

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

Лукашев А. В.¹

DOI:10.21681/3034-4050-2026-5-50-58

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: предложен новый подход к цифровой трансформации сетей связи специального назначения с учетом опыта мирового, в первую очередь, США и Китая, на основе научно обоснованного ее содержания и отличия от типовой модернизации (совершенствования, обновления и пр.). На основе анализа текущих предложений о применении существующих протоколов информационного обмена для перспективных сетей связи обосновано предостережение об ограничении применимости протокола IP/MPLS, продвигаемого некоторыми разработчиками, по основаниям его морального и программно-технического устаревания при обеспечении эволюционного перехода на новый, высший, технологический уровень.

Созданы модели сетевых технологических решений, табличные методики сравнения подходов и представлены научно-обоснованные предложения цифровой трансформации сетей связи в интересах обеспечения безопасного информационного обмена.

Научная новизна: 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.

Введение

Происходящая в мире третья цифровая революция является закономерным этапом исторического развития сетей связи. И не только сетей связи. С середины XX века параллельно зародились и стали внедряться технологии обработки информации на принципах биологических систем. Так появился первый нейрон, так появились нейросети. Впоследствии, в последней трети прошлого столетия искусственные нейроны обрели новое содержание, приблизившись к биологическому образцу. Так появились нейроморфные системы.

Вряд ли кто-то предполагал, что новая отрасль науки – квантовые вычисления, могут оказать влияние на технологии связи и информатики. Но такое влияние, хоть и косвенное,

возникло. И оказало «давление» на системы информационного обмена в форме угроз криптографическим системам. Квантовый компьютер хорошо справляется с задачами факторизации. Причем настолько хорошо, что существующие системы асимметричного шифрования могут оказаться беззащитными перед его могуществом. При этом технологии квантовых вычислений должны использоваться в сетях связи, поскольку они переводят их на принципиально новый уровень эффективности в аспекте скорости передачи информации, решения задач информационного обмена и его безопасности на новом, квантовом уровне.

Таким образом, история развития этих трех смежных направлений привела к их логическому объединению, интеграции, породив

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

принципиально новые методы инфокоммуникационного обеспечения систем управления, а также других высокотехнологичных систем обработки информации и связи.

Новизна настоящей работы состоит в детальном научном обосновании путей построения сетей связи специального назначения путем их цифровой трансформации, единого утвержденного взгляда, который только начинает внедряться в среду научных исследований. Принцип единства гетерогенных сетей связи, объединяемых единой цифровой платформой на основе широкого внедрения элементов искусственного интеллекта, приобретает качественно новый облик.

Различные взгляды на построение перспективных сетей связи в рамках единой цифровой платформы целесообразно привести к общему пониманию ее облика в результате цифровой трансформации. При этом сроки создания данной платформы должны быть привязаны к быстро развивающейся негативной геополитической ситуации.

Происходит слияние трех технологий в единый информационно-коммуникационно-вычислительный организм – единую цифровую платформу, облик которой во многих источниках пока представляется туманным. Надеемся, что к концу данного труда туман может поредеть, чтобы окончательно рассеяться в ближайших исследованиях.

Другим фактором, определяющим необходимость глубокой цифровой трансформации, следует считать появление квантовых компьютеров, представляющих угрозу криптографическим системам, что ведет к пересмотру требований к сетевой безопасности на принципиально новых, инновационных, технологиях. Полноценный квантовый компьютер, внедрение которого не за горами, способен дешифровать перехваченные сообщения в реальном времени, даже, если они зашифрованы современными криптографическими системами гарантированной стойкости.

Пока же, «недружественные страны» внедряют системы «*Save now, hack later*» («Сохрани сейчас, взломай потом»)².

Это требует принятия решения о защите данных «еще вчера». Ведь существуют сведения, сроки свободного доступа к которым отложены на десятилетия.

Поэтому сверхзадача данной работы состоит в том, чтобы побудить читателя к глубокому осознанию сути и содержанию происходящего перехода развитых стран к новому, шестому, постиндустриальному, технологическому укладу

и присоединению к этому процессу России с целью недопущения потери национального суверенитета.

