2. Виртуальная частная сеть (VPN) — технология, которая позволяет установить безопасное подключение к сети Интернет.

При подключении к Интернету через VPN, программное обеспечение создает безопасное соединение между вашим устройством и удаленным VPN-сервером, шифруя ваши данные просмотра веб-страниц и скрывая ваш IP-адрес.

## 3. История VPN

## 1998 год – разработка приложений VPN, позволяющих осуществлять централизованный контроль со стороны пользователей.

## 1999 год – модель аутентификации, дополнительные средства для конфигурирования клиентов

## 2000 год – включение средств VPN в Windows2000

## В настоящее время технология вошла в фазу расцвета. Используются различные технологии и архитектуры с учетом потребностей конкретной сети.

## Использование общедоступной IP-сети для предоставления удаленного доступа к информации может (!) являться безопасным.

* История VPN-технологий начинается с 1996 года, когда сотрудник компании Microsoft — **Gurdeep Singh-Pall**, начал разработку «PPTP» — протокола однорангового туннелирования. Ну, а в 1999 году, данная спецификация стала доступна широким массам и со временем сильно ЭВОЛЮЦИОНИРОВАЛА.
* Хотя, изначально VPN-технологии использовали только крупные организации и корпорации. Виртуальные частные сети позволяли сотрудникам тех или иных компаний безопасно общаться и обмениваться конфиденциальными данными.
* Однако такая полезная технология, как VPN недолго пробыла в тени крупных компаний, т. к. со временем в сети Интернет появилась цензура, новые инструменты для хакерских атак и ужесточилась слежка со стороны государства. Ну и как следствие, все это привело к **мощному росту** рынка VPN-услуг.

## 4. Как работает VPN

Когда вы просматриваете веб-страницы без VPN, ваше соединение проходит прямо с вашего устройства на сервер, на котором размещен нужный веб-сайт или услуга.  
Чтобы отправить вам соответствующий контент, этот веб-сервер должен знать ваш IP-адрес.

Ваш IP-адрес — это уникальный идентификатор, который сообщает другим компьютерам, куда отправлять информацию, если они хотят, чтобы она дошла до вас.  
С вашим IP-адресом связано много личной информации. Он показывает ваше географическое местоположение и может использоваться для создания общей картины вашей активности в Интернете.

По этим причинам многие пользователи предпочитают скрывать свой IP-адрес с помощью VPN.  
Когда вы просматриваете веб-страницы с включенной VPN, ваше соединение всегда направляется на удаленный VPN-сервер, прежде чем оно перейдет к веб-серверу, на котором размещен нужный веб-сайт или служба.  
Когда веб-сервер отправляет вам информацию, он отправляет ее на VPN-сервер, который затем пересылает ее вам. Так просмотренные веб-сайты видят только запрос на подключение от VPN-сервера, передают информацию ему и не знают ваш настоящий IP-адрес.

## 5. Преимущества использования VPN

Три ключевых преимущества использования VPN:

* Маскировка вашего IP-адреса, чтобы скрыть или изменить ваше местоположение от посещаемых веб-сайтов.
* Шифрование веб-трафика для защиты данных при использовании незащищенного Wi-Fi.
* Предотвращение мониторинга вашей интернет-активности от интернет-провайдера и других третьих лиц.

## 6. Недостатки использования VPN

VPN не является универсальным решением для всех проблем с конфиденциальностью и безопасностью в Интернете. Основные недостатки использования VPN связаны с непониманием его ограничений.

О чем следует помнить:

* VPN не обеспечит вам полной анонимности.  
  Например, если вы вошли в личные учетные записи, такие как Facebook и Google, во время работы в Интернете, то не имеет значения, используете ли вы VPN. Эти компании смогут отслеживать вашу активность и связывать ее с IP-адресом вашего VPN-сервера.
* Безопасный VPN с высоким рейтингом стоит денег.  
  Некачественный VPN может допустить утечку вашей личной информации, например, раскрыть истинный IP-адрес или DNS-запросы.
* VPN почти всегда замедляет скорость вашего интернета.
* Использование VPN на мобильных устройствах увеличивает трафик.
* Некоторые онлайн-сервисы пытаются запретить клиентам использовать VPN.
* Многие VPN не могут обойти строгие веб-блокировки в странах с жесткой цензурой.

## 7. Для чего используют VPN

Виртуальная частная сеть используется для защиты вашей конфиденциальности в Интернете, безопасного просмотра в общедоступных сетях Wi-Fi и доступа к контенту, заблокированному или ограниченному в вашем географическом местоположении.

