ТЕХНОЛОГИИ ВИРТУАЛЬНЫХ ЧАСТНЫХ СЕТЕЙ (VPN)

Столешников Никита Сергеевич
преподаватель,
Автономная Некоммерческая Организация Дополнительного Образования Академия ТОП,
Россия, г. Хабаровск

Сличная Ангелина Игоревна
Попов Арсений Юрьевич
студенты
Автономная Некоммерческая Организация Дополнительного Образования Академия ТОП,
Россия, г. Хабаровск

VIRTUAL PRIVATE NETWORK (VPN) TECHNOLOGIES

Stoleshnikov Nikita Sergeevich

Teacher, Autonomous Non-Profit Organization of Additional Education TOP Academy, Russia, Khabarovsk

Slichnaya Angelina Igorevna, Popov Arseniy Yurievich

Students, Autonomous Non-Profit Organization of Additional Education TOP Academy, Russia, Khabarovsk

АННОТАЦИЯ

Цель. Провести комплексный анализ современных технологий виртуальных частных сетей (VPN), их классификаций, протоколов и механизмов безопасности.

Метод. В работе использованы методы сравнительного анализа, обобщения технических характеристик, а также обзор отечественных и зарубежных источников по тематике информационной безопасности.

Результат. Рассмотрены принципы работы VPN, выделены основные протоколы (OpenVPN, WireGuard, L2TP/IPSec и др.), дана их сравнительная оценка по ключевым параметрам: безопасность, производительность, устойчивость и масштабируемость.

Выводы. Технологии VPN продолжают оставаться важным инструментом цифровой безопасности, активно развиваются в направлении интеграции с облачными сервисами, автоматизации и повышения устойчивости к внешним угрозам. Эффективное применение VPN требует не только выбора надёжного программного обеспечения, но и понимания архитектурных, криптографических и юридических аспектов.

ABSTRACT

Background. The aim of this study is to provide a comprehensive analysis of Virtual Private Network (VPN) technologies, including their classifications, protocols, and security mechanisms.

Methods. The research applies comparative analysis, synthesis of technical specifications, and a review of domestic and international sources in the field of information security.

Result. The paper outlines the operation principles of VPNs and compares major protocols such as OpenVPN, WireGuard, and L2TP/IPSec in terms of security, performance, resilience, and scalability.

Conclusion. VPN technologies remain a key element of digital security, continuously evolving towards integration with cloud platforms, automation, and improved resistance to external threats. Efficient

implementation requires not only robust software solutions but also a deep understanding of architectural, cryptographic, and legal considerations.

Ключевые слова: VPN; туннелирование; информационная безопасность; шифрование; протоколы; WireGuard; OpenVPN.

Keywords: VPN; tunneling; information security; encryption; protocols; WireGuard; OpenVPN.

Виртуальные частные сети (Virtual Private Networks — VPN) на сегодняшний день представляют собой одно из наиболее востребованных и гибких решений в области обеспечения информационной безопасности. Возрастающие риски утечки данных, необходимость работы в распределённых командах, а также потребность в обходе ограничений доступа сделали технологии VPN частью повседневной цифровой практики — как в бизнесе, так и в частной жизни [6, с. 328]. Изначально разработанные для удалённого подключения сотрудников к корпоративной инфраструктуре, современные VPN значительно расширили свой функционал и охват применения. Их ключевой задачей остаётся создание защищённого канала связи между двумя или более точками в сети, функционирующего поверх общего интернета.

Работа VPN основывается на механизме туннелирования: исходные пакеты данных инкапсулируются в другой протокол, шифруются и передаются через открытые сети, после чего на другой стороне соединения они расшифровываются и извлекаются. Это позволяет скрыть как содержимое трафика, так и сам факт обращения к определённым ресурсам, особенно если используются дополнительные меры по защите DNS-запросов и IP-адреса. В рамках одного соединения VPN выполняет сразу несколько функций: маскировку, шифрование, аутентификацию и контроль целостности. В совокупности это создаёт иллюзию прямого подключения к частной сети даже при физическом нахождении вне её пределов [2, с. 12].

Применение VPN невозможно без выбора конкретного протокола туннелирования. Наиболее известные среди них — PPTP, L2TP/IPSec, OpenVPN, IKEv2 и WireGuard — отличаются как по архитектуре, так и по уровню защищённости и скорости. Так, PPTP является устаревшим и практически не используется в современных системах из-за серьёзных уязвимостей. L2TP в сочетании с IPSec обеспечивает более надёжную защиту, но может быть чувствительным к настройкам межсетевых экранов. OpenVPN демонстрирует высокую гибкость, поддержку разных платформ и стабильность. WireGuard, разработанный в последние годы, сочетает в себе лаконичный код, простоту настройки и скорость работы, что делает его всё более популярным. IKEv2/IPSec особенно эффективно применяется в мобильных устройствах благодаря своей устойчивости к смене сетей и поддержке механизмов быстрой переаутентификации [7, с. 8].