Почему не IP-MPLS или предотвращение тупиковой ветви развития

В настоящее время в среде разработчиков перспективных сетевых технологий для сетей передачи данных превалирует решение на протоколе *IP/MPLS (Multi-Protocol Label Switching)*, сеть передачи данных с коммутацией по меткам. Целесообразно отметить перечень особенностей и недостатков данного подхода³.

Информация по сетям связи передается, как правило, способом пакетных данных. При этом пакет не содержит данных вне IP-адреса назначения. Так же не существует инструкций о способе доставки пакета данных по назначению. Локальный сетевой маршрутизатор выполняет вычисления и принимает решение об отправке пакета по сети для каждого пакета, руководствуясь метками, содержащимися в заголовке сетевого уровня пакета. Таким образом, каждый раз, когда пакет прибывает на маршрутизатор, он должен осуществить вычисления о дальнейшем маршруте пакета и отправить его дальше, руководствуясь сложными таблицами маршрутизации, которые создаются сетевым администратором (человеком). В случае деструктивного воздействия с выходом из строя участка (фрагмента) сети таблица маршрутов обновляется, как правило, вручную. К этому следует добавить, что такие вычисления вносят свою лепту в рост задержек доставки пакетов, а, следовательно, непосредственно влияют на обеспечение требований по своевременности связи, что по опыту специальной военной операции (СВО) становится критически недопустимым фактором для системы управления в условиях современного боя в тактическом звене управления.

Данный протокол обладает высокой стоимостью внедрения и обслуживания, сложностью настройки (требует высокопрофессионального персонала) и управления, а также проблемы с масштабируемостью и гибкостью, особенно в облачных средах и при работе с удаленными узлами на выделенных операционных направлениях. Протокол менее гибок, чем современные протоколы, например, наиболее популярный *SD-WAN (Software-Defined Wide Area Network)* – технология управления корпоративной WAN-сетью через программные методы в системах передачи данных развитых зарубежных стран.

Высокая стоимость обусловлена необходимостью специализированного оборудования

2 The Intercept: Расследования Э. Сноудена о теневом бюджете АНБ, включая информацию о строительстве дата-центра в штате Юта. – URL: https://theintercept.com/nsa-black-budget/?spm=a2ty_o01.29997173-0.0.33135171rXl4DI (Дата обращения 13.01.2024).

3 Сетевой мир, Интернет ресурс: Многопротокольная коммутация меток надежна, но дорога, что приводит к тому, что предприятия дополняют ее более дешевыми и гибкими SD-WAN // – URL: <https://www.networkworld.com/article/829388/what-is-mpls.html>.

и программного обеспечения, требующего специальной сертификации.

Это ведет к дороговизне при развертывании и обслуживании.

Настройка и управление MPLS-сетью требует специальных знаний и больших трудозатрат (а значит, времени), что осложняет работу в сложных условиях, в том числе, в военное время.

Масштабирование сети является сложным и дорогостоящим, особенно на выделенных направлениях, например, в арктических сценариях. Это обусловлено централизованной маршрутизацией, реализуемой на технической базе, что приводит к задержкам, а также требует дополнительных затрат на развертывание и настройку квалифицированным персоналом. Людские потери в среде обслуживающего персонала, даже одного специалиста могут привести к потере связи на удаленном направлении.

Кроме того, сеть на протоколе MPLS требует использования специализированных протоколов, например, LDP и RSVP-TE, что усложняет настройку системы и управление сетью. К этому следует добавить необходимость постоянной связи с поставщиком оборудования, что ограничивает выбор оптимальных с экономической точки зрения решений и их гибкости, что критически важно для военных систем коммуникаций, требующих оперативного восстановления при деструктивных воздействиях и изменения ситуационной обстановки.

В сети MPLS могут возникать проблемы с адресацией, особенно в больших сетях и особенно при межсетевой интеграции.

Сеть MPLS чувствительна к характерным для военных сетей связям, что может привести к прерыванию соединения и нарушению работы всей сети. Это также ведет к вероятным нарушениям специальных требований к системе связи в части своевременности, достоверности и актуальности переноса трафика в интересах органов управления войсками и оружием.

