

Даниил Куприй



**Бесплатный VPN: ловушка
для миллионов**

Даниил Куприй

**Бесплатный VPN:
ловушка для миллионов**

«Автор»

2026

Куприй Д.

Бесплатный VPN: ловушка для миллионов / Д. Куприй —
«Автор», 2026

Вы скачали бесплатный VPN — и думаете что защищены. Но знаете ли вы на чём он зарабатывает? Спойлер: на вас. Вашей истории браузера, местоположении, данных. Именно так работают 70% бесплатных VPN-приложений. Но не всё так страшно — среди бесплатных есть нормальные варианты. Просто нужно знать как их найти. За час чтения вы научитесь проверять любой VPN за 2 минуты, читать политику конфиденциальности без скуки и выбирать защиту которая реально работает. Никакого технического жаргона. Только практика.

Содержание

Оглавление	5
Введение	6
Глава 1. Почему бесплатный VPN — это риск	7
1.1. Как зарабатывают бесплатные сервисы	7
1.2. Что на самом деле происходит с вашими данными	8
1.3. Реальные случаи утечек через бесплатные VPN	9
1.4. Платный против бесплатного — честное сравнение	10
Глава 2. Как работает VPN — простым языком	11
2.1. Что такое шифрование	12
Конец ознакомительного фрагмента.	13

Даниил Куприй

Бесплатный VPN: ловушка для миллионов

Оглавление

Введение

Глава 1. Почему бесплатный VPN — это риск

Глава 2. Как работает VPN — простым языком

Глава 3. Как проверить свой VPN за 2 минуты

Глава 4. Как читать политику конфиденциальности

Глава 5. Цифровая безопасность в 2026 году

Глава 6. Альтернативы и дополнения к VPN

Глава 7. Семь ошибок при выборе VPN

Глава 8. Как защитить смартфон

Глава 9. Безопасность для всей семьи

Глава 10. Что делать если уже стало плохо

Заключение и чек-лист

Введение

Представьте: вы сидите в кафе, пьёте кофе и листаете ленту. Или оплачиваете покупку в интернет-магазине. Или просто читаете новости. В какой-то момент вы вспоминаете что надо бы защититься и скачиваете первый попавшийся бесплатный VPN с красивым логотипом и тысячами отзывов. Звучит разумно. Но именно в этот момент вы, возможно, открываете дверь для тех, от кого хотели защититься.

История которую я слышал не раз: человек скачал бесплатный VPN с миллионом загрузок и четырьмя звёздами в магазине приложений. Приложение выглядело профессионально — красивый интерфейс, обещания анонимности и защиты. Через месяц начали приходить странные письма — именно на тот email который он использовал только для одного сервиса. Потом попытки войти в его аккаунты. Потом звонки от "банка" с подозрительными вопросами. Данные утекли через то самое приложение которое должно было его защищать. Совпадение? Вряд ли.

Каждый месяц почти два миллиона россиян вводят в поиск слова "бесплатный vpn". Это огромное количество людей которые хотят защитить свои данные. Желание абсолютно правильное. Но большинство из них выбирают не то что нужно — просто потому что не знают на что смотреть и чем руководствоваться при выборе.

Исследования показывают: более 70% бесплатных VPN-приложений передают данные пользователей третьим сторонам. Другое масштабное исследование проверило 283 бесплатных VPN-приложения для Android и обнаружило что 75% использовали библиотеки для скрытого отслеживания пользователей, 38% содержали признаки вредоносного кода, а 84% допускали утечку данных. То есть из десяти бесплатных VPN восемь так или иначе подводят своих пользователей.

Но вот в чём дело: не все бесплатные VPN одинаково опасны. Среди них действительно есть нормальные варианты — сервисы которые зарабатывают честно и не продают ваши данные. Просто нужно знать как их найти и как отличить от опасных. И именно этому посвящена эта книга.

Эта книга написана для обычных людей — не для программистов и не для специалистов по кибербезопасности. Здесь нет сложных технических терминов и формул. Только практика, только конкретные шаги которые вы можете сделать прямо сейчас.

За час чтения вы узнаете: почему бесплатный VPN зарабатывает именно на вас и как именно это происходит, как работает VPN изнутри простым языком, как проверить свой VPN на безопасность прямо сейчас за 2 минуты, что такое политика no-logs и почему это первое что нужно искать, как читать политику конфиденциальности быстро и без скуки, что изменилось в цифровой безопасности в 2026 году, какие альтернативы и дополнения к VPN существуют, и какие 7 ошибок при выборе VPN совершают почти все.

