academic publishers

INTERNATIONAL JOURNAL OF ARTIFICIAL INTELLIGENCE (ISSN: 2692-5206)

Volume 04, Issue 10, 2024

Published Date: 07-12-2024

MEASURES OF INFORMATION AND DATA PROTECTION

Suyarov Akram Musayevich

Associate Professor, PhD. Department of Information Technologies, Samarkand Institute of Economics and Service, Uzbekistan. akramsuyarov@mail.ru

Roziqulov Abdukakhor Ikhtiyorovich

Student of the Samarkand Institute of Economics and Service, Uzbekistan. ahrorproduction5@gmail.com

Abstract: Information security has become one of the main priority issues of each country today. The rapid development of information societies, the widespread use of information and communication technologies, and the growth of information exchange via the global Internet create new risks for countries. This article analyzes the relevance of information security and its importance for the security of countries. It also considers information protection, effective methods of combating illegal access and modification of data, and the importance of advanced technologies. The article is devoted to the analysis of the main problems of information security and the development of the information society.

Key words: Information security, information society, information and communication technologies, global network, Internet risks, data protection, illegal access, information exchange, national security.

Introduction

Information resources of each country are one of the important factors determining its economic and military power. Effective use of this resource plays an important role in ensuring the country's security and developing a democratic information society. In the information society, the exchange of information is accelerating, and advanced information and communication technologies are widely used to collect, store, process and effectively use information.

Today, the information society is rapidly developing, and in this process the concept of state borders is gradually disappearing. Global computer networks are fundamentally changing public administration. Depending on our geographical location, different information enters our lives via the Internet. Therefore, protection against such risks as illegal access to existing information, its modification or loss becomes a pressing issue.

Also, many measures to ensure information security are being implemented in Uzbekistan. Including:

Program for the Implementation of the Action Strategy in the "Year of Support for Active Entrepreneurship, Innovative Ideas and Technologies" published for public discussion[1].

At the same time, Principles 12-13 of the Law of the Republic of Uzbekistan "On the principles and guarantees of freedom of information" also provide information on the storage of information:[2]

Law 12. State policy in the field of information security

is aimed at regulating public relations in the sphere of information and defines the main tasks and areas of activity of state authorities and administration in the field of ensuring information security of the individual, society and society. The state, as well as the citizens themselves, determine the role and

[1] "Strategy of Action" of the Republic of Uzbekistan

[2] At the same time, the Law of the Republic of Uzbekistan "On the principles and guarantees of freedom of information"

importance of self-government bodies, public associations and other non-governmental non-profit organizations, citizens.

Law 13. Security of personal information

"Information security of a person is ensured by creating the necessary conditions and guarantees for the free use of information, maintaining the secrets associated with his personal life, protection from illegal psychological influence in the media. Personal information related to individuals is classified as confidential information.

The main objective of this paper is to review the research conducted in the field of information security and analyze the existing risks. Its main objective is to demonstrate the impact of cyber-attacks, in particular ransomware, phishing and Dodos attacks, and to analyze modern technologies and approaches in response to the growing demand for cyber security. The study will serve as a basis for studying cyber-attacks and their economic consequences, as well as for developing effective security policies for organizations and countries.

Literature review

In the field of information and data protection, many scientists have conducted important research, and their research serves to form modern information security systems and technologies. Research in this area covers such important issues as personal data protection, information security and cybersecurity. Below are some scientific studies conducted in this area and their content.

William Stallings - Cryptography and Network Security: Principles and Practice (2020) William Stallings, a leading expert in cryptography and network security, examines cryptographic algorithms, authentication, information integrity, and confidentiality in the field of information security. This book provides detailed descriptions of the types of cryptographic algorithms, including AES, RSA , and SHA, and discusses their applications and effectiveness. The techniques presented in the book provide an important theoretical and practical foundation in the field of information security .

Bruce Schneier - "Applied Cryptography: Protocols, Algorithms, and Source Code in C" (2015) In this book on cryptography, Bruce Schneier provides an in-depth analysis of the practical aspects of information security. This book provides information on various cryptographic protocols, in particular symmetric and asymmetric encryption methods. Schneier's research shows that information can be protected through the widespread use of cryptographic technologies, especially digital signature and authentication methods.

D. Goelmann - Computer Security (2011) Dieter Goelmann provides a detailed overview of computer security and its key components in this work . Goelmann covers important aspects of computer security, including access rights management, security policies, and data protection methods. This book provides an in-depth analysis of the factors that influence security and protection mechanisms in information systems.

