ЦИФРОВАЯ ТРАНСФОРМАЦИЯ – НОВЫЕ ТЕХНОЛОГИИ ДЛЯ СЕТЕЙ СВЯЗИ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ. Часть II

Лукашев А. В.[1]

DOI:10.21681/3034-4050-2026-6-33-44

Ключевые слова: *опыт специальной военной операции, операционное пространство, архитектура телекоммуникационной сети, динамичная сетевая маршрутизация, бесшовный информационный обмен, гибридная архитектура вычислений, программно-определяемая сеть, маршрутизация по меткам, межсетевая интеграция сетей связи.*

Аннотация

Цель работы: *работа посвящена актуальной теме цифровой трансформации системы связи – научному обоснованию необходимости внедрения новых технологий построения сетей связи специального назначения, обеспечивающих устойчивый и безопасный информационный обмен в сложных условиях современных операций на основе приобретенного опыта боевого применения системы связи в специальной военной операции.*

Метод исследований: *анализ мирового опыта развития сетей связи, его теоретическое обобщение с целью выявления закономерностей развития сетевых технологий с целью научного обоснования способов цифровой трансформации отечественных сетей связи путем внедрения современных виртуальных и программно-определяемых сетевых технологий с встроенными механизмами безопасности и искусственного интеллекта.*

Результаты исследований: *в первой части статьи[2] было обосновано, что протокол IP-MLS является тупиковой ветвью развития сетевых технологий. В этой части показано, что невозможно единовременно отключить тысячи узлов и миллионы строк программного кода в действующих сетях связи. Разумный переход на следующий технологический уклад должен быть эволюционным, но и оперативным. Поэтому не только этот протокол, но и другие сетевые технологии будут использоваться в переходном периоде – они логично перейдут в статус унаследованных и будут интегрированы в сети высших уровней.*

С учетом положений Концепции цифровой трансформации ВС РФ[3], в статье предлагается именовать ТП Единой цифровой платформой ВС РФ (ЕЦП). Такой же подход следует распространить и на перспективные сети связи специального назначения (СССН), которые в ходе цифровой трансформации будут объединены в Интегрированную сеть связи (ИСС). При этом ИСС целесообразно масштабировать на все СССН страны.

Научная новизна: *предложено научно обоснованное определение единой цифровой платформы специального назначения;*

- *новые для отечественных сетей способы применения технологий виртуализации (NFV, SD-WAN и, программно-определяемых сетей (SDN);*
- *рекомендации органам военного управления по содержанию этапов построения единой цифровой платформы специального назначения, а также срокам создания единой цифровой платформы специального назначения;*
- *новые для отечественных сетей связи подходы к обеспечению безопасности на основе встроенных сетевых механизмов с применением элементов искусственного интеллекта и минимизации участия человека в управленческих процессах;*
- *впервые прорывная технология в области оптической связи – полые оптические световоды, представлены в качестве эффективной технологии обновления существующих волоконно-оптических систем, физические возможности которых к настоящему времени «выжаты» до теоретического предела.*

Введение. Обоснование выбора метода цифровой трансформации сетей связи специального назначения

Развитие информационно-коммуникационных технологий (ИКТ) в XXI веке характеризуется переходом от эволюционного совершенствования отдельных элементов сетей связи к фундаментальной цифровой трансформации всей архитектуры информационного пространства. Этот процесс, охватывающий как гражданские, так и специальные сети связи, подчиняется общим закономерностям технологических укладов, сформулированным в работах Н. Д. Кондратьева, К. Перес, Л. Фримена и развитым в современных исследованиях цифровой экономики [1, 2].

Мировой опыт демонстрирует, что каждый технологический уклад сопровождается не просто количественным ростом параметров сетей (пропускной способности, скорости передачи, надежности), но качественным изменением их архитектуры, принципов управления

1 ***Лукашев Анатолий Викторович***, кандидат военных наук, старший научный сотрудник научно-исследовательского центра Военной академии связи им. С. М. Буденного. Санкт-Петербург, Россия. E-mail: lukasheff@mail.ru

2 Лукашев А. В. Цифровая трансформация – новые технологии для сетей связи специального назначения. Часть I // Телекоммуникации и Связь. – 2026, № 5. – С. 50–58.

3 Концепция цифровой трансформации Вооруженных Сил Российской Федерации // Утверждена Министром обороны России.

и взаимодействия с пользователем. Переход от аналоговых систем связи к цифровым в 1970–1980-е годы, внедрение пакетной коммутации и протоколов семейства TCP/IP в 1990-е, распространение широкополосного доступа и мобильной связи третьего-четвертого поколений в 2000–2010-е – все эти этапы сопровождались не только техническими инновациями, но и глубокими организационными изменениями, перестройкой бизнес-моделей и трансформацией нормативно-правовой базы [3, 4].

Особый интерес представляет эволюция сетей связи специального назначения (СССН), которые исторически развивались по пути, отличному от гражданских телекоммуникационных сетей. Если коммерческие сети ориентировались на массовость, экономическую эффективность и совместимость с глобальной инфраструктурой Интернета, то СССН приоритизировали надежность, защищенность, автономность и гарантированное качество обслуживания в экстремальных условиях эксплуатации [5]. Однако в современных условиях, характеризующихся конвергенцией гражданских и военных технологий, ростом угроз кибербезопасности и необходимостью межведомственного взаимодействия, традиционная изолированность СССН становится не только неэффективной, но и рискованной [6].

Научное обоснование цифровой трансформации СССН опирается на несколько взаимосвязанных теоретических и технологических направлений. Во-первых, это концепция программно-конфигурируемых сетей (Software-Defined Networking, SDN) и виртуализации сетевых функций (Network Functions Virtualization, NFV), позволяющая гибко управлять ресурсами и адаптировать архитектуру сети к изменяющимся требованиям [7, 8]. Во-вторых, это развитие технологий облачных вычислений и граничных вычислений (edge computing), обеспечивающих распределенную обработку данных и снижение задержек [9]. В-третьих, это прогресс в области фотонных технологий, полупроводниковой электроники и квантовой криптографии, открывающих новые возможности для защиты информации и повышения пропускной способности [10, 11].

Ключевой проблемой, однако, остается не столько доступность отдельных технологий, сколько необходимость их интеграции в единую, согласованную архитектуру, учитывающую специфику СССН: требования к физической защите каналов связи, работу в условиях радиоэлектронной борьбы, необходимость автономного функционирования при нарушении связи с центральными узлами управления [12]. Решение этой проблемы требует не просто механического переноса гражданских технологий в специальную сферу, но их глубокой адаптации и научного переосмысления с учетом принципов информационной безопасности и национальной безопасности в целом [13].