Никакого технического жаргона. Никакой воды. Только то что реально нужно знать чтобы защитить себя в современном интернете.

Глава 1. Почему бесплатный VPN — это риск

1.1. Как зарабатывают бесплатные сервисы

Давайте начнём с простого и очень важного вопроса: если сервис бесплатный — на чём он зарабатывает? Это не риторический вопрос. За каждым бесплатным VPN стоит компания с реальными расходами.

Серверы в десятках стран мира — это огромные суммы аренды ежемесячно. Один хороший сервер в Европе или США стоит несколько сотен долларов в месяц, а для нормального сервиса нужны десятки и сотни серверов. Команда разработчиков, дизайнеров и специалистов по безопасности получают зарплаты. Техническая поддержка работает круглосуточно. Трафик через серверы тоже стоит денег. Всё это складывается в многомиллионные расходы в год.

И вот перед владельцами бесплатного VPN стоит простой выбор: либо найти способ зарабатывать на пользователях, либо закрыть бизнес. Большинство выбирают первое. И если вы не платите деньгами — вы платите данными.

Вот конкретные способы которыми бесплатные VPN зарабатывают на своих пользователях. Первый и самый распространённый — продажа истории браузера рекламодателям. Каждый сайт который вы посещаете, каждый поисковый запрос, каждая страница которую вы читаете — это ценная информация для маркетологов. Знает рекламодатель что вы искали симптомы определённой болезни — продаст вам лекарства. Знает что смотрели цены на автомобили — покажет рекламу автосалонов.

Второй способ — показ навязчивой рекламы прямо внутри приложения. Это самый честный из нечестных способов монетизации — вы хотя бы знаете что происходит. Но постоянная реклама раздражает и замедляет работу.

Третий способ — передача данных третьим компаниям: аналитическим агентствам, страховым компаниям, рекрутинговым платформам, кредитным бюро. Ваши данные о поведении в интернете стоят серьёзных денег на рынке информации.

Четвёртый способ — внедрение скрытых трекеров в ваш браузер. Эти маленькие программы следят за вами даже когда VPN выключен — и продолжают собирать данные постоянно, незаметно для вас.

Пятый способ — использование мощности вашего устройства и интернет-соединения для своих нужд. Некоторые бесплатные VPN превращают устройства пользователей в часть своей инфраструктуры — фактически используя ваш телефон или компьютер как сервер для других пользователей без вашего ведома.

Это не заговор и не исключение из правил. Это просто бизнес-модель. Ровно как социальные сети и бесплатные почтовые сервисы зарабатывают на внимании и данных пользователей. Разница в том что VPN вы используете именно тогда когда хотите защититься. И если ваш защитник сам продаёт информацию о вас — это серьёзная проблема.

1.2. Что на самом деле происходит с вашими данными

Когда вы подключаетесь к любому VPN-серверу, весь ваш интернет-трафик проходит через него. Это означает что VPN-провайдер технически может видеть всё: какие сайты вы посещаете, когда и как часто, сколько времени проводите на каждом, что скачиваете, с кем общаетесь в мессенджерах если они не используют сквозное шифрование.

Что конкретно могут собирать бесплатные VPN: IP-адрес вашего устройства — это ваш цифровой адрес по которому вас можно идентифицировать в интернете; временные метки подключений — когда именно вы выходили в интернет и на сколько; объём переданного трафика — сколько данных вы передавали и получали; DNS-запросы — это фактически полный список всех сайтов которые вы посещали; в худших случаях — полный контент вашего трафика если сайты не используют собственное шифрование HTTPS.

Хороший платный VPN с честной политикой no-logs не хранит ничего из этого списка. Технически он не может предоставить эти данные даже если его об этом попросят — потому что их просто не существует на серверах. Бесплатный VPN — может хранить всё. А дальше эти данные анализируются, сегментируются и продаются. Вы никогда не узнаете что это произошло — уведомлений вам никто не пришлёт.

Последствия могут быть очень конкретными: повышение цены на авиабилеты потому что система знает что вы ищите их повторно; отказ в кредите потому что анализ поведения в интернете показал риск; навязчивая реклама именно тех вещей о которых вы недавно думали; в худших случаях — кража аккаунтов и финансовые потери.

1.3. Реальные случаи утечек через бесплатные VPN

Это не теория. Исследователи безопасности регулярно публикуют результаты проверок популярных бесплатных VPN — и результаты часто шокирующие.

