ENSURING NETWORK SECURITY: METHODS AND SOLUTIONS

TARMOQ XAVFSIZLIGINI TA'MINLASH: USULLAR VA ECHIMLAR.

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ СЕТИ: МЕТОДЫ И РЕШЕНИЯ.

Mirzaeva Irodaxon Xamdamovna
Department of Department of Pedagogy and Languages Andijan Branch of Turon University
Мирзаева Иродахон Хамдамовна
Кафедра педагогики и языков Андижанский филиал Туронского университета
Mirzayeva Irodaxon Xamdamovna
Turon universiteti Andijon filiali Pedagogik va tillar kafedrasi
irodaxonmirzayeva89@gmail.com
https://orcid.org/0009-0005-7435-8026

Annotation: *This article discusses effective methods for ensuring network security in the context of increasing reliance on computer, information, and telecommunication technologies. It highlights the importance of secure information exchange via networks, especially in governmental and organizational communication. Key threats such as unauthorized access, data interception, and denial-of-service attacks are identified. The article explores modern protective technologies including IPSec, VPN, and Intrusion Detection Systems (IDS), detailing their roles in safeguarding transmitted data and enabling secure remote access. A practical example of establishing a VPN network between a user's home and office is also presented as a reliable solution for maintaining confidentiality and data integrity in network communication.*

Keywords: *Network Security, IPSec, VPN, Intrusion Detection Systems, Eavesdropping, Denial-of-Service, Port Scanning, Data Integrity, Cybersecurity, Secure Communication.*

Annotatsiya: *Maqolada kompyuter, axborot va telekommunikatsiya texnologiyalariga bo‘lgan tobora ortib borayotgan qaramlik sharoitida tarmoq xavfsizligini ta’minlashning samarali usullari muhokama qilinadi. Ayniqsa, davlat va tashkilotlarning aloqa tizimlarida xavfsiz axborot almashishning ahamiyati ta’kidlanadi. Ruxsatsiz kirish, ma’lumotlarni ushlash va xizmatni rad etish (Denial-of-Service) kabi asosiy tahdidlar aniqlanadi. Maqolada IPSec, VPN va Kirishlarni aniqlash tizimlari (Intrusion Detection Systems, IDS) kabi zamonaviy himoya texnologiyalari ko‘rib chiqilib, ularning uzatilayotgan ma’lumotlarni himoya qilish va xavfsiz masofaviy ulanishni ta’minlashdagi ro‘li yoritiladi.*

Shuningdek, foydalanuvchining uy va ofisi o‘rtasida VPN tarmog‘ini tashkil etish amaliy misoli keltiriladi, bu esa tarmoq aloqalarida maxfiylik va ma’lumotlar yaxlitligini ta’minlashda ishonchli yechim sifatida namoyon bo‘ladi.

Kalit so‘zlar: *tarmoq xavfsizligi, IPSec, VPN, kirishlarni aniqlash tizimlari, ma’lumotlarni ushlash, xizmatni rad etish, portlarni skanerlash, ma’lumotlar yaxlitligi, kiberxavfsizlik, xavfsiz aloqa*

Аннотация: *В данной статье рассматриваются эффективные методы обеспечения безопасности сети в условиях растущей зависимости от компьютерных, информационных и телекоммуникационных технологий. Подчёркивается важность безопасного обмена информацией через сети, особенно в государственных и организационных коммуникациях. Выделяются основные угрозы, такие как несанкционированный доступ, перехват данных и атаки типа «отказ в обслуживании» (Denial-of-Service). Статья изучает современные защитные технологии, включая IPSec, VPN и системы обнаружения вторжений (Intrusion Detection Systems, IDS), подробно описывая их роль в защите передаваемых данных и обеспечении безопасного удалённого доступа. Также приведён практический пример организации VPN-сети между домом пользователя и офисом как надёжного решения для поддержания конфиденциальности и целостности данных в сетевой коммуникации.*

Ключевые слова: *сетевая безопасность, IPSec, VPN, системы обнаружения вторжений, перехват данных, отказ в обслуживании, сканирование портов, целостность данных, кибербезопасность, безопасная коммуникация*

Computer and information technologies, telecommunications, data transmission networks, and the use of Internet services, which are among the priority directions of our country's policy, are continuously developing and modernizing. The broad implementation of modern information technologies in all spheres of our society and daily life ensures progress toward achieving our long-term goals. In every sector, the use of the Internet increases work efficiency.Through the use of networks, fast information exchange saves time. Particularly, the formation of the Electronic Government system in our country, and its role in strengthening the interaction between public administration bodies and the population, is made possible through the use of network technologies. Efficient utilization of networks contributes to the formation of a democratic and information-oriented society. In such a society, the speed of information exchange increases, and data can be collected, stored, processed, and utilized rapidly and effectively.

