МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
**«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИМЕНИ Н. Г. ЧЕРНЫШЕВСКОГО»**
Кафедра теоретических основ компьютерной безопасности и криптографии

ВИРТУАЛЬНЫЕ ЧАСТНЫЕ СЕТИ

АВТОРЕФЕРАТ ДИПЛОМНОЙ РАБОТЫ

студента 6 курса 631 группы
специальности 10.05.01 — Компьютерная безопасность
факультета КНиИТ
Ивановой Ксении Владиславовны

Научный руководитель
Старший преподаватель _____ А. А. Лобов

Заведующий кафедрой
д. ф.-м. н., профессор _____ М. Б. Абросимов

Саратов 2026

ВВЕДЕНИЕ

За последние два десятилетия виртуальные частные сети обрели большую популярность, толчком чему стала в том числе пандемия 2020 года, спровоцировавшая масштабный переход сотрудников на удаленную работу. Компаниям же пришлось решать проблему безопасного доступа к своим корпоративным ресурсам. Также востребованность VPN решений очень возросла в последнее время, на фоне введения локальных ограничений доступа к некоторым веб-ресурсам и приложениям большинство пользователей, начиная с совсем детского возраста и заканчивая старшим поколением, устанавливают любые доступные VPN-решения на свои устройства. Эта тенденция породила серьезную проблему безопасности, ведь VPN могут предоставлять вам бесплатное решение вашей проблемы, а взамен провайдеры могут мониторить ваш трафик, собирать метаданные и продавать ваши данные третьим сторонам, кроме всего перечисленного такие VPN могут содержать устаревшие криптографические алгоритмы, использовать слабые протоколы туннелирования, не применять механизмы защиты от утечек DNS и IP адресов, а также могут быть инфицированы вредоносным ПО. В связи с этим, важным является понимание устройства работы VPN технологии, ее особенностей и безопасности.

В ходе работы должны быть решены следующие задачи:

- познакомиться с базовой классификацией VPN;
- изучить ключевые составляющие работы VPN;
- рассмотреть детали реализации на примере наиболее известных протоколов;
- на основе изученных данных выбрать архитектуру для практической реализации VPN;
- реализовать виртуальную частную сеть.

1 Виртуальные частные сети

1.1 История появления VPN

Технология VPN возникла в 90-х годах как ответ на потребность бизнеса в безопасном соединении удалённых офисов без использования дорогостоящих выделенных линий. Первые решения, такие как протокол PPTP от Microsoft и L2F от Cisco, позволили создавать защищённые туннели поверх общедоступных сетей, инкапсулируя данные внутри стандартных пакетов. Это дало старт эпохе доступных корпоративных сетей, работающих через интернет.

Дальнейшее развитие привело к стандартизации безопасности с появлением IPsec, который стал фундаментом для большинства корпоративных VPN, обеспечивая шифрование на сетевом уровне. В 2000-х годах популярность набрал OpenVPN, предложивший гибкость SSL/TLS и работу в пространстве пользователя, что упростило обход блокировок и настройку. Этот период ознаменовался переходом от проприетарных решений к открытым стандартам с высокой криптостойкостью.

Современный этап развития характеризуется стремлением к минимализму и скорости, ярким представителем чего является протокол WireGuard. Он отказался от сложной архитектуры предшественников в пользу компактного кода и современной криптографии (ChaCha20, Curve25519). Новые протоколы ориентированы на мгновенное переключение между сетями и высокую производительность на мобильных устройствах.

В данном разделе была рассмотрена эволюция технологий VPN от первых попыток туннелирования PPP до современных легковесных протоколов. Показано, как индустрия двигалась от сложных аппаратных решений к гибкому программному обеспечению, повышая безопасность и скорость передачи данных.

1.2 Классификация VPN

Классификация VPN проводится по нескольким критериям, главным из которых является способ реализации: программный или аппаратный. Аппаратные шлюзы (Cisco, Juniper) обеспечивают высокую производительность благодаря специализированным чипам, но требуют значительных затрат. Программные решения (OpenVPN, WireGuard) более демократичны и могут быть развернуты на стандартных серверах, что делает их идеальными для малого бизнеса и частных лиц.

По назначению сети делятся на три основных типа: Remote Access (удаленный доступ сотрудников), Intranet (объединение офисов одной компании) и Extranet (доступ внешних партнеров). Также важно разделение на «защищенные» VPN, работающие через публичный интернет с шифрованием, и «доверенные» (например, MPLS), где безопасность гарантируется изоляцией трафика внутри сети провайдера с обеспечением качества обслуживания (QoS).