Перспективный облик будущего единого информационного пространства, формируемого в результате цифровой трансформации СССН, предполагает создание гетерогенной, многоуровневой, адаптивной архитектуры, способной динамически перераспределять ресурсы между различными сегментами (гражданскими, ведомственными, специальными) в зависимости от текущих задач и угроз [14]. Такое пространство должно сочетать преимущества централизованного управления (для координации и оптимизации) с преимуществами распределенной архитектуры (для устойчивости и автономности), обеспечивая при этом сквозную защиту информации на всех уровнях – от физического до прикладного [15].

Цель настоящей статьи – систематизировать мировой опыт цифровой трансформации сетей связи, выявить общие закономерности развития ИКТ, сформулировать научные принципы адаптации этих закономерностей к специфике СССН и предложить концептуальный облик перспективной архитектуры единого информационного пространства.

Общие подходы к реформе сетей связи специального назначения

В целях обеспечения *устойчивого* функционирования системы связи, в ней должны быть внедрены современные сетевые *NFV* (виртуализации), *SDN* (программно-определяемые), *SD-WAN* (управление сетью через программные методы) технологии.

SDN (Software-Defined Networking): это архитектурный подход, при котором управляющая логика сети (*control plane*) отделяется от передачи данных (*data plane*), что позволяет централизованно управлять сетью с помощью программного обеспечения.

NFV (Network Functions Virtualization): это технология виртуализации сетевых функций (например, межсетевых экранов, балансировки нагрузки), которые ранее выполнялись на специализированном оборудовании, и теперь они работают как *виртуальные машины* (VM) или контейнеры на стандартных серверах [16]. В случае широкого внедрения виртуализации будем иметь *Виртуальную инфокоммуникационную платформу* (ВИП).

SD-WAN (Software-Defined Wide Area Network) – это технология управления корпоративной WAN-сетью через программные методы [17]. Суть технологии в построении *распределенных сетей*, которая состоит из маршрутизаторов и интеллектуальной системы управления (SD-WAN контроллера и оркестратора).

Ниже (табл. 3, 4) приведены основные преимущества и недостатки сетей SDN и NFV в сравнении. Наличие недостатков характерно для любых технологий и поставщики аппаратных и программных средств, как правило, стараются их скрыть, поэтому, упреждая данный фактор, читатель, если он потенциальный заказчик, может выработать подход к предлагаемым потенциальным подрядчиком решениям заранее, пользуясь представленной здесь (табл. 3).

Исходя из анализа потенциалов технологий, можно определить их применимость для СССН, имея ввиду не только существующие сети, но и предстоящую цифровую трансформацию.

Для центров обработки данных (ЦОДов), управления масштабными сетями, трафиком и виртуальными машинами в большей степени подходит технология SDN.

Для услуг доступа, функций ядра сети, Интернета вещей (*IoT*), 5G-ВН сетей, развертывания граничных виртуальных функций на периферии, граничных вычислений (*Edge computing*), в большей степени подходит технология NFV.

Поскольку цифровая трансформация систем информационного обмена осуществляется, главным образом, в целях *обеспечения полноты* сервисов и услуг, а также охвата множества разнородных сетей с различными технологиями, протоколами и криптосистемами, *оптимальным* следует считать *гибридный* подход, в котором функции будут распределены по указанным выше признакам.

Если традиционные сети жестко привязаны к аппаратному обеспечению, то синергия SDN и NFV позволяет адаптировать сетевую среду под запросы пользователей за считанные минуты.

Выбор между централизованным и децентрализованным управлением зависит от задач:

- для локальных сетей достаточно централизованного подхода,
- для провайдерских, 5G, IoT – выгоднее гибридный или децентрализованный подход.

Ниже представлен обобщенный автором вклад каждой из технологий в борьбе с деструктивными воздействиями в условиях боевого применения сетей связи (табл. 4).

Таким образом, ЕЦП, использующая комбинацию SDN и NFV, обеспечивает:

- высокую отказоустойчивость;
- быстрое восстановление после аварий;
- гибкость управления как сетью, так и сервисами;
- защиту от атак и физических повреждений.

Другим сетевым решением является сеть SD-WAN, в которой топологические компоненты могут быть сколь угодно разнесены друг от друга, главное, чтобы между ними была *связность*. С помощью системы управления можно построить *защищенные туннели* между всеми удаленными узлами, настроить политики безопасности и передачи данных по этим туннелям, а также *централизованно* контролировать работу всей сети.

Основной целью SD-WAN является *централизованное* управление сетью, упрощение

Таблица 3.

Достоинства и недостатки технологий SDN и NFV

Преимущества	
SDN	**NFV**
Централизованное управление всей сетью. Программируемость: возможность гибкой настройки сетевых политик. Динамическая маршрутизация трафика. Лучшая видимость и контроль за сетевыми потоками. Поддержка автоматизации и оркестровки	Снижение затрат на оборудование (вместо специализированных устройств – стандартные серверы). Быстрое развертывание новых сервисов. Масштабируемость – легко добавлять/удалять виртуальные функции. Независимость от вендора оборудования
Недостатки	
Высокая сложность внедрения и интеграции. Риск централизованного отказа (при отказе центрального контроллера возможна потеря управления всей сетью – нейтрализуется распределенным управлением сетью)	Накладные расходы на виртуализацию (производительность) могут быть ниже, чем у физических устройств. Сложности управления жизненным циклом

Таблица 4.

Вклад каждой технологии в борьбе с деструктивными воздействиями

Тип воздействия	Реагирование через SDN	Реагирование через NFV
Отказ оборудования	Перенаправление трафика на резервные пути	Перемещение сервиса на другой хост
Авария канала связи	Динамическая маршрутизация через другие узлы	нет
DDoS-атака	Блокировка трафика на уровне контроллера	Запуск виртуального сетевого экрана, защита от вторжений
Физическое разрушение	Перенастройка сети в целях обхода поврежденного узла	Миграция сервисов на удаленные серверы
Компрометация сервиса	нет	Запуск нового экземпляра сервиса

подключения удаленных узлов, использование разных типов подключений (*MPLS*, *LTE*, *Интернет и др.*), автоматическая маршрутизация трафика по оптимальным путям.

SD-WAN *абстрагирует* сеть от физического оборудования и позволяет ей работать на уровне программного обеспечения.

Одним из неотъемлемых атрибутов технологии SD-WAN является *сетевая безопасность*. Маршрутизатор SD-WAN сам по себе уже небольшой межсетевой экран, который позволяет в *реальном времени* проводить инспекцию трафика, распознавать используемые приложения и применять политики безопасности и маршрутизации в зависимости от типа приложения. Контроллер SD-WAN при этом позволяет поддерживать целостность политик безопасности для всей сети, максимально быстро вводить новые правила передачи трафика, а также показывать статистику загрузки и изменения качественных параметров каналов связи в реальном времени.

Для обеспечения безопасности в сетях связи предлагаются инструменты модели *Zero Trust*[4] (нулевого доверия), которая создана для предотвращения несанкционированного доступа к данным и службам благодаря детальному и точному контролю доступа. Состав и функциональность модели подробно описаны в текущих научно-исследовательских работах, ведущихся в Военной академии связи.

