TELECOMMUNICATIONS AND COMMUNICATIONS

№ 4 (13) 2026

DOI: 10.21681/3034-4050

THEME OF THE ISSUE:

WWW.TELEMIL.RU
EDITOR.TIS@YANDEX.RU

ТЕЛЕКОММУНИКАЦИИ и СВЯЗЬ

№ 4 (13) 2026

ТЕМА НОМЕРА:

WWW.TELEMIL.RU

DOI: 10.21681/3034-4050

ТЕЛЕКОММУНИКАЦИИ И СВЯЗЬ

НАУЧНЫЙ РЕЦЕНЗИРУЕМЫЙ ЖУРНАЛ
№ 4 (13) 2026 г.
Выходит 6 раз в год

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

Журнал входит в Российский индекс научного цитирования, публикует статьи по специальностям перечня научных специальностей группы 6.0.0

Учредитель и издатель

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

Над номером работали:

Г. И. Макаренко – *шеф-редактор*, Н. В. Селезенев – *отв. секретарь*, С. С. Игнатов – *верстка*, А. В. Матюшин – *маркетинг и подписка*

Подписано к печати 17.08.2026 г.
Общий тираж 120 экз. Цена свободная

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

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

СОДЕРЖАНИЕ

Подписка на журнал осуществляется в 2026 г. через редакцию журнала

ПРИМЕНЕНИЯ СРЕДСТВ БЕСПРОВОДНОГО ШИРОКОПОЛОСНОГО ДОСТУПА В ТРАНСПОРТНОЙ СЕТИ СВЯЗИ ГРУППИРОВКИ ВОЙСК

Иванов В. Г.[1] , Квитка Д. В.[2], Петров И. А.[3], Баширов С. Ю.[4]

DOI:10.21681/3034-4050-2026-4-2-12

Ключевые слова: *система связи, доступ, протокол, узел доступа, опорная сеть, ретранслятор, самоорганизующаяся сеть связи, Mesh-сеть, беспроводный широкополосный доступ.*

Аннотация

Цель работы: *на основе опыта применения средств беспроводного широкополосного доступа в ходе специальной военной операции рассмотрены варианты их применения в целях повышения эффективности функционирования транспортной сети связи группировки войск.*

Метод исследования: *общая теория систем, теория военной связи, теория открытых систем с использованием методов системного анализа. Достоверность результатов обеспечивается практической реализаций приложенных в статье способов применения средств беспроводного широкополосного доступа в системах связи различных уровней управления.*

Результаты исследования: *проведен анализ результатов практического применения средств беспроводного широкополосного доступа как средства транспортной сети связи так и для организации каналов управления наземными робототехническими комплексами и видеотрансляции с беспилотных летательных аппаратов. Внедрение оборудования средств беспроводного широкополосного доступа для расширения высокоскоростной транспортной сети в тактическом и оперативном звене управления позволяет создать надёжную, масштабируемую и отказоустойчивую инфраструктуру различной конфигурации.*

Научная новизна: *заключается в разработке обоснованных направлений повышения эффективности функционирования транспортной сети связи группировки войск на основе применения средств беспроводного широкополосного доступа.*

Введение

В целях повышение эффективности системы связи группировок войск осуществляется поиск новых средств связи и технологий связи обеспечивающих выполнение требования по пропускной способности и устойчивости линий связи транспортной сети связи (ТрСС).

Основу транспортной сети связи (ТрСС) группировки войск в районах, не оборудованных в отношении связи, составляет опорная сеть связи, которая, как правило, строится по зональному принципу [1, 2]. В зоне ответственности группировки войск возможно выделить несколько взаимосвязанных между собой районов – передового, центрального и базового (тыльного) районов (рис. 1).

Передовой район связи охватывает тактические (опорные сети дивизий и бригад) и оперативные (полевые опорные сети связи общевойсковых армий первого эшелона) (до 20 км от зоны ведения боевых действий). Центральный район связи располагается от тыльной границы передового района связи до начала базового сектора связи (40–70 км от переднего края обороны) и включает в себя полевые опорные сети связи общевойсковых армий и бригад второго эшелона. Зона связи базового района начинается на удалении 70 – 100 км от переднего края обороны и охватывает весь оперативный тыл группировки войск. Основу ТрСС в базовом (тыльном) районе составляет полевая опорная сеть связи военного округа и узлы связи стационарной сети связи операторов, которые в зависимости от возможностей подразделяются на магистральные и зональные узлы агрегации трафика.

Кроме того, часть узлов связи ТрСС также выполняет функции узлов связи доступа (УСД) [1, 2].

Следует учитывать, что передовой и центральный район связи находятся в зоне досягаемости применения противником различных

1 ***Иванов Василий Геннадьевич***, доктор военных наук, доцент, профессор кафедры информатики и вычислительной техники инженерного факультета Академии гражданской защиты Министерства Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий имени генерал-лейтенанта Д. И. Михайлика. Химки, Россия. E-mail: v.ivanov@agz.50.mchs.gov.ru

2 ***Квитка Дмитрий Владимирович***, начальник связи-заместитель начальника штаба Московского военного округа. Санкт-Петербург, Россия. E-mail: wasj2006@yandex.ru

3 ***Петров Игорь Александрович***, начальник связи–заместитель начальника штаба Московского военного округа. Санкт-Петербург, Россия. E-mail: petrovigor28@yandex.ru

4 ***Баширов Сергей Юрьевич***, заместитель начальника управления Главного управления связи Вооруженных Сил Российской Федерации. Москва, Россия. E-mail: S.bashirov81@yandex.ru

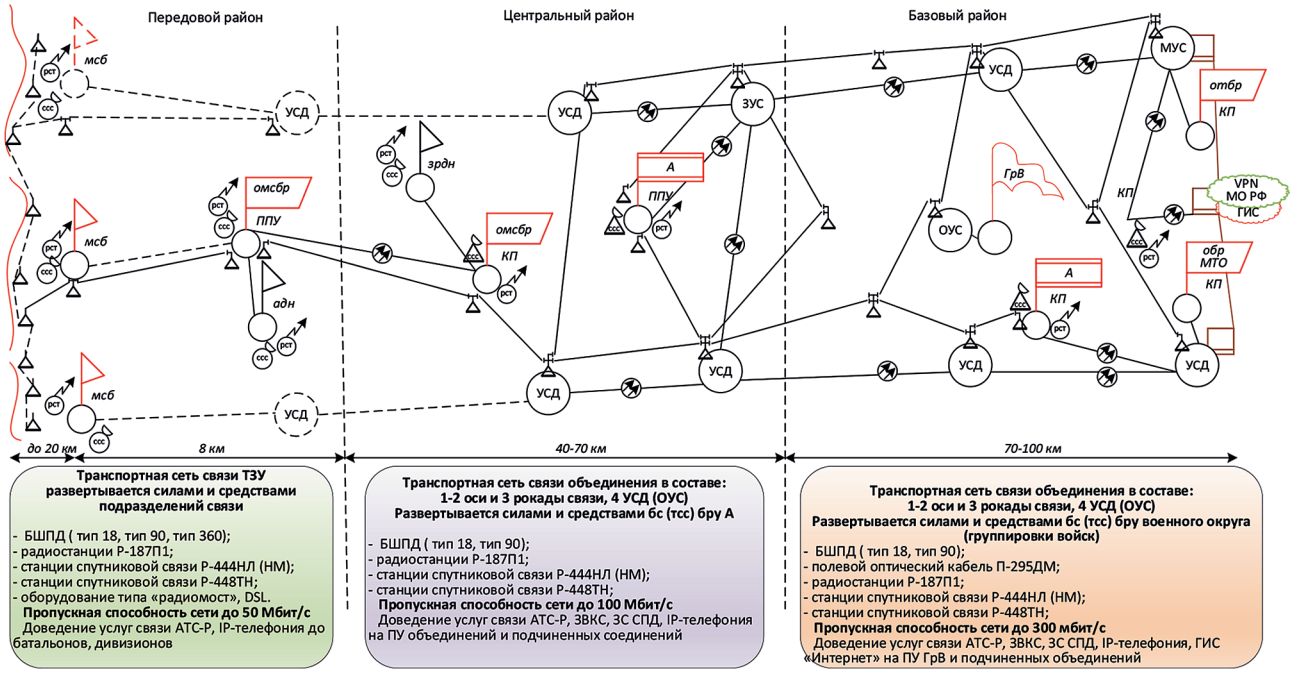


Рис. 1. Вариант построения транспортной сети связи в районах, не оборудованных в отношении связи

средств огневого поражения (в том числе и FPV), поэтому в целях увеличения мобильности, разведывательной защищенности и живучести элементов системы связи, для наращивания ТрСС предлагается применять средства беспроводной широкополосной передачи данных (БШПД) штатные (Р-425) и двойного назначения (InfiNet), с последующим проключением на узлы связи пунктов управления потоков Ethernet и организацией VPN-туннелей [4, 5, 6].

Основная часть

Оборудование БШПД (табл. 1) позволяет строить надёжные масштабируемые и самоорганизующиеся транспортные сети в тактическом и оперативном звене управления, в условиях, где прокладка проводных линий затруднена или экономически нецелесообразна [3, 5].

Особенностью организации связи с помощью средств БШПД является то, что для передачи данных в них используется собственный

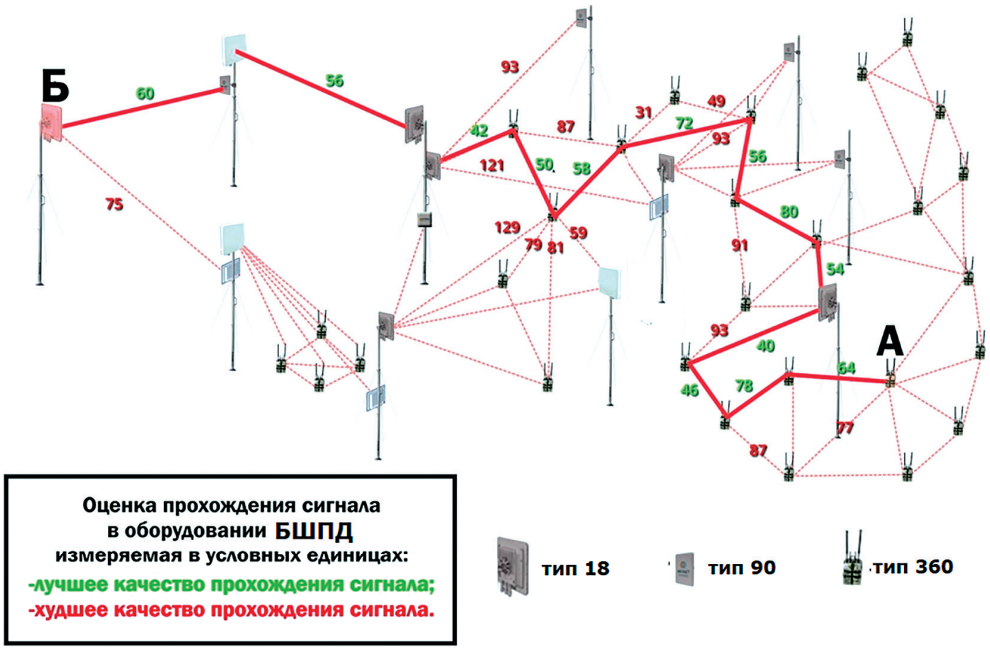
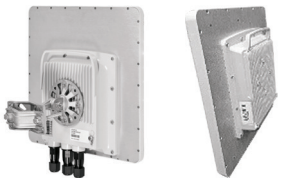


Рис. 2. Построение оптимального маршрута передачи данных протоколом MINT

Таблица 1.

Состав и тактико-технические характеристики оборудования БШПД

Наименование	БШПД тип 18	БШПД тип 90	БШПД тип 360
Внешний вид			
Описание	Абонентский терминал со встроенной двухполяризационной антенной	Базовая станция высокой производительности со встроенной двухполяризационной антенной	Абонентский терминал с двумя антеннами круговой диаграммой направленности
Режим работы	«точка-точка» «точка-многоточка» MESH	«точка-точка» «точка-многоточка» MESH	«точка-точка» «точка-многоточка» MESH
Усиление антенны	18 дБ	16 дБ	8 дБ
Ширина диаграммы направленности	18×18 град	90×8 град	360°
Проводные интерфейсы	1 x Gigabit Ethernet (10/100/1000 Base-T) разъем RJ-45	1x Gigabit Ethernet (10/100/1000 Base-T) разъем RJ-45, 1x SFP, 1x SYNC	1 x Gigabit Ethernet (10/100/1000 Base-T) разъем RJ-45, USB type A, разъем питания LP20
Габариты	188×188×45 мм	371×371×90 мм	495×210м45 мм
Вес	1,3 кг	4,4 кг	5 кг
Пропускная способность	до 670 Мбит/с	до 800 Мбит/с	до 390 Мбит/с
Дальность связи	до 10 км	до 15 км	до 5 км
Ширина полосы	10,20,40,80 МГц		
Диапазон частот	4900–6050 МГц		
Потребляемая мощность	до 15 Вт	до 20Вт	до 15 Вт
Электропитание	PoE 802.3at ±43..56 В	PoE 802.3at ±43...56 В	АКБ DC ±12...19 В
Автономность	–		6–8 ч

протокол канального уровня «MINT» – Mesh Interconnection Network Technology, обозначая этим технологию построения самоорганизующихся широкополосных сетей связи [6]. Протокол просчитывает маршруты и выбирает из них самый оптимальный, делает это постоянно по мере изменения условий в сети и её топологии, что особо актуально в условиях воздействия средств радиоэлектронного подавления противника, а также в случаях вывода из строя оборудования (рис. 2).

Переход на другой маршрут происходит при ухудшении качества связи (падении уровня сигнала более чем на 30 %) – абонентская станция переключается на другую базовую станцию без прерывания передачи данных. Каждый узел самостоятельно рассчитывает качество соединения со своими «соседями» и качество передачи пакетов до каждого узла сети, поэтому, прямой и обратный путь между двумя узлами могут не совпадать. Более того, даже «соседи», имеющие непосредственную связь друг с другом, для реальной передачи данных могут выбрать не прямой путь, а через промежуточный узел (узлы), если при этом скорость и надёжность доставки пакетов окажется выше. В отличие от классической схемы построения связи «звезда» с центральным узлом, здесь нет единой точки отказа: если один узел выходит из строя, трафик автоматически перенаправляется по другим маршрутам.

Кроме того, для повышения помехоустойчивости сети связи в средствах БШПД используется технология DFS (Dynamic Frequency Selection,

динамический выбор частоты), где устройства во время настройки сканируют доступные частотные каналы, а в дальнейшем автоматически переключается между ранее записанными частотными каналами в зависимости от уровня помех [7, 8].

Основной задачей комплекса устройств БШПД в тактическом звене управления является организация широкополосной сети доступа к среде передачи данных с возможностью предоставления ГИС «Интернет» или открытого сегмента передачи данных Министерства обороны Российской Федерации (ОС ПД МО РФ) с целью информационного взаимодействия подразделений, а также резервирования ВОЛС.

На сегодняшний день для обмена текстовой, графической и видео информацией в режиме реального времени применяются программно-технические средства (ПТС) межвидовой системы информационного обмена (МСИО) [9], основу которых составляют ноутбуки, планшеты и смартфоны со специальным программным обеспечением, позволяющие производить расчеты, наносить обстановку на загруженные в эти устройства электронную карту, передавать текстовую, графическую информацию, а также осуществлять вывод видеосигнала с БПЛА в различных звеньях управления.

Также в группировках войск в целях сокращения времени передачи данных и согласованного взаимодействия силами и средствами поражения на объекты (цели) противника, сокращения времени сбора информации, ее обработки и принятия решений на применение войск, пунктом управления связи группировки войск, разработаны другие системы информационного взаимодействия (например «Эльбрус», «Черепаха» и др). В состав данных систем входит специальное программное обеспечение необходимое специалистам РВиА, ПВО, беспилотных систем, разведки, связи и т.д. Широкий спектр СПО делает устройство универсальным для применения общевойсковыми подразделениями родов войск и специальных войск и организации взаимодействия между ними при решении боевых задач [9].

В звене взвод-рота-батальон для встречной работы с устройствами на базе СПО МСИО предлагается использовать носимый вариант исполнения БШПД тип-360 с всенаправленной антенной, а также встроенным модулем Wi-Fi.

В тактическом звене управления БШПД тип-360 образует самоорганизующиеся широкополосные транспортные сети по технологии децентрализованных Mesh-сетей со скоростью передачи данных до 12 Мбит/с на расстоянии до 5 километров между соседними изделиями (рис. 3).

Так же с помощью БШПД возможно организовывать каналы управления наземными робототехническими комплексами (НРТК) и трансляцию видео с беспилотных летательных аппаратов (БПЛА) (рис. 4).

В мотострелковом батальоне и им равным с помощью базовых станций высокой производительности БШПД тип-18 специалистами связи роты управления мсп (тп) развертываются «зоны засветки» для Mesh-сетей нижестоящих подразделений (рот, взводов, расчетов БПЛА). Из расчета на одну БШПД тип-90 до десяти БШПД тип-360 (рис. 5).

От КНП мсб (тб) в направлении ПУ (КП, ППУ) мсп (тп) с помощью абонентских терминалов БШПД тип-18 развертываются линии связи привязки мобильных элементов боевого порядка в режиме функционирования «точка-много точка» (на одну БШПД тип-90 до десяти БШПД тип-18).

Рис. 3. Mesh-сеть в тактическом звене управления

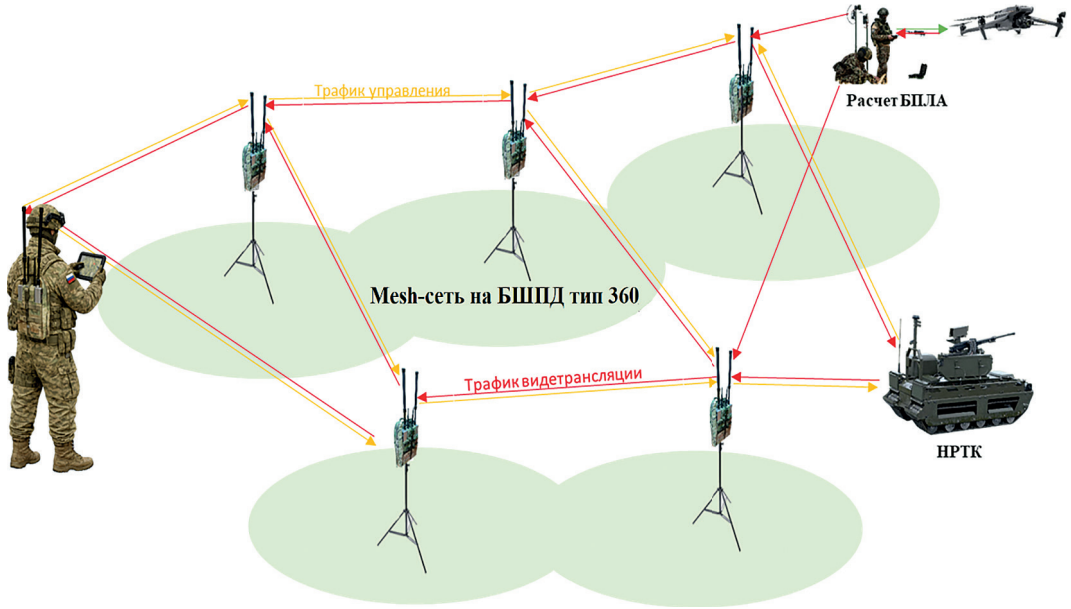


Рис. 4. Схема Mesh-сети на БШПД для управления НРТК и трансляции видео с БПЛА

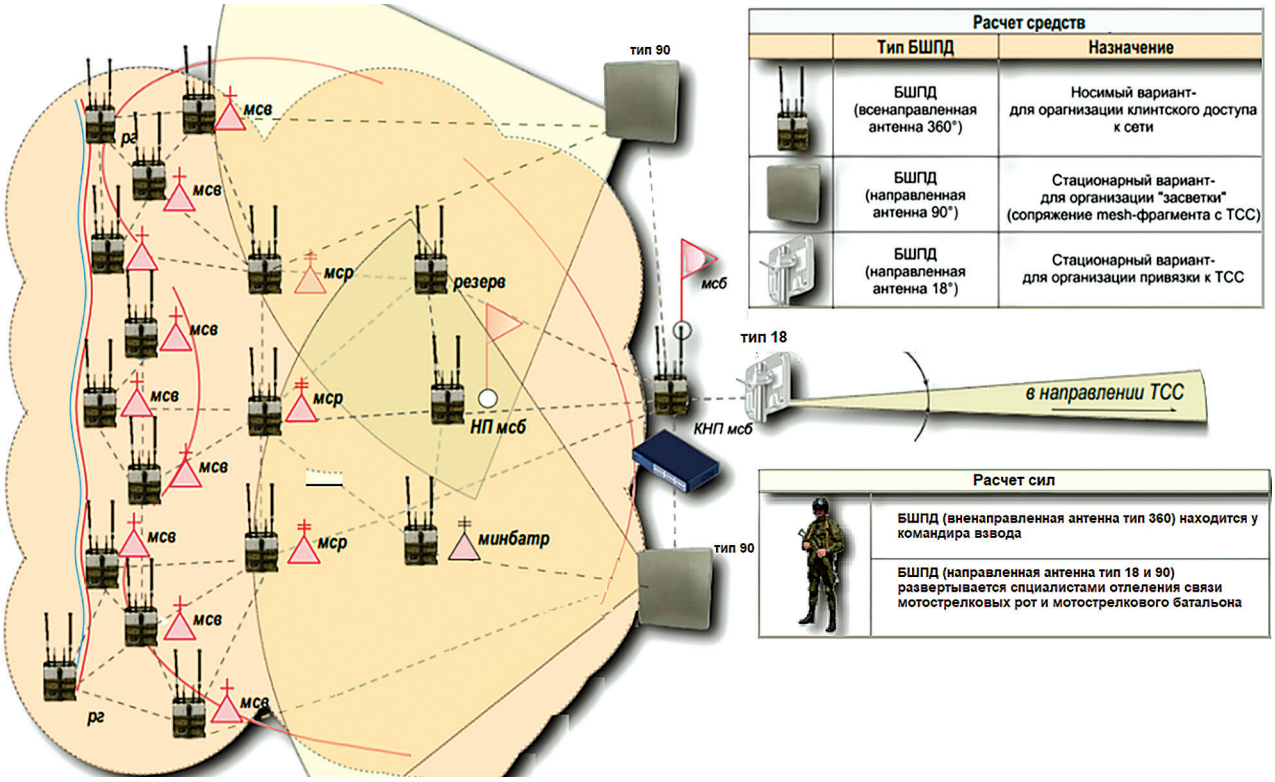


Рис. 5. Вариант использования БШПД в МСБ

Привязка узлов связи пунктов управления соединений, воинских частей и подразделений ТЗУ к ТрСС группировки войск обеспечивается с использованием каналов Ethernet с пропускной способностью до 1 Гбит/с (с наращиванием до 10 Гбит/с), организованных путем развертывания собственных ВОЛС, а в дальнейшем волоконно-оптических сетях связи операторов связи через развернутые в зоне ответственности группировки войск узлы доступа и зоновые узлы агрегации.

Для проверки функциональных возможностей комплекса оборудования БШПД проведена апробация в опытном районе (рис. 6).

По результатам апробации установлено, что комплекс оборудования БШПД обеспечивает

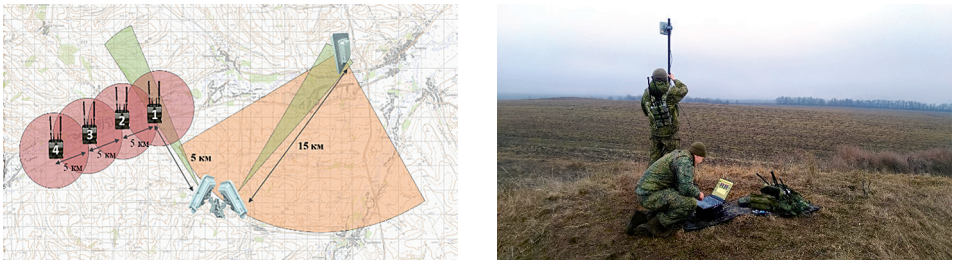


Рис. 6. Один из вариантов апробации в опытном районе средств БШПД

функционирование в тактическом звене управления самоорганизующейся высокоскоростной широкополосной сети связи по технологии децентрализованных Mesh-сетей с возможностями:

- подключения к узлу доступа БШПД тип-90 не более 10 абонентских станций БШПД тип-360 в составе одного сегмента Mesh-сети (рис. 7);
- объединения в единую сеть неограниченного количества подключаемых сегментов Mesh-сетей;
- минимальной пропускной способностью на одного абонента – 2 Мбит/с;
- обеспечения связи с подвижными абонентами при наличии сплошной зоны радиопокрытия;
- наращивания сети связи при перемещении (как пример: наращивание сети связи при ведении наступательных боевых действий подразделений путем использования носимых комплектов и направленных антенн);
- поддержание неразрывного функционирования Mesh-сетей различной конфигурации (линейной, древовидной, ячеистой);
- обеспечение соединения вновь подключаемых узлов доступа или ретрансляторов к Mesh-сети за время не более 30 сек;
- восстановления в минимальные сроки переключения на другое соединение с возможностью обеспечения работы приложений верхнего уровня;
- обеспечения информационной пропускной способности в Mesh -сети при различных значениях ширины полосы частот:
  - для 20 МГЦ – не менее 8 Мбит/с;
  - для 40 МГц – не менее 12 Мбит/с.
- обеспечение автоподстройки мощности передатчиков, скорости обмена между узлами доступа и ретрансляторов;
- обеспечения по команде оператора одновременного перехода изделий в сети на подготовленные частоты с учетом заложенных конфигурационных данных.

Также в ходе апробации проверялась работа функциональных возможностей комплекса оборудования БШПД в режиме TDMA (точка-точка, точка-многоточка) в результате чего были установлены следующие возможности:

- подключение к узлу доступа БШПД тип-90 не более 10 абонентских станций БШПД тип-18 (в режиме точка-многоточка);
- пропускная способность не более 200 Мбит/с между двумя абонентскими терминалами

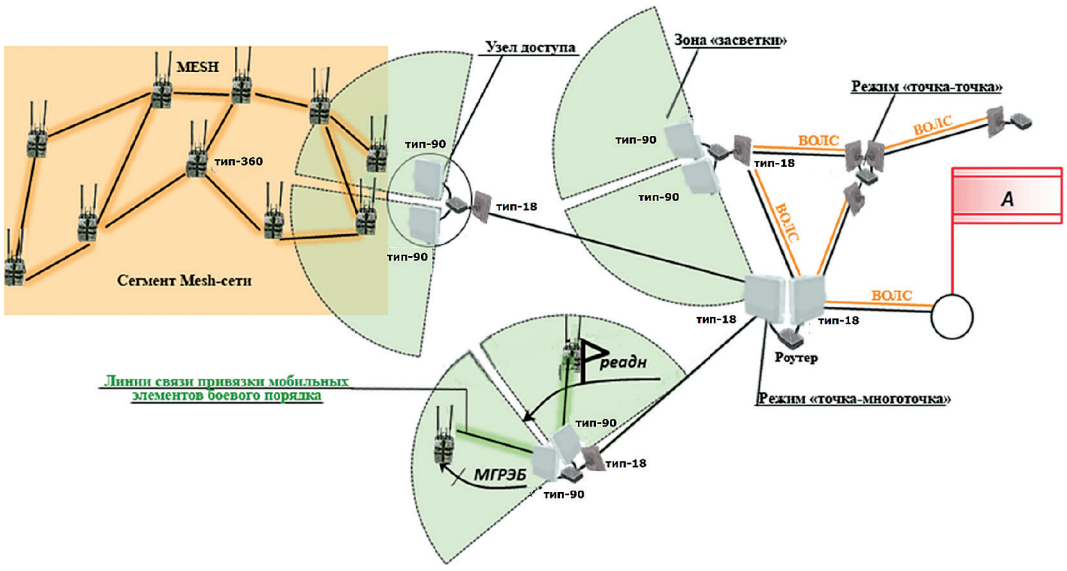


Рис. 7. Вариант применения БШПД

БШПД тип-18 (в режиме точка-точка) на расстоянии 15 км при условии прямой видимости;

- на БШПД тип-360 скорость передачи данных через встроенный Wi-Fi модуль максимально достигала 15 Мб/с в независимости от расстояния.

В условиях боевых действий, а также динамического изменения обстановки, постоянного продвижения войск и работе различных комплексов РЭБ требуется оперативное развертывание точек доступа к сетям передачи данных. Как правило из-за практически уничтоженной инфраструктуры и сложного рельефа не всегда возможна стационарная установка оборудования на мачты или высотные сооружения. Кроме того, при резком изменении обстановки на фронте нецелесообразно развертывать долговременные точки доступа, так как их монтаж требует подготовленного места, промышленного, аварийного и резервного электропитания, а также обслуживания.

Размещение устройств БШПД тип-18 и тип-90 на БПЛА позволяет поднять оборудование на необходимую высоту без использования мачт или занятия господствующих высот. При этом обеспечивается оперативное развёртывание точек доступа в заданной точке без привязки к стационарным конструкциям.

Устройства БШПД могут устанавливаются на грузовую платформу БПЛА одиночно или совместно (если позволяет грузоподъемность БПЛА), в зависимости от поставленной задачи и условий местности.

Первым вариантом является одиночная установка БШПД на БПЛА для расширения зоны покрытия стационарной базовой станции в условиях сложного рельефа или работы средств РЭБ (рис. 8). Устройство одновременно обменивается данными со стационарно установленной базовой станцией, размещённой на узле связи (КНП, КП) и является точкой доступа для БШПД тип-360, находящихся в ее секторе покрытия.

Этот вариант наиболее эффективен при построении сети по схеме «Mesh», так как в зависимости от рельефа местности, уровня шумов и качества сигналов БШПД тип-360 сможет работать как напрямую с базовой станцией, так и через точку доступа на БПЛА, что повышает устойчивость и надежность связи.

Второй вариант, установка на БПЛА БШПД тип-360 (рис. 9), не показал значительного улучшения характеристик устойчивости и дальности связи. Связанно это с небольшой мощностью передатчика, а также высоким уровнем электромагнитных шумов в приемном тракте устройства, за счёт собственных шумов, наводок от бортовой аппаратуры БПЛА и внешних помех, принимаемых всенаправленной антенной.

Третьим вариантом является комбинация установки на БПЛА БШПД тип-18 и тип-90 для увеличения дальности подключения к ГИС «Интернет» или ОС ПД МО РФ и увеличения зоны покрытия (рис. 10).

Оба устройства соединяются между собой кабелем Ethernet.

Схема работает следующим образом:

- базовая станция, размещенная на узле связи доступа (КНП, ПУ) подключена к сети ОС ПД МО РФ или ГИС «Интернет»;
- посредством радиоканала БШПД тип-18, установленное на БПЛА устанавливает связь с базовой станцией;

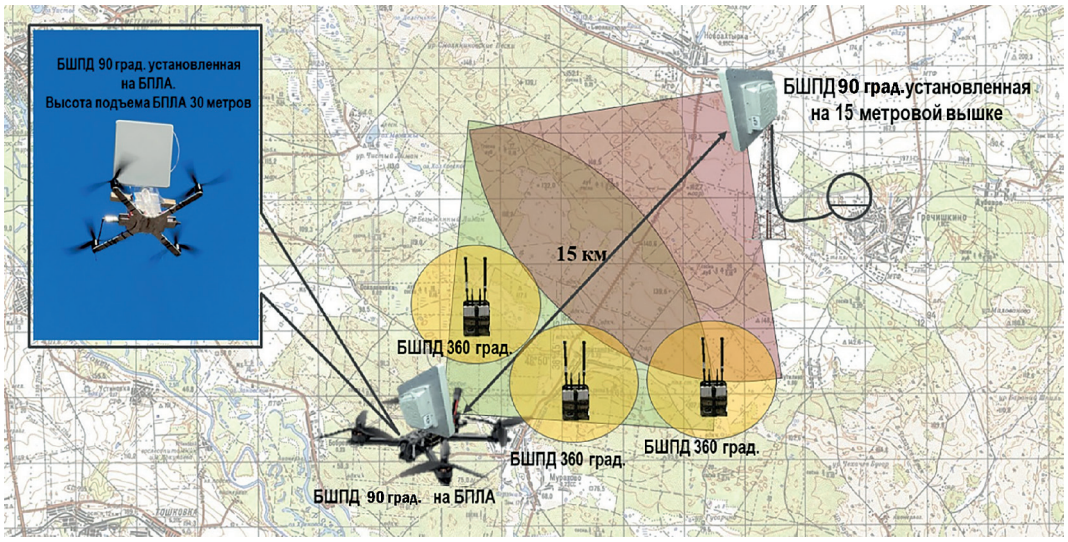


Рис. 8. Применение БШПД тип-90 с БПЛА для расширения зоны покрытия стационарной базовой станции в условиях сложного рельефа или работы средств РЭБ

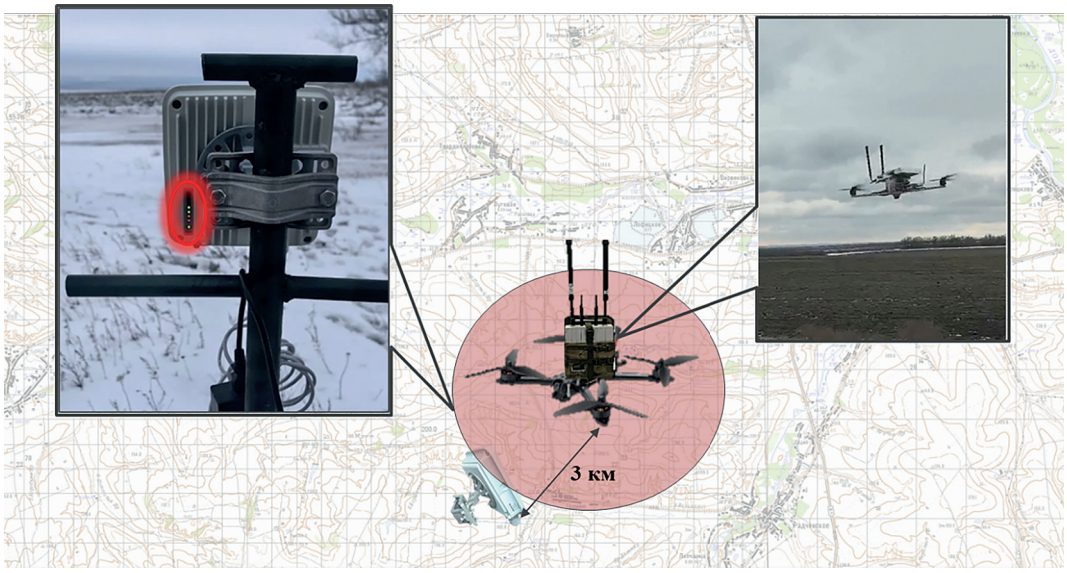


Рис. 9. БПЛА с установленным на нем устройством БШПД тип-360

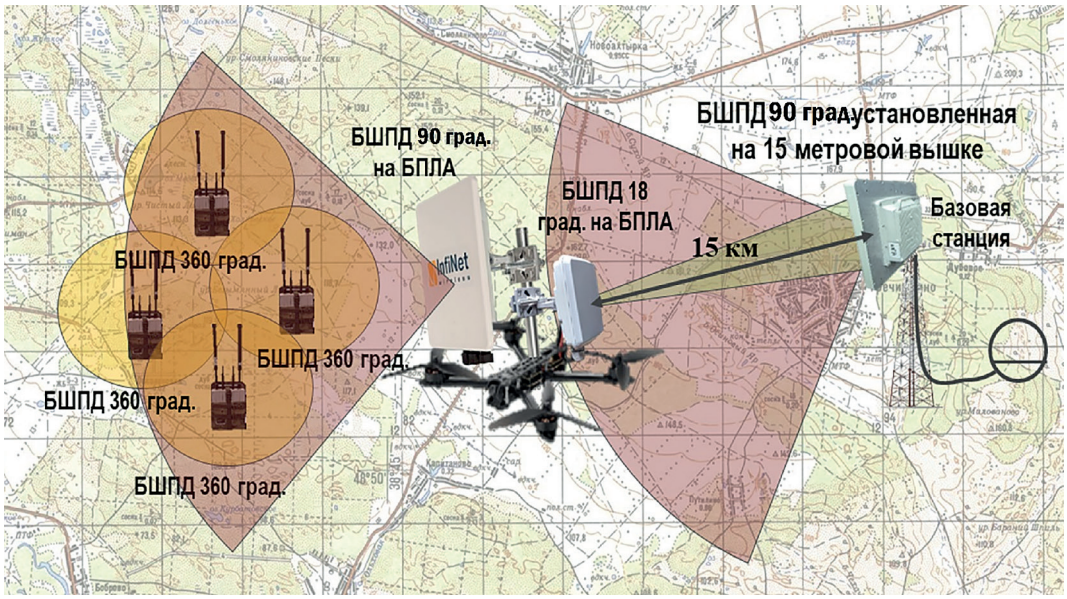


Рис. 10. Способ увеличения дальности и зоны покрытия при применении комплекса устройств БШПД тип-18 и тип-90

- по кабелю Ethernet осуществляется подключение БШПД тип-90, к общей сети базовой станции и БШПД тип-18;
- БШПД тип-90 выступает в качестве точки доступа для нескольких БШПД тип-360, объединённых в сеть типа Mesh или «точка-многоточка».

Установка устройств БШПД тип-18, тип-90 на беспилотные летательные аппараты даёт ряд существенных преимуществ – особенно в условиях, когда традиционная инфраструктура связи недоступна или повреждена.

Главный положительный эффект – возможность быстро развернуть сети передачи данных с доступом к ОС ПД МО РФ или ГИС «Интернет» в необходимых местах. Не требуется прокладки кабелей или строительства стационарных вышек.

Еще один важный положительный эффект – это мобильность и гибкость применения. БПЛА с устройствами БШПД легко переместить в любую точку зоны покрытия. Можно оперативно изменить высоту подвеса (обычно 20–100 м), чтобы улучшить зону покрытия или обойти препятствия. Оптимально подходит для выполнения временных задач и операций. За счёт мобильности и возможности быстрого манёвра повышается живучесть сети.

Таким образом, применение устройств БШПД тип-18, тип-90 установленных на БПЛА позволяет оперативно увеличивать зоны покрытия. Подъём оборудования на высоту позволяет преодолеть препятствия: здания, лес, холмы, сложный рельеф. Один БПЛА с оборудованием может служить ретранслятором для других БПЛА или наземных устройств. Возможно построение Mesh сетей между несколькими БПЛА – это расширяет зону покрытия и повышает устойчивость связи. Немаловажно, что при использовании устройств БШПД совместно с БПЛА снижает риск для личного состава, так как не требуется установка оборудования в опасных зонах.

В оперативном звене управления основным способом применения комплекса БШПД тип-18, тип-90 является развертывание линий связи опорной сети (оси, рокады) и линий связи привязки узлов связи пунктов управления и узлов доступа в режиме функционирования «точка-точка» (рис. 11).

Основными задачами боевого применения оборудования БШПД в оперативном звене управления является [1,2]:

- построение линий радиодоступа по топологии «точка-точка», «точка-многоточка» для привязки абонентов к стационарной опорной сети связи, узлам связи стационарной сети связи операторов с использованием направленных (секторных) антенн на дальностях до 30 км;
- построение высокоскоростной широкополосной полевой опорной сети связи (транспортной сети связи) различной конфигурации (вариации одно - и многокольцевой, многосвязной структур) в интересах группировки войск;
- организация высокоскоростных каналов управления и видеотрансляции с помощью беспилотных средств наземного, морского и воздушного исполнения;
- замена радиорелейных станций в районах повышенного применения противником БПЛА;
- резервирование проводных и ВОЛС.

Вывод

В качестве основных положений вывода сформулированы следующие аспекты, что использование оборудования БШПД для наращивания высокоскоростной широкополосной полевой опорной сети связи (транспортной сети) в тактическом и оперативном звене управления позволяет создать надёжную, масштабируемую и отказоустойчивую инфраструктуру различной конфигурации, предназначенной для предоставления доступа к среде передачи данных с возможностью выхода в ГИС «Интернет» или ОС ПД МО РФ. Технологии MINT и DFS обеспечивают высокое качество связи даже в сложных условиях. Преимуществами использования Mesh сетей в ТЗУ, ОЗУ является:

1. Высокая живучесть и отказоустойчивость сетей за счет динамической переконфигурации и возможности к самовосстановлению. Благодаря множественным резервным путям передачи данных выход из строя отдельных узлов не приводит к коллапсу сети. В боевых условиях это критично: даже при подавлении или уничтожении части оборудования связь сохраняется. Также Mesh-сети автоматически: обнаруживают новые узлы, перестраивают маршруты, оптимизируют пути передачи данных. Это позволяет быстро развёртывать

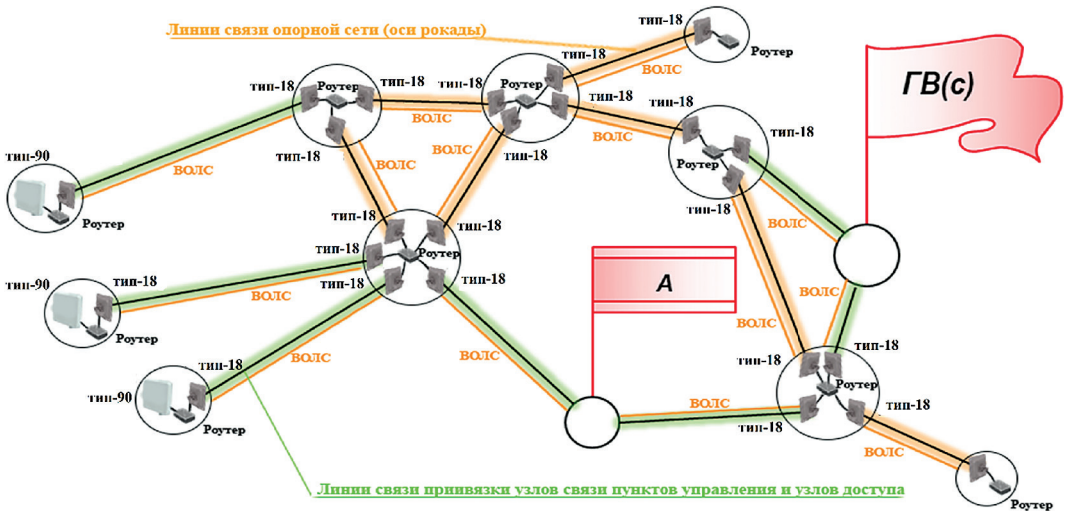


Рис. 11. Вариант использования БШПД в ОЗУ

связь на местности без дополнительных настроек – достаточно включить устройства, и они сами «найдут» друг друга.
2. Непрерывность обеспечения предоставления широкополосных мультисервисных услуг связи как стационарным, так и подвижным абонентам. Сеть можно развернуть: стационарно (на командных пунктах), в движении (на технике, носимых устройствах БШПД тип-360), комбинированно (стационарные ретрансляторы + мобильные узлы).
3. Масштабируемость сети за счет увеличения количества узлов доступа, ретрансляторов и самих абонентов. Возможно добавлять новые узлы (солдаты, техника, расчеты БПЛА, посты наблюдения и др.), расширяя зону покрытия. При этом производительность сети не падает резко, как в централизованных системах.
4. Расширение зоны покрытия. Каждый узел выступает ретранслятором. Это позволяет покрывать большие территории с минимальным числом базовых станций, обеспечивать связь в сложных условиях (горы, лес, городская застройка), где прямой сигнал не проходит.
5. Распределение нагрузки. Трафик распределяется между узлами, что: снижает перегрузку отдельных каналов, повышает общую пропускную способность, уменьшает задержки для критически важных данных.

Литература

1. Иванов В. Г. Основы построения и оценки эффективности функционирования системы связи специального назначения в международном вооруженном конфликте на основе многосферной и конвергентной структуры ее элементов: Монография. – СПб.: ПОЛИТЕХ, 2023. – 298 с.
2. Иванов В. Г. Теория и практика построения и обеспечения функционирования системы связи специального назначения с учётом технологического развития и опытов вооруженных конфликтов: монография – М.: Красная Звезда, 2025. – 304 с.
3. Тишков В. В., Иванов В. Г., Лукьянчик В. Н Обоснование облика построения перспективных комплексов и средств связи на основе опыта организации связи при проведении специальной военной операции // Военная мысль, 2023 г., – № 9 – С. 59–72.
4. Школьников К. Е., Иванов В. Г., Лукьянчик В. Н. Особенности развёртывания полевой системы связи общевойскового соединения на основе применения технологий самоорганизующей сети, реализованных в радиорелейных станциях Р-419 МР // Военная мысль, 2024 г. – № 5. – С. 62–74.
5. Иванов В. Г., Лукьянчик В. Н., Сухотеплый А. П. Влияние опыта СВО на развитие транспортной сети соединения на основе средств беспроводного широкополосного доступа и технологий самоорганизующихся сетей связи // Военная мысль, 2025. – № 4. – С. 78–88.
6. Стаценко Л. Г., Совкова О. И., Скварник И. С. Анализ возможностей технологий беспроводного широкополосного доступа для обеспечения безопасности мореплавания в заливе Петра Великого // Вестник инженерной школы ДВФУ, 2020. – № 3 (44). – С. 104–120.
7. Мельников М. И., Ковтун А. С. Самоорганизующаяся сеть оперативного взаимодействия для нужд населения и специальных служб // Доклады Томского государственного университета систем управления и радиоэлектроники, 2014. – № 2 (32). – С. 281–286.
8. Легков К. Е., Донченко А. А. Беспроводные mesh-сети специального назначения // T-Comm — Телекоммуникации и Транспорт, 2009. – № 2. – С. 36–42.
9. Иванов В. Г., Лукьянчик В. Н., Филин А. А., Назаров А. Д. Применение автоматизированной системы межвидового информационного обмена специального назначения в интересах управления войсками САПР и графика, 2024. – № 3 (331). – С. 56–61.

USE OF WIRELESS BROADBAND ACCESS IN THE TRANSPORT COMMUNICATION NETWORK OF THE GROUPING OF TROOPS

Ivanov V. G.[5], Kvitka D. V.[6], Petrov I. A.[7], Bashirov S. Yu.[8]

Keywords: *communication system, access, protocol, access node, core network, repeater, self-organizing communication network, Mesh network, wireless broadband access.*

5 ***Vasily G. Ivanov***, Doctor of Military Sciences, Associate Professor, Professor of the Department (Informatics and Computer Engineering) of the Faculty (Engineering), Academy of Civil Protection of the Ministry of the Russian Federation for Civil Defense, Emergencies and Elimination of Consequences of Natural Disasters named after Lieutenant General D. I. Mikhailik. Khimki, Russia. E-mail: v.ivanov@agz.50.mchs.gov.ru

6 ***Dmitry V. Kvitka***, Chief of Communications – Deputy Chief of Staff of the Moscow Military District. St. Petersburg, Russia. E-mail: wasj2006@yandex.ru

7 ***Igor A. Petrov***, Chief of Communications - Deputy Chief of Staff of the Moscow Military District. St. Petersburg, Russia. E-mail: petrovigor28@yandex.ru

8 ***Sergey Yu. Bashirov***, Deputy Head of the Department of the Main Directorate of Communications of the Armed Forces of the Russian Federation. Moscow, Russia. E-mail: S.bashirov81@yandex.ru

Abstract

The purpose of the work: *based on the experience of using wireless broadband access tools during a special military operation, the options for their use in order to improve the efficiency of the transport communication network of the group of troops are considered*

Research method: *general theory of systems, theory of military communications, theory of open systems using the methods of system analysis. The reliability of the results is ensured by the practical implementation of the methods of using wireless broadband access in communication systems of various levels of control.*

Results of the study: *the analysis of the results of the practical application of wireless broadband access tools as a means of a transport communication network and for the organization of control channels for ground-based robotic systems and video broadcasting from unmanned aerial vehicles is carried out. Introduction of wireless broadband access equipment to expand the high-speed transport network in the tactical and operational control links allows you to create a reliable, scalable and fault-tolerant infrastructure of various configurations*

The scientific novelty *consists in the development of substantiated directions for improving the efficiency of the functioning of the transport communication network of the group of troops based on the use of wireless broadband access.*

References

1. Ivanov V. G. Osnovy postroeniya i ocenki ehffektivnosti funkcionirovaniya sistemy svyazi special'nogo naznacheniya v mezhdunarodnom vooruzhennom konflikte na osnove mnogosfernoj i konvergentnoj struktury ee ehlementov: Monografiya. – SPb.: POLITEH, 2023. – 298 p.
2. Ivanov V. G. Teoriya i praktika postroeniya i obespecheniya funkcionirovaniya sistemy svyazi special'nogo naznacheniya s uchyotom tehnologicheskogo razvitiya i opytov vooruzhennyh konfliktov: monografiya – M.: Krasnaya Zvezda, 2025. – 304 p.
3. Tishkov V. V., Ivanov V. G., Luk'yanchik V. N. Obosnovanie oblika postroeniya perspektivnyh kompleksov i sredstv svyazi na osnove opyta organizacii svyazi pri provedenii special'noj voennoj operacii // Voennaya mysl', 2023. – No 9. – Pp. 59–72.
4. Shkol'nikov K. E., Ivanov V. G., Luk'yanchik V. N. Osobennosti razvyortyvaniya polevoj sistemy svyazi obshchevojskovogo soedineniya na osnove primeneniya tehnologij samoorganizuyushchej seti, realizovannyh v radiorelejnyh stanciyah R-419 MR // Voennaya mysl', 2024. – No 5. – Pp. 62–74.
5. Ivanov V. G., Luk'yanchik V. N., Suhoteplyj A. P. Vliyanie opyta SVO na razvitie transportnoj seti soedineniya na osnove sredstv besprovodnogo shirokopolosnogo dostupa i tehnologij samoorganizuyushchihsya setej svyazi // Voennaya mysl', 2025. – No 4. – Pp. 78–88.
6. Stacenko L. G., Sovkova O. I., Skvarnik I. S. Analiz vozmozhnostej tehnologij besprovodnogo shirokopolosnogo dostupa dlya obespecheniya bezopasnosti moreplavaniya v zalive Petra Velikogo // Vestnik inzhenernoj shkoly DVFU, 2020. – No 3 (44). – S. 104–120.
7. Mel'nikov M. I., Kovtun A. S. Samoorganizuyushchayasya set' operativnogo vzaimodejstviya dlya nuzhd naseleniya i special'nyh sluzhb // Doklady Tomskogo gosudarstvennogo universiteta sistem upravleniya i radioehlektroniki, 2014. – No 2 (32). – Pp. 281–286.
8. Legkov K. E., Donchenko A. A. Besprovodnye mesh-seti special'nogo naznacheniya // T-Comm — Telekommunikacii i Transport, 2009. – No 2. – Pp. 36–42.
9. Ivanov V. G., Luk'yanchik V. N., Filin A. A., Nazarov A. D. Primenenie avtomatizirovannoj sistemy mezhvidovogo informacionnogo obmena special'nogo naznacheniya v interesah upravleniya vojskami SAPR i grafika, 2024. – No 3 (331). – S. 56–61.

ЗАЩИТА ОТ СОСТЯЗАТЕЛЬНЫХ АТАК НЕЙРОСЕТЕЙ СИСТЕМЫ УПРАВЛЕНИЯ РОБОТОТЕХНИЧЕСКИМИ КОМПЛЕКСАМИ НА ОСНОВЕ МАРКОВСКИХ ПРОЦЕССОВ

Сацута А. И.[1], Липатников В. А.[2]

DOI:10.21681/3034-4050-2026-4-13-24

Ключевые слова: *безопасность искусственного интеллекта, защита моделей машинного обучения, состязательное обучение, компьютерное зрение, распознавание объектов, системы управления роботизированными комплексами.*

Аннотация

Цель работы: *состоит в анализе уязвимостей нейросетевых моделей систем управления робототехническими комплексами к состязательным воздействиям и разработке способа повышения их защиты на основе методов обучения с подкреплением.*

Метод исследования: *подход, основанный на формализации процесса генерации состязательных примеров как задачи Марковского процесса принятия решений.*

Результаты исследования: *разработан агент, адаптивно генерирующий состязательные примеры путем учета состояния среды и характеристик модели. Предложен способ обучения агента генерации состязательных примеров с последующим их использованием в состязательном обучении. Состояние агента формируется на основе карт признаков модели, градиентной информации и величины искажения входных данных, оцениваемой по норме l2. Действия агента соответствуют выбору параметров атаки типа PGD. Функция награды учитывает как снижение качества детекции, так и ограничение на уровень вносимых искажений.*

Научная новизна: *предложена новая функция награды, учитывающая одновременно качество детекции и величину искажения, что обеспечивает баланс между эффективностью атаки и её незаметностью.*

Введение

В условиях растущей нагрузки на наземные сети связи требуется внедрение новых решений для обеспечения стабильного и качественного обслуживания пользователей. Одним из перспективных подходов является применение робототехнических комплексов, которые могут оперативно развертываться в районах с высокой плотностью пользователей или при чрезвычайных ситуациях. Актуальной является задача повышения защиты нейронных сетей систем управления робототехническими комплексами от состязательных атак.

Современные системы управления робототехническими комплексами (СУ РТК), основанные на методах компьютерного зрения, играют ключевую роль в широком спектре прикладных задач, включая мониторинг окружающей среды, автономную навигацию, принятие решений в реальном времени и распознавание объектов, в том числе объектов, создающих непосредственную угрозу для таких РТК. Такие системы активно применяются в гражданских и военных областях, а также в задачах повышенной ответственности, включая транспортные системы, охранные комплексы и военные приложения. Центральным элементом СУ РТК являются нейросетевые модели, в частности, глубокие сверточные нейронные сети, обеспечивающие детекцию и классификацию объектов в стандартных условиях эксплуатации [1, 2, 3].

Данные нейросетевые модели, как элемент СУ РТК, обладают различными уязвимостями, реализуемые посредством воздействия на пакеты данных в сети передачи данных (СПД) или посредством воздействия на оптические элементы системы управления. Рассматриваемая поверхность атаки дополняется уязвимостью НС моделей к состязательным атакам (СА). Данный тип атак представляют из себя специально сконструированные возмущения входных данных. Такие возмущения способны приводить к искажениям предсказаний моделей. Данные возмущения называются состязательными, а итоговые примеры, полученные с их помощью, называются состязательными примерами. Состязательные атаки приводят к ошибкам классификации и распознавания объектов что критично для систем, функционирующих без участия оператора РТК в автономном режиме [1, 4, 5].

1 ***Сацута Анатолий Игоревич***, старший оператор научной роты военной академии связи им. Маршала Советского Союза С. М. Буденного, г. Санкт-Петербург, Россия. E-mail: toha.satzuta@yandex.ru

2 ***Липатников Валерий Алексеевич***, доктор технических наук, профессор, старший научный сотрудник научно-исследовательского центра Военной академии связи им. Маршала Советского Союза С. М. Буденного, Санкт-Петербург. E-mail: lipatnikovanl@mail.ru

Для СУ РТК проблема устойчивости НС к состязательным воздействиям [6], пример которых представлен на рисунке 1, имеет особое значение, так как ошибки в восприятии окружающей среды напрямую влияют на корректность анализа обстановки и управления. Кроме того, в реальных условиях эксплуатации входные данные подвержены не только преднамеренным атакам, но и различным видам естественного шума, который создаётся посредством изменения освещения, погодных условий и другими физическими эффектами [7].

Существующие методы защиты от СА, одним из которых является состязательное обучение [8], демонстрируют определенную эффективность. Однако такие методы обладают рядом существенных ограничений [9]. В большинстве случаев они используют фиксированные алгоритмы генерации атак, так, например, методы состязательного обучения могут использовать Projected Gradient Descent (PGD). Это приводит к ограниченному разнообразию генерируемых состязательных примеров и, как следствие, к недостаточной обобщающей способности моделей в условиях более сложных или адаптивных атак. Кроме того, статический характер параметров атак не позволяет учитывать текущее состояние модели, динамику обучения и особенности входных данных [1, 5].

В связи с этим актуальной является задача разработки адаптивных методов генерации состязательных возмущений. Одним из перспективных направлений решения данной задачи является использование методов обучения с подкреплением, на примере Марковского процесса принятия решений (MDP). Данный метод позволяет формализовать процесс генерации атак как последовательное принятие решений в условиях неопределенности [10].

В данной работе предлагается подход, основанный на формализации процесса генерации состязательных примеров в виде Марковского процесса принятия решений для последующего их использования в состязательном обучении НС модели распознавания объектов. В рамках предложенной модели агент, адаптивно генерирующий состязательные примеры, обучается выбирать параметры атаки уклонения (атаки). При выборе параметров атаки он опирается на текущее состояние среды, включающее характеристики входных данных и реакцию нейросетевой модели. В качестве базового алгоритма для генерации таких примеров был выбран алгоритм PGD, параметры которого будут оптимизироваться.

Такая постановка задачи позволяет реализовать адаптивную стратегию генерации атак, направленную на максимальное ухудшение качества предсказаний модели при сохранении ограничений на величину возмущений.

Пусть задана модель $f(x)$, где x – входное изображение. Требуется найти такое возмущение δ (формула 1) так, что одновременно выполняются условия ухудшения качества предсказания модели и ограничения на допустимую величину искажения входного сигнала.

Формально задача генерации необходимого состязательного возмущения может быть записана как задача условной оптимизации:

$$\delta^* = \arg\max_{\|\delta\| \le \epsilon} L(f(x+\delta), y), \quad (1)$$

где $L(\cdot)$ – функция потерь модели детекции, y – истинные аннотации объектов, а ограничение $\|\delta\| \le \epsilon$ обеспечивает малую визуальную заметность возмущений и сохранение семантической структуры изображения.

Предлагаемый подход обеспечивает более гибкое и разнообразное пространство атак по сравнению с традиционными методами, а, следовательно, более разнообразные состязательные выборки для обучения. Разнообразные тренировочные выборки приводят к повышению обобщающей способности НС моделей при состязательном обучении. Это делает такие модели более устойчивыми.

Использование MDP позволяет учитывать долгосрочные эффекты последовательных действий агента, что является важным фактором при генерации сложных многошаговых атак [10, 11].

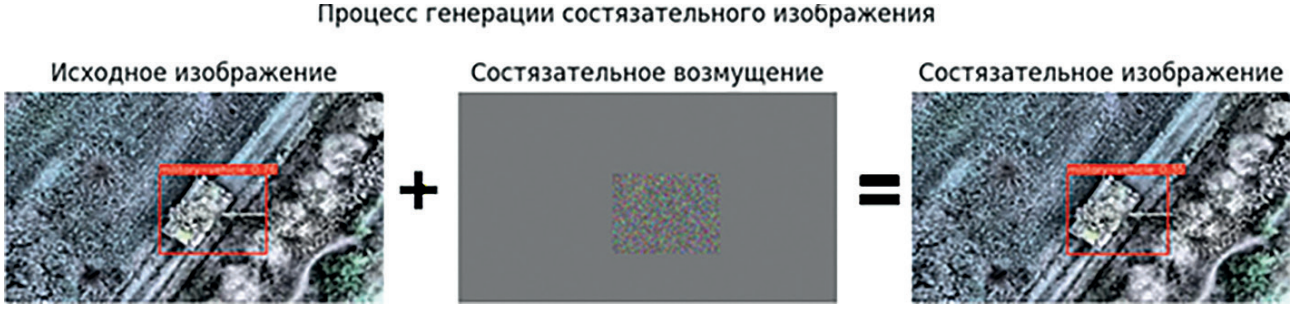


Рис. 1. Уязвимость нейросетевой модели распознавания объектов к состязательным атакам

Достижение поставленной цели по разработке способа и его реализации, в частности путём создания агента Марковского процесса принятия решений, требует выполнения следующих частных задач:

1. Формализация, обоснование и реализация пространства состояний и действий в составе среды агента Марковского процесса принятия решений.
2. Формализация, обоснование и реализация функции наград Марковского процесса принятия решений.
3. Определение подходящего алгоритма обучения агента, его обучение.
4. Выбор метрик для анализа эффективности разрабатываемого способа и агента.
5. Проведение эксперимента и анализ его результатов, сравнение предложенного способа с уже существующими альтернативами, обсуждение результатов.

