УДК 004.056.5

Павел Сергеевич Алямкин
Национальный Исследовательский Мордовский Государственный Университет им. Н. П. Огарёва, Саранск, Россия
Леонид Юрьевич Королев
кандидат технических наук, доцент, Национальный Исследовательский Мордовский Государственный Университет им. Н. П. Огарёва, Саранск,
Николай Сергеевич Соболев
доцент, Национальный Исследовательский Мордовский Государственный Университет им. Н. П. Огарёва, Саранск, Россия

АНАЛИЗ ПЕРСПЕКТИВНЫХ РЕШЕНИЙ В СФЕРЕ VPN-СОЕДИНЕНИЙ

Аннотация. В работе проведен многоаспектный анализ направлений развития виртуальных частных сетей (VPN) в условиях эскалации киберугроз и нормативных ограничений, действующих в Российской Федерации. Рассмотрены переход от традиционных протоколов к облегчённым протоколам нового поколения (например, WireGuard) а также внедрение контейнеризированных распределённых архитектур.

Abstract. This paper provides a multifaceted analysis of virtual private network (VPN) development trends in the context of escalating cyber threats and regulatory restrictions in the Russian Federation. It examines the transition from traditional protocols to lightweight, next-generation protocols (e.g., WireGuard) and the implementation of containerized distributed architectures are discussed.

Ключевые слова: виртуальные частные сети; кибербезопасность; протоколы; информационная безопасность.

Keywords: virtual private networks; cybersecurity; protocols; information security.

Введение

Виртуальные частные сети (VPN) представляют собой ключевой инструмент обеспечения информационной безопасности в современном цифровом мире. Они позволяют создавать защищённые каналы связи поверх общедоступных сетей, таких как Интернет, гарантируя конфиденциальность, целостность и аутентификацию данных. В условиях растущих угроз кибербезопасности, включая хакерские атаки, утечки данных и ужесточение государственного регулирования, задача разработки перспективных решений в сфере VPN-соединений приобретает особую актуальность. Согласно статистике, количество инцидентов с утечками данных в 2023 году выросло на 60% по сравнению с 2022 годом, что подчёркивает необходимость инновационных подходов к защите сетей [8]. Научные труды таких авторов, как С. В. Запечников, Н. Г. Милославская, А. И. Толстой, а также диссертации и статьи в изданиях «International Research Journal» и «CyberLeninka», отражают переход к распределённым системам, интеграции с искусственным интеллектом и адаптации к новым угрозам. Целью данной работы является систематизация перспективных направлений развития VPN с учётом российской специфики: эволюции протоколов, распределённых архитектур, интеграции с современными технологиями, оптимизации производительности и регуляторных аспектов.

Эволюция протоколов VPN и их перспективы

Одним из фундаментальных аспектов развития VPN является эволюция протоколов, обеспечивающих шифрование и туннелирование трафика. Традиционные протоколы, такие как PPTP, L2TP/IPsec и IKEv2, имеют свои преимущества, но также уязвимости, связанные с блокировкой и слабым шифрованием [6]. Например, протокол L2TP/IPsec предлагает устойчивый алгоритм шифрования и встроенную поддержку в операционных системах, но сталкивается с проблемами при прохождении через брандмауэры [4]. Перспективным решением считается OpenVPN – протокол с открытым исходным кодом, обеспечивающий высокий уровень безопасности за счёт использования SSL/TLS для обмена ключами и поддержки аутентификации через сертификаты или пароли. Российские исследователи подчёркивают

гибкость настройки OpenVPN, позволяющую интегрировать его с другими технологиями для создания надёжных VPN-решений [1]. Ещё более инновационным является протокол WireGuard, использующий легковесные контейнеры и современные алгоритмы шифрования, такие как ChaCha20 и Curve25519. Он обеспечивает повышенную производительность и простоту развёртывания, что делает его идеальным для мобильных и распределённых сетей [9]. В будущем развитие протоколов будет направлено на интеграцию с постквантовыми криптоалгоритмами для защиты от квантовых компьютеров, а также на поддержку Perfect Forward Secrecy для генерации уникальных ключей на каждый сеанс. Российские учёные отмечают перспективность таких подходов в контексте банковских и корпоративных сетей, где технологии VPN демонстрируют высокую эффективность [2]. Анализ показывает, что комбинация OpenVPN и WireGuard станет стандартом для обеспечения безопасности в условиях блокировок интернет-ресурсов [1].

