УДК 004.056

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ПРОТОКОЛОВ VPN (IPSEC VS OPENVPN VS WIREGUARD) ДЛЯ БЕЗОПАСНОЙ ПЕРЕДАЧИ ДАННЫХ

Пурус А.О., Голубев А.А, студенты гр.568403

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Чепикова В.В. – старший преподаватель

Аннотация. В работе представлен сравнительный анализ трех основных протоколов виртуальных частных сетей: IPsec, OpenVPN и WireGuard. Рассмотрены особенности их архитектуры, механизмы шифрования, производительность и удобство настройки. Выявлены сильные и слабые стороны каждого протокола, а также даны рекомендации по их применению в различных сценариях использования.

Ключевые слова. VPN, IPsec, OpenVPN, WireGuard, безопасность данных, сравнение протоколов, шифрование, производительность.

Введение

В современном цифровом мире защита передаваемых данных становится одной из приоритетных задач. Виртуальные частные сети (VPN) предоставляют возможность безопасного соединения между удаленными узлами через публичные сети, такие как Интернет [1]. На сегодняшний день существует множество протоколов VPN, каждый из которых имеет свои особенности, преимущества и недостатки. Наиболее распространенными являются IPsec, OpenVPN и WireGuard.

Цель данной работы – провести сравнительный анализ этих трех протоколов по ключевым критериям: безопасность, производительность, удобство настройки и совместимость. Результаты исследования помогут сделать обоснованный выбор протокола в зависимости от конкретных требований к защите данных и условиям эксплуатации.

Обзор протоколов VPN

IPsec (Internet Protocol Security) – это набор протоколов для защиты IP-трафика, который работает на сетевом уровне модели OSI [2]. Стандарт был разработан IETF (Internet Engineering Task Force) и включает два основных протокола: AH (Authentication Header) для аутентификации и ESP (Encapsulating Security Payload) для шифрования и аутентификации [6]. Для управления ключами используется протокол IKE (Internet Key Exchange), который прошел эволюцию от IKEv1 до более совершенного IKEv2 [10].

IPsec широко применяется в корпоративной среде для построения site-to-site VPN и обеспечивает высокий уровень безопасности [5]. Протокол имеет встроенную поддержку в большинстве операционных систем и сетевых устройств, что упрощает его внедрение в существующую инфраструктуру [2].

OpenVPN – это открытое программное решение, которое использует протоколы SSL/TLS для обеспечения безопасности [1]. В отличие от IPsec, OpenVPN работает на прикладном уровне и может использовать как TCP, так и UDP в качестве транспорта [9].

Ключевая особенность OpenVPN – его гибкость. Протокол может работать через любой порт, включая 443 (стандартный порт HTTPS), что позволяет обходить многие сетевые ограничения и межсетевые экраны [9]. OpenVPN поддерживает широкий спектр криптографических алгоритмов, включая AES-256-GCM, ChaCha20-Poly1305 и другие [5].

WireGuard – это современный протокол VPN, который появился в 2015 году и быстро завоевал популярность благодаря своей простоте и высокой производительности [4]. Протокол встроен непосредственно в ядро Linux и состоит всего из 4000 строк кода (для ядерной реализации), что значительно упрощает его аудит безопасности [8].

WireGuard использует современные криптографические алгоритмы: ChaCha20 для шифрования, Poly1305 для аутентификации, Curve25519 для обмена ключами и BLAKE2s для хеширования [4]. Такой ограниченный, но тщательно подобранный набор алгоритмов исключает возможность ошибочной конфигурации [5].

Сравнительный анализ

1. Безопасность. Все три рассматриваемых протокола обеспечивают высокий уровень безопасности при правильной настройке. Однако существуют важные различия в их подходах. IPsec предоставляет надежную защиту на сетевом уровне, используя проверенные временем механизмы шифрования [10]. Протокол поддерживает множество криптографических алгоритмов, включая AES-GCM, ChaCha20-Poly1305 и различные методы аутентификации [2]. Однако сложность конфигурации IPsec

может приводить к ошибкам, снижающим уровень безопасности [9]. OpenVPN, основанный на SSL/TLS, обеспечивает надежную защиту при использовании актуальных версий библиотеки OpenSSL [1]. В 2025 году исследователями были выявлены потенциальные уязвимости, связанные с атаками на начальный вектор инициализации (IV), однако для современных версий протокола разработаны эффективные методы защиты [3]. Основным преимуществом OpenVPN является возможность тонкой настройки параметров безопасности [5]. WireGuard отличается минималистичным дизайном и использованием только современных, проверенных криптографических примитивов [4]. Малый объем кода значительно снижает вероятность наличия необнаруженных уязвимостей [8]. Отсутствие необходимости в управлении сертификатами также упрощает безопасное развертывание [5]. Однако некоторые эксперты отмечают, что ограниченный набор криптографических алгоритмов может стать недостатком в случае обнаружения уязвимости в одном из них [4].