Ключевыми характеристиками VPN являются:

— уровень шифрования и устойчивость к расшифровке;

— производительность (скорость соединения и латентность);

— устойчивость к обрыву связи;

— поддержка кроссплатформенности;

— масштабируемость и возможность централизованного управления.

В зависимости от задач и технических условий VPN может быть классифицирован по нескольким основаниям. По типу подключения различают VPN с удалённым доступом, ориентированные на подключение отдельных пользователей к защищённой сети, и VPN между узлами (site-to-site), объединяющие локальные сети в разных географических точках. По способу реализации можно выделить программные и аппаратные решения. Первые устанавливаются как ПО на серверах и клиентских устройствах, вторые реализуются с использованием маршрутизаторов

и специализированных шлюзов. Также различаются частные (корпоративные) и публичные (провайдерские) VPN — первые управляются конкретной организацией, вторые предоставляются в виде сервиса широкому кругу пользователей [3, с. 4].

Особое внимание при построении VPN-системы уделяется выбору алгоритма шифрования и способу аутентификации. Наиболее широко используется алгоритм AES с длиной ключа 256 бит, признанный международным стандартом для конфиденциальной передачи данных. В мобильных средах всё чаще применяется алгоритм ChaCha20, обладающий высокой скоростью и устойчивостью при меньшем потреблении ресурсов. Что касается аутентификации, то кроме традиционной проверки логина и пароля всё активнее внедряются сертификатные схемы, основанные на инфраструктуре открытых ключей (PKI), а также двухфакторная аутентификация с использованием токенов или одноразовых кодов [8, с. 61].

Актуальность оценки надёжности и эффективности VPN-протоколов обусловлена необходимостью выбора наиболее оптимального решения под конкретные задачи. Сравнение таких протоколов, как OpenVPN, WireGuard, L2TP/IPSec и IKEv2, показывает, что при формально схожей функциональности они реализуют разные архитектурные подходы. OpenVPN использует библиотеку OpenSSL и предоставляет богатые возможности настройки, однако требует значительных ресурсов при работе на старом оборудовании. WireGuard предлагает сжатую кодовую базу, упрощающую аудит безопасности, и демонстрирует высокую производительность даже при больших объёмах трафика. IKEv2 отличается низкой латентностью и устойчивостью к потере соединения, что делает его оптимальным для нестабильных мобильных сетей. Протокол L2TP/IPSec хоть и остаётся широко поддерживаемым, постепенно уступает позиции из-за чувствительности к сетевым фильтрам и недостаточной гибкости [4, с. 27].

При этом эффективность VPN нельзя оценивать без анализа сопутствующих компонентов безопасности. Методы шифрования, как уже отмечалось, варьируются от AES-256 до ChaCha20, и их выбор напрямую влияет на пропускную способность и устойчивость к криптоанализу. Ряд решений предлагает возможность выбора шифра, что позволяет балансировать между безопасностью и производительностью в зависимости от сценария использования. Аутентификационные механизмы в современных VPN-системах всё чаще уходят от паролей в пользу асимметричной криптографии и токенов, включая поддержку аппаратных ключей и протоколов OAuth [1, с. 23].

Кроме того, всё чаще акцент смещается на защиту от утечек, возникающих не столько из-за сбоев шифрования, сколько из-за некорректной маршрутизации, DNS-запросов вне туннеля или работы с нестабильными точками доступа. Для повышения устойчивости к подобным угрозам используются функции принудительной маршрутизации всего трафика через туннель, отказ от split-tunneling, а также так называемый Kill Switch — механизм, прерывающий соединение при обрыве VPN-канала.

Несмотря на все усилия, направленные на укрепление безопасности, технологии VPN не являются полностью защищёнными от уязвимостей. Распространённой проблемой остаётся уязвимость самого клиента — чаще всего по причине устаревшего программного обеспечения или ошибочной настройки. Кроме того, возможны целевые атаки на инфраструктуру провайдера VPN, а в некоторых странах государственные органы используют DPI (Deep Packet Inspection) для обнаружения и блокировки трафика, проходящего через VPN. В связи с этим при выборе решения необходимо учитывать не только технические параметры, но и репутацию и юрисдикцию поставщика услуг [5, с. 128].