Распределенные и облачные архитектуры VPN

Перспективные решения VPN всё чаще ориентируются на распределённые системы, позволяющие масштабировать сети и повышать отказоустойчивость. В работе по созданию распределённой системы построения виртуальных защищённых каналов связи предлагается использовать Docker для автоматизации сборки контейнеров с VPN-серверами и Docker Swarm для их распределения по узлам [5]. Такая архитектура включает модули управления, мониторинга (Portainer) и балансировки нагрузки (Nginx), обеспечивая доступ к корпоративным ресурсам через защищённые соединения [10]. Преимущества распределённых VPN заключаются в минимизации рисков отказа, улучшении производительности за счёт балансировки и гибкой настройке параметров безопасности. Перспективы развития предусматривают интеграцию с дополнительными протоколами, системами логирования и хранения данных, что позволит адаптировать VPN к сложным инфраструктурам [7]. Это позволяет реализовать принцип Zero Trust, когда каждый запрос верифицируется независимо от источника [8]. Подобные решения особенно актуальны для

России, где с 2025 года вводятся ограничения на использование иностранного оборудования, стимулируя переход на отечественные аналоги.

Интеграция VPN с новыми технологиями

Интеграция VPN с инновационными технологиями открывает новые горизонты для обеспечения безопасности. Одним из перспективных направлений является комбинация с Интернетом вещей и SaaS-платформами, где VPN защищает от слабой аутентификации и перехвата трафика [6]. В условиях нестабильной геополитической обстановки VPN-сервисы позволяют обходить цензуру и обеспечивать конфиденциальность в России, где блокировки ресурсов становятся всё более актуальными [1]. Другое направление – применение искусственного интеллекта и нейронных сетей для анализа угроз. При проектировании защищённых сетей предлагается интеграция с системами обнаружения и предотвращения вторжений (IDS/IPS) и межсетевыми экранами нового поколения (NGFW) для глубокого инспектирования пакетов (DPI), что позволяет проактивно реагировать на атаки [8]. В специальных информационных системах, таких как мультисервисные сети связи, VPN интегрируется с протоколами MPLS и RSVP-TE для обеспечения требуемого качества обслуживания [7]. Это гарантирует безопасность в слабо защищённых средах с акцентом на аутентификацию и криптографию.

Регуляторные аспекты и переход на отечественные решения

Развитие VPN в России регулируется федеральными законами и указами, предусматривающими запрет на определённое иностранное оборудование с 2025 года [8]. Это стимулирует импортозамещение и ориентацию на сертифицированные ФСТЭК России средства. Приоритетным становится создание отечественных VPN-решений, интегрированных с национальными стандартами криптографии [4]. Учебные пособия российских авторов, в частности «Основы построения виртуальных частных сетей» Запечникова и др., подчёркивают необходимость совершенствования продуктов для решения проблем совместимости и безопасности [3].

Рекомендации по миграции корпоративных и государственных систем на отечественные VPN-решения

На основе проведённого многоаспектного анализа нормативных ограничений, а также с учётом требований к импортозамещению в сфере информационной безопасности, сформулирован комплекс следующих рекомендаций по миграции корпоративных и государственных информационных систем на отечественные VPN-решения:

1. Инвентаризация и аудит существующей VPN-инфраструктуры. Предлагается осуществить выявление и каталогизацию всех применяемых импортных VPN-компонентов (включая шлюзы, клиентское программное обеспечение и криптографические библиотеки), а также анализ критических сетевых сегментов, требований к пропускной способности, допустимым задержкам и показателям отказоустойчивости.