Разработка агента Марковского процесса принятия решений генерации состязательных примеров

В рамках решаемой задачи генерация состязательных примеров для НС модели детекции объектов формализуется как марковский процесс принятия решений. Данная формализация позволяет рассматривать атаку не как фиксированную последовательность действий, а как последовательность действий, адаптирующихся к текущему состоянию модели и атакуемому изображению. Другими словами, такое представление обеспечивает возможность обучения агента, оптимизирующего стратегию формирования возмущений с учётом как эффективности подавления детекции, так и ограничений на величину искажения входных данных. Формально процесс задаётся кортежем: $\mathcal{MDP} = \{S, A, P, R, \gamma\}$, где S – пространство состояний, A – пространство действий, P – вероятностная функция переходов, R – функция награды, γ – коэффициент дисконтирования.

Состояние среды формируется как минимально достаточное представление информации о поведении модели детекции в текущий момент атаки и уровне внесённого возмущения. В отличие от подходов [12], основанных только на пиксельном представлении изображения, в предлагаемом пространстве состояний используется внутренние представление нейросети, что позволяет агенту учитывать семантические признаки объекта.

Состояние определяется следующим образом: $s_t = \{\|\delta_t\|_2, F_t, \nabla_x L(x_t)\} \in S$, где $\|\delta_t\|$ – l_2 норма текущего возмущения, отражающая уровень отклонения от исходного изображения и контролирующая ограничение заметности атаки, $F_t \in \mathbb{R}^{H \times W \times C}$ – карта признаков предпоследнего слоя детекции, что соответствует высокоуровневым признакам объектов, используемым детектором для принятия решений, $\nabla_x L(x_t)$ – градиент функции потерь по входному изображению, характеризующий чувствительность модели к локальным изменениям входа.

Предложенное пространство состояний позволяет агенту учитывать не только итоговый результат детекции, но и внутреннюю структуру принятия решений модели, включая области наибольшей уязвимости.

Пространство действий агента отражает процесс управления параметрами PGD-атаки. Такое пространство действий позволяет рассматривать генерацию состязательных примеров как процесс адаптивной оптимизации параметров: $a_t = \{\epsilon_t, \alpha_t\} \in A$, где ϵ_t является допустимым радиусом возмущения, ограничивающий максимальное отклонение от исходного изображения, а α_t – шаг градиентного обновления, определяющий скорость изменения изображения на каждой итерации.

Изменение изображения осуществляется с помощью проекционного градиентного спуска, вычисляемый по формуле 2.

$$x_{t+1} = \Pi_{\mathcal{P}_\epsilon(x)}(x_t + \alpha_t sign(\nabla_x L(x_t)), \quad (2)$$

где $\Pi_{\mathcal{P}_\epsilon(x)}$ обозначает проекцию на допустимое множество возмущений.

Таким образом, агент не генерирует возмущение напрямую, а управляет динамикой его формирования через параметры оптимизационного процесса.

Функция награды формализует противоречие между эффективностью атаки и её незаметностью и вычисляется по формуле 3. Такое определение награды приводит к максимизации эффекта подавления детекции при одновременном штрафе за рост искажения входного изображения. Ограниченность компонент на отрезке [0, 1] сохраняет вклад каждого компонента и предотвращает доминирование одного из критериев.

$$(r_t = (1 - \overline{C_t}) + (1 - \overline{IoU_t}) + (1 - \tanh(0{,}1 \times \|\delta_t\|_2)), \quad (3)$$

где $\overline{C_t}$ представляет собой среднюю уверенность модели в предсказаниях объектов, которые были найдены в той или иной степени, верно. В данной работе предсказание считается достаточно верным, если оно покрывает 25 % действительного объекта. Такое уточнение является важным, так как при атаке может возникать большое количество ложных детекций, в которых модель может быть сильно уверена. Большое количество ложных детекций приводит к компрометации среднего значения уверенности и не может быть использовано для обучения агента.

Показатель ($\overline{IoU_t}$) из (3) является средним значением долей правильно обнаруженных объектов, $\|\delta_t\|_2$ – является мерой величины возмущения и численно отображает, как сильно изменилось изображение. Данная мера является эквивалентом евклидовой нормы для матриц вида (Ш, В, Г). Использование гиперболического тангенса необходимо для сведения учитываемого возмущения к отрезку [0, 1], так как в отличии от других компонент функции наград оно неограниченно.

Дополнительной важной частью пространства действий, не относящейся к формализму Марковских процессов принятия решений, является локализованный характер воздействия: возмущение формируется не по всему изображению, а ограничивается областями, содержащими объекты интереса.

Такое ограничение обусловлено тем, что модели распознавания объектов принимают решение на основе признаков, сконцентрированных в пределах ограниченных пространственных регионов. Внесение возмущения в фоновые области, как правило, не приводит к существенной деградации предсказаний объектов, но увеличивает норму искажения, тем самым ухудшая вычисляемую награду. В связи с этим управление процессом генерации возмущений осуществляется с учётом маски, которая выделяет необходимые области изображения. Данная маска постоянна для каждого изображения (сцены) и не изменяется ни в процессе обучения агента, ни в процессе его работы.

Маска атаки M_t представляет собой бинарную или вещественную матрицу размерности входного изображения, формируемую на основе текущих предсказаний модели:

$$M_t(i,j) = \begin{cases} 1, (i,j) \in \text{рамка объектов} \\ 0, \text{иначе} \end{cases}.$$

Физический смысл введения маски заключается в концентрации возмущения в тех регионах, которые непосредственно влияют на формирование признакового описания объекта. Это позволяет более эффективно нарушать внутреннюю структуру представления. Кроме того, локализация воздействия позволяет снизить визуальную заметность атаки для человека.

Для обучения агента, управляющего процессом генерации состязательных примеров, был выбран алгоритм проксимальной оптимизации политики (Proximal Policy Optimization, PPO) [13]. Выбор метода обучения в данной задаче определяется предложенной средой: высокая размерность состояния, стохастичность переходов.

Предложенный агент формирует непрерывные параметры атаки (ϵ_t, α_t), что требует применения алгоритмов обучения с непрерывным пространством действий. Кроме того, функция награды является нестационарной, так как зависит от текущего состояния нейросетевой модели и динамики изменения предсказаний в процессе атаки. Это накладывает дополнительные требования на устойчивость алгоритма обучения.

Алгоритм PPO оптимизирует параметризованную стратегию $\pi_\theta(a_t|s_t)$ посредством максимизации ожидаемой награды. Важной особенностью PPO является использование ограниченного обновления политики, что достигается за счёт ограничения отношения вероятностей действий:

$$L^{CLIP}(\theta) = \mathbb{E}_t[\min(r_t(\theta)\hat{A}_t, clip(r_t(\theta), 1-\epsilon, 1+\epsilon)\hat{A}_t)], \quad (4)$$

где $r_t(\theta) = \frac{\pi_\theta(a_t|s_t)}{\pi_{\theta_{old}}(a_t|s_t)}$ – отношение вероятностей действий; $\hat{A}_t$ – оценка преимущества; ϵ – параметр ограничения.

Использование данного ограничения (4) позволяет избежать резких изменений политики и обеспечивает более стабильную сходимость по сравнению с классическими методами.

Анализ альтернативных подходов демонстрирует ограниченную применимость методов, опирающихся на функцию ценности (например, DQN), в силу их ориентации на дискретное пространство действий. Помимо этого, алгоритмы данного класса чувствительны к колебаниям функции вознаграждения и требуют применения вспомогательных механизмов стабилизации, таких как целевые сети и буфер повторного опыта, что усложняет процесс обучения.

Алгоритмы, работающие с непрерывным пространством действий, такие как DDPG и TD3, подходят для данной задачи, однако отличаются высокой чувствительностью к подбору гиперпараметров и тенденцией к завышению оценок функции ценности. В условиях нестационарной среды указанные особенности приводят к нестабильности обучения и деградации стратегии.

Таким образом, использование алгоритма PPO с параметрами, которые приведены в таблице 1, определяется его способностью поддерживать стабильную и эффективную оптимизацию

Таблица 1.

Параметры алгоритма PPO для обучения агента генерации

Параметр	Количество шагов обучения	Коэффициент дисконтирования	Количество эпох для обучения на подвыборке
Значение	2048	0,9	5

при непрерывном пространстве действий, изменчивой функции вознаграждения и высокой размерности пространства состояний. Данные характеристики полностью соответствуют специфике генерации состязательных воздействий.

Экспериментальная оценка предложенного метода генерации состязательных примеров и его влияние на результаты состязательного обучения

Экспериментальная часть работы направлена на оценку эффективности и сравнительный анализ предложенного подхода генерации состязательных воздействий на основе MDP. Сравнительный анализ проведён с классическим методом атаки. Данный анализ направлен на оценку разности влияния полученных примеров на устойчивость моделей детекции.

В качестве базовой архитектуры использовалась дообученная модель детекции объектов YOLOv8[3], реализованная в рамках фреймворка Ultralytics и адаптированная под задачу многоклассовой детекции военной техники. Обучение и предсказание модели выполнялись с использованием фреймворка PyTorch[4], который обеспечивает гибкую реализацию и удобную интеграцию процедур обучения и тестирования.

Обучение и тестирование агента и моделей проводились на специализированном наборе данных Military Vehicle Dataset[5]. Данный набор содержит изображения различных типов военной техники в условиях, приближенных к реальным сценам наблюдения с высоты полёта дрона, который представляет из себя элемент РТК. Выбор данного набора данных обусловлен необходимостью оценки устойчивости модели в прикладных задачах, где повышены требования к надежности детекции объектов.

Для реализации обучения агента в постановке MDP использовались инструменты библиотеки Stable-Baselines3[6]. Данная библиотека предоставляет стандартные реализации алгоритмов обучения с подкреплением и средства для построения пользовательских сред взаимодействия с моделью детекции.

3 Ultralytics. YOLOv8: State-of-the-art object detection and segmentation model. – URL: https://github.com/ultralytics/ultralytics (дата обращения: 20.04.2026).

4 Paszke A., Gross S., Massa F. et al. PyTorch: An Imperative Style, High-Performance Deep Learning Library. – URL: https://pytorch.org (дата обращения: 20.04.2026).

5 Military Vehicle Dataset (Object Detection Dataset). Roboflow Universe. – URL: https://universe.roboflow.com/vgtu-n8zmy/military-vehicle (дата обращения: 20.04.2026).

6 Raffin A. et al. Stable-Baselines3: Reliable Reinforcement Learning Implementations. – URL: https://github.com/DLR-RM/stable-baselines3 (дата обращения: 20.04.2026).

Эксперименты для оценки эффективности и сравнительного анализа включали три основных сценария, отражающих различные режимы воздействия на модель.

Первый сценарий соответствует работе исходной модели без применения атак и используется как базовый уровень для последующего сравнения.

Второй сценарий предполагает применение фиксированной состязательной атаки (PGD), при которой возмущения формируются по детерминированному градиентному правилу без учета состояния модели в процессе атаки. Данный подход с заданными параметрами (табл. 2) используется как классический метод генерации состязательных примеров и служит ориентиром для сравнения. Ввиду особенности генерации состязательных примеров PGD алгоритмом, а именно сильное зашумление исходного изображения, были выбраны параметры, максимально ухудшающие производительность базовой YOLO-модели.

Третий сценарий основан на обучении и использовании предложенного адаптивного MDP-агента, который формирует состязательные воздействия с учетом текущего состояния модели.

Дополнительно рассматривались сценарии состязательного обучения, в рамках которого сгенерированные примеры включались в обучающую выборку. Под этим добавлением понимается расширение исходного набора данных за счет добавления модифицированных изображений. Далее модель дообучается на смеси исходных и атакованных данных, что позволяет повысить устойчивость к подобным возмущениям в дальнейшем.

Для корректного сопоставления результатов между различными методами генерации атак во всех сценариях состязательного обучения используются одинаковые исходные изображения. При этом доля состязательных примеров в обучающей выборке фиксирована и составляет 25 % от общего числа обучающих данных и также являются фиксированными. Такая доля состязательных примеров в обучающих выборках выбран как компромисс между сохранением качества обучения на чистых данных и достаточной интенсивностью воздействия для повышения устойчивости модели.

Экспериментальная постановка охватывает как анализ эффективности различных типов

Таблица 2.

Параметры алгоритма PGD

Параметр	Максимальная доля возмущения за шаг (ϵ)	Размер шага возмущения за шаг генерации (α)	Количество шагов генерации
Значение	0,5	0,1	10

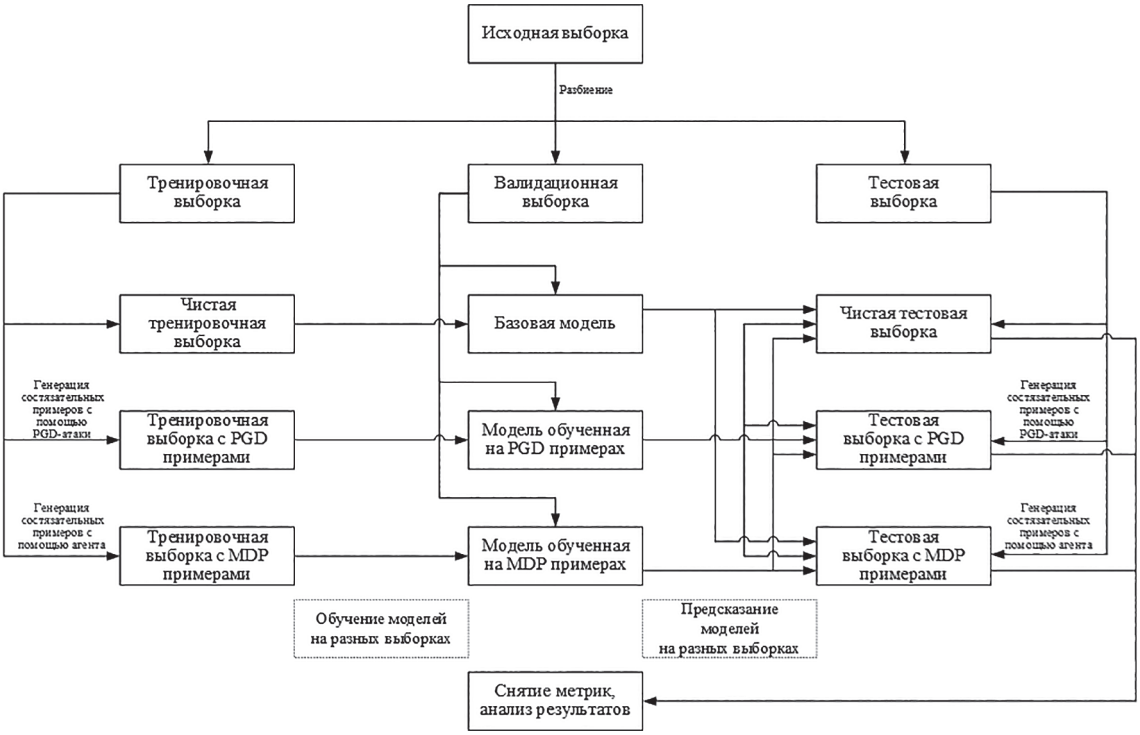


Рис. 2. План проведения эксперимента

атак, так и их влияние на процесс повышения устойчивости модели через состязательное обучение. Всего в ходе валидации результатов оговаривается 9 случаев (предсказание чистых и состязательных примеров двух видов для каждой полученной модели). Итоговый план проведения эксперимента представлен на рисунке 2.

Важным процессом в ходе генерации тренировочных и тестовых выборок является процесс генерации состязательных возмущений, а следовательно, состязательных изображений. Динамики генерации таких примеров относительно метрик-компонент функции наград агента $\overline{C_t}$, $\overline{IoU_t}$ и l_2 и функции наград непосредственно представлены на рисунке 3.

Полученные данные говорят, что с точки зрения влияния подходов на способность модели распознать изменённые объекты, алгоритм PGD обладает значительным преимуществом. В то же время MDP агент решает задачу минимизации не только рассматриваемых метрик, но и задачу минимизации степени возмущения в совокупности.

В соответствии с поставленной задачей анализ полученных результатов обучения моделей на состязательных примерах проводится с точки зрения устойчивости модели к состязательным воздействиям. Оценка эффективности предложенного подхода проводилась на основе совокупности численных метрик, позволяющих анализировать как качество детекции, так и устойчивость модели к состязательным воздействиям.

В качестве первичной оценки используются графики процесса обучения модели в трёх рассматриваемых конфигурациях. Во всех рассматриваемых случаях используются одинаковые параметры для обучения моделей. Данные кривые позволяют сравнить динамику сходимости модели, скорость достижения устойчивого качества и влияние различных типов состязательных данных на процесс оптимизации. Особое внимание уделяется разнице в стабильности обучения и финальном уровне метрик качества детекции.

На рисунке 4 представлены графики динамики функций потерь моделей, обученных на разных вариациях тренировочной выборки (чистой, с 25 % состязательных примеров, полученных с помощью PGD алгоритма и с 25 % состязательных примеров, полученных с помощью агента MDP). На данных графиках потеря точности локализации объекта оценивает точность определения рамки вокруг объекта моделью, Потеря ошибки классификации, оценивает правильность определения моделью класса объекта. Потеря точности границ, отображает точность определения границ объекта непосредственно. На валидации данные функции потерь означают то же самое, но считаются на проверочном наборе и помогают понять, как модель ведёт себя на данных, которых она не видела во время обучения.

В контексте проводимого анализа видно, что модели, обучаемые на состязательных примерах имеют повышенные значения функций потерь относительно обучения базовой модели YOLO на новых данных. Данный факт в совокупности с метриками fitness и fps, представленных на рисунке 5, говорит о том, что моделям тяжелее обучаться на состязательных примерах ввиду их неестественности, так как состязательные возмущения напрямую влияют на карту признаков моделей. В архитектуре YOLO комплексный показатель качества (fitness) служит оценкой работы модели распознования объектов. Он рассчитывается как взвешенная комбинация основных характеристик, включая точность, полноту и среднюю точность (mAP), и применяется для сравнения конфигураций моделей. Скорость обработки кадров (FPS) отражает вычислительную эффективность алгоритма и определяет его пригодность для систем реального времени.

На рисунках 6–8 представлены результаты оценки НС моделей на различных вариантах тестовой выборки. В задачах обнаружения объектов точность характеризует долю верно идентифицированных объектов среди всех предложенных моделью, полнота – долю обнаруженных объектов относительно общего числа реальных, а F1-мера представляет их гармоническое среднее. Показатели mAP50 и mAP50-95 обозначают среднюю точность при пороге пересечения ограничивающих рамок (IoU) 0,5 и усреднённую точность в диапазоне IoU от 0,5 до 0,95 соответственно. Среднее значение IoU отражает степень совпадения предсказанных и эталонных рамок, а средняя уверенность вычисляется как математическое ожидание вероятности,

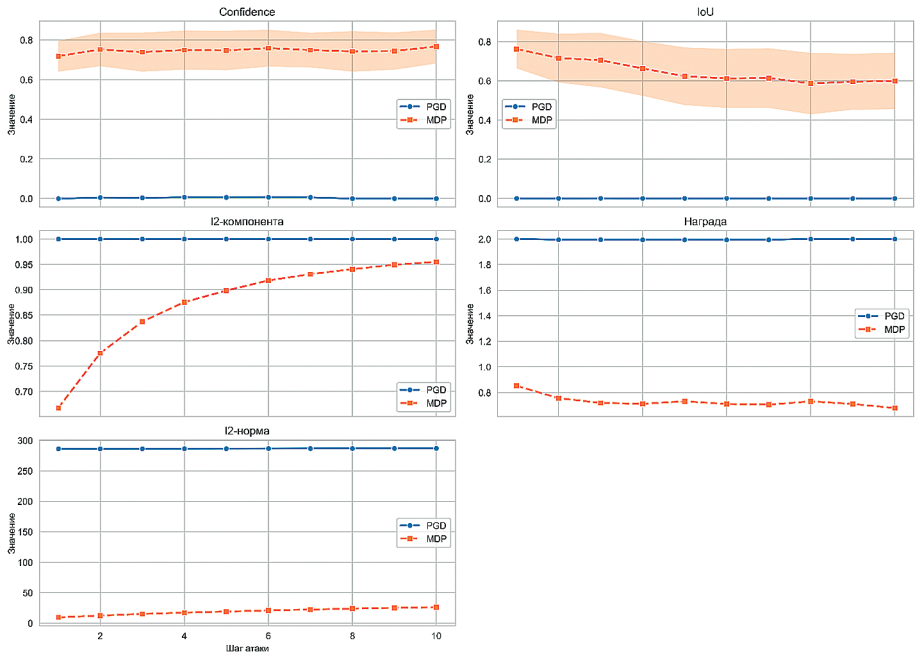


Рис. 3. Динамики генерации состязательных примеров подходами PGD и MDP

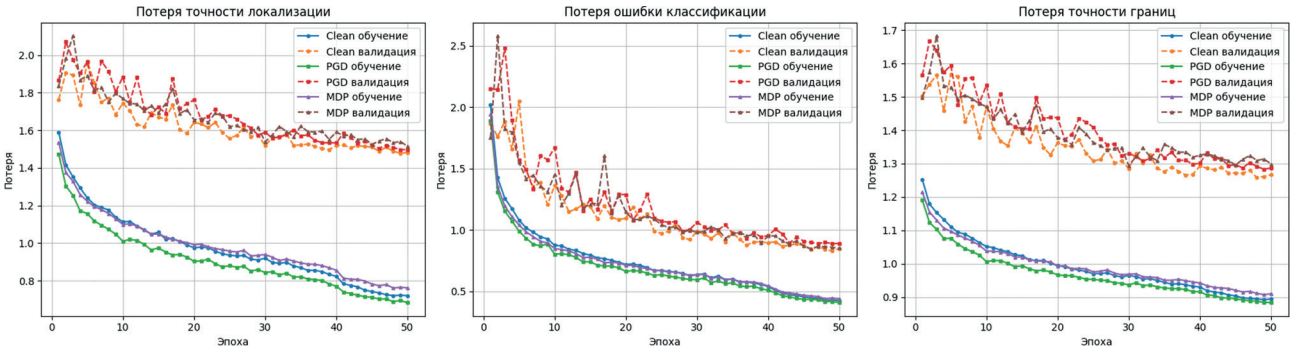


Рис. 4. Динамики функций потерь при обучении YOLO на чистой и состязательных выборках тренировочного набора

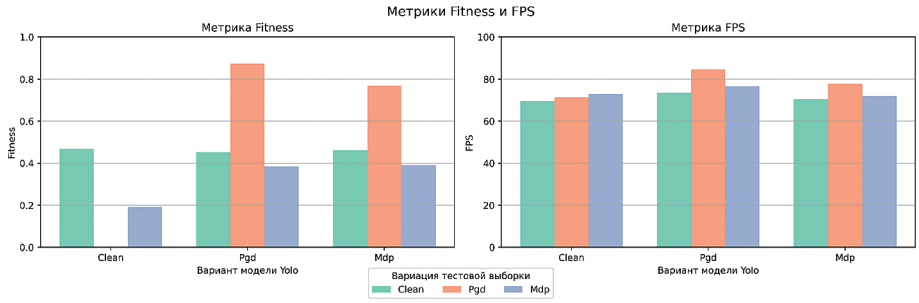


Рис. 5. Метрики качества обучения моделей распознавания

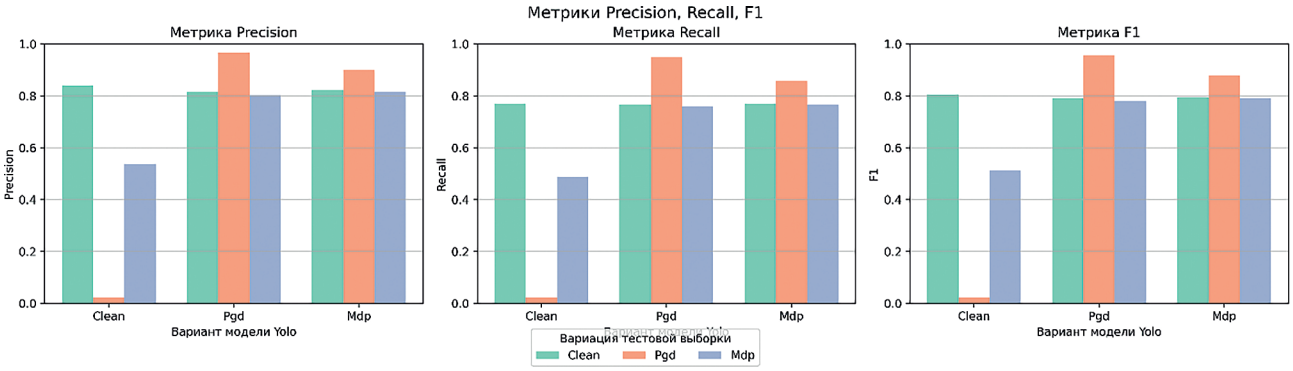


Рис. 6. Метрики precision, recall, F1 моделей распознавания

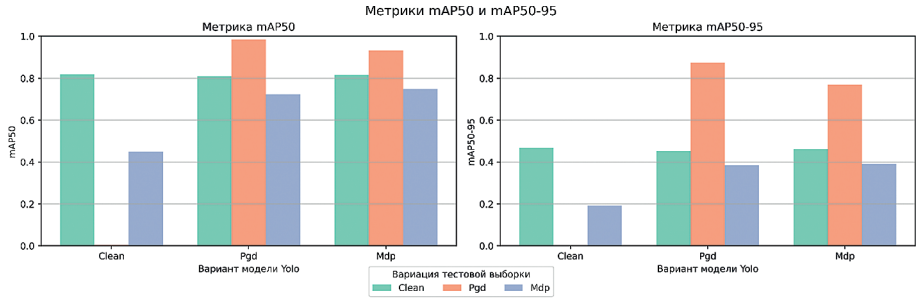


Рис. 7. Метрики mAP50 и mAP50-95 моделей распознавания

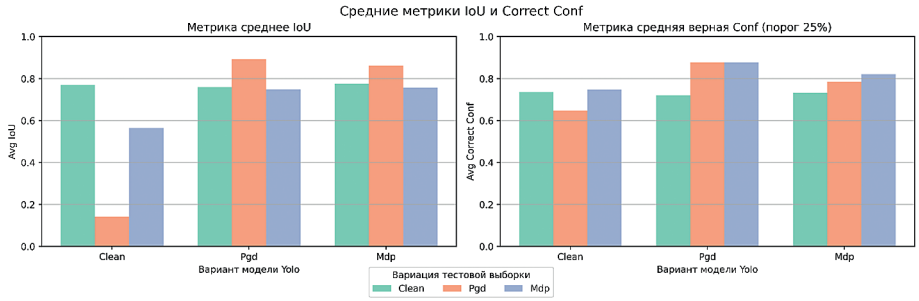


Рис. 8. Метрики IoU и верная Conf моделей распознавания

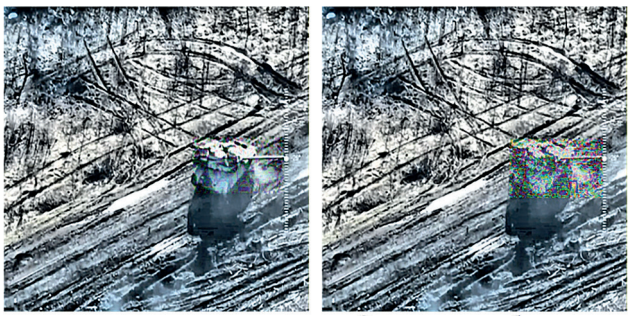
присвоенной моделью верным детекциям при пороге отсечения 0,25.

Базовая модель показывает высокие результаты на исходной выборке, однако её показатели существенно снижаются при обработке данных, подвергнутых атакам PGD и MDP, что свидетельствует о низкой устойчивости к состязательным воздействиям. Модификация, дообученная на примерах, сгенерированных методом PGD (25 % выборки), значительно повышает устойчивость к данному типу атак, демонстрируя наилучшие значения всех основных

метрик. Одновременно с этим модель проявляет признаки избыточной адаптации к специфике PGD: наблюдается завышение уверенности распознавании объектов, при этом на чистой выборке прироста качества не фиксируется. Вариант, использующий генерацию данных по методу MDP, отличается более сбалансированными характеристиками: показатели на атакованных выборках уступают версии, обученной на PGD, но превосходят базовую, а качество работы на исходных данных сохраняется на сопоставимом уровне. Таким образом, дообучение на примерах, полученных с помощью алгоритма PGD, обеспечивает максимальную специализированную устойчивость, тогда как применение MDP способствует лучшей способности к обобщению при умеренном снижении абсолютных значений метрик.

В проведённом эксперименте сравнивались классическая PGD-атака и подход, в котором параметры атаки (ϵ и α (2)) управляются MDP-агентом. Полученные результаты показывают, что, несмотря на способ внесения состязательных возмущений, данные методы в совокупности являются разными и решают разные по смыслу задачи и, соответственно, формируют различные типы состязательных примеров.

PGD, при подборе параметров на максимальное ухудшение качества детекции объектов, генерирует более сильные возмущения, что подтверждается большей l_2-нормой. Такие примеры эффективно снижают качество модели и позволяют обучать более устойчивые модели в условиях наиболее худших сценариев атак. Это достигается ценой сильного искажения изображений: шум визуально заметен (рис. 9), что указывает на выход за пределы естественного распределения данных.



Состязательное изображение, созданное с помощью MDP агента

Состязательное изображение, созданное с помощью алгоритма PGD

Рис. 9. Примеры состязательных изображений, сгенерированных различными способами

В отличие от этого, агент MDP является регулятором параметров атаки. За счёт встроенного штрафа на величину возмущения он находит компромисс между эффективностью атаки и сохранением структуры изображения. В результате генерируются состязательные примеры с существенно меньшей нормой и практически незаметными для человека искажениями (рис. 9). Такие примеры ближе к естественным данным и лучше сохраняют семантику сцены.

Данные различия отражаются на результатах обучения. Модели, обученные на MDP-примерах, демонстрируют сопоставимые, а в ряде случаев более высокие метрики на чистых и MDP-выборках, что говорит о меньшей деградации базового качества. Кроме того, такие модели обладают более стабильным поведением. Они лучше обобщают данные, близкие к исходному распределению. Это делает MDP-подход приоритетным в прикладных сценариях, где важен баланс между устойчивостью и качеством.

Так как MDP является более щадящим подходом, то его использование позволяет применять его как инструмент для регуляризации.

Таким образом, PGD остаётся более сильной атакой в терминах максимального ухудшения качества, тогда как MDP-подход обеспечивает более реалистичные, малозаметные и устойчивые возмущения, выступая эффективным механизмом адаптивной настройки атаки и улучшения обобщающей способности модели.

Заключение

В настоящем исследовании рассмотрена задача повышения устойчивости НС, входящих в состав ИИ СУ РТК, к состязательным атакам. В качестве основного инструмента генерации возмущений использован формализм марковского процесса принятия решений. Данный подход заменяет статические схемы формирования атак на адаптивную стратегию, учитывающую текущее состояние модели распознавания объектов и специфику входных данных. Обученный агент формирует состязательные примеры с ограниченным уровнем искажений. Он сохраняет баланс между снижением точности детекции и сохранением визуальной естественности изображений. По сравнению с классическими итеративными методами (например, PGD), генерируемые возмущения отличаются большей вариативностью и структурной правдоподобностью, что повышает их ценность как тренировочного материала для состязательной настройки моделей.

Экспериментальная проверка подтвердила, что включение сгенерированных примеров в процесс дообучения НС повышает их устойчивость без существенного падения производительности на исходных данных. Подобный

результат важен для робототехнических систем, функционирующих в условиях неполной информации и внешних помех, где необходимы как высокая точность распознавания, так и отказоустойчивость. Метод усиливает безопасность РТК за счёт создания моделей восприятия, устойчивых не только к целевым атакам, но и к естественным шумам окружающей среды. Это напрямую снижает вероятность ошибочных управляющих решений, повышает общую надёжность системы и расширяет допустимую область её применения в задачах повышенной ответственности.

Полученные результаты подтверждают целесообразность применения методов обучения с подкреплением для формирования адаптивных состязательных воздействий. Данное направление представляется перспективным инструментом обеспечения киберфизической безопасности [14–16] интеллектуальных СУ РТК.

В заключение следует отметить, что представленный подход соотносится с результатами работы[7] по решению задачи защиты ИИ СУ РТК от атак отравления данных. В указанном исследовании механизм MDP применялся для контроля входных данных и принятия решений об их использовании в процессе обучения, что позволяло предотвращать деградацию модели за счёт фильтрации потенциально скомпрометированных выборок. В отличие от этого, в данной работе MDP используется на этапе генерации состязательных воздействий, где агент управляет параметрами атаки с целью формирования релевантных примеров для последующего состязательного обучения.

Несмотря на различие в уровне применения (контроль входных данных и активное формирование атакующих воздействий), оба подхода опираются на единую концепцию принятия решений в условиях неопределённости и динамики состояния модели. Их совместное использование позволяет реализовать комплексную стратегию повышения устойчивости ИИ СУ РТК. Данная стратегия объединяет механизмы предотвращения внедрения вредоносных данных и повышения защищённости моделей к атакам уклонения, что в совокупности сужает поверхность для атаки РТК и обеспечивает более высокий уровень устойчивости их интеллектуальных подсистем.

7 Программа генератора агентов для обнаружения атак отравления наборов данных: свидетельство о гос. регистрации программы для ЭВМ RU 2026613545 / правообладатель А. А. Шевченко. – № 2026612373; зарегистрировано 02.02.2026; опубл. 06.02.2026. – 1 электрон. опт. диск (Python; 77521 байт).

Литература

1. Akhtar N., Mian A. Threat of adversarial attacks on deep learning in computer vision: A survey // IEEE Access. – 2021. – Vol. 9. – P. 12315–12336. – DOI: 10.1109/ACCESS.2021.3052020.
2. Wang Z., Wang X., Liu J., et al. Adversarial attacks on deep learning-based object detection systems: A survey // Neurocomputing. – 2022. – Vol. 493. – P. 1–19. – DOI: 10.1016/j.neucom.2022.03.045.
3. Qiu S., Liu Q., Zhou S., Wu C. Review of adversarial attacks and defense strategies in deep learning-based computer vision systems // Applied Sciences. – 2022. – Vol. 12 (15). – Art. 7583. – DOI: 10.3390/app12157583.
4. Xu H., Ma Y., Liu H., Deb D., Liu H., Tang J., Jain A. D. Adversarial attacks and defenses in images, graphs and text: A review // International Journal of Automation and Computing. – 2021. – Vol. 18 (2). – P. 151–178. – DOI: 10.1007/s11633-021-1274-3.
5. Li Y., Li X., Wang X., et al. Survey of adversarial machine learning in deep neural networks: attacks, defenses and robustness evaluation // ACM Computing Surveys. – 2023. – Vol. 55 (10). – P. 1–38. – DOI: 10.1145/3562695.
6. Pavlitskaya S. et al. Adversarial Vulnerability of Temporal Feature Networks for Object Detection // Sensors. – 2023. – Vol. 23 (23). – DOI: 10.3390/s23239579.
7. Zhou Z., Chen X., Li E., et al. Robustness of deep learning models under real-world corruption: A survey // Pattern Recognition. – 2023. – Vol. 138. – Art. 109386. – DOI: 10.1016/j.patcog.2023.109386.
8. Nguyen K. N. T., Zhang W., Lu K., Wu Y.-H., Zheng X., Tan H. L., Zhen L. A Survey and Evaluation of Adversarial Attacks in Object Detection // IEEE Transactions on Neural Networks and Learning Systems. – 2025. – DOI: 10.1109/TNNLS.2025.3561225.
9. Thunuguntla A., Tadepalli P., Raffa G. Defenses Against Adversarial Attacks on Object Detection: Methods and Future Directions // Information. – 2025. – Vol. 16 (11). – DOI: 10.3390/info16111003.
10. Huang Y., Zhang Y., Wu X., et al. Reinforcement learning for adversarial example generation and defense: A comprehensive survey // IEEE Transactions on Neural Networks and Learning Systems. – 2024. – DOI: 10.1109/TNNLS.2024.3351123.
11. Chen J., Wu Y., Liang J., et al. Robust adversarial reinforcement learning: A survey and taxonomy // Information Sciences. – 2022. – Vol. 608. – P. 1–24. – DOI: 10.1016/j.ins.2022.06.033.
12. Domico K., Sheatsley R., Pauley E., Hanna J., McDaniel P. Adversarial Agents: Black-Box Evasion Attacks with Reinforcement Learning // ResearchGate: научная социальная сеть. – 2025. – DOI: 10.48550/arXiv.2503.01734.
13. Schulman J., Wolski F., Dhariwal P., Radford A., Klimov O. Proximal Policy Optimization Algorithms // arXiv.org: электронный архив. – 2021. – arXiv:1707.06347. – Режим доступа: https://arxiv.org/abs/1707.06347 (дата обращения: 20.04.2026).

14. Липатников В. А., Тихонов В. А. Распознавание вторжений нарушителя при управлении кибербезопасностью инфраструктуры интегрированной организации на основе нейро-нечетких сетей и когнитивного моделирования // В сборнике: Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО, 2019). сборник научных статей VIII Международной научно-технической и научно-методической конференции: в 4 т. – 2019. – С. 659–664.
15. Липатников В. А., Парфиров В. А. Метод поддержки принятия решения при управлении сетью связи на основе технологии нейронных сетей // В сборнике: Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО, 2024). Материалы XIII Международной научно-технической и научно-методической конференции. Санкт-Петербург, 2024. – С. 467–472.
16. Синдеев М. А., Васильев Н. А., Смирнов В. А., Шевченко А. А., Косолапов В. С., Липатников В. А., Парфиров В. А. Программный комплекс для прогнозирования и поддержки принятия решений администратором сети по парированию многоэтапной атаки. Свидетельство о регистрации программы для ЭВМ RU 2022616751, 15.04.2022. Заявка № 2022615448 от 29.03.2022.

PROTECTION AGAINST ADVERSARIAL ATTACKS OF NEURAL NETWORKS CONTROL SYSTEMS FOR ROBOTIC COMPLEXES BASED ON MARKOV PROCESSES

Satsuta A. I.[8], Lipatnikov V. A.[9]

Keywords: *artificial intelligence security, protection of machine learning models, adversarial learning, computer vision, object recognition, control systems for robotic complexes.*

Abstract

Objective: *the purpose of the work is to analyze the vulnerabilities of neural network models of robotic control systems to adversarial influences and to develop a way to increase their protection based on reinforcement learning methods.*

Research method: *an approach based on the formalization of the process of generating adversarial examples as a task of the Markov decision-making process.*

Results of the study: *an agent has been developed that adaptively generates adversarial examples by taking into account the state of the environment and the characteristics of the model. It is proposed to train the agent to generate adversarial examples with subsequent use in adversarial training. The agent's state is formed on the basis of model feature maps, gradient information, and the value of input data distortion, estimated according to the l2 norm. The agent's actions correspond to the choice of PGD attack parameters.*

Scientific novelty: *a new reward function is proposed, which takes into account both the quality of detection and the amount of distortion, which provides a balance between the effectiveness of the attack and its stealth.*

References

1. Akhtar N., Mian A. Threat of adversarial attacks on deep learning in computer vision: A survey // IEEE Access. – 2021. – Vol. 9. – P. 12315–12336. – DOI: 10.1109/ACCESS.2021.3052020.
2. Wang Z., Wang X., Liu J., et al. Adversarial attacks on deep learning-based object detection systems: A survey // Neurocomputing. – 2022. – Vol. 493. – P. 1–19. – DOI: 10.1016/j.neucom.2022.03.045.
3. Qiu S., Liu Q., Zhou S., Wu C. Review of adversarial attacks and defense strategies in deep learning-based computer vision systems // Applied Sciences. – 2022. – Vol. 12 (15). – Art. 7583. – DOI: 10.3390/app12157583.
4. Xu H., Ma Y., Liu H., Deb D., Liu H., Tang J., Jain A. D. Adversarial attacks and defenses in images, graphs and text: A review // International Journal of Automation and Computing. – 2021. – Vol. 18 (2). – P. 151–178. – DOI: 10.1007/s11633-021-1274-3.
5. Li Y., Li X., Wang X., et al. Survey of adversarial machine learning in deep neural networks: attacks, defenses and robustness evaluation // ACM Computing Surveys. – 2023. – Vol. 55 (10). – P. 1–38. – DOI: 10.1145/3562695.
6. Pavlitskaya S. et al. Adversarial Vulnerability of Temporal Feature Networks for Object Detection // Sensors. – 2023. – Vol. 23 (23). – DOI: 10.3390/s23239579.
7. Zhou Z., Chen X., Li E., et al. Robustness of deep learning models under real-world corruption: A survey // Pattern Recognition. – 2023. – Vol. 138. – Art. 109386. – DOI: 10.1016/j.patcog.2023.109386.
8. Nguyen K. N. T., Zhang W., Lu K., Wu Y.-H., Zheng X., Tan H. L., Zhen L. A Survey and Evaluation of Adversarial Attacks in Object Detection // IEEE Transactions on Neural Networks and Learning Systems. – 2025. – DOI: 10.1109/TNNLS.2025.3561225.

8 ***Anatoly I. Satsuta***, Senior Operator of the Scientific Company of the Military Academy of Communications named after Marshal of the Soviet Union S. M. Budyonny, St. Petersburg, Russia. E-mail: toha.satzuta@yandex.ru

9 ***Valery A. Lipatnikov***, Dr.Sc. of Technical Sciences, Professor, Senior Researcher of the Research Center of the Military Academy of Communications named after Marshal of the Soviet Union S. M. Budyonny, St. Petersburg. E-mail: lipatnikovanl@mail.ru

9. Thunuguntla A., Tadepalli P., Raffa G. Defenses Against Adversarial Attacks on Object Detection: Methods and Future Directions // Information. – 2025. – Vol. 16 (11). – DOI: 10.3390/info16111003.
10. Huang Y., Zhang Y., Wu X., et al. Reinforcement learning for adversarial example generation and defense: A comprehensive survey // IEEE Transactions on Neural Networks and Learning Systems. – 2024. – DOI: 10.1109/TNNLS.2024.3351123.
11. Chen J., Wu Y., Liang J., et al. Robust adversarial reinforcement learning: A survey and taxonomy // Information Sciences. – 2022. – Vol. 608. – P. 1–24. – DOI: 10.1016/j.ins.2022.06.033.
12. Domico K., Sheatsley R., Pauley E., Hanna J., McDaniel P. Adversarial Agents: Black-Box Evasion Attacks with Reinforcement Learning // ResearchGate: nauchnaya social'naya set'. – 2025. – DOI: 10.48550/arXiv.2503.01734.
13. Schulman J., Wolski F., Dhariwal P., Radford A., Klimov O. Proximal Policy Optimization Algorithms // arXiv.org: ehlektronnyj arhiv. – 2021. – arXiv:1707.06347. – Rezhim dostupa: https://arxiv.org/abs/1707.06347 (data obrashcheniya: 20.04.2026).
14. Lipatnikov V. A., Tihonov V. A. Raspoznavanie vtorzhenij narushitelya pri upravlenii kiberbezopasnost'yu infrastruktury integrirovannoj organizacii na osnove nejro-nechetkih setej i kognitivnogo modelirovaniya. V sbornike: Aktual'nye problemy infotelekommunikacij v nauke i obrazovanii (APINO, 2019). sbornik nauchnyh statej VIII Mezhdunarodnoj nauchno-tehnicheskoj i nauchno-metodicheskoj konferencii: v 4 t. – 2019. – S. 659–664.
15. Lipatnikov V. A., Parfirov V. A. Metod podderzhki prinyatiya resheniya pri upravlenii set'yu svyazi na osnove tehnologii nejronnyh setej. V sbornike: Aktual'nye problemy infotelekommunikacij v nauke i obrazovanii (APINO, 2024). Materialy XIII Mezhdunarodnoj nauchno-tehnicheskoj i nauchno-metodicheskoj konferencii. Sankt-Peterburg, 2024. – S. 467-472.
16. Sindeev M. A., Vasil'ev N. A., Smirnov V. A., Shevchenko A. A., Kosolapov V. S., Lipatnikov V. A., Parfirov V. A. Programmnyj kompleks dlya prognozirovaniya i podderzhki prinyatiya reshenij administratorom seti po parirovaniyu mnogoehtapnoj ataki. Svidetel'stvo o registracii programmy dlya EHVM RU 2022616751, 15.04.2022. Zayavka № 2022615448 ot 29.03.2022.

АЛГОРИТМЫ МНОГОУРОВНЕВОГО КОНТРОЛЯ ЦЕЛОСТНОСТИ ЭЛЕКТРОННЫХ ДОКУМЕНТОВ В РАСПРЕДЕЛЕННЫХ СИСТЕМАХ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА

Васильев Я. А.[1], Пешнин М. А.[2], Тали Д. И.[3], Захаров И. Л.[4]

DOI:10.21681/3034-4050-2026-4-25-37

Ключевые слова: *цифровизация, цифровая трансформация документооборота, цифровой документ, целостность электронного документа, целостность системы, распределенные системы электронного документооборота.*

Аннотация

Цель *статьи состоит в разработке алгоритмов подготовки и реализации многоуровневого контроля целостности электронных документов, обрабатываемых распределенными системами электронного документооборота, в условиях деструктивных воздействий злоумышленников.*

Метод исследования: *для достижения поставленной цели используется иерархический подход в алгоритмизации процесса подготовки и проверки целостности многоуровневых структурно-сложных систем на примере электронного документооборота. В целях оценивания полученных результатов использовался логико-вероятностный метод И. А. Рябинина.*

Результаты исследования: *предложен комплекс алгоритмов многоуровневого контроля целостности электронных документов, обрабатываемых распределенными системами электронного документооборота, а также его программная реализация. Численная оценка результатов исследования позволила определить преимущество разработанного решения в сравнении с известным, выражающееся в повышении защищенности исследуемых систем за счет обеспечения целостности их структурных уровней путем обнаружения и локализации электронных документов и их компонентов, подвергшихся несанкционированному изменению в результате вероятной компрометации ключей подписи. Полученный результат достигается за счет применения криптографических преобразований к компонентам (контенту и метаданным) электронных документов по принципу небинарного дерева Меркла в сочетании с технологией цепной записи данных.*

Практическая ценность *разработанного решения состоит в иерархическом применении ключей подписи и проверки, генерируемых сервером вышестоящего уровня, к электронным документам, сформированным на сервере нижестоящего уровня, что позволяет повысить уровень защищенности распределенных систем электронного документооборота в условиях деструктивных воздействий со стороны злоумышленников (внутренних и внешних нарушителей) при вероятной компрометации ключей подписи.*

Вклад авторов: *Васильев Я. А. – разработка программной модели многоуровневого контроля целостности электронных документов, обрабатываемых распределенной системой электронного документооборота; Пешнин М. А. – разработка алгоритмов подготовки и реализации многоуровневого контроля целостности электронных документов, обрабатываемых распределенной системой электронного документооборота; Тали Д. И. – разработка идеи, контроль и коррекция результатов, общее руководство; Захаров И. Л. – верификация (оценка) полученных результатов.*

Введение

Широкое использование цифровых технологий и их непрерывное совершенствование становится завершающим этапом третьей промышленной революции, а также предпосылкой к трансформации общества. Повсеместная цифровизация способствует повышению эффективности бизнес-процессов и государственного управления. Следствием этих тенденций является широкое использование автоматизированных систем (АС), предназначенных для обработки информации, в том числе электронных документов (ЭлД). Активное внедрение систем электронного документооборота (СЭД) и их дальнейшая модернизация является одной из инициатив социально-экономического развития Российской Федерации[5], в рамках которого Правительство Российской Федерации запустило проведение

1 ***Васильев Ярослав Александрович***, сотрудник Краснодарского высшего военного училища им. генерала армии С. М. Штеменко, г. Краснодар, Россия. E-mail: yawasilevs@mail.ru

2 ***Пешнин Макар Андреевич***, сотрудник Краснодарского высшего военного училища им. генерала армии С. М. Штеменко, г. Краснодар, Россия. E-mail: m.peshnin@yandex.ru

3 ***Тали Дмитрий Иосифович***, кандидат технических наук, докторант специальной кафедры Краснодарского высшего военного училища им. генерала армии С. М. Штеменко, г. Краснодар, Россия. E-mail: dimatali@mail.ru

4 ***Захаров Иван Леонидович***, кандидат технических наук, старший преподаватель специальной кафедры Краснодарского высшего военного училища им. генерала армии С. М. Штеменко, г. Краснодар, Россия. E-mail: zakharovivanl@yandex.ru

5 Российская Федерация. Правительство Российской Федерации. Об утверждении стратегического направления в области цифровой трансформации государственного управления: распоряжение Правительства Российской Федерации от 16 марта 2024 г. № 637-р // Информационно-правовой портал Гарант. – URL: https://www.garant.ru/products/ipo/prime/doc/408634367/ (дата обращения: 06.05.2026).

эксперимента по цифровизации процессов электронного документооборота[6,7]. Особенностью этого эксперимента является использование цифровых документов в повседневной деятельности органов государственной власти.

Вместе с тем, говорить о переходе на полноценный безбумажный документооборот преждевременно в связи с возникновением ряда проблемных вопросов, одним из которых является несоответствие нормативной базы требованиям современного этапа технологического развития, что препятствует формированию полноценного юридически значимого электронного документооборота в рамках парадигмы «Индустрия 4.0» [1, 2].

В свою очередь, цифровая трансформация документооборота подразумевает процесс перехода организации на работу с цифровыми документами, сопровождаемый изменениями в ее цифровой и организационной структуре[8]. При этом, специалисты[9] отмечают, что существующие решения построения СЭД не позволяют перейти к принципиально новому способу управления, в целях исключения смешанных форм ЭлД, заменив их на цифровые.

Под цифровым документом (ЦД) понимается категория ЭлД, изначально созданная в цифровой форме с соблюдением правил документирования без издания его на бумажном носителе и подписанного электронной подписью (ЭП)[10]. Вместе с тем, учитывая определение «документированная информация»[11], цифровую документированную информацию (ЦДИ) можно рассматривать, как информационный объект, не подписанный ЭП, но обладающий свойствами ЦД или его части. Подобное расширение термина «электронный документ» позволяет окончательно разграничить бумажный и электронный документооборот, подводя итог в выборе методов и средств обработки такой категории ЭлД.

Изменения в терминологическом аппарате приводят к появлению новой формы перспективных СЭД, представляющей собой информационную инфраструктуру, включающую систему, обеспечивающую управление документами и доступ к ним в течение определенного времени, и системы, являющиеся источниками данных для создания ЦД[12]. Подобное представление СЭД свидетельствует о высокой степени интеграции с различными АС, что указывает на ее распределенную структуру. При этом внедрение в действующие системы таких технологий, как искусственный интеллект, распределенные реестры, облачные технологии и т.д., не только повышают эффективность исследуемых систем, но и способствует возникновению уязвимостей, что вкупе с эволюционным развитием методов и средств криптоанализа вызывает ряд угроз безопасности информации (УБИ), обрабатываемой СЭД [3–6]. Эти обстоятельства вызывают необходимость переосмысления подходов в организации управления ЦД / ЦДИ и их защите на всех этапах жизненного цикла.

Постановка задачи

Целевым предназначением СЭД является управление документами, включающее в себя их создание, ввод в систему и принятие надлежащих мер защиты при хранении. Результатом нарушения целевой функции СЭД в условиях деструктивных воздействий злоумышленников станет нарушение целостности системы в целом[13,14]. Таким образом, возникает задача по предотвращению несанкционированной модификации обрабатываемой информации в период ее жизненного цикла. В связи с этим отметим ряд особенностей, которые должны быть учтены при проектировании перспективных СЭД, в целях совершенствования документационного обеспечения управления и обеспечения защиты информации, циркулирующей в них [7].

При создании ЦД / ЦДИ $D_j^{(t_i)}(j = 1, 2, \ldots, n)$ необходимо учитывать их компонентный состав, представляющий собой в момент времени $t_i\,(i = 0, 1, \ldots, \tau)$ совокупность содержательной информации – контента $K_j^{(t_i)}$, и набора его метаданных $M_j^{(t_i)} = \{m_{i1}, m_{i2}, \ldots, m_{ig}\}$, где $m_{i1}, m_{i2}, \ldots, m_{ig}$ – реквизиты ЦД / ЦДИ (рис. 1). При подобной структуре целостность ЦД / ЦДИ имеет функциональную зависимость от двух компонент (контент

6 Российская Федерация. Правительство Российской Федерации. О проведении эксперимента по цифровизации процессов электронного документооборота, исполнения поручений и контроля исполнительской дисциплины в отдельных федеральных органах исполнительной власти: постановление Правительства Российской Федерации от 8 мая 2025 г. № 629 // Официальный интернет-портал правовой информации. URL: http://publication.pravo.gov.ru/document/0001202505140033 (дата обращения: 06.05.2026).

7 Российская Федерация. Правительство Российской Федерации. О запуске пилотного проекта по формированию единых для госорганов стандартов работы с цифровыми документами и поручениями, включая правила подготовки соответствующих документов и обмена ими: распоряжение Правительства Российской Федерации от 28 мая 2025 г. № 1350 // Информационно-правовой портал Гарант. – URL: https://www.garant.ru/products/ipo/prime/doc/411992288/ (дата обращения: 06.05.2026).

8 ГОСТ Р 59999-2025 «Цифровой документооборот организации. Требования к эталонной модели». – М.: Российский институт стандартизации, 2025.

9 Ларин М. В. Суровцева Н. Г., Терентьева Е. В. и др. Управление документами в цифровой экономике: организация, регламентация, реализация. – М.: РГГУ, 2021. – 242 с.

10 ГОСТ Р 59999-2025 «Цифровой документооборот организации. Требования к эталонной модели». – М.: Российский институт стандартизации, 2025.

11 ГОСТ Р 7.0.8-2025 «Система стандартов по информации, библиотечному и издательскому делу. Делопроизводство и архивное дело. Термины и определения». – М.: Стандартинформ, 2025.

12 ГОСТ Р 59999-2025 «Цифровой документооборот организации. Требования к эталонной модели». – М.: Российский институт стандартизации, 2025.

13 Приказ Министерства связи и массовых коммуникаций «Об утверждении требований по обеспечению целостности, устойчивости функционирования и безопасности информационных систем» от 25 августа 2009 г. № 104 // Информационно-правовой портал Гарант. – URL: https://base.garant.ru/196351/ (дата обращения: 06.05.2026).

14 ГОСТ Р 59341-2021 «Системная инженерия. Защита информации в процессе управления информацией системы». – М.: Стандартинформ, 2021.

и метаданные), имеющих между собой только логическую связь. Учитывая эту особенность, полная или частичная утрата одной из компонент, в условиях деструктивных воздействий злоумышленников, приведет к нарушению целостности ЦД / ЦДИ и, как следствие, сбою в работе СЭД.

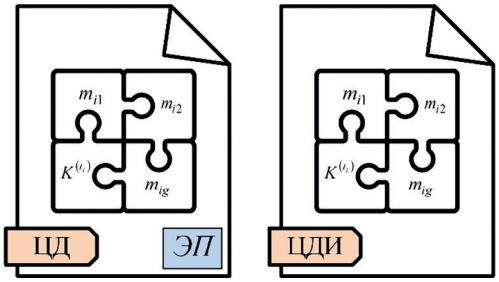


Рис. 1. Схема формирования цифрового ЦД / ЦДИ

С момента ввода в систему ЦД / ЦДИ $D_j^{(t_i)}$ подвергаются постоянным изменениям, что приводит к необходимости контроля их состояния на протяжении всего жизненного цикла. При этом хранение массивов документов $\boldsymbol{D}_{1\ldots n}^{(t_{0,\ldots,\tau})}$ в большинстве современных СЭД осуществляется в виде баз данных, где ЦД / ЦДИ должны быть структурированы таким образом, чтобы контроль целостности производился в режиме реального времени (рис. 2). В противном случае, исходя из структурных особенностей, уничтожение или несанкционированное изменение ЦД / ЦДИ $D_j^{(t_i)}$, содержащихся в массиве $\boldsymbol{D}_{1\ldots n}^{(t_{0,\ldots,\tau})}$, впоследствии приведет к нарушению функционирования системы в целом.

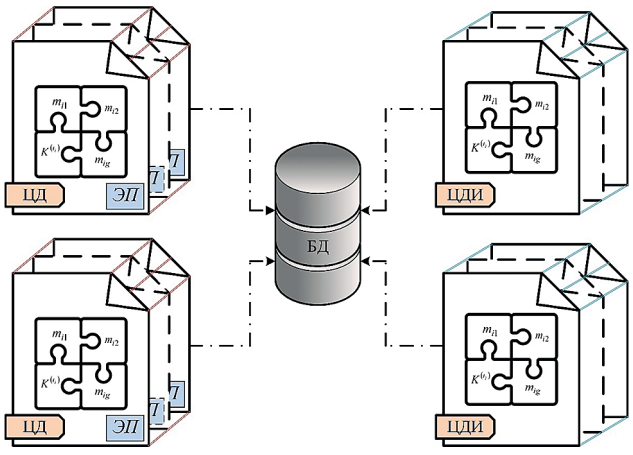


Рис. 2. Динамические изменения ЦД / ЦДИ

Кроме того, учитывая тенденции цифрового развития, современные СЭД носят территориально-распределенный характер с иерархическим принципом управления [8, 9] (рис. 3). В этих условиях выход из строя любой составляющей одного из организационных уровней по указанным выше причинам приведет к нарушению целостности[15] всей распределенной системы.

Рис. 3. Территориально-распределенная СЭД

В целях устранения выявленных недостатков к разработке предлагается комплекс алгоритмов многоуровневого контроля целостности ЦД / ЦДИ в распределенных СЭД на основе технических решений [10–12], представленный в нотации псевдокода.

Критерием качества функционирования распределенной СЭД служит выполнение условия:

$$P_{\text{н.ц.}}^{\text{разр.}} < P_{\text{н.ц.}}^{\text{прототипа}}, \quad (1)$$

где $P_{\text{н.ц.}}^{\text{разр.}}$ и $P_{\text{н.ц.}}^{\text{прототипа}}$ – вероятность нарушения целостности распределенной СЭД при разработанном и существующем способе контроля целостности ЦД / ЦДИ в условиях деструктивных воздействий злоумышленников [7].

Ограничение: в качестве деструктивных воздействий злоумышленников рассматривается компрометация ключей подписи ЦД / ЦДИ, обрабатываемых распределенной СЭД (УБИ 003: использование слабостей криптографических протоколов)[16].