2. Производительность. Производительность VPN-протоколов критически важна для обеспечения комфортной работы пользователей и эффективной передачи данных. IPsec демонстрирует хорошую производительность благодаря работе на сетевом уровне и встроенной поддержке в ядре операционной системы [2]. При использовании аппаратного ускорения шифрования IPsec способен обеспечивать высокую пропускную способность, что делает его предпочтительным для site-to-site соединений [5]. OpenVPN традиционно считается наименее производительным среди рассматриваемых протоколов [5]. Это связано с тем, что он работает в пользовательском пространстве, что требует дополнительных копирований данных между ядром и пользовательским режимом [9]. Двойное шифрование (на уровне TLS и на уровне туннеля) также увеличивает вычислительную нагрузку на процессор [1]. WireGuard признан лидером по производительности [5]. Работа в ядре Linux в сочетании с оптимизированными алгоритмами шифрования позволяет достигать более высокой скорости передачи данных при меньшей задержке по сравнению с конкурентами [4]. Статистический характер протокола (отсутствие необходимости поддерживать постоянное состояние соединения) также положительно влияет на производительность [8].

3. Удобство настройки и эксплуатации. Сложность настройки VPN напрямую влияет на вероятность ошибок конфигурации и время развертывания. IPsec считается наиболее сложным в настройке протоколом [9]. Администратору необходимо определить политики шифрования, настроить обмен ключами, маршрутизацию и правила межсетевого экрана [2]. В больших корпоративных сетях это требует высокой квалификации специалистов [5]. OpenVPN предлагает баланс между гибкостью и сложностью. Настройка осуществляется через конфигурационные файлы и не требует глубокого понимания работы протоколов безопасности [1]. Наличие готовых шаблонов и скриптов упрощает развертывание [9]. Однако использование стороннего клиентского ПО может создавать дополнительные сложности [5]. WireGuard отличается максимальной простотой [4]. Для настройки требуется всего несколько строк конфигурации: указать приватный ключ, порт и список пиров с их публичными ключами и IP-адресами [8]. Отсутствие необходимости в управлении сертификатами и сложных протоколах обмена ключами делает WireGuard доступным даже для начинающих администраторов [5].

4. Совместимость и обход ограничений. Возможность работы в различных сетевых условиях критична для удаленного доступа.

IPsec может испытывать трудности при работе через NAT (трансляцию сетевых адресов) из-за использования фиксированных портов и протоколов [2]. Хотя современные реализации поддерживают NAT-Traversal, это добавляет сложности в настройку [10]. OpenVPN обладает наилучшей способностью обходить сетевые ограничения [9]. Возможность использования TCP-порта 443 позволяет маскировать VPN-трафик под обычный HTTPS, что делает его практически неотличимым для систем глубокого анализа трафика [1]. WireGuard использует только UDP и фиксированный порт (по умолчанию 51820), что может создавать проблемы в сетях с жесткими политиками файрвола [5]. Однако благодаря своей простоте и современной архитектуре, WireGuard успешно работает через NAT в большинстве случаев [4]. Сводные результаты сравнительного анализа представлены в таблице 1.

Таблица 1 – Сравнение характеристик протоколов VPN

Критерий	IPsec	OpenVPN	WireGuard
Уровень работы	Сетевой	Прикладной	Сетевой
Криптография	AES, ChaCha20 и др. [2]	AES, ChaCha20 и др.[2]	ChaCha20, Poly1305, Curve25519 (фиксированный набор) [4]
Производительность	Высокая [5]	Средняя [9]	Очень высокая [4]
Сложность настройки	Высокая [9]	Средняя [5]	Низкая [8]
Обход NAT/файрволов	Средний [10]	Отличный [1]	Хороший [4]
Поддержка платформ	Встроенная во все ОС [2]	Требует сторонний клиент [5]	Встроена в ядро Linux, клиенты для всех ОС [4]
Размер кодовой базы	Крупный	Крупный	Малый (~4000 строк) [8]

Заключение

Проведенный сравнительный анализ позволяет сделать вывод, что выбор протокола VPN зависит от конкретных требований и условий эксплуатации.