2. Выбор отечественного VPN-продукта с верифицированной совместимостью с национальными криптографическими стандартами. Обосновывается целесообразность выбора решений, включённых в реестр отечественного ПО (Минцифры России) и имеющих действующие сертификаты ФСБ России (например, «VipNet Coordinator», «Континент-4», «S-terra VPN»). Критически значимым условием является поддержка алгоритмов ГОСТ Р 34.10-2012 (электронная цифровая подпись), ГОСТ Р 34.11-2012 (хэш-функция), а также блочных шифров ГОСТ 28147-89 («Магма») и «Кузнечик».

3. Разработка поэтапного плана миграции при условии непрерывности предоставления сетевых сервисов.

Этап 1 (пилотирование): параллельное развёртывание отечественного VPN-шлюза с маршрутизацией части трафика в тестовом режиме.

Этап 2 (масштабирование): последовательное переключение удалённых филиалов и пользователей на отечественные клиентские приложения.

Этап 3 (завершение): демонтаж импортных компонентов после подтверждения штатной работоспособности и соответствия заявленным характеристикам производительности.

4. Обеспечение обратной совместимости в переходный период. Рекомендуется применение VPN-шлюзов с поддержкой двух стеков протоколов, позволяющих эмулировать интерфейсы импортных решений для устаревших клиентов. Для гетерогенных сред, включающих внешних контрагентов, сохраняющих использование импортных VPN, целесообразно использовать протоколы с возможностью согласования криптографических параметров.

5. Подготовка персонала и организация технической поддержки. Необходимо проведение программ повышения квалификации сетевых администраторов в части настройки отечественных VPN-средств (включая особенности управления сертификатами ГОСТ, интеграцию с Единой системой идентификации и аутентификации (ЕСИА)).

6. Мониторинг и аудит безопасности по завершении миграции. Предлагается внедрение систем анализа защищённости VPN-туннелей на предмет соответствия требованиям ФСТЭК России, а также регулярная проверка совместимости с отечественными ОС (Astra Linux Special Edition, Ред ОС) и изменениями нормативной базы (например, приказ ФСТЭК России № 21).

7. Документальное оформление процессов и формирование внутренних регламентов.

Завершающим этапом рекомендуется утверждение порядка подключения новых филиалов через отечественную VPN-инфраструктуру и разработка инструктивно-методических материалов для конечных пользователей по установке и эксплуатации отечественных VPN-клиентов.

Заключение

Таким образом, перспективные решения в сфере VPN-соединений направлены на повышение безопасности, масштабируемости и адаптивности. От эволюции протоколов (WireGuard) до распределённых систем на базе Docker и интеграции с искусственным интеллектом – эти инновации обеспечивают защиту в динамичном цифровом ландшафте. Дальнейшие исследования должны быть сосредоточены на постквантовой криптографии и автоматизации управления для противодействия будущим угрозам.

Список литературы:

1. Выбор технологии VPN в условиях блокировок ресурсов в сети Интернет // CyberLeninka. – 2023. – URL: https://cyberleninka.ru/article/n/vybor-tehnologii-vpn-v-usloviyah-blokirovok-resursov-v-seti-internet (дата обращения: 22.05.2026).

2. Гринёв А. В. Анализ корпоративной банковской сети, построенной с применением технологии VPN: дис. – URL: https://www.dissercat.com/content/analiz-korporativnoi-bankovskoi-seti-postroennoi-s-primeneniem-tekhnologii-vpn (дата обращения: 22.05.2026).

3. Запечников С. В., Милославская Н. Г., Толстой А. И. Виртуальные частные сети. Основы построения и применения. – 2006. – URL: https://cyberleninka.ru/article/n/17914693.pdf (дата обращения: 22.05.2026).

4. Защита компьютерных сетей на основе технологии Virtual Private Network // Молодой учёный. – URL: https://cyberleninka.ru/article/n/zaschita-kompyuternyh-setey-na-osnove-tehnologii-virtual-private-network (дата обращения: 22.05.2026).

5. Использование перспективных технологий для развития распределённых корпоративных сетей связи // Геосиб (CyberLeninka). – URL: https://cyberleninka.ru/article/n/ispolzovanie-perspektivnyh-tehnologiy-dlya-razvitiya-raspredelennyh-korporativnyh-setey-svyazi (дата обращения: 22.05.2026).

