Минобрнауки России

Федеральное государственное бюджетное образовательное учреждение

высшего образования

**«САРАТОВСКИЙ национальный исследовательский  
ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ**

**Н. Г. ЧЕРНЫШЕВСКОГО»**

Факультет компьютерных наук и информационных технологий

УТВЕРЖДАЮ

Зав. кафедрой \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(ФИО)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(подпись, дата)

**Практика - учебная (научно-исследовательская работа)**

студента 3 курса, 341 группы, факультета КНиИТ

**Филиппенко Дмитрий Александрович \_**

(ФИО полностью, в родительном падеже)

вид практики: учебная ("Научно-исследовательская работа")

кафедра: кафедра информатики и программирования

(наименование кафедры)

курс: 3 .

(номер курса)

семестр: 5 .

(номер семестра)

продолжительность: с 02.09.2024 по 27.12.2024 .

(дата начала) (дата окончания)

Руководитель практики:

зав. кафедрой \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Огнева М. В. .

(должность) (подпись, дата) (ФИО)

**СОДЕРЖАНИЕ**

[ВВЕДЕНИЕ 3](#_Toc184674946)

[1. Обзор источников 5](#_Toc184674947)

[2. Принципы работы протоколов VPN 10](#_Toc184674948)

[3. Инструментальные аспекты разработки ПО 13](#_Toc184674949)

[СПИСОК ИСПОЛЬЗУЕМЫХ ИСТОЧНИКОВ 15](#_Toc184674950)

# **ВВЕДЕНИЕ**

В условиях стремительного развития информационных технологий и широкого распространения интернета вопросы безопасности и защиты персональных данных приобретают особую актуальность. Каждый день миллионы пользователей обмениваются данными в сети, подвергаясь рискам несанкционированного доступа, утечки информации и кибератак. Одним из эффективных решений для обеспечения конфиденциальности и защиты данных является использование виртуальных частных сетей (VPN).

VPN (Virtual Private Network) — это технология, позволяющая создать защищённое соединение между устройством пользователя и сервером через интернет. Основная задача VPN — шифрование передаваемых данных и скрытие реального местоположения пользователя, что обеспечивает защиту от перехвата данных, повышает конфиденциальность и анонимность в сети.

Актуальность изучения и внедрения VPN обусловлена возрастающим количеством угроз кибербезопасности, увеличением числа удалённых рабочих мест и ростом использования облачных технологий. VPN активно применяется для:

1. Защиты корпоративных данных при удалённой работе сотрудников;
2. Обеспечения безопасного доступа к локальным сетям из любой точки мира;
3. Защиты персональной информации при использовании общедоступных сетей Wi-Fi;
4. Обхода интернет-ограничений и цензуры.

Развитие технологий VPN способствует усилению уровня безопасности в цифровой среде, что особенно важно в условиях глобализации и цифровой трансформации общества. Это позволяет организациям минимизировать риски утечек данных и обеспечить устойчивость к кибератакам, а пользователям — сохранять конфиденциальность своей личной информации.

Цель НИР: исследование технологии виртуальных частных сетей (VPN), включая её архитектуру, принципы работы, основные протоколы и аспекты безопасности, а также разработка приложения для безопасного соединения с серверами с использованием технологии VPN.

Задачи НИР:

1. Изучить существующие технологии используемы для работы VPN и описать историю их развития
2. Разобрать основные принципы работы VPN, включая механизмы шифрования, туннелирования и авторизации.
3. Описать существующие технологии и средства для реализации практической части.

# **Обзор источников**

**Исторические аспекты**

VPN-технологии начали развиваться в конце 1990-х годов, когда компании стали искать способ безопасного подключения удалённых сотрудников к корпоративным сетям. Первым значительным этапом стал разработанный Microsoft протокол **PPTP (Point-to-Point Tunneling Protocol)**, который позволял устанавливать защищённые соединения поверх незащищённого интернета. Этот подход открыл возможности для удалённой работы и защиты корпоративных данных. [1]

Со временем VPN развивались, чтобы соответствовать новым угрозам. Например, появление шифрования на основе алгоритмов AES и внедрение более безопасных протоколов (IPSec, L2TP) стало ответом на уязвимости PPTP. В 2000-х годах начали использовать **OpenVPN**, а позднее появились новые протоколы, такие как **WireGuard** (2015), ставший революционным за счёт своей простоты и высокой скорости.