Предлагаемое решение обеспечивает выполнение всех условий, в которых сети ВС РФ и силовых ведомств должны устойчиво функционировать в мирное и военное время, и является *оптимальным*, основанным на ранее описанных технологиях.

Владелец сети получает одновременно несколько преимуществ, связанных не только с безопасностью, но и экономической эффективностью:

- снижение стоимости организации распределенной сети – можно комбинировать различные каналы связи для повышения скорости и надежности информационного обмена;
- централизованное управление сетью, высокая степень видимости и широкие возможности анализа;
- сложность администрирования и применения политик значительно снижается благодаря централизованному интерфейсу управления.

Кроме того, внедрение SD-WAN позволит *ускорить* подключение новых узлов. Каждый маршрутизатор SD-WAN поддерживает функцию *автоматического* подключения к контроллеру и получения конфигурации устройства в сети SD-WAN, для чего достаточно любым способом подключить его к каналам связи, например, установить *SIM-карту*.

Таким образом, основным преимуществом централизованных контроллеров является возможность в реальном времени *контролировать качество* всех каналов связи и направлять трафик приложений по маршрутам с *наименьшей задержкой* и с *минимальными* потерями пакетов.

Эти функции потенциально позволяют заказчикам *отказаться* от аренды MPLS-каналов сетей связи общего пользования (ССОП) и перейти на менее дорогие каналы, например, Интернета, в том числе LTE и существующие собственные стационарные и полевые линии связи. К тому же «умные» SD-WAN-маршрутизаторы позволяют использовать одновременно несколько каналов связи, поэтому вместо MPLS-канала можно использовать несколько сетевых или LTE-подключений и агрегировать их пропускную способность.

Внедрение сетевой технологии SD-WAN в комплексе с сетью SDN позволяет получить дополнительные преимущества (табл. 5).

4 Касперская Н.: Что такое SD-WAN и нужен ли он вашей сети? – URL: https://www.kaspersky.ru/blog/what-is-sd-wan/34943 (28.07.2025 г.).

Таблица 5.

Дополнительные преимущества при внедрении SD-WAN

Преимущество	Обоснование
Быстрое развертывание	Свойство устройства Zero-Touch Provisioning (ZTP): «подключил – работает» (самонастройка)
Гибкость маршрутизации	Маршрутизация послойно по типу трафика: голос, видео, данные – можно применять разные политики
Контроль над инфраструктурой	Заказчик владеет политиками, правилами, данными
Виртуализация	Можно развернуть как полностью в облаке, так и смешанно, с использованием собственных сетей связи
Интеграция с NFV	Легко сочетается с виртуальными SBC, медиасерверами и другими функциями

Таким образом, процесс цифровой трансформации объективно должен включать в себя внедрение динамических технологий в СССН, реализуемых вышеперечисленными видами сетей.

Практическая реализация цифровой трансформации сетей связи специального назначения

С учетом внешних условий, в которых необходимо осуществить цифровую трансформацию, а также необходимости оптимизации экономических затрат на реализацию, требуется обосновать концептуальные положения в части распределения технологических ресурсов.

Один из вариантов состоит в *аренде* темных оптических волокон, средств каналообразования и коммутации в сетях, принадлежащих ПАО «Ростелеком». Обозначим сумму общих затрат как $C_{\text{аренд}}$ и поставим задачу рассчитать ее величину в соотношении с условием по срокам реализации – $T_{\text{постр}}$.

Другой путь – выкуп темных волокон, установка на узлах коммутации ПАО «Ростелеком» собственного оборудования, организация и всестороннее обеспечение эксплуатации. Обозначим затраты на реализацию как $C_{\text{выкуп}}$ в соотношении с условиями по срокам реализации. Отметим, что организация эксплуатации потребует подготовки персонала по обслуживанию и эксплуатации оборудования с расширением штатов войск связи, затраты на материально-техническое обеспечение и эксплуатационное обслуживание, ремонт, поддержку программного обеспечения, обеспечение кибернетической и физической безопасности в *условиях переоборудования узлов*.

В обоих вариантах:

а) должны выполняться спецтребования;
б) могут достраиваться стационарные волоконно-оптические линии связи (ВОЛС);
в) сроки построения ЕЦП должны соответствовать требованиям заказчика;
г) затраты на построение ЕЦП должны отвечать возможностям государственного бюджета, выделенного на построение и последующую эксплуатацию платформы силовых ведомств в общем составе ИСС в интересах военного управления.

Задача выбора пути построения ЕЦП определяется расчетом соотношения:

$$C_{\text{аренд}} \mid T_{\text{постр}} \; vs \; C_{\text{выкуп}} \mid T_{\text{постр}}, \qquad (1)$$

В процессе цифровой трансформации безусловно, возникнут трудности поскольку предстоит сложная интеграция сетей связи, принадлежащих различным ведомствам. Сумма основных проблем представлена в ниже (табл. 6).

Существует два подхода к решению перечисленных проблем интеграции разнородных систем – создание метаконтроллера над двумя и более системами (упрощенный подход) и полная интеграция – полноценный подход на долгие годы.

Для реализации первого подхода – с метаконтроллером, потребуется создать единое ИИ-ядро над гетерогенными системами. Искусственный интеллект, при его внедрении, повышает эффективность автоматизации, осуществляя:

- прогнозирование сбоев по метрикам;
- оптимизацию маршрутов в реальном времени;
- обнаружение аномалий в трафике;
- реализует политики самонастройки и самовосстановления, *QoS*.

Таким образом, выше рассмотрены следующие основные вопросы цифровой трансформации Вооруженных Сил Российской Федерации в полном соответствии с Концепцией цифровой трансформации ВС РФ:

- научное обоснование метода создания интегрированной сети связи с созданием

Таблица 6.

Основные технологические проблемы интеграции

Проблема	Причина	Решение
Разные форматы представления данных	Разные ведомства, разные стандарты	Преобразование данных в единый формат
Разные протоколы	Например, одна система использует OPC UA, другая – SNMP	Адаптеры протоколов (API Gateway)
Разные частоты опроса	Одна система может обновляться каждые 5 секунд, другая – раз в минуту	Интерполяция / экстраполяция
Разделенные права доступа	Разные ведомства – разные уровни доступа	*RBAC*[13] *+ Zero Trust Networking*
Отсутствие единого понимания контекста	Каждая система «видит» только «свою» часть	Объединение данных в едином контексте
Разнородность сетевого оборудования	Состав арендуемого оборудования разнороден	Унификация оборудования
Отсутствие в штатах войск связи специалистов по настройке сетей связи на различных видах протоколов и виртуализации	Отсутствие учебной программы сетевой настройки различных видов сетей в военных вузах	Обновление учебных программ военных вузов

и внедрением Единой цифровой платформы ВС РФ;

- рассмотрены преимущества технологий SDN и NFV в аспекте перехода к динамически маршрутизируемым сетям связи и даны рекомендации по их рациональному применению;
- даны рекомендации по практической реализации цифровой трансформации на обобщенном сетевом уровне;
- рассмотрены основные проблемы, которые могут возникнуть при реализации цифровой трансформации и предложены решения данных проблем.