С технической точки зрения классификация опирается на уровень модели OSI. Протоколы могут работать на канальном уровне L2 (PPTP, L2TP), передавая кадры Ethernet, на сетевом уровне L3 (IPsec, IPIP), маршрутизируя пакеты, или на сеансовом уровне L4-L7 (SSL VPN). Выбор уровня определяет функциональность: от объединения локальных сетей в единый широковещательный домен до точечного доступа к веб-приложениям.

В разделе были проанализированы основные виды VPN, их архитектурные и функциональные различия. Было показано, что выбор конкретного типа VPN зависит от задач безопасности, бюджета и требований к сетевой топологии (доступ к приложениям или объединение сетей).

2 Составляющие элементы VPN сети

2.1 Архитектура клиент-сервер

Доминирующей моделью построения VPN является архитектура клиент-сервер, где центральный узел (сервер) управляет доступом, а удаленные устройства (клиенты) инициируют подключение. Сервер берет на себя задачи аутентификации, маршрутизации трафика и ведения логов. Клиентская часть отвечает за шифрование исходящих данных и поддержание туннеля в активном состоянии.

Процесс установления связи начинается с рукопожатия (handshake), в ходе которого стороны согласовывают алгоритмы шифрования и проверяют учетные данные. После успешной проверки сервер выделяет клиенту виртуальный IP-адрес внутри защищенной сети и передает необходимые маршруты. Весь трафик клиента (или его часть) начинает проходить через сервер, который выступает шлюзом в интернет или корпоративную сеть.

Такая централизация значительно упрощает администрирование: изменение политик безопасности на сервере мгновенно применяется ко всем клиентам. Однако она создает единую точку отказа, если сервер перегружен или недоступен, работа всей сети останавливается, а пропускная способность ограничивается шириной канала сервера.

В раздел описаны принципы работы классической централизованной модели VPN, были выделены её ключевые преимущества в виде простоты управления и недостатки, связанные с масштабируемостью и зависимостью от работоспособности центрального узла.

2.2 Система аутентификации

Система аутентификации обеспечивает верификацию субъектов доступа (пользователей и устройств) перед установлением защищенного туннелируемого соединения. В современных реализациях VPN процесс установления соединения разделяется на две части: аутентификация оконечного оборудовния и аутентификация пользователя.

Аутентификация — это первый рубеж обороны VPN, предотвращающий доступ посторонних лиц. Она включает в себя проверку как самого устройства (машинная аутентификация), так и пользователя. Для этого применяются пароли, предварительные ключи (PSK) или цифровые сертификаты X.509 в рамках

инфраструктуры PKI. Последний вариант считается наиболее надежным, так как компрометация пароля не дает доступа без наличия файла ключа.

В крупных корпоративных сетях управление доступом часто делегируется внешним системам через протоколы AAA (RADIUS, TACACS+). VPN-шлюз не хранит базу пользователей, а перенаправляет запросы в Active Directory или LDAP. Это позволяет централизованно управлять правами сотрудников, блокируя доступ при увольнении или смене роли без перенастройки VPN-серверов.

Современные протоколы, такие как WireGuard, меняют подход, используя криптографические ключи как единственный идентификатор (Identity-based authentication). Здесь нет традиционных логинов: если у пира есть правильный приватный ключ, соответствующий прописанному на сервере публичному ключу, он считается аутентифицированным. Это упрощает код и исключает сложные фазы согласования параметров.

В данном разделе были рассмотрены механизмы проверки подлинности субъектов в VPN. Описан переход от простых парольных методов к многофакторной аутентификации на основе сертификатов и криптографических ключей, обеспечивающих высокий уровень доверия.

2.3 Криптографические алгоритмы

Основой безопасности VPN является гибридное шифрование, сочетающее скорость симметричных алгоритмов и удобство обмена ключами асимметричных. Для передачи самого трафика используются быстрые симметричные шифры, такие как AES-256 или ChaCha20. Асимметричная криптография (RSA, Elliptic Curves) применяется на этапе установления соединения для безопасного согласования общего сессионного ключа.

Помимо конфиденциальности, критически важна целостность данных, защищающая от скрытой модификации пакетов в пути. Для этого используются коды аутентификации сообщений (HMAC) или режимы шифрования с аутентификацией (AEAD), такие как Poly1305. Они добавляют к каждому пакету цифровую подпись; если она не совпадает при расшифровке, пакет немедленно уничтожается.

