

Когда речь идет о выборе VPN, важно помнить о двух ключевых факторах, которые определяют, насколько подходящий этот сервис для вашей конфиденциальности. Это:

1. Политика отсутствия логов (No-logs policy)

Это основа, которая гарантирует, что VPN-сервис не будет отслеживать или хранить вашу активность в сети. Это критически важно для анонимности.

2. Юрисдикция компании

Страна, в которой зарегистрирован VPN-поставщик, играет важную роль. Если сервис работает в странах с жесткими законами по хранению данных или в странах, входящих в международные альянсы по обмену разведывательной информацией, это может стать угрозой для вашей безопасности.

Важно: В первую очередь, отсекаем сервисы, которые не соответствуют этим двум критериям. Когда мы уже сузили выбор, стоит обратить внимание на использование современных технологий шифрования и репутацию самого сервиса.

Что важно знать о шифровании?

Для обеспечения безопасности данных оптимальным выбором является использование протоколов **WireGuard**.

Он считается самым быстрым и безопасным на данный момент. Протоколы **OpenVPN** и **IKEv2/IPSec** также достойны внимания, но WireGuard — это тот, который заслуживает доверия и на который стоит опираться в вопросах конфиденциальности. OpenVPN, IKEv2/IPSec и WireGuard — кратко по факту.
(<https://telegra.ph/OpenVPN-IKEv2IPSec-i-WireGuard-kratko-po-faktu-12-13>).

Рейтинг VPN-сервисов по безопасности

1. ProtonVPN

Страна: Швейцария (не входит в альянсы 5/9/14, что означает, что она не обязана передавать данные третьим странам).

Политика конфиденциальности: ProtonVPN заявляет о строгой политике отсутствия логов. Подробнее можно ознакомиться с политикой конфиденциальности здесь (<https://protonvpn.com/privacy-policy>).

Аудит: Компания прошла независимый аудит безопасности, результаты которого доступны по ссылкам:

- Аудит для iOS (<https://protonvpn.com/files/proton-vpn-ios-app-audit-report-2020.pdf>).
- Аудит для Android (<https://protonvpn.com/files/proton-vpn-android-app-audit-report-2020.pdf>).
- Аудит для Windows (<https://protonvpn.com/files/proton-vpn-windows-app-audit-report-2020.pdf>).
- Аудит для macOS (<https://protonvpn.com/files/proton-vpn-macos-app-audit-report-2020.pdf>).

Результаты аудита показывают, что были обнаружены две уязвимости низкого риска в коде приложения.

Технологии шифрования: ProtonVPN поддерживает OpenVPN, IKEv2/IPSec и WireGuard.

2. Mullvad

Страна: Швеция (страна входит в международные альянсы по обмену разведывательной информацией, что может быть важно для тех, кто ищет абсолютную безопасность в экстремальных ситуациях).

Политика конфиденциальности: Mullvad не требует личных данных для регистрации, и вы получаете случайный номер счета для входа. Компания не хранит логи. Подробнее о политике конфиденциальности

можно почитать [здесь](https://mullvad.net/en/help/no-logging-data-policy) (<https://mullvad.net/en/help/no-logging-data-policy>).

Аудит: Проведенный аудит подтвердил безопасность сервиса. Подробности можно найти в отчете [здесь](https://cure53.de/pentest-report_mullvad_2024_v1.pdf) (https://cure53.de/pentest-report_mullvad_2024_v1.pdf).

Технологии шифрования: Mullvad использует WireGuard, что делает его отличным выбором для тех, кто ищет безопасное решение.

3. NordVPN

Страна: Панама (страна не имеет законов о хранении данных и не входит в альянсы по обмену информацией).

Политика конфиденциальности: NordVPN заявляет, что они не хранят логи, что было подтверждено независимым аудитом. Подробнее о политике конфиденциальности можно прочитать [здесь](https://my.nordaccount.com/legal/privacy-policy/) (<https://my.nordaccount.com/legal/privacy-policy/>).

Аудит: Недавний независимый аудит от Deloitte подтвердил полное соответствие заявленной политике отсутствия логов. Подробнее об этом можно почитать [здесь](https://cyberinsider.com/independent-deloitte-audit-verifies-nordvpns-no-logs-claim/) (<https://cyberinsider.com/independent-deloitte-audit-verifies-nordvpns-no-logs-claim/>).

Технологии шифрования: NordVPN использует WireGuard, IKEv2/IPSec и AES-256, что обеспечивает высокую степень безопасности.

Особенности: Для обхода цензуры сервис предоставляет **Obfuscated Servers**, которые помогут скрыть ваше соединение в странах с жестким интернет-контролем (Китай, Россия).

4. Surfshark

Страна: Британские Виргинские острова (не входят в альянсы по обмену информацией).

Политика конфиденциальности: Surfshark также заявляет, что не хранит логи. Подробнее о политике конфиденциальности можно прочитать [здесь](https://surfshark.com/privacy) (<https://surfshark.com/privacy>).

Аудит: Surfshark прошел аудит от компании Cure53, который подтвердил безопасность браузерных расширений. Подробнее можно ознакомиться с отчетом [здесь](https://surfshark.com/wp-content/uploads/2021/05/SRF-02-summary.pdf) (<https://surfshark.com/wp-content/uploads/2021/05/SRF-02-summary.pdf>).

Технологии шифрования: Surfshark использует WireGuard, IKEv2/IPSec и AES-256.

Дополнительные функции: Surfshark предлагает **MultiHop** (маршрутизация трафика через несколько серверов) и **CleanWeb** (блокировка рекламы и трекеров).

Итог

- **Для максимальной анонимности: Mullvad** — это лучший выбор, если конфиденциальность для вас на первом месте.
- **Для универсального VPN с высокой скоростью и дополнительными функциями: NordVPN** или **Surfshark**.
- **Для бесплатного использования с хорошей конфиденциальностью: ProtonVPN**.