Переход на новые системы криптографической защиты

20 марта 2025 // 13:15 UTC Национальный центр кибербезопасности Великобритании (NCSC) запустил официальный обратный отсчет времени наступления эры постквантовой криптографии (PQC), заявив, что у организаций есть *десять* лет, чтобы мигрировать в более безопасное будущее[5]. Руководство определяет *три ключевые вехи*, о которых, по утверждению NCSC, организации должны знать, поскольку квантовые компьютеры, воспринимаемые как следующее крупное технологическое изменение, но все еще находящиеся на ранней стадии разработки, будут представлять угрозу для текущих стандартов шифрования.

5 Sahara D., NCSC.gov.uk: Великобритания опубликовала план перехода на криптографию, устойчивую к квантовым атакам, к 2035 году // – URL: https://share.google/ZjnJi2lHGoASE2Zs.

Первая произойдет всего через *три года*: к 2028 г. организациям необходимо определить свои *цели по миграции PQC*, точно определить системы, которые необходимо модернизировать, и разработать первоначальный план для этого перехода.

К 2031 году должны быть завершены наиболее *приоритетные* миграции PQC, а первоначальный план, принятый на три года раньше, должен быть уточнен и показан более четкий путь к полной устойчивости PQC.

К 2035 году полная миграция PQC должна быть *завершена* во всех системах, продуктах и услугах.

«Действия, описанные при планировании миграции, являются существенными и имеют решающее значение для снижения кибернетических рисков».

«*Миграция произойдет по всему миру. Избежать миграции PQC не удастся, поэтому подготовка и планирование сейчас будут означать, что вы сможете безопасно и упорядоченно мигрировать*» (там же).

Основным средством снижения риска является переход на постквантовую криптографию (PQC) – криптографию, основанную на математических задачах, которые квантовые компьютеры не могут эффективно решать.

С оценкой Национального центра кибербезопасности Великобритании автор настоящей статьи «согласился» задолго до запуска «обратного отсчета времени наступления постквантовой эры». В работе (ссылка [3] в Части I), опубликованной

в 2024 г., сроки наступления эры господства квантовых компьютеров указаны примерно такие же, как и британским центром.

Между тем, 2026 г. вносит еще более жесткие факторы влияния на необходимость цифровой трансформации инфокоммуникационных сетей и систем. Это – экспоненциальное развитие систем искусственного интеллекта, который стал критической угрозой для информационной безопасности. Данное направление в статье не рассматривается, поскольку требует отдельной публикации.

Полые оптические волноводы – новый прорыв в технологиях связи. Влияние на планы развития системы связи

Полые оптические волноводы или световоды, далее ПОС – это один из важнейших и наиболее перспективных инструментов современной фотоники [18].

Если фотоника – это наука и технология управления световыми сигналами (аналогично электронике, но с использованием фотонов вместо электронов), то полые волноводы служат уникальной «транспортной системой» для этих фотонов. Их главное отличие от классических кварцевых световодов заключается в том, что свет распространяется не в кварцевом ядре волокна, а в воздушной (газовой) или вакуумной сердцевине, окруженной отражающей оболочкой специальной конструкции. Здесь важно заметить, что мы переходим в масштабы микромира, ведь такой световод тоньше человеческого волоса, а его внутренний диаметр может составлять 25–35 мкм.

Внутри такового световода создаются капилляры, крепящиеся к внутренней поверхности ПОС. Капилляры могут иметь различную форму и структуру и предназначены для создания отрицательной кривизны внутренней поверхности волновода. За счет этого фотонный поток распространяется внутри ПОС не рассеиваясь, т.е., «организовано» смещаясь к центру волокна. Принцип структуры ПОС в наиболее общем виде показан на рисунке 1.

Ключевые аспекты соотношения фотоники и полых волноводов состоят в следующих положениях.

1. Преодоление фундаментальных лимитов стандартной фотоники

Классические волоконные световоды (из монолитного кварцевого стекла) к настоящему времени достигли физического предела своего совершенствования, перейдя в статус *устаревающих* систем. ПОС позволяют фотонике обойти этот барьер за счет своих свойств:

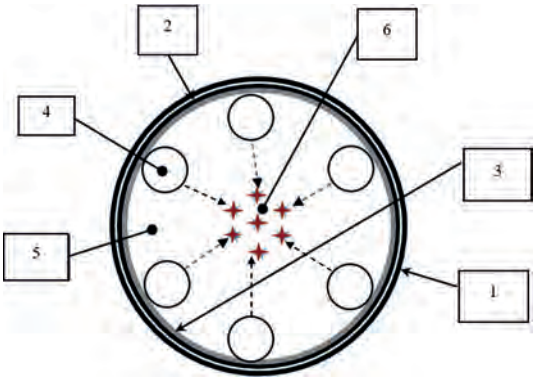

Рис 1. Общий структурный принцип полого оптического волокна
1 – внешняя защитная полимерная оболочка; 2 – внутренняя оболочка; 3 – внутренняя фотонно-кристаллическая оболочка; 4 – капилляры, создающие отрицательную кривизну внутреннего пространства; 5 – промежуток между капиллярами должен быть меньше длины волны сигнала; 6 – условное обозначение фотонного потока внутри полой оптической структуры.

- сверхвысокой лучевой стойкости – в ПОС свет распространяется по воздуху, что позволяет передавать киловаттные лазерные мощности без повреждения самого волокна;
- фотоника полых волноводов позволяет передавать данные со скоростью на 45 % выше, чем в классической ВОЛС – максимально близкой к абсолютной скорости света (с);
- рекордно низкая нелинейность: стеклянное ядро ВОЛС искажает форму мощных световых импульсов. В ПОС воздушная среда сводит эти искажения практически к нулю, сохраняя чистоту сигнала.

2. Расширение спектрального диапазона фотоники

Стандартный кварц поглощает ультрафиолетовое и среднее инфракрасное излучение. Полые волноводы позволяют фотонным устройствам эффективно работать в этих «трудных» диапазонах (S и L).

3. Области применения ПОС в СССН

- сверхскоростной интернет и сети 5G/6G: использование полых фотонно-кристаллических волокон (*HCF – Hollow Core Fiber*) снижает задержку данных (*latency*) в линиях связи на 31 %;
- лазерная медицина и промышленность: гибкая доставка мощного излучения CO_2; использование эрбиевых лазеров для резки металлов или хирургических операций;
- квантовая фотоника: передача одиночных фотонов и распределение запутанных состояний без искажений и потерь, вызванных

материалом стекла в системах квантового распределения ключа;
- системы межбанковского клиринга и высокочастотного трейдинга (*HFT – High Frequency Trading*) [19].