Развёртывание VPN-сервера возможно как на базе Linux, так и на Windows Server. Наиболее часто используется OpenVPN на Linux, поскольку предоставляет гибкие настройки, высокую

стабильность и активную поддержку со стороны сообщества. Процесс установки включает создание криптографических ключей, настройку конфигурационного файла, активацию маршрутизации и брандмауэра, а также развёртывание клиентских конфигураций. На Windows Server используется служба RRAS (Routing and Remote Access Service), позволяющая настроить соединение с использованием L2TP или SSTP. Несмотря на то, что конфигурация на платформе Microsoft может быть менее гибкой, она подходит для организаций, уже использующих другие продукты экосистемы Windows [8, с. 59].

Что касается клиентской стороны, то здесь предпочтение отдается кроссплатформенным решениям. Для OpenVPN существует как консольный интерфейс, так и графические оболочки, включая OpenVPN GUI для Windows и Tunnelblick для macOS. WireGuard отличается особенно простой конфигурацией, доступной даже на мобильных устройствах. Для корпоративного использования рекомендуется централизованное развертывание с помощью групповых политик или систем управления конфигурациями.

VPN нашёл широкое применение в самых разных сферах. В корпоративной среде он используется для безопасного доступа сотрудников к внутренним ресурсам. Частные пользователи применяют VPN для защиты в общественных сетях Wi-Fi, а также для обхода цензуры и региональных ограничений контента. В журналистике, правозащите и IT-безопасности VPN становится неотъемлемой частью обеспечения анонимности и свободы коммуникации. В телемедицине VPN обеспечивает защиту персональных данных пациентов, а в сфере образования — доступ к внутренним сетям университетов [6, с. 328].

Оценка производительности VPN играет важную роль при его использовании в высоконагруженных системах. На скорость работы влияют как характеристики сети, так и сложность алгоритмов шифрования. Протокол WireGuard, благодаря минималистичному коду, показывает высокую пропускную способность и минимальные задержки, в то время как OpenVPN может оказаться более ресурсоёмким, особенно при использовании TLS. Критериями оценки являются время установления соединения, пропускная способность (throughput), задержка (latency), устойчивость к разрыву соединения и нагрузка на процессор. Все эти показатели должны учитываться при выборе технологии для конкретной задачи [9, с. 262].

Текущие тенденции развития рынка VPN демонстрируют смещение акцента в сторону более лёгких, гибких и «умных» решений. VPN всё чаще интегрируются в браузеры, антивирусы и корпоративные облачные платформы. Возрастает интерес к архитектурам SASE (Secure Access Service Edge), где VPN является лишь одним из компонентов, наряду с системами авторизации, мониторинга и фильтрации трафика. Отдельного внимания заслуживают разработки в области квантово-устойчивого шифрования, которые, по мнению специалистов, будут играть всё большую роль по мере развития квантовых вычислений.

Таким образом, можно заключить, что технологии VPN продолжают играть ключевую роль в обеспечении цифровой безопасности. Они эволюционируют вместе с угрозами, демонстрируя устойчивость и способность к адаптации. Будущее VPN, по-видимому, связано с дальнейшей автоматизацией, интеграцией в гибридные архитектуры и повышением интеллектуальности систем управления доступом. Для эффективного использования этих технологий необходим не только выбор надёжного программного обеспечения, но и комплексное понимание архитектурных, криптографических и правовых аспектов, связанных с передачей информации в цифровом пространстве.

Список литературы:

1. Авласевич Д. В. Технологии создания виртуальных частных сетей //Форум молодых ученых.

— 2020. — №. 3 (43). — С. 23-27.

2. Авласевич Д. В. Использование технологии VPN для обеспечения информационной безопасности //Форум молодых ученых. — 2020. — №. 3 (43). — С. 12-18.

3. Абдулхаликов М. А., Качаева Г. И. Уязвимости виртуальных частных сетей VPN //Вопросы обеспечения безопасности в киберпространстве. — 2022. — С. 3-5.

4. Алексеев В. В. Протоколы и методы реализации частных виртуальных сетей //Нейрокомпьютеры и их применение. — 2022. — С. 27-28.

5. Гостеева А. И., Истратова Е. Е. Сравнительный анализ технологий организации VPN-соединений //Программно-техническое обеспечение автоматизированных систем. — 2021. — С. 128-131.

6. Кузьмич А. А. и др. Анализ угроз информационной безопасности виртуальных частных сетей, построенных на базе сети MPLS //Состояние и перспективы развития современной науки по направлению «Информационная безопасность». — 2021. — С. 328-333.

7. Росляков А. В., Ефремов Д. А. Анализ технологии WireGuard для реализации VPN //Вестник связи. — 2022. — №. 12. — С. 8.

8. Сердюк В. Организация и технологии защиты информации: обнаружение и предотвращение информационных атак в автоматизированных систем предприятий. — 2022. — С. 51-67.

9. Черепанов А. С., Шарлаев Е. В. Современные протоколы для построения виртуальных частных сетей //Измерение, контроль, информатизация. — 2023. — С. 262-270.