С учетом изложенного, требуются наиболее современные решения в организации и эксплуатации сетей связи, свойства и характеристики которых отвечают специальным требованиям⁴.

Ниже (табл. 1) представлены сравнительные характеристики существующей сети на протоколе MPLS и сети SD-WAN.

- 4 ■ Alaettinoglu C. – Проблемы мультисервисных сетей. – URL: <https://www.factorgroup.ru/blogs/news/strukturnyy-razbor-dannyh-sdn-vse-delo-v-analitike?ysclid=mfmtj7cnn0695632275>. (Дата обращения сентябрь 2025).
- Enhancing IP-MPLS Networks: Overcoming Challenges and Embracing SDN Advancements. – URL: <https://5gnetworkarchitecture.com/enhancing-ip-mpls-networks-overcoming-challenges-and-embracing-sdn-advancements> (Дата обращения сентябрь 2025).
- Daniel x.: – URL: https://www.academia.edu/38878253/Chapter_1_Introduction_to_MPLS_and_SDN (Дата обращения сентябрь 2025).
- Sam K. Aldrin.: – SDN and MPLS in DataCenters. – URL: https://www.sanog.org/resources/sanog23/SANOG23_SDN_and_MPLS_in_DC.pdf (Дата обращения сентябрь 2025). (Дата обращения сентябрь 2025).
- David Jacobs, The Jacobs Group: With MPLS-TP and SDN, a simpler dynamic control plane. – URL: <https://www.techtarget.com/searchnetworking/tip/With-MPLS-TP-and-SDN-a-simpler-dynamic-control-plane>
- Seremet I., Čaušević S.: Advancing IP/MPLS with Software Defined Network in Wide Area Network. // September 2019. – URL: https://www.researchgate.net/publication/335691420_Advancing_IPMPLS_with_Software_Defined_Network_in_Wide_Area_Network_Conference_FOAN-8th_INTERNATIONAL_CONFERENCE_ON_FIBER_OPTICS_IN_ACCESS_NETWORKSAt_Sarajevo (Дата обращения сентябрь 2025).

Таблица 1.

Сравнение MPLS vs SD-WAN (типовой вариант)

Параметр	MPLS	SD-WAN
Время восстановления при сбое	5–10 с (при наличии динамической маршрутизации)	<1 с
Поддержка нескольких видов каналов связи	Только MPLS	LTE, Интернет, VSAT, Wi-Fi mesh
Latency (задержка)	10-50 мс	10-80 мс (в зависимости от типа канала)
Jitter (колебание задержки)	Низкий	Средний, компенсируется политиками QoS (контроля качества связи)
Packet loss (потери пакетов)	<0,1%	0,1–2%
Автоматизация управления	Ограниченная	Полная (через приложение)
Управление политиками маршрутизации	Локальное или через провайдера	Централизованное через оркестратор
Шифрование точка-точка	Дополнительно	Интегрировано (IPsec, DTLS)
Поддержка мобильных узлов	Нет	Да (например, БПЛА, самолеты)
Количество одновременных путей между узлами	1 (LSP)	До 5 (LTE + Интернет + спутниковый канал и др.)
Возможность масштабирования	Сложно (из-за ограничений MPLS-сети)	Просто (любое количество новых или резервных узлов)

Сравнение качественных характеристик, существующих морально устаревших решений на протоколе MPLS и сети SD-WAN позволяет однозначно отдать предпочтение последнему решению.

Обоснование принципов цифровой трансформации сетей связи

В целях более глубокого понимания сути цифровой трансформации сетей связи, прежде всего, специального назначения, ниже (табл. 2), приводятся основные отличия типовой модернизации технических систем от цифровой трансформации, как она понимается (и осуществляется) мировыми технологическим лидерами.

Следует отметить, что логичным путем развития гетерогенных сетей силовых ведомств, государственных ведомственных сетей, Единой сети электросвязи страны (ЕСЭ) является их интеграция путем создания *единой цифровой платформы национального масштаба*, поэтому исходным пониманием цели и сути цифровой трансформации является установление отличий базовых понятий цифровой трансформации от типовой модернизации.

