VPN VS PROXY VS TOR

Что из этого
реально защищает
вас в интернете?

VPN | PROXY | TOR

@lionsoulbatyshchikov

ЭТО НЕ ТАКАЯ ПРИВАТНОСТЬ, КАК ВЫ ДУМАЕТЕ.

VPN, proxy или Tor могут скрыть ваш IP-адрес, но это не делает вас полностью невидимым. Каждый инструмент работает по-своему — и у каждого есть ограничения.

ВАШ IP

Это ваш цифровой адрес. По нему можно определить ваше местоположение, ISP и многое другое.

МАРШРУТИЗАЦИЯ

Определяет, куда направляются ваши данные и кто может их увидеть.

ВИДИМОСТЬ

Разные инструменты скрывают разные части вашей активности.

АНОНИМНОСТЬ ≠ ПОЛНАЯ ПРИВАТНОСТЬ

Скрытый IP — это не то же самое, что полная анонимность.

ГЛАВНЫЙ ВЫВОД

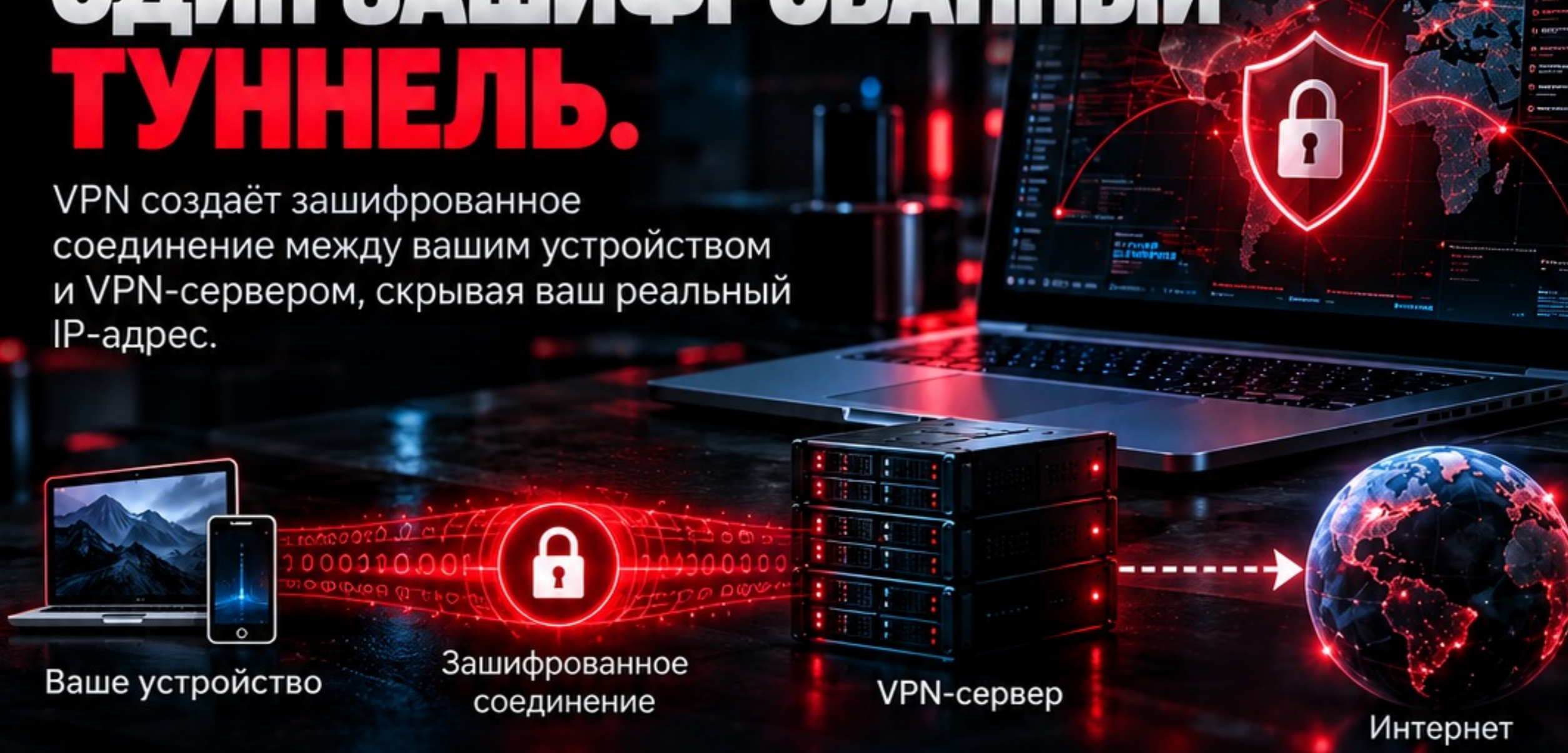
Эти инструменты повышают вашу приватность, но ни один из них не делает вас полностью анонимным.