В сфере управления системами специального назначения ПОС должны разрабатываться *уже сейчас* с пересмотром программ научных исследований, учебных программ военных вузов, а также профильных разделов Госпрограммы вооружений, поскольку ПОС обладают *уникальными* свойствами, основными из которых являются:

- *абсолютная* защита от взлома и перехвата на *уровне физических законов* – здесь *нет* математических алгоритмов и специального программного обеспечения, которое можно взломать с помощью ИИ-агентов (уже сейчас) или посредством квантовых компьютеров (в обозримом будущем);
- сверхнизкая задержка сигнала (*low latency*) за счет скорости распространения сигнала в ПОС, что критически важно для специальных систем управления;
- увеличенный шаг между промежуточными узлами (усиления/регенерации) до 300 – 500 – 1000 км[6], что снижает стоимость линий оптической связи на *порядок*, позволяет отказаться от «доверенных» узлов переприема квантового и классического засекреченного каналов, что критически важно для безопасности и оптимизации штатов войск связи;
  увеличенный срок службы линий и промежуточных узлов, не требующих регулярного обслуживания, до 25 и более лет;
- протяженные линии не требуют тысяч датчиков для контроля – место повреждения линии определяется практически мгновенно с точностью до нескольких метров, а ремонт волокна занимает около 3-х часов после прибытия ремонтной бригады;
- идеально подходят для создания систем квантового распределения ключей (*QKD*), квантового интернета и межконтинентального квантового компьютера, например стран БРИКС, ресурсы которого могут использоваться в интересах национальных систем связи и управления специального назначения.

Следует отметить, что ПОС активно разрабатываются крупнейшими западными гигантами, такими как SubCom, ASN, Nokia. В фотонную гонку включилась и компания Microsoft, купив передового производителя ПОС британскую компанию Lumenisity. Компания планирует осуществлять информационный обмен между своими ЦОД со сверхнизкими задержками, что позволит повысить производительность вычислений за счет интеграции мощностей суперкомпьютеров[7].

Недавно компания поставила рекорд в экспериментальной передаче сигнала на расстояние 301,7 км *без промежуточного усиления* с суммарной скоростью 25,6 Тбит/с. Рекорд достигнут благодаря изобретению ПОС с геометрией *DNANF* (*Double-Nested Anti-Resonant Nodeless Fiber*) с рекордно низким затуханием 0,091 дБ/км на стандартной длине волны 1550 нм. Для передачи сигнала, кроме стандартного С-диапазона, были задействованы диапазоны S (1460–1530 нм) и L (1565–1625 нм), при этом общая полоса пропускания составила 66 ТГц [20].

Поскольку компания Майкрософт в структуре узлов ПОС *применяет существующее* оборудование, то разработчики считают свои решения наиболее целесообразными и эффективными, планируя в перспективе увеличить безусилительные участки до 400 км за счет совершенствования геометрии своего волокна DNANF.

В этой связи возьмем на себя смелость изложить альтернативное мнение. Ответим «Да», если строить ПОС на территории США и европейских стран НАТО. Но для российских реалий, также, как и для стран БРИКС, это – *стратегическая ловушка*. Экосистема *Microsoft* плюс *Corning*, плюс западные *DSP*-чипы (*Digital Signal Processing*) создает полную зависимость от санкционного регулирования. Поэтому мы не можем строить критическую инфраструктуру РФ/КНР/Индии на «черном ящике», который *могут отключить* очередным обновлением прошивки. Наша архитектура должна быть открыта для интеграции с компонентами китайских производителей *YOFC*, *Huawei*, но и, в первую очередь, с отечественными разработками. Мы заплатим немного больше за кастомизацию, но «купим» *технологический суверенитет*. Это главный аргумент.

Другой аргумент лежит в технической плоскости – на оконечных и промежуточных узлах, если они потребуются при использовании линий большой протяженности, применяются специализированные микропроцессоры DSP, в которых оптико-электронное преобразование вносит задержку в 100 мкс.

И это не один его недостаток, данная архитектура *неприменима* в системах квантового распределения ключа (КРК) – на больших расстояниях, требующих усиления, она разрушает квантовые состояния одиночных фотонов при

6 Шаг между узлами в 500–1000 км доступен теоретически для газонаполненных ПОС и требует экспериментального подтверждения.

7 Карасев С. : Servernews.ru // Microsoft купила разработчика необычного волокна Lumenisity. – URL: https://servernews/1149024

оптико-электронном преобразовании. В этой связи, выполнение поручения Президента Российской Федерации о доведении квантовых систем до Дальневосточного региона[8] на данной архитектуре окажется невозможным.

В свою очередь, существующая практика строительства квантовых линий с переприемными пунктами – «доверенными узлами», устарела и в развитых странах не применяется уже много лет в силу критических трудностей в обеспечении безопасности и запредельной стоимости по сравнению с альтернативными протоколами КРК.

Для отечественных масштабов подходят другие решения, в частности, диссипативные солитоны в качестве носителей информации, нелинейная газовая среда внутри ПОС, параметры которой управляются в реальном времени нейросетью и усилительные пункты без традиционного высоковольтного электроснабжения, забирающего до 40 % стоимости кабеля. Такие системы уже созданы в России и готовы к внедрению.

Следует отметить, что в случае продолжения простоя в сфере внедрения полых оптических структур в стационарные линии связи специального и гражданского назначения, через 5–7 лет вместо цифрового суверенитета мы снова окажемся в цифровом рабстве у западных стран. Но это уже будет рабство с потерей самостоятельной государственности.

В заключение ниже представлена пятиуровневая модель эволюционной цифровой трансформации гетерогенных сетей связи – от унаследованных (существующих) к фотонно-семантическим (рис. 2).

8 – URL: https://www.kremlin.ru / Пленарное заседание XI Восточного экономического форума. – 03.09.2026.

Заключение

Подводя итог изложенному, следует отметить, что не все аспекты цифровой трансформации были представлены, это невозможно в рамках журнальной статьи. В синергии с утвержденной Министром обороны Российской Федерации Концепции цифровой трансформации ВС РФ автором углублены и раскрыты базовые положения предстоящей трансформации. Здесь следует подчеркнуть, что содержание Концепции полномасштабно отображает мировые тренды развития инфокоммуникационных систем, поскольку в ней затронуты самые передовые направления: утверждены положения о важности исследований в области применения искусственного интеллекта; в аспекте обеспечения информационной безопасности упомянута роль *доверенной программно-аппаратной среды* и поставлен ряд задач цифровой трансформации.

Впервые реформы будут осуществляться под управлением Координационного совета по цифровой трансформации ВС РФ, а сама цифровая трансформация охватит не только системы, средства и органы управления связи, но и Вооруженные Силы в целом. Поэтому и статус руководителя цифровой трансформации повышен до уровня заместителя Министра обороны РФ.

