MODERN METHODS OF INFORMATION PROTECTION

https://doi.org/10.5281/zenodo.15129097

Saidov Jasur Doniyor o‘g‘li
Gulistan State University, Department of Information Technologies, Doctor of Philosophy (PhD) in Pedagogical Sciences,
Asrorova Mavludaoy Umurzoq qizi
First year student of the Faculty of Information Technology and Physics and Mathematics, Gulistan State University

Abstract: *This article reviews advanced information security methods such as cryptography, authentication, network security, artificial intelligence-based security systems, blockchain technology, and cloud security. The advantages and areas of application of each method are analyzed, and their effectiveness in ensuring information security is assessed. It also provides guidance for organizations and users in choosing the most effective protection methods.*

Keywords*: Information and communication, cryptography (encryption), algorithm, identification and authentication, entity, cybersecurity, cyber defense, cyberspace, IDS, cyberattack, blockchain, cloud and artificial intelligence-based security, software updates.*

Today, the price of information is often several times higher than the price of the computer system in which it is located. Therefore, there is a need to protect information from unauthorized use, intentional modification, destruction and other destructive actions.

Since the advent of the Internet in information and communication networks, cases of information theft, unauthorized modification and destruction of information content, unauthorized use of networks and servers, network attacks, retransmission of previously acquired transmissions, evasion of service or access to information, and sending shipments through unauthorized channels have increased worldwide.

In order to apply information technologies in various fields, it is necessary to ensure their reliability and security. Security is understood as the ability of an information system to maintain its integrity and operability in the event of external events in unforeseen situations. The widespread use of information technologies has led to the rapid development of various methods for ensuring information security, primarily cryptography. The use of cryptographic methods in the protection of information systems is becoming especially active today. Indeed, on the one hand, the rapid and high-quality transmission and reception of large amounts of state and military information, as well as economic and personal information, as well as other types of information, using Internet

networks in computer systems is expanding. On the other hand, the issues of ensuring the protection of such information are becoming increasingly important.

Currently, cryptographic methods and tools are used to ensure the information security of not only the state, but also organizations and ordinary individuals. Standards in this area have been adopted in developed countries. In September and December 2003, laws on electronic digital signatures were adopted in our republic, in 2005 the state standard for the encryption algorithm and in 2009 the state standard for the digital signature algorithm were approved.

Identification and authentication are interrelated processes of determining and verifying the authenticity of subjects (users). The system's permission to use system resources for a particular user or process depends on them. After identifying and authenticating the subject, its authorization begins. When protecting data transmission channels, mutual authentication of subjects, that is, mutual confirmation of the authenticity of subjects communicating through communication channels, is mandatory. Authentication is usually performed at the beginning of a session, during the connection of subscribers to each other. The term "connection" is understood as a logical connection between two network entities. The purpose of this procedure is to ensure confidence that the connection was made with a legitimate entity and that all information reaches its intended destination.

Protecting the interests of individuals, society and the state from external and internal threats in cyberspace is a priority area of ensuring state cybersecurity.

Cybersecurity is a set of legal, organizational, financial, economic, engineering and technical measures aimed at preventing cybersecurity incidents, detecting and protecting against cyberattacks, eliminating the consequences of cyberattacks, restoring the stability and reliability of the operation of telecommunication networks, information systems and resources, as well as measures to protect data cryptographically and technically.

As for the tasks of cybersecurity, they mainly consist in developing a national defense system to warn of cyberattacks and cyberthreats in our republic and forming a cybersecurity threat model and measures to counter them, that is, ensuring the protection of information transmission channels.

It should not be forgotten that the global information space has no geographical and state borders, therefore, information and cybersecurity can only be fully ensured through the efforts of the world community, that is, all states. In this regard, it is necessary to consider the issues of harmonizing our current national regulatory and legal documents, including our standards with world standards, as well as cooperation in their implementation, the adoption of international agreements on the functioning of the international information space in the social, political, cultural, and legal spheres.

An intrusion detection system (IDS) is used to identify methods or means by which an attempt is made to violate the security policy of a system or network. Intrusion detection systems have a history of almost a quarter of a century. Early models and prototypes of

intrusion detection systems used the analysis of audit data from computer systems. These systems fall into two main classes: Network Intrusion Detection Systems and Host Intrusion Detection Systems.

Organizations often use piecemeal approaches to address security issues. These approaches are usually determined primarily by the current level of available resources. In addition, security administrators often respond to security threats that are clear to them. In fact, there can be many threats. Only a comprehensive approach that provides strict current control of corporate information systems and a common security policy can significantly reduce security threats.

Recently, a number of approaches have been developed by various companies that allow not only to identify existing vulnerabilities, but also to identify old or emerging vulnerabilities that have changed and to implement appropriate protection measures. In particular, the adaptive security management model ANS (Adaptive Network Security) was developed by the company ISS (Internet Security Systems).