**Современные VPN** используют несколько основных технологий:

**Shadowsocks**: Протокол, созданный для обхода цензуры, использует прокси и шифрование. Основная особенность – легковесность и фокус на скрытности. Shadowsocks не совсем VPN в традиционном смысле, но отлично подходит для целей, связанных с обходом блокировок и минимизацией трафика. [2]

**WireGuard**: Новый и простой VPN-протокол, основанный на современных криптографических методах. Он предлагает высокую скорость соединения и простоту настройки.

**OpenVPN**: Универсальный протокол, работающий практически на всех устройствах и поддерживающий широкий выбор шифров. Хотя он сложнее в настройке, его надёжность делает его популярным выбором.

**IPSec/L2TP**: Старые, но проверенные временем технологии. Они часто используются для интеграции с сетевым оборудованием.

Каждый из этих протоколов имеет свои сильные и слабые стороны. Например, Shadowsocks прост и быстрый, но не предоставляет такой же защиты трафика, как WireGuard или OpenVPN. WireGuard фокусируется на минималистичности, что позволяет ему быть быстрее, но он пока не получил такую широкую поддержку, как OpenVPN. [2]

VPN стали неотъемлемой частью современного интернета, решая задачи:

1. Защиты данных в публичных сетях, таких как Wi-Fi в кафе или аэропортах.
2. Обхода интернет-цензуры в странах с ограниченным доступом к информации.
3. Удалённой работы с корпоративными данными, что особенно важно в эпоху пандемий и удалённой занятости.
4. Повышения анонимности, чтобы скрыть данные о местоположении и действиях пользователя.

VPN (Virtual Private Network) широко используется для обеспечения безопасности данных в корпоративной среде, включая банки, государственные учреждения и другие организации, где защита информации является приоритетом.

**Варианты использования VPN в организациях:**

**Удаленный доступ для сотрудников** VPN становится ключевым элементом для организаций, которые предоставляют своим сотрудникам возможность удаленной работы. С помощью VPN сотрудники могут безопасно подключаться к корпоративной сети из любой точки мира, обеспечивая конфиденциальность данных и защиту от потенциальных угроз в открытых сетях, таких как Wi-Fi в кафе или отелях. VPN создаёт зашифрованное соединение, что позволяет исключить перехват данных при передаче. Это особенно актуально для крупных корпораций и компаний с распределенными офисами.

**Для защиты конфиденциальных данных**, которые передаются между офисами компании или различными филиалами. Это особенно важно для таких секторов, как финансы, здравоохранение и телекоммуникации, где важна защита личных данных клиентов и сотрудников. VPN позволяет защитить трафик между филиалами и централизованными серверами, минимизируя риски утечек информации.

**Организации, которые обрабатывают чувствительные данные**, такие как финансовая информация, персональные данные сотрудников и клиентов, должны использовать VPN для защиты передачи этих данных. Это особенно важно для банков, страховых компаний и здравоохранительных организаций, которые обязаны соблюдать требования законодательства о защите данных (например, GDPR в Европе или HIPAA в США). VPN помогает зашифровать каналы связи, предотвращая перехват данных во время их передачи.

**VPN также применяется** для защиты данных, **передаваемых** между локальными серверами и облачными сервисами (например, Amazon Web Services или Microsoft Azure). Важно использовать VPN для безопасной связи с облачными сервисами, поскольку они могут быть уязвимы для атак, если данные передаются без шифрования.

**Готовые решения** для VPN в организациях:

**OpenVPN** OpenVPN — это бесплатное и популярное решение для создания защищенных VPN-сетей. Оно подходит для разных организаций, от небольших до крупных. Это открытое ПО, что дает гибкость в настройке, а также надежное шифрование данных. Его можно изучать и использовать на GitHub OpenVPN. [3]

**WireGuard** WireGuard — это новый и быстрый VPN-протокол, который известен своей простотой и высокой скоростью работы. Он использует современные методы шифрования и подходит для тех, кто ищет быстрое и безопасное решение. Документацию и код можно найти на GitHub WireGuard.