IPsec остается оптимальным выбором для корпоративных site-to-site соединений, где требуется надежность, стандартизация и встроенная поддержка в сетевом оборудовании [2]. Несмотря на сложность настройки, этот протокол предоставляет все необходимые механизмы для построения защищенных каналов между офисами и дата-центрами [5].

OpenVPN является универсальным решением, особенно подходящим для удаленного доступа в условиях строгих сетевых ограничений [9]. Возможность работы через порт 443 делает его незаменимым в странах с жесткой интернет-цензурой или в корпоративных сетях с ограниченным выходом в интернет [1].

WireGuard представляет собой будущее VPN-технологий [4]. Сочетание высокой производительности, современных криптографических алгоритмов и простоты настройки делает его лучшим выбором для большинства современных сценариев использования, особенно в облачных и IoT-средах [5]. Ожидается, что с расширением поддержки WireGuard в различных операционных системах и сетевых устройствах его популярность будет только расти [8].

Рекомендуется использовать WireGuard для новых проектов, требующих высокой производительности и простоты развертывания, OpenVPN – для обхода строгих сетевых ограничений, а IPsec – в корпоративных средах с существующей инфраструктурой, построенной на этом протоколе [5].

Список использованных источников:

1 noBGP. Compare VPN Protocols and an Alternative [Электронный ресурс]. – 2025. – Режим доступа: https://www.nobgp.com/info/compare-vpn-protocols. – Дата доступа: 21.03.2026.

2 Libreswan Project. Implemented Standards: IKE and IPsec RFCs [Электронный ресурс]. – 2025. – Режим доступа: https://libreswan.org/wiki/Implemented_Standards. – Дата доступа: 21.03.2026.

3 IETF. RFC 4301: Security Architecture for the Internet Protocol [Электронный ресурс]. – 2005. – Режим доступа: https://datatracker.ietf.org/doc/html/rfc4301. – Дата доступа: 21.03.2026.

4 IETF. RFC 7296: Internet Key Exchange Protocol Version 2 (IKEv2) [Электронный ресурс]. – 2014. – Режим доступа: https://datatracker.ietf.org/doc/html/rfc7296. – Дата доступа: 21.03.2026.

5 Telnyx. The Best VPN for IoT Security: OpenVPN vs. IPsec vs. WireGuard [Электронный ресурс]. – 2025. – Режим доступа: https://telnyx.com/resources/ipsec-vs-openvpn-vs-wireguard. – Дата доступа: 21.03.2026.

6 OpenVPN Inc. OpenVPN Reference Manual [Электронный ресурс]. – 2024. – Режим доступа: https://openvpn.net/community-resources/reference-manual-for-openvpn-2-6/. – Дата доступа: 21.03.2026.

7 WireGuard LLC. WireGuard Documentation [Электронный ресурс]. – 2025. – Режим доступа: https://www.wireguard.com/documentation/. – Дата доступа: 21.03.2026.

8 Donenfeld J.A. WireGuard: Next Generation Kernel Network Tunnel // Proceedings of the 2017 Network and Distributed System Security Symposium (NDSS). – San Diego, 2017. – P. 1-12.

9 OpenVPN Security Overview. OpenVPN Security Architecture [Электронный ресурс]. – 2024. – Режим доступа: https://openvpn.net/security-overview/. – Дата доступа: 21.03.2026.

10 WireGuard Security Audit. WireGuard Formal Verification and Security Audit Report [Электронный ресурс]. – 2020. – Режим доступа: https://www.wireguard.com/audit/. – Дата доступа: 21.03.2026.

UDC 004.056

COMPARATIVE ANALYSIS OF VPN PROTOCOLS (IPSEC VS OPENVPN VS WIREGUARD) FOR SECURE DATA TRANSMISSION

Purus A.O., Golubev A.A.

Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus

Chepikova V.V. – senior lecturer

Annotation. The paper presents a comparative analysis of three main virtual private network protocols: IPsec, OpenVPN and WireGuard. The features of their architecture, encryption mechanisms, performance and ease of configuration are considered. The strengths and weaknesses of each protocol are identified, as well as recommendations for their use in various usage scenarios.

Keywords. VPN, IPsec, OpenVPN, WireGuard, data security, protocol comparison, encryption, performance.