Возвращаясь к подведению итогов статьи, наметим направления дальнейших исследований. В первую очередь к ним следует отнести очень сложные вопросы применения искусственного интеллекта, в том числе больших языковых моделей (LLM), технологии встроенной сетевой безопасности в комплексе с решениями по созданию *доверенных информационных*

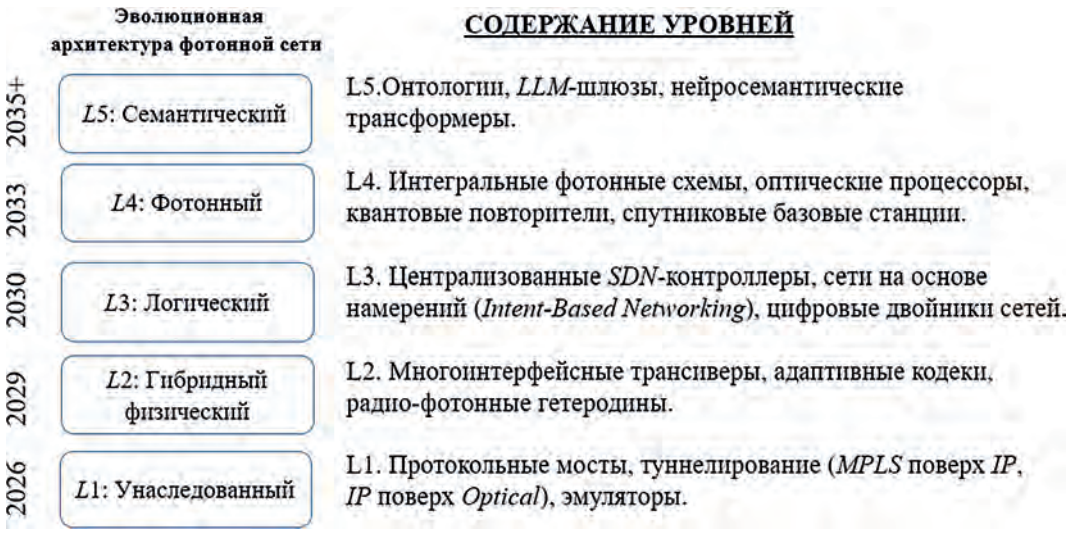

Рис.2. Эволюционная архитектура цифровой трансформации сетей связи специального назначения

пространств, разработку средств и систем управления робототехническими комплексами.

Важное внимание следует уделить многоуровневым сетям космической связи, *интегрированными* с сетями радиосвязи. Следует также уделить внимание повышению уровня обеспечения связью мобильных абонентов, а также фотонике и *полым оптическим структурам* – именно здесь находится становой хребет *цифрового суверенитета* не только России, но и стран БРИКС, поэтому целесообразно проявить с инициативу совместного освоения данного направления. Ведь в рамках сотрудничества могут быть оперативно решены многие научно-практические задачи цифровой трансформации в интересах СССН.

В заключение несколько слов о наболевшем. В определенной степени успех цифровой трансформации, принятые решения в области информационной безопасности, как в самом процессе реформ, так и в результатах, будут зависеть от комплекса мер безопасности. В этой связи остановлюсь на одном из аспектов, влияющих на условия, в которых придется работать. Ниже приводятся ряд *сентенций* Президента России В. В. Путина по вопросу комплементарных отношений между рабочими и регуляторными органами, которые в текущий момент *не должны затруднять* исполнение планов цифровой трансформации.

I. Конференция AI Journey «О развитии искусственного интеллекта»[9]

«Технологии ИИ не должны быть скованы чрезмерными запретами… Регуляторные ограничения и требования безопасности не должны *тормозить* технологический прогресс, иначе страна отстанет от мировых лидеров».

II. В контексте цифровизации бизнеса[10]**…**

Цифровая среда должна быть защищенной, но требования информационной безопасности должны помогать развитию экономики, а не ставиться для нее «*стоп-краном*»…

III. О генетических технологиях и инновациях[11]

Президент России указал Правительству РФ «своевременно снимать ограничения для работы… нужно находить *гибкий баланс* между защитой интересов общества и *свободой* научного поиска, чтобы бюрократия и безопасность не превращались в *непреодолимый барьер* для инноваций».

Будем надеяться, что будем услышаны. Ведь на пути цифровой трансформации систем информационной безопасности будут очевидные трудности – предстоит «интеллектуализировать» данные системы, а искусственному интеллекту при этом *не следует доверять безоглядно*. Это – с одной стороны. С другой стороны, без него «никак» – кибернетическая война ведется в недоступном человеку *миллисекундном* масштабе времени. Поэтому решения следует искать в компромиссе между рисками и технологической необходимостью внедрения новых систем встроенной сетевой безопасности на базе интеллектуальных систем. А все вместе взятое требует свободного творческого поиска *ранее неизвестных* идей, подходов и решений, недоступного в устаревшей системе ограничений и запретов.

Всего лишь один пример: Пентагон официально открыл доступ своему персоналу (более 3 млн чел.) к большим языковым моделям через специализированную внутреннюю платформу *GenAI.mil*[12].

На практике это означает, что аналитики, обрабатывающие большие данные, готовящие управленческие решения командованию будут работать в *тысячи* раз быстрее своих зарубежных коллег, не имеющих возможностей такого доступа.

9 Сетевой ресурс. – URL: https://www/RusEmbassySousAfrica/posts/-president-of-russia-vladimir-putin-speaking-at-the-future-technologies-forumih/12550573471544.

10 Сетевой ресурс. – URL: https://aa.com/eneurasia/putin-says-russia-intends-to-create-technological-with-other-countries/3937663.

11 Сетевое издание «Коммерсант», Россия. – URL: https://kommersant.ru/doc/9599.

12 Сетевой ресурс. – News channel underwritten by NORTRTOP GRUMMAN / Artifical Intelligens &Autonomy / A NEW ERA IN DEFENS: Pentagon rolls out GenAI platform to all personnel, using Google's Gemini. – URL: https://share.google/FMEy2NCBofmhVerj8.