**Shadowsocks** — это инструмент для создания защищенных прокси-соединений, который стал популярен среди пользователей, которым нужно обходить блокировки и обеспечивать безопасность связи в условиях ограничений. Хотя Shadowsocks не является традиционным VPN, он может быть использован для туннелирования интернет-трафика через зашифрованные каналы. Это решение имеет легковесную архитектуру и хорошую производительность, но требует настройки на стороне как клиента, так и сервера. Shadowsocks используется в основном для обхода цензуры в странах с ограничениями на интернет-доступ. Исходный код доступен на GitHud ShadowSocks. [4]

**Cisco AnyConnect** — это коммерческое решение для удаленного доступа, которое используется многими крупными компаниями. Оно предлагает дополнительные функции безопасности и легко интегрируется с другими продуктами Cisco, но требует платной лицензии. Исходный код недоступен, но больше информации можно найти на официальном сайте Cisco.

**Palo Alto Networks GlobalProtect** от компании Palo Alto — это решение для защиты корпоративных данных и мониторинга безопасности. Оно используется крупными организациями и подходит для комплексной защиты сети, но оно также требует значительных затрат на покупку и поддержку. Описание решения можно найти на официальном сайте Palo Alto Networks.

**IPsec** — это один из старых и проверенных протоколов для создания безопасных VPN-соединений. Он часто используется в корпоративных решениях для защиты данных при передаче. Этот протокол поддерживается большинством устройств, но его настройка может быть более сложной.

Эти решения могут быть полезными для разных организаций в зависимости от их потребностей в безопасности, бюджета и технических возможностей. Shadowsocks, в частности, является хорошим вариантом для организаций, которым нужно быстро и эффективно обходить блокировки, но оно не заменяет полноценный VPN и больше ориентировано на определенные задачи, такие как обход цензуры и повышение анонимности.

# **Принципы работы протоколов VPN**

**Туннелирование** — это процесс создания виртуального канала или «туннеля» между клиентом (пользователем) и сервером через общедоступную сеть. Все данные, которые передаются между устройством пользователя и сервером, проходят через этот туннель. [5]

Когда пользователь подключается к VPN-серверу, создается защищенный туннель между его устройством и сервером. Этот туннель скрывает данные пользователя от внешнего мира.

Этот туннель может быть создан с использованием разных протоколов (например, OpenVPN, IPsec, WireGuard и другие). Протокол туннелирования определяет, как данные будут упаковываться и передаваться по сети.

Существует несколько видов туннелирования VPN, каждый из которых выполняет определенные функции в защите данных и настройке соединения:

**Раздельное туннелирование**. Метод, при котором VPN-туннель создается только для определенных сетевых соединений, в то время как другие остаются открытыми. Позволяет экономить на пропускной способности сети путем исключения передачи трафика. Однако это менее безопасный метод: информация, которая передается через обычное подключение к интернету, может быть украдена. [5]

**Полное туннелирование**. Метод, при котором весь сетевой трафик проходит через VPN-туннель. Этот метод обеспечивает большую степень безопасности, поскольку вся передаваемая информация защищена от внешних угроз. Однако может замедлить скорость соединения и использовать большую пропускную способность сети, чем раздельное туннелирование. [5]

**Алгоритмы шифрования**

Одно из главных условий VPN-технологии — это качественное шифрование данных для защиты пользовательской информации во время передачи через интернет. Традиционные стандарты включают в себя симметричное и асимметричное шифрование.

**Симметричное шифрование** использует один и тот же ключ для шифрования и дешифрования информации. В случае VPN-технологий, клиент и сервер обмениваются одним ключом шифрования, так что все передаваемые данные могут быть зашифрованы и дешифрованы с помощью него. Симметричное шифрование обеспечивает быстрое и эффективное шифрование данных, что делает его наиболее распространенным методом.