Алгоритм подготовки многоуровневого контроля целостности ЦД / ЦДИ, обрабатываемых распределенной СЭД

В качестве исходных данных используется ЦД / ЦДИ $D_j^{\delta(t_i)}$ в формате *.docx, представляющий собой совокупность содержательной $K_j^{\delta(t_i)}$ и реквизитной частей $M_j^{\delta(t_i)}$, j – номер документа в массиве, где $j = 1, 2, \ldots, n$. $M_j^{\delta(t_i)} = \{m_{i1}, m_{i2}, \ldots, m_{i5}\}$, где $m_{i1}, m_{i2}, \ldots, m_{i5}$ – реквизиты ЦД / ЦДИ, t_i – момент времени, где $i = 0, 1, \ldots, \tau$, а δ – номер уровня сервера, обрабатывающего ЦД / ЦДИ, где $\delta = 1, 2, \ldots, k$. Одна из записей метаданных

15 Приказ Министерства связи и массовых коммуникаций «Об утверждении требований по обеспечению целостности, устойчивости функционирования и безопасности информационных систем» от 25 августа 2009 г. № 104 // Информационно-правовой портал Гарант. – URL: https://base.garant.ru/196351/ (дата обращения: 06.05.2026).

16 Банк данных угроз ФСТЭК // Официальный сайт. – URL: https://bdu.fstec.ru/threat (дата обращения: 06.05.2026).

$m_{i5} \in M_j^{\delta(t_i)}$ определяет уровень значимости ЦД / ЦДИ.

В целях многоуровневого контроля целостности ЦД / ЦДИ в распределенной СЭД применяются ключи $V_U = V_U^*$ (V_U – ключи подписи ЦД / ЦДИ, V_U^* – ключи проверки подписи ЦД / ЦДИ), где $V_U^{\delta(1)} = \{v_1^{\delta(1)}, v_2^{\delta(1)}, \dots, v_{\varsigma_1}^{\delta(1)}\}$ – ключи исполнителя (автора) ЦД / ЦДИ, $V_U^{\delta(2)} = \{v_1^{\delta(2)}, v_2^{\delta(2)}, \dots, v_{\varsigma_2}^{\delta(2)}\}$ – внутренние системные ключи, $V_U^{\delta(3)} = \{v_1^{\delta(3)}, v_2^{\delta(3)}, \dots, v_{\varsigma_3}^{\delta(3)}\}$ – ключи администратора системы.

Algorithm 1: Preparation of multi-level integrity control

Input: $D_j^{\delta(t_i)} = \{K_j^{\delta(t_i)}, M_j^{\delta(t_i)}\}$.
Output: $\boldsymbol{D}_{1\dots n}^{\delta(t_{0,\dots,\tau})}$.
1:**for** δ **in range** (1, ..., k):
2: **for** j **in range** (1, ..., n):
3: **for** i **in range** (0, ..., τ):
4: $H_j^{\delta(t_i)} = f(K_j^{\delta(t_i)})$
5: $h_{j1}^{\delta(t_i)} = f(m_{i1}), h_{j2}^{\delta(t_i)} = f(m_{i2}), \dots, h_{j5}^{\delta(t_i)} = f(m_{i5})$
6: $b_{j1}^{\delta(t_i)} = h_{j1}^{\delta(t_i)} \parallel h_{j2}^{\delta(t_i)}, b_{j2}^{\delta(t_i)} = h_{j3}^{\delta(t_i)} \parallel h_{j4}^{\delta(t_i)}$
7: $h_{j,1-4}^{\delta(t_i)} = b_{j1}^{\delta(t_i)} \parallel b_{j2}^{\delta(t_i)}$
8: $\tilde{H}_j^{\delta(t_i)} = f^{(v_x^{\delta(1)})}(H_j^{\delta(t_i)})$
9: $\tilde{h}_{j,1-4}^{\delta(t_i)} = f^{(v_x^{\delta(2)})}(h_{j,1-4}^{\delta(t_i)})$
10: $\tilde{h}_{j,5}^{\delta(t_i)} = f^{(v_x^{\delta(3)})}(h_{j,5}^{\delta(t_i)})$
11: $\tilde{S}_j^{\delta(t_i)} = f^{(v_x^{\delta(2)})}\tilde{H}_j^{\delta(t_i)} \parallel \tilde{h}_{j,1-4}^{\delta(t_i)} \parallel \tilde{h}_{j,5}^{\delta(t_i)}$
12: **if** ($j = 1$ **and** $i = 0$):
13: $B^{\delta(t_i)} = f^{(v_x^{\delta(2)})}(S_j^{\delta(t_i)})$
14: **else**:
15: $\hat{B}^{\delta(t_{i-1})} = f^{(v_x^{*\delta(2)})}(B^{\delta(t_{i-1})})$
16: $B^{\delta(t_i)} = f^{(v_x^{\delta(2)})}(\hat{B}^{\delta(t_{i-1})} \parallel S_j^{\delta(t_i)})$
17: **if** (δ < k):
18: $\xi^{\delta(t_i)} = f^{(v_x^{\delta+1(2)})}(B^{\delta(t_i)})$
19: **else:**
20: $\xi^{\delta(t_i)} = f^{(v_x^{\delta(2)})}(B^{\delta(t_i)})$
21:**return** $\boldsymbol{D}_{1\dots n}^{\delta(t_{0,\dots,\tau})}$.

В целях пояснения работы алгоритма изложим его реализацию в виде пошагового описания.

Шаг 1–3. Все операции повторяются в отношении каждого ЦД / ЦДИ $D_j^{\delta(t_i)}$ массива на протяжении всего жизненного цикла $t_0, t_1, \dots, t_\tau$ на серверах всех уровней.

Шаг 4–5. Процедура вычисления сигнатур контента $H_j^{\delta(t_i)}$ и метаданных $h_{j1}^{\delta(t_i)}, h_{j2}^{\delta(t_i)}, \dots, h_{j5}^{\delta(t_i)}$ ЦД / ЦДИ $D_j^{\delta(t_i)}$.

Шаг 6. Процедура формирования бинарных пар $b_{j1}^{\delta(t_i)}, b_{j2}^{\delta(t_i)}$ сигнатур метаданных ЦД / ЦДИ $D_j^{\delta(t_i)}$.

Шаг 7. Процедура вычисления корневой сигнатуры $h_{j,1-4}^{\delta(t_i)}$ метаданных ЦД / ЦДИ $D_j^{\delta(t_i)}$ посредством конкатенации вычисленных ранее сигнатур бинарных пар.

Шаг 8. Криптографическое преобразование сигнатуры контента $H_j^{\delta(t_i)}$ ЦД / ЦДИ $D_j^{\delta(t_i)}$ с использованием ключей $v_x^{\delta(1)} \in V_U^{\delta(1)}$, где $x \in \{1, \dots, \varsigma_1\}$.

Шаг 9. Криптографическое преобразование корневой сигнатуры $h_{j,1-4}^{\delta(t_i)}$ метаданных ЦД / ЦДИ $D_j^{\delta(t_i)}$ с использованием ключей $v_x^{\delta(2)} \in V_U^{\delta(2)}$, где $x \in \{1, \dots, \varsigma_2\}$.

Шаг 10. Криптографическое преобразование сигнатуры $h_{j,5}^{\delta(t_i)}$ одной из записей метаданных, определяющей уровень значимости ЦД / ЦДИ $D_j^{\delta(t_i)}$, с использованием ключей $v_x^{\delta(3)} \in V_U^{\delta(3)}$, где $x \in \{1, \dots, \varsigma_3\}$.

Шаг 11. Над преобразованными сигнатурами контента $\tilde{H}_j^{\delta(t_i)}$, метаданных $\tilde{h}_{j,1-4}^{\delta(t_i)}$ и одной из записей метаданных, определяющей уровень значимости $\tilde{h}_{j,5}^{\delta(t_i)}$ ЦД / ЦДИ $D_j^{\delta(t_i)}$ производятся операции конкатенации и криптографического преобразования с использованием ключей $v_x^{\delta(2)} \in V_U^{\delta(2)}$, где $x \in \{1, \dots, \varsigma_2\}$ в целях формирования общей сигнатуры $S_j^{\delta(t_i)}$ ЦД / ЦДИ в i-й момент времени.

Шаг 12–13. В случае первичного добавления документа в систему массив будет состоять из одного документа, что влечет за собой формирование корневой сигнатуры $B^{\delta(t_i)}$ многомерной структуры ЦД / ЦДИ $\boldsymbol{D}_1^{\delta(t_{0,\dots,\tau})}$ путем криптографического преобразования общей сигнатуры ЦД / ЦДИ $S_j^{\delta(t_i)}$ с использованием ключей $v_x^{\delta(2)} \in V_U^{\delta(2)}$, где $x \in \{1, \dots, \varsigma_2\}$.

Шаг 14–16. При добавлении документа в массив, содержащий другие документы, формирование корневой сигнатуры $B^{\delta(t_i)}$ многомерного массива ЦД / ЦДИ $\boldsymbol{D}_{1\dots n}^{\delta(t_{0,\dots,\tau})}$ производится в ходе выполнения операции криптографического преобразования с использованием ключей $v_x^{*\delta(2)} \in V_U^{*\delta(2)}$ ($V_U = V_U^*$), где $x \in \{1, \dots, \varsigma_2\}$ над сигнатурой многомерной структуры ЦД / ЦДИ за предыдущий момент времени $B^{\delta(t_{i-1})}$. После этого выполняются операции конкатенации и криптографического преобразования над преобразованной сигнатурой многомерного массива ЦД / ЦДИ за предыдущий момент времени $\hat{B}^{\delta(t_{i-1})}$ и общей сигнатурой $S_j^{\delta(t_i)}$ ЦД / ЦДИ за текущий момент времени с использованием ключей $v_x^{\delta(2)} \in V_U^{\delta(2)}$, где $x \in \{1, \dots, \varsigma_2\}$.

Шаг 17–18. В случае выполнения операций вычисления сигнатур на серверах нижестоящего уровня, полученный результат $B^{\delta(t_{i-1})}$ отправляется в подсистему защиты информации, размещенную на сервере вышестоящего уровня, где над ним в целях вычисления сигнатуры контроля целостности массива ЦД / ЦДИ уровня δ производится операция криптографического преобразования с использованием ключей вышестоящего уровня $v_x^{\delta+1(2)} \in V_U^{\delta+1(2)}$.

Шаг 19–20. В случае выполнения операций вычисления сигнатур на сервере максимального уровня полученный результат $B^{\delta(t_i)}$ подлежит хранению в подсистеме защиты информации, размещенной на этом сервере, где над ним в целях вычисления сигнатуры контроля целостности

массива ЦД / ЦДИ максимального уровня δ производится операция криптографического преобразования с использованием, вырабатываемых им ключей $v_x^{\delta(2)} \in V_U^{\delta(2)}$.

Последующее сохранение в доверенной среде сигнатур: $H_j^{\delta(t_i)}$, $h_{j,1-5}^{\delta(t_i)}$, $\tilde{H}_j^{\delta(t_i)}$, $\tilde{h}_{j,1-4}^{\delta(t_i)}$, $\tilde{h}_{j,5}^{\delta(t_i)}$, $S_j^{\delta(t_i)}$, $B^{\delta(t_i)}$, $\xi^{\delta(t_i)}$ ЦД / ЦДИ, вычисленных на шагах 1–20.

Шаг 21. Процедура вывода многомерных массивов ЦД / ЦДИ, обрабатываемых на функционально разделенных серверах, в среду обработки, причем связность ЦД / ЦДИ достигается за счет применения криптографических преобразований к компонентам (контенту и метаданным) ЦД / ЦДИ по принципу небинарного дерева Меркла с получением корневой сигнатуры всего массива, обрабатываемых ЦД / ЦДИ.

Алгоритм реализации многоуровневого контроля целостности ЦД / ЦДИ, обрабатываемых распределенной СЭД

В качестве исходных данных используются многомерные массивы ЦД / ЦДИ $\mathbf{D}_{1\ldots n}^{\delta(t_0,\ldots,\tau)}$ в формате *.docx.

Algorithm 2: Implementation of multi-level integrity control

Input: $\boldsymbol{D}_{1\ldots n}^{\delta(t_0,\ldots,\tau)}$.

Output: $\boldsymbol{D}_{1\ldots n}^{\delta(t_0,\ldots,\tau)'}$.

1:**for** δ **in range** (1, ..., *k*):
2: **for** *j* **in range** (1, ..., *n*):
3: **for** *i* **in range** (0, ..., τ):
4: $H_j^{\delta(t_i)**} = f(K_j^{\delta(t_i)**})$
5: $h_{j1}^{\delta(t_i)**} = f(m_{i1}), h_{j2}^{\delta(t_i)**} = f(m_{i2}), \ldots, h_{j5}^{\delta(t_i)**} = f(m_{i5})$
6: $b_{j1}^{\delta(t_i)**} = h_{j1}^{\delta(t_i)**} \parallel h_{j2}^{\delta(t_i)**}$, $b_{j2}^{\delta(t_i)**} = h_{j3}^{\delta(t_i)**} \parallel h_{j4}^{\delta(t_i)**}$
7: $\tilde{h}_{j,1-4}^{\delta(t_i)**} = b_{j1}^{\delta(t_i)**} \parallel b_{j2}^{\delta(t_i)**}$
8: $\tilde{H}_j^{\delta(t_i)**} = f^{(v_x^{\delta(1)})}(H_j^{\delta(t_i)**})$
9: $\tilde{h}_{j,1-4}^{\delta(t_i)**} = f^{(v_x^{\delta(2)})}(h_{j,1-4}^{\delta(t_i)})$
10: $\tilde{h}_{j,5}^{\delta(t_i)**} = f^{(v_x^{\delta(3)})}(h_{j,5}^{\delta(t_i)**})$
11: $S_j^{\delta(t_i)**} = f^{(v_x^{\delta(2)})}(\tilde{H}_j^{\delta(t_i)**}) \parallel \tilde{h}_{j,1-4}^{\delta(t_i)**} \parallel \tilde{h}_{j,5}^{\delta(t_i)**}$
12: **if** ($j = 1$ **and** $i = 0$):
13: $B^{\delta(t_i)**} = f^{(v_x^{\delta(2)})}(S_j^{\delta(t_i)**})$
14: **else**:
15: $\hat{B}^{\delta(t_{i-1})**} = f^{(v_x^{*\delta(2)})}(B^{\delta(t_{i-1})**})$
16: $B^{\delta(t_i)**} = f^{(v_x^{\delta(2)})}(\hat{B}^{\delta(t_{i-1})**} \parallel S_j^{\delta(t_i)**})$
17: **if** ($\delta < k$):
18: $\xi^{\delta(t_i)**} = f^{(v_x^{\delta+1(2)})}(B^{\delta(t_i)**})$
19: **else**:
20: $\xi^{\delta(t_i)**} = f^{(v_x^{\delta(2)})}(B^{\delta(t_i)**})$
21: **if** $\xi^{\delta(t_i)**} = \xi^{\delta(t_i)*}$:
22: **print** (“Целостность $\boldsymbol{D}_{1\ldots n}^{\delta(t_0,\ldots,\tau)}$ подтверждена”)
23: **else**:
24: print (“Целостность $\boldsymbol{D}_{1\ldots n}^{\delta(t_0,\ldots,\tau)}$ нарушена”)
25:**return** $\mathbf{D}_{1\ldots n}^{\delta(t_0,\ldots,\tau)'}$.

В целях пояснения работы алгоритма изложим его реализацию в виде пошагового описания.

Шаг 1–3. Все повторные операции вычисления выполняются в отношении каждого ЦД / ЦДИ $D_j^{(t_i)}$ массива на протяжении всего его жизненного цикла $t_0, t_1, \ldots, t_\tau$ на серверах всех уровней.

Шаг 4–5. Процедура вычисления сигнатур контента и метаданных ЦД / ЦДИ, где символ $H_j^{\delta(t_i)**}$ обозначает повторно вычисленную сигнатуру контента, символы $h_{j1}^{\delta(t_i)**}$, $h_{j2}^{\delta(t_i)**}$, ... , $h_{j5}^{\delta(t_i)**}$ обозначают повторно вычисленные сигнатуры метаданных.

Шаг 6. Повторная процедура формирования бинарных пар $b_{j1}^{\delta(t_i)**}$, $b_{j2}^{\delta(t_i)**}$ сигнатур метаданных ЦД / ЦДИ.

Шаг 7. Повторная процедура вычисления корневой сигнатуры $h_{j,1-4}^{\delta(t_i)}$ метаданных ЦД / ЦДИ посредством конкатенации вычисленных ранее бинарных сигнатур.

Шаг8.Повторноекриптографическоепреобразование сигнатуры контента $H_j^{\delta(t_i)**}$ ЦД / ЦДИ с использованием ключей $v_x^{\delta(1)} \in V_U^{\delta(1)}$, где $x \in \{1, \ldots, \varsigma_1\}$.

Шаг 9. Повторное криптографическое преобразование корневой сигнатуры $h_{j,1-4}^{\delta(t_i)}$ метаданных ЦД / ЦДИ с использованием ключей $v_x^{\delta(2)} \in V_U^{\delta(2)}$, где $x \in \{1, \ldots, \varsigma_2\}$.

Шаг 10. Повторное криптографическое преобразование сигнатуры $h_{j5}^{\delta(t_i)**}$ одной из записей метаданных, определяющей уровень значимости ЦД / ЦДИ, с использованием ключей $v_x^{\delta(3)} \in V_U^{\delta(3)}$, где $x \in \{1, \ldots, \varsigma_3\}$.

Шаг 11. Повторная процедура вычисления общей сигнатуры $S_j^{\delta(t_i)**}$ ЦД / ЦДИ в *i*-й момент времени путем конкатенации сигнатуры контента $\tilde{H}_j^{\delta(t_i)**}$, корневой сигнатуры метаданных $\tilde{h}_{j,1-4}^{\delta(t_i)**}$ и сигнатуры одной из метаданных, определяющей уровень значимости $\tilde{h}_{j,5}^{\delta(t_i)**}$ с последующим криптографическим преобразованием с использованием ключей $v_x^{\delta(2)} \in V_U^{\delta(2)}$, где $x \in \{1, \ldots, \varsigma_2\}$.

Шаг 12–13. В случае, если многомерная структура ЦД / ЦДИ $\boldsymbol{D}_1^{\delta(t_0,\ldots,\tau)}$ состоит из одного документа, корневая сигнатура $B^{\delta(t_i)**}$ будет повторно формироваться путем криптографического преобразования общей сигнатуры ЦД / ЦДИ $S_j^{\delta(t_i)**}$ с использованием ключей $v_x^{\delta(2)} \in V_U^{\delta(2)}$, где $x \in \{1, \ldots, \varsigma_2\}$.

Шаг 14–16. В случае, если многомерный массив ЦД / ЦДИ $\boldsymbol{D}_{1\ldots n}^{\delta(t_0,\ldots,\tau)}$ состоит из *n* документов, корневая сигнатура $B^{\delta(t_i)**}$ будет повторно формироваться в ходе выполнения операции криптографического преобразования с использованием ключей $v_x^{\delta(2)} \in V_U^{\delta(2)}$ ($V_U = V_U^*$), где $x \in \{1, \ldots, \varsigma_2\}$ над сигнатурой многомерного массива ЦД / ЦДИ за предыдущий момент времени $B^{\delta(t_{i-1})**}$.

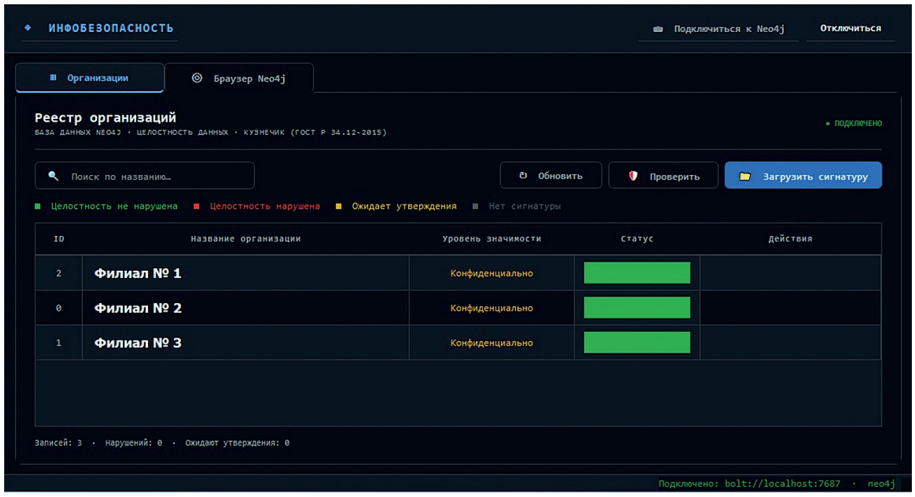


Рис. 4. Главное диалоговое окно программы

После этого выполняются операции конкатенации и криптографического преобразования над преобразованной сигнатурой многомерной структуры ЦД / ЦДИ за предыдущий момент времени $\hat{B}^{\delta(t_{i-1})**}$ и общей сигнатурой $S_j^{\delta(t_i)**}$ ЦД / ЦДИ за текущий момент времени с использованием ключей $v_x^{\delta(2)} \in V_U^{\delta(2)}$, где $x \in \{1, \dots, \varsigma_2\}$.

Шаг 17–18. В случае повторного выполнения операций вычисления сигнатур на серверах нижестоящего уровня, полученный результат $B^{\delta(t_i)**}$ отправляется в подсистему защиты информации, размещенную на сервере вышестоящего уровня, где над ним в целях повторного вычисления сигнатуры контроля целостности массива ЦД / ЦДИ уровня δ производится операция криптографического преобразования с использованием ключей вышестоящего уровня $v_x^{\delta+1(2)} \in V_U^{\delta+1(2)}$.

Шаг 19–20. В случае повторного выполнения операций вычисления сигнатур на сервере максимального уровня полученный результат $B^{\delta(t_i)**}$ подлежит хранению в подсистеме защиты информации, размещенной на этом же сервере, где над ним в целях повторного вычисления сигнатуры контроля целостности массива ЦД / ЦДИ максимального уровня δ производится операция криптографического преобразования с использованием вырабатываемых им ключей $v_x^{\delta(2)} \in V_U^{\delta(2)}$.

Выгрузка сигнатур контроля целостности массивов ЦД / ЦДИ $\xi^{\delta(t_i)*}$, прошедших процедуру хранения, из доверенной среды.

Шаг 21–24. Процедура сравнения повторно вычисленных сигнатур контроля целостности массивов ЦД / ЦДИ $\xi^{\delta(t_i)**}$ за все моменты времени $t_0, t_1, \dots, t_\tau$ их жизненного цикла, с сигнатурами контроля целостности массивов ЦД / ЦДИ $\xi^{\delta(t_i)*}$, прошедших процедуру хранения, в целях локализации нарушения целостности конкретного массива ЦД / ЦДИ. В результате сравнения делается заключение, какой из массивов ЦД / ЦДИ $\boldsymbol{D}_{1\dots n}^{\delta(t_{0,\dots,\tau})}$ был изменен.

Шаг 25. Процедура вывода многомерных массивов $\boldsymbol{D}_{1\dots n}^{\delta(t_{0,\dots,\tau})'}$ ЦД / ЦДИ, прошедших процедуру проверки, в среду обработки.

Программная реализация разработанного комплекса алгоритмов

Разработанные алгоритмы позволяют обеспечить интегративную целостность ЭлД (шаг 4–11 алгоритма № 1), а также контроль целостности многомерной структуры ЭлД (шаг 12–16 алгоритма № 2). Эти функции были реализованы в программном виде [13, 14]. Однако, предыдущие решения не учитывают процесс формирования сигнатур контроля целостности массивов ЦД / ЦДИ $\xi^{\delta(t_i)}$ и сравнение текущих значений со значениями, хранимыми в доверенной среде для проверки целостности системы. В целях практической реализации данного процесса разработано программное решение [15], экранные формы которого представлены на рис. 4–9.

Для загрузки сигнатур контроля целостности массивов ЦД / ЦДИ $\xi^{\delta(t_i)*}$ пользователю необходимо нажать кнопку «Загрузить сигнатуру». В открывшемся диалоговом окне (рис. 5) добавить файлы, полученные от предприятий нижнего организационного уровня и содержащие сигнатуры контроля целостности, а также указать криптографический ключ, предназначенный для их преобразования. После нажатия кнопки «Загрузить» преобразованные сигнатуры сохраняются в графовой базе данных Neo4j.

В случае повторной загрузки сигнатуры контроля целостности пользователь утверждает ее

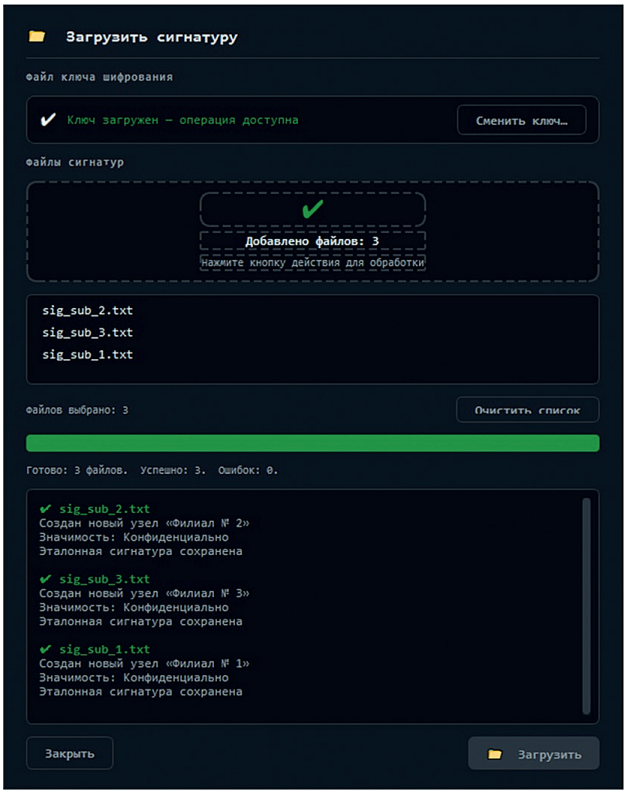


Рис. 5. Экранная форма загрузки сигнатур контроля целостности

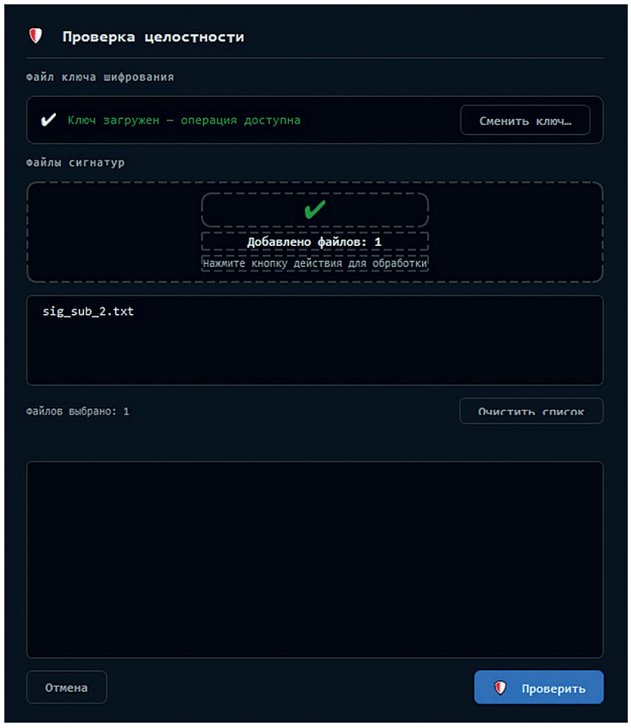


Рис. 7. Экранная форма проверки целостности многомерных массивов ЦД / ЦДИ, обрабатываемых в структурных организациях

новое значение для внесения изменений в базу данных (рис. 6).

Для проверки целостности многомерных массивов ЦД / ЦДИ, обрабатываемых в организациях нижнего организационного уровня, необходимо нажать кнопку «Проверить», после чего во всплывающей форме (рис. 7) указать проверяемые сигнатуры и криптографический ключ, с применением которого они были преобразованы перед сохранением в базе данных. Далее нажать кнопку «Проверить».

Результаты проверки представлены на рисунках 8–9.

Предполагается, что представленное программное решение найдет свое применение в перспективных СЭД в целях обеспечения целостности обрабатываемых массивов информации.

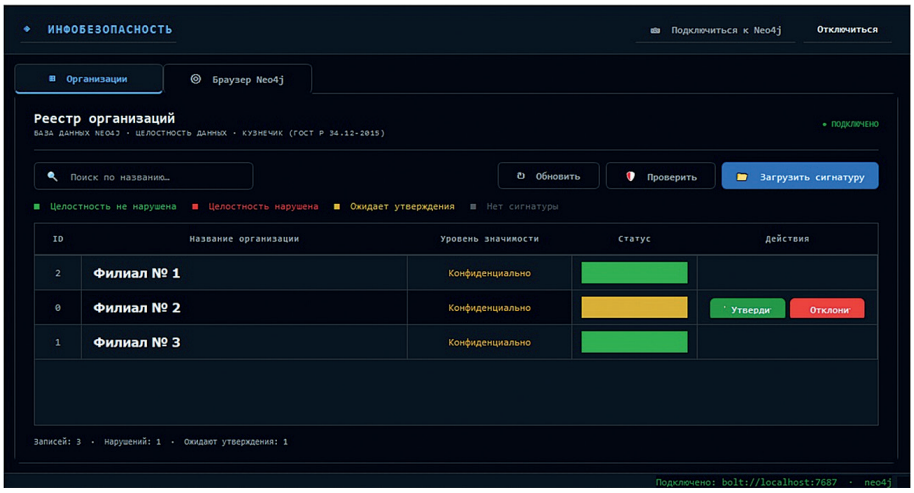
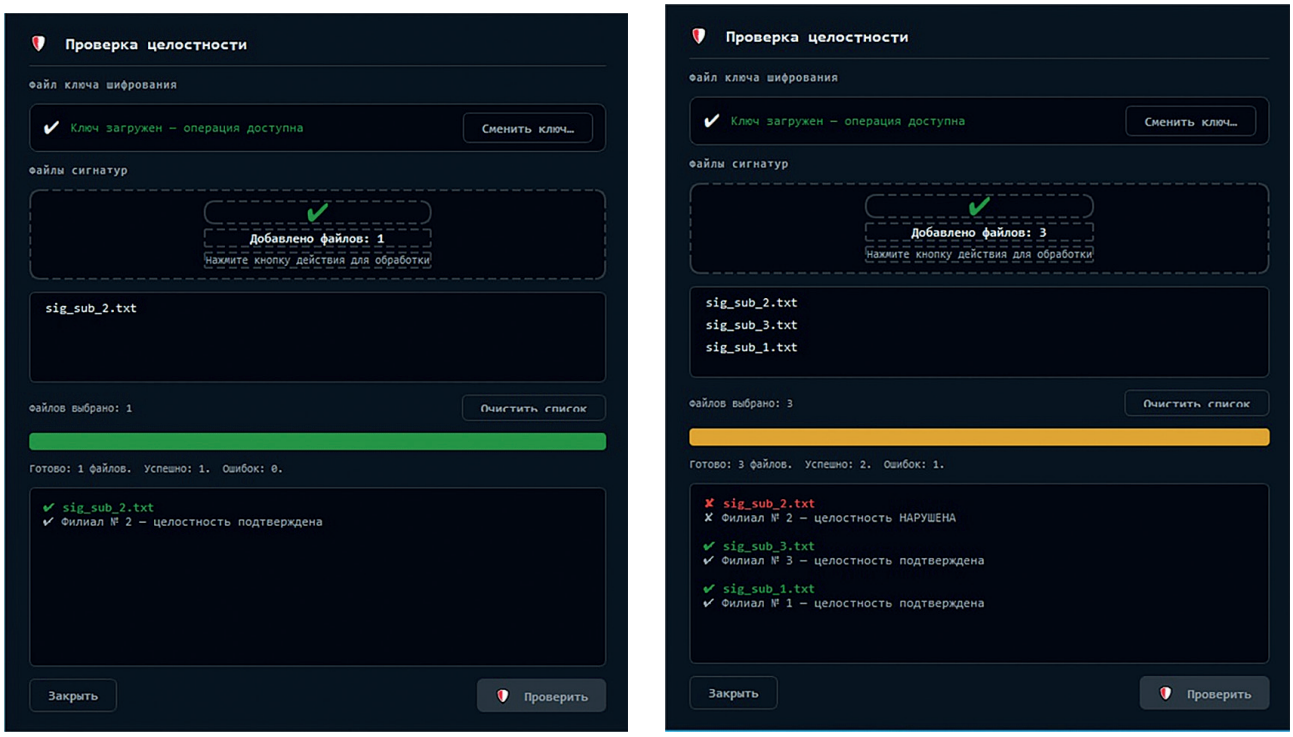


Рис. 6. Экранная форма в случае повторной загрузки сигнатуры контроля целостности



а) *б)*

Рис. 8. Заключение о состоянии обрабатываемых многомерных массивов ЦД / ЦДИ: а) при отсутствии нарушений целостности; б) при наличии нарушений целостности

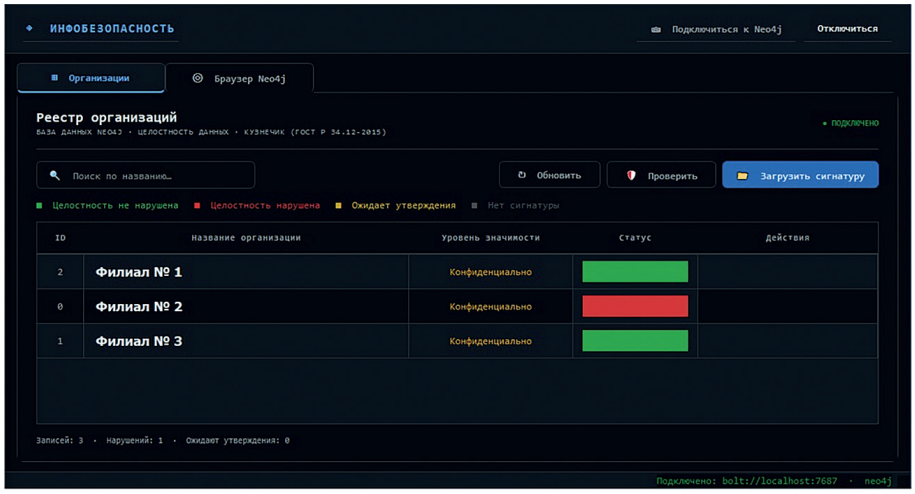


Рис. 9. Главное диалоговое окно программы при наличии элементов с нарушением целостности

Оценка полученных результатов и выводы

Воспользуемся логико-вероятностным методом (ЛВМ) [16-21] для сравнения уровня защищенности распределенной СЭД, обеспечиваемого за счет использования разработанного решения [15], с прототипом, в качестве которого выступает распределенная СЭД с «линейной» процедурой[17] контроля целостности массива ЦД / ЦДИ, осуществляемой внутри каждого уровня независимо от вышестоящего.

17 Месарович М. Д., Мако Д., Такахара И. Теория иерархических многоуровневых систем // М.: Мир, 1973. – 344 с.

В целях моделирования процесса функционирования распределенной СЭД с «линейной» процедурой контроля целостности массива ЦД / ЦДИ, построим один из возможных сценариев ее перехода в опасное состояние (нарушение целостности) в результате успешной реализации УБИ злоумышленником (рис. 10). В этом случае функционирование распределенной СЭД будет нарушено при условии одновременной компрометация ключей: $v_x^{\delta(1)} \in V_U^{\delta(1)}$, $v_x^{\delta(2)} \in V_U^{\delta(2)}$, $v_x^{\delta(3)} \in V_U^{\delta(3)}$, вырабатываемых сервером одного из трех уровней.

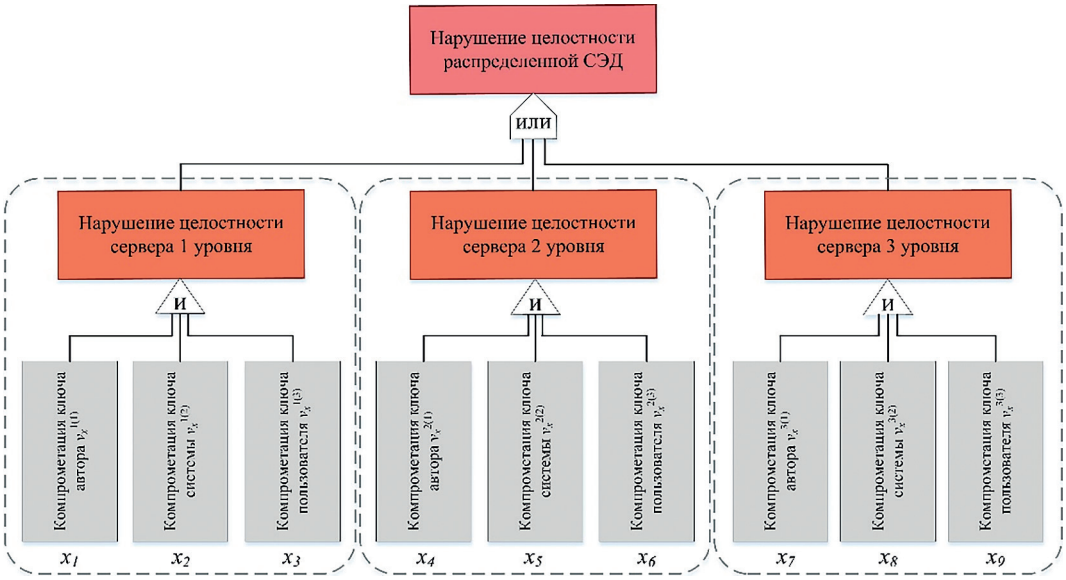


Рис. 10. Сценарий реализации угрозы нарушения функционирования распределенной СЭД при осуществлении «линейной» процедуры контроля целостности массива ЦД / ЦДИ

Рассматриваемому сценарию будет соответствовать следующая ФАЛ, описывающая функцию перехода распределенной СЭД в опасное состояние:

$$f(x_1, \dots, x_9) = \\ = (x_1 \wedge x_2 \wedge x_3) \vee (x_4 \wedge x_5 \wedge x_6) \vee (x_7 \wedge x_8 \wedge x_9). \quad (2)$$

В соответствии с ЛВМ преобразуем полученную ФАЛ (2) в форму перехода к полному замещению, допускающую замену логических переменных соответствующими вероятностями. Для этого представим рассматриваемую функцию в виде СДНФ. Затем осуществим переход от логической функции к ее вероятностной интерпретации. При этом каждая буква заменяется вероятностью ее равенства единице: $P\{x_r = 1\} = R_r$, $P\{x_r = 0\} = P\{\bar{x}_r = 1\} = Q_r = 1 - R_r$, где R_r – вероятность наступления события x_r.

Принимая во внимание отсутствие статистических данных и, как следствие, допущение о том, что все события равновероятны, получим следующий полином, определяющий вероятность перехода распределенной СЭД в опасное состояние[18]:

$$P^{f(x_1, \dots, x_9) = 1} = R^9 - 3R^6 + 3R^3. \quad (3)$$

18 Рябинин И. А. Надежность и безопасность структурно-сложных систем // СПб.: Политехника, 2012. – 276 с.

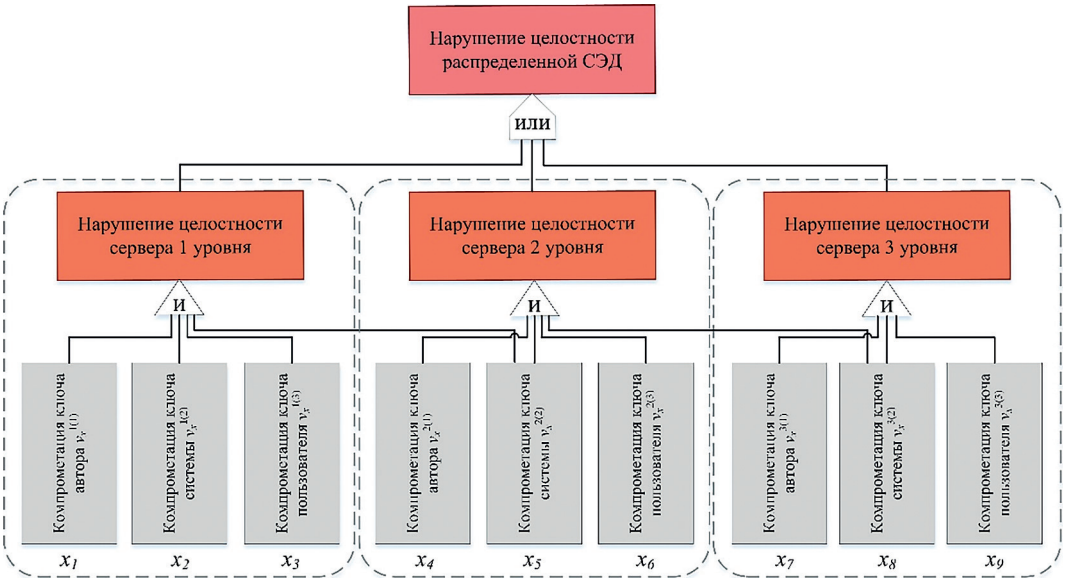


Рис. 11. Сценарий реализации угрозы нарушения функционирования распределенной СЭД с учетом разработанного программного решения

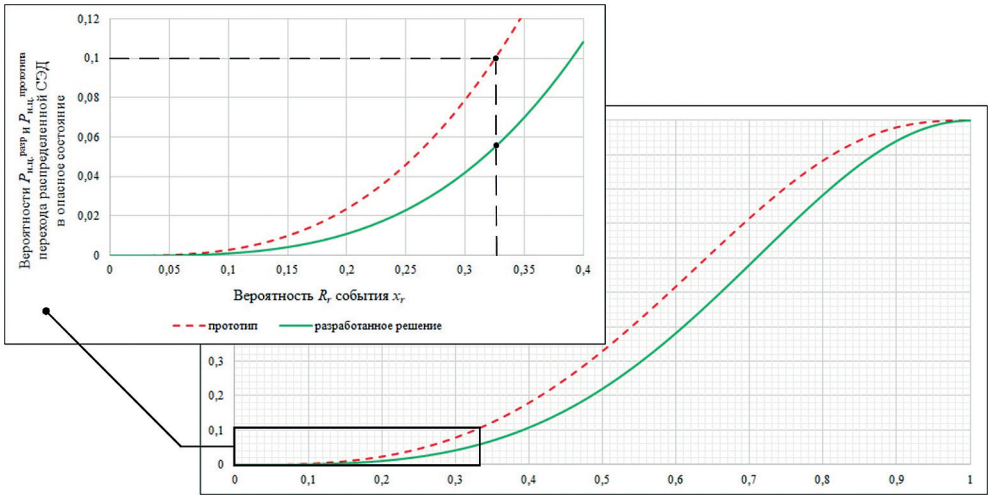


Рис. 12. Сравнительный анализ зависимостей вероятности перехода распределенной СЭД в опасное состояние в результате реализации угрозы компрометации ключей подписи

Далее на основе ЛВМ построим сценарий реализации угрозы нарушения функционирования распределенной СЭД с учетом разработанного решения (рис. 11). В этом случае функционирование распределенной СЭД будет нарушено при одновременной компрометации ключей: $v_x^{\delta(1)} \in V_U^{\delta(1)}$, $v_x^{\delta(2)} \in V_U^{\delta(2)}$, $v_x^{\delta(3)} \in V_U^{\delta(3)}$, вырабатываемых сервером одного из трех уровней, а также ключа $v_x^{\delta+1(2)} \in V_U^{\delta+1(2)}$, вырабатываемого сервером вышестоящего уровня.

При условии, что все события равновероятны, получим следующий полином, определяющий вероятность перехода распределенной СЭД в опасное состояние:

$$P^{f(x_1, \ldots, x_9)\,9} - 2R^7 - R^6 + 2R^4 + R^3. \quad (4)$$

На основе (3) и (4) построим графики зависимостей вероятностей $P_{н.ц.}^{разр.}$ и $P_{н.ц.}^{прототипа}$ перехода распределенной СЭД в опасное состояние в результате реализации угрозы компрометации ключей подписи с учетом «линейной» процедуры контроля целостности массива ЦД / ЦДИ, осуществляемой внутри каждого уровня независимо от вышестоящего, и разработанного решения (рис. 12).

Рассчитаем выигрыш разработанного решения [15] в сравнении с использованием «линейной» процедуры контроля целостности массива ЦД / ЦДИ, осуществляемой внутри каждого уровня независимо от вышестоящего:

$$Ср.\ выигрыш = \left(1 - \frac{\int_0^{0,33} P_{н.ц.}^{разр.} dR}{\int_0^{0,33} P_{н.ц.}^{прототипа} dR}\right) \cdot 100\ \%. \quad (5)$$

Расчет выигрыша производился на практически значимом интервале вероятности перехода распределенной СЭД в опасное состояние (0; ...; 0,1), так как при переходе за его пределы события x_r будет считаться реализованными, а распределенная СЭД перейдет в опасное состояние (средний выигрыш составил ≈ 49 % при $R \approx 0{,}33$).

Полученные результаты свидетельствуют о достижении критерия (1), а применение разработанного решения позволяет повысить уровень защищенности распределенных СЭД за счет снижения вероятности нарушения целостности их структурных уровней. Достоверность полученных результатов определяется использованием апробированного математического аппарата логико-вероятностного метода.

Предполагается, что предлагаемый комплекс алгоритмов и представленная программная модель могут послужить основой для разработки протоколов функционирования существующих и перспективных СЭД.

Литература

1. Ларин М. В. Цифровая трансформация управления документами // В сборнике: «Генеральный регламент»: 300 лет на службе России: От коллежского делопроизводства до цифровой трансформации управления документами. Материалы Международной научно-практической конференции. Российский государственный гуманитарный университет, Историко-архивный институт, Факультет архивоведения и документоведения, Кафедра автоматизированных систем документационного обеспечения управления, Российское общество историков-архивистов (РОИА). Москва, 2021. – С. 10–19.
2. Ларин М. В. Документоведение в цифровую эпоху // В сборнике: Пичетовские чтения – 2024. История: наука, образование, память. Материалы международной научно-практической конференции, посвященной 90-летию исторического факультета Белорусского государственного университета. Минск, 2024. – С. 16–22.
3. Doosti M. Unclonability and Quantum Cryptanalysis: From Foundations to Applications // Laboratory for Foundations of Computer Science. School of Informatics. University of Edinburgh, 2022. – P. 341.
4. Veda Chatiyode, Baghavathi Priya S. Cryptanalysis of post-quantum cryptographic schemes: securing IoT and smart cities in the quantum era // In book: Post-Quantum cryptography and IoT communications for sustainable urban development. 2025. – Pp. 171–204.
5. Xie H., Xia Q., Wang K., Li Y., Yang L. Quantum automated tools for finding impossible differentials // Mathematics, 2024. – № 12, 2598. – URL: doi.org/10.3390/math12162598.
6. Blessing Guembe, Ambrose Azeta, Sanjay Misra, Victor Chukwudi Osamor, Luis Fernandez-Sanz & Vera Pospelova (2022) // The Emerging Threat of Ai-driven Cyber Attacks: A Review, Applied Artificial Intelligence, 36:1, 2037254, DOI: 10.1080/08839514.2022.2037254.
7. Тали Д. И., Финько О. А. Концептуальная модель функционирования системы цифрового документооборота в рамках парадигмы «Индустрия 4.0» // Вопросы кибербезопасности, 2025. – № 5 (69). – С. 68–77. – DOI 10.21681/2311-3456-2025-5-68-77.
8. Саяркин В. А., Михайличенко А. В., Паращук И. Б. Вопросы формулировки комплексных показателей надежности и защищенности системы электронного документооборота на базе распределенной сети мобильных дата-центров // В сборнике: «Проблемы технического обеспечения войск в современных условиях. Труды VII межвузовской научно-практической конференции». Санкт-Петербург, 2022. – С. 210–214.
9. Das M., Tao X., Cheng J.C.P. A Secure and Distributed Construction Document Management System Using Blockchain // In book: Proceedings of the 18th International Conference on Computing in Civil and Building Engineering, 2021. – P. 850–862. – DOI:10.1007/978-3-030-51295-8_59.
10. Тали Д. И., Финько О. А. и др Способ обеспечения интегративной целостности электронного документа // Патент на изобретение RU 2812304, опубл. 29.01.2024, бюл. № 4.
11. Тали Д. И., Финько О. А., Диченко С. А. Способ формирования и контроля целостности многомерной структуры электронных документов // Патент на изобретение RU 2840783, опубл. 28.05.2025, бюл. № 16.
12. Тали Д. И., Финько О. А. Способ и система распределенного контроля целостности электронных документов при вероятной компрометации ключей подписи // Патент на изобретение RU 2844401, опубл. 29.07.2025, бюл. № 22.
13. Пешнин М. А., Васильев Я. А., Тали Д. И. Алгоритмическое обеспечение интегративной целостности электронных документов, обрабатываемых системами электронного документооборота // Защита информации. Инсайд, 2025. – № 6 (126). – С. 38–44.
14. Пешнин М. А., Васильев Я. А., Тали Д. И. Программная модель контроля целостности многомерных массивов электронных документов // Свидетельство о государственной регистрации программы для ЭВМ RU 2025697115, опубл. 23.12.2025.
15. Пешнин М. А., Васильев Я. А., Тали Д. И. Программная модель многоуровневого контроля целостности многомерных массивов электронных документов // Свидетельство о государственной регистрации программы для ЭВМ RU 2026665081, опубл. 20.05.2026.
16. Калашников А. О., Аникина Е. В., Бугайский К. А., Молотов А. А. Применение логико-вероятностного метода в информационной безопасности. Часть 6 // Вопросы кибербезопасности, 2025. – № 1 (65). – С. 96–107. – DOI: 10.21681/2311-3456-2025-1-96-107.
17. Калашников А. О., Аникина Е. В., Бугайский К. А. Применение логико-вероятностного метода в информационной безопасности. Часть 7 // Вопросы кибербезопасности, 2026. – № 1 (71). – С. 59–68. – DOI: 10.21681/2311-3456-2026-1-59-68.
18. Попков Г. В., Гумиров В. Ш., Гумиров А. В., Овчинникова Е. А. К вопросу применения логико-вероятностных методов для реализации систем поддержки, принятия решений в области кибербезопасности // Телекоммуникации, 2025. – № 2. – С. 32–39.
19. Крюкова Е. С., Ткаченко В. В., Михайличенко А. В., Паращук И. Б. Вопросы оценки надежности современных систем хранения данных для мобильных дата-центров // Наукоемкие технологии в космических исследованиях Земли, 2021. – Т. 13. – № 5. – С. 86–95.
20. Демин А. В. Глубокое обучение адаптивных систем управления на основе логико-вероятностного подхода // Известия Иркутского государственного университета. Серия: Математика, 2021. – Т 38. – С. 65– 83. – DOI: https://doi.org/10.26516/1997-7670.2021.38.65
21. Викторова В. С., Степанянц А. С. Вычисление показателей надежности в немонотонных логико-вероятностных моделях многоуровневых систем // Автоматика и телемеханика, 2021. – № 5. – С. 106–123. – DOI: 10.31857/S000523102105007X.

MULTI-LEVEL INTEGRITY CONTROL ALGORITHMS FOR ELECTRONIC DOCUMENTS IN DISTRIBUTED ELECTRONIC DOCUMENT MANAGEMENT SYSTEMS

Vasiliev Y. A.[19], Peshnin M. A.[20], Tali D. I.[21], Zakharov I. L.[22]

Keywords: *digitalization, digital transformation of document management, digital document, integrity of electronic document, integrity of system, distributed electronic document management systems.*

Abstract

The purpose *of the article is to develop algorithms for the preparation and implementation of multi-level integrity control of electronic documents processed by distributed electronic document management systems under the conditions of destructive influences of intruders.*

Research method: *to achieve this goal, a hierarchical approach to algorithmic design of the process of preparing and verifying the integrity of multi-level, structurally complex systems was used, using electronic document management as an example. I. A. Ryabinin's logical-probabilistic method was used to evaluate the obtained results.*

Research results: *a set of algorithms for multi-level integrity control of electronic documents processed by distributed electronic document management systems, as well as its software implementation, are proposed. A numerical evaluation of the research results revealed the advantage of the developed solution over existing approaches, resulting in increased security of the studied systems by ensuring the integrity of their structural levels through the detection and localization of electronic documents and their components that have been subject to unauthorized modification due to the potential compromise of signature keys. This result is achieved by applying cryptographic transformations to components (content and metadata) of electronic documents based on the non-binary Merkle tree principle in combination with chain-based data recording technology.*

The practical value *of the developed solution lies in the hierarchical application of signature and verification keys generated by a higher-level server to electronic documents generated on a lower-level server, which allows for an increased level of security for distributed electronic document management systems in the face of destructive attacks from intruders (internal and external) in the event of a possible compromise of signature keys.*

Contribution of the authors: *Vasiliev Ya. A. – development of a software model for multi-level control of the integrity of electronic documents processed by a distributed electronic document management system; Peshnin M. A. – development of algorithms for the preparation and implementation of multi-level integrity control of electronic documents processed by a distributed electronic document management system; Tali D. I. – development of the idea, control and correction of results, general management; Zakharov I. L. – verification (evaluation) of the obtained results.*

References

1. Larin M.V. Tsifrovaya transformatsiya upravleniya dokumentami // V sbornike: «General'nyy reglament»: 300 let na sluzhbe Rossii: Ot kollezhskogo deloproizvodstva do tsifrovoy transformatsii upravleniya dokumentami. Materialy Mezhdunarodnoy nauchno-prakticheskoy konferentsii. Rossiyskiy gosudarstvennyy gumanitarnyy universitet, Istoriko-arkhivnyy institut, Fakul'tet arkhivovedeniya i dokumentovedeniya, Kafedra avtomatizirovannykh sistem dokumentatsionnogo obespecheniya upravleniya, Rossiyskoye obshchestvo istorikov-arkhivistov (ROIA). M.:, 2021. – Pp. 10–19.
2. Larin M. V. Dokumentovedeniye v tsifrovuyu epokhu // V sbornike: Pichetovskiye chteniya – 2024. Istoriya: nauka, obrazovaniye, pamyat'. Materialy mezhdunarodnoy nauchno-prakticheskoy konferentsii, posvyashchennoy 90-letiyu istoricheskogo fakul'teta Belorusskogo gosudarstvennogo universiteta. Minsk, 2024. – Pp. 16–22.
3. Doosti M. Unclonability and Quantum Cryptanalysis: From Foundations to Applications // Laboratory for Foundations of Computer Science. School of Informatics. University of Edinburgh, 2022. – P. 341.
4. Veda Chatiyode, Baghavathi Priya S. Cryptanalysis of post-quantum cryptographic schemes: securing IoT and smart cities in the quantum era // In book: Post-Quantum cryptography and IoT communications for sustainable urban development, 2025. Pp. 171–204.
5. Xie H., Xia Q., Wang K., Li Y., Yang L. Quantum automated tools for finding impossible differentials // Mathematics, 2024. – No 12, 2598. – URL: doi.org/10.3390/math12162598.
6. Blessing Guembe, Ambrose Azeta, Sanjay Misra, Victor Chukwudi Osamor, Luis Fernandez-Sanz & Vera Pospelova (2022) // The Emerging Threat of Ai-driven Cyber Attacks: A Review, Applied Artificial Intelligence, 36:1, 2037254, DOI: 10.1080/08839514.2022.2037254.

19 ***Yaroslav A. Vasiliev***, employee of the Krasnodar Higher Military School named after General of the Army S. M. Shtemenko, Krasnodar, Russia. E-mail: yawasilevs@mail.ru

20 ***Makar A. Peshnin***, employee of the Krasnodar Higher Military School named after General of the Army S. M. Shtemenko, Krasnodar, Russia. E-mail: m.peshnin@yandex.ru

21 ***Dmitry I. Tali***, Ph.D. of Technical Sciences, doctoral student of the special department of the Krasnodar Higher Military School named after General of the Army S. M. Shtemenko, Krasnodar, Russia. E-mail: dimatali@mail.ru

22 ***Ivan L. Zakharov***, Ph.D. of Technical Sciences, Senior Lecturer of the Special Department of the Krasnodar Higher Military School named after General of the Army S. M. Shtemenko, Krasnodar, Russia. E-mail: zakharovivanl@yandex.ru

7. Tali D. I., Fin'ko O. A. Kontseptual'naya model' funktsionirovaniya sistemy tsifrovogo dokumentooborota v ramkakh paradigmy «Industriya 4.0» // Voprosy kiberbezopasnosti, 2025. – No 5 (69). – Pp. 68–77. – DOI: 10.21681/2311-3456-2025-5-68-77.
8. Sayarkin V. A., Mikhaylichenko A. V., Parashchuk I. B. Voprosy formulirovki kompleksnykh pokazateley nadezhnosti i zashchishchennosti sistemy elektronnogo dokumentooborota na baze raspredelennoy seti mobil'nykh data-tsentrov // V sbornike: «Problemy tekhnicheskogo obespecheniya voysk v sovremennykh usloviyakh. Trudy VII mezhvuzovskoy nauchno-prakticheskoy konferentsii». Sankt-Peterburg, 2022. – Pp. 210–214.
9. Das M., Tao X., Cheng J. C. P. A Secure and Distributed Construction Document Management System Using Blockchain // In book: Proceedings of the 18th International Conference on Computing in Civil and Building Engineering, 2021. – Pp. 850–862. – DOI:10.1007/978-3-030-51295-8_59.
10. Tali D. I., Fin'ko O. A. i dr. Sposob obespecheniya integrativnoy tselostnosti elektronnogo dokumenta // Patent na izobreteniye RU 2812304, opubl. 29.01.2024, byul. No 4.
11. Tali D. I., Fin'ko O. A., Dichenko S. A. Sposob formirovaniya i kontrolya tselostnosti mnogomernoy struktury elektronnykh dokumentov // Patent na izobreteniye RU 2840783, opubl. 28.05.2025, byul. No 16.
12. Tali D. I., Fin'ko O. A. Sposob i sistema raspredelennogo kontrolya tselostnosti elektronnykh dokumentov pri veroyatnoy komprometatsii klyuchey podpisi // Patent na izobreteniye RU 2844401, opubl. 29.07.2025, byul. No 22.
13. Peshnin M. A., Vasil'yev Ya. A., Tali D. I. Algoritmicheskoye obespecheniye integrativnoy tselostnosti elektronnykh dokumentov, obrabatyvayemykh sistemami elektronnogo dokumentooborota // Zashchita informatsii. Insayd, 2025. – No 6 (126). – Pp. 38–44.
14. Peshnin M. A., Vasil'yev Ya.A., Tali D. I. Programmnaya model' kontrolya tselostnosti mnogomernykh massivov elektronnykh dokumentov // Svidetel'stvo o gosudarstvennoy registratsii programmy dlya EVM RU 2025697115, opubl. 23.12.2025.
15. Peshnin M. A., Vasil'yev Ya. A., Tali D. I. Programmnaya model' mnogourovnevogo kontrolya tselostnosti mnogomernykh massivov elektronnykh dokumentov // Svidetel'stvo o gosudarstvennoy registratsii programmy dlya EVM RU 2026665081, opubl. 20.05.2026.
16. Kalashnikov A. O., Anikina Ye.V., Bugayskiy K. A., Molotov A. A. Primeneniye logiko-veroyatnostnogo metoda v informatsionnoy bezopasnosti. Chast' 6 // Voprosy kiberbezopasnosti, 2025. – No 1 (65). – Pp. 96–107. DOI: 10.21681/2311-3456-2025-1-96-107.
17. Kalashnikov A. O., Anikina Ye. V., Bugayskiy K. A. Primeneniye logiko-veroyatnostnogo metoda v informatsionnoy bezopasnosti. Chast' 7 // Voprosy kiberbezopasnosti, 2026. – No 1 (71). – Pp. 59–68. – DOI: 10.21681/2311-3456-2026-1-59-68.
18. Popkov G. V., Gumirov V. Sh., Gumirov A. V., Ovchinnikova Ye. A. K voprosu primeneniya logiko-veroyatnostnykh metodov dlya realizatsii sistem podderzhki, prinyatiya resheniy v oblasti kiberbezopasnosti // Telekommunikatsii, 2025. – No 2. – Pp. 32–39.
19. Kryukova Ye. S., Tkachenko V. V., Mikhaylichenko A. V., Parashchuk I. B. Voprosy otsenki nadezhnosti sovremennykh sistem khraneniya dannykh dlya mobil'nykh data-tsentrov // Naukoyemkiye tekhnologii v kosmicheskikh issledovaniyakh Zemli, 2021. – V. 13. – No 5. – Pp. 86–95.
20. Demin A. V. Glubokoye obucheniye adaptivnykh sistem upravleniya na osnove logiko-veroyatnostnogo podkhoda // Izvestiya Irkutskogo gosudarstvennogo universiteta. Seriya: Matematika, 2021. – V. 38. – Pp. 65–83. DOI: https://doi.org/10.26516/1997-7670.2021.38.65.
21. Viktorova V. S., Stepanyants A. S. Vychisleniye pokazateley nadezhnosti v nemonotonnykh logiko-veroyatnostnykh modelyakh mnogourovnevykh sistem // Avtomatika i telemekhanika, 2021. – No 5. – Pp. 106–123. DOI: 10.31857/S000523102105007X .