На текущем этапе планирования развития системы связи мероприятия по повышению

безопасности информационного обмена не включают новые угрозы, например, со стороны уже массово применяемых ИИ-агентов, способных имитировать поведение человека, находить уязвимости в сетях связи, внедряться в их внутреннюю структуру, подменить данные, передавать шпионские данные в скрытом фоновом режиме для их обработки противостоящей стороной. В ближайшей перспективе такая обработка будет осуществляться в реальном масштабе времени с помощью квантовых компьютеров. Поэтому в создаваемой единой цифровой платформе (ЕЦП) должны применяться встроенные механизмы защиты, самовосстановления, за счет которых сети обеспечивают устойчивость к внешним и внутренним воздействиям: кибератакам, природным катастрофам, ошибкам персонала и техническим отказам в мили- и микросекундном масштабе времени, где оператор-человек бессильен в борьбе с современными атаками на сетевую безопасность.

Таким образом, цели цифровой трансформации, ее принципиальные отличия от типовой (стандартной) модернизации сформулированы и предложены условия, в которых цифровая трансформация должна осуществляться.

Следует выделить следующие основные принципы формирования ЕЦП:

Таблица 2.

Основные отличия стандартной модернизации информационных и коммуникационных систем от цифровой трансформации

Стандартная модернизация	Цифровая трансформация
Замена старого оборудования на новое, более эффективное, без изменения принципов работы	Системные изменения, затрагивающие всю инфраструктуру и процессы взаимодействия между участниками экосистемы
Локальные изменения, направленные на улучшение конкретных параметров, корректировки общих и частных требований	Фундаментальное изменение архитектуры, технологий и подходов к управлению сетью. Программно-определяемые сети (SDN) позволяющие управлять сетью через программное обеспечение, что делает ее гибкой и масштабируемой
Ограниченная автоматизация, основная роль остается за человеком	Повсеместное внедрение ИИ для самовосстановления и ликвидации сбоев в сети в мили- и микросекундном масштабе времени, управление и оптимизация ресурсов, персонализация услуг, снижение зависимости от человеческого фактора
Обновление оборудования и программного обеспечения без изменения парадигмы функционирования. Сеть остаётся жестко структурированной и недостаточно гибкой	Переход от иерархических структур к распределённым инвариантным моделям управления. Сеть становится гибкой, масштабируемой и способной адаптироваться к меняющимся условиям в реальном времени по внешним условиям и внутреннему потенциалу
Мероприятия по повышению безопасности информационного обмена осуществляются персоналом соответствующих служб с ограниченным применением искусственного интеллекта и не включают защиту от новых угроз кибернетической войны – ИИ-агентов и квантовых компьютеров	Встроенные механизмы защиты, самовосстановления, за счет которых сети обеспечивают устойчивость к внешним воздействиям: кибератакам, природным катастрофам

1. Новые системы должны создаваться на принципе двойного применения – для гражданской и специальной областей.
2. Сети информационного обмена должны использовать единое для всех ведомств программное обеспечение. Оно должно быть модульным, предусматривающим установку дополнительных блоков, обеспечивающих реализацию требований безопасности в сетях специального назначения.
3. Оборудование должно быть унифицированным, с двойным применением и возможностью доукомплектования дополнительными аппаратными средствами для обеспечения специальных требований.
4. Стек протоколов информационного обмена должен быть единым, при этом выполняется принцип разграничения прав доступа. Заметим, что по запросу, должно обеспечиваться сквозное (бесшовное) взаимодействие ведомственных сетей в целях предоставления информационных услуг с заданным качеством – они должны быть своевременными, достоверными, актуальными и обеспечивать безопасный информационный обмен.

Следование данным принципам системой информационного обмена служит основанием *нового*, более высокого технологического уровня предоставляемых органам управления информационных и телекоммуникационных услуг.

Цифровая трансформация сетей связи – это процесс кардинального изменения архитектуры, функциональности и управления сетями на основе единых правил и цифровых технологий, что позволит не только модернизировать их, но и создать принципиально новые возможности для взаимодействия между людьми, устройствами и системами. Это качественный скачок, который выходит за рамки простой модернизации или обновления оборудования.

