih razvedok. – M.: Izd-vo MGTU im. N.Je. Baumana, 2011. – 478 s.
6. Anufriev A.A., Chirkin P.M., Shipunov V.A. Radiojelektronnaja bor'ba v urbanizirovannoj dejatel'nosti // V sbornike: Innovacionnaja dejatel'nost' v vooruzhennyh silah Rossijskoj Federacii. Trudy vsearmejskoj nauchno-prakticheskoj konferencii. Sankt-Peterburg, 2022. S. 55–59.
7. Makarenko S. I. Analiz sredstv i sposobov protivodejstvija bespilotnym letatel'nym apparatam. Chast' 3. Radiojelektronnoe podavlenie sistem navigacii i radiosvjazi // Sistemy upravlenija, svjazi i bezopasnosti. 2020. № 2. S. 101–175. DOI: 10.24411/2410-9916-2020-10205.
8. Anufriev A.A., Chirkin P.M., Shipunov V.A. Analiz pomehoustojchivosti sistemy navigacionno-vremennogo obespechenija «Navstar» // V sbornike: Innovacionnaja dejatel'nost' v vooruzhennyh silah Rossijskoj Federacii. Trudy vsearmejskoj nauchno-prakticheskoj konferencii. Sankt-Peterburg, 2022. S. 42-51.
9. A.A. Anufriev, V.V. Panasjuk, P.M. Chirkin, V.A. Shipunov. Ocenka verojatnosti jenergeticheskoj dostupnosti podavljaemyh linij radiosvjazi // V sbornike: Innovacionnaja dejatel'nost' v Vooruzhennyh Silah Rossijskoj Federacii. Trudy vsearmejskoj nauchno- prakticheskoj konferencii. Sankt-Peterburg, 2023. S. 94–01.
10. Makarenko S.I. Protivodejstvie bespilotnym letatel'nym apparatam. Monografija. – SPb.: Naukoemkie tehnologii. 2020. –204 s.

TELECOMMUNICATIONS AND THE CONNECTION

SCIENTIFIC PEER-REVIEWED JOURNAL
№2 (02) 2024 г.
Published 6 times a year

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

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

Signed to the press on 10/20/2024.
The total circulation is 120 copies. The price is free Postal address: 1st Rusakovsky lane, 1, 141006, Mytishchi, Moscow region, Russia
E-mail: editor@telemil.ru Tel.: +7 (985) 939-75-01.

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

CONTENTS

TELECOMMUNICATIONS AND THE CONNECTION

№2 (02) 2024

DOI: 10.24682/3034-4050

WWW.TELEMIL.RU
EDITOR@TELEMIL.RU