ПРЕДЛОЖЕНИЯ ПО ПОСТРОЕНИЮ ПОДСИСТЕМЫ УПРАВЛЕНИЯ СЕТИ ПЕРЕДАЧИ ДАННЫХ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

Шинкарев С. А.[1], Волошенюк А. С.[2], Коваленко Е. С.[3]

DOI:10.21681/3034-4050-2026-4-38-41

Ключевые слова: *программно-конфигурируемые сети, структура сети связи, кондиционное остовное дерево, контроллер.*

Аннотация

В статье представлено описание структуры сети передачи данных специального назначения как программно-конфигурируемой сети, рассмотрены основные принципы построения подсистемы управления. Также приведены решения оптимального построения подсистемы управления с учетом предъявляемых требований с использованием алгоритма определения рационального размещения контроллера в подсистеме, а также предложения по нахождению сетки линий, соединяющей контроллер со всеми сетевыми элементами.

Цель работы *состоит в предложении порядка нахождения оптимального построения подсистемы управления сети передачи данных специального назначения.*

Результаты исследования: *алгоритм определения рационального размещения контроллера в подсистеме управления, предложения по определению оптимальной сетки линий, соединяющей контроллер со всеми сетевыми элементами.*

Научная новизна: *представлен алгоритм определения рационального размещения контроллера в подсистеме управления, а также предложены решения по нахождению сетки линий, соединяющей контроллер со всеми элементами сети.*

Введение

К числу основных задач, направленных на развитие сетей передачи данных специального назначения, относится совершенствование методов построения подсистемы управления для обеспечения устойчивого информационного обмена в сложных условиях функционирования сети. Существующие принципы построения, предполагающие децентрализованное управление сетью, не позволяют в заданной мере наращивать производительность и пропускную способность сети. Указанное обстоятельство обусловлено возрастанием временных затрат на процессы маршрутизации, усложнением процедур конфигурирования сетевой структуры и управления потоками данных, а также необходимостью реализации современных политик качества обслуживания в высокоскоростных глобальных сетях и сетях центров обработки данных. Дополнительным фактором выступает возрастающая потребность в виртуализации сетей. Вследствие этого возникает необходимость разработки и внедрения новых концептуальных подходов к построению подсистемы управления инфотелекоммуникационных сетей в целом и сетей передачи данных в частности.

Основная часть

Под сетью передачи данных (СПД) специального назначения будет пониматься часть сети связи, выполняющая передачу сообщений, команд и сигналов управления, подтверждений, донесений и неформализованной информации в автоматизированных системах управления, при отсутствии функций содержательной обработки передаваемой информации. Структурно сеть передачи данных представляет собой совокупность узлов связи и каналов электросвязи, дополненную обеспечивающими подсистемами переноса данных, восстановления, сигнализации, синхронизации, коммутации и управления.

Переход на концепцию программно-конфигурируемых сетей предполагает формирование архитектуры сети, в рамках которой уровень управления (УУ) (состоянием сетевой инфраструктуры и потоками данных в сети) и уровень передачи данных (УПД) разделяются посредством переноса управляющих функций, традиционно реализуемых маршрутизаторами и коммутаторами, на специализированное централизованное устройство – контроллер [1, 2]. В результате подобного разделения обеспечивается логическая централизация процессов

1 ***Шинкарев Семен Александрович***, кандидат технических наук, доцент, профессор кафедры Автоматизированных систем управления Военной академии связи, г. Санкт-Петербург, Россия. E-mail: se_men82@mail.ru

2 ***Волошенюк Анастасия Сергеевна***, курсант 4 курса Военной академии связи, г. Санкт-Петербург, Россия. E-mail: voloshenuk2004@gmail.com

3 ***Коваленко Елизавета Сергеевна***, курсант 4 курса Военной академии связи, г. Санкт-Петербург, Россия. E-mail: elizavetka_zubtsova@mail.ru

мониторинга состояния сети и управления потоками данных. Кроме того, применение данного подхода позволяет абстрагировать уровень управления от физической инфраструктуры уровня передачи данных за счёт использования логического представления сети.

Подсистема управления сетью передачи данных специального назначения, являясь составной частью общей сетевой инфраструктуры, реализует три базовые функции: сбор информации о состоянии сети, её анализ и передачу управляющих воздействий элементам сети [3].

В связи с этим подсистему управления можно представить в виде структуры, включающую в себя все элементы сети (вершины графа) и соединяющие определенным образом их линии. При этом на множестве сетевых элементов должны быть определены место размещения контроллера (контроллеров), имеющего либо прямую, либо составную линию до каждого сетевого устройства. Место размещения контролера должно быть оптимальным и удовлетворять следующему условию – расстояние от контроллера до всех сетевых элементов должно быть минимальным. Сетка линий подсистемы управления СПД, построенная от контролера, должна быть минимальной (ранг пути от контроллера до сетевого элемента).

Задачу определения местоположения контролера подсистемы управления СПД можно сформулировать, как задачу нахождения центра графа.

Для дальнейшего исследования вводятся следующие понятия [4]:

Эксцентриситет $e(a_i)$ вершины связного графа $G(A,B)$ определяется как максимальное расстояние от рассматриваемой вершины до остальных вершин графа: $\max\{l(a_i,a_j)\}$;

Радиус графа $r(G)$ представляет собой минимальное значение эксцентриситета среди всех вершин.

Центральной вершиной графа называется вершина (a_i), эксцентриситет которой равен радиусу графа: $e(a_i) = r(G)$, $a_i \in A$.

Дополнительно вводится множество всех вершин, расстояние от a_i до которых не больше $\lambda: N_\lambda^0(a_i) = \{a_i | l_{ij} \le \lambda,\ a_i \in A\}$. Для каждой вершины определяется $C_0(a_i) = \max(l_{ij})$, $a_i \in A$; Пусть λ_0 – минимальное значение λ такое, что для некоторой вершины $a_i: N_\lambda^0(a_i) = A$, то есть длина пути от a_i до любой вершины графа не превосходит λ_0. Тогда $C_0(a_i) = \lambda_0$. Вершина a_0^* такая, что $C_0(a_0^*) = \min[N_0(a_i)]$, $a_0^* \in A$ является центром графа $G(A,B)$.

Для нахождения центра графа формируется матрица кратчайших путей $L_{n\times n}$ (n – мощность множества A), где $l_{ij} = l(i,j)$. Построение указанной матрицы может быть реализовано, например, с использованием алгоритма Флойда–Уоршелла [5]. Далее для каждой строки матрицы определяется максимальное значение расстояния до остальных вершин, в результате чего формируется массив эксцентриситетов длины n. Минимальный элемент данного массива соответствует центру графа. В случае, когда этих вершин несколько, все они могут являться центром графа.

Одним из возможных способов формирования сетки линий подсистемы управления является построение остовных деревьев от всех вершин графа с последующей интеграцией полученных структур и оптимизацией итоговой конфигурации.

В настоящее время существует ряд алгоритмов, предназначенных для построения остовных деревьев. Наиболее распространёнными являются алгоритмы Прима, Краскала и протокол STP (Spanning Tree Protocol), использующиеся для формирования остовного дерева с минимальной протяжённостью сетки линий. Кроме того, применяется алгоритм, основанный на теореме О. Б. Лупанова, позволяющий осуществлять нахождение кондиционного остовного дерева.

Алгоритм Краскала основан на сортировке всех возможных связей по стоимости и последовательном добавлении наименее затратных соединений без образования циклов. Такой алгоритм наиболее предпочтителен для разреженных графов, в которых количество рёбер значительно меньше максимального возможного и не эффективен для сетей с частым изменением топологии.

Для работы с полными сетями преимущественно используется алгоритм Прима, основанный на постепенном наращивании сети от центрального узла и выбора на каждом шаге самого выгодного соединения, что отражает его преобладающую эффективность при построении иерархических сетей с центром [6].

Алгоритм, реализованный в протколе STP, способен построить логическую схему сети, аналогичную дереву, с контроллером в центре с задачей предотвратить появление петель, которые могут нарушить сетевой трафик. Использование данного механизма способствует более равномерному распределению потоков данных по доступным маршрутам. При отказе основного пути автоматически активируются ранее заблокированные резервные маршруты, что позволяет сократить время восстановления работоспособности сети [7].

Алгоритм, разработанный на основе теоремы О. Б. Лупанова о разложении булевых функций по переменным, обеспечивает построение

Таблица 1

Сравнительный анализ алгоритмов Прима–Краскала, STP и метода построения кондиционного остовного дерева

	Нахождение кондиционного остовного дерева	Алгоритм Прима–Краскала	STP
Количество уровней иерархии	3	8 (+266 %)	3
Протяженность сетки линий	89	74 (-20 %)	90
Количество «шагов» для построения	3	11 (+366 %)	7 (+233 %)

кондиционного остовного дерева на топологических структурах произвольной размерности. При этом достигается выполнение следующих условий: размещение основного контроллера в вершине иерархии, минимизация ранга остовного дерева, а также сокращение общей протяжённости линий связи между узлами сети [8].

Проведённый сравнительный анализ алгоритмов Прима–Краскала, STP и метода построения кондиционного остовного дерева показал, что наибольшей эффективностью характеризуется алгоритм нахождения кондиционного остовного дерева.

Результаты сравнительного анализа алгоритмов приведен в таблице 1.

Полученные результаты позволяют сделать вывод, что алгоритм построения кондиционного остовного дерева в наибольшей степени удовлетворяет совокупности критериев эффективности. Рассматриваемый метод обеспечивает минимальную глубину иерархической структуры, сравнительно небольшую протяжённость линий связи и минимальное число этапов построения. Несмотря на то, что по показателю протяжённости сетки линий данный алгоритм уступает алгоритмам Прима–Краскала, различие составляет лишь около 20 %, что компенсируется преимуществами по остальным параметрам. Следовательно, алгоритм, основанный на теореме О. Б. Лупанова, может рассматриваться как наиболее рациональный инструмент построения структуры подсистемы управления.

Вывод

Процесс технического проектирования сетей передачи данных представляет собой сложную научно-техническую задачу, базирующуюся на применении положений теории систем, теории графов и методов математического программирования. Особую значимость при проектировании приобретают требования, предъявляемые к подсистеме управления, поскольку именно её параметры в значительной степени определяют эффективность функционирования сети в целом. В работе представлены подходы к нахождению рациональной структуры подсистемы управления сети передачи данных, позволяющие создать необходимые, но недостаточные условия для построения оптимальной подсистемы управления, решающей задачи эффективного функционирования сетей передачи данных специального назначения.

Литература

1. Фёдеров Н.К. Программно-конфигурируемые сети. Проблемы при переходе к сетям ПКС. Научно-образовательный журнал для студентов и преподавателей «StudNet», 2022. – Вып. 4. – С. 3137–3148.
2. Никитин С. В., Лоборчук А. А. Программно-конфигурируемые сети как новый этап развития сетей передачи данных. MEANS OF COMMUNICATION EQUIPMENT, 2023. – Вып. 1. – С. 89–93.
3. Татаринов В. И. Модель системы управления сетью передачи данных специального назначения в условиях компьютерных сетевых атак. Журнал «Известия тульского государственного университета», 2021. – Вып. 8. – С. 33–37.
4. Jernej Azarija, Sandi Klavzar. Moore Graphs and Cycles Are Extremal Graphs for Convex Cycles // Journal of Graphs Theory. – 2015. – Т. 80. – С. 34–42.
5. Блинов И. В., Бугаев Ю. В., Чикунов С. В. Обобщение алгоритма Флойда–Уоршалла на случай нескольких критериев. Вестник ТГТУ, 2009. – № 4. – С. 885–892.
6. Иванова А. П., Сапожников Н. А. Сравнительный анализ алгоритмов Краскала и Прима для графов с различным количеством вершин. Электронный научный журнал «Дневник науки», 2024. – № 12.
7. Макаренко С. И., Михайлов Р. Л. Модель функционирования коммутатора в сети с использованием протокола покрывающего дерева STP и исследование устойчивости сети в условиях ограниченной надёжности каналов связи. Радиотехнические и телекоммуникационные системы, 2013. – Вып. 2. – С. 61–68.
8. Евглевская Н. В., Пак Р. С., Привалов А. А., Хмелляр Н. А., Шинкарев С. А. Алгоритм нахождения кондиционного остовного дерева для передачи сигналов синхронизации на сети связи. Автоматизация процессов управления. – Ульяновск: ФНПЦ АО НПО «Марс». – 2020. – № 2 (60). – С.117–123.

.

PROPOSALS FOR CONSTRUCTING THE CONTROL SUBSYSTEM OF A SPECIAL-PURPOSE DATA TRANSMISSION NETWORK

Shinkarev S. A.[4], Voloshenyuk A. S.[5], Kovalenko E. S.[6]

Keywords: *software-defined networks, communication network architecture, conditional spanning tree, controller.*

Abstract

This article describes the architecture of a special-purpose data transmission network modeled as a software-defined network and outlines the fundamental principles for constructing its control subsystem. It further presents solutions for the optimal design of the control subsystem subject to specified requirements, including an algorithm for determining the rational placement of the controller within the subsystem, as well as proposals for identifying the network topology that connects the controller to all network elements.

Objective: *the objective of this study is to propose a procedure for determining the optimal configuration of the control subsystem of a special-purpose data transmission network.*

Research results: *an algorithm for determining the rational placement of the controller within the control subsystem is developed, along with proposals for defining an optimal network topology that ensures connectivity between the controller and all network elements.*

Scientific novelty: *the study introduces an algorithm for the rational placement of the controller within the control subsystem and proposes solutions for constructing a network topology that connects the controller with all elements of the network.*

References

1. N. K. Fedorov. «Software-Defined Networks: Challenges in the Transition to SDN». StudNet: Research and Educational Journal for Students and Teachers, 2022. – No 4. – Pp. 3137–3148.
2. S. V. Nikitin and A. A. Loborchuk. «Software-Defined Networks as a New Stage in the Development of Data Transmission Networks». Means of Communication Equipment, 2023. – No 1. – Pp. 89–93.
3. V. I. Tatarinov. «A Model of the Control System for a Special-Purpose Data Transmission Network under Computer Network Attacks», Izvestiya of Tula State University, 2021. – No. 8. – Pp. 33–37.
4. J. Azarija and S. Klavžar. «Moore Graphs and Cycles Are Extremal Graphs for Convex Cycles». Journal of Graph Theory, 2015. – Vol. 80. – Pp. 34–42.
5. I. V. Blinov, Yu. V. Bugaev, S. V. Chikunov. «Generalization of the Floyd–Warshall Algorithm for the Multicriteria Case». Vestnik of TSTU, 2009. – No. 4. – Pp. 885–892.
6. A. P. Ivanova, N. A. Sapozhnikov. «Comparative Analysis of Kruskal's and Prim's Algorithms for Graphs with Varying Numbers of Vertices». Science Diary (Electronic Scientific Journal), 2024. – No 12.
7. S. I. Makarenko, R. L. Mikhailov. «A Model of Switch Operation in a Network Using the Spanning Tree Protocol (STP) and an Analysis of Network Stability under Limited Channel Reliability». Radio Engineering and Telecommunication Systems, 2013. – No. 2. – Pp. 61–68.
8. N. V. Evglevskaya, R. S. Pak, A. A. Privalov, N. A. Khmellyar, S. A. Shinkarev. «An Algorithm for Constructing a Conditional Spanning Tree for Synchronization Signal Transmission in Communication Networks». Automation of Control Processes, 2020. – No 2 (60). – Pp. 117–123.

4 ***Semyon A. Shinkarev***, Ph.D. of Technical Sciences, Associate Professor, Professor of the Department of Automated Control Systems of the Military Academy of Communications, St. Petersburg, Russia. E-mail: se_men82@mail.ru

5 ***Anastasia S. Voloshenyuk***, 4th year cadet of the Military Academy of Communications, St. Petersburg, Russia. E-mail: voloshenuk2004@gmail.com

6 ***Elizaveta S. Kovalenko***, 4th year cadet of the Military Academy of Communications, St. Petersburg, Russia. E-mail: elizavetka_zubtsova@mail.ru

ОСОБЕННОСТИ ОБЕСПЕЧЕНИЯ РАЗВЕДЫВАТЕЛЬНОЙ ЗАЩИЩЁННОСТИ И ЖИВУЧЕСТИ ПОЛЕВЫХ УЗЛОВ СВЯЗИ

Медведев А. А.[1], Юров Е. С.[2]

DOI:10.21681/3034-4050-2026-4-42-48

Ключевые слова: *сеть воздушной радиосвязи, резервирование каналов, адаптивное распределение ресурсов, беспилотные авиационные системы.*

Аннотация

Цель исследования: *разработка научно-технического подхода к оценке и повышению разведывательной защищённости и живучести полевого узла связи (ПУС) пункта управления (ПУ) в тактическом звене управления (ТЗУ) с учётом современного характера разведывательно-ударных воздействий.*

Метод исследования: *системный анализ, сравнительный анализ отечественных научных публикаций, элементы теории надёжности и графовых моделей сетей связи, а также сценарный подход к оценке воздействия разведки, радиоэлектронного подавления (РЭП) и физического поражения на направления связи.*

Результат исследования: *уточнены современные угрозы полевым узлам связи, предложена формализованная модель живучести, объединяющая коэффициент готовности направления связи, его структурную связность и вес приоритетности, а также показан пример расчёта интегрального показателя живучести узла связи для многомаршрутной структуры.*

Научная новизна: *состоит в увязке разведывательной защищённости, многомаршрутной связности и временных параметров восстановления в едином расчётном показателе, пригодном для последующего использования при адаптивном распределении ограниченных ресурсов сети воздушной радиосвязи.*

Введение

Опыт современных вооружённых конфликтов показывает, что устойчивость управления войсками всё в большей степени определяется не только пропускной способностью систем связи, но и способностью полевых узлов связи сохранять работоспособность в условиях непрерывного разведывательного наблюдения, радиоэлектронного подавления и высокоточного огневого воздействия. Классические представления о пункте управления как о сравнительно устойчивом и заранее оборудованном элементе боевого порядка нуждаются в уточнении применительно к современной тактической обстановке, где цикл «обнаружение – классификация – поражение» существенно сократился [1, с. 13–20; 2, с. 13–47].

В профильных исследованиях подчёркивается, что устойчивость и живучесть системы связи должны рассматриваться как интегральные свойства, объединяющие надёжность, скрытность, способность к восстановлению, резервированию и перестройке маршрутов передачи информации [3, с. 41–58]. В работах, посвящённых оценке устойчивости систем управления в конфликте со средствами воздушно-космического нападения, дополнительно показано, что для корректного расчёта необходимо учитывать не только вероятность поражения элементов, но и факторы разведки, РЭП и время перехода к резервным способам управления [4, с. 227–233; 4, с. 257–262].

Для ТЗУ проблема приобретает особую остроту. Полевой узел связи (ПУС) находится в непосредственной близости от линии боевого соприкосновения, развертывается в ограниченное время и вынужден обеспечивать одновременно несколько приоритетных направлений связи, каждое из которых имеет различную значимость для управления, взаимодействия и обмена данными. При этом потеря даже одного направления связи не всегда критична, тогда как отказ нескольких приоритетных направлений может привести к срыву управления ПУ в целом [5, с. 60–68; 6, с. 52–58].

Отдельным фактором современного боя стало массовое применение малых беспилотных летательных аппаратов, способных выполнять разведывательные, ретрансляционные и ударные функции. Их использование расширяет возможности противника по ведению оптико-электронной, радиотехнической и радиолокационной разведки, а также усложняет требования к рассредоточению, маскировке и резервированию узлов связи. Одновременно собственные беспилотные средства всё активнее интегрируются в контур управления подразделениями, что дополнительно повышает нагрузку на сеть

1 ***Медведев Алексей Александрович***, адъюнкт Военной академии связи. Санкт-Петербург, Россия. E-mail: aleksey750rus@mail.ru

2 ***Юров Евгений Сергеевич***, заместитель начальника направления Главного управления связи. Москва, Россия. E-mail: yurov_es@mail.ru

воздушной радиосвязи и иные ресурсы связи тактического звена [7, с. 57–61].

В этой связи задача повышения разведывательной защищённости и живучести ПУС должна решаться не как совокупность разрозненных организационных мероприятий, а как единая научно-техническая задача, включающая формализацию объекта оценки, описание воздействующих факторов, выбор показателей важности направлений связи и расчёт интегрального критерия, пригодного для сравнения вариантов развёртывания и функционирования узла связи.

Современные угрозы полевому узлу связи и требования к его функционированию

Современные подходы к обеспечению разведывательной защищённости и живучести системы связи объединения исходят из того, что ПУС является не просто набором аппаратных средств, а пространственно-распределённой системой, уязвимость которой определяется одновременно её структурой, внешними признаками, интенсивностью радиообмена и длительностью пребывания в районе развертывания [8, с. 72–77]. С этой точки зрения узел связи демаскируется не только радиосредствами, но и инженерными изменениями местности, характерным размещением техники, работой вспомогательных энергетических средств и активностью обслуживающего персонала.

Существенным направлением повышения живучести выступает рассредоточенное или модульное построение узла связи. Функциональная модель структуры узла связи специального назначения рассредоточенного ПУ показывает, что разделение узла на модули, связанные основными и резервными маршрутами, позволяет уменьшить вероятность одномоментного выхода из строя всей системы и повышает возможность гибкого перераспределения функций при частичном поражении [9, с. 231–236]. Такой подход особенно важен в тактическом звене, где плотность угроз высока, а время на восстановление ограничено.

Одновременно обоснование требований к узлам связи ПУ должно учитывать не только традиционные показатели пропускной способности и развёртываемости, но и структурные требования к резервированию, приоритетности направлений связи, допустимому времени восстановления и устойчивости к совокупному воздействию разведки, РЭП и огневого поражения [10, с. 90–95]. Иными словами, задача проектирования и применения ПУС постепенно смещается от простой организации каналов к управлению живучестью сети направлений.

На устойчивость функционирования подвижного узла связи специального назначения влияют факторы различной природы: пространственное рассредоточение, наличие резервных путей, техническая приспособленность к быстрому ремонту, совместимость разнородных средств связи, а также способность узла сохранять функциональную целостность при частичном выведении из строя отдельных элементов [11, с. 339–344]. Для ПУС ТЗУ эти факторы должны оцениваться не изолированно, а в совокупности.

Графовые подходы к оценке устойчивости системы (сети) военной связи показывают, что связность, число альтернативных маршрутов, коэффициенты посредничества узлов и иные сетевые характеристики могут использоваться как количественная база для оценки структурной живучести [12, с. 87–97]. Однако применительно к ПУС этого недостаточно: наряду со связностью необходимо учитывать и временные параметры восстановления, поскольку даже кратковременная потеря связи в ходе высокоманёвренных действий способна привести к дезорганизации управления.

Роль беспилотных систем и новая конфигурация угроз

В монографии, посвящённой противодействию беспилотным летательным аппаратам (БПЛА), показано, что наиболее сложными объектами с точки зрения обнаружения и поражения являются малые БПЛА, которые обладают низкой заметностью, гибкостью применения и возможностью действовать группами [13, с. 36–44]. Для ПУС это означает появление постоянной угрозы воздушной разведки малого радиуса действия, способной оперативно фиксировать изменения обстановки в районе ПУ и передавать данные средствам поражения.

Одновременно опыт современных боевых действий свидетельствует о том, что БПЛА необходимо рассматривать не только как угрозу, но и как собственный ресурс повышения эффективности действий подразделений. В исследованиях, посвящённых усовершенствованному способу десантно-штурмовых действий с применением БПЛА, показано, что беспилотные платформы могут использоваться для разведки, ретрансляции, нанесения ударов, создания ложной активности и обеспечения манёвра подразделений в распределённом боевом порядке [14, с. 34–43]. В таком случае ПУС получает дополнительную нагрузку как центр сопряжения каналов управления подразделениями, группами БПЛА и ретрансляционными звеньями.

При анализе устойчивости сети связи в условиях воздействия дестабилизирующих факторов показано, что для корректной оценки необходимо увязать надёжность элементов, последствия внешних воздействий и возможности сети к сохранению связности за счёт альтернативных путей [15, с. 69–79]. Этот вывод особенно актуален для сети воздушной радиосвязи в ТЗУ, где ограниченные энергетические и частотно-временные ресурсы должны распределяться между несколькими задачами одновременно – от управления подразделениями до сопровождения применения БПЛА.

Следовательно, современная постановка задачи должна учитывать два взаимосвязанных обстоятельства. Во-первых, противник получает возможность ускоренного разведывательного вскрытия ПУ за счёт совмещения БПЛА, РРТР, ОЭР и РЛР. Во-вторых, собственная система управления также всё сильнее зависит от устойчивости сети, в которой воздушные, наземные и распределённые элементы управления образуют единый контур обмена информацией. Это делает актуальным переход от качественных оценок живучести к формализованной модели.

Формализованная постановка задачи и модель живучести полевого узла связи

В рамках настоящей статьи ПУС ПУ рассматривается как совокупность направлений связи НСi, $i = 1…N$, каждое из которых обеспечивает определённую функцию управления: связь с вышестоящим ПУ, связь с подчинёнными пунктами, взаимодействие, связь с элементами сети воздушной радиосвязи и средствами управления беспилотными платформами. Для каждого направления связи задаются основной маршрут и k резервных маршрутов, а также коэффициент важности α_i, отражающий вклад данного направления в общую устойчивость управления [9, с. 231–236; 10, с. 90–95; 12, с. 87–97].

Элементами маршрута являются узлы, каналы, частоты, ретрансляторы и иные компоненты, участвующие в передаче информации. Работоспособность элемента v определяется с учётом трёх основных групп факторов: вероятности физического поражения $P_{\text{ФП},v}$, вероятности радиоэлектронного подавления $P_{\text{РЭП},v}$ и собственной вероятности отказа $P_{\text{отк},v}$. Тогда вероятность работоспособного состояния элемента принимается в виде

$$P_{\text{раб,эл},v} = (1 - P_{\text{ФП},v})\,(1 - P_{\text{РЭП},v})\,(1 - P_{\text{отк},v}), \qquad (1)$$

где $P_{\text{раб,эл},v}$ – вероятность того, что элемент маршрута сохранит способность участвовать в передаче информации в рассматриваемый момент времени.

Если j-й путь i-го направления связи содержит z_j элементов, то вероятность работоспособности пути определяется произведением вероятностей работоспособности составляющих его элементов. С учётом наличия основного и резервных путей связность направления связи может быть оценена как вероятность сохранения хотя бы одного работоспособного пути:

$$P_{\text{св},i} = 1 - \prod[j=1 \to k_i](1 - \prod[v=1 \to z_j]P_{\text{раб,эл},v}). \quad (2)$$

Такое представление соответствует многомаршрутной структуре полевого узла связи и учитывает ключевой практический вывод о том, что для современных условий недостаточно обеспечить только наличие канала – необходимо обеспечить возможность оперативного перехода на резервный маршрут при деградации основного [5, с. 60–68; 6, с. 52–58].

Структурная связность сама по себе не исчерпывает проблему живучести. Для направления связи i следует учитывать и временную составляющую – способность сети обнаружить отказ, выполнить диагностику, уведомление, переключение на резервный путь и восстановление работоспособности. Временная живучесть направления в статье описывается через коэффициент готовности $K_{\text{Г},i}$, определяемый как отношение среднего времени сохранения работоспособности $T_{\text{О},i}$ к сумме времени сохранения работоспособности и среднего времени восстановления $T_{\text{В},i}$:

$$K_{\text{Г},i} = T_{\text{О},i} / (T_{\text{О},i} + T_{\text{В},i}). \qquad (3)$$

Используя связность направления и коэффициент его готовности, живучесть i-го направления связи определяется выражением

$$P_{\text{жив},i} = K_{\text{Г},i} \cdot P_{\text{св},I}, \qquad (4)$$

а интегральный показатель живучести полевого узла связи задаётся взвешенной суммой живучести направлений с учётом их важности:

$$P_{\text{жив,ПУС}} = \sum[i=1 \to N]\alpha_i \cdot P_{\text{жив},i},\ \sum[i=1 \to N]\alpha i = 1. \quad (5)$$

Предлагаемая логика интеграции воздействий, структурной связности, готовности и приоритетности направлений связи представлена на рисунке 1. Данная схема не подменяет детальную модель каждого канала или протокола, но задаёт единый формализм для сравнения вариантов развертывания и оценки влияния различных мер повышения живучести.

Сценарная оценка и пример расчёта

Для иллюстрации работоспособности модели целесообразно использовать сценарный подход. На практике исходные данные задаются не только абсолютными вероятностями, но и уровнями воздействий противника: умеренный,

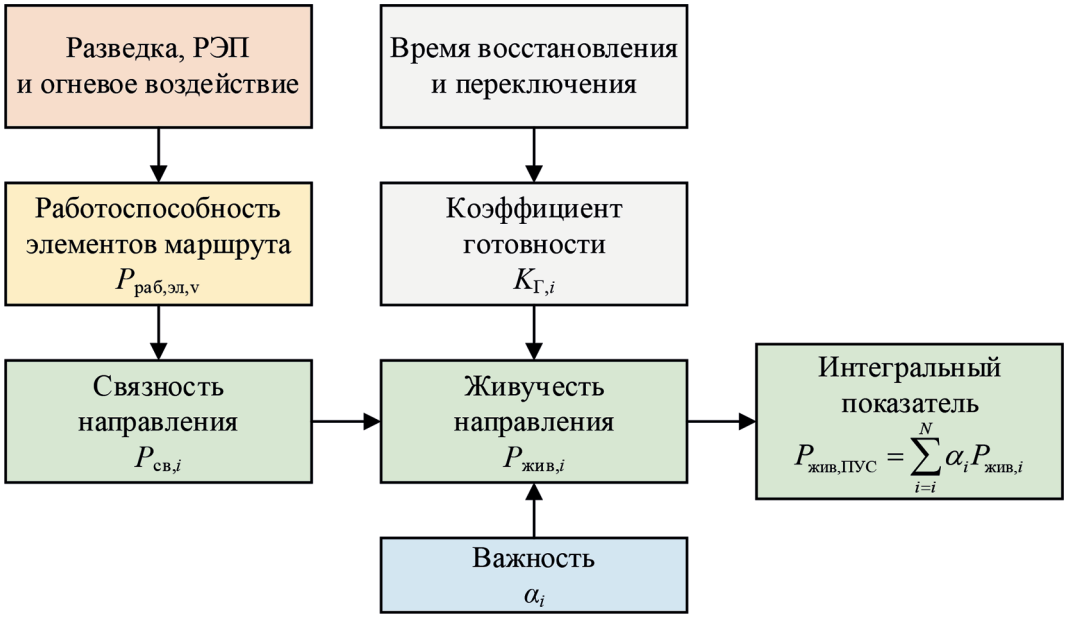


Рис. 1. Логика формирования интегрального показателя живучести полевого узла связи

базовый и усиленный. В каждом сценарии фиксируются структура направлений связи, схема основного и резервных маршрутов, а также коэффициенты важности α_i; варьируются уровни разведывательного воздействия, радиоэлектронного подавления, огневого поражения и параметры восстановления. Сводная характеристика сценариев приведена в таблице 1.

Сценарный подход соответствует логике современных операций, в которых точные значения входных параметров часто известны лишь приближённо, но уровень интенсивности угроз и время реакции на них могут быть заданы достаточно обоснованно по опыту применения средств разведки, РЭП и огневого поражения [4, с. 257–262; 13, с. 168–169; 14, с. 34–43].

Рассмотрим пример для трёх приоритетных направлений связи: НС1 – связь с вышестоящим ПУ, НС2 – связь с подчинёнными подразделениями, НС3 – взаимодействие и управление распределёнными элементами сети, включая средства ретрансляции и группы БПЛА. Пусть каждому направлению поставлены в соответствие один основной и два резервных маршрута. Для момента времени t = 10 ч в базовом сценарии S2 после оценки работоспособности элементов, связности маршрутов и временных параметров восстановления получены следующие значения живучести направлений: $P_{жив,1}$ = 0,660; $P_{жив,2}$ = 0,549; $P_{жив,3}$ = 0,396.

Если принять веса приоритетности α_1 = 0,5, α_2 = 0,3, α_3 = 0,2, то интегральный показатель живучести полевого узла связи составит $P_{жив,ПУС}$ = 0,574. Такой результат имеет содержательную интерпретацию: даже при удовлетворительной живучести двух направлений низкое значение наиболее уязвимого направления существенно снижает общую устойчивость узла связи. Следовательно, при ограниченных ресурсах сети воздушной радиосвязи наибольший эффект дадут мероприятия, направленные либо на увеличение связности НС3 за счёт дополнительных резервных путей, либо на сокращение времени его восстановления и переключения.

Таблица 1.

Сценарные уровни воздействия и восстановления для оценки живучести ПУС ПУ

Сценарий	Разведывательное воздействие	Радиоэлектронное подавление	Огневое воздействие	Восстановление/ переключение
S1 (умеренный)	пониженный уровень	пониженный уровень	пониженный уровень	облегчённое
S2 (базовый)	базовый уровень	базовый уровень	базовый уровень	типовой порядок
S3 (усиленный)	повышенный уровень	повышенный уровень	повышенный уровень	осложнённое

Практический вывод из приведённого примера состоит в том, что сравнение вариантов развертывания узла связи и распределения ресурсов сети воздушной радиосвязи должно выполняться не только по средним сетевым показателям, но и по интегральному показателю живучести, который учитывает приоритетность конкретных направлений. Иначе говоря, равномерное распределение ресурсов между всеми направлениями не всегда рационально; приоритет должен отдаваться тем направлениям, отказ которых приводит к наибольшей потере устойчивости управления [8, с. 72–77; 10, с. 90–95; 15, с. 69–79].

Направления практического повышения разведывательной защищённости и живучести

Полученная модель позволяет перейти от описательных мер к научно обоснованному выбору организационно-технических решений. К числу первоочередных мер следует отнести рассредоточение элементов узла связи, вынос наиболее уязвимых ретрансляционных и антенных средств, сокращение длительности пребывания на одной позиции, организацию ложных позиций и введение в боевой порядок дополнительных резервных маршрутов для приоритетных направлений связи [8, с. 72–77; 11, с. 339–344].

Вторая группа мер связана с адаптивным распределением ресурсов сети воздушной радиосвязи. При ограниченном частотно-временном ресурсе и росте количества управляемых БПЛА необходимо предусматривать механизм перераспределения полосы, времени доступа и ретрансляционных ресурсов в пользу тех направлений, которые в данный момент имеют наибольшую важность для сохранения управления. Предлагаемый интегральный показатель живучести может быть использован как целевая функция такой перестройки.

Третья группа мер относится к восстановлению и ремонту. Современный ПУС должен проектироваться и эксплуатироваться исходя из блочно-модульного принципа замены аппаратуры, что сокращает время восстановления, а значит, непосредственно повышает коэффициенты готовности направлений связи [6, с. 52–58; 11, с. 339–344]. При этом сами процедуры диагностики, уведомления и переключения на резерв должны быть максимально автоматизированы.

Наконец, особое значение имеет совместное учётное использование средств связи штатного и двойного назначения, включая спутниковые и проводные компоненты, а также воздушные ретрансляторы на БПЛА или аэростатных платформах. В современных конфликтах именно комбинирование разнородных технологий связи позволяет увеличить связность приоритетных направлений и снизить зависимость от одного класса уязвимых радиосредств [7, с. 57–61; 13, с. 168–169; 14, с. 34–43].

Заключение

В статье рассмотрены особенности обеспечения разведывательной защищённости и живучести ПУС ПУ на основе опыта современных вооружённых конфликтов. Установлено, что ключевое влияние на устойчивость функционирования ПУС оказывают совокупность разведывательных воздействий, радиоэлектронного подавления, физического поражения, ограниченность сетевых ресурсов и временные параметры восстановления нарушенных направлений связи.

Разработана формализованная модель живучести ПУС, в которой живучесть отдельного направления связи определяется как произведение коэффициента готовности и структурной связности, а общая живучесть узла связи – как взвешенная сумма живучести приоритетных направлений. Такой подход позволяет сопоставлять варианты развертывания, резервирования и распределения ресурсов сети воздушной радиосвязи по единому количественному критерию.

Достигнутый эффект состоит в том, что качественные требования к рассредоточению, резервированию, сокращению времени восстановления и приоритизации направлений связи переведены в форму расчётного научно-технического аппарата. Это даёт возможность использовать модель в научной области исследования военных систем управления и связи для обоснования организационных и технических решений в ТЗУ.

Практическое подтверждение и достоверность предлагаемых решений обеспечиваются корректной постановкой задачи, согласованностью показателей модели с общепринятыми представлениями о связности и готовности, а также воспроизводимостью расчёта при сценарном задании исходных параметров. Модель применима как база для последующей разработки методики адаптивного распределения ограниченных ресурсов сети воздушной радиосвязи в интересах сохранения работоспособности приоритетных направлений связи.

Литература

1. Ворогушин Е. Б., Савушкин Н. И. Военная энциклопедия. – М.: Воениздат, 1997. – Т. 1. –147 с.
2. Иванов В. Г. Теория и практика построения и обеспечения функционирования системы связи специального назначения с учётом технологического развития и опытов вооруженных конфликтов /монография В. Г. Иванов. – М.: Красная Звезда, 2025. – 304 с.
3. Макаренко С. И. Модели системы связи в условиях преднамеренных дестабилизирующих воздействий и ведения разведки: монография. СПб.: Наукоемкие технологии, 2020. – 337 с.
4. Афонин И. Е., Макаренко С. И., Петров С. В. Модель оценивания устойчивости системы управления воздушно-космической обороной в конфликте со средствами воздушно-космического нападения // Системы управления, связи и безопасности, 2023. – № 3. – С. 227–266. – DOI: 10.24412/2410-1916-2023-3-227-266.
5. Дудко С. М., Морару А. А., Смелов А. Е. К вопросам живучести пунктов управления общевойсковых формирований тактического звена // Военная мысль, 2023. – № 10. – С. 60–68.
6. Вольхин С. Д., Пустошкин М. М. Повышение эффективности применения средств и комплексов связи путем проведения мероприятий по обеспечению живучести // Телекоммуникации и связь, 2025. – № 4 (7). – С. 52–58.
7. Гусева А. С., Дурнев Р. А., Кудряшов А. С., Свиридок Е. В. Оценка эффективности систем противодействия массированному применению мини-БПЛА: методические основы // Известия Российской академии ракетных и артиллерийских наук, 2021. – № 1 (116). – С. 57–61.
8. Костарев С. В., Воробьёв И. Г. Современные подходы к обеспечению разведывательной защищенности и живучести системы связи объединения в операциях (боевых действиях) // Вестник Академии военных наук, 2019. – № 4 (69). – С. 72–77.
9. Иванов Р.М. Функциональная модель структуры узла связи специального назначения рассредоточенного (модульного) пункта управления // Известия Тульского государственного университета. Технические науки, 2021. – № 9. – С. 231–236. – DOI: 10.24412/2071-6168-2021-9-231-236.
10. Густов А. А., Пылинский М. В., Латушко М. М. Методический подход обоснования требований к узлам связи пунктов управления // Военная мысль, 2020. – № 3. – С. 90–95.
11. Милашевский А. В., Мякотин А. В., Привалов А. А., Чеботарев В. И. Факторы, влияющие на функциональную целостность и устойчивость функционирования подвижного узла связи специального назначения // Известия Тульского государственного университета. Технические науки, 2020. – Вып. 12. – С. 339–344.
12. Мещанин В. Ю. Оценка устойчивости системы (сети) военной связи высокой размерности // Военная мысль, 2021. – № 3. – С. 87–97.
13. Макаренко С. И. Противодействие беспилотным летательным аппаратам: монография. СПб.: Наукоемкие технологии, 2020. – 204 с. – ISBN 978-5-6044793-6-0.
14. Макаренко С. И., Медведев А. А., Зеленов А. В. Усовершенствованный способ десантно-штурмовых действий с применением беспилотных летательных аппаратов // Военная мысль, 2025. – № 1. – С. 34–43.
15. Михайлов Р. Л., Макаренко С. И. Оценка устойчивости сети связи в условиях воздействия на неё дестабилизирующих факторов // Радиотехнические и телекоммуникационные системы, 2013. – № 4 (12). – С. 69–79.

FEATURES OF ENSURING RECONNAISSANCE PROTECTION AND SURVIVABILITY OF FIELD COMMUNICATION CENTERS

Medvedev A. A.[3], Yurov E. S.[4]

Keywords: *aeronautical radio communication network, channel redundancy, adaptive resource allocation, unmanned aerial systems.*

Abstract

The purpose of the study: *to develop a scientific and technical approach to assessing and improving the reconnaissance protection and survivability of the field communication center (CS) of the control post (CP) in the tactical control link (TA) taking into account the modern nature of reconnaissance and strike actions.*

Research method: *system analysis, comparative analysis of domestic scientific publications, elements of reliability theory and graph models of communication networks, as well as scenario approach to assessing the impact of reconnaissance, electronic warfare (EW) and physical damage on communication directions.*

The result of the study: *the current threats to field communication centers have been clarified, a formalized survivability model has been proposed, combining the availability factor of the communication direction, its structural connectivity and priority weight, and an example of calculating the integral survivability index of a communication center for a multi-route structure has been shown.*

The scientific novelty *consists in the linking of reconnaissance security, multi-path connectivity and time parameters of recovery in a single calculated indicator suitable for subsequent use in the adaptive distribution of limited resources of the aeronautical radio communication network.*

3 ***Alexey A. Medvedev***, adjunct of the Military Academy of Communications. St. Petersburg, Russia. E-mail: aleksey750rus@mail.ru

4 ***Evgeny S. Yurov***, Deputy Head of the Main Communications Directorate. Moscow, Russia. E-mail: yurov_es@mail.ru

References

1. Vorogushin E. B., Savushkin N. I. Voennaya entsiklopediya. M.: Voenizdat, 1997. – Vol. 1. – 147 p.
2. Ivanov V. G. Teoriya i praktika postroeniya i obespecheniya funkcionirovaniya sistemy' svyazi special'nogo naznacheniya s uchyotom texnologicheskogo razvitiya i opy'tov vooruzhenny'x konfliktov: monografiya – M.: Krasnaya Zvezda, 2025. – 304 p.
3. Makarenko S. I. Modeli sistemy svyazi v usloviyakh prednamerennykh destabiliziruyushchikh vozdeystviy i vedeniya razvedki: monografiya. Saint Petersburg: Naukoemkie tekhnologii, 2020. – 337 p.
4. Afonin I. E., Makarenko S. I., Petrov S. V. Model otsenivaniya ustoychivosti sistemy upravleniya vozdushno-kosmicheskoy oboronoy v konflikte so sredstvami vozdushno-kosmicheskogo napadeniya. Sistemy upravleniya, svyazi i bezopasnosti, 2023. – No 3. – Pp. 227–266. – DOI: 10.24412/2410-1916-2023-3-227-266.
5. Dudko S. M., Moraru A. A., Smelov A. E. K voprosam zhivuchesti punktov upravleniya obshchevoyskovykh formirovaniy takticheskogo zvena. Voennaya mysl', 2023. – No 10. – Pp. 60–68.
6. Volkhin S. D., Pustoshkin M. M. Povyshenie effektivnosti primeneniya sredstv i kompleksov svyazi putem provedeniya meropriyatiy po obespecheniyu zhivuchesti. Telekommunikatsii i svyaz', 2025. – No 4 (7). – Pp. 52–58.
7. Guseva A. S., Durnev R. A., Kudryashov A. S., Sviridok E. V. Otsenka effektivnosti sistem protivodeystviya massirovannomu primeneniyu mini-BPLA: metodicheskie osnovy. Izvestiya Rossiyskoy akademii raketnykh i artilleriyskikh nauk, 2021. – No 1 (116), – Pp. 57–61.
8. Kostarev S. V., Vorob'ev I. G. Sovremennye podkhody k obespecheniyu razvedyvatel'noy zashchishchennosti i zhivuchesti sistemy svyazi ob''edineniya v operatsiyakh (boevykh deystviyakh). Vestnik Akademii voennykh nauk, 2019. – No 4 (69). – Pp. 72–77.
9. Ivanov R. M. Funktsional'naya model' struktury uzla svyazi spetsial'nogo naznacheniya rassredotochennogo (modul'nogo) punkta upravleniya. Izvestiya Tul'skogo gosudarstvennogo universiteta. Tekhnicheskie nauki, 2021. – No 9. – Pp. 231–236. – DOI: 10.24412/2071-6168-2021-9-231-236.
10. Gustov A. A., Pylinskiy M. V., Latushko M. M. Metodicheskiy podkhod obosnovaniya trebovaniy k uzlam svyazi punktov upravleniya. Voennaya mysl', 2020. – No. 3. – Pp. 90–95.
11. Milashevskiy A. V., Myakotin A. V., Privalov A. A., Chebotarev V. I. Faktory, vliyayushchie na funktsional'nuyu tselostnost' i ustoychivost' funktsionirovaniya podvizhnogo uzla svyazi spetsial'nogo naznacheniya. Izvestiya Tul'skogo gosudarstvennogo universiteta. Tekhnicheskie nauki, 2020. – Issue 12. – Pp. 339–344.
12. Meshchanin V. Yu. Otsenka ustoychivosti sistemy (seti) voennoy svyazi vysokoy razmernosti. Voennaya mysl', 2021. – No 3. – Pp. 87–97.
13. Makarenko S. I. Protivodeystvie bespilotnym letatel'nym apparatam: monografiya. SPb.: Naukoemkie tekhnologii, 2020. – 204 p. – ISBN 978-5-6044793-6-0.
14. Makarenko S. I., Medvedev A. A., Zelenov A. V. Usovershenstvovannyy sposob desantno-shturmovykh deystviy s primeneniem bespilotnykh letatel'nykh apparatov. Voennaya mysl', 2025. – No 1. – Pp. 34–43.
15. Mikhaylov R. L., Makarenko S. I. Otsenka ustoychivosti seti svyazi v usloviyakh vozdeystviya na nee destabiliziruyushchikh faktorov. Radiotekhnicheskie i telekommunikatsionnye sistemy, 2013. – No 4 (12). – Pp. 69–79.

МЕТОДИКА ПОСТРОЕНИЯ ОДИНОЧНЫХ ПРОФИЛЕЙ ФУНКЦИОНИРОВАНИЯ ИНФОРМАЦИОННО-УПРАВЛЯЮЩЕЙ СИСТЕМЫ

Остроумов О. А.[1], Лепешкин О. М.[2], Синюк А. Д.[3]

DOI:10.21681/3034-4050-2026-4-49-57

Ключевые слова: *функции и задачи системы, одиночный профиль функционирования, техническая система.*

Аннотация

Цель работы: *исследование подхода формализации процесса функционирования системы, выполняемых в ней задач, ее целевого предназначения в виде совокупности взаимосвязанных одиночных профилей ее функционирования.*

Методы исследования: *в работе используется методы теории графов, теории матриц, теории множеств.*

Результаты исследования: *в работе получена методика построения профилей функционирования системы. Полученные профили могут использоваться в системе управления для контроля выполнения регламентов в системе, выявлении критических элементов, влияющих на способность системы выполнить ее главную задачу.*

Научная новизна работы *заключается в предложенном одиночном профиле функционирования, который может использоваться при построении информационно-управляющей системы и контроле ее функционирования.*

Введение

Структурная сложность современных технических систем определяется множеством ее элементов, разнесенных в пространстве, функциональная сложность – многозадачностью и наличием связей с другими системами. Наличие связей и потребность в выполнении задач системы определяют их критичность и необходимость обеспечения функциональной устойчивости [1, 2]. Нарушение функционирования таких систем может пагубно сказываться на жизни общества, отдельных отраслей промышленности и государства в целом, при этом, допустимая длительность не выполнения ими требуемого предназначения с каждым годом сокращается. Возникает необходимость обеспечения устойчивого функционирования сложных технических систем (СТС), что невозможно без знания о состоянии системы и ее элементов в любой момент времени [3, 4]. Для анализа поведения таких систем и обеспечения их устойчивого функционирования требуется построение моделей и формализации процесса их функционирования [5–7], при этом, для современных технических систем возникают сложности по их формализации из-за необходимости учета большого количества различных факторов, влияющих на процесс функционирования системы [2, 8, 9].

Для любой системы, в том числе информационно-управляющей системы (ИУС) характерно наличие частных задач, которых, как правило, много, и главной задачи, которая бывает, как правило, она одна, но для некоторых сложных распределенных многофункциональных систем их может быть несколько. Совокупность (или одна) главных задач объединяют в виде целевого предназначения системы для достижения которого и функционирует система выполняя частные задачи и функции [10, 11]. Выполнение таких задач возможно только при наличии достаточного ресурсного обеспечения в системе. Системы, выполняющие одну цель, как правило, не представляют сложности [12, 13]. Развитие системы, появление новых многофункциональных элементов и связей, как внутренних, так и внешних формируют ее многоцелевую структуру [12–15].

К СТС можно отнести системы управления, связи, мониторинга и контроля состояния систем, автоматизированные системы управления, информационные и информационно-управляющие системы и др. [16–18]. Всех их объединяет трудность формализации процесса их функционирования. Увеличение сложности системы создает трудности при восприятии человеком процесса функционирования системы и обеспечения своевременной реакции на изменение состояния системы или возникновение предпосылок к нарушению их функционирования. Усложнение системы, многозадачность в ней, а также наличие большого количества внутренних и внешних связей и необходимость

1 ***Остроумов Олег Александрович***, кандидат технических наук, преподаватель кафедры Военной академии связи. Санкт-Петербург, Россия. E-mail: oleg-26stav@mail.ru

2 ***Лепешкин Олег Михайлович***, доктор технических наук, доцент, профессор кафедры Военной академии связи. Санкт-Петербург, Россия. E-mail: lepeshkin1@yandex.ru

3 ***Синюк Александр Демьянович***, доктор технических наук, доцент Военной академии связи. Санкт Петербург, Россия. E-mail: eentrop@rambler.ru

их учета, а также потребность в реакции на нарушения функционирования в режиме реального времени требует автоматизации процессов управления такими системами.

Для реализации адекватного цикла управления с возможностью быстрой реакции на изменения в системе осуществляется формализация главной задачи системы (ее целевого предназначения) [15, 19, 20]. В самом общем значении целью является состояние к которому направлено движение рассматриваемого объекта. В качестве цель может выступать пожелание перехода ИУС в состояние, определяемое как результат ее функционирования. Формализованная цель может выступать в качестве задания для системы контроля, определяемая как желаемый результат, к которому стремится СТС в своем движении.

Современные систем, выполняя известные цели, как правило, используют устоявшуюся известную структуру ИУС [21, 22]. Любая цель задается типом ранее сложившихся взаимодействий элементов системы. Сложности возникают при изменении цели, обстановки, потребностей вышестоящих систем. В этом случае требуется формирование новых целей и построение новой системы для достижения новых целей. Возникновение новой цели всегда обусловлено появлением проблемной ситуации, когда разрешить ее имеющимися средствами невозможно [17, 23–25].

Процесс функционирования системы неразрывно связан с взаимодействием ее с внешней и внутренней средой. При этом взаимодействие с другими системами осуществляется через входные и выходные характеристики, т.е. результаты функционирования ИУС могут использоваться другими системами, а также она может использовать результаты работы других систем, которые выступают для нее в качестве ресурса. Воздействие на систему дестабилизирующих факторов (ДФ) может приводить к нарушению структуры взаимодействия элементов ИУС и нарушению выполнения целей системы. При этом, степень последствий нарушения функционирования разных элементов системы различная, т.е. значение этих элементов для системы разное. Некоторые элементы становятся критически значимыми для системы [26–28].

Процесс функционирования технической системы будет определяться его структурой, позволяющей системе получить основные ресурсы, а также целевым предназначением и взаимосвязанными с ним функциями и задачами системы. Немаловажным элементом процесса функционирования системы выступает критерий требования к системе, ее структуре, элементам структуры, целевому предназначению, функциям, задачам и ресурсам системы. Нарушение требований или снижение количественных показателей критериев оценки требований приводит к неэффективному функционированию системы или невозможности выполнить свое целевое предназначение. Для описания целевого предназначения ИУС предлагается использовать древовидную структуру зависимости между целями, функциями, требованиями и задачами системы.

Модель информационно-управляющей системы

Для описания функциональной характеристики системы воспользуемся моделью, представленной на рисунке 1 [29]. Каждый элемент модель может включать подэлементы: подцели, подфункции, подзадачи. Своевременное и правильное, в соответствии с требованиями, предъявляемыми к системе, выполнение задач, функций и целей характеризует достижение целевого предназначения. Обеспечение функционирования системы осуществляется за счет ресурса, отсутствие или невозможность использования которого для выполнения текущих регламентов системы может приводить к нарушению устойчивого функционирования системы.

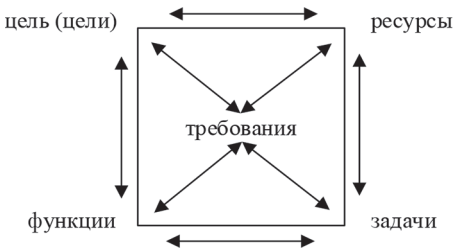


Рис. 1. Концептуальная модель процесса функционирования ИУС

Функционал системы опирается на ее структуру, описание которых будем осуществлять на основе теории графов и теории матриц [30].

Для примера, структуру системы можно представить в виде графа на рисунке 2. Вершины графа $\{X1, \ldots, X10\}$ будут соответствовать элементами системы. При наличии связи в системе между элементами на графе структуры будут присутствовать ребра, показывающие эту связь. Полученный граф условно описывает любую СТС и не требует внесения дополнительных элементов в него. Структура и процесс функционирования большинства технических систем представляет собой иерархически устроенное образование с устоявшимися связями.

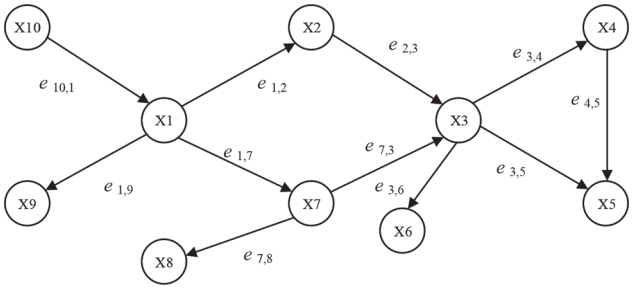


Рис. 2. Графического представления структуры ИУС W (G, L)

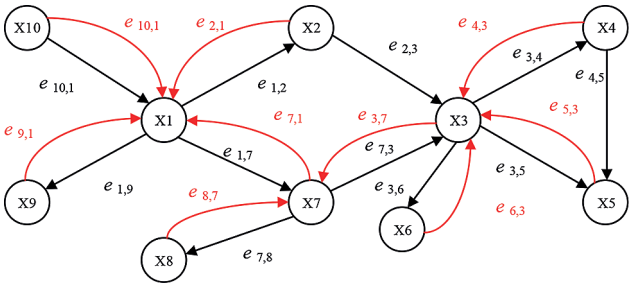


Рис. 3. Графическое представление структуры ИУС W (G, L) с каналами управления

Существование системы самой по себе бессмысленно. Для определения цели и стремления к ее достижению в системе существуют органы управления или подсистема управления. Процесс управления технической системой реализуется через обратную связь при реализации управляющих воздействий и получении отклика системы на их применение. Управление осуществляется через особые технологические каналы управления, наличие которых для системы, описываемой графом на рисунке 2, показано на рисунке 3. Структурная характеристика системы выступает в качестве основы профиля ее функционирования.

Описание одиночного профиля функционирования системы

Для формализации процесса функционирования ИУС в работе предложен подход к построению одиночных профилей функционирования системы (ОПФС) [10, 26].

ОПФС называется такая характеристика системы и ее элемента для формализации которой требуется только ресурс системы. Выполнение ОПФС при функционировании системы в заданных временных рамках описывается регламентом ОПФС.

Аксиома

Любой простейший элемент информационно-управляющей системы, характеризующий ее структуру или функционал, можно описать в виде как минимум одного ОПФС, позволяющего описать его функционирование (выполнение). В качестве простейшего элемента структуры системы рассматривается такой объект деление, которого на элементы не производится, простейший элемент функционала – задача (регламент) для выполнения которой требуется только ресурс системы.

В работе предлагается деление одиночных профилей на два вида:

- профиль регламента (задачи);
- профиль простейшего объекта системы.

Формирование ОПФС обоих типов включает его наименование, предназначение, тип, перечень ресурсов, необходимых для его выполнения, перечень элементов системы, использующихся для его выполнения, пространственно-временное расположение ресурсов системы, временные характеристики его выполнения (время начала и окончания выполнения, длительность, время проверки готовности к выполнению), порядок резервирования элементов профиля для его выполнения, возможные варианты задействования различных ресурсов системы для выполнена этого профиля, эффективность каждого, требования предъявляемые к процессу его выполнения и критерии оценки его выполнения, характеристики динамической и статической критичности профиля, его элементов, ресурсов, использующихся для его выполнения, перечень и последовательность выполнения групповых профилей для выполнения которых он используется, перечень и последовательность выполнения одиночных и групповых профилей для выполнения которых он может использоваться как резерв.

ОПФС второго типа дополнительно включает перечень ресурсов, которые предоставляет для системы данный объект, из которого выделяются ресурсы необходимые для выполнения текущего целевого предназначения, состав объекта, общее время задействования в рамках выполнения текущего целевого предназначения, а также периоды использования, их количество и длительность, технические характеристики объекта, типовые неисправности и перечень угроз функционированию объекта, статистика нарушения функционирования, отказов и сбоев объекта и его элементов.