@lionsoulbatyshchikov

VPN

ОДИН ЗАШИФРОВАННЫЙ ТУННЕЛЬ.

VPN создаёт зашифрованное соединение между вашим устройством и VPN-сервером, скрывая ваш реальный IP-адрес.



ЧТО СКРЫВАЕТ VPN

- Ваш реальный IP-адрес
- Ваше местоположение (для большинства сайтов)
- Ваш интернет-трафик (от вашего ISP)
- Вашу активность (в локальных сетях, например Wi-Fi)

КЛЮЧЕВЫЕ МОМЕНТЫ

- Шифрует ваш трафик (обычно с использованием AES-256).
- Использует VPN-сервер для маскировки вашего IP.
- Требует доверия к вашему VPN-провайдеру.

ЧЕГО VPN НЕ ДЕЛАЕТ

VPN не защищает от вредоносного ПО, фишинга или ваших действий в интернете. Ваш провайдер по-прежнему может видеть вашу активность, а некоторые сайты всё ещё могут вас отслеживать.

ГЛАВНЫЙ ВЫВОД

VPN повышает вашу приватность и безопасность соединения, но не делает вас **полностью анонимным**.

@lionsoulbatyshchikov

PROXY

ПОСРЕДНИК ДЛЯ ВАШЕГО СОЕДИНЕНИЯ.

Proxy выступает промежуточным звеном между вашим устройством и интернетом. Он пересылает ваши запросы, скрывает реальный IP (для поддерживаемого трафика) и подменяет его на свой.



КАК ЭТО РАБОТАЕТ

1. Устройство отправляет запрос на proxy-сервер.
2. Proxy пересылает его на нужный сайт или сервис.
3. Ответ приходит обратно через proxy к вам.

ЧТО СКРЫВАЕТ

- ✓ Ваш реальный IP-адрес (для поддерживаемого типа трафика).
- ✓ Ваше местоположение (в определённой степени).
- ✓ Вашу идентичность (в зависимости от типа proxy).

ТИПЫ PROXY

- **HTTP/HTTPS Proxy** (веб-трафик)
- **SOCKS Proxy** (более гибкий, поддерживает больше приложений)
- **Transparent Proxy** (не скрывает ваш IP)

ОГРАНИЧЕНИЯ

Proxy не всегда шифрует ваши данные. Соединение безопасно только если proxy поддерживает шифрование (например, HTTPS или SOCKS5).

ГЛАВНЫЙ ВЫВОД

Proxy даёт вам другой IP и помогает с маршрутизацией, но это не то же самое, что VPN.

@lionsoulbatyshchikov

TOR

НЕСКОЛЬКО РЕТРАНСЛЯТОРОВ. МНОГОУРОВНЕВОЕ ШИФРОВАНИЕ.

Tor направляет ваш трафик через три случайных ретранслятора (entry, middle и exit), используя многоуровневое шифрование на каждом этапе, чтобы скрыть ваш IP-адрес и местоположение.



1 ENTRY RELAY

Знает ваш IP-адрес, но не знает, куда вы идёте.

2 MIDDLE RELAY

Знает только предыдущий и следующий узел. Скрывает ваше местоположение.

3 EXIT RELAY

Знает ваш запрос (куда вы идёте), но не знает ваш реальный IP-адрес.

4 МНОГОУРОВНЕВОЕ ШИФРОВАНИЕ

На каждом узле снимается один слой шифрования, как у луковицы (onion).

ВАЖНО ПОМНИТЬ

Tor — это не просто VPN с дополнительными шагами. Он использует другой подход: маршрутизацию через несколько узлов с многоуровневым шифрованием.