Для формирования определения ЕЦП следует учесть все факторы, определяющие ее *сущность*. Сущность нового облика данной платформы должна учитывать:

1. *Главный принцип*: «Внедряются только самые передовые, мирового уровня, технологии информационного обмена при условии взаимодействия новых систем с существующими путём интегрирования «старых» сетей в сети нового уровня с помощью аппаратных и программных средств (эволюционный подход)».
2. *Основное предназначение*: предназначение единой цифровой платформы основано на отечественном, в том числе, негативном, и мировом опыте создания больших инфокоммуникационных сетей (платформ),

включающих разнородные сети, принадлежащие различным ведомствам, органам управления, многочисленным организациям и предприятиям.

3. *Общее назначение*: возможность простого доступа любого пользователя, с любого устройства, из любого местоположения к *доверенной* среде единой платформы.
4. *Конечную цель* обеспечения (уже бесшовного) информационного обмена. Пользователям передаваемые сообщения различной природы (речь, медиа контент, передача данных, телеметрическая информация и пр.) должна быть предоставлена в форме услуги. При этом в существующем положении вещей предоставление услуг может быть существенно затруднено или вообще невозможно в силу несовместимости окончного оборудования и программных компонентов. Отсюда – окончное оборудование и программное обеспечение должны быть *унифицированы* по функциональности и распределено по кластерам для всех участников информационного обмена, являющихся участниками единой цифровой платформы.
5. *Доставка сообщений* платформа должна обеспечивать *актуальность* доставляемой информации. Этого можно добиться снижением задержек при обработке и передаче сообщений об изменении ситуации и новых событий. Опыт внедрения подобных решений в мировой практике показывает эффективность *гибридную архитектуру вычислений*, осуществляемых в сетях. Термин гибридной архитектуры вычислений подразумевает комплексно-распределенную организацию вычислений⁵.
Часть вычислений, наиболее сложную, следует осуществлять в специализированных центрах обработки данных (ЦОДах). Обычно такой способ вычислений называется «облачным». При этом, базы знаний и оперативных данных различных ведомств, имеющих ресурсы в ЦОД, должны содержать непротиворечивые сведения. В целях ускорения прохождения сообщений, уменьшения задержек, могут применяться граничные (на стыках сетей) или конечные вычисления (непосредственно на рабочем месте пользователя). Таким образом, единая цифровая платформа должна использовать *гибридную архитектуру вычислений*.
6. *Обеспечение бесшовного* взаимодействия гетерогенных сетей возлагается на единую цифровую платформу. Следовательно, для

5 Былин А., ГК «Ланит»: Распределенные вычисления и надежность гибридных сред. – URL: <https://www.iksmmedia.ru/articles/5851462-Raspredelennye-vychisleniya-i-nadezh.html?ysclid=mffr4bc2kk704260919>. (Дата обращения сентябрь 2025).

присоединения к ней разнородных сетей должен использоваться единый стек протоколов, исключая трудности взаимодействия данных сетей.

7. *Большие данные.* Современные системы информационного обмена характеризуются большим объемом передаваемых данных, которые собираются из различных источников. В данной ситуации возможности человека не соответствуют объему задач по обработке такого объема данных. Поэтому большие данные обрабатываются с помощью нейросетей (если они «не очень большие», т.е. частные) или генеративными нейроморфными системами искусственного интеллекта (языковыми моделями), если данные имеют достаточно большой объем, а требования по времени их обработки критически малое. При этом персонал Министерства обороны РФ должен иметь доступ к языковым моделям в целях обеспечения обработки данных в реальном масштабе времени. Таким образом, в ЕЦП для обработки должны использоваться *системы искусственного интеллекта*.
8. *Качество услуг* единой цифровой платформы. Внедрение единой цифровой платформы подразумевает повышение ее эффективности практически по всем показателям предъявляемых пользователями различного ранга. Повышение эффективности, в частности, может быть обеспечено за счет *самоорганизации и самовосстановления* сетей связи, в том числе, и самой ЕЦП. Такие свойства также достигаются применением искусственного интеллекта для управления сетями связи. Другим способом повышения эффективности предоставляемых услуг, является *инвариантный доступ* пользователя к сети (линии) связи, обеспечивающей наиболее эффективное предоставление услуги (ресурса) пользователю, абоненту по ситуационному состоянию сетей и ЕЦП.
9. *Сроки* создания единой цифровой платформы. На создание ЕЦП, на фоне геополитической обстановки, которая приобретает угрожающие формы для национальной безопасности России, целесообразно отвести не более 4–5 лет [1, 2]. Обеспечить это возможно, по зарубежному опыту наиболее развитых стран, использованием средств, систем и программного обеспечения двойного назначения и коренным пересмотром регулирования отрасли [3]. Существующее положение характеризуется ведомственным подходом – каждое силовое ведомство, госкорпорация, и даже местная платформа государственных услуг разрабатываются