Наполнение ОПФС не ограничивается представленным выше перечнем характеристик и будет зависеть от типа системы, требований к ней и условий ее функционирования.

Постановка задачи на разработку методики построения ОПФС

Проведенный анализ и описание одиночного профиля функционирования ИУС показали, что существует потребность в формализации процесса функционирования системы и ее элементов, одним из элементов такого описания можно считать профиль функционирования системы. Сложность, критичность системы и динамика изменения ее состояния определяет потребность рассматривать ее как иерархическое образование элементов, имеющих определенные связи между собой [29, 30]. Традиционные подходы к формализации технических систем ориентированы на описание их структуры, однако при формировании профиля упор делается на описание выполнения главной задачи системы, нарушение выполнения элементов которого может приводить к неспособность системы выполнить возложенное на нее предназначение. В этом случае в системе возникает противоречие, обусловленное потребностями ЛПР и возможностями системы по их реализации существующей структурой системы [31]. Следствием этого противоречия является потребность ЛПР с одной стороны постоянно иметь информацию о состоянии системы, а с другой иметь варианты устранения ситуаций невыполнения функциональных элементов системы для чего требуется инструмент в качестве которого предлагается использовать профиль функционирования системы.

Наличие противоречий позволяет сформулировать актуальную **научную задачу**, заключающуюся в потребностях ИУС и лиц, принимающих решение (ЛПР), в разработке методики построения одиночного профиля функционирования ИУС, что позволит формализовать структуру и процесс функционирования информационно-управляющей системы и описать требования ЛПР по выполнению целевого предназначения системы, кроме этого, структурировать процесс функционирования системы, а также сформировать задание для системы контроль, что позволит удовлетворить потребности ЛПР в получении информации нарушении функционирования системы и ее состоянии.

Суть методики заключается в определении целевого предназначения системы, выделении элементов системы необходимых для его выполнения и их формализации в виде множества одиночных профилей функционирования системы, что позволит за счет ресурса системы его выполнить.

Показателями эффективности являются вероятность построения одиночного профиля функционирования ИУС, позволяющего своевременно выполнить целевое предназначение системы при минимальном количестве ресурсов затрачиваемых для этого

$$P_A\left(Q_0|t_{Q_0}\right) \le t_{Q_0\text{треб}},\ E(Q_0) \to 0\Big).$$

Вводимые **ограничения**:

- элементы и ресурсы системы распределены на пространстве на ограниченной территории и перемещаются в зависимости от требуемых задач;
- связь между разнесенными в пространстве элементами осуществляется при наличии технического ресурса;
- выполнение системой и ее элементами заданного набора частных задач, функций, целей, требований определяет выполнение главной задачи (целевого предназначения);
- ресурс в системе имеется, исправен и его достаточно для формирования ОПФС и выполнения ею главной задачи.

Исходными данными в методике являются:

- состав системы, включающий G-элементов и L-линий, и ее структура в виде графа $W = (G, L)$;
- множество технических средств, находящихся на элементах системы, выступающих в качестве ресурса системы $N_k = \{N_1, N_2, \ldots, N_k\}$;
- множество ресурсов системы, являющихся результатом функционирования технических средств, находящихся на элементах системы $E_N = \{ E_{N1}, E_{N2}, \ldots, E_{Nm}\}$;
- множество ресурсов системы, находящихся в ней $E_m = \{N_k, E_N\}$;
- множество задач в выполнении которых участвуют элементы технической системы $Z_{Nq} = \{Z_{N1}, Z_{N2}, \ldots, Z_{Nq}\}$;
- множество функций в выполнении которых участвуют элементы технической системы за счет выполнения задач системы $F_{Nc} = \{F_{N1}, F_{N2}, \ldots, F_{Nc}\}$;
- целевое предназначение системы, выполнение которого обеспечивается выполнением функций системы $A = \{F_1, F_2, \ldots, F_c\}$.

Описание методики

1. Формирование множества требований к процессу выполнения целевого предназначения системы, которое характеризуется величиной конечной цели системы из множества, выполняемых в процессе реализации регламента

$$f_{\text{треб}}(A) \to f(A_a) \to A_a.$$

2. Определить последовательность достижения целей системы, т.е. порядок перехода

из первого состояния A_1 в последнее состояние A_a

$$A_1 \rightarrow A_2 \rightarrow ... \rightarrow A_a.$$

3. Определение требований к функциям исходя из требований, предъявляемых к целевому предназначению и системе в целом

$$f_{\text{треб}}(A_a) \rightarrow f_{\text{треб}}(F_c).$$

4. Последовательное выполнение функций системы определяет достижение каждой цели

$$A_1(F_{11} \rightarrow F_{12} \rightarrow ... \rightarrow F_{1c}) ... A_a(F_{a1} \rightarrow F_{a2} \rightarrow ... \rightarrow F_{ac}).$$

5. Формируется множество последовательно выполняемых требований, предъявляемых к задачам, исходя из требований, предъявляемых к выполнению функций системы, что позволяет обеспечить выполнение целевого предназначения

$$f_{\text{треб}}(A_a) \rightarrow f_{\text{треб}}(F_c) \rightarrow f_{\text{треб}}(Z_q).$$

6. Последовательное выполнение задач системы определяет выполнение каждой функции

$$F_1(Z_{11} \rightarrow Z_{12} \rightarrow ... \rightarrow Z_{1q}) ... F_c(Z_{c1} \rightarrow Z_{c2} \rightarrow ... \rightarrow Z_{cq}).$$

7. На основании требований, предъявляемых к процессу выполнения функций и задач системы формируется множество последовательно выполняемых требований, предъявляемых к ресурсам

$$f_{\text{треб}}(A_a) \rightarrow f_{\text{треб}}(F_c) \rightarrow f_{\text{треб}}(Z_q) \rightarrow f_{\text{треб}}(E_m).$$

8. Последовательное задействование требуемого ресурса системы определяет выполнение каждой задачи

$$Z_1(E_{11} \rightarrow E_{12} \rightarrow ... \rightarrow E_{1m}) ... Zq(E_{q1} \rightarrow E_{q2} \rightarrow ... \rightarrow E_{qm}).$$

9. Для описания процесса выполнения главной задачи системы, формируется множество потребных к выполнению ОПФС

$$Q = \{Q_1, Q_2, ... ,Q_i\}.$$

10. Определение для каждого ОПФ ИУС множества вариантов задействования ресурсов системы для его выполнения

$$Q_i = \{Q_{1i}, Q_{2i}, ... ,Q_{ji}\}.$$

11. Оценка необходимого ресурсного обеспечения для выполнения каждого варианта выполнения одиночного профиля функционирования ИУС

$$Q_{1i} < Q_{2i} <. .. < Q_{ji}.$$

12. Выбор оптимального по минимуму ресурса варианта выполнения одиночного профиля функционирования ИУС и определение его как основного (при этом, в качестве критерия могут быть выбраны: стоимость, эффективность выполнения профиля, надежность, устойчивость элементов системы, участвующих в его выполнении, минимальное задействование технических средств для его выполнения и т.д.)

$$\underset{E}{opt}\, Q_{ji}.$$

13. Формирование множества дополнительных вариантов выполнения каждого одиночного профиля функционирования ИУС, которые являются не оптимальными,

$$Q_{i\text{доп}} = \{Q_{1i}, Q_{2i}, ... ,Q_{(j-1)i}\}.$$

14. Ранжирование дополнительных вариантов выполнения каждого одиночного профиля функционирования ИУС по критерию минимального необходимого ресурса (аналогичным образом может быть выбран другой критерий ранжирования).

Для выполнения любой задачи требуется ресурс, который при построении ОПФС закрепляется за задачей в определенные моменты времени, что позволяет сформировать регламент выполнения задачи и ОПФС. Множество регламентов и порядок их выполнения используются при построении групповых профилей функционирования системы. Множество задач и их необходимое ресурсное обеспечение позволяет сформировать матрицу ресурсного обеспечения ОПФС

$$q_{Z-E} = \begin{vmatrix} 0 & 1 & ... & 0 \\ 1 & 0 & ... & 0 \\ ... & ... & ... & ... \\ 0 & 0 & ... & 1 \end{vmatrix},$$

где столбцы описывают ресурсы системы, а строки выполняемые задачи.

Матрица временно́го задействования ресурсов характеризует временные характеристики, такие как длительность, время начала и окончания выполнения, интервалы задействования ресурса

$$q_{E-t} = \begin{vmatrix} 1 & 1 & 1 & 0 & ... & 0 \\ 0 & 1 & 1 & 1 & ... & 0 \\ ... & ... & ... & ... & ... & ... \\ 0 & 1 & 1 & 0 & ... & 1 \end{vmatrix},$$

где столбцы соответствуют временны́м отрезкам $\Delta t = t_a - t_{a-1}$, которые выбираются исходя из требований системы контроля, а также условий функционирования системы, $a = [0, N)$, N – множество натуральных чисел, строки соответствуют ресурсам системы используемым для выполнения целевого предназначения. Общее время функционирования системы будет

определяться, как $\Delta t = t_a - t_0$, где, как правило, t_0 выбирают равным 0.

Аналогичная матрица, характеризующая временны́е характеристики, строится при выполнении ОПФС

$$q_{Z-t} = \begin{vmatrix} 1 & 1 & 1 & 0 & ... & 0 \\ 0 & 1 & 1 & 1 & ... & 0 \\ ... & ... & ... & ... & ... & ... \\ 0 & 1 & 1 & 0 & ... & 1 \end{vmatrix},$$

где столбцы описывают временны́е интервалы, а строки задачи системы.

Использование элементов системы для выполнения задач показано в матрице задач

$$q_{O-Z} = \begin{vmatrix} 1 & 1 & 1 & 0 & ... & 0 \\ 0 & 1 & 1 & 1 & ... & 0 \\ ... & ... & ... & ... & ... & ... \\ 0 & 1 & 1 & 0 & ... & 1 \end{vmatrix}.$$

Матрица возможностей используется при формировании вариантов задействования ресурсов для выполнения ОПФС, а также для поиска резерва, который мог бы использоваться для каждого ОПФС

$$q_{O-E} = \begin{vmatrix} 1 & 1 & 1 & 0 & ... & 0 \\ 0 & 1 & 1 & 1 & ... & 0 \\ ... & ... & ... & ... & ... & ... \\ 0 & 1 & 1 & 0 & ... & 1 \end{vmatrix}.$$

Таким образом ОПФС имеет следующий вид:

- первого типа

$$Q_0 = \{v_i, F_c, t, r\},$$

где v – объект (элемент) системы, i – объекты (элементы) системы, t – время выполнения (задействования), r – ресурс системы, который необходим для выполнения данного одиночного профиля, F_c – перечень функций в выполнении которых участвует данный профиль;

- второго типа

$$Q_0 = \{v, t, Z_q, F_c, (r_{\text{вх}}, r_{\text{вых}})\},$$

где r – ресурс системы (на входе объекта и на выходе), Z_q – перечень задач в выполнении которых участвует объект, F_c – перечень функций в выполнении которых участвует объект.

Выводы

Полученные в системе одиночные ПФС определяют нижний уровень ПФС. Одиночных профилей больше всего, и они вариативны, что позволяет обеспечивать гибкость функционирования системы и выполнения целевого предназначения за счет управления одиночными профилями, а также формирования из множества возможных вариантов выполнения каждого одиночного профиля групповых профилей более высокого уровня иерархии процесса функционирования системы, что позволит их использовать для обеспечения ФУ системы.

Будущие направления развития. Множество ОПФС являются основой для построения группового ПФС. Степень влияния выполнения ОПФС и групповых ПФС друг на друга различная. Последовательность выполнения ПФС будет определяться требуемым целевым предназначением системы и потребностями лиц, принимающих решение. Все это определяет необходимость согласования ПФС.

Литература

1. Дурняк Б. В., Машков О. А., Усаченко Л. М., Сабат В. И. Методология обеспечения функциональной устойчивости иерархических организационных систем управления // Сборник научных статей: Институт проблем моделирования в энергетике, НАН Украины, 2008. – В. 48. – С. 3–21.
2. Остроумов О. А., Базир Г. И., Черных И. С., Лепешкин О. М. Особенности синтеза сложных технических систем // Электроника: наука, технология, бизнес, 2025. – № 9 (250). – С. 134–138.
3. Лукьянчик В. Н., Иванов В. Г., Кузин П. И., Новикова М. А. Использование беспилотной авиации при ведении воздушной визуализации в сложных метеоусловиях // Телекоммуникации, 2026. – № 3. – С. 13–24.
4. Иванов В. Г., Кузина Е. И., Гоманов Д. Е., Гришин П. С., Чеглов А. В., Кузин П. И. Мониторинг изменения местности по разновременным аэрокосмическим изображениям с применением технологий глубогого обучения нейронных сетей // Геодезия и картография, 2025. – Т.86. – № 5. – С. 39–46.
5. Филатов В. А., Козырь О. Ф. Модель поведения автономного сценария в задачах управления распределенными информационными ресурсами // Инженерный вестник Дона, 2013. – № 3. URL: ivdon.ru/ru/magazine/archive/n3y2013/1771.
6. Одоевский С. М., Лебедев П. В. Методика оценки устойчивости функционирования системы технологического управления инфокоммуникационной сетью специального назначения с заданной топологической и функциональной структурой // Системы управления, связи и безопасности, 2021. – № 1. – С. 152–189. DOI: 10.24411/2410-9916-2021-10107.
7. Кондрашов Ю. В., Сатдинов А. И., Синюк А. Д., Остроумов О. А. Концептуальная модель контроля функций системы связи для выявления конфликтных ситуаций // T-Comm: Телекоммуникации и транспорт, 2022. – Т. 16. – № 5. – С. 21–27.

8. Zhang, H. The optimal control theory – a scientific approach to fundamentally solving control problems. Sci. China Inf. Sci. 68, 116201 (2025). – URL: https://doi.org/10.1007/s11432-024-4180-2.
9. Khettabi, I., Benyoucef, L. & Boutiche, M. A. Sustainable reconfigurable manufacturing system design using adapted multi-objective evolutionary-based approaches. Int. J. Adv. Manuf. Technol. – 115, 3741–3759 (2021). – URL: https://doi.org/10.1007/s00170-021-07337-3.
10. Лаута О. С, Баленко Е. Г., Федоров В. Х., Лепешкин О. М., Остроумов О. А. Метод построения профиля функционирования сложной технической системы // Инженерный вестник Дона, 2023. – № 2. – URL: ivdon.ru/ru/magazine/archive/n2y2023/8183.
11. Chen, J., Pan, H., Zhang, K. et al. Predictive control approach incorporating incremental learning. Appl. Intell. – 55, 401 (2025). – URL: https://doi.org/10.1007/s10489-025-06243-5.
12. Тарасов А. А. Проблема обеспечения гарантоспособности информационных систем и пути ее решения // Системы безопасности, связи и телекоммуникаций, 2000. – № 32. – С. 78–80.
13. Остроумов О. А. Проблема обеспечения функциональной устойчивости систем критически важных объектов // Электросвязь. – 2022. – № 1. – С.14–18.
14. Петренко С. А. Концепция поддержания работоспособности киберсистем в условиях информационно-технических воздействий // Труды ИСА РАН, 2009. – Т. 41. – С. 175–193.
15. Макаренко С. И., Козлов К. В. Автоматизированная система управления беспилотными летательными аппаратами при совместном решении ими специальных задач // Системы управления, связи и безопасности, 2025. – №1. – DOI: 10.24412/2410-9916-2025-1-131-155.
16. Иванов С. А. Методика обеспечения функционирования информационного направления в сети связи с памятью в условиях нестабильности характеристик элементов сети // Известия ТулГУ. Технические науки. – 2021. – № 11.
17. Fathabadi A. S., Snook C., Dghaym D. et al. Systematic hierarchical analysis of requirements for critical systems. Innovations Syst Softw Eng (2024). – URL: https://doi.org/10.1007/s11334-024-00551-8.
18. Bai, Z., Li, C., Pourzamani, J. et al. Optimizing the resource allocation in cyber physical energy systems based on cloud storage and IoT infrastructure. J. Cloud Comp. – 13, 59 (2024). – URL: https://doi.org/10.1186/s13677-024-00615-x.
19. Смирнов А. В., Левашова Т. В., Петров М. В. Базовый сценарий поддержки принятия решений на основе моделей жизни пользователей в цифровой среде. Информационно-управляющие системы, 2021. – № 4. – С. 47–60. – DOI: 10.31799/1684-8853-2021-4-47-60.
20. Ding, D., Han, QL., Ge, X. et al. Privacy-preserving filtering, control and optimization for industrial cyber-physical systems. Sci. China Inf. Sci. – 68, 141201 (2025). – URL: https://doi.org/10.1007/s11432-024-4328-1.
21. Аунг Чжо Мью, Анисимов А. А., Гагарина Л. Г., Портнов Е. М. Методика повышения эффективности управления ресурсоемкими задачами в распределенных вычислительных системах // Инженерный вестник Дона, 2022. – № 2. – URL: ivdon.ru/ru/magazine/archive/n2y2022/6294.
22. Ala-Laurinaho, R., Autiosalo, J., Laine, S. et al. Paradigm shift in mechanical system design: toward automated and collaborative design with digital twin web. Softw. Syst. Model (2024). – URL: https://doi.org/10.1007/s10270-024-01215-8.
23. Tsapko S. G., Tsapko I. V. & Tarakanov D. V. Efficiency of the Design Processes for Complex Systems with the Mathematical Apparatus of Fuzzy Sets. Autom. Doc. Math. Linguist. – 57. 258–266 (2023). – URL: https://doi.org/10.3103/S0005105523050096.
24. Yang X., Jia K. & Peng Z. Construction of integrated network order system of main distribution network based on power grid operation control platform. Energy Inform. – 7, 70 (2024).– URL: https://doi.org/10.1186/s42162-024-00368-6.
25. Ribeiro R., Pilastri A., Moura C. et al. A data-driven intelligent decision support system that combines predictive and prescriptive analytics for the design of new textile fabrics. Neural Comput. & Applic. – 35, 17375–17395 (2023). – URL: https://doi.org/10.1007/s00521-023-08596-9.
26. Остроумов О. А., Лепешкин О. М., Синюк А. Д., Филимонов В. А. Оптимизация профиля функционирования сложной технической системы // Информационно-управляющие системы, 2023. – № 4 (125). – С. 12–25.
27. Menaceur A., Drid H. & Rahouti M. Fault Tolerance and Failure Recovery Techniques in Software-Defined Networking: A Comprehensive Approach. J Netw Syst Manage. – 31, 83 (2023). – URL: https://doi.org/10.1007/s10922-023-09772-x.
28. Ahmad I., Clark A., Ali M. et al. Determining critical nodes in optimal cost attacks on networked infrastructures. Discov. Internet Things. – 4, 2 (2024). – URL: https://doi.org/10.1007/s43926-023-00054-1.
29. Остроумов О. А. Построение профиля функционирования сложной технической систем // Электросвязь, 2026. – № 1. – С. 18–26.
30. Лепешкин О. М., Лебедев П. В., Синюк А. Д., Лепешкин О. М. Графо-матричная структурно-функциональная модель сложной технической системы // Проблемы машиностроения и автоматизации. – №4-s1-2025. – С. 117–128.
31. Макаренко С. И., Нестеров А. А. Структурно-функциональная модель интероперабельности организационно-технических систем // Труды учебных заведений связи, 2023. – № 4. – DOI: 10.31854/1813-324X-2023-9-4-65-74.

METHODOLOGY FOR BUILDING SINGLE PROFILES OF THE FUNCTIONING OF THE INFORMATION AND MANAGEMENT SYSTEM

Ostroumov O. A.[4], Lepeshkin O. M.[5], Sinyuk A. D.[6]

Keywords: *functions and tasks of the system, single profile of functioning, technical system.*

Abstract

The purpose of the work *is to study the approach to formalizing the process of functioning of the system, the tasks performed in it, its purpose in the form of a set of interrelated single profiles of its functioning.*

Research methods: *the author uses the methods of graph theory, matrix theory, and set theory.*

Results of the study: *the method of building profiles of the system's functioning is obtained in the work. The obtained profiles can be used in the management system to monitor the implementation of regulations in the system, to identify critical elements that affect the ability of the system to perform its main task.*

The scientific novelty *of the work lies in the proposed single profile of functioning, which can be used in the construction of an information and management system and control of its functioning.*

References

1. Durnyak B. V., Mashkov O. A., Usachenko L. M., Sabat V. I. Metodologiya obespecheniya funkcional'noj ustojchivosti ierarhicheskih organizacionnyh sistem upravleniya // Sbornik nauchnyh statej: Institut problem modelirovaniya v ehnergetike, NAN Ukrainy, 2008. – V. 48. – Pp. 3–21.
2. Ostroumov O. A., Bazir G. I., Chernyh I. S., Lepeshkin O. M. Osobennosti sinteza slozhnyh tehnicheskih sistem // Ehlektronika: nauka, tehnologiya, biznes, 2025. – 9 (250). – Pp. 134–138.
3. Luk'yanchik V. N., Ivanov V. G., Kuzin P. I., Novikova M. A. Ispol'zovanie bespilotnoj aviacii pri vedenii vozdushnoj vizualizacii v slozhnyh meteousloviyah // Telekommunikacii, 2026. – No 3. – Pp. 13–24.
4. Ivanov V. G., Kuzina E. I., Gomanov D. E., Grishin P. S., Cheglov A. V., Kuzin P. I. Monitoring izmeneniya mestnosti po raznovremennym aehrokosmicheskim izobrazheniyam s primeneniem tehnologij glubogogo obucheniya nejronnyh setej // Geodeziya i kartografiya, 2025. – V.86. – No 5. – Pp. 39–46.
5. Filatov V. A., Kozyr' O. F. Model' povedeniya avtonomnogo scenariya v zadachah upravleniya raspredelennymi informacionnymi resursami // Inzhenernyj vestnik Dona, 2013. – No 3. – URL: ivdon.ru/ru/magazine/archive/n3y2013/1771.
6. Odoevskij S. M., Lebedev P. V. Metodika ocenki ustojchivosti funkcionirovaniya sistemy tehnologicheskogo upravleniya infokommunikacionnoj set'yu special'nogo naznacheniya s zadannoj topologicheskoj i funkcional'noj strukturoj // Sistemy upravleniya, svyazi i bezopasnosti, 2021. – No 1. – Pp. 152–189. – DOI: 10.24411/2410-9916-2021-10107.
7. Kondrashov Yu. V., Satdinov A. I., Sinyuk A. D., Ostroumov O. A. Konceptual'naya model' kontrolya funkcij sistemy svyazi dlya vyyavleniya konfliktnyh situacij // T-Comm: Telekommunikacii i transport, 2022. – V. 16. – No 5. – Pp. 21–27.
8. Zhang, H. The optimal control theory – a scientific approach to fundamentally solving control problems. Sci. China Inf. Sci. – 68, 116201 (2025). – URL: https://doi.org/10.1007/s11432-024-4180-2.
9. Khettabi I., Benyoucef L. & Boutiche M. A. Sustainable reconfigurable manufacturing system design using adapted multi-objective evolutionary-based approaches. Int J Adv Manuf Technol. – 115, 3741–3759 (2021). – URL: https://doi.org/10.1007/s00170-021-07337-3.
10. Lauta O. S, Balenko E. G., Fedorov V. H., Lepeshkin O. M., Ostroumov O. A. Metod postroeniya profilya funkcionirovaniya slozhnoj tehnicheskoj sistemy // Inzhenernyj vestnik Dona, 2023. – No 2. – URL: ivdon.ru/ru/magazine/archive/n2y2023/8183.
11. Chen J., Pan H., Zhang K. et al. Predictive control approach incorporating incremental learning. Appl Intell. – 55, 401 (2025). – URL: https://doi.org/10.1007/s10489-025-06243-5.
12. Tarasov A. A. Problema obespecheniya garantosposobnosti informacionnyh sistem i puti ee resheniya // Sistemy bezopasnosti, svyazi i telekommunikacij, 2000. – No 32. – Pp. 78–80.
13. Ostroumov O. A. Problema obespecheniya funkcional'noj ustojchivosti sistem kriticheski vazhnyh ob"ektov // Ehlektrosvyaz', 2022. – No 1. – Pp. 14–18.
14. Petrenko S. A. Koncepciya podderzhaniya rabotosposobnosti kibersistem v usloviyah informacionno-tehnicheskih vozdejstvij // Trudy ISA RAN, 2009. – V. 41. – Pp. 175–193.
15. Makarenko S. I., Kozlov K. V. Avtomatizirovannaya sistema upravleniya bespilotnymi letatel'nymi apparatami pri sovmestnom reshenii imi special'nyh zadach // Sistemy upravleniya, svyazi i bezopasnosti, 2025. – No 1. – DOI: 10.24412/2410-9916-2025-1-131-155.

4 ***Oleg A. Ostroumov***, Ph.D. of Technical Sciences, Lecturer of the Department of the Military Academy of Communications. St. Petersburg, Russia. E-mail: oleg-26stav@mail.ru

5 ***Oleg M. Lepeshkin***, Dr.Sc. of Technical Sciences, Associate Professor, Professor of the Department of the Military Academy of Communications. St. Petersburg, Russia. E-mail: lepeshkin1@yandex.ru

6 ***Alexander D. Sinyuk***, Dr.Sc. of Technical Sciences, Associate Professor, Military Academy of Communications. St. Petersburg, Russia. E-mail: eentrop@rambler.ru

16. Ivanov S. A. Metodika obespecheniya funkcionirovaniya informacionnogo napravleniya v seti svyazi s pamyat'yu v usloviyah nestabil'nosti harakteristik ehlementov seti // Izvestiya TulGU. Tehnicheskie nauki, 2021. – No 11.
17. Fathabadi A. S., Snook C., Dghaym D. et al. Systematic hierarchical analysis of requirements for critical systems. Innovations Syst Softw Eng (2024). – URL: https://doi.org/10.1007/s11334-024-00551-8.
18. Bai Z., Li C., Pourzamani J. et al. Optimizing the resource allocation in cyber physical energy systems based on cloud storage and IoT infrastructure. J Cloud Comp. – 13, 59 (2024). – URL: https://doi.org/10.1186/s13677-024-00615-x.
19. Smirnov A. V., Levashova T. V., Petrov M. V. Bazovyj scenarij podderzhki prinyatiya reshenij na osnove modelej zhizni pol'zovatelej v cifrovoj srede. Informacionno-upravlyayushchie sistemy, 2021. – No 4. – Pp. 47–60. – DOI: 10.31799/1684-8853-2021-4-47-60.
20. Ding D., Han Q. L., Ge X. et al. Privacy-preserving filtering, control and optimization for industrial cyber-physical systems. Sci. China Inf. Sci. – 68, 141201 (2025). – URL: https://doi.org/10.1007/s11432-024-4328-1.
21. Aung Chzho M'yu, Anisimov A. A., Gagarina L. G., Portnov E. M. Metodika povysheniya ehffektivnosti upravleniya resursoemkimi zadachami v raspredelennyh vychislitel'nyh sistemah // Inzhenernyj vestnik Dona, 2022. – No 2. – URL: ivdon.ru/ru/magazine/archive/n2y2022/6294.
22. Ala-Laurinaho R., Autiosalo J., Laine S. et al. Paradigm shift in mechanical system design: toward automated and collaborative design with digital twin web. Softw. Syst. Model (2024). – URL: https://doi.org/10.1007/s10270-024-01215-8.
23. Tsapko S. G., Tsapko I. V. & Tarakanov D. V. Efficiency of the Design Processes for Complex Systems with the Mathematical Apparatus of Fuzzy Sets. Autom. Doc. Math. Linguist. – 57, 258–266 (2023). – URL: https://doi.org/10.3103/S0005105523050096
24. Yang X., Jia K. & Peng Z. Construction of integrated network order system of main distribution network based on power grid operation control platform. Energy Inform. – 7, 70 (2024). – URL: https://doi.org/10.1186/s42162-024-00368-6.
25. Ribeiro R., Pilastri A., Moura C. et al. A data-driven intelligent decision support system that combines predictive and prescriptive analytics for the design of new textile fabrics. Neural Comput & Applic. – 35, 17375–17395 (2023). – URL: https://doi.org/10.1007/s00521-023-08596-9.
26. Ostroumov O. A., Lepeshkin O. M., Sinyuk A. D., Filimonov V. A. Optimizaciya profilya funkcionirovaniya slozhnoj tehnicheskoj sistemy // Informacionno-upravlyayushchie sistemy, 2023. – No 4 (125). – Pp. 12–25.
27. Menaceur A., Drid H. & Rahouti M. Fault Tolerance and Failure Recovery Techniques in Software-Defined Networking: A Comprehensive Approach. J Netw Syst Manage. – 31, 83 (2023). – URL: https://doi.org/10.1007/s10922-023-09772-x.
28. Ahmad I., Clark A., Ali M. et al. Determining critical nodes in optimal cost attacks on networked infrastructures. Discov. Internet Things. – 4, 2 (2024). – URL: https://doi.org/10.1007/s43926-023-00054-1.
29. Ostroumov O. A. Postroenie profilya funkcionirovaniya slozhnoj tehnicheskoj sistem // Ehlektrosvyaz', 2026. – No 1. – Pp. 18–26
30. Lepeshkin O. M., Lebedev P. V., Sinyuk A. D., Lepeshkin O. M. Grafo-matrichnaya strukturno-funkcional'naya model' slozhnoj tehnicheskoj sistemy // Problemy mashinostroeniya i avtomatizacii. – No 4 s1-2025. – Pp. 117–128.
31. Makarenko S. I., Nesterov A. A. Strukturno-funkcional'naya model' interoperabel'nosti organizacionno-tehnicheskih sistem // Trudy uchebnyh zavedenij svyazi, 2023. – No 4. – DOI: 10.31854/1813-324X-2023-9-4-65-74.

СТАТИСТИЧЕСКИЙ АНАЛИЗ РАДИОПРИЕМНИКА СИГНАЛОВ С ППРЧ И СЛУЧАЙНОЙ ЧАСТОТНОЙ МАНИПУЛЯЦИЕЙ В РЕЛЕЕВСКОМ КАНАЛЕ ПЕРЕДАЧИ ДАННЫХ С ШУМОВОЙ ПОМЕХОЙ И ДИФФУЗНОЙ МНОГОЛУЧЕВОСТЬЮ

Зеленевский В. В.[1], Бочкарев А. А.[2]

DOI:10.21681/3034-4050-2026-4-58-64

Ключевые слова: *псевдослучайная перестройка рабочей частоты, генератор псевдослучайных чисел, широкополосный фильтр, перемножитель, линия задержки, полосовой фильтр, сумматор, детектор огибающей, вычитающее устройство, вероятность битовой ошибки, шумовая помеха, диффузная многолучевость, отношение помеха/сигнал, коэффициент расширения спектра сигнала.*

Аннотация

Цель работы: *на основе общих теоретических положений, определяющих возможности использования сигналов с расширенным спектром для передачи данных в условиях релеевских замираний, вызванных диффузной многолучевостью, и воздействия преднамеренных шумовых помех, разработать математическую модель приёмника сигнала с псевдослучайной перестройкой радиочастоты (ППРЧ) и случайной частотной манипуляцией и оценить его помехоустойчивость..*

Метод: *статистический анализ помехоустойчивости радиоприемника двоичного сигнала с ППРЧ со случайной и неслучайной частотной манипуляцией с различной стратегией воздействия помех.*

Результат: *представлены результаты анализа статистических характеристик демодуляции сигнала с ППРЧ, установлено преимущество сигнала со случайной частотной манипуляцией по помехоустойчивость по сравнению с известными приемниками сигналов с неслучайной частотной манипуляцией.*

Научная новизна: *проведено обобщение и систематизированы известные модели сигналов с расширенным спектром, принимаемых в условиях релеевских замираний, вызванных диффузной многолучевостью сигнала. Сформирована математическая модель приемника сигнала со случайной частотной манипуляцией и ППРЧ, которая, в отличие от известных моделей, позволяет учитывать число разделяемых лучей, закон распределения плотности вероятностей, параметры сигналов и помех.*

Введение

Известно [1,3,4,5], стратегия борьбы с преднамеренными помехами в каналах передачи данных с частотной манипуляцией сигнала и ППРЧ заключается в «уходе» сигнала от воздействия помехи, а не в «противоборстве» с помехой, как это реализуется в приемниках радиосигналов с расширенным спектром методом прямой модуляции псевдослучайной последовательностью. Помехоустойчивость радиоканалов с ППРЧ зависит от времени работы на одной частоте, от вида помехи и ее мощности, мощности полезного сигнала, структуры приемного устройства, учитывающего характер многолучевости сигнала.

Для оценки помехоустойчивости радиоканала передачи данных в условиях замирания сигнала и воздействия помех необходимо иметь соответствующие характеристики замираний и показатели. При определенных моделях замираний сигнала, собственного шума приемника и аддитивных помех предпочтительным показателем помехоустойчивости является средняя вероятность ошибки на бит на выходе демодулятора.

Основная часть

Реализация режима ППРЧ в системе передачи данных со случайной двоичной частотной манипуляцией (ЧМ), при которой единичный и нулевой каналы передачи двоичных символов разнесены по частоте случайным образом для постановщика помех, представлена структурной схемой (рис. 1) [6,7].

Наличие двух независимых синтезаторов частоты позволяет излучать радиопередатчиком такие пары частот для единичного и нулевого двоичных символов, разность между которыми является случайной величиной при каждом скачке частоты. Это затрудняет радиоразведку сигнала с ППРЧ, так как случайная величина частотного разноса между единичным и нулевым

1 ***Зеленевский Владимир Владимирович***, доктор технических наук, профессор, профессор филиала Военной Академии Ракетных войск стратегического назначения им. Петра Великого. Серпухов, Россия. E-mail: zelenevsky.vladimir@gmail.com

2 ***Бочкарев Александр Алексеевич***, адъюнкт филиала Военной Академии Ракетных войск стратегического назначения им. Петра Великого. Серпухов, Россия. E-mail: bocha413@gmail.com

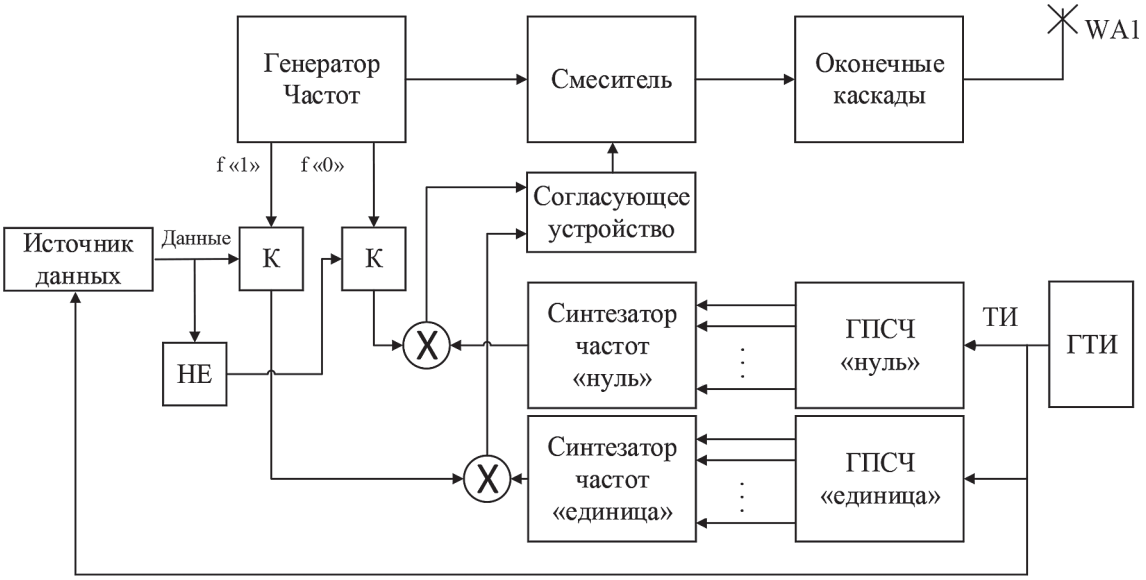


Рис. 1. Структурная схема радиопередатчика со случайной двоичной ЧМ и ППРЧ

символами не позволяет определить частоту свободного (дополнительного) канала передачи, воздействие помех на который является более эффективным, чем на действующий (активный в данном скачке) канал передачи данных[1,2,5,7].

При этом ключи К и инвертор НЕ обеспечивают поочередное и случайное подключение источника данных и синтезатеров частот нулевого и единичного каналов через согласующее устройство к смесителю радиопередатчика.

В условиях диффузной многолучевости принимаемого сигнала с частотной манипуляцией и ППРЧ, порождающей релеевские замирания, разделение лучей электромагнитной волны осуществляют корреляционным способом [2]. Структурная схема радиоприемника в этом случае имеет вид (рис. 2) [8].

Принимаемый сигнал на выходе широкополосного фильтра (ШПФ), который состоит из входных цепей и усилителя радиочастоты, во время i-го скачка частоты представляется как

$$U(t) = U\cos[(\omega_i + \theta_i)t - \varphi_i],\ 0 \le t \le T_в, \qquad (1)$$

где θ_i – частота модуляции; φ_i – начальная фаза i-го скачка частоты; $\omega_i = \omega_1, \omega_2$ (ω_1 – частота единичного символа, ω_2 – частота нулевого символа); $T_в$ – длительность двоичного символа.

Приемник имеет два канала обработки сигнала с ППРЧ. В случае идеальной временной синхронизации, обеспечиваемой блоком синхронизации (БС), на выходах перемножителей (П) будет формироваться сигнал промежуточной частоты $f_{ПЧ1} = const$, который выделяется полосовым фильтром (ПФ) в «единичном» канале, и $f_{ПЧ0} = const (f_{ПЧ0} \ne f_{ПЧ1})$, который выделяется полосовым фильтром (ПФ) в «нулевом» канале.

Для корреляционного разделения лучей сигнала устанавливаются линии задержки (ЛЗ), которые обеспечивают временной сдвиг сигналов генераторов сетки частот (ГСЧ) в «единичном» и «нулевом» каналах.

Сумматоры (Σ) осуществляют алгебраическое сложение мощностей сигналов по N лучам. Детекторы огибающей (ДО) и вычитающее устройство (ВУ) выносят решение о принятом двоичном символе.

Известно [1, 3], что для двоичной случайной ЧМ помехоустойчивость декаметрового радиоканала передачи данных с релеевскими замираниями принимаемого сигнала следует оценивать с учетом следующих условий:

- помеха воздействует на оба канала (активный, по которому идет передача данных, и свободный, по которому в данном скачке сигнала с ППРЧ данные не передаются);
- помеха воздействует только на один из возможных каналов передачи данных;
- помеха не воздействует ни на один из возможных каналов передачи данных.

При таком условии вероятность битовой ошибки с учетом релеевских замираний $P_{вг}$ будет определяться выражением [3].

$$P_{вг} = \int_0^\infty w(r) P_в\left(\alpha, L, \frac{P_П}{P_С}, r\right) dr, \qquad (2)$$

где $w(r)$ – плотность вероятностей результирующего отношения сигнал/шум на входе демодулятора, равная [2, 3]:

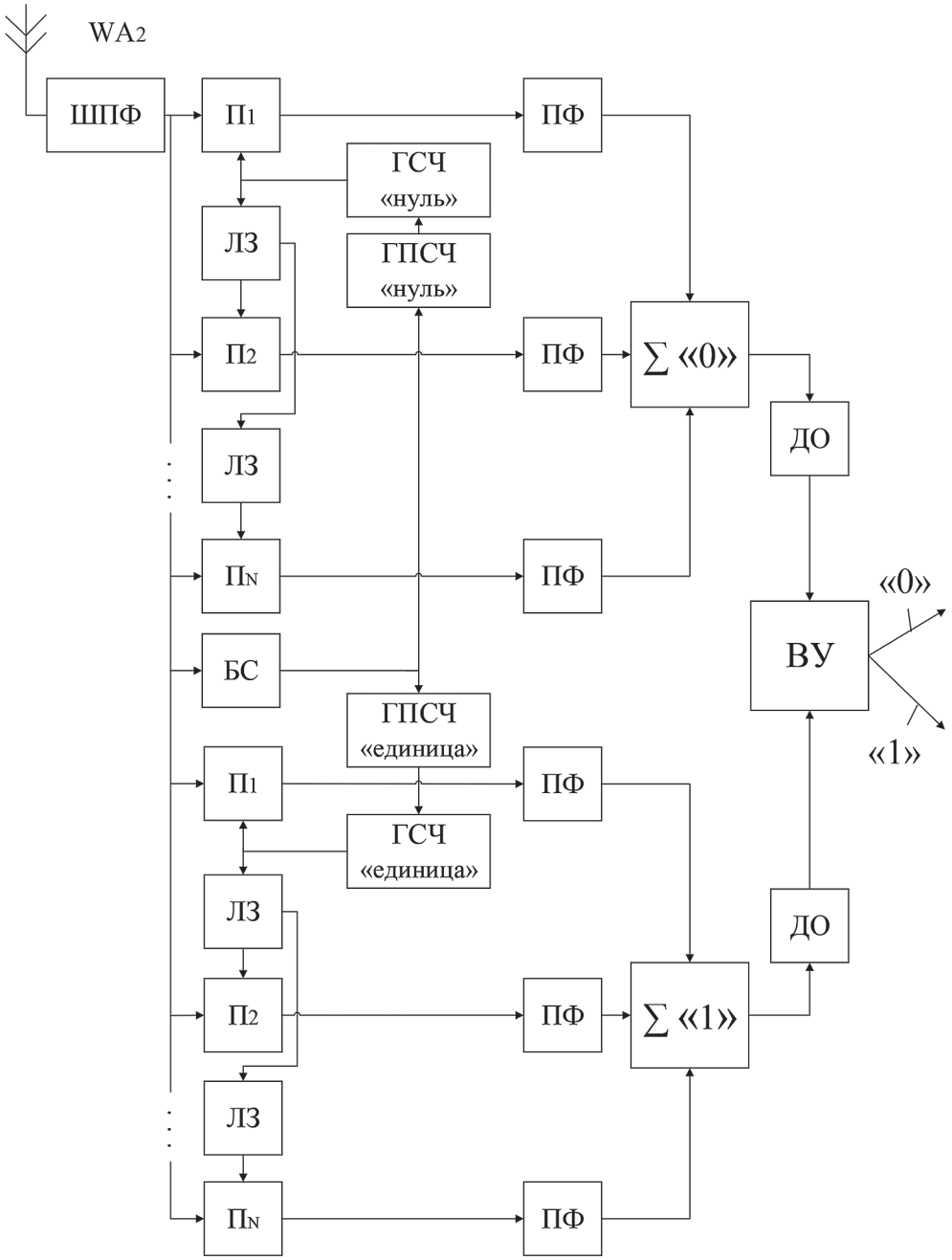


Рис. 2. Структурная схема радиоприемника с корреляционным разделением лучей

$$w(r) = \frac{\exp\left(-\frac{r}{Nh_0^2}\right)}{Nh_0^2}, \qquad (3)$$

где N – число лучей сигнала, которое принимает и обрабатывает радиоприемник; h_0^2 – отношение сигнал/шум в одном луче; $P_{\text{в}}(\alpha, L, \frac{P_{\text{П}}}{P_{\text{С}}}, r)$ – условная вероятность битовой ошибки, учитывающая три условия (представлены выше) воздействия шумовой помехи и равная [1, 2]

$$P_{\text{в}}(\alpha,2) = \frac{\alpha^2}{2}\exp\left[-\frac{1}{2}\left(\frac{1}{h_\Sigma^2 \equiv r} + \frac{P_{\text{П}}}{\alpha L P_{\text{С}}}\right)\right]^{-1},$$

при воздействии помехи на оба канала;

$$P_{\text{в}}(\alpha,1) = \alpha(1-\alpha)\exp\left[-\left(\frac{2}{h_\Sigma^2 \equiv r} + \frac{P_{\text{П}}}{\alpha L P_{\text{С}}}\right)^{-1}\right],$$

при воздействии помехи только на один канал передачи;

$$P_{\text{в}}(\alpha,0) = \frac{(1-\alpha)^2}{2}\exp\left(-\frac{h_\Sigma^2 \equiv r}{2}\right),$$

при отсутствии воздействия помехи; α – доля полосы частот сигнала, пораженная помехой с отношением помеха/сигнал $\frac{P_{\text{П}}}{P_{\text{С}}}$; L – коэффициент расширения спектра ЧМ сигнала в канале передачи данных с ППРЧ.

Тогда выражение для вероятности $P_{вz}$ запишем в виде [2]:

$$P_{вz} = \int_0^{\infty} \frac{\exp\left(-\frac{r}{Nh_0^2}\right)}{Nh_0^2} \left\{ \frac{\alpha^2}{2} \exp\left[-\frac{1}{2}\left(\frac{1}{r} + \frac{P_П}{\alpha L P_C}\right)\right]^{-1} + \right.$$
$$\left. + \alpha(1-\alpha)\exp\left[-\left(\frac{2}{r} + \frac{P_П}{\alpha L P_C}\right)^{-1}\right] + \frac{(1-\alpha)^2}{2}\exp\left(-\frac{2}{r}\right)\right\} dr. \quad (4)$$

В таблице 1 представлены оценки вероятности $P_{вz}$, рассчитанные по выражению (4).

Анализ результатов расчетов, представленных в таблице 1, показывает:

- при $N = const$, $\frac{P_П}{P_C} = const$, $L = const$ существует оптимальное значение α_{opt}, при котором вероятность $P_{вz}$ максимальная (помеха наносит наибольший ущерб каналу передачи данных);
- с изменением отношения $\frac{P_П}{P_C}$, коэффициента L значение α_{opt} также изменяется;
- изменение h_0^2 слабо влияет на изменение α_{opt} и $P_{вz}$ (например, при $h_0^2 = 10$ значение $\alpha_{opt} = 0{,}1445$, $h_0^2 = 100$ значение $\alpha_{opt} = 0{,}1387$, хотя $N = 15$, $\frac{P_П}{P_C} = 5$, $L = 15$ остались неизменными, а вероятность $P_{вz} = 0{,}0595$ соответствует $\alpha_{opt} = 0{,}1445$, $P_{вz} = 0{,}05312$ соответствует $\alpha_{opt} = 0{,}1387$);
- при $N = const$, $L = const$, $\frac{P_П}{P_C} = const$, $\alpha = const$ наблюдается медленное уменьшение вероятности $P_{вz}$ при больших изменениях h_0^2.

Для сравнения оценим вероятность ошибки $P_{вz}$ в канале с использованием ППРЧ и неслучайной частотной манипуляцией сигнала по выражению [2]:

$$P_{вz} = \frac{\alpha}{2}\int_0^{\infty}\left\{-\frac{e^{\left(\frac{-r}{N\cdot h}\right)}}{N\cdot h} e^{\left[\frac{-1}{2}\cdot\left(\frac{1}{r}+\frac{P_П}{P_C\cdot\alpha\cdot L}\right)^{-1}\right]} + \frac{(1-\alpha)}{2} e^{\frac{-r}{2}}\right\} dr. \quad (5)$$

В таблице 2 представлены оценки $P_{вz}$ для разных значений N, L и отношений h_0^2 и $\frac{P_П}{P_C}$, а на рисунке 3 соответствующие графики $P_{вz} = f(a)$.

При $\alpha = 1$, когда шумовая помеха в части полосы (полосы рабочих частот) трансформируется в широкополосную шумовую помеху (заградительную помеху), каналы передачи данных с релеевскими замираниями с неслучайной и случайной двоичной ЧМ имеют одну и ту же помехоустойчивость $P_{вz}$ равную:

$$P_{вz} = \frac{1}{2}\int_0^{\infty}\frac{\exp\left(\frac{-r}{Nh_0^2}\right)}{Nh_0^2}\exp\left[-\frac{1}{2}\left(\frac{1}{r}+\frac{P_П}{LP_C}\right)^{-1}\right]dr =$$
$$= \frac{1}{2}\int_0^{\infty}\frac{\exp\left\{-\left[\frac{r}{Nh_0^2}+\frac{1}{2}\left(\frac{1}{r}+\frac{P_П}{LP_C}\right)^{-1}\right]\right\}}{Nh_0^2}dr.$$

Анализ таблиц 1 и 2, графиков (рис. 3) показывает:

- как для случайной, так и неслучайной частотной модуляции сигнала с ППРЧ существует

Таблица 1.

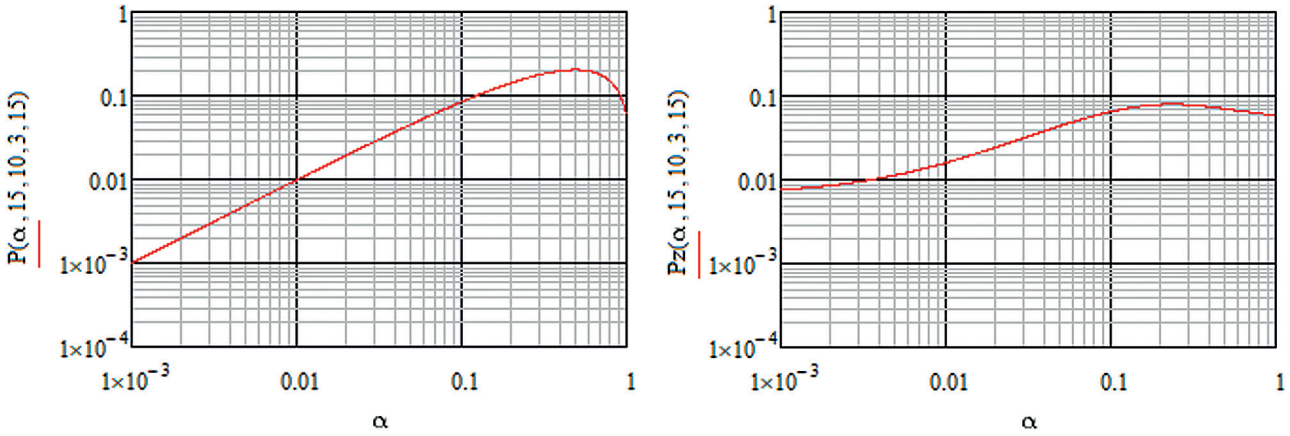
Оценки вероятности $P_{вz}$ для случайной ЧМ

$N = 7$; $h_0^2 = 10$; $\frac{P_п}{P_с} = 1$; $L = 15$	α	10^{-3}	10^{-2}	0,07047	0,1	1
	$P_{вz}$	0,015	0.022	0,039	0,039	0,02
$N = 15$; $h_0^2 = 10$; $\frac{P_п}{P_с} = 5$; $L = 31$	α	10^{-3}	10^{-2}	0,1	0,1445	1
	$P_{вz}$	$7{,}557 \cdot 10^{-3}$	0,016	0,059	0,064	0,039
$N = 15$; $h_0^2 = 100$; $\frac{P_п}{P_с} = 5$; $L = 15$	α	10^{-3}	10^{-2}	0,1	0,1387	1
	$P_{вz}$	$1{,}667 \cdot 10^{-3}$	0,01	0,072	0,087	0,114
$N = 15$; $\alpha = 0{,}14$; $\frac{P_п}{P_с} = 5$; $L = 31$	h_0^2	1,59	5	10	100	800
	$P_{вz}$	0,094	0,07	0,064	0,058	0,057

Таблица 2.

Оценки вероятности $P_{вz}$ для неслучайной ЧМ

$N = 7$; $h_0^2 = 10$; $\frac{P_п}{P_с} = 1$; $L = 15$	α	10^{-3}	10^{-2}	0,07047	0,1	1
	$P_{вz}$	$9{,}958 \cdot 10^{-4}$	$9{,}593 \cdot 10^{-3}$	0,054	0,054	0,02
$N = 15$; $h_0^2 = 10$; $\frac{P_п}{P_с} = 5$; $L = 31$	α	10^{-3}	10^{-2}	0,1	0,1445	1
	$P_{вz}$	$9{,}979 \cdot 10^{-4}$	$9{,}798 \cdot 10^{-3}$	0,082	0,109	0,039
$N = 15$; $h_0^2 = 100$; $\frac{P_п}{P_с} = 5$; $L = 15$	α	10^{-3}	10^{-2}	0,1	0,1387	1
	$P_{вz}$	$9{,}988 \cdot 10^{-4}$	$9{,}878 \cdot 10^{-3}$	0,088	0,116	0,114
$N = 15$; $\alpha = 0{,}14$; $\frac{P_п}{P_с} = 5$; $L = 31$	h_0^2	1,59	5	10	100	800
	$P_{вz}$	0,108	0,107	0,107	0,106	0,106



а) *б)*

Рис. 3. Зависимости вероятности битовой ошибки $P_{вг} = f(\alpha)$
а) для неслучайной частоты манипуляции; б) для случайной частотной манипуляции

Таблица 3.

Значения вероятности $P_{вг}$ для $\alpha = 1$

$N = 15;$ $h_0^2 = 2;$ $L = 15$	$\frac{P_п}{P_с}$	0,1	0,5	1	1,5	2	2,5	3	4
	$P_{вг}$	$6{,}76 \cdot 10^{-3}$	$7{,}664 \cdot 10^{-3}$	$9{,}964 \cdot 10^{-3}$	0,0161	0,02688	0,0413	0,058	0,093
$N = 15;$ $h_0^2 = 2;$ $L = 31$	$\frac{P_п}{P_с}$	0,5	1	1,5	2	2,5	3	4	8
	$P_{вг}$	$7{,}037 \cdot 10^{-3}$	$7{,}616 \cdot 10^{-3}$	$8{,}44 \cdot 10^{-3}$	$9{,}75 \cdot 10^{-3}$	0,01193	0,01525	0,0252	0,088
$N = 15;$ $h_0^2 = 15;$ $L = 15$	$\frac{P_п}{P_с}$	0,1	0,5	1	1,5	2	2,5	3	4
	$P_{вг}$	$4{,}52 \cdot 10^{-3}$	$5{,}142 \cdot 10^{-3}$	$6{,}85 \cdot 10^{-3}$	0,0123	0,02254	0,0367	0,0534	0,089
$N = 15;$ $h_0^2 = 15;$ $L = 31$	$\frac{P_п}{P_с}$	0,5	1	1,5	2	2,5	3	4	8
	$P_{вг}$	$4{,}72 \cdot 10^{-3}$	$5{,}11 \cdot 10^{-3}$	$5{,}69 \cdot 10^{-3}$	$6{,}68 \cdot 10^{-3}$	$8{,}51 \cdot 10^{-3}$	0,01148	0,02	0,084
$N = 15;$ $\frac{P_п}{P_с} = 15;$ $L = 15$	h_0^2	10	20	50	100	500	1000		
	$P_{вг}$	0,09284	0,086	0,081	0,079	0,077	0,077		
$N = 31;$ $\frac{P_п}{P_с} = 4;$ $L = 15$	h_0^2	10	20	50	100	500	1000		
	$P_{вг}$	0,086	0,0821	0,079	0,078	0,077	0,077		
$N = 15;$ $\frac{P_п}{P_с} = 4;$ $L = 31$	h_0^2	1,4	7	10	50	100	500		
	$P_{вг}$	0,081	0,0303	0,025	0,014	0,0121	0,011		
$N = 15;$ $\frac{P_п}{P_с} = 4;$ $L = 63$	h_0^2	1,4	3	10	50	200	1000		
	$P_{вг}$	0,0607	0,029	$9{,}59 \cdot 10^{-3}$	$2{,}25 \cdot 10^{-3}$	$5{,}84 \cdot 10^{-4}$	$1{,}2 \cdot 10^{-4}$		
$N = 15;$ $\frac{P_п}{P_с} = 10;$ $L = 63$	h_0^2	1,3	2	20	100	200	1000		
	$P_{вг}$	0,098	0,078	0,031	0,024	0,023	0,022		
$N = 1;$ $h_0^2 = 15;$ $L = 1$	$\frac{P_п}{P_с}$	0,1	0,5	1	2	3	4		
	$P_{вг}$	0,087	0,239	0,329	0,399	0,429	0,445		
$N = 2;$ $h_0^2 = 15;$ $L = 1$	$\frac{P_п}{P_с}$	0,1	0,5	1	2	3	4		
	$P_{вг}$	0,053	0,219	0,319	0,395	0,426	0,443		

экстремум в зависимости $P_{вz} = f(\alpha)$ при $N = const$, $h_0^2 = const$, $\frac{P_п}{P_с} = const$, $L = const$, для которого значение вероятности $P_{вz}$ наибольшее (например, для случайной частотной манипуляции $N = 7$, $h_0^2 = 10$, $\frac{P_п}{P_с} = 1$, $L = 15$ наибольшее значение $P_{вz} = 0{,}039$ и ему соответствует $0{,}1 > \alpha_{opt} \geq 0{,}07047$, а при $N = 15$, $h_0^2 = 10$, $\frac{P_п}{P_с} = 5$, $L = 31$ наибольшее значение $P_{вz} = 0{,}064$ и ему соответствует $\alpha_{opt} = 0{,}1445$);

- для неслучайной частотной манипуляции сигнала с ППРЧ (табл. 2) при $\alpha = \alpha_{opt}$ вероятность $P_{вz}$ заметно увеличивается по сравнению со случайной частотной манипуляцией (например, при $\alpha_{opt} = 0{,}07047$, $h_0^2 = 10$, $\frac{P_п}{P_с} = 1$, $L = 15$ наибольшее значение $P_{вz} = 0{,}054$, что больше, чем $P_{вz} = 0{,}039$ для случайной частотной манипуляции, при $\alpha_{opt} = 01445$, $N = 10$, $h_0^2 = 10$, $\frac{P_п}{P_с} = 5$, $L = 31$ наибольшее значение $P_{вz} = 0{,}109$, что значительно превышает $P_{вz} = 0{,}064$ для случайной частотной манипуляции сигнала;
- при $\alpha = 1{,}0$ вероятность $P_{вz}$ одинаковая как для случайной, так и для неслучайной частотной манипуляции.

В таблице 3 представлены оценки вероятности $P_{вz}$ для различных значений N и L, отношений h_0^2 и $\frac{P_п}{P_с}$ при $\alpha = 1$.

Анализ результатов расчетов, представленных в таблице 3, показывает:

- при $N = 15$, $h_0^2 = 10$ увеличение коэффициента L с 15 до 31 позволяет повысить помехоустойчивость радиоприемника (для $\frac{P_п}{P_с} = 4$ вероятность $P_{вz}$ уменьшилась примерно в 3,5 раза);
- при $\frac{P_п}{P_с} = 4 = const$, $L = 15 = const$ увеличение числа корреляторов (согласованных фильтров) N с 15 до 31 весьма слабо влияет на уменьшение вероятности $P_{вz}$ (для $h_0^2 = 20$ вероятность $P_{вz} = 0{,}086$ при $N = 15$, а при $N = 31$ значение $P_{вz} = 0{,}082$), а при $h_0^2 \geq 100$ значения $P_{вz}$ не отличаются;
- коэффициент расширения спектра сигнала L играет определяющую роль в уменьшении вероятности $P_{вz}$ (при $N = 15 = const$, $\frac{P_п}{P_с} = 4 = const$, $L = 15$, $h_0^2 = 50$ вероятность $P_{вz} = 0{,}079$, а при $L = 63$, $h_0^2 = 50$ значение $P_{вz} = 2{,}25 \cdot 10^{-3}$, т.е. уменьшилось более чем в 30 раз);
- при $L = 63$, $N = 15$, $\frac{P_п}{P_с} = 10$ обеспечивается $P_{вz} = 0{,}078$ для $h_0^2 = 2$, а для $L = 31$, $N = 15$ вероятность $P_{вz} = 0{,}078$ обеспечивается при $\frac{P_п}{P_с} = 4$ и $h_0^2 = 100$;
- без расширения спектра ($L = 1$) сигнала, даже при $N = 2$, работа радиоканала возможна только при $\frac{P_п}{P_с} \leq 0{,}1$.