6. Использование технологии VPN для обеспечения информационной безопасности // CyberLeninka. – URL: https://cyberleninka.ru/article/n/ispolzovanie-tehnologii-vpn-dlya-obespecheniya-informatsionnoy-bezopasnosti (дата обращения: 22.05.2026).

7. Основы организации и управления VPN-сетями современных информационных систем специального назначения // CyberLeninka. – URL: https://cyberleninka.ru/article/n/osnovy-organizatsii-i-upravleniya-vpn-setyami-sovremennyh-informatsionnyh-sistem-spetsialnogo-naznacheniya (дата обращения: 22.05.2026).

8. Проектирование защищённой корпоративной сети с применением VPN // International Research Journal. – URL: https://cyberleninka.ru/article/n/proektirovanie-zaschischennoy-korporativnoy-seti-s-primeneniem-vpn (дата обращения: 22.05.2026).

9. Разработка и внедрение защищенного VPN-решения на базе WireGuard и Bitvise SSH Client // Международный научно-исследовательский журнал. – URL: https://research-journal.org/archive/8-158-2025-august/10.60797/IRJ.2025.158.18?ysclid=mpe1d37djb130020354 (дата обращения: 22.05.2026).

10. Современные VPN-сети // Научные труды КубГТУ. – 2023. – URL: https://elibrary.ru/item.asp?id=49204511 (дата обращения: 22.05.2026).

List of literature:

1.The choice of VPN technology in conditions of blocking resources on the Internet // CyberLeninka. – 2023. – URL: https://cyberleninka.ru/article/n/vybor-tehnologii-vpn-v-usloviyah-blokirovok-resursov-v-seti-internet (date of request: 05/22/2026).

2.Grinev A.V. Analysis of a corporate banking network built using VPN technology: dis. – URL: https://www.dissercat.com/content/analiz-korporativnoi-bankovskoi-seti-postroennoi-s-primeneniem-tekhnologii-vpn (date of request: 05/22/2026).

3.Zapechnikov S. V., Miloslavskaya N. G., Tolstoy A. I. Virtual private networks. Fundamentals of construction and application. – 2006. – URL: https://cyberleninka.ru/article/n/17914693.pdf (date of access: 05/22/2026).

4.Protection of computer networks based on Virtual Private Network technology // Young scientist. – URL: https://cyberleninka.ru/article/n/zaschita-kompyuternyh-setey-na-osnove-tehnologii-virtual-private-network (date of request: 05/22/2026).

5.The use of advanced technologies for the development of distributed corporate communications networks // Geosib (CyberLeninka). – URL: https://cyberleninka.ru/article/n/ispolzovanie-perspektivnyh-tehnologiy-dlya-razvitiya-raspredelennyh-korporativnyh-setey-svyazi (accessed: 05/22/2026).

6.Using VPN technology to ensure information security // CyberLeninka. – URL: https://cyberleninka.ru/article/n/ispolzovanie-tehnologii-vpn-dlya-obespecheniya-informatsionnoy-bezopasnosti (date of request: 05/22/2026).

7.Fundamentals of the organization and management of VPN networks of modern special-purpose information systems // CyberLeninka

8.. – URL: https://cyberleninka.ru/article/n/osnovy-organizatsii-i-upravleniya-vpn-setyami-sovremennyh-informatsionnyh-sistem-spetsialnogo-naznacheniya (accessed: 05/22/2026). Designing a secure corporate network using a VPN // International Research Journal. – URL: https://cyberleninka.ru/article/n/proektirovanie-zaschischennoy-korporativnoy-seti-s-primeneniem-vpn (date of request: 05/22/2026).

9.Development and implementation of a secure VPN solution based on WireGuard and Bitvise SSH Client // International Scientific Research Journal. – URL: https://research-journal.org/archive/8-158-2025-august/10.60797/IRJ.2025.158.18?ysclid=mpe1d37djb130020354 (accessed: 05/22/2026).

10.Modern VPN networks // Scientific papers of KubSTU. – 2023. – URL: https://elibrary.ru/item.asp?id=49204511 (date of request: 05/22/2026).