# Что такое виртуальные частные сети?

Виртуальные частные сети (VPN) - это технология, которая позволяет создавать

сетевые соединения типа “точка-точка”, поверх другой сети. Подключиться к

такой сети может только тот, кому предоставили к ней доступ, а весь трафик в

ней шифруется.

# Применение VPN

С помощью VPN можно объединить офисы одной компании, которые могут на-

ходиться в разных частях города, или даже в разных точках мира. Также с по-

мощью VPN можно изолировать или объединить отделы внутри компании. Во

время пандемии сотрудники часто работали из дома, и именно с помощью VPN

они могли получить доступ к сети своей организации, а соответственно к серви-

сам и всей документации. Такое соединение безопасно, данные сложно перехва-

тить, и даже если данные будут перехвачены, то их будет тяжело расшифровать.

С помощью VPN также можно получить доступ к сайтам, которые заблокиро-

ваны в стране. Сейчас в нашей стране есть некоторые социальные сети, к кото-

рым у нас нет доступа, но с помощью VPN можно получить доступ к ним. Также,

в путешествиях можно получать доступ к сайтам, которые заблокированы в тех

странах.

Еще с VPN можно создать безопасное подключение для использования в пуб-

личных сетях, то есть Ваши данные социальных сетей, банковских приложений,

и другая конфиденциальная информация не будет перехвачена злоумышленниками.

# Как использовать VPN

Чтобы подключиться к VPN сети нужно установить на свое устройство специ-

альную программу - VPN-клиент. Это самый простой способ, но в большинстве бесплатных сервисов выдается случайный IP-адрес, принадлежащий случайной стране, без возможности выбора. Это не самый безопасный способ, потому в таких сервисах владелец моет получить доступ к вашим данным, и передать их третьим лицам.

Второй способ подключения к VPN – настройки, необходимо зайти в настройки сети свой ОС, найти функцию подключения к удаленной сети, и ввести данные для аутентификации в сети.

# Как работает VPN

Виртуальная частная сеть является посредником между устройством пользо-

вателя и сетью(подключение типа “клиент-сервер”), или же она является ло-

кальной сетью с двумя маршрутизаторами(подключение типа “сервер-сервер”).

Клиент подключается к сети с помощью сервера доступа, который подключает-

ся к внешней, и к внутренней сети. В момент, когда вы подключаетесь к сети

VPN, система проверяет вашу сеть, и авторизует вас в своей сети, между ком-

пьютером пользователя и сервером создается зашифрованный канал, который

можно назвать своеобразным тоннелем. В этот момент IP пользователя меняет-

ся на IP сервера, откуда все данные передаются ресурсам, с которыми вы рабо-

таете. VPN-пакеты смешиваются с трафиком основной сети, а затем шифруют-

ся, чтобы сохранить конфиденциальность данных, которые передаются в дан-

ной сети. Чтобы виртуальная сеть работала, создаются специальные протоколы

типа TCP/IP, которые называются туннельными. Все точки сети поддерживают

несколько соединений с другими точками, но при этом они все являются изо-

лированными.

# Недостатки VPN

Прежде всего - низкая скорость подключения, потому что сеть чаще всего нахо-

дится на большом растоянии, а также весь трафик проходит шифрование.

Периодически сети разрывают подключение, из-за чего трафик выходит в

публичную сеть. Сами сети не умеют восстанавливать подлкючения, но многие

современные ОС имеют функцию переплдключения в случае разрыва.

На законодательном уровне тоже могут возникнуть проблемы. Не во всех

странах разрешен VPN, а трафик часто проходит через другие страны.

Многие сервисы имеют бесплатные возможности, но по-настоящему безопас-

ные VPN сервисы требуют платы за свои услуги. Также бесплатные провайдеры

могут отслеживать вашу активность в сети, так как они имеют доступ к своим серверам.