Выводы

- как для случайной, так и неслучайной ЧМ существует оптимальное значение доли полосы частот сигнала с ППРЧ, пораженной помехой с отношением $\frac{P_п}{P_с}$, при которой вероятность $P_{вz}$ наибольшая;
- для одинаковых исходных данных h_0^2, N, L, $\frac{P_п}{P_с}$ радиоканал передачи данных со случайной двоичной частотной манипуляцией более помехоустойчив (имеет меньшую вероятность $P_{вz}$) к шумовой помехе в части полосы рабочих частот, чем радиоканал с неслучайной ЧМ;
- при заградительной помехе, когда шумовая помеха в части полосы превращается в широкополосную помеху ($\alpha = 1$) радиоканалы со случайной и неслучайной ЧМ имеют одну и ту же помехоустойчивость (равные значения $P_{вz}$) и для защиты от такой помехи целесообразно использовать сигнал с ППРЧ, имеющий коэффициент расширения спектра $L \geq 31$.

Литература

1. Борисов В. И., Зинчук В. М., Лимарев А. Е., Немчилов А. В., Чаплыгин А. А. Пространственные и вероятностно-временные характеристики эффективности станций ответных помех при подавлении систем радиосвязи / Под ред. В. И. Борисова. – М.: Радио Софт, 2008. – 362 с.
2. Зеленевский В. В., Зеленевский Ю. В., Попов А. В., Наконечный А. Б. Методика оценки помехоустойчивости и надежности радиоканалов передачи данных при диффузной многолучевости сигнала // Известия Института инженерной физики: научн.-техн. журн. – Серпухов: 2025. – № 3. – С.17–24.
3. Зеленевский В. В. Помехоустойчивость приема избыточных частотно-манипулированных сигналов на фоне гармонических помех. Научно-технический журнал. Радиотехника, – М.: 2002. – №7. – С. 32–36.
4. Куликов Г. В. Влияние гармонической помехи на помехоустойчивость корреляционного демодулятора сигналов с МЧМ. Н/Т Радиотехника – М: 2002. – № 7. – С 42–44.
5. В. И. Борисов, В. М. Зинчук, А. Е. Лимаров, В. И. Шестопалов. Помехоустойчивость систем радиосвязи с расширением спектра прямой модуляцией псевдослучайной последовательностью / Под ред. В. И. Борисова. Изд. 2, перераб. и доп. – М.: Радиософт, 2011. – 550 с.
6. Зеленевский Ю. В. Методы информанционно-статического анализа и алгебраического синтеза в конечном поле корректирующих кодов повышенной помехозащищенности с широкополосным доступом. Диссертация на соискание ученой степени ДТН. – Серпухов: МОУ ИИФ. – 2014. – 322 с.

7. Зеленевский В. В. Зеленевский Ю. В., Попов А. В., Наконечный А. Б. Статистический анализ радиоканалов передачи данных с расширенным спектром сигналов. // Известия ИИФ: научно-технический журнал. – Серпухов: 2025. – № 2. – С. 32–35.
8. Наконечный А. Б. Методика оценки помехоустойчивости и надежности радиоканалов передачи данных при диффузной многолучевости сигнала [Текст]. В. В. Зеленевский, Ю. В. Зеленевский, А. В. Попов. //Известия ИИФ: научно-технический журнал. – Серпухов: 2025. – № 3. – С. 17–24.

STATISTICAL ANALYSIS OF A RADIO RECEIVER OF RF-FREQUENCY SIGNALS AND RANDOM FREQUENCY MANIPULATION IN A RAYLEIGH DATA TRANSMISSION CHANNEL WITH NOISE INTERFERENCE AND DIFFUSE MULTIPATH

Zelenevsky V. V.[3], Bochkarev A. A.[4]

Keywords: *pseudorandom tuning of the operating frequency, pseudorandom number generator, broadband filter, multiplier, delay line, bandpass filter, adder, envelope detector, subtractor, bit error probability, noise interference, diffuse multipath, interference/signal ratio, signal spectrum expansion coefficient.*

Abstract

The purpose of the work: *based on general theoretical principles that determine the possibilities of using extended-spectrum signals for data transmission in conditions of relay fading and exposure to intentional interference, a mathematical model of a signal receiver with pseudorandom radio frequency tuning (RFRF) has been developed.*

Method: *statistical analysis of the noise immunity of a binary RF radio receiver with random and non-random frequency manipulation with different interference strategies.*

Result: *the results of an analysis of the static characteristics of the demodulation of a signal with a frequency converter are presented, and the advantage of a signal with random frequency manipulation is established.*

Scientific novelty: *the well-known models of signals with an extended spectrum received under conditions of Rayleigh fading caused by diffuse multipath signals are generalized and systematized. A mathematical model of a signal receiver with random frequency manipulation and RF frequency response has been formed, which, unlike known models, allows taking into account the number of split beams, the law of probability density distribution, signal parameters and interference.*

References

1. Borisov V. I., Zinchuk V.M ., Limarev A. E., Nemchilov A. V., Chaplygin A. A. Prostranstvennye i veroyatnostno-vremennye harakteristiki ehffektivnosti stancij otvetnyh pomeh pri podavlenii sistem radiosvyazi / Pod red. V. I. Borisova. – M.: RadioSoft, 2008.– 362 p.
2. Zelenevskij V. V., Zelenevskij Yu. V., Popov A. V., Nakonechnyj A. B. Metodika ocenki pomehoustojchivosti i nadezhnosti radiokanalov peredachi dannyh pri diffuznoj mnogoluchevosti signala.// Izvestiya Instituta inzhenernoj fiziki: nauchn.-tehn. zhurn. – Serpuhov: 2025. – No 3. – Pp. 17–24.
3. Zelenevskij V. V. Pomehoustojchivost' priema izbytochnyh chastotno-manipulirovannyh signalov na fone garmonicheskih pomeh. Nauchno-tehnicheskij zhurnal. Radiotehnika. – M.: 2002. – No 7. – Pp. 32–36.
4. Kulikov G. V. Vliyanie garmonicheskoj pomehi na pomehoustojchivost' korrelyacionnogo demodulyatora signalov s MCHM. N/T Radiotehnika. – M.: 2002. – No 7. – Pp. 42–44.
5. V. I. Borisov, V. M. Zinchuk, A. E. Limarov, V. I. Shestopalov. Pomehoustojchivost' sistem radiosvyazi s rasshireniem spektra pryamoj modulyaciej psevdosluchajnoj posledovatel'nost'yu / Pod red. V. I. Borisova. Izd. 2, pererab. i dop. – M.: Radiosoft, 2011. – 550 p.
6. Zelenevskij Yu. V. Metody informancionno-staticheskogo analiza i algebraicheskogo sinteza v konechnom pole korrektiruyushchih kodov povyshennoj pomehozashchishchennosti s shirokopolosnym dostupom. Dissertaciya na soiskanie uchenoj stepeni DTN. – Serpuhov: MOU IIF. – 2014. – 322 p.
7. Zelenevskij V. V. Zelenevskij Yu. V., Popov A. V., Nakonechnyj A. B. Statisticheskij analiz radiokanalov peredachi dannyh s rasshirennym spektrom signalov. // Izvestiya IIF: nauchno-tehnicheskij zhurnal – Serpuhov: 2025. – No 2. – Pp. 32–35.
8. Nakonechnyj A. B. Metodika ocenki pomehoustojchivosti i nadezhnosti radiokanalov peredachi dannyh pri diffuznoj mnogoluchevosti signala [Tekst]. V. V. Zelenevskij, Yu. V. Zelenevskij, A. V. Popov. //Izvestiya IIF: nauchno-tehnicheskij zhurnal. – Serpuhov: 2025. – №3. – Pp. 17–24.

3 ***Vladimir V. Zelenevsky***, Doctor of Technical Sciences, Professor, Professor of the Branch of the Military Academy of Strategic Missile Forces named after Peter the Great, Serpukhov. Russia. E-mail: zelenevsky.vladimir@gmail.com

4 ***Alexander A. Bochkarev***, adjunct of the branch of the Military Academy of the Strategic Missile Forces named after Peter the Great, Serpukhov, Russia. E-mail: bocha413@gmail.com

РАЗРАБОТКА АДАПТИВНОЙ АНТЕННОЙ РЕШЕТКИ ДЛЯ БПЛА

Бабенко В. Ю.[1], Федоров П.Н.[2]

DOI:10.21681/3034-4050-2026-4-65-74

Ключевые слова: *программируемая логическая интегральная схема, Zynq UltraScale+, диаграммообразование, круговая поляризация, микрополосковая антенна, взаимная связь, зондовое питание.*

Аннотация

Цель работы: *разработка и исследование комплексной архитектуры 4-канальной малогабаритной адаптивной антенной решетки диапазона 2,4–2,5 ГГц, включающей вычислительное ядро на базе ПЛИС Xilinx Kria, многоканальный приемопередающий тракт и излучающую систему с круговой поляризацией.*

Метод исследования: *работа основывается на совместном применении методов теории цифровой обработки сигналов для пространственной фильтрации (алгоритм RAIS-LCMV), методов вычислительной электродинамики (САПР CST Microwave Studio) для проектирования высокочастотных структур, а также теории микрополосковых антенн для обеспечения требуемых поляризационных характеристик.*

Результаты исследования: *предложена и обоснована аппаратная архитектура цифровой адаптивной антенной решетки на базе кристалла XCK26-SFVC784-2LV-C и 4-канального трансивера, обеспечивающего жесткую фазовую когерентность. Разработана излучающая система на диэлектрической подложке FR-4 в конфигурации матрицы 2x2. Для формирования круговой поляризации применен метод усечения диагональных углов изолированного квадратного резонатора при одноточечном зондовом питании. Успешно реализован метод пространственной ортогональной ориентации элементов (последовательный поворот на 90°), позволивший радикально снизить взаимную связь до уровня –16 дБ без увеличения физических габаритов. Электродинамическое моделирование подтвердило формирование стабильного главного лепестка с коэффициентом направленного действия 10 дБи и шириной луча более 60 градусов. Выявлено, что физические ограничения одноточечной запитки формируют минимальный осевой коэффициент (Axial Ratio) на уровне 4 дБ, что успешно компенсируется алгоритмами пространственной фильтрации.*

Научная новизна: *обосновано комплексное применение робастного алгоритма пространственной фильтрации RAIS-LCMV для компенсации аппаратных и электродинамических искажений (отклонения поляризации, кросс-поляризационные помехи, технологические допуски FR 4), возникающих в малогабаритных печатных антенных решетках с зондовым питанием, что позволяет формировать глубокие нули в диаграмме направленности при неидеальных характеристиках излучателей.*

Введение и постановка задачи

В современных условиях эксплуатации беспилотных летательных аппаратов (БПЛА) и портативных наземных станций связи одной из наиболее важных в комплексе проблем является обеспечение высокой надежности и непрерывности работы радиоканалов управления и телеметрии. Подавляющее большинство малогабаритных коммерческих и специализированных комплексов функционирует в ISM-диапазоне частот 2,4–2,5 ГГц. Данный спектр подвержен не только высокому уровню непреднамеренных помех из-за перегруженности гражданскими системами связи, но и интенсивному преднамеренному воздействию средств радиоэлектронной борьбы (РЭБ), применяющих как широкополосные заградительные, так и узкополосные прицельные помехи.

Классические методы повышения помехозащищенности, работающих на основе псевдослучайной перестройки рабочей частоты (ППРЧ) и помехоустойчивом канальном кодировании [1], в условиях сложной помеховой обстановки оказываются недостаточными. При превышении уровня мощности помехи над полезным сигналом (отрицательное отношение сигнал/шум) входные каскады приемников уходят в режим насыщения или нелинейный режим усиления входного тракта приемника, блокируя полезный сигнал. Наиболее эффективным решением данной проблемы является переход к пространственной селекции сигналов с использованием бортовых цифровых адаптивных антенных решеток (ААР, или CRPA – Controlled Reception Pattern Antenna) [2–4]. Методы цифрового диаграммообразования и пространственной фильтрации сегодня являются стандартом де-факто и активно внедряются не только в комплексах специальной связи, но и в спутниковых системах навигации, а также перспективных гражданских сетях 5G и 6G [5–11]. Метод CRPA позволяет в реальном масштабе времени формировать глубокие

1 ***Бабенко Вячеслав Юрьевич***, оператор научной роты военной академии связи им. Маршала Советского Союза С. М. Буденного, г. Санкт-Петербург, Россия. E-mail: babenko.vya@mail.ru

2 ***Федоров Павел Николаевич***, старший научный сотрудник научно-исследовательского центра военной академии связи им. Маршала Советского Союза С. М. Буденного, г. Санкт-Петербург, Россия. E-mail: fedorovpn@yandex.ru

провалы («нули») в диаграмме направленности (ДН) в секторах пространственного расположения источников помех, сохраняя при этом высокий коэффициент усиления в направлении полезного сигнала.

Однако реализация ААР для маневрирующих БПЛА представляет собой сложную техническую задачу. Жесткие ограничения на массогабаритные характеристики, энергопотребление и вычислительную мощность требуют совместного проектирования аналоговой СВЧ-части, цифрового вычислителя и излучающей системы. Целью данной работы является разработка, обоснование и электродинамическое моделирование комплексной аппаратной архитектуры 4-канальной цифровой антенной решетки, от вычислительного ядра до топологии излучающих элементов, с учетом специфики полета беспилотных платформ.

Архитектура радиочастотного тракта и вычислительного ядра цифровой ААР

Современная парадигма построения малогабаритных ААР подразумевает полный отказ от использования громоздких и узкополосных аналоговых СВЧ-фазовращателей в пользу полностью цифрового диаграммообразования (Digital Beamforming). В разрабатываемой архитектуре сигнал от каждого из четырех антенных элементов (конфигурация решетки 2x2) проходит индивидуальный путь: усиливается, фильтруется, оцифровывается выделенным каналом аналого-цифрового преобразователя (АЦП) и передается в вычислительное ядро для математической обработки комплексными весовыми коэффициентами.

Для корректной работы алгоритмов пространственной фильтрации важно обеспечить строгую фазовую когерентность всех приемных каналов. На начальных этапах прототипирования системы рассматривалось использование сдвоенных микросхем приемопередатчиков Lime Microsystems LMS7002M (каждый из которых обеспечивает формулу 2x2 MIMO). Однако масштабирование такой архитектуры до 4 независимых каналов приема путем каскадирования двух чипов выявило фундаментальную проблему: при каждом цикле инициализации внутренние синтезаторы частот (PLL) и гетеродины (LO) микросхем запускаются с произвольной начальной фазой. Возникающий случайный межканальный фазовый сдвиг делает невозможным точную пеленгацию на источник помехи без проведения постоянной внешней калибровки, что недопустимо в динамичных условиях полета [12].

В связи с этим, для реализации радиочастотного тракта действующего макета выбран подход на базе интегрированных 4-канальных широкополосных приемопередатчиков с архитектурой прямого преобразования (Zero-IF). Подобные трансиверы имеют общий внутренний синтезатор частот, который аппаратно обеспечивает фазовую привязку и нулевой фазовый дрейф между всеми четырьмя приемными каналами. Архитектура аналоговой части до входа в трансивер включает в себя малошумящие усилители (МШУ) для обеспечения требуемого коэффициента шума системы и узкополосные поверхностно-акустические фильтры (ПАВ/SAW) на диапазон 2,4–2,5 ГГц, защищающие встроенные АЦП от внеполосного блокирования мощными сигналами. Оцифрованный квадратурный поток (I/Q) данных с трансивера передается в вычислительное устройство по высокоскоростному дифференциальному интерфейсу JESD204B, что кардинально минимизирует количество сигнальных линий на печатной плате.

Адаптивная обработка сигналов требует выполнения ресурсоемких матричных операций (обращение ковариационной матрицы, перемножение векторов) с фиксированной или плавающей точкой в жестком реальном времени. Классические микропроцессоры общего назначения не способны обеспечить необходимый уровень параллелизма для расчета многоканальных цифровых фильтров на высоких частотах дискретизации.

Оптимальным решением является использование гетерогенной системы на кристалле (SoC) Xilinx Zynq UltraScale+, в частности кристалла XCK26-SFVC784-2LV-C, входящего в семейство Kria. Архитектура SoC логически разделена на две независимые, но тесно взаимодействующие подсистемы. Программируемая логика (Programmable Logic – PL) берет на себя весь массив параллельных вычислений. В PL-части реализуются каскады цифрового понижения частоты (DDC), блоки децимации, а также конвейерные вычислители весовых коэффициентов с активным использованием аппаратных DSP-блоков (DSP48E2). Аппаратный параллелизм ПЛИС гарантирует минимальную латентность системы от момента оцифровки до формирования очищенного сигнала. Процессорная система (Processing System – PS) включает в себя многоядерный кластер ARM Cortex-A53, который функционирует под управлением операционной системы реального времени (ОСРВ). В его задачи входит инициализация трансивера по шине SPI, мониторинг сигнальной обстановки, управление калибровкой и обмен отфильтрованными пакетами данных с полетным контроллером БПЛА (рис. 1).

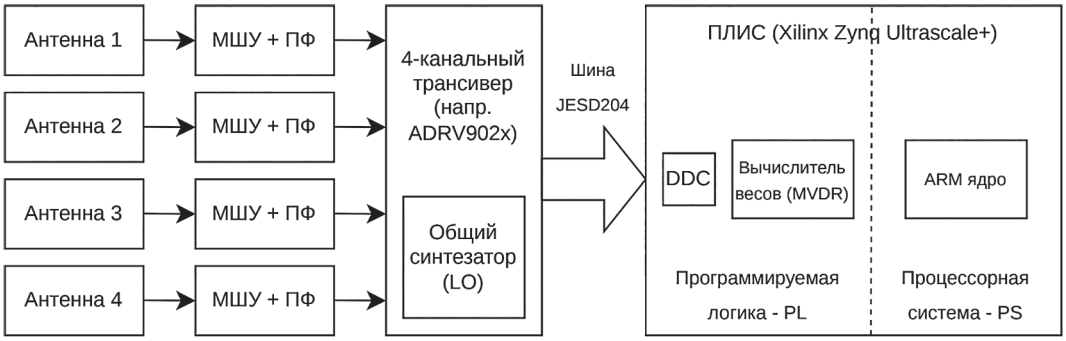


Рис. 1. Структурная схема аппаратной платформы

В вычислительном ядре ПЛИС реализован робастный алгоритм адаптивного подавления помех RAIS-LCMV (Robust Adaptive Interference Suppression based on Linearly Constrained Minimum Variance) [13]. Вектор входных сигналов решетки $\mathbf{x}(t)$ размерности 4×1 можно представить как сумму полезного сигнала, пространственных помех и теплового шума. Задача алгоритма заключается в нахождении вектора комплексных весовых коэффициентов $\mathbf{w}$, который минимизирует выходную мощность решетки (подавляет помехи), при этом сохраняя заданный коэффициент передачи в направлении прихода полезного сигнала.

Классическая оптимизационная задача алгоритма LCMV имеет вид [14]:

$$\min \mathbf{w}^H \mathbf{R}_{xx} \mathbf{w}, \text{ при условии } \mathbf{w}^H \mathbf{A}(\theta_0) = 1, \qquad (1)$$

где $\mathbf{R}_{xx} = E[\mathbf{x}(t)\mathbf{x}^H(t)]$ – ковариационная матрица входных сигналов, $\mathbf{A}(\theta_0)$ – управляющий вектор в направлении прихода полезного сигнала θ_0, а $(\cdot)\mathrm{H}$ – оператор эрмитова сопряжения.

Оптимальное решение данной задачи задается формулой:

$$\mathbf{w}_{opt} = \frac{\mathbf{R}_{xx}^{-1}\mathbf{A}(\theta_0)}{\mathbf{A}^H(\theta_0)\mathbf{R}_{xx}^{-1}\mathbf{A}(\theta_0)}. \qquad (2)$$

Однако в реальных условиях эксплуатации физические параметры малогабаритной антенной решетки (допуски изготовления подложки из текстолита, взаимная электромагнитная связь антенных элементов, несовершенство поляризации) приводят к тому, что реальный вектор направленности отличается от теоретического $\mathbf{A}(\theta_0)$. В таких условиях классический LCMV может непреднамеренно подавлять сам полезный сигнал, воспринимая его как помеху. Для решения этой проблемы применяется модификация RAIS, которая включает диагональное нагружение ковариационной матрицы ($\mathbf{R}_{xx} + \alpha\mathbf{I}$, где α – коэффициент регуляризации) и расширение ограничений на сектор углов. Это требует от ПЛИС XCK26 высокой разрядности вычислений для предотвращения потери точности при обращении матриц, но гарантирует высокую устойчивость (робастность) диаграммы направленности в сложной помеховой обстановке.

Проектирование излучающей системы адаптивной антенной решетки

Высочайшая вычислительная мощность ядра алгоритма RAIS-LCMV, реализованного в ПЛИС XCK26, может быть конвертирована в реальную помехозащищенность канала связи только при наличии высококачественной первичной пространственной выборки сигналов. Эту задачу выполняет электродинамическая часть комплекса – антенная решетка. К излучающей системе малогабаритного БПЛА предъявляются строгие противоречивые требования: минимальные масса и габариты, низкий аэродинамический профиль, а также способность поддерживать стабильный канал связи при сложном пространственном маневрировании аппарата (по тангажу, крену и рысканью).

В качестве материала диэлектрической подложки для действующего макета был выбран доступный фольгированный стеклотекстолит марки FR-4. Прототипирование излучающей поверхности осуществлялось методом высокоточного фрезерования на гравировальном станке с ЧПУ. Выбор данного диэлектрика обусловлен технологичностью изготовления макетов, однако высокий тангенс угла потерь ($tg\delta \approx 0{,}02$) и нестабильность эффективной диэлектрической проницаемости ($\varepsilon r \approx 4{,}4$) текстолита в СВЧ-диапазоне предъявляют повышенные требования к топологической оптимизации излучателей.

В качестве базового элемента решетки была выбрана микрополосковая антенна (патч), обеспечивающая низкий профиль. На начальных этапах исследований рассматривалась топология планарного питания излучателей, при котором подвод СВЧ-энергии осуществляется посредством микрополосковой линии, врезающейся

в полотно патча (inset fed). Однако электродинамический анализ показал, что для четырехканальной решетки конфигурации 2x2 такой подход непригоден. Разветвленная сеть питающих линий на лицевой стороне платы значительно увеличивает физическую площадь антенной системы, не позволяя сблизить центры излучателей на оптимальное для алгоритмов обработки сигналов расстояние (порядка $d \approx \lambda/2$). Кроме того, сами планарные линии становятся источником паразитного излучения, которое деформирует фазовый фронт и искажает диаграмму направленности антенной решетки.

Для решения этой проблемы был реализован переход к независимому коаксиальному зондовому питанию (pin-fed). В данной конфигурации центральная жила коаксиального перехода проходит сквозь диэлектрическую подложку и экранный слой, электрически соединяясь с полотном патча, в то время как оплетка замыкается на полигон заземления. Зондовое питание позволяет разместить трансиверы и всю радиочастотную разводку с обратной (теневой) стороны решетки, полностью изолировав цифровую и ВЧ-часть схемы от излучающей апертуры.

Координата точки запитки (feed offset) критически важна для обеспечения согласования с волновым сопротивлением тракта (50 Ом). В ходе параметрической оптимизации в САПР смещение зонда от центра патча было точно рассчитано и составило 9,52 мм. Топология одиночного элемента и его базовые параметры представлены ниже (рис. 2, табл. 1).

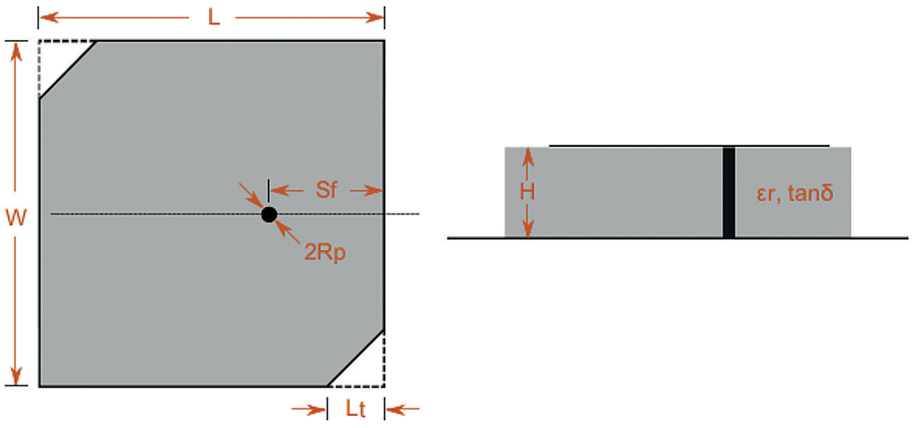
В реальных условиях эксплуатации ориентация вектора напряженности электрического поля антенны БПЛА относительно наземной станции постоянно меняется. При использовании антенн с линейной поляризацией это приводит к критическому поляризационному рассогласованию (вплоть до полных замираний сигнала с потерями более 20 дБ). Для устранения данной уязвимости излучатель должен обладать круговой поляризацией (КП).

Таблица 1.
Основные параметры антенной решетки

Параметр	Обозначение	Значение
Размер патча	L, W	28,49 мм
Длина среза угла	L_t	2,10 мм
Координата зонда	S_f	9,52 мм
Радиус проводника	R_p	0,14 мм
Толщина подложки	H	1,5 мм
Диэл. прониц. подложки	ε_r	4,4
Период антенной решетки	d	60,5 мм

Для минимизации габаритов и упрощения конструкции (отказ от гибридных квадратурных 90-градусных делителей мощности) была поставлена задача получить КП с помощью только одной точки питания на каждый элемент. Базовая форма патча была изменена с прямоугольной на строго квадратную с физическими размерами сторон $L = W = 28{,}49$ мм. Принцип получения круговой поляризации в такой топологии заключается в искусственном снятии вырождения резонансных мод. В идеальном квадратном резонаторе возбуждается основная мода TM_{10}. Однако, если усечь два противоположных диагональных угла квадрата (размер катета срезаемого треугольника $\Delta L = 2{,}10$ мм), симметрия структуры нарушается.

Математически это приводит к расщеплению основной моды на две пространственно



а) *б)*

Рис. 2. Топология одиночного антенного элемента:
а) вид сверху; б) в разрезе

ортогональные вырожденные моды (TM_{10} и TM_{01}). Вследствие изменения путей протекания поверхностных токов, резонансная частота одной моды смещается немного вниз, а другой – немного вверх относительно центральной частоты. При возбуждении зондом, расположенным на оси симметрии усеченных углов, обе моды возбуждаются с равной амплитудой. На центральной рабочей частоте (пересечение скатов резонансных кривых) разность фаз между этими модами достигает ровно 90°. Суперпозиция двух ортогональных векторов с равной амплитудой и квадратурным фазовым сдвигом формирует электромагнитную волну с круговой (эллиптической) поляризацией.

Масштабирование одиночного излучателя в матрицу 2x2 неизбежно сопровождается эффектом взаимного влияния (Mutual Coupling). Электромагнитная связь возникает как за счет распространения поверхностных волн (surface waves) в слое диэлектрика FR-4, так и за счет связи в ближней зоне (near-field coupling) через свободное пространство. Взаимная связь является одним из главных деструктивных элементов алгоритмов цифрового диаграммообразования, так как она искажает амплитудно-фазовое распределение, ухудшает коэффициент эллиптичности поляризации и приводит к ошибкам при вычислении ковариационной матрицы помех $\mathbf{R}_{xx}$ в ПЛИС.

Для значительного снижения взаимной связи без увеличения физических размеров решетки был применен метод взаимной пространственной ортогональности. Каждый антенный элемент в матрице был развернут на 90° вокруг своей оси относительно соседнего элемента.

Физический смысл данного решения заключается в том, что векторы поверхностных токов и структура ближнего поля патч-антенны резко асимметричны. Направляя сильно излучающую E-плоскость (плоскость электрического вектора) одного патча на слабо излучающую H-плоскость (плоскость магнитного вектора) соседнего патча, удается минимизировать перекрестные помехи. Для сохранения синфазности принимаемых сигналов при цифровой обработке, аппаратный поворот физических антенн математически компенсируется в ПЛИС путем внесения статического фазового сдвига $ej\pi/2$ в весовые коэффициенты соответствующих цифровых каналов.

На представленной модели (рис. 3) наглядно отображена геометрия резонаторов: усечение противоположных углов для генерации ортогональных мод TM10 и TM01, а также координаты точек коаксиальной запитки (выделены маркерами портов). Как видно из топологии, порты смещены относительно центральных осей симметрии матрицы. Строго последовательный поворот каждого из четырех элементов формирует пространственно-асимметричную структуру ближнего поля. Данный топологический прием является критически важным для изоляции портов трансивера от мощных перекрестных наводок, неизбежно возникающих при размещении излучателей на общей диэлектрической подложке FR-4 с высокой плотностью компоновки.

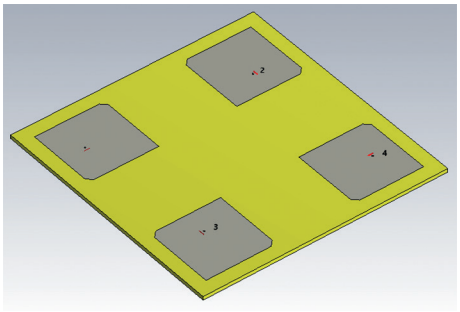


Рис. 3. Трехмерная CAD-модель 4-канальной антенной решетки в среде CST Microwave Studio: демонстрация метода последовательного поворота элементов на 90° и топологии усеченных углов

Результаты электродинамического моделирования и системный анализ

Для оценки характеристик антенной решетки в CST Microwave Studio использовался частотный решатель на базе метода конечных элементов (МКЭ). Выбор данного метода обусловлен его высокой точностью при расчете узкополосных структур и параметров круговой поляризации.

Для корректного учета геометрии усеченных углов и зондового питания применялась адаптивная тетраэдральная сетка, автоматически уплотняющаяся в зонах высокой напряженности поля. Моделирование проводилось в условиях свободного пространства с использованием поглощающих граничных условий, что обеспечило высокую достоверность расчета S-параметров и коэффициента эллиптичности.

Первым этапом анализа стала оценка качества согласования антенных элементов с волновым сопротивлением питающего тракта (50 Ом). На графике параметра $S11$ (коэффициент отражения) зафиксировано формирование выраженного резонанса (рис. 4).

Установлено, что уровень коэффициента отражения по входу не превышает критической отметки –10 дБ (что соответствует КСВ $\leq$ 2) в полосе частот от 2,415 до 2,465 ГГц. Ширина рабочей полосы по уровню –10 дБ составляет 50 МГц (относительная полоса пропускания около 2 %), что полностью перекрывает центральную,

DOI: 10.21681/3034-4050-2026-4-65-74

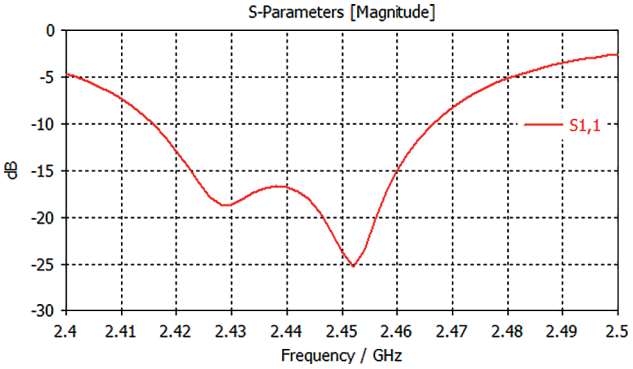


Рис. 4. График параметра S11

наиболее загруженную часть целевого ISM-диапазона. Относительно узкополосный характер согласования является классическим следствием использования одиночного микрополоскового резонатора на относительно тонкой подложке. Тем не менее, достигнутое качество согласования (минимум кривой опускается ниже –15 дБ) минимизирует потери на отражение и исключает риск самовозбуждения малошумящих усилителей приемного тракта.

Критически важным параметром для матричных алгоритмов обработки сигналов является уровень развязки между соседними каналами.

Анализ коэффициентов передачи (рис. 5) показал, что благодаря применению предложенного метода ортогональной пространственной ориентации излучателей (поворот на 90°) максимальный уровень взаимной связи во всем рабочем диапазоне не превышает –16 дБ. С физической точки зрения это означает, что менее 2 % электромагнитной энергии, излучаемой или переотражаемой одним элементом, наводится на соседний порт. Для печатных решеток на FR-4 с шагом элементов $\lambda/2$ значение –16 дБ является отличным показателем. Для сравнения, классическое коллинеарное расположение патчей на аналогичной подложке обычно дает развязку не лучше –11...–13 дБ из-за сильной связи по поверхностной волне TM_0.

Для оценки эффективности пространственного излучения был проведен анализ характеристик направленности системы в дальней зоне (Farfield). Результаты расчета трехмерной диаграммы направленности (ДН) антенной решетки при синфазном возбуждении всех четырех портов показаны в виде 3D-диаграммы (рис. 6).

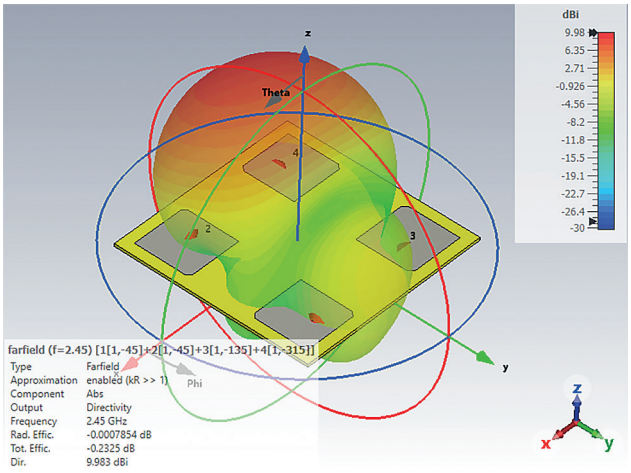
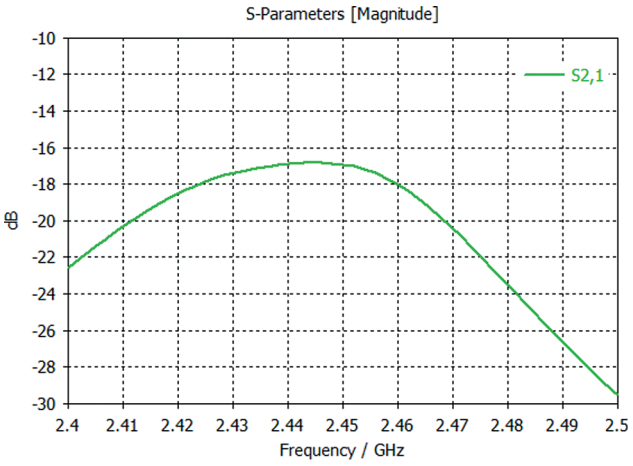
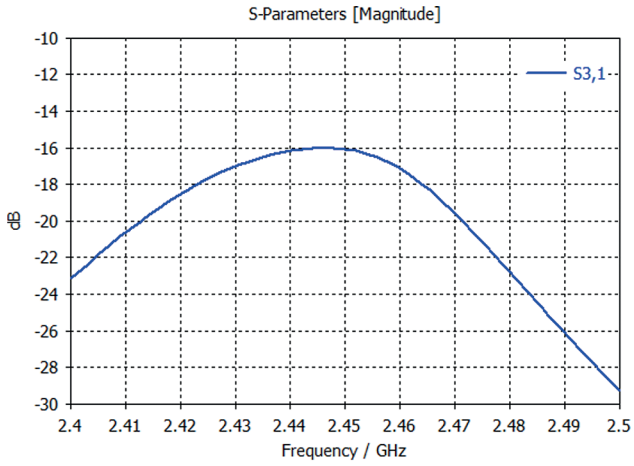


Рис. 6. Пространственная (3D) диаграмма направленности антенной решетки 2x2 на частоте 2,45 ГГц с формированным нулем в направлении 30°

Как следует из результатов моделирования, излучающая система формирует стабильный, ярко выраженный главный лепесток с максимумом излучения строго по нормали к плоскости решетки (вдоль оси Z, $\theta = 0°$). Коэффициент направленного действия (Directivity) всей решетки



а)



б)

Рис. 5. Графики коэффициентов передачи: а) S21; б) S31

2x2 составляет 9,98 дБи. Данный результат полностью согласуется с классической теорией антенных решеток [15]. Учитывая, что расчетный коэффициент усиления одиночного микрополоскового элемента на текстолите FR-4 составляет порядка 5–6 дБи, когерентное сложение полей от четырех элементов обеспечивает теоретический прирост множителя антенной решетки (Array Factor) примерно на 6 дБ ($10\log_{10}(4)$). Итоговое значение ~10 дБи подтверждает высокую эффективность согласования и отсутствие синфазных потерь в апертуре. Кроме того, на 3D-диаграмме наблюдается полное отсутствие паразитных дифракционных лепестков, что подтверждает правильность выбора шага между излучателями ($d \leq \lambda/2$).

Для более детального анализа угловых характеристик был исследован двумерный полярный срез диаграммы направленности в ортогональной плоскости ($\phi = 90°$) (рис. 7).

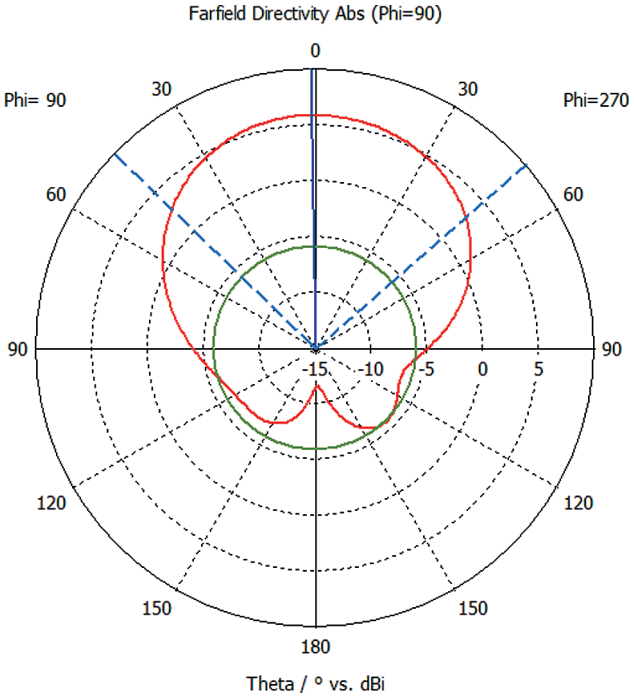


Рис. 7. Полярный срез диаграммы направленности антенной решетки в плоскости $\phi = 90°$ (маркерами отмечена ширина луча по уровню –3 дБ)

Анализ полярного графика позволяет сделать несколько важных выводов, критичных для радиоканалов управления беспилотными комплексами. Во-первых, ширина главного лепестка по уровню половинной мощности (Half-Power Beamwidth, HPBW), ограниченная пунктирными маркерами на графике, составляет более 60°. Столь широкий луч является оптимальным для БПЛА, так как он гарантирует удержание устойчивого радиоканала с наземной станцией управления даже при активном маневрировании аппарата с большими углами крена и тангажа. Во-вторых, уровень излучения в заднюю полусферу (Front-to-Back ratio) надежно подавлен экранирующим слоем печатной платы (более чем на 15 дБ относительно главного максимума). Это минимизирует влияние корпуса БПЛА и внутренней электроники на характеристики антенны, а также снижает уязвимость системы к помехам, приходящим с нерабочих направлений.

Особый научный интерес представляет анализ круговой поляризации. Оценка качества КП производится с помощью осевого коэффициента (Axial Ratio, AR), определяемого как отношение большой оси эллипса поляризации к его малой оси: $AR = 10\log_{10}(E_{major}/E_{minor})$. В идеальной круговой поляризации AR составляет 0 дБ, приемлемым на практике считается значение $AR \leq 3$ дБ (рис. 8).

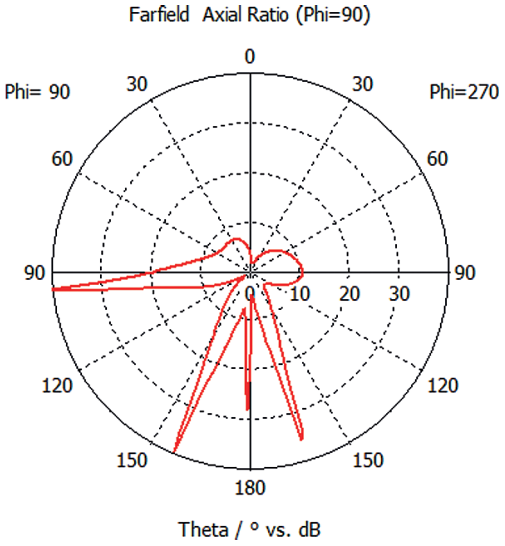


Рис. 8. График осевого коэффициента на частоте 2,43 ГГц

Результаты электродинамического моделирования показали, что на наилучшей частоте из целевого набора (2,43 ГГц) минимальное значение осевого коэффициента составило 4 дБ. Данный результат свидетельствует о том, что сформированная поляризация является выраженно эллиптической, а не круговой.

Данный факт рассматривается не как ошибка проектирования, а как физический компромисс, обусловленный рядом технологических ограничений:

1. Использование одной точки запитки (зондового питания) ограничивает формирование строгой 90-градусной разности фаз между

ортогональными модами (TM_{10} и TM_{01}) лишь одной бесконечно узкой частотной точкой. Малейший сдвиг по частоте приводит к резкому росту AR.

2. Применение бюджетного диэлектрика FR-4 с высоким тангенсом угла потерь вызывает «уплощение» резонансных кривых мод, что смещает точку их амплитудного равенства относительно точки фазовой квадратуры.
3. Технологические допуски станков с ЧПУ при фрезеровании печатных плат вносят асимметрию в размеры усеченных углов (ΔL), что дополнительно деградирует поляризацию.

Именно электродинамические особенности реальной антенны, такие как остаточная взаимная связь (–16 дБ) и эллиптическая поляризация (AR = 4 дБ), полностью обосновывают и оправдывают применение сложного робастного алгоритма RAIS-LCMV в вычислительном ядре ПЛИС.

Классические алгоритмы формирования нулей (например, алгоритм Кейпона) основываются на предположении идеальной формы диаграммы направленности и строгой поляризации. При AR = 4 дБ амплитуда принимаемого полезного сигнала будет флуктуировать при вращении БПЛА, что приведет к ошибкам в матрице управления и, как следствие, к подавлению полезного сигнала.

Алгоритм RAIS-LCMV, за счет диагонального нагружения ковариационной матрицы $\mathbf{R}_{xx}$ и расширения секторных ограничений, обеспечивает нечувствительность (робастность) адаптивной решетки к подобным аппаратным и поляризационным искажениям. Вычислительная мощность ПЛИС Xilinx Kria XCK26 позволяет в реальном масштабе времени адаптировать весовые коэффициенты, формируя глубокие пространственные «нули» в направлениях активных помех, компенсируя физическое несовершенство малогабаритной антенной подсистемы.

Заключение

В рамках проведенного исследования решена комплексная задача проектирования аппаратной и электродинамической базы для малогабаритной четырехканальной цифровой адаптивной антенной решетки диапазона 2,4–2,5 ГГц.

Обоснована высокопроизводительная цифровая архитектура, базирующаяся на применении когерентного 4-канального радиочастотного трансивера и гетерогенной системы на кристалле Xilinx Zynq UltraScale+ (семейства Kria). Разделение вычислительных задач между программируемой логикой и процессорной системой обеспечивает эффективную аппаратную реализацию сложных матричных алгоритмов фильтрации в жестком реальном времени.

Разработана и промоделирована в САПР CST Microwave Studio микрополосковая излучающая система с независимым коаксиальным (зондовым) питанием. Доказано, что применение квадратных патчей с усеченными углами обеспечивает генерацию эллиптической поляризации без применения громоздких схем распределения мощности.

Продемонстрирована высокая эффективность метода ортогональной пространственной ориентации элементов, позволившего минимизировать уровень взаимной связи между соседними каналами до –16 дБ при размещении на общей диэлектрической подложке FR-4.

Теоретически обосновано, что достигнутый уровень осевого коэффициента (AR = 4 дБ) является закономерным следствием одноточечной запитки и характеристик текстолита. Доказано, что данные физические ограничения успешно нивелируются на программном уровне за счет математического аппарата робастного алгоритма RAIS-LCMV.

Предложенная концепция глубокой интеграции (ко-дизайна) алгоритмической и электродинамической частей открывает перспективы создания бюджетных, компактных и высоконадежных систем связи для малых беспилотных комплексов. В качестве направления для дальнейших исследований целесообразно рассмотреть применение высокочастотных ламинатов (например, серии Rogers) и внедрение двухточечной схемы запитки через гибридный мост Ланге для расширения полосы рабочих частот по критерию идеальной круговой поляризации (AR < 3 дБ).

Литература

1. Тузов Г. И. Помехозащищённость радиосистем со сложными сигналами / М.: Радио и связь, 1986. – 264 с.
2. Монзинго Р. А., Миллер Т. У. Адаптивные антенные решетки: Введение в теорию: Пер. с англ. – М.: Радио и связь, 1986. – 448 с.
3. Марчук Л. А. Пространственно-временная обработка сигналов в линиях радиосвязи / Л.: ВАС, 1991. – 135 с.
4. Риглер, Комптон Р. Т. Адаптивная антенная решетка для подавления помех. // ТИИЭР. – 1973. – том 61. – № 6. – С. 75–86.
5. Чистяков В. А. Алгоритм адаптивной фильтрации помех в цифровых антенных решетках спутниковой связи // Труды МАИ, В.105, 2019. – С. 100–113.

6. Аббас С., Хаддур Р., Кузьменко И. Ю. Метод слепого формирования луча для GPS-приемников // Телекоммуникационные и вычислительные системы. Сборник трудов Тридцать первого международного научно-технического форума. Москва, 2023. – С. 33 39.
7. Глушанков Е. И., Царик И. В., Царик В. И. Пространственно-распределенная технология адаптивного формирования диаграммы направленности антенной решетки // Научные известия, 2022. – № 29. – С. 165–170.
8. Malviya, Leeladhar & Rao, Leevanshi & Pant, Mohit & Parmar, Ajay & Charhate, Sandhya. (2020). 5G beamforming techniques for the coverage of intended directions in modern wireless communication: In-depth review. International Journal of Microwave and Wireless Technologies. – 13. – С. 1039-1062.
9. Feng, Rui & Wang, Cheng-Xiang & Huang, Jie & Gao, Xiqi. (2025). Recent Advances of 6G Ultra-Massive MIMO Technologies in Spatial and Beam Domains.
10. Фокин Г. А., Шеремет Н. В. Использование алгоритмов адаптивного диаграммообразования в сетях 5G // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО, 2024). Санкт-Петербург, 2024. – С. 460–464.
11. Чернов В. С. Повышение помехоустойчивости и пропускной способности с помощью направления луча // Информационные технологии. Радиоэлектроника. Телекоммуникации (ITRT – 2024). Тольятти, 2025. – С. 405–410.
12. Джиган В. И., Курганов В. В. Калибровка цифровых антенных решеток с помощью алгоритмов адаптивной обработки сигналов // Телекоммуникации, 2021. – № 2. – С. 8–16.
13. Leqiang Su, Hongwei Liu, Xu Xu, Zhongfu Ye, Mingquan Jia, Yun Hou. Robust adaptive beamforming algorithm for multipath coherent reception based on iterative adaptive approach and covariance matrix reconstruction, Digital Signal Processing, 2026. – V. 168 – Part B.
14. Бойко И. А., Глушанков Е. И., Лялина А. Ж. Алгоритмы адаптивной обработки сигналов в геостационарных системах // Труды учебных заведений связи. – 2025. – Т. 11. – № 5. – С. 74–83.
15. Звонарев В. В., Питрин А. В., Попов А. С. Методика расчета коэффициента направленного действия адаптивной антенной решетки при наличии помех // Изв. вузов. Приборостроение, 2025. – Т. 68. – № 3. – С. 198–206.

DEVELOPMENT OF AN ADAPTIVE ANTENNA ARRAY FOR UAVs

Babenko V. Yu.[3], Fedorov P. N.[4]

Keywords: *FPGA, Zynq UltraScale+, beamforming, circular polarization, microstrip antenna, mutual coupling, probe feed.*

Abstract

Purpose of the work: *the study aims to develop and investigate a comprehensive architecture for a 4-channel compact adaptive antenna array operating in the 2.4–2.5 GHz frequency range. The system includes a computational core based on the Xilinx Kria FPGA, a multi-channel transceiver path, and a radiating system with circular polarization.*

Research methods: *the research is based on a combined approach involving digital signal processing (DSP) for spatial filtering (using the RAIS-LCMV algorithm), computational electromagnetics (CST Microwave Studio) for high-frequency structure design, and microstrip antenna theory to achieve the required polarization characteristics.*

Results of the study: *a hardware architecture of a digital adaptive antenna array based on the XCK26-SFVC784-2LV-C chip and a 4-channel transceiver providing strict phase coherence is proposed and justified. A radiating system on an FR-4 dielectric substrate in a 2x2 matrix configuration has been developed. To form circular polarization, a diagonal corner truncation method of an isolated square resonator with a single-point probe feed was applied. A method of spatial orthogonal orientation of the elements (sequential 90-degree rotation) was successfully implemented, which allowed a radical reduction of mutual coupling to a level of –16 dB without increasing physical dimensions. Electrodynamic modeling confirmed the formation of a stable main lobe with a directivity of 10 dBi and a beamwidth of more than 60°. It was revealed that the physical limitations of a single-point feed form a minimum axial ratio (AR) of 4 dB, which is successfully compensated by spatial filtering algorithms.*

The scientific novelty: *the study justifies the comprehensive application of the robust spatial filtering algorithm RAIS-LCMV to compensate for hardware and electromagnetic distortions (polarization deviations, cross-polarization interference, and FR-4 manufacturing tolerances) occurring in compact printed antenna arrays with probe feeding. This approach enables the formation of deep nulls in the radiation pattern despite the non-ideal characteristics of the individual emitters.*

References

1. Tuzov G. I. Pomehozashchishchyonnost' radiosistem so slozhnymi signalami / M.: Radio i svyaz', 1986. – P. 264.
2. Monzingo R. A., Miller T. U. Adaptivnye antennye reshetki: Vvedenie v teoriyu: Per. s angl. – M.: Radio i svyaz', 1986. – P. 448.

3 ***Vyacheslav Yu. Babenko***, Operator of the Scientific Company of the Military Academy of Communications named after Marshal of the Soviet Union S. M. Budyonny, St. Petersburg, Russia. E-mail: babenko.vya@mail.ru

4 ***Pavel N. Fedorov***, Senior Researcher, Scientific Research Center of the Military Academy of Communications named after Marshal of the Soviet Union S. M. Budyonny, St. Petersburg, Russia. E-mail: fedorovpn@yandex.ru

3. Marchuk L. A. Prostranstvenno-vremennaya obrabotka signalov v liniyah radiosvyazi. / L.: VAS, 1991. – P. 135.
4. Rigler, Kompton R. T. Adaptivnaya antennaya reshetka dlya podavleniya pomeh // TIIEHR. – 1973. – V. 61. – No 6. – Pp. 75–86.
5. Chistyakov V. A. Algoritm adaptivnoj fil'tracii pomeh v cifrovyh antennyh reshetkah sputnikovoj svyazi // Trudy MAI, 2019. – V.105. – Pp. 100–113.
6. Abbas S., Haddur R., Kuz'menko I. Yu. Metod slepogo formirovaniya lucha dlya GPS-priemnikov // Telekommunikacionnye i vychislitel'nye sistemy. Sbornik trudov Tridcat' pervogo mezhdunarodnogo nauchno-tehnicheskogo foruma. Moskva, 2023. Pp. 33–39.
7. Glushankov E. I., Carik I. V., Carik V. I. Prostranstvenno-raspredelennaya tehnologiya adaptivnogo formirovaniya diagrammy napravlennosti antennoj reshetki // Nauchnye izvestiya, 2022. – No 29. – Pp. 165–170.
8. Malviya, Leeladhar & Rao, Leevanshi & Pant, Mohit & Parmar, Ajay & Charhate, Sandhya. (2020). 5G beamforming techniques for the coverage of intended directions in modern wireless communication: In-depth review. International Journal of Microwave and Wireless Technologies. – 13. – Pp. 1039–1062.
9. Feng, Rui & Wang, Cheng-Xiang & Huang, Jie & Gao, Xiqi. (2025). Recent Advances of 6G Ultra-Massive MIMO Technologies in Spatial and Beam Domains.
10. Fokin G. A., Sheremet N. V. Ispol'zovanie algoritmov adaptivnogo diagrammoobrazovaniya v setyah 5G // Aktual'nye problemy infotelekommunikacij v nauke i obrazovanii (APINO, 2024). Sankt Peterburg, 2024. – Pp. 460–464.
11. Chernov V. S. Povyshenie pomehoustojchivosti i propusknoj sposobnosti s pomoshch'yu napravleniya lucha // Informacionnye tehnologii. Radioehlektronika. Telekommunikacii (ITRT – 2024). Tol'yatti, 2025. – Pp. 405–410.
12. Dzhigan V. I., Kurganov V. V. Kalibrovka cifrovyh antennyh reshetok s pomoshch'yu algoritmov adaptivnoj obrabotki signalov // Telekommunikacii. – 2021. – No 2. – Pp. 8–16.
13. Leqiang Su, Hongwei Liu, Xu Xu, Zhongfu Ye, Mingquan Jia, Yun Hou. Robust adaptive beamforming algorithm for multipath coherent reception based on iterative adaptive approach and covariance matrix reconstruction, Digital Signal Processing, 2026. – V. 168. – Part B.
14. Bojko I. A., Glushankov E. I., Lyalina A. Zh. Algoritmy adaptivnoj obrabotki signalov v geostacionarnyh sistemah // Trudy uchebnyh zavedenij svyazi. – 2025. – V. 11. – No 5. – Pp. 74–83.
15. Zvonarev V. V., Pitrin A. V., Popov A. S. Metodika rascheta koehfficienta napravlennogo dejstviya adaptivnoj antennoj reshetki pri nalichii pomeh // Izv. vuzov. Priborostroenie. – 2025. – V. 68. – No 3. – Pp. 198–206.

СТАНДАРТЫ 5G-ADVANCED И ПОДГОТОВКА К 6G: ПРОМЕЖУТОЧНЫЙ ЭТАП ЭВОЛЮЦИИ

Горохов А. В.[1], Николаева П. А.[2]

DOI:10.21681/3034-4050-2026-4-75-83

Ключевые слова: *Release 18, Release 19, IMT-2030, радиодоступ, сетевое расслоение, интеллектуальное управление, энергоэффективность, интегрированное зондирование, негеостационарная инфраструктура.*

Аннотация

Целью работы *является разработка научно обоснованной модели оценки стандартов 5G-Advanced как промежуточного этапа эволюции мобильных сетей от пятого поколения к шестому поколению связи. Особое внимание уделено определению тех функциональных направлений, которые одновременно решают прикладные задачи развития 5G и формируют технологический задел для будущих систем 6G.*

Метод исследования: *применение системно-технического анализа публикаций по эволюции 5G-Advanced, развитию 3GPP Release 18, Release 19 и ранних направлений Release 20, а также по перспективным технологиям 6G. Использован сравнительный метод, позволяющий сопоставить функциональные блоки 5G-Advanced по критериям радиоинтерфейса, сетевой архитектуры, интеллектуализации, поддержки вертикальных сервисов, энергоэффективности и готовности к интеграции с будущими сценариями IMT-2030. Для исключения описательного характера исследования предложена формализованная качественная модель переходного слоя, в которой каждая группа стандартных функций рассматривается по трем признакам: текущий эксплуатационный эффект, вклад в развитие сетевой архитектуры и потенциал переноса в 6G.*

Результаты исследования: *результаты показывают, что 5G-Advanced не следует рассматривать только как очередное улучшение существующей сети 5G. Более корректно определять его как переходный технологический слой, в котором одновременно выполняются три взаимосвязанные функции: повышение зрелости уже развернутых сетей, расширение набора промышленных и массовых сценариев применения, а также проверка решений, потенциально необходимых для 6G. Установлено, что наибольшую переходную значимость имеют направления, связанные с внедрением искусственного интеллекта в радиодоступ и управление сетью, развитием massive MIMO и многоточечной передачи, повышением точности позиционирования, поддержкой негеостационарных и воздушных сегментов, энергоэффективностью, расширенной работой с устройствами пониженной сложности, интегрированным зондированием и коммуникациями, а также устойчивым сетевым расслоением. Предложенная модель позволяет отделить функции, обеспечивающие краткосрочный коммерческий эффект, от функций, создающих архитектурную основу для 6G.*

Научная новизна *заключается в представлении 5G-Advanced как формализованного промежуточного слоя эволюции, а не как простой совокупности улучшений 5G. Предложена структурная модель оценки стандартных направлений 5G-Advanced по их вкладу в текущую эксплуатационную эффективность, архитектурную преемственность и подготовку к IMT-2030.*

Введение

Развитие мобильных сетей после завершения базовой фазы 5G сопровождается изменением самой логики стандартизации. Если первые релизы 5G были направлены преимущественно на создание единой платформы для широкополосного доступа, низкой задержки, массовых машинных подключений и начальной поддержки вертикальных отраслей, то 5G-Advanced ориентирован на более сложную задачу: повысить практическую отдачу от уже созданной инфраструктуры и одновременно подготовить технологические элементы, которые будут востребованы в будущих сетях 6G. Поэтому 5G-Advanced нельзя ограниченно трактовать как «улучшенный 5G». В инженерном смысле это промежуточный этап стандартизации, на котором проверяются архитектурные, радиотехнические и алгоритмические решения для следующего поколения сетей связи.

Актуальность темы определяется несколькими обстоятельствами. Во первых, коммерческое внедрение 5G во многих странах показало, что заявленные преимущества пятого поколения не реализуются автоматически после установки нового радиодоступа. Для достижения устойчивого эффекта необходимы зрелая автономная архитектура 5G Core, развитые механизмы управления качеством обслуживания, поддержка сетевого расслоения, эффективное использование спектра, снижение энергопотребления и адаптация сети к неоднородным классам устройств. Во-вторых, запрос на новые сервисы становится более сложным: расширенная

1 ***Горохов Александр Владимирович***, научный сотрудник, Военная академия связи. Санкт-Петербург, Россия. E-mail: sanya.gorokhov.97@mail.ru

2 ***Николаева Полина Арсеновна***, младший научный сотрудник, Военная академия связи. Санкт-Петербург, Россия. E-mail: panicolaeva@mail.ru

реальность, промышленный интернет вещей, беспилотные платформы, интеллектуальный транспорт, спутниково наземная связность, высокоточное позиционирование и распределенные вычисления требуют не только увеличения скорости передачи, но и повышения предсказуемости, надежности и управляемости сети. В-третьих, к 6G предъявляются ожидания, которые невозможно удовлетворить одномоментным переходом от 5G к новой радиосистеме. Для этого необходим длительный переходный этап, где часть решений проходит апробацию в рамках 5G-Advanced.