КЛЮЧЕВЫЕ МОМЕНТЫ

- Обеспечивает более высокий уровень анонимности, чем VPN или обычные proxy (в большинстве случаев).
- Работает медленнее из-за нескольких узлов.
- Лучше подходит для приватности, а не для высокоскоростного серфинга.

@lionsoulbatyshchikov

VPN vs Proxy vs Tor
В чём разница?



Характеристика	VPN	Proxy	Tor
Скрывает ваш IP	**Да** (для сайтов)	**Обычно да** (для перенаправляемого трафика)	**Да** (для конечных сайтов)
Шифрование	Между устройством и VPN-сервером	Зависит от протокола (может не быть)	Многоуровневое шифрование внутри Tor
Анонимность	Ограниченная	Обычно ограниченная	**Выше** (по сравнению с VPN и многими proxy)
Скорость	Обычно высокая	Зависит (может быть высокой)	**Часто ниже** (из-за нескольких узлов)
Доверие	Доверие к VPN-провайдеру	Доверие к оператору proxy	Распределённая сеть ретрансляторов (нет единого оператора)

Главный вывод

Ни один инструмент не даёт полной анонимности. Важно понимать свои цели, настройки и модель угроз.

Стоит помнить

- Tor шифрует трафик внутри своей сети, но трафик на выходном узле может быть не зашифрован самим Tor.
- HTTPS остаётся важным во всех случаях.
- VPN смещает доверие от вашего ISP к VPN-провайдеру, а не устраняет его полностью.

@lionsoulbatyshchikov

СКРЫТЫЙ IP ≠ СКРЫТАЯ ЛИЧНОСТЬ.

Даже если вы скрываете свой IP, сайты всё равно могут распознавать вас по другим признакам. Ваш цифровой след намного шире, чем просто IP-адрес.

Cookies

Сайты могут узнавать ваш браузер при повторных посещениях.

Браузерный отпечаток

Характеристики вашего браузера и устройства могут быть уникальными и позволять вас идентифицировать.

Вход в аккаунты

Авторизация напрямую связывает вашу активность с вашей личностью.

Личная информация

Ваши действия в сети могут раскрывать дополнительные данные о вас.



ГЛАВНЫЙ ВЫВОД

Скрытие IP — это только один уровень приватности. Важно учитывать ваш онлайн-поведенческий профиль, устройство и модель угроз.

ПОМНИТЕ

Tor шифрует трафик внутри своей сети, но трафик на выходном узле может быть не зашифрован самим Tor. HTTPS остаётся важным во всех случаях.

@lionsoulbatyshchikov

Выбирайте инструмент под вашу задачу.

У каждого инструмента своя специализация.
Подбирайте решение под конкретные потребности,
а не просто «для галочки».



VPN

Когда выбирать:

- ✔ Нужна зашифрованная связь.
- ✔ Используете публичные или небезопасные сети (например, Wi-Fi).
- ✔ Доверяете VPN-провайдеру и готовы к тому, что трафик будет логироваться.

Proxy

Когда выбирать:

- ✔ Нужен доступ к конкретным приложениям или сервисам.
- ✔ Проводите тестирование, исследования или автоматизацию.
- ✔ Хотите скрыть свой IP (с ограниченным шифрованием).

Tor

Когда выбирать:

- ✔ Нужен высокий уровень анонимности в сети.
- ✔ Доступ к чувствительному контенту или ресурсам с ограничениями.
- ✔ Нужна более низкая скорость браузинга.

БЕЗОПАСНОЕ СОЕДИНЕНИЕ

МАРШРУТИЗАЦИЯ ТРАФИКА

БОЛЕЕ СИЛЬНАЯ АНОНИМНОСТЬ

Важно помнить

Ни один инструмент не гарантирует полной анонимности. Ваша безопасность зависит от правильной настройки и выбора модели угроз.

Ключевые моменты

- Tor шифрует трафик внутри своей сети, но выходной узел может быть не зашифрован самим Tor.
- VPN смещает доверие от вашего IP к провайдеру, а не убирает полностью следы.

@lionsoulbatyshchikov

ПРИВАТНОСТЬ — ЭТО НАВЫК.

Разбирайтесь в инструментах.
Понимайте их ограничения.
Защищайте свою цифровую личность.

@lionsoulbatyshchikov