Исследование австралийского университета CSIRO стало одним из самых известных в этой области. Учёные методично проверили 283 бесплатных VPN-приложения для Android. Результаты оказались тревожными: 75% приложений использовали сторонние библиотеки для отслеживания пользователей, 38% содержали признаки вредоносного кода, 84% допускали утечку данных пользователей, 18% вообще не шифровали трафик — несмотря на громкие заявления о защите и безопасности.

Другой показательный случай: популярное бесплатное VPN-приложение с десятками миллионов загрузок и высоким рейтингом оказалось создано компанией связанной с иностранными структурами. Приложение собирало детальную информацию о пользователях и отправляло её на удалённые серверы. Компания это отрицала — но исследователи доказали факт передачи данных технически, проанализировав сетевой трафик самого приложения.

Ещё одна распространённая проблема — бесплатные VPN которые заявляют о шифровании и анонимности но используют устаревшие или намеренно ослабленные алгоритмы. Такой VPN создаёт иллюзию защиты — но реально не защищает практически ни от чего. Пользователь думает что в безопасности, а на самом деле открыт для атак.

Важный урок из всего этого: красивое приложение с миллионом загрузок и пятью звёздами не означает безопасность. Звёзды легко накрутить — стоимость тысячи фейковых отзывов смехотворна для компании которая зарабатывает на продаже данных. Настоящая безопасность проверяется независимым техническим аудитом, а не маркетинговыми обещаниями.

1.4. Платный против бесплатного — честное сравнение

Сразу скажу честно: не все платные VPN тоже одинаково хороши. Среди них тоже встречаются сомнительные сервисы которые не выполняют своих обещаний. И наоборот — есть бесплатные варианты которые заслуживают доверия и работают честно. Но в целом разница между качественным платным и среднестатистическим бесплатным VPN очень значительная.

Хороший платный VPN стоит от 100 до 300 рублей в месяц при оплате на год. Это буквально меньше одной чашки кофе в кафе. За эти деньги вы получаете честную политику `logs` которая подтверждена независимым аудитом, современные протоколы шифрования без намеренных уязвимостей, быструю скорость соединения без искусственных ограничений, стабильную работу серверов 24/7 без неожиданных отключений, Kill Switch который защищает данные при разрыве соединения, реальную техническую поддержку которая помогает решить проблемы, и регулярные независимые проверки безопасности которые подтверждают честность сервиса.

Если вы серьёзно относитесь к защите своих данных — качественный платный VPN это не роскошь, а разумная инвестиция в собственную безопасность. Но если бюджет ограничен — в следующих главах мы подробно разберём как выбрать безопасный бесплатный вариант используя конкретные критерии проверки.

Глава 2. Как работает VPN — простым языком

Прежде чем выбирать VPN нужно понять как он работает. Не на глубоком техническом уровне — а на уровне "что конкретно происходит с моими данными когда я нажимаю кнопку включить". Это понимание поможет осознанно оценивать любой VPN-сервис и задавать правильные вопросы.

2.1. Что такое шифрование

Представьте что вы хотите передать другу секретное письмо через публичную почту. Вы можете написать его обычным языком — и любой кто перехватит письмо всё прочитает. Или вы можете написать его тайным кодом который понятен только вам двоим — и перехватчик увидит лишь бессмысленный набор символов.

Шифрование — это именно такой тайный код для ваших данных в интернете. Когда вы включаете VPN, все данные которые покидают ваше устройство сначала превращаются в зашифрованный поток. Этот поток идёт через интернет до VPN-сервера. Там расшифровывается и отправляется дальше к нужному сайту. Обратный путь — тоже через шифрование.

Современное шифрование настолько надёжно что взломать его перебором всех возможных вариантов не смог бы даже суперкомпьютер работающий миллиарды лет. Это не преувеличение — это математика. Алгоритмы которые используют хорошие VPN созданы именно с таким запасом прочности.

Конец ознакомительного фрагмента.

Текст предоставлен ООО «Литрес».

Прочитайте эту книгу целиком, [купив полную легальную версию](#) на Литрес.

Безопасно оплатить книгу можно банковской картой Visa, MasterCard, Maestro, со счета мобильного телефона, с платежного терминала, в салоне МТС или Связной, через PayPal, WebMoney, Яндекс.Деньги, QIWI Кошелек, бонусными картами или другим удобным Вам способом.