Выбор конкретных алгоритмов влияет на производительность и безопасность. Например, ChaCha20-Poly1305 работает быстрее AES на мобильных процессорах без аппаратного ускорения, а Curve25519 обеспечивает ту же стойкость, что и RSA, при гораздо меньшей длине ключа. Современные VPN-

протоколы жестко фиксируют набор алгоритмов (cipher suites), чтобы исключить использование устаревших и уязвимых шифров.

В разделе описана роль криптографии в обеспечении конфиденциальности и целостности VPN-туннелей. Был сделан вывод о важности использования современных алгоритмов (AEAD, ECC) для защиты от атак и обеспечения высокой производительности

2.4 Туннелирование

Туннелирование представляет собой процесс упаковки пакетов одного протокола внутрь другого для передачи через транзитную сеть. В VPN исходный IP-пакет шифруется и помещается в поле данных (payload) транспортного пакета UDP или TCP. Для внешних наблюдателей это выглядит как обычный обмен данными между двумя узлами, содержимое которого скрыто.

Реализация туннелирования опирается на виртуальные сетевые интерфейсы: TUN (L3) и TAP (L2). TUN-интерфейс оперирует IP-пакетами и оптимален для маршрутизации и выхода в интернет, создавая минимальные накладные расходы. TAP-интерфейс эмулирует Ethernet-карту, позволяя передавать любые протоколы канального уровня, что необходимо для объединения удаленных сегментов сети в один мост (bridging).

Различия в реализации также касаются уровня исполнения: в пространстве пользователя (OpenVPN) или ядра (WireGuard, IPsec). Работа в userspace проще для разработки, но требует постоянного переключения контекста процессора, что снижает скорость. Реализация в ядре (Kernel space) обеспечивает максимальную пропускную способность, избегая лишних операций копирования памяти.

В этом разделе был разобран механизм инкапсуляции трафика и роль виртуальных интерфейсов TUN/TAP. Сделан вывод о том, что выбор типа интерфейса и уровня реализации напрямую влияет на производительность и функциональные возможности VPN-решения.

3 Угрозы безопасности и анализ популярных VPN

3.1 Безопасность использования

Чтобы устранить риски связанные с безопасностью использования доступных на рынке VPN-решений, необходимо учитывать дополнительные функции при выборе продукта. К ним относятся обязательные функции безопасности, установленные NSA-CISA:

- поддержка надежной аутентификации;
- надежные алгоритмы шифрования;
- использование антивирусного программного обеспечения и средств обнаружения и предотвращения вторжений;
- надежная защита по умолчанию для портов администрирования и обслуживания;
- поддержка цифрового сертификата;
- поддержка регистрации и аудита;
- возможность назначать адреса клиентам в частной сети, при этом все адреса остаются закрытыми.

Раздел был посвящен анализу ограничений безопасности VPN. Сделан вывод, что для полноценной защиты требуется комплексный подход: доверенный провайдер, правильная настройка клиента для предотвращения утечек и использование HTTPS.

3.2 Методы атак и уязвимости

Наиболее опасными для VPN являются атаки «Человек посередине» (MitM), когда злоумышленник получает доступ к процессу рукопожатия. Без строгой проверки сертификатов или ключей клиент может установить защищенное соединение с сервером хакера. Также актуальны атаки повторного воспроизведения (Replay Attacks), от которых защищаются с помощью временных меток и уникальных номеров пакетов (nonce).

Исторические уязвимости старых протоколов, таких как PPTP, показали опасность использования слабых алгоритмов хеширования (MS-CHAPv2). Современные угрозы часто направлены не на взлом шифра, а на реализацию протокола: переполнение буфера, ошибки в парсинге пакетов или DoS-атаки, истощающие ресурсы сервера бесконечными запросами на подключение.

Протокол WireGuard демонстрирует новый подход к защите, работая по

принципу «не отвечать, если не спросили». Он не реагирует на невалидные пакеты, делая сервер невидимым для сканеров портов. Это значительно снижает поверхность атаки по сравнению с традиционными решениями, которые активно отвечают на попытки рукопожатия ошибками, выдавая свое присутствие.

В разделе были классифицированы основные векторы атак на VPN-инфраструктур
Выделили, что современные протоколы проектируются с учетом прошлых ошибок (MitM, DoS), минимизируя возможность эксплуатации уязвимостей реализации.