В научно-технической литературе 5G-Advanced часто рассматривается как начало второй фазы 5G и как мост к 6G [1, 2]. При этом основная проблема состоит в том, что отдельные направления стандартизации анализируются разрозненно: отдельно рассматриваются искусственный интеллект в радиодоступе, отдельно massive MIMO, отдельно негеостационарные сети, отдельно интегрированное зондирование и отдельно энергосбережение. Такой подход полезен для изучения отдельных технологий, но недостаточен для ответа на вопрос, какие именно функции 5G-Advanced имеют переходное значение для 6G и по каким признакам это значение может быть оценено.

Постановка задачи. Сформировать целостную модель оценки 5G-Advanced как промежуточного этапа эволюции. Для этого необходимо определить основные технологические направления 5G-Advanced, установить их связь с будущими требованиями 6G, выделить признаки переходности и показать, какие элементы стандартизации имеют преимущественно краткосрочный эксплуатационный эффект, а какие формируют архитектурную и методическую базу для сетей IMT 2030.

Обзор связанных работ

Первые публикации, посвященные 5G-Advanced, фиксируют его связь с 3GPP Release 18 и подчеркивают, что данный релиз является не точечной модернизацией, а началом новой фазы развития 5G [1]. В этих работах отмечается расширение функциональных возможностей радиодоступа, развитие вертикальных сценариев, внедрение методов искусственного интеллекта и машинного обучения, а также повышение гибкости сетевого управления. Значимость Release 18 состоит в том, что он переводит многие исследовательские направления в область стандартизируемых функций, пригодных для промышленного внедрения.

Комплексный анализ эволюции 5G-Advanced в направлении 6G представлен в работах, где рассматриваются прошлые, текущие и перспективные этапы развития мобильных сетей [2]. В них подчеркивается, что 5G-Advanced строится на базе Release 15, Release 16 и Release 17, но вводит более широкий набор функций, связанных с MIMO, позиционированием, расширенной реальностью, sidelink, негеостационарными сетями, беспилотными системами, искусственным интеллектом и энергоэффективностью. Такая постановка позволяет рассматривать 5G-Advanced не только как развитие радиоинтерфейса, но и как переход к более интеллектуальной и сервисно-ориентированной сети.

Отдельное направление исследований связано с искусственным интеллектом и машинным обучением в 5G-Advanced [3]. В отличие от ранних подходов, где AI/ML рассматривались как внешние инструменты оптимизации сети, в 5G-Advanced они начинают входить в контур стандартизации. Это имеет принципиальное значение для 6G, поскольку сети шестого поколения обычно описываются как интеллектуальные, адаптивные и самонастраивающиеся. Следовательно, 5G-Advanced выполняет роль практической среды для проверки того, какие AI/ML-функции могут быть стандартизированы без потери воспроизводимости, совместимости и управляемости.

Существенное место в развитии 5G-Advanced занимает massive MIMO и дальнейшая эволюция многоточечной передачи [4]. Для 5G эти технологии являются средством увеличения спектральной эффективности и улучшения покрытия, но в переходе к 6G они приобретают дополнительное значение. Будущие сети предполагают более плотное использование распределенных антенных систем, гибридных схем формирования луча, адаптивного управления пространственными ресурсами и тесной интеграции радиодоступа с вычислительными механизмами. Поэтому развитие MIMO в Release 18 и последующих релизах может рассматриваться как важнейший элемент радиотехнической преемственности.

Параллельно эволюционирует концепция 6G как всеобъемлющей интеллектуальной сети, в которой связь трансформируется из услуги передачи данных в базовую инфраструктуру для цифровых, физических и киберфизических объектов [5]. Данный подход подразумевает, что промежуточные стандарты должны обеспечивать не только высокую пропускную способность, но и взаимодействие с сенсорными системами, распределенными вычислениями, автономными устройствами и пространственно распределенными сервисами. В этом контексте 5G-Advanced представляет собой этап накопления эксплуатационного опыта, необходимого для последующего перехода к IMT 2030.

Исследования, касающиеся видения ITU для 6G, указывают на необходимость поддержки будущими системами расширенных сценариев, включая интегрированное зондирование и связь (ISAC), сверхнадежные сервисы с низкой задержкой, повсеместную связность, интеллектуальные приложения и устойчивую энергетическую модель [6]. Эти направления коррелируют с функциями, разрабатываемыми в рамках 5G-Advanced. Важность 5G-Advanced заключается в возможности верификации реализуемости отдельных требований IMT-2030 до полного перехода к новой системе радиодоступа.

Интегрированное зондирование и коммуникации играют ключевую роль [7]. В 5G эта область еще не является широко распространенной эксплуатационной функцией, однако для 6G она рассматривается как один из определяющих сценариев. Если сеть должна не только передавать данные, но и воспринимать окружающую среду, то требования к радиосигналам, канальным моделям, синхронизации, обработке отражений, безопасности и конфиденциальности существенно усложняются. Таким образом, исследование ISAC в контексте 5G-Advanced имеет значение как подготовка к принципиально новому классу сетевых возможностей.

Перспективные интеллектуальные радиосреды, включая реконфигурируемые интеллектуальные поверхности (RIS), также рассматриваются как одно из направлений развития 6G [8]. Однако их массовое внедрение требует совместимости с существующей радиоинфраструктурой, адекватных моделей управления и апробированных сценариев применения. 5G-Advanced в данном случае выступает не столько как конечная среда для внедрения RIS, сколько как этап подготовки сетевой архитектуры к более гибкому управлению распространением радиосигнала.

В работах по 6G IoT отмечается, что будущие сети должны поддерживать не только массовое количество устройств, но и интеллектуальную обработку данных, взаимодействие с беспилотными системами, промышленными объектами, спутниковыми сегментами и критически важными сервисами [9]. Для 5G-Advanced это означает необходимость развития RedCap, энергоэффективных профилей устройств, механизмов низкого энергопотребления, расширенного позиционирования и устойчивой поддержки вертикальных сценариев. Связь между 5G-Advanced и 6G проявляется именно в том, что устройства и сервисы будущего не возникают в момент утверждения нового поколения, а постепенно формируются в переходной архитектуре.

Наконец, вопросы безопасности и конфиденциальности для 6G требуют особого внимания [10]. Чем выше степень интеллектуализации сети, тем больше зависимость от данных, моделей машинного обучения, распределенных вычислений и программно определяемых функций. Это создает новые угрозы: атаки на обучающие выборки, подмена контекста, манипуляция сетевыми политиками, нарушение изоляции сетевых срезов, компрометация пользовательской телеметрии и уязвимости в цепочке управления радиоресурсами. Поэтому 5G-Advanced должен рассматриваться как этап, на котором необходимо заранее проверять не только функциональные возможности, но и защитные механизмы будущей сети.

Методика и формализованное решение задачи

Для оценки стандартов 5G-Advanced как промежуточного этапа эволюции от 5G к 6G в работе предлагается воспроизводимый текстовый метод качественной оценки. Метод не использует численные расчеты и формулы, однако задает последовательные правила анализа, позволяющие одинаково применять его к различным направлениям Release 18, Release 19 и ранних направлений Release 20.

Объектом оценки выступают ключевые технологические направления 5G-Advanced, отражающие развитие радиодоступа, сетевой архитектуры, интеллектуального управления, энергоэффективности, поддержки вертикальных сервисов и подготовки к IMT-2030. Каждое направление оценивается по трем критериям: эксплуатационная зрелость, архитектурная преемственность и инновационная переходность.

Критерий «эксплуатационная зрелость» отражает степень готовности направления к практическому использованию в существующих или ближайших сетях 5G-Advanced. Низкая оценка присваивается в том случае, если направление находится преимущественно на уровне исследований, требует значительной перестройки инфраструктуры и не имеет устойчивых сценариев внедрения. Средняя оценка присваивается, если направление уже включено в повестку стандартизации, имеет ограниченные сценарии применения, но требует дальнейшей апробации в сетях операторского класса. Высокая оценка присваивается, если направление опирается на уже применяемые механизмы 5G, может быть внедрено эволюционно и дает понятный эксплуатационный эффект: повышение покрытия, устойчивости соединения, энергоэффективности, качества обслуживания или управляемости сети.

Критерий «архитектурная преемственность» характеризует способность направления сохранять совместимость с существующей 5G-архитектурой и одновременно быть перенесенным в будущую 6G-среду. Низкая оценка присваивается, если реализация направления требует принципиально новой сетевой архитектуры и слабо связана с текущими механизмами 5G. Средняя оценка присваивается, если направление может быть частично реализовано в рамках 5G-Advanced, но для полноценного раскрытия потенциала требует новых интерфейсов, моделей управления или более глубокой интеграции с вычислительной инфраструктурой. Высокая оценка присваивается, если направление естественно продолжает функции 5G, может развиваться в рамках Release 18–20 и формирует основу для последующего переноса в 6G без полного разрыва архитектурной логики.

Критерий «инновационная переходность» показывает, насколько направление способствует подготовке к качественно новым возможностям 6G. Низкая оценка означает, что направление преимущественно улучшает уже известные функции 5G и не меняет принципов построения сети. Средняя оценка означает, что направление расширяет функциональность 5G-Advanced и может быть использовано в отдельных сценариях 6G, но не является системообразующим. Высокая оценка означает, что направление формирует принципиально важный задел для 6G: интеллектуальное управление, интеграцию связи и зондирования, пространственно распределенную инфраструктуру, энергоосознанную архитектуру, новые классы устройств или сетевую автоматизацию.

Последовательность применения метода включает четыре этапа. На первом этапе выделяется технологическое направление 5G-Advanced и определяется его связь с Release 18, Release 19 или ранними направлениями Release 20. На втором этапе направление оценивается по критерию эксплуатационной зрелости с учетом возможности внедрения в существующих сетях. На третьем этапе определяется архитектурная преемственность, то есть способность направления быть частью перехода от 5G-Advanced к 6G. На четвертом этапе устанавливается инновационная переходность, то есть вклад направления в формирование будущих возможностей IMT-2030. Итоговая интерпретация строится не как численная сумма, а как качественный профиль направления. Если направление имеет высокую эксплуатационную зрелость, но низкую инновационную переходность, оно рассматривается как инструмент текущего улучшения 5G. Если направление имеет среднюю эксплуатационную зрелость, но высокую архитектурную преемственность и высокую инновационную переходность, оно рассматривается как ключевой элемент подготовки к 6G.

Применение метода к ключевым направлениям 5G-Advanced показывает следующие результаты:

Первое направление: развитие massive MIMO, многоточечной передачи и усовершенствованного управления лучами. Эксплуатационная зрелость данного направления оценивается как высокая, поскольку MIMO является одним из базовых механизмов 5G NR, а его развитие в Release 18 связано с повышением спектральной эффективности, улучшением покрытия и устойчивости соединения. Архитектурная преемственность также оценивается как высокая, так как пространственная обработка сигнала сохранит значение в будущих сетях 6G. Инновационная переходность оценивается как средняя или высокая: само направление не является новым для 6G, но его развитие создает основу для распределенных антенных систем, более точного управления радиоресурсами и интеллектуального формирования радиосреды.

Второе направление: AI/ML в радиодоступе и управлении RAN. Эксплуатационная зрелость оценивается как средняя, поскольку AI/ML уже включается в повестку 5G-Advanced, но требует проверки устойчивости моделей, качества обучающих данных, совместимости оборудования и доверенности принимаемых решений. Архитектурная преемственность оценивается как высокая, так как будущая 6G-архитектура предполагает более глубокую автоматизацию и самонастройку сети. Инновационная переходность оценивается как высокая, поскольку AI/ML переводит сеть от статического управления к адаптивному, контекстно-зависимому и предиктивному управлению ресурсами.

Третье направление: поддержка негеостационарных сетей, воздушных сегментов и спутниково-наземной связности. Эксплуатационная зрелость оценивается как средняя, поскольку соответствующие механизмы уже развиваются в 5G-Advanced, но их массовое внедрение зависит от доступности спутниковых группировок, терминалов, частотного регулирования и устойчивых моделей роуминга. Архитектурная преемственность оценивается как высокая, поскольку 6G предполагает переход к пространственно распределенной инфраструктуре, объединяющей наземные, воздушные и космические сегменты. Инновационная переходность также

оценивается как высокая, так как данное направление изменяет представление о сети как о преимущественно наземной сотовой системе.

Четвертое направление: интегрированное зондирование и коммуникации. Эксплуатационная зрелость оценивается как низкая или средняя, поскольку ISAC еще не является массовой функцией операторских сетей и требует решения задач синхронизации, обработки отраженных сигналов, электромагнитной совместимости и защиты данных. Архитектурная преемственность оценивается как средняя, так как отдельные элементы могут быть апробированы в 5G-Advanced, но полноценное раскрытие ISAC ожидается уже в 6G. Инновационная переходность оценивается как высокая, поскольку ISAC принципиально расширяет назначение сети: она становится не только средством передачи данных, но и инструментом восприятия физической среды.

Пятое направление: сетевое расслоение, поддержка вертикальных сервисов и гарантированного качества обслуживания. Эксплуатационная зрелость оценивается как высокая, поскольку Network slicing уже является важной частью 5G-архитектуры и получает дальнейшее развитие в 5G-Advanced. Архитектурная преемственность оценивается как высокая, так как будущие 6G-сервисы будут еще более неоднородными и потребуют изолированных логических сетей с различными требованиями к задержке, надежности, безопасности и пропускной способности. Инновационная переходность оценивается как средняя или высокая: само сетевое расслоение уже известно, но его развитие в сторону автоматизированного, интеллектуального и междоменного управления будет иметь ключевое значение для 6G.

Шестое направление: энергоэффективность и энергоосознанное управление сетью. Эксплуатационная зрелость оценивается как средняя или высокая, поскольку энергосберегающие механизмы могут внедряться в существующую инфраструктуру, но их эффективность зависит от режима нагрузки, плотности сети, возможностей оборудования и качества алгоритмов управления. Архитектурная преемственность оценивается как высокая, поскольку энергопотребление становится одним из определяющих ограничений будущих сетей. Инновационная переходность также оценивается как высокая, так как 6G потребует перехода от локального энергосбережения отдельных базовых станций к целостной энергоосознанной архитектуре, охватывающей радиодоступ, транспорт, ядро сети, граничные вычисления и пользовательские устройства.

Седьмое направление: устройства пониженной сложности, RedCap, Ambient IoT и массовые киберфизические подключения. Эксплуатационная зрелость оценивается как средняя, поскольку часть функций уже развивается в рамках 5G-Advanced, однако их массовое применение зависит от стоимости устройств, энергопотребления, сценариев промышленного внедрения и устойчивости радиопокрытия. Архитектурная преемственность оценивается как высокая, так как 6G будет ориентирован на массовое подключение объектов, сенсоров, исполнительных устройств и автономных платформ. Инновационная переходность оценивается как высокая, поскольку данное направление формирует основу для будущей сети, обслуживающей не только абонентов, но и распределенную среду киберфизических объектов.

Проведенное применение метода показывает, что направления 5G-Advanced имеют различный профиль переходности. Massive MIMO, сетевое расслоение и повышение энергоэффективности обладают высокой эксплуатационной зрелостью и могут рассматриваться как ближайшие инструменты развития сетей. AI/ML, ISAC, NTN и Ambient IoT обладают более выраженной инновационной переходностью, поскольку именно они формируют качественные признаки будущей 6G-архитектуры. Следовательно, 5G-Advanced выполняет двойную функцию: обеспечивает прикладное улучшение текущих сетей и одновременно служит управляемой средой проверки технологий, которые в дальнейшем могут стать базовыми для IMT-2030.

Решение задачи

На основе предложенной модели 5G-Advanced следует определить переходный технологический слой, выполняющий четыре функции:

Первая функция – стабилизационная. Она заключается в доведении 5G до более зрелого эксплуатационного состояния. Это включает улучшение покрытия, повышение устойчивости при мобильности, снижение энергопотребления, поддержку более широкого набора устройств и повышение качества обслуживания. Без этой функции переход к 6G был бы преждевременным, поскольку значительная часть возможностей 5G не получила бы достаточной практической проверки.

Вторая функция – расширяющая. Она выражается в подключении новых сценариев, которые не были полностью раскрыты в ранних вариатах 5G. К ним относятся расширенная реальность, промышленная автоматизация, беспилотные системы, критические сервисы, спутниково-наземная связность, высокоточное

позиционирование и интеллектуальное управление ресурсами. Эти сценарии важны не только сами по себе, но и как прообраз будущих требований 6G.

Третья функция – экспериментально-архитектурная. 5G-Advanced позволяет вводить в стандартизацию элементы, которые в 6G могут стать базовыми. Это относится к AI/ML в радиодоступе, интегрированному зондированию, развитию негеостационарных сетей, управлению распределенными антенными системами, энергетически осознанной архитектуре и более глубокой автоматизации сетевого управления.

Четвертая функция – фильтрующая. Она обусловлена тем, что не все перспективные технологии, обсуждаемые в контексте 6G, обязательно будут интегрированы в будущий стандарт. 5G-Advanced предоставляет возможность дифференцировать инженерно зрелые решения от концептуальных гипотез. В случае, если технология не демонстрирует обеспечения совместимости, управляемости, воспроизводимости и безопасности в рамках переходной архитектуры, ее интеграция в 6G требует тщательной оценки. Эта функция фильтрации имеет особую значимость для таких направлений, как AI-native networking, RIS, ISAC и интеграция наземных и негеостационарных сегментов.

Практическая ценность данного подхода заключается в возможности оценки стандартов 5G-Advanced не на основе простого перечня новых функций, а с учетом их стратегической роли в эволюции сетевой инфраструктуры. Например, развитие технологий MIMO демонстрирует очевидный эксплуатационный эффект. Однако его переходная значимость определяется не исключительно приростом пропускной способности, но и формированием условий для более гибкой пространственной обработки сигнала. Применение AI/ML в RAN имеет значение не только как средство оптимизации текущих процессов, но и как этап подготовки к автономному управлению сетями следующего поколения. Негеостационарные спутниковые сети ценны не только с точки зрения расширения зоны покрытия, но и как фундамент для создания будущей пространственно распределенной инфраструктуры. Повышение энергоэффективности рассматривается не только как фактор снижения операционных затрат, но и как необходимое условие для масштабирования сетей нового поколения.

Результаты и выводы

Исследование предлагает структурную интерпретацию 5G-Advanced как промежуточный этап между сформировавшимся 5G и перспективным 6G. В отличие от упрощенного представления 5G-Advanced как совокупности улучшений Release 18 и Release 19, предложенная модель дифференцирует эти усовершенствования по их эволюционному предназначению. Выявлено, что отдельные функции направлены на текущую эксплуатацию, другие – на расширение диапазона предоставляемых услуг, третьи – на подготовку к новой архитектуре, а четвертые – на апробацию технологий, не готовых к полномасштабному внедрению в коммерческие сети.

Наиболее разработанными и практически востребованными направлениями являются развитие massive MIMO, повышение мобильности, улучшение эффективности радиодоступа, расширение поддержки абонентских устройств и реализация сетевого сегментирования. Эти аспекты непосредственно связаны с текущими потребностями операторов и могут быть внедрены на существующей инфраструктурной базе. Для 6G их значимость определяется тем, что они формируют преемственный фундамент для создания более плотных, адаптивных и программно управляемых сетей.

Функции искусственного интеллекта и машинного обучения (AI/ML), интегрированное зондирование и коммуникации, негеостационарные сети, энергоэффективное управление и интеллектуальные радиосреды обладают высоким переходным потенциалом. Несмотря на то, что их текущая операционная зрелость может уступать традиционным усовершенствованиям радиодоступа, именно эти направления определяют качественное отличие будущих 6G-систем. Следовательно, оценка 5G-Advanced должна основываться не только на готовности технологии к немедленному внедрению, но и на способности трансформировать архитектурные принципы построения сети.

Выявлено, что 5G-Advanced функционирует как технологический буфер. С одной стороны, он предоставляет операторам и производителям оборудования возможность внедрять новые функции, не дожидаясь полного завершения стандартизации 6G. С другой стороны, он минимизирует риск преждевременного перехода к не апробированным решениям, поскольку перспективные функции вводятся в контролируемой среде. Эта буферная функция имеет критическое значение для отраслей, где надежность, совместимость и долговечность оборудования имеют преимущество над демонстрационными пиковыми характеристиками.

Полученные данные также свидетельствуют о том, что развитие 5G-Advanced требует оценки не только на физическом уровне. Хотя радиоинтерфейс сохраняет свою ключевую роль, переход к 6G определяется интеграцией различных

уровней: радиодоступа, ядра сети, транспортной инфраструктуры, управления услугами, безопасности, энергопотребления, граничных вычислений и данных для интеллектуального управления. Следовательно, академический анализ 5G-Advanced должен носить межуровневый характер.

Предложенная модель позволяет преодолеть распространенное упрощенное представление, согласно которому 5G-Advanced описывается исключительно через увеличение скорости, снижение задержки или расширение полосы пропускания. Хотя эти показатели имеют значение, они не отражают фундаментальную сущность перехода к 6G. Более важным представляется вопрос о трансформации сети в интеллектуальную, контекстно-зависимую, энергоэффективную, распределенную систему, способную обслуживать гетерогенные классы сервисов.

Транзитный характер 5G-Advanced проявляется в его способности сохранять совместимость с существующей 5G-инфраструктурой, одновременно включает в себя элементы будущей архитектуры. Это принципиальное отличие от ранних фаз 5G, основной целью которых было формирование новой радиосистемы и реализация базовых сценариев. В контексте 5G-Advanced сеть начинает эволюционировать как управляемая цифровая платформа. В ее рамках значительно возрастает роль данных, моделей, политик управления, сетевых срезов, автоматизации и межуровневой координации.

Особое внимание следует уделить потенциальным рискам. Интеллектуализация сети способствует повышению эффективности, однако формирует зависимость от качества исходных данных и устойчивости используемых моделей. Негеостационарные сегменты расширяют зону покрытия, но усложняют задачи маршрутизации, синхронизации и обеспечения безопасности. Интегрированное зондирование открывает новые возможности для сервисов, но требует проработки вопросов конфиденциальности и обеспечения электромагнитной совместимости. Реконфигурируемые интеллектуальные поверхности (RIS) и интеллектуальные радиосреды обещают управляемое распространение сигнала, но требуют разработки зрелых моделей управления, измерения и сертификации. Таким образом, 5G-Advanced следует рассматривать не только как катализатор перехода к 6G, но и как механизм выявления сопутствующих ограничений.

В практическом отношении предложенная модель применима при планировании модернизации сетевой инфраструктуры. Операторы связи могут оценивать каждое направление развития не только по текущему коммерческому эффекту, но и по вкладу в формирование будущей архитектуры. Производители оборудования могут использовать эту модель для приоритизации научно-исследовательских и опытно-конструкторских работ. Академические учреждения могут применять ее для выбора исследовательских тем, обладающих не только теоретической новизной, но и потенциалом для стандартизации.

Для российских научно-технических исследований данная тема имеет особое значение. Развитие сетей связи связано не только с импортом готового оборудования, но и с подготовкой инженерных кадров, исследованием радиодоступа, моделированием сетевых сценариев, разработкой средств защиты, созданием испытательных стендов и формированием компетенций в области программно определяемых и интеллектуальных сетей. 5G-Advanced в этом отношении является удобной предметной областью: он достаточно близок к существующей практике, но уже содержит направления, которые будут определять будущую 6G-повестку.

Заключение

В работе выполнен системно-технический анализ стандартов 5G-Advanced как промежуточного этапа эволюции мобильных сетей от 5G к 6G. Показано, что 5G-Advanced не является только набором улучшений пятого поколения, а представляет собой переходный технологический слой, объединяющий эксплуатационное развитие существующей инфраструктуры, расширение вертикальных сервисов и проверку решений, значимых для IMT-2030.

Достигнутый научный эффект заключается в формализации признаков переходности 5G-Advanced. Предложено оценивать стандартные направления по трем критериям: эксплуатационная зрелость, архитектурная преемственность и инновационная переходность. Такой подход позволяет отделять функции краткосрочного улучшения сети от функций, создающих основу для будущей 6G-архитектуры.

Наиболее значимыми направлениями перехода определены AI/ML в радиодоступе и управлении сетью, эволюция massive MIMO, многоточечная передача, расширенное позиционирование, поддержка негеостационарных и воздушных сегментов, энергоэффективность, сетевое расслоение, интегрированное зондирование и коммуникации, а также подготовка к интеллектуальным радиосредам. Эти направления образуют связный технологический контур, в котором 5G-Advanced выполняет роль инженерного моста к 6G.

Практическая достоверность предложенных решений подтверждается сопоставлением модели с актуальными научными публикациями, посвященными Release 18, Release 19, Release 20, AI/ML, MIMO, ISAC, RIS, IoT, безопасности и энергетической эффективности будущих сетей. Практическое значение работы состоит в возможности использовать предложенную модель при планировании исследований, модернизации сетей связи, разработке учебных материалов и обосновании приоритетов перехода от 5G к 6G.

Литература

1. Lin X. An Overview of 5G Advanced Evolution in 3GPP Release 18 // IEEE Communications Standards Magazine, 2022. – Vol. 6, – No 3. – Pp. 58–65. – URL: https://arxiv.org/abs/2201.01358 (дата обращения: 14.06.2026).
2. Chen W., Lin X., Lee J., Toskala A., Sun S., Chiasserini C. F., Liu L. 5G-Advanced Towards 6G: Past, Present and Future // arXiv, 2023. – arXiv:2303.07456. – URL: https://arxiv.org/abs/2303.07456 (дата обращения: 14.06.2026).
3. Lin X. Artificial Intelligence in 3GPP 5G-Advanced: A Survey // arXiv, 2023. – arXiv:2305.05092. – URL: https://arxiv.org/abs/2305.05092 (дата обращения: 14.06.2026).
4. Jin H., Liu K., Lee G., Farag E. J., Zhang M., Zhu D., Zhang L., Onggosanusi E., Shafi M., Tataria H. Massive MIMO Evolution Towards 3GPP Release 18 // arXiv, 2022. – arXiv:2210.08218. – URL: https://arxiv.org/abs/2210.08218 (дата обращения: 14.06.2026).
5. Pennanen H., Hänninen T., Tervo O., Tölli A., Latva-aho M. 6G: The Intelligent Network of Everything // arXiv, 2024. – arXiv:2407.09398. – URL: https://arxiv.org/abs/2407.09398 (дата обращения: 14.06.2026).
6. Liu R., Zhang L., Li R. Y.-N., Di Renzo M. The ITU Vision and Framework for 6G: Scenarios, Capabilities and Enablers // arXiv, 2023. – arXiv:2305.13887. – URL: https://arxiv.org/abs/2305.13887 (дата обращения: 14.06.2026).
7. Kaushik A., Singh R., Dayarathna S., Senanayake R., Di Renzo M., Dajer M., Ji H., Kim Y., Sciancalepore V., Zappone A., Shin W. Towards Integrated Sensing and Communications for 6G: A Standardization Perspective // arXiv, 2023. – arXiv:2308.01227. – URL: https://arxiv.org/abs/2308.01227 (дата обращения: 14.06.2026).
8. Basar E., Alexandropoulos G. C., Liu Y., Wu Q., Jin S., Yuen C., Dobre O. A., Schober R. Reconfigurable Intelligent Surfaces for 6G: Emerging Hardware Architectures, Applications, and Open Challenges // arXiv, 2023. – arXiv:2312.16874. – URL: https://arxiv.org/abs/2312.16874 (дата обращения: 14.06.2026).
9. Nguyen D. C., Ding M., Pathirana P. N., Seneviratne A., Li J., Niyato D., Dobre O. A., Poor H. V. 6G Internet of Things: A Comprehensive Survey // IEEE Internet of Things Journal, 2022. – Vol. 9, – No 1. – P. 359–383. – DOI: 10.1109/JIOT.2021.3103320.
10. Nguyen V.-L., Lin P.-C., Cheng B.-C., Hwang R.-H., Lin Y.-D. Security and Privacy for 6G: A Survey on Prospective Technologies and Challenges // IEEE Communications Surveys & Tutorials, 2022. – Vol. 24, – No 4. – Pp. 2384–2428. – DOI: 10.1109/COMST.2021.3108618.

5G-ADVANCED STANDARDS AND PREPARATION FOR 6G: AN INTERMEDIATE STAGE OF EVOLUTION

Gorokhov A. V.[3], Nikolaeva P. A.[4]

Keywords: *Release 18, Release 19, IMT-2030, radio access, Network slicing, intelligent control, energy efficiency, integrated sensing, non-geostationary infrastructure.*

Abstract

The purpose of the work *is to develop a scientifically grounded model for evaluating 5G Advanced standards as an intermediate stage in the evolution of mobile networks from the fifth generation to the sixth generation of communication. Particular attention is paid to identifying those functional areas that simultaneously address the practical challenges of 5G development and lay the technological groundwork for future 6G systems.*

Research method: *application of a systematic and technical analysis of publications on the evolution of 5G-Advanced, the development of 3GPP Release 18, Release 19, and early aspects of Release 20, as well as on promising 6G technologies. A comparative method was used to compare the functional blocks of 5G Advanced based on criteria such as radio interface, network architecture, intelligence, support for vertical services, energy efficiency, and readiness for integration with future IMT-2030 scenarios. To move beyond a purely descriptive approach, this study proposes a formalized qualitative model of the transition layer, in which each group of standard functions is evaluated based on three criteria: current operational impact, contribution to the development of network architecture, and potential for migration to 6G.*

Research results: *the results show that 5G Advanced should not be viewed merely as another upgrade to the existing 5G network. It is more accurate to define it as a transitional technology layer that simultaneously performs*

3 ***Alexander V. Gorokhov***, Researcher, Military Academy of Communications, St. Petersburg, Russia. E-mail: sanya.gorokhov.97@mail.ru

4 ***Polina A. Nikolaeva***, Junior Researcher, Military Academy of Communications, St. Petersburg, Russia. E-mail: panicolaeva@mail.ru

three interrelated functions: enhancing the maturity of already deployed networks, expanding the range of industrial and mass-market use cases, and testing solutions that may be necessary for 6G. It has been established that the areas of greatest transitional significance are those related to the implementation of artificial intelligence in radio access and network management, the development of massive MIMO and multipoint transmission, improved positioning accuracy, support for non-geostationary and airborne segments, energy efficiency, enhanced support for low-complexity devices, integrated sensing and communications, and sustainable Network slicing. The proposed model makes it possible to distinguish between functions that deliver short-term commercial benefits and those that lay the architectural foundation for 6G.

Scientific novelty: *consists of presenting 5G Advanced as a formalized intermediate stage of evolution, rather than simply a collection of 5G enhancements. A structural model is proposed for evaluating standard 5G-Advanced initiatives based on their contribution to current operational efficiency, architectural continuity, and readiness for IMT-2030.*

References

1. Lin X. An Overview of 5G Advanced Evolution in 3GPP Release 18 // IEEE Communications Standards Magazine, 2022. – Vol. 6. – No 3. – Pp. 58–65. – URL: https://arxiv.org/abs/2201.01358 (дата обращения: 14.06.2026).
2. Chen W., Lin X., Lee J., Toskala A., Sun S., Chiasserini C. F., Liu L. 5G-Advanced Towards 6G: Past, Present and Future // arXiv, 2023. – arXiv:2303.07456. – URL: https://arxiv.org/abs/2303.07456 (дата обращения: 14.06.2026).
3. Lin X. Artificial Intelligence in 3GPP 5G-Advanced: A Survey // arXiv, 2023. – arXiv:2305.05092. – URL: https://arxiv.org/abs/2305.05092 (дата обращения: 14.06.2026).
4. Jin H., Liu K., Lee G., Farag E. J., Zhang M., Zhu D., Zhang L., Onggosanusi E., Shafi M., Tataria H. Massive MIMO Evolution Towards 3GPP Release 18 // arXiv, 2022. – arXiv:2210.08218. – URL: https://arxiv.org/abs/2210.08218 (дата обращения: 14.06.2026).
5. Pennanen H., Hänninen T., Tervo O., Tölli A., Latva-aho M. 6G: The Intelligent Network of Everything // arXiv, 2024. – arXiv:2407.09398. – URL: https://arxiv.org/abs/2407.09398 (дата обращения: 14.06.2026).
6. Liu R., Zhang L., Li R. Y.-N., Di Renzo M. The ITU Vision and Framework for 6G: Scenarios, Capabilities and Enablers // arXiv, 2023. – arXiv:2305.13887. – URL: https://arxiv.org/abs/2305.13887 (дата обращения: 14.06.2026).
7. Kaushik A., Singh R., Dayarathna S., Senanayake R., Di Renzo M., Dajer M., Ji H., Kim Y., Sciancalepore V., Zappone A., Shin W. Towards Integrated Sensing and Communications for 6G: A Standardization Perspective // arXiv, 2023. – arXiv:2308.01227. – URL: https://arxiv.org/abs/2308.01227 (дата обращения: 14.06.2026).
8. Basar E., Alexandropoulos G. C., Liu Y., Wu Q., Jin S., Yuen C., Dobre O. A., Schober R. Reconfigurable Intelligent Surfaces for 6G: Emerging Hardware Architectures, Applications, and Open Challenges // arXiv, 2023. – arXiv:2312.16874. – URL: https://arxiv.org/abs/2312.16874 (дата обращения: 14.06.2026).
9. Nguyen D. C., Ding M., Pathirana P. N., Seneviratne A., Li J., Niyato D., Dobre O. A., Poor H. V. 6G Internet of Things: A Comprehensive Survey // IEEE Internet of Things Journal, 2022. – Vol. 9, No 1. Pp. 359–383. – DOI: 10.1109/JIOT.2021.3103320.
10. Nguyen V.-L., Lin P.-C., Cheng B.-C., Hwang R.-H., Lin Y.-D. Security and Privacy for 6G: A Survey on Prospective Technologies and Challenges // IEEE Communications Surveys & Tutorials, 2022. – Vol. 24, – No 4. – Pp. 2384–2428. – DOI: 10.1109/COMST.2021.3108618.

О РЕАЛИЗАЦИИ НОВЫХ ТРЕБОВАНИЙ ЗАКОНОДАТЕЛЬСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ О ЗАЩИТЕ ИНФОРМАЦИИ В ГОСУДАРСТВЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ

Волостных В. А.[1], Задбоев В. А.[2], Шевченко А. А.[3]

DOI:10.21681/3034-4050-2026-4-84-92

Ключевые слова: *информационные системы, криптография, угрозы безопасности, информационная безопасность, правовые документы.*

Аннотация

Цель работы: *проанализировать действующие изменения требований к безопасности государственных информационных систем и разработать подходы к их внедрению в современных условиях.*

Результаты исследования: *рассмотрены изменения требований российских нормативных документов в области информационной безопасности в государственных информационных системах, не затрагивая информацию по государственной тайне.*

На основе анализа современного применения практического опыта в области защиты информации в организациях, предложены рекомендации по обновлению систем защиты в соответствии с нововведениями. Показаны основные проблемы развития систем безопасности крупных информационных систем и пути их решения, определены существенные изменения в законодательстве о защите информации, разработаны предложения по рекомендации обновления систем защиты в соответствии с нововведениями, для обеспечения безопасности информации, обрабатываемой в информационно-телекоммуникационных системах предприятий, организаций, воинских частей и учреждений.

Практическая полезность: *заключается в том, что в рамках единого исследования проводится системное документальное сравнение ряда нормативных правовых документов и выработаны рациональные подходы к реализации требований в современных условиях, которые могут быть применены при обеспечении безопасности информации в информационных системах предприятий, организаций, воинских частей и учреждений.*

Введение и постановка задачи

В современных условиях информационные системы (ИС) Российской Федерации подвергаются множеству угроз, среди которых компьютерные атаки, направленные на государственные информационные системы (ГИС), занимают одно из ведущих мест. В последние годы в связи с известными событиями наблюдается значительный рост компьютерных атак, направленных на нарушение безопасности информационных ресурсов (ИР) и на нарушение работоспособности ИС. Такие атаки могут полностью остановить работу предприятий, организаций и воинских частей, нарушить или серьёзно затруднить работу их информационных систем и тем самым нанести значительный ущерб государству. В условиях цифровой трансформации и растущей зависимости управленческих решений от безопасности информационных ресурсов и качества функционирования ИС, их защищенность приобретает важнейшее значение. Вопросы защиты информационных ресурсов рассматривались в ряде работ [1–5], но рассмотренные в данных работах материалы, во-первых, несколько устарели и кроме того, рассматриваемые подходы к защите информационных ресурсов касались в основном негосударственных ИС, и из этого следует необходимость данного исследования.

В России вопросам информационной безопасности (ИБ) уделяется серьёзное внимание [6–8]. В 2000 году была принята «Доктрина информационной безопасности Российской Федерации», обновленная в 2016 года. В 2021 г. Указом Президента РФ № 400 была утверждена новая Стратегия национальной безопасности Российской Федерации, которая вышла в свет несколько раньше установленного срока. Обновление подобных «стратегических» документов вызвано, во-первых, появлением новых угроз в сфере информационной безопасности, а во-вторых, изменением технологий обработки информации. В последние пять лет во исполнение Стратегии национальной безопасности вышел ряд новых документов, определяющих требования к защищенности государственных информационных ресурсов. В целях выработки подходов к реализации данных требований

1 ***Волостных Виктор Анатольевич***, кандидат военных наук, доцент, научный сотрудник Военной академии связи, г. Санкт-Петербург, Россия. E-mail: ra1alo@mail.ru

2 ***Задбоев Вадим Александрович***, младший научный сотрудник Военной академии связи, г. Санкт-Петербург, Россия. E-mail: zadboev89@mail.ru

3 ***Шевченко Александр Александрович***, кандидат технических наук, доцент, старший научный сотрудник Военной академии связи, г. Санкт-Петербург, Россия. E-mail: alex_pavel1991@mail.ru

необходимо провести их анализ и определить перечень основных первоочередных мероприятий по обеспечению защиты информационных ресурсов, обрабатываемых в ГИС.

Постановка задачи в данной работе заключается в анализе новых требований законодательства Российской Федерации, их существенных особенностей и в разработке рациональных мероприятий по их реализации в современных условиях.

Под современными условиями функционирования ГИС в работе понимаются:

- высокая интенсивность сложных компьютерных атак [9–10];
- сложность финансирования мероприятий по обеспечению информационной безопасности; отсутствие требуемого количества подготовленного персонала подразделений технической защиты (информационной безопасности);
- отсутствие четкой методологии защиты государственных информационных ресурсов.

В соответствии с законодательством в работе используется следующая терминология:

1. Информационная система – совокупность данных в базах и средств, которые обеспечивают их обработку: программ, технологий и оборудования.
2. ГИС – федеральные и региональные ИС, созданные на основании законов РФ, законов субъектов или решений государственных органов. Данные, которые хранятся в ГИС, а также другие документы и сведения госорганов относятся к государственным информационным ресурсам.

Задача исследования – определить основные первоочередные меры путем анализа действующего законодательства и выявить необходимые для выполнения этих требований и приведения систем защиты ГИС в соответствие с действующими нормами.

Решение поставленной задачи

При решении поставленной задачи был составлен перечень основных нормативных правовых документов по защите информационных ресурсов в ГИС, вступивших в силу в последние пять лет и выделены основные новые требования к защите информации, которые в явном виде законодательством не были установлены. В данный перечень (табл. 1) не входят документы, определяющие порядок защиты государственной тайны и объектов критической информационной инфраструктуры.

Анализ нормативных правовых документов, определяющих требования по защите государственных информационных ресурсов, приведен ниже:

1. Основополагающим документом в сфере защиты информации является **Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»**, который систематически дополняется и уточняется.

В обновленной редакции закона определено, что ГИС создаются для выполнения задач госорганов и обмена данными между ними, а также для других целей, установленных федеральными законами.

Такие системы разрабатываются, обновляются и используются с учётом требований законодательства Российской Федерации.

Правительство Российской Федерации устанавливает правила создания, развития, ввода в работу, эксплуатации и вывода из эксплуатации ГИС, а также порядок хранения данных в их базах. В этих правилах прописаны этапы работ и сроки их выполнения.

Так же в обновленной редакции определено, что передача данных из ГИС в другие системы, которые не обеспечивают должный уровень защиты, запрещена.

В статье 16 Федерального закона, защита информации включает в себя правовые, организационные и технические меры, направленные на:

- защиту данных от несанкционированного доступа, удаления, изменения, блокировки, копирования и других незаконных действий;
- сохранение конфиденциальности информации с ограниченным доступом;
- обеспечение права на доступ к информации.

Требования к защите информации в ГИС и других ИС, устанавливаются федеральной службой безопасности (ФСБ России) и Федеральной службой по техническому и экспортному контролю (ФСТЭК России), в пределах их полномочий. При создании и эксплуатации таких систем используемые методы защиты должны соответствовать этим требованиям.

В соответствии с изложенным, рассмотрим основные требования к защите информационных ресурсов в ГИС, определенные регуляторами.

2. Документом, который существенно изменил требования к защите информации (ЗИ), является **Указ Президента РФ от 1 мая 2022 г. № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации»**.

Таблица 1.

Перечень новых нормативных правовых документов, определяющих требования по защите государственных информационных ресурсов

№ п/п	Наименование документа	Примечание
1	Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»	Редакция 1 апреля 2025 г.
2	Указ Президента РФ от 1 мая 2022 г. № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации»	
3	Постановление от 15 июля 2022 г. № 1272 «Об утверждении типового положения о заместителе руководителя органа (организации), ответственном за обеспечение информационной безопасности в органе (организации), и типового положения о структурном подразделении в органе (организации), обеспечивающем информационную безопасность органа (организации)»	
4	Приказ ФСБ России от 18 марта 2025 г. № 117 «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений, с использованием шифровальных (криптографических) средств»	
5	Приказ ФСТЭК России от 11 апреля 2025 № 117 «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений»	В силе с 1 марта 2026 г.
6	Приказ ФСТЭК России от 29.04.2021 № 77 «Об утверждении Порядка организации п проведении работ по аттестации объектов информатизации на соответствие требованиям о защите ограниченного доступа информации, не составляющей государственную тайну»	В ожидании новой редакции
7	Постановление Правительства РФ от 3 ноября 1994 г. № 1233 «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти, уполномоченном органе управления использованием атомной энергии и уполномоченном органе по космической деятельности»	В редакции от 4 марта 2026 г.
8	Методические рекомендации ФСТЭК России «Состав и содержание мероприятий и мер по защите информации, содержащейся в информационных системах»	Опубликованы 14 апреля 2026 г.

Указ направлен на повышение устойчивости и безопасности работы информационных систем в России. В соответствии с ним на заместителей руководителей организаций возложена ответственность за информационную безопасность, включая выявление и предотвращение компьютерных атак, устранение их последствий и реагирование на инциденты.

Также предписано создавать в организациях отдельные подразделения, которые занимаются вопросами безопасности и выполняют те же задачи. Государственным органам поручено обеспечить выполнение требований данного указа.

Руководителям государственных органов, госкорпораций, стратегических предприятий и других значимых организаций предписано оперативно внедрять организационные и технические меры, которые определяются ФСБ России и ФСТЭК России с учётом актуальных угроз.

Кроме того, установлено, что с 1 января 2025 г. организациям запрещено использовать средства защиты информации иностранного происхождения.

3. Во исполнение Указа, правительством Российской Федерации было принято **Постановление от 15 июля 2022 г. № 1272 «Об утверждении типового положения о заместителе руководителя органа (организации), ответственном за обеспечение информационной безопасности в органе (организации), и типового положения о структурном подразделении в органе (организации), обеспечивающем информационную безопасность органа (организации)»**.

Данный документ определяет, какие полномочия и обязанности есть у заместителя руководителя или другого ответственного лица, которое отвечает за информационную безопасность в государственном органе или организации. В его зону ответственности входит защита систем, а также выявление и устранение последствий компьютерных атак и инцидентов.

К специалисту предъявляются требования в необходимости профильного высшего образования в области информационной безопасности. Если образование получено по другой специальности, требуется дополнительная переподготовка. Также документ описывает его рабочие обязанности, права и ответственность. Он участвует в формировании внутренней политики организации и согласовании её стратегии развития в части безопасности.

Кроме того, утверждено типовое положение о подразделении, которое занимается вопросами информационной безопасности. В нём прописаны его цели, задачи и функции.

Работа подразделения направлена на снижение возможного ущерба от сбоев и атак, защиту конфиденциальных данных, повышение устойчивости организации к внешним и внутренним угрозам, а также обеспечение стабильной и безопасной работы информационных систем и инфраструктуры.

Среди основных задач подразделения:

- планирование и координация мер по защите информации и контроль их выполнения;
- выявление угроз и уязвимостей в системах и программном обеспечении;
- предотвращение утечек данных и несанкционированного доступа;
- поддержание работы организации даже при атаках;
- взаимодействие с профильными государственными центрами;
- обеспечение соблюдения требований законодательства при работе с информацией.

На основе этих задач определены функции подразделения, его права и порядок взаимодействия с другими структурами. Также установлены показатели эффективности работы и ответственность сотрудников за выполнение своих обязанностей.

4. **Приказ ФСБ России от 18 марта 2025 г. № 117 «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений, с использованием шифровальных (криптографических) средств»**.

Анализ содержания рассматриваемых документов показал, что оно незначительно различается, но самое главное, что издание нового документа существенно расширяет круг его действия, что следует из названия. Однако установлено, что данный приказ не касается систем, в которых обрабатываются сведения, составляющие государственную тайну, а также не распространяется на ИС Администрации Президента РФ, Совета Безопасности, Федерального Собрания, Правительства, Конституционного и Верховного судов, а также ФСБ.

Документ устанавливает, что данные в ГИС и других ИС госорганов, предприятий и учреждений должны защищаться с помощью криптографических средств в следующих случаях:

- если по законам Российской Федерации прямо требуется защита информации с использованием криптографии;
- если данные передаются по каналам связи вне охраняемой территории или защищённых помещений;
- если нужно приравнять электронные документы с электронной подписью к бумажным с подписью от руки;
- если информация хранится на носителях, к которым невозможно полностью исключить несанкционированный доступ обычными средствами защиты.

Решение о применении криптографической защиты должно быть обосновано в модели угроз, техническом задании и проектной документации системы.

Модель угроз безопасности информации и (или) техническое задание на создание или развитие ГИС согласуются с ФСБ России в части применения криптографии.

Для защиты информации используются только сертифицированные ФСБ криптографические средства защиты.

Для предотвращения возможных угроз ИБ, направленных на взлом или обход криптозащиты, применяются средства нужного класса, который выбирается в зависимости от значимости данных и масштаба системы (табл. 2).

Порядок определения уровня значимости информации, актуальной угрозы безопасности информации и возможностей источника угроз по осуществлению подготовки и проведению атак, подробно изложены в тексте документа.

5. **Приказ ФСТЭК России от 11.04.2025 № 117 «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений»**.

Таблица 2.

Определение минимально допустимого класса СКЗИ, подлежащих использованию для защиты информации, содержащейся в ИС

Уровень значимости информации	Масштаб ИС		
	ИС (сегмент ИС), предназначенная для решения задач ИС на всей территории Российской Федерации или в пределах двух и более субъектов Российской Федерации	ИС (сегмент ИС), предназначенная для решения задач ИС в пределах одного субъекта Российской Федерации	ИС (сегмент ИС), предназначенная для решения задач ИС в пределах объекта (объектов) одного государственного органа, муниципального образования и (или) организации
Высокий уровень значимости	КВ	КС3	КС2
Средний уровень значимости	КС3	КС3	КС1
Низкий уровень значимости	КС2	КС1	КС1

Документ пришёл на смену приказу ФСТЭК России от 11 февраля 2013 г. № 17, при этом его требования распространяются на более широкий круг информационных систем. В нём описаны меры защиты данных в государственных и связанных с ними системах, предотвращающие вторжения на информационные системы за исключением высших органов власти, а также к системам, связанным с разведкой, контрразведкой и управлением вооружением.

Отмечается, что требования к защите информации стали более строгими. Организация, владеющая системой, должна обеспечивать защиту данных на всех этапах её жизненного цикла от разработки и модернизации до эксплуатации и вывода из работы.

При обеспечении защиты информации, важной целью является снизить риск негативных последствий, связанных как с утечкой или искажением данных, так и с нарушением работы самой системы. Для этого внутри организации должна быть выстроена система работы с безопасностью:

- определены ответственные лица;
- внедрены необходимые программные и технические средства;
- разработаны внутренние правила и выделены ресурсы.

Руководитель организации или назначенное им лицо отвечает за организацию защиты, для этого при необходимости создаётся отдельное подразделение или назначаются специалисты, которые должны обладать нужной квалификацией. При этом часть сотрудников обязана иметь профильное образование или пройти соответствующее обучение.

Работа по защите информации ведётся совместно с другими подразделениями, которые используют и обслуживают систему. Используются инструменты для выявления угроз, мониторинга состояния безопасности, поиска уязвимостей и анализа работы системы.

Внутренние правила и регламенты утверждаются руководством и доводятся до сотрудников и подрядчиков. Управление безопасностью включает планирование мер, их реализацию, оценку текущего состояния и последующее улучшение.

Состояние защиты регулярно оценивается с помощью установленных показателей. Такие проверки проводятся периодически, а их результаты направляются руководству и в уполномоченные органы.

Для защиты информации выполняется комплекс мер: анализ существующих угроз, контроль состояния системы, исправление уязвимостей, проведения систематических обновлений, защита при работе с различными устройствами и каналами доступа, активный мониторинг безопасности, разработка безопасного программного обеспечения, физическая защита и обеспечение устойчивой работы системы при сбоях.

Особое внимание уделяется защите данных ограниченного доступа, для этого фиксируются все активные обращения и контролируется доступ. Также предусмотрены меры по обеспечению непрерывной работы системы и её восстановлению при сбоях, для чего создаются резервные копии и используются отказоустойчивые решения.

Проводится обучение сотрудников, во время которого им объясняют основные правила безопасности, проводят тренировки и проверяют устойчивость к методам социальной инженерии.

Отдельно рассматривается использование технологий искусственного интеллекта, при котором необходимо исключить несанкционированное

влияние на модели и данные, а также применять только проверенные решения.

Выбор мер защиты зависит от уровня значимости системы и предполагаемых возможностей нарушителя. При необходимости могут применяться более строгие меры.

Перед началом работы системы проводится её проверка на соответствие установленным требованиям. В дальнейшем контроль уровня защиты осуществляется регулярно или после инцидентов.

Все меры защиты реализуются с учётом методических рекомендаций ФСТЭК. Защита должна обеспечиваться на всех уровнях от оборудования до прикладных программ и сетевой инфраструктуры.

Используются только сертифицированные средства защиты (табл. 3), соответствующие классу системы. Требования к защите также учитываются на всех этапах жизненного цикла системы от создания до завершения её эксплуатации.

Перечень требуемых мероприятий по выполнению обеспечения защищенности ИС для каждого класса защиты разработан, опубликован 14 апреля 2026 г. и требует изучения и реализации на практике.

6. **Приказ ФСТЭК России от 29.04.2021 № 77 «Об утверждении Порядка организации проведении работ по аттестации объектов информатизации на соответствие требованиям о защите ограниченного доступа информации, не составляющей государственную тайну**».

В данном названии данного документа уже точно обозначены определяемые и разрабатываемые вопросы, Единственное дополнение, что в настоящее время ведется его доработка с учетом новых требований к ГИС.

7. **Постановление Правительства РФ от 3 ноября 1994 г. № 1233 «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти, уполномоченном органе управления использованием атомной энергии и уполномоченном органе по космической деятельности»**.

Данный документ вышел в новой редакции, которая существенно меняет привычных стиль обращения с документами ограниченного распространения. Во-первых, существенно расширен круг организаций, в которых данные документы могут создаваться и обрабатываться, во-вторых, введено понятие электронный документ и порядок обращения с электронными документами, содержащими информацию ограниченного доступа, а также определены порядок и ответственность должностных лиц за обеспечение защиты документов, данной категории. Это потребует от специалистов систем электронного документооборота, доработки информационных систем и инструкций по их эксплуатации.

Таким образом, на основе анализа требований, вступивших в силу, можно выделить перечень основных направлений по их реализации:

1. Специалистам служб ИБ необходимо изучить Требования к защите ГИС, и определить подпадает ли ИС предприятия под действие рассмотренных документов.
2. Если ИС подпадает под действие данных требований, то необходимо:
   - провести обследование ИС с целью выявления несоответствий уровня защищенности ИС установленным требованиям;
   - разработать эскизный проект системы защиты ИС;
   - составить перечень необходимых средств защиты и заложить в бюджет предприятия соответствующие расходы на приобретение СЗИ и СКЗИ, а также на привлечение сторонних организаций для создания системы защиты;
   - провести аттестацию персонала подразделения ИБ и разработать план повышения квалификации персонала;
   - провести актуализацию нормативных документов предприятия по функционированию ИС и обеспечению безопасности информационных ресурсов в соответствии с установленными требованиями.

По рекомендациям ФСТЭК России разработать план приведения системы защиты в соответствие с Требованиями.

Таблица 3.

Класс защищенности ИС

Уровень значимости информационной системы	Масштаб информационной системы		
	Федеральный	Региональный	Объектовый
УЗ 1	К1	К1	К1
УЗ 2	К1	К2	К2
УЗ 3	К2	К3	К3

В настоящее время можно, с учетом рассмотренных выше требований, приступать к формирования эскизного проекта системы защиты ИС органа государственной власти, предприятия, организации, воинской части.

Выводы

По результатам исследования достигнуты следующие результаты:

1. Проведен краткий анализ требований новых документов, определяющих мероприятия по защите государственных информационных систем. Установлено, что круг информационных систем, подпадающих под действие новых требований существенно расширен и значительное количество должностных лиц подразделений по обеспечению информационной безопасности предприятий обязаны выполнять новые требования. стороны.

2. Система защита государственных информационных ресурсов вышла на новую систему координат, требования к системе защиты носят системный характер и отличаются новыми подходами к организации защиты и новыми критериями оценки их защищенности.

3. Анализ требований показал, что для обеспечения защищенности информационных ресурсов требуется проведение обследования информационных систем, и разработка планов (проектов) приведения систем защиты ИС в соответствие с требованиями, установленными регуляторами.

4. При разработке (модифицировании) системы защиты ГИС следует провести оценку защищенности ГИС по показателям ее защищенности – Кзи и по показателю уровня зрелости – Пзи, и на основе полученных значений формировать систему защиты. Данные показатели эффективности системы защиты являются основными для оценки возможности функционирования ГИС.

5. Очевидно, что к числу основных факторов, затрудняющих обеспечение защиты ИС является отсутствие сертифицированных средств защиты информации и сложности привлечения сторонних организаций для выявления уязвимости ИС, установки СЗИ, СКЗИ и проведения аттестационных испытаний, что объясняется необходимостью существенных финансовых затрат, которые необходимо иметь в бюджете предприятия.

6. Законодательством установлен обязательный перечень нормативных документов, которые должны быть разработаны на предприятии, что необходимо для создания и эксплуатации ГИС. Разработка этого ряда документов требует наличия высоко квалифицированного персонала и, в условиях отсутствия методических материалов, наличия значительного времени.

7. Целесообразно с целью экономии временных ресурсов приступать к разработке типовых документов (форм документов) и методических рекомендаций по их разработке. При этом научным подразделениям Вооруженных сил, уполномоченным на разработку методических документов по обеспечению информационной безопасности целесообразно обеспечить должное взаимодействие с регуляторами.

8. Исходя из значимости обеспечения защиты информационных систем Вооруженных сил и их специфики целесообразно формировать перечень средств обеспечения информационной безопасности, в том числе средств мониторинга событий ИС и/или вырабатывать требования к их разработке.

9. Приведенные в работе документы показывают, что одним из важнейших требований по обеспечению защиты информационных ресурсов является наличие достаточного количества подготовленных специалистов подразделениях технической защиты информации. Опыт показывает не хватку специалистов по информационной безопасности, особенно в государственных организациях. Предлагается учебным заведениям, которые готовят специалистов по работе с информационными системами и защите информации, добавить в учебные программы соответствующие темы, соответствующие требованиям, изложенных в рассмотренных документах.

10. Следует предполагать, что основные существенные требования о защите информационных систем установленные регуляторами должны быть реализованы в большинстве информационных систем Министерства обороны (за исключением оговоренных соответствующими приказами). Очевидно, что эти требования с учетом специфической деятельности необходимо выполнять в Вооруженных силах и необходимо приступать к разработке планов по их реализации.

11. Учитывая трудоемкость мероприятий по защите, ГИС, можно считать целесообразным органам обеспечения информационной безопасности (подразделениям по защите информации) готовиться к их реализации в настоящее время, поскольку соответствующие документы Министерства обороны Российской Федерации будут разработаны на основе документов от регуляторов.

12. В настоящее время разрабатывается новая Доктрина информационной безопасности Российской Федерации и к реализации положений Доктрины необходимо быть готовым, всем структурам, уполномоченным обеспечивать информационную безопасность органов, организаций, предприятий, учреждений и воинских частей.

Литература

1. Волостных В. А. Организация защиты конфиденциальной информации на предприятии средствами криптографической защиты / В. А. Волостных, П. А. Воробьев, В. А. Задбоев // Перспективы безопасности – 2024: Сборник материалов II научно-технической конференции, посвященной информационной безопасности, Санкт-Петербург, 19–20 июня 2024 г. – Санкт-Петербург: ООО «Специальный Технологический Центр», 2024. – С. 9–13.
2. Костарев С. В., Карганов В. В., Липатников В. А., Волостных В. А. Нормативная правовая база Российской Федерации обеспечения информационной безопасности. В книге: технологии защиты информации в условиях кибернетического противоборства. Санкт-Петербург, 2020. – С. 94–158.
3. Викулова А. Ю., Волостных В. А., Кононов П. А., Парфиров В. А. Защита персональных данных территориально-распределенных предприятий. В сборнике: Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО, 2021), сборник научных статей: в 4 т. Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича. СПб., 2021. – С. 155–160.
4. Волостных В. А., Задбоев В. А. Создание систем защищенного электронного документооборота, предназначенных для обработки документов, содержащих информацию ограниченного распространения. В Сборнике трудов конференции Сборник научных статей, 65-я научно-техническая конференция профессорско-преподавательского состава, научных работников и аспирантов (НТК ППС, 2025) СПб., СПбГУТ, 2025. – С 79–84.
5. Викулова А. Ю., Волостных В. А., Кононов П. А., Парфиров В. А. Защита персональных данных территориально-распределенных предприятий. В сборнике: Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО, 2021), сборник научных статей: в 4 т. Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича. СПб., 2021. – С. 155–160.
6. Задбоев В. А. анализ возможностей отечественных средств, применяемых для мониторинга информационной безопасности сетей передачи данных / В. А. Задбоев, Н. А. Роговой, А. А. Шевченко // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО, 2024): Материалы XIII Международной научно-технической и научно-методической конференции, Санкт-Петербург, 27–28 февраля 2024 года. – СПб.: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича, 2024. – С. 308-313.
7. Крюкова Е. С. Контроль качества электронных справочных и образовательных ресурсов для подготовки специалистов по техническому обслуживанию и ремонту средств и комплексов автоматизации управления / Е. С. Крюкова, А. Г. Емельяненко, И. Б. Паращук // Проблемы технического обеспечения войск в современных условиях: Труды X Межвузовской научно-практической конференции, Санкт-Петербург, 16 мая 2025 года. – СПб.: Федеральное Государственное Казенное Военное Образовательное Учреждение Высшего Образования «Военная академия связи им. Маршала Советского Союза С. М. Буденного» Министерства Обороны Российской Федерации, 2025. – С. 153–157.
8. Паращук И. Б. Классификационные признаки процедур мониторинга защищенности программно-аппаратных комплексов электронного документооборота, использующих каналы инфокоммуникационных сетей / И. Б. Паращук, Е. С. Владимирова, Л. А. Саяркин // 65-я научно-техническая конференция профессорско-преподавательского состава, научных работников и аспирантов (НТК ППС, 2025) : Сборник научных статей. В 3 т., Санкт-Петербург, 17–21 февраля 2025 года. – СПб.: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича, 2025. – С. 305–309.
9. Основы построения сертифицированных защищенных баз данных Российской Федерации / А. В. Красов, А. А. Миняев, И. Е. Пестов, И. А. Ушаков. – СПб.: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича, 2025. – 189 с.
10. Киселев Н. Н. Требования защищённости объекта КИИ с учетом развития требований регуляторов / Н. Н. Киселев, А. В. Красов // Региональная информатика и информационная безопасность: Сборник трудов Санкт-Петербургской международной конференции и XIV Санкт-Петербургской межрегиональной конференции, Санкт-Петербург, 29–31 октября 2025 года. – СПб.: Региональная общественная организация «Санкт-Петербургское Общество информатики, вычислительной техники, систем связи и управления», 2025. – С. 162–165.