Семь популярных способов использования виртуальной частной сети:

1. Защита конфиденциальности в Интернете.

Без VPN ваш интернет-провайдер (ISP) может видеть все веб-сайты, которые вы посещаете.

Когда вы используете VPN, ваш веб-трафик шифруется при передаче с вашего устройства на частный сервер, поэтому третьим лицам намного сложнее следить за вашей активностью в Интернете.

1. Доступ к скрытому контенту.

Сайты используют IP-адрес для определения вашего физического местоположения и могут предлагать уникальный контент для разных стран.

VPN маскирует ваш личный IP-адрес и заменяет его IP-адресом в выбранной вами стране, что позволяет обойти географические ограничения и разблокировать «скрытый» контент.

1. Безопасность в общедоступных сетях Wi-Fi.

Службы VPN шифруют весь трафик, исходящий от вашего устройства.

Вы можете использовать VPN для защиты своих конфиденциальных данных в незащищенных сетях Wi-Fi.

1. Обход государственной цензуры.

Некоторые правительства контролируют использование Интернета и блокируют доступ к определенным веб-сайтам.

VPN позволит разблокировать веб-сайты и получить доступ к глобальному Интернету.

1. Избежание ограничения пропускной способности.

Некоторые интернет-провайдеры намеренно замедляют ваше интернет-соединение, чтобы избежать перегрузки сети.

Вы можете использовать VPN для шифрования своей активности в Интернете, что не позволит вашему интернет-провайдеру ограничивать скорость вашего Интернета.

1. Экономия денег при совершении покупок в Интернете.

Интернет-магазины могут использовать ваш IP-адрес для изменения цен на свои товары в зависимости от вашего местоположения.

Помимо защиты платежной информации, вы можете использовать VPN для подмены своего местоположения и поиска наиболее выгодных цен.

1. Подключение к виртуальной офисной сети.

Вы можете использовать VPN, чтобы подключить свое устройство напрямую к внутренней сети вашей компании.

## Алгоритмы шифрования

VPN используют шифрование, чтобы скрыть детали вашей активности в Интернете, когда они перемещаются между вашим устройством и VPN-сервером.

Наиболее часто используемые шифры в VPN-сервисах.

| Алгоритм шифрования | Описание |
| --- | --- |
| Advanced Encryption Standard (AES) | Один из самых безопасных шифров. Доступен с длиной ключа 128 и 256 бит. |
| Blowfish | Раньше он был шифром по умолчанию, используемым в большинстве VPN-подключений, но теперь его в значительной степени заменил AES-256. |
| ChaCha20 | Набирает популярность как единственный совместимый с протоколом WireGuard. Как и AES, ChaCha20 использует ключ длиной 256 бит, что считается очень безопасным. |
| Camellia | Шифр, очень похожий на AES с точки зрения безопасности и скорости. Считается, что даже при использовании опции меньшей длины ключа (128 бит) невозможно взломать с помощью атаки грубой силы, учитывая современные технологии. |

## Протоколы VPN

Протоколы VPN — это правила и процессы, которым следует ваше устройство, чтобы установить безопасное соединение с сервером VPN.

В зависимости от используемого протокола VPN будет иметь разные скорости, возможности и уязвимости. Большинство сервисов позволят вам выбрать, какой протокол вы хотите использовать в настройках приложения.

Приводим краткий обзор наиболее распространенных протоколов.

| Протокол | Описание |
| --- | --- |
| OpenVPN | Открытый исходный код. Считается безопасным и совместим практически со всеми устройствами с поддержкой VPN. |
| WireGuard | Подойдет пользователям мобильных VPN. Не так хорош в обходе брандмауэров, как другие протоколы VPN. |
| IKEv2/IPsec | Протокол с закрытым исходным кодом, который подходит, если вы используете VPN на своем мобильном телефоне и регулярно переключаетесь между WiFi и, например, 3G/4G. |
| SoftEther | Не поддерживается многими VPN-сервисами, но он быстр, безопасен и отлично подходит для обхода цензуры. |
| L2TP/IPsec | Более медленный протокол. Не рекомендуется выбирать его, если вы раскрываете личную информацию или используете VPN, которая публично делится своими ключами шифрования в Интернете. |
| SSTP | Хорошо взаимодействует с брандмауэрами, но имеет закрытый исходный код и потенциально уязвим для атак. |
| PPTP | PPTP работает быстро, потому что не защищает ваши данные. Устаревший, небезопасный протокол, который рекомендуют избегать. |