собственными или привлеченными подрядными командами. Отсюда беспрецедентный расход финансовых, материальных и интеллектуальных ресурсов из-за параллелизма разработок, которые, в итоге, трудно или вообще никак не стыкуются. Развитые страны уже много лет применяют подход *двойного применения (назначения)* разрабатываемых средств и систем⁶. Предприятия ОПК страны, принадлежащие различным ведомствам, при таком подходе, могли бы объединиться в единый научно-промышленный комплекс.

10. *Структура трафика.* Передаваемая в сетях информация разнородна по видам и назначению. Отсюда логически вытекает необходимость внедрения *многоуровневой архитектуры* трафика. В некоторых источниках такой подход называют «многослойностью». Основными уровнями (слоями) могут быть: уровень доступа, уровень транспорта, уровень вычислений, уровень управления. При необходимости можно организовать и другие уровни, например, IoT (интернет вещей) и пр.
11. *Приоритетность.* В сетях постоянно циркулируют информационные потоки. Они порождаются пользователями (абонентами). Пользователи имеют различный *статус*, в соответствии со своим служебным положением. Поэтому пользователям должен присваиваться определенный владельцем сети *ранг*. Присвоенный ранг по отношению к информационному обмену, должен иметь соответствующий *приоритет*. Другая часть информации представляет собой *большие данные* от разнородных датчиков и систем обмена информацией между устройствами, это – интернет вещей, IoT. Здесь приоритеты устанавливаются в соответствии с важностью информации, ее категорией. Поэтому приоритеты такой информации отображаются в *категориях срочности сообщений, общими* для всех ведомств, учреждений и корпораций.
12. *Цифровые двойники.* Цифровой двойник изделия, согласно ГОСТ Р 57700.37-2021, (следует читать «и программного компонента») применяется на всех стадиях жизненного цикла, п. 3.24. Это означает, цифровой двойник (ЦД) должен разрабатываться на этапе проектирования (разработки) изделия, системы, ЦД должен широко использоваться в процессе приемных испытаний (сокращение сроков принятия на вооружение), а также,

⁶ Techniques for satellite communications. November 2020. – URL: https://irp.fas.org/16_Joint_Publication_1-02 (15.12.2023 г.). (Дата обращения декабрь 2023).

что важно для сетей и систем обмена информацией, прогнозирования отказов, угроз и немедленной передаче сообщения о возможном инциденте управляющему ИИ для предотвращения отказа и нивелирования угрозы.

Итак, основными факторами, определяющими создаваемую единую цифровую платформу, являются:

1. *Приоритет* новейших мировых достижений при планировании создания ЕЦП в форме цифровой трансформации сетей связи.
2. *Бесшовный* информационный обмен.
3. Унифицированное конечное и сетевое оборудование.
4. *Гибридная* архитектура вычислений.
5. *Единый* стек протоколов информационного обмена.
6. Системы искусственного интеллекта для обработки больших данных.
7. Система поддержки принятия решений (СППР) должна трансформироваться в интеллектуальную СППР.
8. *Самоорганизация и самовосстановление* сетей с автоматизацией вхождения в связь.
9. *Инвариантный* доступ пользователей к сетям, обеспечивающих наиболее эффективное предоставление запрошенной услуги (ресурса). При этом перспективные автоматизированные рабочие места и инструменты пользователей должны исполняться с применением эргономичного подхода – применением промышленного дизайна рабочей среды должностных лиц.
10. Внедрение принципа *двойного применения* (назначения) разрабатываемых средств и систем.
11. *Многослойная* (многоуровневая) архитектура трафика в соответствии с приоритетностью передаваемых сообщений и рангом пользователей. Очевидно, что «слоистость» трафика будет иметь *динамический* характер. Это также предопределяет применение SDN сетей в платформе.
12. *Цифровой двойник* ЕЦП, создающийся на этапе ее проектирования и внедрения, обеспечивающий устойчивость системы связи в целом.