Литература

1. Perez, C. Technological Revolutions and Financial Capital: The Dynamics of Bubbles and Golden Ages / C. Perez. – Cheltenham: Edward Elgar Publishing, 2002. – 224 p. – DOI 10.4337/9781781005323.
2. Freeman, C. As Time Goes By: From the Industrial Revolutions to the Information Revolution / C. Freeman, F. Louçã. – Oxford: Oxford University Press, 2001. – 424 p. – ISBN 978-0-19-924107-1.
3. Castells, M. The Rise of the Network Society / M. Castells. – 2nd ed., with a new preface. – Chichester: Wiley-Blackwell, 2009. – 656 p. – ISBN 978-1-405-19686-4.
4. Mansell, R. Imagining the Internet: Communication, Innovation, and Governance / R. Mansell. – Oxford: Oxford University Press, 2012. – 296 p. – ISBN 978-0-19-969704-5. – DOI 10.1093/acprof:oso/9780199697045.001.0001.
5. Resilience and Survivability in Communication Networks: Strategies, Principles, and Survey of Disciplines / J. P. G. Sterbenz, D. Hutchison, E. K. Çetinkaya [и др.] // Computer Networks. – 2010. – Vol. 54, № 8. – P. 1245–1265. – DOI 10.1016/j.comnet.2010.03.005.
6. Alberts, C. J. Managing Information Security Risks: The OCTAVE Approach / C. J. Alberts, A. J. Dorofee. – Boston: Addison-Wesley, 2003. – 471 p. – ISBN 978-0-321-11886-8.

7. OpenFlow: Enabling Innovation in Campus Networks / N. McKeown, T. Anderson, H. Balakrishnan [и др.] // ACM SIGCOMM Computer Communication Review. – 2008. – Vol. 38, № 2. – Pp. 69–74. – DOI 10.1145/1355734.1355746.
8. Han, B., Gopalakrishnan, V., Ji, L., Lee, S. Network Function Virtualization: Challenges and Opportunities for Innovations / B. Han, V. Gopalakrishnan, L. Ji, S. Lee // IEEE Communications Magazine. – 2015. – Vol. 53, № 2. – Pp. 90–97. – DOI 10.1109/MCOM.2015.7045396.
9. Shi, W., Cao, J., Zhang, Q., Li, Y., Xu, L. Edge Computing: Vision and Challenges / W. Shi, J. Cao, Q. Zhang, Y. Li, L. Xu // IEEE Internet of Things Journal. – 2016. – Vol. 3, № 5. – Pp. 637–646. – DOI 10.1109/JIOT.2016.2579198.
10. Roelkens, G., Abassi, A., Cardile, P. [и др.] III–V-on-Silicon Photonic Devices for Optical Communication and Sensing / G. Roelkens, A. Abassi, P. Cardile [и др.] // Photonics. – 2015. – Vol. 2, № 3. – Pp. 969–1004. – DOI 10.3390/photonics2030969.
11. Gisin, N., Thew, R. Quantum Communication / N. Gisin, R. Thew // Nature Photonics. – 2007. – Vol. 1, № 3. – Pp. 165–171. – DOI 10.1038/nphoton.2007.22.
12. Rowe, N. C. Introduction to Cyberdeception / N. C. Rowe, J. Rrushi. – Cham: Springer, 2016. – XIV, 334 p. – ISBN 978-3-319-41185-9. – DOI 10.1007/978-3-319-41187-3.
13. Schneier, B. Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World / B. Schneier. – New York: W. W. Norton & Company, 2015. – 400 p. – ISBN 978-0-393-24481-6.
14. Clark, D. D., Wroclawski, J., Sollins, K. R., Braden, R. Tussle in Cyberspace: Defining Tomorrow's Internet / D. D. Clark, J. Wroclawski, K. R. Sollins, R. Braden // IEEE/ACM Transactions on Networking. – 2005. – Vol. 13, № 3. – Pp. 469–478. – DOI 10.1109/TNET.2005.850224.
15. Anderson, R. Security Engineering: A Guide to Building Dependable Distributed Systems / R. Anderson. – 2nd ed. – Indianapolis: 3rd ed. – Indianapolis: Wiley, 2020. – 1232 p. – ISBN 978-1-119-64278-7. – DOI 10.1002/9781119644682.
16. A Comprehensive Survey of Network Function Virtualization / B. Yi, X. Wang, K. Li [и др.] // Computer Networks. – 2018. – Vol. 133. – Pp. 212–262. – DOI 10.1016/j.comnet.2018.01.021.
17. Fu, C., Wang, B., Wang, W. Software-Defined Wide Area Networks (SD-WANs): A Survey / C. Fu, B. Wang, W. Wang // Electronics. – 2024. – Vol. 13, № 15. – Article 3011. – DOI 10.3390/electronics13153011.
18. Прямиков, А. Д. Полые световоды: современное состояние и перспективы развития / А. Д. Прямиков, А. В. Гладышев, А. Ф. Косолапов, И. А. Буфетов // Успехи физических наук. – 2024. – Т. 194, № 2. – С. 138–168. – DOI 10.3367/UFNr.2023.12.039616.
19. Virgilio, G. P. M. High-frequency Trading: A Literature Review / G. P. M. Virgilio // Financial Markets and Portfolio Management. – 2019. – Vol. 33, № 2. – P. 183–208. – URL: (дата обращения: 01.11.2026). – DOI 10.1007/s11408-019-00331-6.
20. Russell, P. St. J. Invited Commentary: Hollow Core Glass Fibre – The Perfect Pipe for Light / P. St. J. Russell // eLight. – 2025. – Vol. 5. – Article 4. – DOI 10.1186/s43593-025-00086-w.

DIGITAL TRANSFORMATION – NEW TECHNOLOGIES FOR SPECIAL-PURPOSE COMMUNICATION NETWORKS. Part II

Lukashev A. V.[13]

Keywords: *experience of a special military operation, operational space, telecommunications network architecture, dynamic network routing, seamless information exchange, hybrid computing architecture, software-defined networking, label routing, internetwork integration of communication networks.*

Abstract

The purpose of the work: *the work is devoted to the topical topic of digital transformation of the communication system – the scientific substantiation of the need to introduce new technologies for building special-purpose communication networks that provide stable and secure information exchange in the difficult conditions of modern operations based on the acquired experience of combat use of the communication system in a special military operation.*

Research method: *analysis of the world experience in the development of communication networks, its theoretical generalization in order to identify the patterns of development of network technologies in order to scientifically substantiate the methods of digital transformation of domestic communication networks through the introduction of modern virtual and software-defined network technologies with built-in security and artificial intelligence mechanisms*

Research results: *In the first part of the article*[14]*, it was substantiated that the IP-MLS protocol is a dead-end branch of network technology development. In this part, it is shown that it is impossible to simultaneously disable thousands of nodes and millions of lines of program code in existing communication networks. A reasonable transition to the next technological mode should be evolutionary, but also operational. Therefore, not only this protocol, but also other network technologies will be used in the transition period – they will logically move into the status of inherited and will be integrated into higher-level networks.*

13 ***Anatoly V. Lukashev***, Ph.D. of Military Sciences, Senior Research Officer, Military Academy of Communications named after S. M. Budyonny. Saint-Petersburg, Russia. E-mail: lukasheff@mail.ru

14 Lukashev A. V. Digital Transformation – New Technologies for Special Purpose Communication Networks. Part I // Telecommunications and Communications. – 2026. – No. 5.– Pp. 50–58.

