

Что такое VPN на самом деле

Он меняет того, кто может тебя видеть, а не то, может ли кто-то вообще.

Проще говоря: VPN не дает твоему интернет-провайдеру или Wi-Fi в аэропорту видеть, куда ты подключаешься. Эта информация не исчезает: она передается компании VPN, которая теперь ее видит. То, что уже передавалось в зашифрованном виде, например почта или банк, было зашифровано и раньше. Он служит для нескольких конкретных задач, а продают его зачастую так, будто он решает гораздо больше.

Годами я слышал о VPN и не обращал на них внимания, как и на антивирусы: я не пользуюсь антивирусом, или почти никогда. У меня есть копии всего в трех местах в реальном времени, и я очень внимателен к тому, что скачиваю, по каким ссылкам перехожу и какие сайты посещаю. Это не стопроцентная безопасность, но мне этого хватает. Однажды я увидел предложение VPN чуть дороже двух евро в месяц и оформил подписку из любопытства. Работает хорошо, но пригодился мало: например, протестировать сервис, который тогда открывался только в США. Чувствую ли я себя в большей безопасности? Нет. Если мне снова предложат его по такой цене, возможно, продлю; если нет — нет. Это лишь мой опыт, он ничего не доказывает. Поэтому я спросил себя, что именно делает VPN. Вот как я это понял.

Представь, что ты опускаешь письмо в почтовый ящик с четко видимым адресом получателя. Почтальон видит, кому ты его отправляешь, даже если не может прочесть его, пока конверт запечатан. Этот почтальон — твой интернет-провайдер. VPN вкладывает твоё письмо в другой конверт, адресованный посреднику, который вскрывает его и пересылает дальше. Твой привычный почтальон больше не видит реального адреса. Он видит лишь то, что ты пишешь этому посреднику.

Тот, кто контролирует сеть, из которой ты подключаешься (например, Wi-Fi в аэропорту), перестает видеть, куда ты заходишь. Но посредник теперь видит то, что раньше видел твой провайдер, а иногда и больше, ведь весь твой трафик проходит через него. Слежка не исчезает: она переходит в другие руки. Отсюда и название.

Кроме того, почти все, что ты делаешь сегодня (например, проверяешь почту илиходишь в банк), уже передается в зашифрованном виде до конечного сервера благодаря замочку в браузере. Это происходит как с VPN, так и без него. VPN добавляет защиту только на первом участке — до своего собственного сервера. Оттуда путь остается прежним.

Поэтому есть вещи, которых он не может тебе обещать, даже если его иногда так преподносят. Если ты вошел в свою почту или в банк, этот сервис знает, что это ты, с VPN или без. Он также не гарантирует, что никто не смотрит твой трафик: меняется лишь тот, кто смотрит. Заявление компании о том, что она «не ведет журналы», — это обещание, точно такое же, как когда крупная платформа заявляет: «Ваши сообщения зашифрованы, мы их не читаем». Аудит может подтвердить это в конкретный момент, но это остается вопросом твоего доверия обещанию, а не тем, что невозможно нарушить архитектурно.

И содержание беседы остается прежним. Если твоё приложение для сообщений уже шифрует из конца в конец, VPN ничего не добавляет. Если нет — VPN это тоже не исправит: он защищает путь сообщения, а не то, что приложение или его сервер сделают с ним по прибытии.

Ничто из этого не делает его бесполезным. Скрыть место своего подключения от публичного Wi-Fi, от провайдера, желающего продать эту историю, или от страны, блокирующей сервис, — это реальная задача, и он справляется с ней хорошо. Маркетинг, правда, обычно обещает больше, чем этот уровень способен дать.

Вопрос, который стоит себе задать при использовании VPN или любого сервиса, обещающего защиту, звучит не «зашифровано ли это?». Скорее всего да, хотя бы на одном участке. Вопрос в другом: кому я вверяю то доверие, которое отнял у другого? И с чем я останусь, если оно окажется неоправданным?

VPN, когда он хорошо выполняет свою работу, лишь меняет посредника в твоём подключении. Такое приложение, как Solo2, чьи сообщения не проходят ни через один сервер, полностью убирает посредника из разговора. Они не соперничают: они решают совершенно разные задачи.

Путать их — очень распространённый способ считать себя более защищённым, чем ты есть на самом деле.

От редакции: когда в этих Cuadernos упоминаются компании или продукты, это делается не для того, чтобы кого-то обвинить. Те, кто их создает, делают работу, которой пользуются и которую ценят миллионы людей. Мы указываем на структурную проблему — модель, а не бренд. Бренды появляются в качестве примера, потому что они узнаваемы для читателя.

Источники и дополнительная литература

- Протокол HTTPS и транспортное шифрование являются открытыми стандартами, публично задокументированными IETF.
- В этой же серии: «Когда никого нет посередине» и «Вы не анонимны» раскрывают под другими углами то же самое различие между структурой и обещанием.

[← Предыдущий](#) [Ты не анонимен](#)

Недавние материалы

- [Размышление · 29 июня 2026 г. Ты не анонимен](#)
- [Размышления · 27 мая 2026 г. То, что подпись не может исправить](#)
- [Анализ · 26 мая 2026 г. Реальная vs мнимая конфиденциальность: вопросы, которые стоит себе задать](#)

Возьми эту статью с собой туда, где она тебе понадобится.

[↓ Markdown](#) [↓ Простой текст](#) [↓ PDF](#)

Файл будет загружен на твоё устройство. Оттуда ты можешь сохранить его, импортировать в Solo2 или поделиться им где угодно. Cuadernos не решает место назначения за тебя.

Сургучная печать · SHA-256 630c65bb55d790e0cc0c97ba53714aeb9c1eca8173271d5869a1ebe56adf7e8f
[Возможности](#) [Цены](#) [Установить](#) [Новости](#) [Блог](#) [Про](#) [Помощь](#) [О нас](#) [Контакты](#)
[Прозрачность](#) [Верификация](#) [Приватность](#) [Условия](#) [Файлы cookie](#)

Cuadernos Lacre · Издание [Menzuri Gestión S.L.](#) ·
текст R.Eugenio · под редакцией команды [Solo2](#).

Этот сайт не использует куки. Всё, что загружает твой браузер, написано или контролируется нами и размещено на наших европейских серверах: анонимный счетчик посещений (Umami, самостоятельно размещенный) и минимум JavaScript, необходимый для выбора языка и твоей настройки светлой/темной

темы, которая сохраняется на твоём собственном устройстве. Без сторонних ресурсов, без трекеров, без профилирования, без передачи данных. Если ты хочешь следить за нами: [RSS](#).