На основании вышеизложенных аргументов, изучения компонентов шестого технологического уклада, признаков цифровой трансформации (табл. 1) и ее принципов, а также выявленных факторов, влияющих на функциональность единой цифровой платформы, можно сформировать подход к определению сущности

платформы, вытекающий из выше проведенного анализа.

Определение. *Единая цифровая платформа есть комплекс инфокоммуникационных технологий, реализуемый сетевыми программно-аппаратными средствами под управлением искусственного интеллекта с гибридной архитектурой вычислений, объединяющий и оптимизирующий ресурсы присоединяемых сетей различной принадлежности по единому стеку протоколов.*

Единая цифровая платформа предназначена для устойчивого информационного обеспечения органов государственного и специального управления, пользователей различного ранга путем сквозного бесшовного взаимодействия гетерогенных сетей различной принадлежности в целях предоставления унифицированных услуг с инвариантным доступом.

Кратко опишем функциональную структуру и принцип действия создаваемой платформы.

Функционально ЕЦП может включать два сегмента – виртуальный и физический. Виртуальный сегмент представляет собой временные соединения для предоставления услуг по запросу пользователей. От окончного оборудования до транспортной сети вычисления оптимального пути обеспечиваются конечными вычислителями на объекте пользователя. На стыке канала с транспортной сетью осуществляются граничные вычисления оптимального маршрута внутри данной сети. Далее, на границе транспортной сети и сети, которой принадлежит вызываемый пользователь, осуществляется коммутация и сообщение, в форме распределенных пакетов, доставляется по адресу. Совокупность соединений представляют собой программно-определяемую сеть (SDN), которая непрерывно изменяет собственную структуру без участия человека.

В случае запроса пользователем услуги вычислений при использовании системы поддержки принятия решения, может использоваться гибридная архитектура вычислений – конечные и облачные вычисления, если принятие решения основано на обработке больших данных. В этом случае пользователь считается приоритетным и ему предоставляется канал (с резервированием) наивысшего качества и удовлетворяющий требованию по пропускной способности.

Виртуальный сегмент опирается на сегмент физический, который, в зависимости от масштаба сети, может включать космический, воздушный (авиационный и/или беспилотный) и наземный (стационарный и /или полевой) компоненты гетерогенных (принадлежащих разным ведомствам и различающиеся по технологиям) сетям,

а все вместе представляющие собой транспортную сеть общего пользования.

Наземный компонент может использовать средства радиосвязи, интегрированные с линиями сети космической связи (используются низкоорбитальные спутники), стационарные и полевые медные (постепенно изживающие себя) и волоконно-оптические проводные линии связи.

Транспортная сеть должна обеспечивать, в том числе, мобильных абонентов, для чего может применяться мобильная связь *5G-BH*, в перспективе *6G-BH*, которые обеспечивают высокие скорости передачи данных и ультранизкие задержки.

Воздушный компонент беспилотных средств может быть основан на роевой структуре, когда группа беспилотных летательных аппаратов (БПЛА) различной численности, «зависает» над определенной территорией, непрерывно псевдохаотично перемещаясь в пространстве на расстоянии доступа к ближайшим аппаратам. При этом рой обладает близкой к полносвязности структурой. При выработке ресурса двигателя БПЛА автоматически возвращается на базу, а ему на замену направляется подменный аппарат. База, с которой осуществляются запуски участников роя, должна быть подвижной с обеспечением радио привода по местоположению. При уничтожении участников воздушного роя они заменяются резервными аппаратами, заранее запрограммированными на выполняемую задачу. Каждый аппарат роя должен обладать компонентом общей нейросети, обучающейся в процессе боевого применения. В рое компоненты объединяются в нейросеть, обладающую искусственным разумом.

