# Article information:

Какие VPN самые надежные? Как понять, что сервис сотрудничает со спецслужбами? Могут ли Россию вообще отключить от нормального интернета? Эксперты отвечают на вопросы читателей «Медузы» o VPN — Meduza
<https://meduza.io/feature/2022/07/29/kakie-vpn-samye-nadezhnye-kak-ponyat-chto-servis-sotrudnichaet-so-spetssluzhbami-mogut-li-rossiyu-voobsche-otklyuchit-ot-normalnogo-interneta>

# Article summary:

1. Blocking a specific VPN service is easy by blocking the IP addresses of the servers of that service.

2. If a VPN service does not have a wide pool of IP addresses, does not change servers, and does not use tricks against censorship, then blocking by IP is a reliable measure.

3. Firewalls or traffic filters can be used to block VPN services if the traffic can be determined.

# Article rating:

Appears moderately imbalanced: The article provides some useful information, but is missing several important points or pieces of evidence that would be required to present the discussed topics in a balanced and reliable way. You are encouraged to seek a more balanced perspective on the presented issues by exploring the provided research topics and looking at different information sources.

# Article analysis:

The article titled "Какие VPN самые надежные? Как понять, что сервис сотрудничает со спецслужбами? Могут ли Россию вообще отключить от нормального интернета? Эксперты отвечают на вопросы читателей «Медузы» o VPN" provides some useful information about VPN technology and how to deal with potential issues related to blocking of VPN services in Russia. However, the article has several limitations that need to be addressed.

Firstly, the article seems to have a bias towards promoting the use of VPN services and other tools for bypassing censorship and surveillance. While it is important to protect online privacy and freedom of expression, it is also necessary to consider the potential risks associated with using such tools. For example, some VPN services may not be as secure or private as they claim to be, and may even collaborate with government agencies or hackers. Moreover, using Tor or other anonymity networks can also expose users to various threats such as malware, phishing attacks, and illegal activities.

Secondly, the article does not provide enough evidence or sources to support some of its claims and recommendations. For instance, it suggests that switching protocols or turning on obfuscation mode can solve problems with VPN connectivity, but does not explain how these features work or which protocols are more reliable than others. Similarly, it recommends installing Tor, Psiphon and Lantern without explaining their pros and cons or how they compare to each other in terms of security and usability.

Thirdly, the article overlooks some important factors that affect the effectiveness of blocking VPN services in Russia. For example, it does not mention the role of DNS filtering or DPI (Deep Packet Inspection) techniques that can detect and block VPN traffic even if the IP addresses of the servers are changed frequently. It also does not address the legal and political implications of using VPN services in Russia, where the government has been cracking down on online dissent and imposing harsh penalties on those who violate internet regulations.

Fourthly, the article presents only one side of the debate about VPN technology and censorship, without exploring alternative views or counterarguments. For instance, it does not mention the arguments of those who support internet regulation and surveillance as a means to combat terrorism, cybercrime, and other threats to national security. Nor does it discuss the challenges faced by law enforcement agencies in investigating crimes that involve encrypted communications or anonymous online activities.

In conclusion, while the article provides some useful tips and insights about VPN technology and its potential risks and benefits, it also has some limitations that need to be addressed. To provide a more balanced and informative perspective on this topic, future articles should consider a wider range of sources and viewpoints, as well as provide more evidence-based analysis of the technical, legal, and social aspects of VPN technology and censorship.

# Topics for further research:

* DNS filtering and DPI techniques for blocking VPN traffic
* Legal and political implications of using VPN services in Russia
* Arguments for internet regulation and surveillance to combat national security threats
* Challenges faced by law enforcement agencies in investigating crimes involving encrypted communications
* Comparison of Tor
* Psiphon
* and Lantern in terms of security and usability
* Risks associated with using VPN services that may collaborate with government agencies or hackers

# Report location:

<https://www.fullpicture.app/item/b79fdd37f477a14b7efcd83bdefdb04a>