Ross J. Anderson - Security Engineering: A Guide to Building Trustworthy Distributed Systems (2008) This work by Anderson is an important source on system security. The book provides detailed information on the fundamental principles, security engineering principles, and information security techniques needed to ensure system security. This resource provides a detailed analysis of information security defenses, including resilience to attacks and processes for developing secure systems.

Joseph Migga Kizza - "Computer Network Security and Cyber Ethics" (2013) In this book, Kizza presents his research in the field of computer network security and cyber security. The book examines types of cyber-attacks, methods of ensuring data security and managing access rights to information. Kizza provides relevant recommendations for the information security industry, paying special attention to the legal and ethical aspects of cyber security.

Wade Trapp and Lawrence K. Washington - "Introduction to Cryptography with Coding Theory" (2014). This book covers the basic concepts of cryptography and its aspects related to coding theory. Trapp and Washington elaborate on the role of encryption methods in information security. In particular, the study of information security methods through coding theory plays a key role in ensuring information security.

The above resources provide a deep scientific basis and theoretical knowledge of information security tools and technologies. Their research serves as a key resource for implementing new approaches to information security and taking effective measures to counter existing security threats and risks.

Research Methodology

The study widely used a systematic approach to scientific knowledge, monographic observations, statistical abstracts, logical reasoning and methods of long-term forecasting. Also, the method of analysis and synthesis was effectively used in the implementation of scientific research.

Analysis and discussion of results

The table presented in the annual reports of Verizon, IBM, ENISA contains information on the most common cyberattacks for the period 2020-2023:

Year	Total number of cyber attacks (worldwide)	Number of ransomware attacks	Number of phishing attacks	Number of DDoS attacks	Average economic damage ($ per attack)
2020	1,500,000	304,000	468,000	215,000	3830 US dollars
2021	1,850,000	450,000	610,000	280,000	4240 US dollars
2022	2,400,000	623,000	780,000	360,000	4350 US dollars
2023	3 100 000	820,000	950,000	410,000	4500 US dollars

The table above shows the number of global cyberattacks from 2020 to 2023, broken down into three main types: ransomware (malware that demands payment from its victims), phishing (phishing), and DDoS (distributed service attack), along with information on the average economic damage from each attack.

1.5 million in 2020 to 3.1 million in 2023, doubling in four years. This trend shows that cybersecurity threats are growing worldwide. Data shows that the total number of attacks is increasing by about 30% annually, highlighting the need for tougher cybersecurity measures. The trends in attack types are as follows:

➢ increased from 304,000 in 2020 to 820,000 in 2023, confirming its effectiveness and prevalence. This increase can be attributed to the profitability of ransomware attacks, as attackers demand payment to unlock the malware.

➢ The number of phishing attacks has increased from 468,000 in 2020 to 950,000 in 2023, almost doubling. Phishing is one of the most common and simple types of attacks, which is explained by the fact that it is technically simple and successful.

➢ increased from 215 thousand in 2020 to 410 thousand in 2023. DDoS attacks are commonly used to disrupt business operations, and the increase in such attacks indicates the vulnerability of online services and infrastructures.

The average economic damage from each cyberattack increased from $3,860 in 2020 to $4,500 in 2023. This means that cyber-attacks are not only increasing in number, but also becoming more-costly economically. Increased costs may be due to the emergence of more sophisticated attack methods, recovery costs, and financial or reputational losses for organizations.

Conclusions

Growing demand for cybersecurity. This information is getting stronger going cybersecurity necessity emphasizes , especially cyberattacks often And Expensive be gathers Organizations , especially a lot of p attack happening fields , extended cybersecurity decisions , employees learn and must invest in preparedness for attacks.

Ransomware and phishing attacks are the most common attacks these areas should be a priority in the cybersecurity policy. Endpoint security, regular software updates and employee awareness programs are recommended as countermeasures to these attacks . Given the growing economic impact of cyber-attacks, companies should evaluate their risk management systems and consider cybersecurity insurance to mitigate financial losses. Investments in rapid detection systems can also help reduce the response time to attacks and the overall cost of attacks.

The main reasons for the increase in the number of cyber-attacks include the following:

— The proliferation of Internet-connected devices, or IoT (Internet of Things), and digital transformation present new opportunities for attackers as the number of devices and networks increases.

— New attack methods : Cyber attackers are developing increasingly complex, advanced, and specialized software, while using automated and targeted methods to identify network vulnerabilities.

— Remote work and online learning during the pandemic has provided cyberattacks with new opportunities to attack people and organizations.