Авиационный ретранслятор функционирует по классическому формату, обеспечивая связь на более высоком иерархическом уровне системы управления.

Как виртуальный, так и физический компоненты являются гибкими – они предоставляют свой ресурс пользователям по запросу, в том числе, способом инвариантного доступа (независимо от иерархической и ведомственной принадлежности) и это тоже SDN, пришедшая на смену отслужившей свой век сервис-ориентированной архитектуры.

Для предлагаемой архитектуры требуется разработка специальных требований, разграничивающих пользователей по статусу, рангу, а также по приоритетам сообщений или услуг в соответствии с решаемыми системой (органами) управления задачами. Данная задача выходит за рамки статьи и будет решаться в предстоящих исследованиях.

Для доступа к ЕЦП пользователь использует унифицированное оборудование требуемого вида, в соответствии с запрашиваемой услугой. Это может быть голосовой вызов (смартфон, планшет, настольный терминал), видеосвязь (ноутбук и т. п.), передача данных (ноутбук, персональный компьютер, портативный вычислитель, контроллер и пр.), а также аппаратура шифрования. При создании единой цифровой платформы, в предвидении создания полноценного квантового компьютера, шифрование должно обеспечиваться постквантовыми алгоритмами шифрования с эволюционным внедрением систем квантового распределения ключей.

Продолжение следует.

Литература

1. Bahnasse A., Ezzahraa Louhab F., Khiat A., Badri A., Talea M., Pandey B.: Springer. – 2020. – Pp. 1107–1131. – URL: <https://link.springer.com/article/10.1007/s11277-020-07411-1>.
2. Лукашев А., Лаута О., Чаднов А. В ожидании российской квантовой революции в военной сфере // Военная мысль. – 2024. – № 4. – С. 140–147.
3. Dr. Mosks M., Dr. Piani M. – Quantum Threat Timeline report 2022 // Global Risk Institute, Toronto, Canada, December 2022. – Pp. 1–67.
4. Айзексон У., Илон Маск. – М.: АСТ, 2023 г. – 720 с. – ATP 6–02.54.

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

Lukashev A. V.⁸

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, and internetwork integration of communication networks.*

7 RSA and Diffie-Hellman Cryptosystems. – URL: <https://www.moodyanalitics.com/articles/2023/rsa-and-diffie-hellman-cryptosystems-under-threat-sooner-than-previously-thought> (Дата обращения 15.10.2024).

8 Anatoly V. Lukashev, Ph.D. of Military Sciences, Senior Researcher of the Research Center of the Military Academy of Communications named after S. M. Budenny. St. Petersburg, Russian Federation. E-mail: lukasheff@mail.ru

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: a new approach to the digital transformation of special-purpose communication networks is proposed, considering the experience of the world, primarily the USA and China, based on its scientifically based content and difference from standard modernization (improvement, updating, etc.). Based on the analysis of current proposals for the use of existing information exchange protocols for promising communication networks, a warning is substantiated about the limitation of the applicability of the IP/MPLS protocol, promoted by some developers, on the grounds of its moral and software-technical obsolescence while ensuring an evolutionary transition to a new, higher, technological level.

Models of network technological solutions, tabular methods for comparing approaches have been created, and scientifically based proposals for the digital transformation of communication networks in the interests of ensuring secure information exchange have been presented.

Scientific novelty: scientifically based definition of a single special-purpose digital platform; 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 unified 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.

References

1. Bahnasse A., Ezzahraa Louhab F., Khiat A., Badri A., Talea M., Pandey B.: Springer. – 2020. – Pp. 1107–1131. – URL: <https://link.springer.com/article/10.1007/s11277-020-07411-1>.
2. Lukashev A., Lauta O., Chadnov A. V ozhidanii rossijskoj kvantovoj revolyucii v voennoj sfere // Voennaya mysl'. – 2024. – No. 4. – Pp. 140–147.
3. Dr. Mosks M., Dr. Piani M. – Quantum Threat Timeline report 2022 // Global Risk Institute, Toronto, Canada, December 2022. – Pp. 1–67.
4. Ajzekson U., Ilon Mask. – M.: AST, 2023. – 720 p. – ATP 6–02.54.