Однако симметричное шифрование является менее безопасным, чем асимметричное, поскольку использует один и тот же ключ. Если злоумышленник получит к нему доступ, все данные могут быть легко прочитаны. [6]

**Асимметричное шифрование**, напротив, использует два ключа — открытый и закрытый. Первый может распространяться свободно и используется для шифрования, в то время как второй — для дешифрования и является конфиденциальным.

Асимметричное шифрование обеспечивает более высокий уровень безопасности, чем симметричное. Однако является менее эффективным и зачастую требует больше ресурсов для шифрования и дешифрования данных. [7]

**Методов шифрований** множетсво, самые популярные алгоритмы: AES, ChaCha20, Blowfish и Twofish. В практической части будет использован именно AES, так как именно он был реализован в прошлой курсовой.

**Сертификатная аутентификация**

Создаётся свой центр сертификации, который выпускает пользовательские сертификаты. С помощью центра сертификации обеспечивается контроль за подключением пользователей к OpenVPN серверу. При окончании времени действия сертификата или его отзыве, доступ пользователя блокируется. Приватные ключи с установленным на них паролем, выпускаемые совместно с сертификатом обеспечивают безопасность от несанкционированного подключения к внутренним ресурсам.

**Приватные point-to-point ключи**

С точки зрения подключения к ресурсам компании только одного пользователя/сервера, используется схема с приватными ключами. На одном из хостов генерируется ключ, который является общим для сервера и клиента.

**Внешняя аутентификация пользователей**

Для упрощения контроля за подключением пользователей, вместо схемы со своим PKI, можно использовать схему [с внешней аутентификацией пользователей по логину/паролю](https://community.openvpn.net/openvpn/wiki/HOWTO#Usingalternativeauthenticationmethods). Данная схема удобна для аутентификации пользователей скажем по доменному логину/паролю. Для подключения к серверу в конфигурационный файл клиента добавляется сертификат сервера и ключ подписи передаваемых пакетов [HARDENING OPENVPN SECURITY](https://openvpn.net/community-resources/how-to/).

# **Инструментальные аспекты разработки ПО**

Для разработки собственного VPN-приложения необходимо учитывать как теоретические аспекты, так и практические инструменты.

**Язык программирования**

C/C++/C#

- Часто используются для разработки сетевых протоколов из-за их высокой производительности и низкого уровня абстракции.

- VPN-протоколы, такие как OpenVPN и WireGuard, написаны именно на этих языках.

- Подходят для создания высокопроизводительных VPN-серверов и клиентов. [8]

**Протоколы**

1. TLS/SSL - Основные технологии для шифрования соединений в OpenVPN и других протоколах.

2. IPSec - Популярный протокол для обеспечения безопасности на уровне IP.

3. SOCKS5 - Используется в Shadowsocks для маршрутизации данных через прокси. [9]

**Сетевые технологии**

1. Маршрутизация - Настройка маршрутов для перенаправления сетевого трафика через VPN.

2. NAT (Network Address Translation) - Часто используется для скрытия реальных IP-адресов клиентов за общим IP-адресом VPN-сервера.

3. DNS - Для предотвращения утечек DNS-запросов через публичные серверы, используют специальные DNS-серверы внутри VPN. [10]

**Протокол для разработки VPN**

Shadowsocks — это прокси-сервер с открытым исходным кодом, специально разработанный для обхода интернет-цензуры. Он поддерживает VPN-функциональность, обеспечивая шифрование и передачу данных через TCP и UDP. Shadowsocks отличается от традиционных VPN своей легковесностью, высокой скоростью и устойчивостью к блокировке. В этой работе подробно рассматривается, как Shadowsocks реализует сетевые функции и обеспечивает безопасность соединений.

