

УДК 004.056.5

Букатка С. – ст. гр. СБс-42

Тернопільський національний технічний університет ім. І. Пулюя

THE ROLE OF VIRTUAL PRIVATE NETWORKS (VPNS) IN THE MODERN DIGITAL WORLD

Науковий керівник: к.філол.н., доцент Боднар О.І.

Bukatka S.

Ternopil Ivan Puluj National Technical University

THE ROLE OF VIRTUAL PRIVATE NETWORKS (VPNS) IN THE MODERN DIGITAL WORLD

Supervisor: PhD in Philology, Assoc. Prof. Bodnar O.I.

Keywords: virtual private network, device, protection, secure, access.

A virtual private network (VPN) is a mechanism for creating a secure connection between a computing device and a computer network, or between two networks, using an insecure communication medium such as the public Internet. [1]

The basic idea is to create an encrypted tunnel connection between the user's device and a VPN server located in another location. When a user connects to a VPN, their data is encrypted before it is sent over the Internet. After that, the encrypted traffic passes through the VPN server, where it is decrypted and sent to its final destination, be it a website, email server, or other online resource.

Virtual private networks have become an essential tool for both corporate environments and ordinary Internet users. Here are some aspects of their role:

— Protection against data interception. VPNs encrypt the information transmitted between the user and the Internet. This prevents sensitive data such as passwords, financial information, etc. from being intercepted, even if the connection is over untrusted networks such as public Wi-Fi hotspots.

— Ensuring privacy. VPNs hide the user's IP address by replacing it with the IP address of the VPN server. This makes it harder for third parties, such as advertising companies or intruders, to monitor your online activity and identify you. [2]

— Bypassing blocking and censorship. In countries with restricted Internet access or in organizations with limited access to certain web resources, VPNs can bypass these restrictions, allowing users to access the entire network.

— Secure access to corporate networks. For enterprises, VPNs are an important means of ensuring security and protecting sensitive information during remote work access. They allow employees to connect to corporate networks over the Internet without exposing company data to the risk of attack.

— Ensuring the security of mobile devices. Using a VPN on mobile devices allows you to protect user data even when connecting to untrusted networks, which is especially important in a world where mobility has become a standard.

There are advantages and disadvantages to using virtual private networks (VPNs), which are outlined below. [3]

Advantages of VPNs:

- Traffic protection: a VPN encrypts your data, which helps to prevent information from being intercepted by intruders.
- Ensuring online privacy: using a VPN helps to hide your real IP address and keep you private.
- Change your IP address: users can mask their IP address, which allows you to bypass restrictions and censorship.
- Protection in countries with strict government controls: VPN helps you bypass restrictions that may be imposed by your provider or government.
- Prevents bandwidth restrictions: using a VPN allows you to get a better internet experience.

Disadvantages of VPNs:

- Slower Internet: using a VPN can result in slower connection speeds because data has to be encrypted and routed through a remote server.
 - Some VPN services are not secure: not all VPN providers are reliable. Some free VPNs may collect user data and display annoying ads.
 - Subscription costs: premium VPN services cost money.
 - Incompatibility with certain devices: some VPNs may not support all devices.
 - Does not protect against voluntary disclosure of personal information: it's important to remember that a VPN doesn't protect you from sharing personal information on social media.
- Below are five of the most popular and reliable VPN providers that are widely recognized for their security and quality of service:
- ExpressVPN. ExpressVPN is known for its speed and reliability. They have a wide network of servers in many countries, as well as strong cryptographic security and a zero-logging policy.
 - NordVPN. NordVPN is also a popular choice due to its high security standards, wide server selection, and ability to bypass geo-blocking. They also offer binary protection, which provides double encryption.
 - CyberGhost. This VPN provider is known for its ease of use and wide selection of servers in more than 90 countries. CyberGhost also has strong encryption protocols and a zero-logging policy.
 - Surfshark. Surfshark stands out for its affordable price and the ability to connect to many devices simultaneously. They also offer strong security and connection speeds.
 - ProtonVPN. ProtonVPN is known for its strong focus on privacy and security. They have advanced privacy protection features such as Secure Core, which routes your traffic through safe countries, as well as a zero-logging policy.

VPNs certainly play a key role in ensuring the privacy and security of virtual connections, and their use is recommended for all users who want to protect their data and personal information while online.

Список використаних джерел:

1. Contributors to Wikimedia projects. Virtual private network - Wikipedia. Wikipedia, the free encyclopedia. https://en.wikipedia.org/wiki/Virtual_private_network.
2. 5 Reasons to Use a VPN. CNET. <https://www.cnet.com/tech/services-and-software/5-reasons-to-use-a-vpn/>.
3. Benefits of using a VPN in 2024 - Surfshark. Surfshark. <https://surfshark.com/blog/benefits-of-vpn>.