However, protecting against issues such as unauthorized network access, data manipulation, and loss remains a pressing concern. Enterprises, organizations, and government bodies that rely on networks for communication must prioritize network security before connecting. Network security involves ensuring the reliable and systematic protection of transmitted, stored, and processed data through various tools, methods, precautions, and actions. Any tool used for ensuring network security must be capable of rapidly identifying threats and taking appropriate countermeasures.

There are various types of threats to network security, typically classified into categories such as:

- Eavesdropping: unauthorized interception and modification of data during transmission;
- Denial-of-service (DoS): attempts to disrupt service availability;
- Port scanning: unauthorized scanning of open communication ports.

Eavesdropping and modification attacks can target voice communications, instant messaging via the Internet, video conferences, and fax transmissions without the user noticing. These attacks can be implemented using certain network analysis protocols. Malicious software can convert digital voice data, encoded in CODEC standards (used for converting analog audio/video signals to digital format), into high-quality but large-sized audio files (e.g., WAV). The attack is often undetectable to users as the system functions seamlessly without unusual behavior or noise, raising no suspicion about data theft. Only users informed about such threats and utilizing secure network communication systems are able to protect their data integrity and privacy.

There are several effective technologies to counter eavesdropping and data manipulation, including:

- IPSec (Internet Protocol Security);
- VPN (Virtual Private Network);
- IDS (Intrusion Detection System).

IPSec is a protocol suite that ensures secure data exchange over networks using encryption algorithms. This standard guarantees compatibility between hardware, software, and data exchange processes within networked systems. IPSec ensures:

- Data confidentiality — only sender and receiver can interpret the message;
- Data integrity — ensuring information is not altered;
- Authentication of data packets.

Modern information technologies are vital for the development of any organization. IPSec is especially effective for:

- Connecting headquarters with branches via a global network;

- Managing enterprises remotely via the Internet;
- Securing communication networks with partners;
- Enhancing the security level of e-commerce platforms.

VPN (Virtual Private Network) technology allows for secure data exchange by creating an internal network over an external one, typically the Internet. It connects separate local networks through secure "tunnels" at a relatively low cost and high level of security. Each segment of the network must include a VPN gateway to manage data transmission between branches. When a user sends data across the network, it is first encrypted by the VPN gateway using a reliable algorithm and then transmitted via the Internet to another branch's gateway, where it is decrypted and delivered to the target computer. This process is invisible to users and feels identical to working within a local network.

VPN effectively counters eavesdropping attacks, making intercepted data unreadable. Additionally, VPN provides a convenient method of connecting an external computer (e.g., during a business trip) to an organization's internal network. With appropriate software, users can connect to their office VPN gateway and access internal data securely and conveniently, just like being physically present in the office.

To implement a VPN, two fundamental components are required in addition to hardware and software:

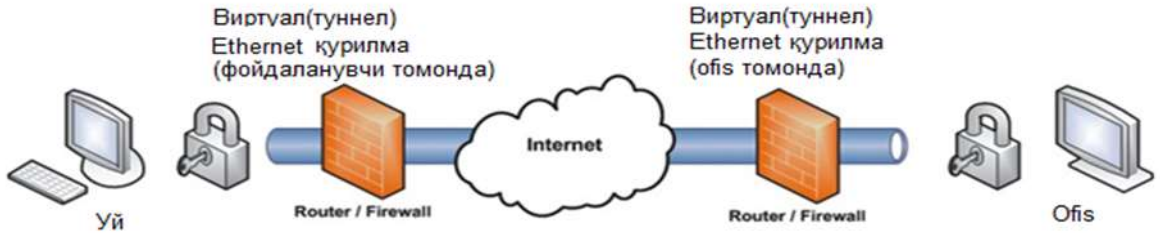
- A data transmission protocol;
- Security tools for that protocol.

IDS (Intrusion Detection System) detects attempts to breach network or system security policies using unauthorized means. These systems have been in development for nearly 25 years and originated from auditing computer system logs. IDS can be categorized into:

- Network-based IDS (NIDS) — monitors traffic across a network;
- Host-based IDS (HIDS) — monitors activity on individual computers.

Figure 1: Scheme for Establishing a VPN Connection Between Home and Office

(The image illustrates a secure VPN configuration enabling a user to access office data remotely.)



The proposed method ensures the secure exchange of information via network technologies. Users can access confidential office data directly from home. The VPN network and the authentication system offer reliable protection for secure data usage .

References

1. Stallings, W. (2017). Network Security Essentials: Applications and Standards (6th ed.). Pearson Education.
2. Tanenbaum, A. S., & Wetherall, D. J. (2011). Computer Networks (5th ed.). Pearson.
3. Kurose, J. F., & Ross, K. W. (2017). Computer Networking: A Top-Down Approach (7th ed.). Pearson.
4. Schneier, B. (2015). Applied Cryptography: Protocols, Algorithms, and Source Code in C (20th Anniversary ed.). Wiley.
5. Scarfone, K., & Mell, P. (2007). Guide to Intrusion Detection and Prevention Systems (IDPS). National Institute of Standards and Technology (NIST) Special Publication 800-94.