**Shadowsocks** был разработан китайским программистом под псевдонимом Clowwindy в 2012 году. Изначально протокол создавался для обхода интернет-цензуры, а также для защиты приватности пользователей. В отличие от классических VPN, Shadowsocks является высокоспециализированным прокси-протоколом, нацеленным на скрытие интернет-активности пользователей через зашифрованные туннели, что позволяет избежать блокировок и фильтрации трафика. [4]

Работает на основе модели клиент-сервер. Клиентская программа Shadowsocks устанавливает соединение с сервером, расположенным за пределами заблокированной сети, и перенаправляет через него сетевой трафик. Схема взаимодействия построена на использовании протокола SOCKS5, который поддерживает различные типы трафика, включая HTTP, FTP и другие виды сетевых запросов. На стороне сервера Shadowsocks принимает зашифрованные пакеты данных от клиента, расшифровывает их и перенаправляет в интернет, а затем отправляет ответ обратно клиенту в зашифрованном виде.

Использует технику маскировки трафика, чтобы он выглядел как обычный HTTPS-трафик, что делает его менее заметным для систем глубокого анализа пакетов (Deep Packet Inspection, DPI), которые применяются интернет-провайдерами и государственными органами для блокировки прокси-сервисов и VPN. Shadowsocks не устанавливает постоянное соединение, как это делает VPN, а вместо этого подстраивается под каждую сессию, что делает его менее уязвимым для анализа.

Поддерживает современные симметричные алгоритмы шифрования, включая AES (Advanced Encryption Standard) и ChaCha20. Эти алгоритмы обеспечивают высокий уровень безопасности и быстродействия.

**ЗАКЛЮЧЕНИЕ**

В процессе работы были выполнены все поставленные задачи. Изучены технологии VPN, принципы работы, механизмы шифрования, туннелирования и авторизации. Рассмотрены основные протоколы, такие как OpenVPN и WireGuard. VPN как технология защиты данных имеет важное значение в современном цифровом мире, где вопросы конфиденциальности и безопасности информации становятся всё более актуальными.

Таким образом, разработка и внедрение приложений для безопасного соединения с серверами является актуальной и важной задачей, которая требует дальнейших исследований и совершенствования существующих решений. Полученные знания и навыки будут использованы в дальнейшем для реализации программы.

# **СПИСОК ИСПОЛЬЗУЕМЫХ ИСТОЧНИКОВ**

1. William Stallings Cryptography and Network Security. Principles and Practice. 7th ed. Global Edition [Текст] / William Stallings — 7. — : Pearson Education Limited, 2017 — 753 c. (дата обращения: 13.11.2024).
2. The Evolution of VPN Technology — Текст : электронный // techblog.sdstudio.top : [сайт]. — URL: https://www.paloaltonetworks.com/cyberpedia/history-of-vpn (дата обращения: 26.11.2024).
3. OpenVPN / [Электронный ресурс] // : [сайт]. — URL: https://github.com/OpenVPN (дата обращения: 27.11.2024).
4. ShadowSocks / [Электронный ресурс] // : [сайт]. — URL: https://github.com/shadowsocks (дата обращения: 28.12.2024).
5. Туннелирование / [Электронный ресурс] // : [сайт]. — URL: https://www.thewindowsclub.com/what-is-vpn-tunnel-tunneling-protocols (дата обращения: 28.11.2024).

6. Симметричные криптосистемы / [Электронный ресурс] // wikipedia : [сайт]. — URL: <https://ru.wikipedia.org/wiki/Симметричные_криптосистемы> (дата обращения: 20.11.2023).

7. Асимитричное шифрование / [Электронный ресурс] // kaspersky : [сайт]. — URL: <https://encyclopedia.kaspersky.ru/glossary/asymmetric-encryption/> (дата обращения: 20.11.2023).

8. C# / [Электронный ресурс] // : [сайт]. — URL: https://learn.microsoft.com/ru-ru/dotnet/csharp/ (дата обращения: 09.12.2024).

9. Протоколы сетевой безопасности / [Электронный ресурс] // : [сайт]. — URL: https://blog.skillfactory.ru/glossary/proksi/ (дата обращения: 05.12.2024).

10. DNS / [Электронный ресурс] // : [сайт]. — URL: https://skillbox.ru/media/code/dns-chto-eto-takoe-i-kak-eye-ispolzuyut/ (дата обращения: 04.12.2024).