4 Разработка VPN-решения

4.1 Архитектура

В дипломе разработана архитектура P2P (Peer-to-Peer) VPN, целью которой является создание прямой связи между клиентами без пропуска трафика через центральный сервер. Центральный узел (Signaling Server) используется исключительно для начальной координации: обмена IP-адресами и публичными ключами. Это решение устраняет узкое место в производительности и повышает приватность данных.

Для обеспечения прямой связи в условиях NAT (трансляции сетевых адресов) применяется техника UDP Hole Punching. Клиенты, находящиеся за домашними роутерами, одновременно отправляют пакеты друг другу, создавая временные записи в таблицах трансляции своих маршрутизаторов. Это позволяет установить прямой канал связи, даже если у обоих пользователей нет "белых"IP-адресов.

Программная часть реализована на языке Go с использованием библиотеки NaCl (box) для криптографии. Архитектура модульная: отдельно выделены компоненты работы с сетью, криптографическое ядро и логика управления тунелем. Такой подход обеспечивает кроссплатформенность и легкость поддержки кода, а также высокую скорость обработки пакетов благодаря многопоточности Go.

В этом разделе описана концепцию децентрализованной VPN-сети. Основной вывод заключается в том, что использование P2P архитектуры и техники Hole Punching позволяет создать масштабируемую и приватную сеть, снижая затраты на инфраструктуру ретрансляции трафика.

4.2 Реализация

Реализация клиента базируется на взаимодействии с виртуальным TUN-интерфейсом через библиотеку water. Программа работает в бесконечном цикле: считывает IP-пакеты из интерфейса, шифрует их и отправляет в UDP-сокет. В обратном направлении: получает данные из UDP, расшифровывает и пишет в TUN-интерфейс, откуда они попадают в операционную систему.

Важным элементом реализации является поддержание соединения (Keepalive). Поскольку UDP — протокол без состояния, а NAT-таблицы роутеров быстро очищаются от неактивных записей, программа периодически отправляет пу-

стые пакеты. Это поддерживает «дыру» в NAT открытой и гарантирует, что входящий трафик от партнера не будет заблокирован фаерволом.

Обработка ошибок и смена IP-адресов (Mobility) реализованы автоматически. Если партнер меняет сеть (например, переходит с Wi-Fi на LTE), программа обновляет его адрес назначения при получении первого корректно расшифрованного пакета с нового IP. Это обеспечивает непрерывность сессии без необходимости ручного перезапуска соединения.

Тестирование подтвердило полную работоспособность разработанного VPN-решения. Клиенты успешно устанавливали прямое соединение (P2P) через двойной NAT, используя сигнальный сервер только для обмена координатами. Проверка связности утилитой ping показала стабильное прохождение пакетов между виртуальными адресами 10.0.0.1 и 10.0.0.2.

Анализ pcap-файлов в Wireshark подтвердил надежность защиты данных. Весь перехваченный UDP-трафик был зашифрован и не поддавался анализу. Попытки модификации пакетов или повторной отправки старых дампов (Replay Attack) успешно блокировались клиентом, что подтвердило корректность работы криптографии и проверки целостности.

Система продемонстрировала способность к самовосстановлению. При разрыве связи или смене IP-адреса одного из пиров соединение восстанавливалось автоматически. Механизм Keepalive эффективно удерживал туннель в активном состоянии, предотвращая закрытие портов на NAT-устройствах при простое канала.

Заключение: Финальный раздел подвел итоги практической части работы. Был сделан вывод, что разработанное ПО успешно решает задачу создания защищенной децентрализованной сети, обеспечивая конфиденциальность, целостность данных и обход ограничений NAT.

ЗАКЛЮЧЕНИЕ

В ходе выполнения данной данной работы были достигнуты все поставленные цели и решены задачи исследования. Проведен всесторонний анализ технологии виртуальных частных сетей, который включет изучение базовой классификации VPN, ключевых компонентов их работы и подробное рассмотрение наиболее распространенных протоколов туннелирования.

На основе изученного теоретического материала было спроектировано и реализовано VPN-решение с использованием языка программирования Golang. В практической части работы была продемонстрирована: реализация составных компонентов базового VPN-решения, была достигнута работоспособность механизма UDP Hole Punching, позволяющего устанавливать прямое соединение между узлами за NAT без необходимости в центральном сервере-посреднике. Реализованное криптографическое решение на основе библиотеки NaCl Box обеспечивает надежное шифрование и расшифровку передаваемых данных с использованием современных криптографических алгоритмов.

Разработанная система демонстрирует практическую применимость изученных протоколов, а также подтверждает важность глубокого понимания принципов работы VPN-технологий для обеспечения информационной безопасности в современных условиях.