Lubko Dmytro
Candidate of iences, Associate Professor,
Associate professor of Department of Computer Science
Dmytro Motornyi Tavria State Agrotechnological University

PROBLEMS OF INFORMATION PROTECTION AND SECURITY

Annotation*. The main purpose of this publication it consider the problem of protecting and ensuring information security both in organizations and at home. Implementation and proof of principles information security to everyone (at home, at work, etc.) should be effective and able to protect information (work, personal, etc.) from unauthorized access, modification, disclosure or destruction.*

Key words: *protection issues, information security, data encryption, security, authentication and authorization, control and monitoring.*

Лубко Д.В. Проблематика захисту та безпеки інформації. Основна мета даної публікації це розглянути проблему захисту та забезпечення безпеки інформації як організаціях так і вдома. Впровадження та доведення принципів безпеки інформації до кожного (вдома, на роботі, тощо) має дати ефект та здатно захистити інформацію (роботу, особисту, тощо) від несанкціонованого доступу, модифікації, розголошення чи знищення.

Ключові слова: проблематика захисту, безпека інформації, шифрування даних, безпека, аутентифікація та авторизація, контроль та моніторинг.

Introduction. In today's world, information is a treasure that determines many directions. It not only helps in decision-making and business development, but can also be subject to abuse. This is why ensuring data security has become critical for any organization, regardless of its size or industry. Data security is not only about restricting access, but also about guaranteeing the confidentiality, integrity and availability of information. Confidentiality becomes a guarantee that only authorized persons have access to the data. Integrity ensures that information remains intact and uncorrupted. And availability means providing access to information at the right time.

In Information security domains distinguish several security classes that are used to classify data and systems according to their importance and sensitivity. These security classes help organizations design and implement effective security measures to protect their data. Unfortunately, the number of cyber crimes is increasing every day, a large part of these crimes is identity theft. Most often, this happens due to negligence and ignorance of users. That is why all this is a problem that needs to be solved both personally and collectively.

As the analysis of the latest research and publications on this problem area shows (on the identification of security mechanisms, information and data protection issues, information security issues, security issues, etc.), many scientists and scientists have been actively working in this area. Namely, these are such specialists and scientists as: Parkhuts′ Yu.L [1], Mykhaylov A.O. [2], Shevchuk D.T. [3], Skrypka M.V. [4], Tivets′ka A.V. [5], Hovorushchenko T.O. [5], Oleshko I.V. [6], Shevchenko S. [7], Blyznyuk I. [8], Lehka O.V. [10], Chunar′ova A. [11], Fedorenko R.M. [12], Oksiyuk O.G. [13], Zinchenko D.A. [14], Dumans′ka N.O. [15]. Also, all these issues are solved and periodically highlighted by teachers of TDATU, such as Sharov S.V. [16], Miroshnychenko M.Yu. [17] and D.V. Lubko [16, 17].

Despite the large number of works and studies in this area, many aspects of information security and data protection issues are not sufficiently covered.

The purpose of the study it consider the problem of protecting and ensuring information security both in organizations and at home.

Outline of the main material. Data encryption is a key security mechanism that ensures confidentiality and protection of information during transmission or storage. In today's digital world, where data is exchanged continuously, encryption acts as a reliable shield that protects against unauthorized access and possible threats. Encryption ensures that data crosses networks and is stored in the form of unintelligible text for everyone except those who are assigned to decipher it [16, c. 23]. This is ensured with the help of special algorithms that transform the plain text into an incomprehensible encrypted form, which can only be decoded with the help of the appropriate key.There are two main types of encryption: symmetric and asymmetric. Symmetric encryption uses the same key to encrypt and decrypt data. The encryption key is known only to authorized users. Asymmetric encryption uses two keys: an encryption key and a decryption key. The encryption key is

known to anyone, and the decryption key is known only to authorized users. There are many different encryption algorithms used for different purposes.