Taking into account the provisions of the Concept of Digital Transformation of the Armed Forces of the Russian Federation[15], the article proposes to call the TP the Unified Digital Platform of the Armed Forces of the Russian Federation (UDS). The same approach should be extended to promising special-purpose communication networks (SSNS), which in the course of digital transformation will be combined into the Integrated Communication Network (ISS).

Scientific novelty: *a scientifically based definition of a single special-purpose digital platform is proposed;*

- *new ways of using virtualization technologies for domestic networks (NFV, SD-WAN and software-defined networks (SDN);*
- *recommendations to military authorities on the content of the stages of building a single special-purpose digital platform, as well as the timing of the creation of a unified special-purpose digital platform;*
- *new approaches to ensuring security for domestic communication networks based on built-in network mechanisms using elements of artificial intelligence and minimizing human participation in management processes;*
- *For the first time, a breakthrough technology in the field of optical communication – hollow optical light guides – is presented as an effective technology for updating existing fiber-optic systems, the physical capabilities of which have now been «squeezed out» to the theoretical limit.*

References

1. Perez, C. Technological Revolutions and Financial Capital: The Dynamics of Bubbles and Golden Ages / C. Perez. – Cheltenham: Edward Elgar Publishing, 2002. – 224 p. – DOI 10.4337/9781781005323.
2. Freeman, C. As Time Goes By: From the Industrial Revolutions to the Information Revolution / C. Freeman, F. Louçã. – Oxford: Oxford University Press, 2001. – 424 p. – ISBN 978-0-19-924107-1.
3. Castells, M. The Rise of the Network Society / M. Castells. – 2nd ed., with a new preface. – Chichester: Wiley-Blackwell, 2009. – 656 p. – ISBN 978-1-405-19686-4.
4. Mansell, R. Imagining the Internet: Communication, Innovation, and Governance / R. Mansell. – Oxford: Oxford University Press, 2012. – 296 p. – ISBN 978-0-19-969704-5. – DOI 10.1093/acprof:oso/9780199697045.001.0001.
5. Resilience and Survivability in Communication Networks: Strategies, Principles, and Survey of Disciplines / J. P. G. Sterbenz, D. Hutchison, E. K. Çetinkaya [et al.] // Computer Networks. – 2010. – Vol. 54, No. 8. – Pp. 1245–1265. – DOI 10.1016/j.comnet.2010.03.005.
6. Alberts, C. J. Managing Information Security Risks: The OCTAVE Approach / C. J. Alberts, A. J. Dorofee. – Boston: Addison-Wesley, 2003. – 471 p. – ISBN 978-0-321-11886-8.
7. OpenFlow: Enabling Innovation in Campus Networks / N. McKeown, T. Anderson, H. Balakrishnan [et al.] // ACM SIGCOMM Computer Communication Review. – 2008. – Vol. 38, No. 2. – Pp. 69–74. – DOI 10.1145/1355734.1355746.
8. Han, B., Gopalakrishnan, V., Ji, L., Lee, S. Network Function Virtualization: Challenges and Opportunities for Innovations / B. Han, V. Gopalakrishnan, L. Ji, S. Lee // IEEE Communications Magazine. – 2015. – Vol. 53, No. 2. – Pp. 90–97. – DOI 10.1109/MCOM.2015.7045396.
9. Shi, W., Cao, J., Zhang, Q., Li, Y., Xu, L. Edge Computing: Vision and Challenges / W. Shi, J. Cao, Q. Zhang, Y. Li, L. Xu // IEEE Internet of Things Journal. – 2016. – Vol. 3, No. 5. – Pp. 637–646. – DOI 10.1109/JIOT.2016.2579198.
10. Roelkens, G., Abassi, A., Cardile, P. [et al.] III–V-on-Silicon Photonic Devices for Optical Communication and Sensing / G. Roelkens, A. Abassi, P. Cardile [et al.] // Photonics. – 2015. – Vol. 2, No. 3. – Pp. 969–1004. – DOI 10.3390/photonics2030969.
11. Gisin, N., Thew, R. Quantum Communication / N. Gisin, R. Thew // Nature Photonics. – 2007. – Vol. 1, No. 3. – Pp. 165–171. – DOI 10.1038/nphoton.2007.22.
12. Rowe, N. C. Introduction to Cyberdeception / N. C. Rowe, J. Rrushi. – Cham: Springer, 2016. – XIV, 334 p. – ISBN 978-3-319-41185-9. – DOI 10.1007/978-3-319-41187-3.
13. Schneier, B. Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World / B. Schneier. – New York: W. W. Norton & Company, 2015. – 400 p. – ISBN 978-0-393-24481-6.
14. Clark, D. D., Wroclawski, J., Sollins, K. R., Braden, R. Tussle in Cyberspace: Defining Tomorrow's Internet / D. D. Clark, J. Wroclawski, K. R. Sollins, R. Braden // IEEE/ACM Transactions on Networking. – 2005. – Vol. 13, No. 3. – Pp. 469–478. – DOI 10.1109/TNET.2005.850224.
15. Anderson, R. Security Engineering: A Guide to Building Dependable Distributed Systems / R. Anderson. – 2nd ed. – Indianapolis: Wiley, 2008. – 1040 p. – ISBN 978-0-470-06852-6.
16. A Comprehensive Survey of Network Function Virtualization / B. Yi, X. Wang, K. Li [et al.] // Computer Networks. – 2018. – Vol. 133. – P. 212–262. – DOI 10.1016/j.comnet.2018.01.021.
17. Fu, C., Wang, B., Wang, W. Software-Defined Wide Area Networks (SD-WANs): A Survey / C. Fu, B. Wang, W. Wang // Electronics. – 2024. – Vol. 13, No. 15. – Article 3011. – DOI 10.3390/electronics13153011.
18. Pryamikov, A. D., Gladyshev, A. V., Kosolapov, A. F., Bufetov, I. A. Polye svetovody: sovremennoye sostoyaniye i perspektivy razvitiya / A. D. Pryamikov, A. V. Gladyshev, A. F. Kosolapov, I. A. Bufetov // Uspekhi Fizicheskikh Nauk (Physics-Uspekhi). – 2024. – Vol. 194, No. 2. – Pp. 138–168. – DOI: 10.3367/UFNr.2023.12.039616 (In Russ.)
19. Virgilio, G. P. M. High-frequency Trading: A Literature Review / G. P. M. Virgilio // Financial Markets and Portfolio Management. – 2019. – Vol. 33, No. 2. – Pp. 183–208. – URL: (accessed: 01.11.2026). – DOI 10.1007/s11408-019-00331-6.
20. Russell, P. St. J. Invited Commentary: Hollow Core Glass Fibre — The Perfect Pipe for Light / P. St. J. Russell // eLight. – 2025. – Vol. 5. – Article 4. – DOI 10.1186/s43593-025-00086-w.

15 The Concept of Digital Transformation of the Armed Forces of the Russian Federation // Approved by the Minister of Defense of Russia.