Attack detection is the process of assessing suspicious activity on a corporate network. Attack detection is carried out by analyzing operating system and application logs or real-time traffic. Attack detection components deployed on network nodes or segments also evaluate various events, in particular, actions that exploit certain vulnerabilities

The adaptive network security management model also allows you to reduce network abuse, increase the level of awareness of users, administrators and company management about network events. It should be noted that this model does not abandon previously used protection mechanisms (access restrictions, authentication, etc.). It expands their functionality with the help of new technology. Organizations that want their information security systems to meet modern requirements should supplement existing solutions with three new components - protection analysis, attack detection and threat assessment.

In the 21st century, modern methods of protecting information are increasingly becoming more and more advanced. In particular, cloud and artificial intelligence-based security systems, regular software updates, and blockchain technology.

Many organizations prefer to store their data on cloud servers. To effectively use cloud technologies, it is necessary to take privacy and security measures. Modern cloud security systems have the ability to encrypt data, identify users, and ensure network security.

Artificial intelligence (AI) and machine learning technologies are ushering in a new era in cybersecurity. These systems are used to detect malware, predict cyberattacks, and automatically monitor anomalies.

Modern applications and operating systems are frequently updated. These updates help eliminate security flaws. Therefore, it is important to constantly update operating systems and applications.

Blockchain technology is an effective tool for preventing information from being altered or corrupted. Blockchain, which acts as a decentralized database, provides the following capabilities:

- Immutability: Data cannot be changed once it is entered;
- Trustworthiness and transparency: Every transaction is public and traceable;
- Decentralized governance: The lack of a single point of control increases the security of the system.

Information security is a necessity for every organization and individual today. The methods listed above will help you effectively protect yourself from cyberattacks. You can reliably protect your data by using modern technologies and security measures.

REFERENCES:

1. M. Aripov, A.S. Matyakubov. Information Protection Methods. Tashkent: University, 2014. p. 96.
2. I.M. Karimov, N.A. Turgunov. Fundamentals of Information Security. Tashkent: Academy of the Ministry of Internal Affairs of the Republic of Uzbekistan, 2016. p. 91.
3. Institute of Personnel Training and Statistical Research. Ensuring Information Security. Tashkent: 2024.
4. Ross, J. (2020). Cybersecurity Threats and Defenses. O'Reilly Media.
5. Bishop, M. (2018). Computer Security: Art and Science. Addison-Wesley.
6. O‘G‘Li, S. J. D., Qizi, M. M. Z., & Qizi, T. R. Z. O. (2024). AXBOROT TIZIMLARI VA ULARNING RIVOJLANISHI OMILLARI. Central Asian Journal of Multidisciplinary Research and Management Studies, 1(4), 66-69.
7. Saidov, J. D. (2021). Study of the process of database and creation in higher education. In International scientific and practice conference on" International experience in increasing the effectiveness of distance education: problems and solutions". Guliston.
8. Jasur Doniyor, O. G., Saidov, L., Allayorov, S. P., OMBORINI, S., & BAHOLASH, Y. M. Scientific progress. 2021. № 1. URL: https://cyb erleninka. ru/articl e/n/ma-lumotl ar-omborini-yarati sh-bo-yicha-kasbiy-kompetentligini-baholash-mezonlari (дата обращения: 02.06. 2022).
9. Saidov, J., Ishchanova, I., Temirxolova, B., & Nurmuhammedova, Z. (2024). BILIMLAR BAZASINING ASOSIY XUSUSIYATLARI VA ULARGA OID LOYIHALASH. Theoretical aspects in the formation of pedagogical sciences, 3(7), 23-27.
10. Saidov, J., Nazarqulov, A., & Danaboyev, N. Z. (2024). ELEKTRON DIDAKTIK VOSITALAR YORDAMIDA BILIMLARNI SINASH MUAMMOLARI. Центральноазиатский журнал междисциплинарных исследований и исследований в области управления, 1(2), 143147.
11. Джураев, М. Э. (2021). ЗНАЧЕНИЕ ГЕОХИМИЧЕСКИХ ПРОЦЕССОВ В ВЕРТИКАЛЬНОЙ И ГОРИЗОНТАЛЬНОЙ СВЕЗИ ПАРА

12. Sattarov, S. M., Khudaykulov, S. I., Djuraev, M. E., & Axunbabaev, M. M. (2018). DETERMINATION OF THE CONCENTRATION OF NON-CONSERVATIVE SUBSTANCES IN A MULTI-DENSITY FLOW. Bulletin of Gulistan State University, 2018(2), 7-12.

13. Djurayev, M., & Husenov, J. (2022). STUDIES IN GEOGRAPHY, CONFLICTS AND SOLUTIONS IN APPLIED GEOGRAPHY. Journal of Geography and Natural Resources, 2(01), 2428.