UDC 004.771

FEATURES OF USING OPENVPN FOR COMPUTER NETWORKS OF ENTERPRISES WITH REMOTE OFFICES

***Kostiantyn Dobarskyi*[1]**

[1] master's student of the Computer Engineering and Programming department, NTU "KhPI", Kharkiv, Ukraine

Modern conditions for the development of information technology dictate the need for their accelerated use as the most rapid means of control, management and exchange of data both within a single division and on the scale of a large enterprise. Ukraine's entry into the global information space entails the widest use of the latest information technologies, and in the first place, corporate networks. Corporate network is a set of geographically dispersed computers that can exchange messages through the medium of data transmission. The main purpose of corporate networks is to share resources and establish communication both within one division or organization and beyond its borders. Properly designed computer network provides speed and reliability of data transmission, timely communication with customers, quality service in the enterprise.

One of the possible options for creating conditions for the transfer of information within a distributed information system is the use of technology VPN (Virtual Private Network - virtual private network). VPN is a technology that provides network connections over other networks, such as the Internet. Communication within the virtual network is carried out on basic channels with low level of trust, and the use of encryption allows for maximum transmission security. This relatively inexpensive and easy-to-implement technology has recently become increasingly popular. VPN is easily scalable and is the best option for enterprises with multiple branch offices, as well as for firms whose employees frequently travel or work from home.

Different protocols can be used to organize VPN, one of the most popular is OpenVPN. OpenVPN is an open-source implementation of VPN distributed under the GNU GPL license.

The level of reasonability of using VPN with OpenVPN is already quite good, this is due to higher data security than before using VPN with OpenVPN, as evidenced by the test results of data interception using Wireshark software by sending username and password. The results obtained by using OpenVPN username and password can be seen and detected, and after using OpenVPN username and password the data is not detected or encrypted by OpenVPN, so it is protected against the action The QoS measurement results have suffered a decrease in network quality, latency parameters increased from 51.4 ms to 463.4 ms, packet loss increased from 7.8% to 20.2%, and throughput fell from 82.8% to 71.6% this is due to the encryption and encapsulation process, which takes time. But despite this decline OpenVPN is a balanced option. It is more likely than others and much less susceptible to attack by attackers. Connecting a new office or a remote employee is done without additional communication costs. In addition, the initial organization of the virtual system requires a minimum of cash expenditures. In the future, the financial investment will be made to pay for the Internet provider's services.

References:

1. *Олифер В. Г.* Компьютерные сети. Принципы, технологии, протоколы / В.Г. Олифер, Н.А.Олифер. // Учебник для вузов. – 5-е изд. – СПб.: Питер, 2016. – 992с.: ил.

2. OpenVPN [Електрон. ресурс]. – Режим доступу: *https://openvpn.net/*

3. Wireshark [Електрон. ресурс]. – Режим доступу: *https://www.wireshark.org/*