From 2020 to 2023, the number of cyberattacks continued to increase year on year, with an average annual growth rate of 25-30%. formed The number of common cyberattacks increases every year, which further increases the need for improved cyber security. It is important for organizations to ensure security, protect information, and develop new technologies to counter cyber-attacks.

Conclusions and suggestions

Cybersecurity is important in today's digital economy because it directly affects the economic stability and development of countries. Research shows that countries with high levels of cybersecurity have the potential to accelerate economic growth because they create a safe environment for investors and businesses. However, as cyberattacks take many forms and become more sophisticated, governments and businesses need to adopt more robust defenses. In this sense, investing in cybersecurity, upgrading security technologies, and training specialists are of strategic importance for countries to ensure economic security.

As a result of the above study, it is necessary to implement security measures to protect information and data. Based on the results of the study, we can make the following suggestions:

- ❖ **Using encryption technologies**
- ❖ **Cybersecurity training and development**
- ❖ **antivirus and security software**
- ❖ **Implementation of multi-factor authentication (MFA).**
- ❖ **Create backups, develop and implement security policies**
- ❖ **Updating systems regularly**

1. How to use encryption technologies. Making data unreadable using data encryption technologies (cryptography). A special key is required to access encrypted data, which increases security. As a result, encryption makes it difficult for unauthorized persons to access information, and the level of confidentiality is increased.

2. Cybersecurity training and development of personnel, i.e. training of IT and security personnel through regular training, familiarization with industry innovations. As a result, employees will be able to quickly identify and prevent cyberattacks and threats, and the protection of the enterprise or organization will be strengthened.

3. By using antivirus and security software installation of high-quality antivirus and security programs on each device, their regular updating. As a result, protection from cyber attacks, malware and viruses increases, systems operate safely.

4. With the introduction of multi-factor authentication (MFA), users must authenticate using an SMS code or mobile app in addition to a password, increasing the level of protection against password theft or hacking by ensuring that only authorized users have access.

5. How to create backups, develop and implement security policies. The focus is on setting up a regular data backup system and allocating storage space to an external device or the cloud. Result if the system is damaged or data is lost, it can be restored using backup copies. Also, security policies and rules are developed in the organization, employees are trained to comply with them, the rules for ensuring the organization's information security are systematically observed, employees acquire a security culture.

6. Regularly updating systems by updating operating systems, programs and security mechanisms eliminates their vulnerabilities , and updated systems and programs are less susceptible to cyber attacks and the level of security is increased.

By implementing these measures, organizations and companies will be able to ensure the security of their data, gain the trust of customers and users, comply with information security legislation and avoid economic losses.

References:

1. 1. "Action Strategy" of the Republic of Uzbekistan
2. 2. Law of the Republic of Uzbekistan "On Principles and Guarantees of Freedom of Information"
3. 3. Resolution of the President of the Republic of Uzbekistan "On Measures to Improve the System of Control over the Introduction of Information Technologies and Communications and Their Protection"
4. William Stallings – "Cryptography and Network Security: Principles and Practice" (2020)

5. Bruce Schneier – “Applied Cryptography: Protocols, Algorithms, and Source Code in C” (2015)

6. D. Gollmann – “Computer Security” (2011)

7. Ross J. Anderson – “Security Engineering: A Guide to Building Dependable Distributed Systems” (2008)

8. Joseph Migga Kizza – “Computer Network Security and Cyber Ethics” (2013)

9. Wade Trappe va Lawrence C. Washington – “Introduction to Cryptography with Coding Theory” (2014).

10. Suyarov A.M. Formation of information and communication competence of the teacher as an one of the main tasks of modern education. Web of Scientist: International Scientific Research Journal. Volume 4, Issue 4, April-2023.–C.243-257.

11. Suyarov A.M. Ways and models of providing integration of information technology science with mathematical sciences. «E3S Web of Conferences». Indexed by SCOPUS and submitted for indexing to Web of Science (CPCI) «E3S Web of Conferences» 402, 03016 (2023).

12. Smolyaninova O.G. Article: Formation of information and communicative competence of the future teacher on the basis of multimedia technologies // Journal of Informatics and Education, No. 9, 2012. - From 48-55.

13. 10. Course of lectures / under the general editorship of Candidate of Physical and Mathematical Sciences, Senior Researcher I.M. Karimov. – T.: Academy of the Ministry of Internal Affairs of the Republic of Uzbekistan, 2013. – 123 p.

14. 11. M. Aripov, A.S. Matyakubov “Information Protection Methods” Tashkent: University, 2014. 96 p.

15. Verizon DBIR (Data Breach Investigation Report)

16. Cybersecurity Ventures Global Report

17. Cisco Annual Cybersecurity Report