ON THE IMPLEMENTATION OF NEW REQUIRED INFORMATION PROTECTION LEGISLATION OF THE RUSSIAN FEDERATION IN STATE INFORMATION SYSTEMS

Volostnykh V. A.[4], Zadboev V. A.[5], Shevchenko A. A.[6]

4 ***Viktor A. Volostnykh***, Ph.D. of Military Sciences, Associate Professor, Researcher of the Military Academy of Communications, St. Petersburg, Russia. E-mail: ra1alo@mail.ru

5 ***Vadim A. Zadboev***, Junior Researcher, Military Academy of Communications, St. Petersburg, Russia. E-mail: zadboev89@mail.ru

6 ***Alexander A. Shevchenko***, Ph.D. of Technical Sciences, Associate Professor, Senior Researcher of the Military Academy of Communications, St. Petersburg, Russia. E-mail: alex_pavel1991@mail.ru

Keywords: *information systems, cryptography, security threats, information security, legal documents.*

Abstract

The purpose of the work: *to analyze the current changes in the requirements for the security of state information systems and to develop approaches to their implementation in modern conditions.*

Results of the study: *changes in the requirements of Russian regulatory documents in the field of information security in state information systems are considered, without affecting information on state secrets.*

Based on the analysis of the modern application of practical experience in the field of information security in organizations, recommendations are proposed for updating protection systems in accordance with innovations. The main problems of the development of security systems of large information systems and ways to solve them are shown, significant changes in the legislation on information protection are identified, proposals are developed to recommend updating protection systems in accordance with innovations, to ensure the security of information processed in the information and telecommunication systems of enterprises, organizations, military units and institutions.

Practical usefulness: *lies in the fact that within the framework of a single study, a systematic documentary comparison of a number of regulatory legal documents is carried out and rational approaches to the implementation of requirements in modern conditions are developed, which can be applied to ensure the security of information in the information systems of enterprises, organizations, military units and institutions.*

References

1. Volostnykh V. A. Organization of the protection of confidential information at the enterprise by means of cryptographic protection / V. A. Volostnykh, P. A. Vorobyov, V. A. Zadboev // Security Prospects – 2024: Collection of materials from the II scientific and technical conference dedicated to information security, St. Petersburg, June 19–20, 2024. – St. Petersburg: OOO «Special Technology Center», 2024. – Pp. 9–13.
2. Kostarev S. V., Karganov V. V., Lipatnikov V. A., Volostnykh V. A. Regulatory legal framework of the Russian Federation for ensuring information security. In the book: Information security technologies in the context of cyber confrontation. St. Petersburg, 2020. – Pp. 94–158.
3. Vikulova A. Yu., Volostnykh V. A., Kononov P. A., Parfirov V. A. Personal data protection of geographically distributed enterprises. In the collection: Actual problems of infotelecommunications in science and education (APINO, 2021), a collection of scientific articles: in 4 volumes. Saint Petersburg State University of Telecommunications named after prof. M. A. Bonch-Bruevich. Saint Petersburg, 2021. – Pp. 155–160.
4. Volostnykh V. A., Zadboev V. A. Creation of secure electronic document management systems designed to process documents containing restricted information. In the Conference Proceedings, Collection of Scientific Articles, 65th Scientific and Technical Conference of Faculty, Researchers, and Postgraduate Students (NTK PPS, 2025), St. Petersburg, SPbSUT, 2025. – Pp. 79–84.
5. Vikulova A. Yu., Volostnykh V. A., Kononov P. A., Parfirov V. A. Personal Data Protection of Geographically Distributed Enterprises. In the collection: Current Issues of Infotelecommunications in Science and Education (APINO, 2021), collection of scientific articles: in 4 volumes. Saint Petersburg State University of Telecommunications named after prof. M. A. Bonch-Bruevich. Saint Petersburg, 2021. – Pp. 155–160.
6. Zadboev V. A. Analysis of the Capabilities of Domestic Tools Used to Monitor the Information Security of Data Transmission Networks / V. A. Zadboev, N. A. Rogovoy, A. A. Shevchenko // Actual Problems of Infotelecommunications in Science and Education (APINO, 2024): Proceedings of the XIII International Scientific, Technical and Scientific-Methodological Conference, Saint Petersburg, February 27–28, 2024. – Saint Petersburg: Saint Petersburg State University of Telecommunications named after prof. M. A. Bonch-Bruevich, 2024. – Pp. 308–313.
7. Kryukova E. S. Quality control of electronic reference and educational resources for training specialists in the maintenance and repair of automation control systems and systems / E. S. Kryukova, A.G. Emelyanenko, I. B. Parashchuk // Problems of technical support of troops in modern conditions: Proceedings of the X Interuniversity Scientific and Practical Conference, St. Petersburg, May 16, 2025. – St. Petersburg: Federal State Treasury Military Educational Institution of Higher Education «Military Academy of Communications named after Marshal of the Soviet Union S. M. Budyonny» of the Ministry of Defense of the Russian Federation, 2025. – P. 153–157.
8. Parashchuk I. B. Classification features of security monitoring procedures for software and hardware complexes of electronic document management using infocommunication network channels / I. B. Parashchuk, E. S. Vladimirova, L. A. Sayarkin // 65th Scientific and Technical Conference of the Faculty, Researchers and Postgraduate Students (NTK PPS, 2025): Collection of scientific articles. In 3 volumes, St. Petersburg, February 17–21, 2025. – St. Petersburg: St. Petersburg State University of Telecommunications named after prof. M. A. Bonch-Bruevich, 2025. – P. 305–309.
9. Fundamentals of constructing certified secure databases of the Russian Federation / A. V. Krasov, A. A. Minyaev, I. E. Pestov, I. A. Ushakov // – Saint Petersburg: Saint Petersburg State University of Telecommunications named after prof. Bonch-Bruevich, 2025. – 189 p.
10. Kiselev N. N. Security requirements for a critical information infrastructure facility, taking into account evolving regulatory requirements / N. N. Kiselev, A. V. Krasov // Regional informatics and information security: Proceedings of the Saint Petersburg International Conference and the XIV Saint Petersburg Interregional Conference, St. Petersburg, October 29–31, 2025. – Saint Petersburg: Regional public organization «Saint Petersburg Society of Informatics, Computer Engineering, Communications and Control Systems», 2025. – pp. 162–165.

ИННОВАЦИОННЫЙ ПОДХОД К ОБУЧЕНИЮ ОПЕРАТОРОВ СИСТЕМ РАДИОЭЛЕКТРОННОЙ БОРЬБЫ С БПЛА

Поликарпов Д. С.[1], Пономарев Д. Ю.[2], Бисултанов Р. С.[3]

DOI:10.21681/3034-4050-2026-4-93-98

Ключевые слова: *симулятор, тренировочные сценарии, радиоподавление, электромагнитное воздействие, учебные миссии, тактическая подготовка, виртуальная среда.*

Аннотация

Цель работы: *анализ и разработка симулятора для обучения операторов антидроновых ружей, направленного на формирование базовых теоретических знаний и практических навыков противодействия беспилотным летательным аппаратам в безопасной виртуальной среде.*

Результаты исследования: *разработанный симулятор позволяет значительно повысить уровень подготовки специалистов без необходимости использования реального оборудования. Пользователи получают возможность отрабатывать обнаружение и подавление каналов управления БПЛА в различных условиях, включая городскую среду, открытую местность и зоны с ограниченной видимостью. Система оценки фиксирует точность обнаружения, скорость реакции и правильность применения антидроновых средств, что способствует формированию устойчивых навыков.*

Научная новизна: *интеграция реалистичной физической модели радиопомех с адаптивными учебными сценариями, что позволяет максимально приблизить виртуальное обучение к реальным условиям эксплуатации антидроновых ружей.*

Введение

С развитием технологий беспилотных летательных аппаратов (БПЛА) произошла трансформация в сфере безопасности. Изначально разработанные для гражданских и коммерческих целей, дроны стали представлять серьезную опасность для защиты различных объектов. Широкая доступность, невысокая стоимость и легкость управления дронами создали совершенно новую обстановку, в которой потенциальная угроза может исходить от множества лиц.

В связи с этим необходимо пересмотреть подходы к подготовке специалистов, способных эффективно бороться с угрозами, исходящими от БПЛА. Устаревшие методы обучения, основанные на использовании реального оборудования в полевых условиях, теряют свою актуальность. Высокая цена антидроновых систем делает массовое обучение операторов нерентабельным, а потребность в специализированных полигонах ограничивает доступность обучения [1].

Современные виртуальные тренировочные комплексы предлагают кардинально новый путь решения указанной задачи. Формирование цифрового окружения, в высокой степени имитирующего реальность, дает возможность обойти ключевые недостатки классических способов обучения. Передовые технологии компьютерного моделирования достигли такого уровня, что стало возможным создание сложных симуляторов, способных воспроизводить не только внешний облик устройств, но и основные законы их работы.

Разработка обучающего симулятора для подготовки специалистов по антидроновым системам на базе Unreal Engine 5 представляется закономерным ответом на существующие вызовы. Unreal Engine 5 – это игровой движок, позволяющий создавать предельно реалистичные условия для обучения. Отличительной особенностью разрабатываемого симулятора является его комплексность. Таким образом, тренажёр не представляет собой поверхностный обзор оборудования, а воспроизводит основные аспекты работы систем борьбы с дронами. Это включает как практические навыки использования устройства, так и навыки оценки ситуации и принятия решений. Таким образом, обучаемые получают целостное представление о процессе противодействия беспилотным летательным аппаратам.

Важнейшей частью разработки является создание различных учебных миссий, которые будут охватывать широкий спектр сценариев. В виртуальном пространстве можно симулировать различные типы дронов, различающихся по своим летным характеристикам и схемам действий. Условия видимости, уровень

1 ***Поликарпов Дмитрий Сергеевич***, старший преподаватель кафедры радиоэлектронной борьбы Южного федерального университета. Таганрог, Россия. E-mail: polikarpov@sfedu.ru

2 ***Пономарёв Даниил Юрьевич***, студент Южного федерального университета. Таганрог, Россия. E-mail: daponomarev@sfedu.ru

3 ***Бисултанов Раджаб Сулайманович***, студент Южного федерального университета. Таганрог, Россия. E-mail: bisultanov@sfedu.ru

радиоэлектронных помех, особенности ландшафта – все эти переменные можно регулировать, обеспечивая подходящие условия для последовательного получения навыков.

Внедрение виртуальной реальности радикально преображает образовательный процесс. Полное вовлечение в искусственно созданную среду позволяет обучающимся оттачивать умения в обстановке, максимально имитирующей реальность. Это критически важно для выработки моторики при работе с оборудованием и развития пространственного воображения, необходимого для эффективного реагирования на быстро движущиеся объекты.

Создаваемый симулятор демонстрирует успешное воплощение передовых компьютерных технологий для решения актуальных задач в сфере безопасности. Сочетание современных графических технологий, точной физической симуляции и методически выверенной системы обучения формирует мощный инструмент для подготовки специалистов. Данный подход открывает новые горизонты для организации широкомасштабного обучения пользователей с минимальными финансовыми затратами (рис. 1).

Рис. 1. Теоретические материалы

Дальнейшее развитие проекта связано с непрерывным расширением функционала системы. Внедрение новых видов угроз, усовершенствование физической модели, добавление дополнительных сценариев – все это будет способствовать повышению отдачи от подготовки специалистов. Значительное внимание уделяется вопросам адаптивности решения для различных групп пользователей.

Внедрение подобных симуляторов в программы обучения знаменует новый этап в подготовке специалистов по противодействию беспилотным угрозам. Виртуальные тренировочные системы становятся не просто дополнением к традиционным методам, а полноценной альтернативой, обладающей рядом неоспоримых преимуществ. Это особенно важно в условиях, когда скорость появления новых угроз опережает возможности традиционных систем подготовки кадров.

Постановка задач

Создание тренажера для нейтрализации беспилотных летательных аппаратов (БПЛА) сопряжено с решением ряда переплетающихся проблем, направленных на создание действенного и безопасного инструмента обучения [2, 3]. Ключевой задачей является точное воспроизведение работы антидроновых ружей, включая их спецификации, принципы функционирования и ограничения. Данные средства используют различные способы воздействия на дроны, например, направленное электромагнитное излучение. Тренажер призван детально имитировать эти процессы, чтобы пользователи понимали, как и при каких условиях целесообразно применять тот или иной режим работы.

Второй немаловажной задачей является разработка различных ситуаций, правдоподобно отображающих реальные сценарии использования антидроновых систем. Это включает в себя разнообразные типы БПЛА (мультикоптеры, самолетного типа и гибридные модели), особенности их полетов (одиночные вылеты, групповые атаки, уклонение от воздействия), а также влияние окружающей среды (погодные условия, городская застройка, сторонние радиопомехи) [4]. Уровень сложности заданий должен гибко изменяться в зависимости от навыков пользователя, начиная с элементарных обучающих упражнений и переходя к комплексным тактическим маневрам.

Третья важной целью является развитие у обучаемых способностей по обнаружению и квалификации БПЛА. Они могут быть оснащены камерами, передающими устройствами и даже взрывчатые вещества, поэтому оператору необходимо быстро определять степень опасности. Тренажер должен обеспечивать обучение не только путем визуального распознавания, но и с использованием вспомогательных средств, таких как детекторы дронов и тепловизоры. Существенно, чтобы специалист разбирался в различиях между мультикоптерами, FPV-дронами и БПЛА самолетного типа, а также знал, какие ответные меры следует применять в каждом отдельном случае.

Четвертая задача – совершенствование тактических навыков. Работа с антидроновым оружием требует не только технических знаний, но и понимания тактики. Специалист должен грамотно выбирать позицию и менять её после подавления БПЛА, рассчитывать расстояние до цели, предвидеть траекторию движения БПЛА и ожидать появление последующих БПЛА. В тренажере должны быть сценарии, подразумевающие действия в условиях дефицита времени и минимизации сопутствующего ущерба.

И, наконец, пятая задача – создание системы оценки эффективности обучения. Тренажер должен фиксировать ключевые показатели, такие как время реакции, точность обнаружения, правильность выбора метода противодействия и соблюдение правил безопасности. На основе этих данных формируется индивидуальная статистика, позволяющая выявить пробелы в подготовке обучающегося и скорректировать программу обучения.

Таким образом, поставленные задачи охватывают техническое моделирование, разработку реалистичных сценариев, формирование практических навыков и объективную оценку результатов обучения [5]. Такой комплексный подход обеспечивает не только имитацию работы с антидроновыми ружьями, но и полноценную подготовку специалистов, готовых к эффективным действиям в реальных условиях.

Решение поставленной задачи

Разработка комплексного симулятора для подготовки операторов антидроновых ружей потребовала создания многоуровневой архитектуры, объединяющей передовые технологии моделирования с методически обоснованной системой обучения. Основой решения стал выбор платформы Unreal Engine 5, предоставляющей уникальный набор инструментов для реализации всех компонентов системы [6]. Этот современный игровой движок сочетает мощные графические возможности с гибкостью программирования, что делает его идеальной основой для специализированных тренажерных систем.

Применения технологий Nanite и Lumen обеспечивают фотореалистичную визуализацию интерактивной учебной среды. Nanite позволяет использовать высокодетализированные модели оборудования и окружающей среды без потери производительности, что крайне важно для идеального воспроизведения всех нюансов противодронового оружия, чтобы каждый элемент управления работал (рис. 2). Динамическое глобальное освещение обеспечивается Lumen, что обеспечивает реалистичные эффекты света и тени в различных ситуациях – от яркого дневного света до сложных ночных условий с тепловизорами [7].

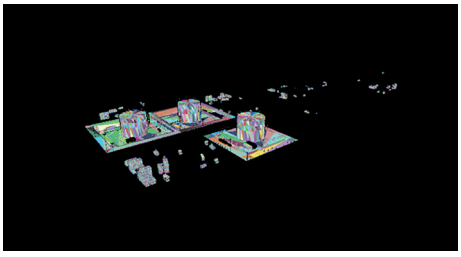


Рис. 2. Визуализация Nanite

Физическая модель для симулятора основана на системе Chaos, где она с высокой точностью эмулирует основные принципы работы противодронового ружья (рис. 3). При моделировании особое внимание уделяется имитации электромагнитного излучения с учетом мощности сигнала, характеристик антенны, а также эффектов затухания в различных средах. Для устройств радиоэлектронного подавления разработана детализированная модель генерации помех, учитывающая задержки во времени распространения сигнала и особенности модуляции. Визуализация отображает зону эффективного действия в режиме реального времени, позволяя оператору оценивать эффективность своих действий.

Рис. 3. Физическая модель на системе Ghaos

Моделирование поведения БПЛА представляет собой сложную инженерную задачу (рис. 4). В симуляторе реализована библиотека типовых моделей дронов, различающихся по аэродинамическим характеристикам, системам навигации и алгоритмам полета. Для реалистичного воспроизведения применяются физически обоснованные модели, учитывающие массу, подъемную силу, инерцию и ветровые нагрузки. Особый интерес представляют алгоритмы реакции на внешние воздействия – при подавлении каналов управления дрон может переходить в различные режимы: возврат к оператору, автопосадка или продолжение полета по последним известным координатам.

Рис. 4. Моделирование поведения БПЛА

Функциональность симулятора обеспечивается комплексом инструментов Unreal Engine 5. Blueprints позволяют создавать интуитивно понятный интерфейс и систему управления [8],

в то время как MetaSounds отвечает за пространственное звуковое сопровождение, критически важное для локализации целей [9]. Niagara используется для визуализации специальных эффектов, включая электромагнитное воздействие и радиопомехи.

Система оценки эффективности обучения построена на анализе множества параметров, включая время реакции, точность наведения, выбор оптимального метода нейтрализации и соблюдение мер безопасности. Для каждого упражнения разработаны комплексные критерии оценки, учитывающие как технические навыки, так и тактическое мышление оператора [10]. Статистика сохраняется в индивидуальном профиле обучаемого, позволяя отслеживать прогресс и выявлять проблемные области подготовки.

Система обучения построена по модульному принципу, сочетая теоретические материалы с практическими упражнениями. Теоретический блок включает интерактивные лекции по физическим принципам работы антидроновых ружей, классификации БПЛА и правовым аспектам их нейтрализации. Практическая часть начинается с простых упражнений по обнаружению и завершается комплексными миссиями, требующими применения всех полученных навыков в условиях, приближенных к реальным.

Использование Unreal Engine 5 в качестве технологической основы позволяет создать многофункциональную обучающую платформу, сочетающую техническую достоверность с методической эффективностью. Движок предоставляет все необходимые средства для точного моделирования как физических процессов, так и тактических ситуаций, с которыми операторы могут столкнуться в реальных условиях эксплуатации антидроновых ружей [11].

Выводы

Разработанный симулятор на базе Unreal Engine 5 представляет собой современное решение для подготовки операторов антидроновых ружей, сочетающее технологическую инновационность с практической эффективностью. Реализация проекта подтвердила возможность создания высоко реалистичной учебной среды, где специалисты могут отрабатывать навыки противодействия БПЛА без рисков и затрат, связанных с полевыми учениями.

Ключевым достижением стала интеграция фотореалистичной визуализации с точной физической моделью работы антидроновых ружей. Использование технологий Nanite и Lumen позволило достичь беспрецедентного уровня детализации, критически важного для идентификации типов БПЛА и оценки дистанций. Система Chaos обеспечила достоверное моделирование электромагнитного воздействия и аэродинамики беспилотников, что принципиально отличает данный симулятор от аналогичных решений.

Практическая ценность разработки заключается в ее адаптивности и комплексном подходе к обучению. Встроенная система оценки не просто фиксирует результаты, но и анализирует тактические решения оператора, формируя персонализированные рекомендации.

Перспективы развития проекта связаны с расширением библиотеки сценариев за счет включения новых типов угроз и условий окружающей среды. Особое внимание будет уделено моделированию группового взаимодействия операторов и интеграции с другими системами противодействия БПЛА. Дальнейшая оптимизация позволит развертывать решение на мобильных платформах без потери качества симуляции.

Внедрение данного симулятора в программы подготовки специалистов позволит существенно повысить уровень их квалификации при значительном снижении эксплуатационных расходов [12]. Разработка устанавливает новый стандарт в области виртуальной тренировки операторов антидронового оборудования, сочетая технологические возможности Unreal Engine 5 с глубокой проработкой предметной области.

Литература

1. Адаптивное персонализированное обучение: внедрение современных технологий в высшем образовании / М. В. Максимова, О. В. Фролова, Х. Х. Этуев, Л. Д. Александрова // Информатика и образование. – 2023. – Т. 38. – № 4. – С. 14–27. – DOI 10.32517/0234-0453-2023-38-4-14-27.
2. Мельник В. Н. Технологии виртуальной реальности в военном образовании: мировой опыт и лучшие практики / В. Н. Мельник // Динамика развития системы военного образования: Материалы VII Международной научно-практической конференции, Омск, 14 марта 2025 года. – Омск: Омский государственный технический университет, 2025. – С. 496–501.
3. Уварина Н. В. Анализ и перспективы применения иммерсивных технологий в системе подготовки офицеров российской армии / Н. В. Уварина, А. В. Полковников // Современная высшая школа: инновационный аспект. – 2020. – Т. 12 – № 4 (50). – С. 10–19. – DOI 10.7442/2071-9620-2020-12-4-10-19.

4. Кудряшов В. А. Тренажеры, тренажеры-симуляторы управления беспилотным воздушным судном / В. А. Кудряшов // Академический вестник войск национальной гвардии Российской Федерации. – 2024. – № 3. – С. 8–14.
5. Федулов В. А. Оценка эффективности системы поражения малоразмерных беспилотных летательных аппаратов методом имитационного моделирования / В. А. Федулов, Н. В. Быков, В. Д. Баскаков // Системы управления, связи и безопасности. – 2023. – № 4. – С. 63–104. – DOI 10.24412/2410-9916-2023-4-63-104.
6. Французов А. М. Сравнительный анализ графических движков Unreal Engine 4 и Unreal Engine 5 / А. М. Французов, И. М. Камалутдинов // Научные открытия: междисциплинарные аспекты: Сборник статей Международной научно-практической конференции, Саратов, 20 января 2024 года. – Москва: Издательство «Доброе слово и Ко», 2024. – С. 243–249.
7. Карпов Д. Е. Lumen и Nanite в Unreal Engine 5: разбор новых технологий глобального освещения и визуализации, их влияние на процесс разработки и качество графики / Д. Е. Карпов // Актуальные исследования. – 2024. – № 21-1 (203). – С. 80–84.
8. Model Checking of Visual Scripts Created by UE4 Blueprints / N. Igawa, T. Yokogawa, M. Takahashi, K. Arimoto // Proceedings – 2020, 9th International Congress on Advanced Applied Informatics, IIAI-AAI 2020: 9, Kitakyushu, 01–15 сентября 2020 года. – Kitakyushu, 2020. – P. 512–515. – DOI: 10.1109/IIAI-AAI50415.2020.00107.
9. Евграфова Е. Е. Технология создания звукового сопровождения в интерактивной виртуальной среде / Е. Е. Евграфова, Л. С. Землянникова // Актуальные проблемы информатизации в цифровой экономике и научных исследованиях: Материалы V Научно-практической конференции с международным участием, Москва, 21–22 ноября 2024 года. – Москва: Национальный исследовательский университет «Московский институт электронной техники», 2024. – С. 14–19.
10. Среда моделирования трехмерных сцен для обучения и тестирования алгоритмов компьютерного зрения / А. В. Колдомасов, П. А. Гессен, А. И. Лизин [и др.] // Перспективные системы и задачи управления: Материалы XVIII Всероссийской научно-практической конференции и XIV молодежной школы-семинара. Посвящается памяти Почетного члена Оргкомитета Конференции, водителя первого лунохода, генерал-майора В. Г. Довганя, п. Домбай, Карачево-Черкесская Республика, 03–07 апреля 2023 года. – Таганрог: Общество с ограниченной ответственностью Издательство «Лукоморье», 2023. – С. 365–376.
11. Король М. А. Продвинутая система передвижения и ее использование в Unreal Engine / М. А. Король, А. Г. Дзюба, В. В. Верютина // Инноватика – 2022 : Сборник материалов XVIII международной школы-конференции студентов, аспирантов и молодых ученых, Томск, 21–22 апреля 2022 года. – Томск: Общество с ограниченной ответственностью «СТТ», 2022. – С. 428–430.
12. Прищепа В. Н. Интерактивный тренировочный комплекс по формированию первичных навыков выполнения упражнений армейской тактической стрельбы / В. Н. Прищепа, А. В. Северенко, И. Г. Кириллов // Военная мысль. – 2024. – № 10. – С. 54–59.

INNOVATIVE APPROACH TO TRAINING OPERATORS OF ELECTRONIC COMBAT SYSTEMS AGAINST UAVS

Polikarpov D. S.[4], Ponomarev D. Yu.[5], Bisultanov R. S.[6]

Keywords: *simulator, training scenarios, radio suppression, electromagnetic effects, training missions, tactical training, virtual environment.*

Abstract

The purpose of the work: *analysis and development of a simulator for training anti-drone gun operators, aimed at forming basic theoretical knowledge and practical skills in countering unmanned aerial vehicles in a safe virtual environment.*

Research results: *the developed simulator allows to significantly increase the level of training of specialists without the need to use real equipment. Users get the opportunity to practice detection and suppression of UAV control channels in various conditions, including urban environments, open areas and areas with limited visibility. The assessment system records the accuracy of detection, reaction speed and correctness of the use of anti-drone means, which contributes to the formation of sustainable skills.*

Scientific novelty: *integration of a realistic physical model of radio interference with adaptive training scenarios, which allows virtual training as close as possible to the real conditions of operation of anti-drone guns.*

References

1. Adaptive personalized learning: implementation of modern technologies in higher education / M. V. Maksimova, O. V. Frolova, H. H. Etuev, L. D. Aleksandrova // Computer Science and Education. – 2023. – Vol. 38, No 4. – Pp. 14–27. – DOI 10.32517/0234-0453-2023-38-4-14-27.

4 ***Dmitry S. Polikarpov***, Senior Lecturer, Department of Electronic Warfare, Southern Federal University. Taganrog, Russia. E-mail: polikarpov@sfedu.ru
5 ***Daniil Yu. Ponomarev***, Student, Southern Federal University. Taganrog, Russia. E-mail: daponomarev@sfedu.ru
6 ***Radzhab S. Bisultanov***, Student, Southern Federal University, Taganrog. Russia. E-mail: bisultanov@sfedu.ru

2. Melnik V. N. Virtual reality technologies in military education: world experience and best practices / V. N. Melnik // Dynamics of development of the military education system: Proceedings of the VII International Scientific and Practical Conference, Omsk, March 14, 2025. – Omsk: Omsk State Technical University, 2025. – Pp. 496–501.
3. Uvarina N. V. Analysis and prospects of using immersive technologies in the training system of officers of the Russian army / N. V. Uvarina, A. V. Polkovnikov // Modern higher education: innovative aspect. – 2020. – Vol. 12. – No 4 (50). – P. 10–19. – DOI 10.7442/2071-9620-2020-12-4-10-19.
4. Kudryashov V. A. Simulators, training simulators for controlling an unmanned aerial vehicle / V. A. Kudryashov // Academic Bulletin of the National Guard Troops of the Russian Federation. – 2024. – No. 3. – P. 8–14.
5. Fedolov V. A. Evaluation of the effectiveness of the system for defeating small-sized unmanned aerial vehicles using the simulation modeling method / V. A. Fedolov, N. V. Bykov, V. D. Baskakov // Control, Communications and Security Systems. – 2023. – No 4. – P. 63–104. – DOI 10.24412 / 2410-9916-2023-4-63-104.
6. Frantsuzov A. M. Comparative analysis of the graphics engines Unreal Engine 4 and Unreal Engine 5 / A. M. Frantsuzov, I. M. Kamalutdinov // Scientific discoveries: interdisciplinary aspects: Collection of articles from the International Scientific and Practical Conference, Saratov, January 20, 2024. – Moscow: Izdatelstvo «Dobroe slovo i Ko», 2024. – P. 243–249.
7. Karpov D. E. Lumen and Nanite in Unreal Engine 5: Analysis of New Global Illumination and Visualization Technologies, Their Impact on the Development Process and Graphics Quality / D. E. Karpov // Actual Research. – 2024. – No 21-1 (203). – P. 80–84.
8. Model Checking of Visual Scripts Created by UE4 Blueprints / N. Igawa, T. Yokogawa, M. Takahashi, K. Arimoto // Proceedings – 2020, 9th International Congress on Advanced Applied Informatics, IIAI-AAI 2020: 9, Kitakyushu, September 01–15, 2020. – Kitakyushu, 2020. – P. 512–515. – DOI 10.1109/IIAI-AAI50415.2020.00107.
9. Evgrafova E. E. Technology of creating sound accompaniment in an interactive virtual environment / E. E. Evgrafova, L. S. Zemlyannikova // Actual problems of informatization in the digital economy and scientific research: Proceedings of the V Scientific and Practical Conference with international participation, Moscow, November 21–22, 2024. – Moscow: National Research University «Moscow Institute of Electronic Technology», 2024. – P. 14–19.
10. Three-dimensional scene modeling environment for training and testing computer vision algorithms / A. V. Koldomasov, P. A. Gessen, A. I. Lizin [et al.] // Advanced control systems and tasks: Proceedings of the XVIII All-Russian scientific and practical conference and the XIV youth school-seminar. Dedicated to the memory of the Honorary Member of the Organizing Committee of the Conference, the driver of the first lunar rover, Major General V. G. Dovgan, p. Dombay, Karachevo-Cherkess Republic, April 3–7, 2023. – Taganrog: Limited Liability Company Publishing House «Lukomorye», 2023. – P. 365–376.
11. Korol, M. A. Advanced movement system and its use in Unreal Engine / M. A. Korol, A. G. Dzyuba, V. V. Veryutina // Innovatika – 2022: Collection of materials of the XVIII international school-conference of students, graduate students and young scientists, Tomsk, April 21–22, 2022. – Tomsk: Limited Liability Company «STT», 2022. – P. 428–430.
12. Prishchepa, V. N. Interactive training complex for the formation of primary skills in performing army tactical shooting exercises / V. N. Prishchepa, A. V. Severenko, I. G. Kirillov // Military Thought. – 2024. – No 10. – P. 54–59.

ПОДХОДЫ К СОЗДАНИЮ БАЗОВОЙ ЦИФРОВОЙ НАУЧНО-ОБРАЗОВАТЕЛЬНОЙ ПЛАТФОРМЫ В ВЫСШИХ УЧЕБНЫХ ЗАВЕДЕНИЯХ ДЛЯ ПОДГОТОВКИ СПЕЦИАЛИСТОВ СВЯЗИ

Богданов А. В.[1], Казакевич Е. В.[2]

DOI:10.21681/3034-4050-2026-4-99-105

Ключевые слова: *цифровые технологии, программно-аппаратные комплексы, инфокоммуникационная сеть.*

Аннотация

Цель работы: *обоснование системотехнических решений при формировании облика базовой цифровой научно-образовательной платформы.*

Метод исследования: *анализ инфокоммуникационной сети военного образовательного учреждения и программно-аппаратных средств, обеспечивающих синтезирующие решения технической основы создания сетевой инфраструктуры и информационно-вычислительного кластера базовой цифровой научно-образовательной платформы.*

Результаты исследования: *получено обоснование системотехнических решений при формировании облика БЦНОП, обеспечивающей техническую основу создания аппаратно-программных средств для эффективной подготовки специалистов войск связи к эксплуатации высокотехнологичных средств и комплексов связи.*

Практическая полезность: *представленные предложения и рекомендации позволяют сформировать перспективный облик научно-образовательной платформы, обеспечивающей повышение качества образовательного процесса.*

Введение

Успешное внедрение цифровой научно-образовательной платформы, как автоматизированной системы должно опираться на использование передовых технологий в процессе обучения, гибридных лабораторий, перспективных интеллектуальных и адаптивных средств обучения, последних достижений в науке и технике, современных подходов в области нейронных технологий, технологий искусственного интеллекта и робототехники. Все представленные факторы обусловили актуальность и необходимость создания базовой цифровой научно-образовательной платформы (БЦНОП) для повышения качества специальной и технической подготовки специалистов связи.

Анализ отечественных и мировых тенденций показывает [1–3], что системы образования и науки должны опираться на адаптивную среду с персонализированными научно-образовательными траекториями, направленными на практико-ориентированное обучение, где обучающиеся, преподаватели, научные работники и представители заказывающих органов могут совместно работать над развитием новых идей, техники и научно-исследовательской деятельности.

Современная система подготовки специалистов связи в высших учебных заведениях, в том числе для Вооруженных Сил Российской Федерации, должна опираться на использование передовых технологий в процессе обучения, гибридных лабораторий, перспективных интеллектуальных и адаптивных средств обучения, последних достижений в науке и технике, современных подходов в области нейронных технологий, технологий искусственного интеллекта и робототехники – см.[3], а также [4–8].

В материалах статьи показано, что для реализации и внедрения данных технологий в процесс подготовки специалистов связи необходимо создать техническую платформу, обладающую гибкой, масштабируемой и функциональной совместимой (интероперабельной) архитектурой.

1 ***Богданов Александр Валентинович***, кандидат военных наук, доцент, старший научный сотрудник НИЦ Военной академии связи им. Маршала Советского Союза С. М. Буденного. Санкт-Петербург, Россия. E-mail: bog-saha@yandex.ru

2 ***Казакевич Елена Владимировна***, кандидат технических наук, доцент, заведующий кафедрой «Электрическая связь» Петербургского государственного университета путей сообщения Императора Александра I. С-Петербург, Россия. E-mail: kev-pgups@yandex.ru

3 Указ Президента РФ от 09.05.2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы». Https://www.garant.ru/products/ipo/prime/doc/71570570/?ysclid=mo4ve6t1b3682737958
Распоряжение Правительства Российской Федерации от 5 июля 2025 г. № 1805-р «О стратегическом направлении в области цифровой трансформации отрасли науки и высшего образования до 2030 г.» Https://www.garant.ru/products/ipo/prime/doc/412194202/?ysclid=mnybwkusd1321455637
Распоряжение Правительства Российской Федерации от 24 ноября 2023 г. № 3339-р «Об утверждении Стратегии развития отрасли связи РФ на период до 2035 года.» Https://www.garant.ru/products/ipo/prime/doc/408020989/?ysclid=mnyjhrj14q33534432

Обоснование необходимости создания базовой цифровой научно-образовательной платформы ВУЗа

Опыт внедрения цифровых технологий в научно-образовательной сфере показал [2, 3], что необходимо развивать системы информационного обмена обеспечивающих устойчивую работу автоматизированных систем. При этом устойчивость информационного обмена в основном определяется состоянием телекоммуникационной системы. Технологическое развитие телекоммуникационных систем образовательных организаций, в том числе высших учебных заведений (ВУЗов), предполагает не только использование программно-аппаратной реализации средств и комплексов связи, но и создание единого телекоммуникационного пространства.

Кроме того, сложившаяся за последнее время в ВС РФ парадигма реализации концепции многосферной операции, характеризуется расширением пространства ведения боевых действий за счет увеличения количества локальных областей применения силы и расстояния между ними, интеллектуализацией и роботизацией боевых и обеспечивающих платформ, появлением новой среды ведения военных действий – кибернетического пространства, что налагает дополнительные требования при подготовке военных специалистов связи.

Имеющийся опыт обучения специалистов войск связи и результаты проведенных исследований [5, 7, 8] показывают, что требуемый уровень эффективности подготовки специалистов достигается при проведении согласованного обучения курсантов и адъюнктов ВУЗов, а также повышения квалификации профессорско-преподавательского состава учебных заведений и должностных лиц представителей работодателей, на единой сетевой учебно-лабораторной базе, которая основывается на архитектуре научно-образовательной платформы ВУЗа (рис. 1).

Существующие инфотелекоммуникационные системы учебных заведений недостаточно интегрированы в учебный процесс межвузовского пространства и низком взаимодействии с представителями работодателей (заказчиком). Для реализации этой задачи требуется ведение информационного обмена на всех уровнях стека протоколов автоматизированных систем ВУЗов и разработки такой формы организации, как сетевая структура, обеспечивающая программное, информационное, математическое и лингвистическое взаимодействие, которая требует нового подхода к построению цифровой научно-образовательной платформы.

Тенденция технологического развития отрасли связи[4] и построение единого телекоммуникационного пространства приводит к необходимости внедрения на сетях связи инновационных архитектурных решений, автоматизации управления их работой и обеспечения информационной безопасности.

В соответствии со стратегией цифровой трансформации науки и высшего образования[5] построение единого телекоммуникационного пространства отраслевых образовательных организаций высшего образования с использованием программного обеспечения и программно-аппаратных комплексов российского производства обеспечит повышение эффективности подготовки не только кадров войск связи, но и специалистов телекоммуникационной отрасли в целом.

Подходы к созданию базовой цифровой научно-образовательной платформы ВУЗа

Структурно базовая цифровая научно-образовательная платформа (БЦНОП) представлена на рисунке 1 и должна включать в свой состав:

- техническую основу, обеспечивающую интерактивное, адаптивное и дистанционное обучение;
- распределенные центры инженерной, специальной и технической подготовки специалистов (учебные центры и полигоны ВУЗов и подразделений работодателей).

Техническая основа базовой цифровой научно-образовательной платформы представляет собой программно-аппаратный комплекс инфокоммуникационной сети связи и информационно-вычислительного кластера, предназначенного для обеспечения интеграции и взаимодействия с информационно-образовательными средами учебных подразделений. Гибридные учебные лаборатории предназначены для обеспечения технической подготовки, в том числе и путем дистанционного обучения (переподготовки и повышения квалификации) специалистов на рабочих местах по предназначению.

Вариант построения инфотелекоммуникационной сети ВУЗа

Инфотелекоммуникационная сеть (ИТКС) ВУЗа представляет собой сложную инфраструктуру, спроектированную для обеспечения обмена

4 Распоряжение Правительства Российской Федерации от 24 ноября 2023 г. № 3339-р «Об утверждении Стратегии развития отрасли связи РФ на период до 2035 года.» Https://www.garant.ru/products/ipo/prime/doc/408020989/?ysclid=mnyjhrj14q33534432

5 Распоряжение Правительства Российской Федерации от 5 июля 2025 г. № 1805-р «О стратегическом направлении в области цифровой трансформации отрасли науки и высшего образования до 2030 г.» Https://www.garant.ru/products/ipo/prime/doc/412194202/?ysclid=mnybwkusd1321455637

Рис. 1. Облик базовой научно-образовательной платформы ВУЗа

информации между объектами учреждения. Ее структура включает несколько уровней, каждый из которых выполняет определённые функции и обеспечивает бесперебойную работу всех сервисов. Сеть должна быть построена по классической трехуровневой модели: доступ, агрегация и ядро (Core-Distribution-Access). Каждый из уровней выполняет определённые задачи, связанные с подключением устройств и обработкой трафика.

Задача уровня доступа по подключению оконечных устройств (ПК, серверов) к сети обеспечивается коммутаторами второго уровня (L2). Коммутаторы уровня доступа не связаны друг с другом, связь между конечными точками происходит через уровень агрегации.

Задача уровня агрегации решается коммутаторами третьего уровня (L3), обеспечивающими маршрутизацию между виртуальными локальными сетями (VLAN) и подсетями, фильтрацию, балансировку трафика, управление приоритетами системы обеспечения качества информационного обмена (QoS) и механизмы безопасности. Устойчивость информационного обмена обеспечивается за счет избыточности, которая позволяет резервировать каналы за счёт реконфигурации сети при выходе из строя одного из каналов передачи.

Задача уровня ядра заключается в передаче данных между агрегационными узлами с помощью маршрутизаторов-коммутаторов, которые поддерживают расширенные функции коммутации уровня 3 и протоколы динамической маршрутизации.

Схема сети классической трехуровневой модели Core-Distribution-Access представлена на рисунке 2.

Управление сетью передачи данных должно осуществляться с помощью центра обработки данных (ЦОД) и включать в себя различные компоненты, инженерные системы и оборудование.

Основными компонентами ЦОД являются:

- специализированное помещение или комплекс помещений, где размещается оборудование ЦОД;
- информационная инфраструктура, состоящая из серверного комплекса, системы хранения данных (выделенная сеть для объединения устройств хранения данных Storage Area Network – SAN) с использованием коммутаторов Brocade работающих по протоколу для высокоскоростной передачи данных (Fibre Channel – FC) и резервного копирования;
- сетевая инфраструктура включает маршрутизаторы, коммутаторы и межсетевые экраны, которые обеспечивают информационный обмен между серверами и внешними сетями;
- инженерные системы: системы электроснабжения ЦОД, которые подключают к нескольким независимым источникам питания, в том числе резервные генераторы, и устанавливают системы бесперебойного питания (ИБП); системы охлаждения, которые поддерживают оптимальную температуру, предотвращают перегрев оборудования; систему безопасности, обеспечивающую контроль доступа, видеонаблюдение, пожарную сигнализацию и системы пожаротушения;

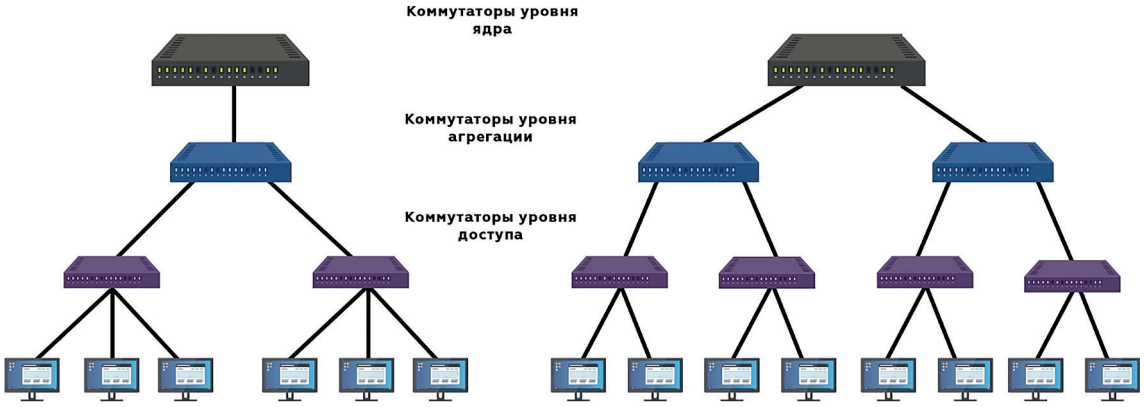


Рис. 2. Схема сети Core-Distribution-Access

- системы мониторинга и диспетчеризации отслеживают состояние оборудования в режиме реального времени, обеспечивают оперативное реагирование на проблемы.

Инфотелекоммуникационную сеть между объектами БЦНОП предлагается строить на технологии высокоскоростной передачи данных MPLS (Multiprotocol Label Switching), которая использует метки (labels) для маршрутизации пакетов вместо традиционной IP-маршрутизации. Она сочетает преимущества коммутации на уровне доступа (L2), как в технологии Ethernet, и маршрутизации на уровне агрегации (L3), как в технологии IP, обеспечивая низкие задержки и высокую производительность.

Предварительный анализ функционирования ИТКС ВУЗа, проведенный в Военной академии связи, показал, что минимально допустимыми требованиями по пропускной способности между слоями определяются следующим образом:

- на уровне доступа (L2) при подключении оконечных устройств, таких как компьютеры, точки доступа к автоматизированным рабочим местам (АРМ) и IP-телефонам, скорость подключения с любого АРМ до коммутаторов уровня L2 должна составлять 100 Мбит/с, а между уровнем доступа и агрегации – 1 Гбит/с.
- на уровне агрегации (L3) объединение трафика с уровнем доступа и его передача на уровень ядра, при использовании коммутаторов типа Edge-Core ECS 4660, должна обеспечиваться со скоростью не менее 10 Гбит/с;
- на уровне ядра (L3) должна обеспечиваться высокоскоростная маршрутизация трафика между сегментами сети при использовании маршрутизаторов типа Juniper SRX 650 и коммутаторов типа Juniper EX4500, а также оборудования T-Metro 7224, со скоростью не менее 10 Гбит/с. При этом, применяется протокол внутренней маршрутизации (OSPF), который позволяет эффективно управлять динамическими изменениями топологии.

Вариант аппаратной и технологической части ИТКС БЦНОП предлагается строить на прототипах следующих устройств и оборудования:

- T-Metro 7224 является агрегирующим свитч/маршрутизатором доступа Carrier Ethernet с поддержкой MPLS и обеспечения требований QoS;
- оборудование T-Marc гибридных учебных лабораторий является граничным устройством и поддерживает технологии Carrier Ethernet, MPLS и L3-функции, QoS;
- оборудование SI-3000 представляет собой мультисервисную платформу фирмы Iskratel, обеспечивающую работу в транспортной сети с временным разделением каналов потока E1, и предоставлением услуг телефонии, оповещения/видео;
- мультиплексоры E1 для обеспечения скорости передачи информации 2,048 Мбит/с.

Плюсы и минусы предлагаемых решений

Преимущества предлагаемой архитектуры ИТКС:

- разграничение доступа клиентской части оборудования к центру обработки данных и возможности контроля и мониторинга отдельных элементов сети;
- единая транспортная шина для всех сервисов;
- экономия телекоммуникационного ресурса при предоставлении услуг телефонии, оповещения/видео;
- совместимость с оборудованием предыдущего поколения.

Недостатки предлагаемой архитектуры ИТКС:

- для передачи видео трафика канал E1 является «узким местом», для этого необходимо обеспечивать передачу информации

по протоколу Ethernet поверх MPLS, а канал E1 использовать для служебной связи или резерва;
- при организации широковещательной передачи данных (групповой) возможна перегрузка каналов связи;
- операционная сложность реализации MPLS при развертывании, управлении и эксплуатации сети.

Проведенный анализ аппаратной и технологической части прототипов оборудования и описание структуры инфотелекоммуникационной сети ВУЗа позволяет сделать вывод о возможности создания БЦНОП на ее основе. Однако выбор вычислительных мощностей серверного оборудования ИТКС ВУЗа и пропускных способностей линий, соединяющих подразделения и гибридные учебные лаборатории в единый кластер возможно будет определить после проведения информационного обследования подразделений ВУЗа и оценки производительности приобретаемого и внедряемого оборудования для создания БЦНОП.

Кроме того, предложенный подход к построению ИТКС ВУЗа позволяет также создавать распределенные центры подготовки при объединении БЦНОП других ВУЗов, которые предназначены для совместного обучения должностных лиц структурных подразделений заказчика, адъюнктов и курсантов в рамках проведения многоуровневых компьютерных специальных игр. Они должны представлять собой систему учебных пунктов, подключенных к имитационно-моделирующей виртуальной среде, построенной на основе технологии «цифровых двойников» для осуществления организационного, оперативно-технического и технологического управления процессами при выполнении учебных задач, с доступом пользователей в масштабе времени близком к реальному.

Для реализации данных подходов необходимо:
- разработать проект архитектуры и макета аппаратно-программного комплекса межвузовской цифровой научно-образовательной платформы для подготовки специалистов отрасли;
- разработать проект архитектуры распределенных центров подготовки специалистов;
- создать имитационную моделирующую виртуальную среду, построенной на основе технологий «цифровых двойников» на различных уровнях для осуществления технологического управления программно-аппаратными комплексами связи и автоматизации, создания и использования специального программного обеспечения обеспечивающих работу лабораторных комплексов кафедр, факультетов, полигонов и учебных центров, а также расчетно-моделирующих комплексов и информационно-расчетных задач обеспечивающих обучение специалистов;
- разработать и внедрить технологии мониторинга состояния инфотелекоммуникационных систем, систем управления оперативно-технической службой, администрирования сетевых служб, физических параметров линий связи, в том числе построенных на основе квантовых технологий, маршрутизацией и автоматизированным распределением сетевого трафика, контроля информационной безопасности;
- создать учебную автоматизированную систему организации информационного обмена для отработки задач оперативного управления подразделениями заказчика, на основе систем поддержки принятия решений, обработки больших данных о показателях и характеристиках инфотелекоммуникационной системы, имитационных моделирующих систем, учитывающих возможности и способы критических воздействующих факторов на инфраструктуру системы управления в целом, автоматизированных систем постановки задач и контроля их исполнения;
- создать автоматизированную систему контроля действий обучающихся, оценку полученных ими знаний и анализа проблемных вопросов обучения.

Базовая цифровая научно-образовательная платформа позволит обеспечить:
- создание «центра специальных игр», а также информационно-телекоммуникационной системы в едином кибернетическом пространстве;
- совершенствование процесса совместной подготовки специалистов заказчика, повышения квалификации профессорско-преподавательского состава ВУЗов, образовательной деятельности курсантов и адъюнктов, повышение эффективности их обучения на базе научно-технических достижений, новых методов моделирования, информационных технологий и современных способов организации и управления;
- овладение знаниями алгоритмов и навыков работы должностных лиц системы управления, при планировании и ведении повседневной деятельности, усвоению форм и способов применения информационных и телекоммуникационных технологий в управленческой деятельности, в том числе обеспечение необходимой информацией по поддержке

принятия решений, а также организации и обеспечении информационного обмена на всех уровнях управления отрасли;
- апробацию и реализацию своих научных разработок курсантами и адъюнктами, полученных при подготовке выпускных квалификационных и диссертационных работ;
- повышение качества групповых упражнений и практических занятий за счет реализации компетентностного подхода к обучению курсантов и адъюнктов за счет развития у обучаемых творческого и оперативного мышления в виртуальном моделируемом едином «игровом пространстве»;
- дистанционную подготовку специалистов по эксплуатации высокотехнологичных средств управления и автоматизации критической номенклатуры оборудования отрасли на единой методической основе разрабатываемых в ВУЗах интерактивных курсов;
- развитие научных и прикладных исследований, инновационных разработок, информационных, телекоммуникационных и проектных технологий и их внедрение в учебный процесс ВУЗа;
- создание условий для участия в проведении межвузовских многостепенных исследований на новом качественном уровне, с применением современных информационных и телекоммуникационных технологий и систем прикладного назначения, разрабатываемых в интересах функционирования подразделений работодателей.

Заключение

Таким образом, для повышения качества подготовки специалистов связи необходимо создание базовой цифровой научно-образовательной платформы ВУЗов. При этом, дальнейшие исследования предлагается направить на разработку и создание:

- аппаратно-программного комплекса цифровой научно-образовательной платформы, предназначенного для повышения эффективности проведения специальной и технической подготовки специалистов связи на основе распределенной учебно-материальной базы высших учебных заведений и распределенных учебных центров подготовки кадров для отрасли;
- аппаратно-программного комплекса цифровой лабораторно-испытательной платформы, предназначенного для выработки системотехнических решений, обоснования тактико-технических требований (основных технических требований), а также проверке требований, предъявляемых к разрабатываемым средствам и элементам управления в подразделениях отрасли.

Литература

1. Глотова М. И. Анализ опыта цифровой трансформации отечественного высшего образования // Современные проблемы науки и образования. – 2021. – № 1. – URL: https://science-education.ru/ru/article/view?id=30503 (дата обращения: 14.04.26). – DOI: 10.17513/spno.30503.
2. Маматова, Г. Д., Кучкаров Т. С. Актуальность концепции «Цифровой университет»: литературный обзор отечественных и зарубежных исследований. Информатика. Экономика. Управление – Informatics. Economics. Management. – № 3 (1). – С. 0101–0158. – DOI: 10.47813/2782-5280-2024-3-1-0101-0158.
3. Жуковская И. Е. Цифровые платформы – важный аспект цифровизации высшего образования / Открытое образование, 2022. – Т.26. – № 3. – С. 31–40.
4. Захарова О. И., Кадирова В. А. Семантический анализ в искусственном интеллекте // Технологии информационного общества. Сборник трудов конференции. Самара, 2023. – С. 268–270.
5. Белоусова М. Н., Алехина А. В., Здоровец С. О. Подготовка специалистов в высших учебных заведениях в реалиях цифровой трансформации // Современные проблемы науки и образования, 2023. – № 6. – URL: https://science education.ru/ru/article/view?id=33052 (дата обращения: 14.04.2026). – DOI: 10.17513/spno.33052.
6. Анахов С. В., Анахов Д. С. Цифровые платформы: аспекты развития в научно-образовательной сфере // Новые информационные технологии в образовании и науке, 2020. – Вып. 3. – С. 6–15.
7. Иванов В. Г., Григорьева К. М., Андриенко Е. П. Современные подходы по созданию единого образовательного пространства в целях подготовки специалистов связи с учетом развития учебно-тренировочных средств // «САПР и Графика», 2020. Спецвыпуск 3 «Проектирование объектов инфраструктуры». – С.37– 41. – URL: https://sapr.ru/article/26023.
8. Голубев С. В., Толстых А. В., Арьков Г. В. Подготовка специалистов связи в войсках на основе электронной информационной образовательной среды военного ВУЗа // Вестник Воронежского института МВД России, 2020. – № 4. – С. 39–47.

APPROACHES TO CREATING BASIC DIGITAL RESEARCH AND EDUCATIONAL PLATFORM IN HIGHER EDUCATIONAL INSTITUTIONS FOR TRAINING COMMUNICATION SPECIALISTS

Bogdanov A. V.[6], Kazakevich E. V.[7]

Keywords: *digital technologies, scientific and educational platform, software and hardware complexes, information and communication network, training of communication specialistst.*

Abstract

The purpose of the work: *substantiation of system engineering solutions in the formation of the image of the basic digital scientific and educational platform.*

Research method: *analysis of the infocommunication network of a military educational institution and software and synthesizing solutions for the technical basis for the creation of a network infrastructure and an information and computing cluster of the basic digital scientific and educational platform.*

Results of the study: *the substantiation of system-technical solutions in the formation of the appearance of the BCNOP, which provides the technical basis for the creation of hardware and software for the effective training of specialists of the signal troops for the operation of high-tech means and communication complexes, has been obtained.*

The successful implementation of a digital scientific and educational platform as an automated system should be based on the use of advanced technologies in the learning process, hybrid laboratories, promising intelligent and adaptive learning tools, the latest achievements in science and technology, and modern approaches in the field of neural technologies, artificial intelligence, and robotics. All of these factors have made it necessary and relevant to create a basic digital scientific and educational platform (BDSEP) to improve the quality of specialized and technical training for communication specialists

Practical usefulness: *the presented proposals and recommendations make it possible to form a promising image of a scientific and educational platform that ensures the improvement of the quality of the educational process.*

References

1. Glotova M. I. Analiz opyta cifrovoj transformacii otechestvennogo vysshego obrazovaniya // Sovremennye problemy nauki i obrazovaniya, 2021. – No 1. – URL: https://science-education.ru/ru/article/view?id=30503 (data obrashcheniya: 14.04.26). – DOI: https://doi.org/10.17513/spno.30503.
2. Mamatova, G. D., Kuchkarov T. S. Aktual'nost' koncepcii «Cifrovoj universitet»: literaturnyj obzor otechestvennyh i zarubezhnyh issledovanij. Informatika. Ehkonomika. Upravlenie – Informatics. Economics. Management. – No 3(1). – Pp. 0101–0158. – URL: https://doi.org/10.47813/2782-5280-2024-3-1-0101-0158.
3. Zhukovskaya I. E. Cifrovye platformy – vazhnyj aspekt cifrovizacii vysshego obrazovaniya / Otkrytoe obrazovanie, 2022. – T. 26. – No 3. – Pp. 31-40.
4. Zaharova O. I., Kadirova V. A. Semanticheskij analiz v iskusstvennom intellekte // Tehnologii informacionnogo obshchestva. Sbornik trudov konferencii. Samara, 2023. – Pp. 268–270.
5. Belousova M. N., Alehina A. V., Zdorovec S. O. Podgotovka specialistov v vysshih uchebnyh zavedeniyah v realiyah cifrovoj transformacii // Sovremennye problemy nauki i obrazovaniya, 2023. – No 6. – URL: https://science education.ru/ru/article/view?id=33052 (data obrashcheniya: 14.04.2026). – DOI: 10.17513/spno.33052.
6. Anahov S. V., Anahov D. S. Cifrovye platformy: aspekty razvitiya v nauchno-obrazovatel'noj sfere //Novye informacionnye tehnologii v obrazovanii i nauke, 2020. – Vyp.3. – Pp. 6–15.
7. Ivanov V. G., Grigor'eva K. M., Andrienko E. P. Sovremennye podhody po sozdaniyu edinogo obrazovatel'nogo prostranstva v celyah podgotovki specialistov svyazi s uchetom razvitiya uchebno-trenirovochnyh sredstv // «SAPR i Grafika», 2020. Specvypusk 3 «Proektirovanie ob'ektov infrastruktury». – Pp. 37–41. URL: https://sapr.ru/article/26023.
8. Golubev S. V., Tolstyh A. V., Ar'kov G. V. Podgotovka specialistov svyazi v vojskah na osnove ehlektronnoj informacionnoj obrazovatel'noj sredy voennogo VUZa // Vestnik Voronezhskogo instituta MVD Rossii, 2020. – No 4. – S. 39–47.

6 ***Alexander V. Bogdanov***, Ph.D. of Military Sciences, Associate Professor, Senior Researcher at the Research Center of the Military Academy of Communications named after Marshal of the Soviet Union S. M. Budyonny, St. Petersburg, Russia. E-mail: bog-saha@yandex.ru

7 ***Elena V. Kazakevich***, Ph.D. of Technical Sciences, Associate Professor, Head of the Department of Electrical Communications at the St. Petersburg State Transport University named after Emperor Alexander I, St. Petersburg, Russia. E-mail: kev-pgups@yandex.ru

TELECOMMUNICATIONS and COMMUNICATIONS

SCIENTIFIC PEER-REVIEWED JOURNAL
№ 4 (13) 2026
Published 6 times a year

The journal is registered by the Federal Service for Supervision of Communications, Information Technology and Mass Communications.

Registration Certificate
PI № FS77-88069 from 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 17/08/2026
The total circulation is 120 copies. The price is free

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

E-mail: editor.tis@yandex.ru. Tel.: +7 (985) 939-75-01

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

CONTENTS