Authentication and authorization are also important aspects of security that help protect information from unauthorized access. Authentication is the process of confirming the user's identity. Authentication can be implemented using various methods, such as: ppasswords are the most common authentication method (passwords should be long and complex so that they are difficult to guess); biometrics are physical or behavioral characteristics of a person that can be used for authentication (biometrics include fingerprints, face, iris and voice); digital signature certificates are electronic documents that confirm the user's identity (digital signature certificates are used to sign electronic documents to guarantee their integrity).

Authorization is the process of granting permission to the user to perform certain actions. Authorization can be implemented using various methods, such as [1, p. 5]: krole-based access control (RBAC), is an authorization method based on user roles [3, p. 58]; attribute-based access control (ABAC) [2, p. 44];

Another mechanism is access control - this is one of the most important aspects of physical data protection [4, p. 12]. It allows you to control access to physical objects such as buildings, server rooms and workstations. Access control can be implemented using methods, such as passwords, key cards, biometric scanners and video cameras.

Passwords are the most common method of access control. Passwords should be long and complex so that they are difficult to guess.

Do not forget about cyber attacks, they are a serious threat to organizations and individuals. They can lead to leakage of confidential data, financial losses or even business shutdown. Cyber attacks today are not just a threat, they have become a reality that inevitably affects all spheres of life – from government structures to private households. These attacks reveal vulnerabilities in digital systems, using technology to abuse data, destroy infrastructure, or steal sensitive information. Today's cyberattacks have become more complex, more cunning and larger in scale, requiring constant improvement and improvement of the level of protection. Their consequences can be devastating both for individual users and for large corporations or even entire countries.

A cyber attack is any attempt to gain unauthorized access to a computer system or network. Cyber attacks can be carried out for a variety of reasons,

such as data theft, sabotage or ransom. There is a wide range of methods that can be used for cyber attacks. Some of the most common methods include [15, p. 120]: password Cracking (using software or manual methods to crack user passwords); social engineering is tricking users into providing sensitive information or performing unwanted actions; malware – downloading malicious software onto the victim's computer that can be used for data theft, sabotage or ransom; malicious network attacks - exploiting vulnerabilities in a network to gain unauthorized access to computers or systems.

There are many steps you can take to protect yourself from cyber attacks. Some of the most important activities include: pcreating strong passwords; use of multi-factor authentication; software updates; use of a firewall; use of anti-virus software; all employees must be informed about cyber attacks and how to avoid them.

Multi-factor authentication (MFA) is an additional level of security that requires users to enter additional information, such as a code from a mobile phone, for authentication [7, p. 22]. MFA makes cyberattacks much more difficult, as an attacker would need to obtain not only a password, but also access to another device, such as a mobile phone. Software often contains vulnerabilities that can be exploited for cyber attacks. It is important to update your software regularly to close these vulnerabilities. Software vendors regularly release updates to fix vulnerabilities.

A firewall is a device or software that helps protect a computer or network from unauthorized access. A firewall works by blocking access to your computer or network from unauthorized sources. Antivirus software [8, p. 66] helps protect your computer from malicious software such as viruses, Trojan horses, and malware. Antivirus software works by scanning your computer for malware and removing it if it finds it.

Vulnerabilities are errors in software [6, p. 5], which can be used for cyber attacks. You can use vulnerability scanning tools to find vulnerabilities in your software.

Data backups are an important defense against cyber attacks. If your data is lost or damaged due to a cyber attack, you can restore it from backups. You should back up your data regularly and store it in a safe place. It is important to develop and implement cyber attack response plans. A cyber attack response plan defines what to do in the event of a cyber attack.

It is also necessary to monitor and analyze security - these are important processes that help organizations protect their information and assets from cyber attacks [13, p. 24]. Security monitoring involves constantly watching the security system to detect any potential threats. Security analysis involves evaluating the data collected during monitoring to determine whether these threats are real. Modern trendssecurity monitoring and analysis include: growing use of automation (automating security monitoring and analysis can help organizations save time and resources); growing use of artificial intelligence (artificial intelligence can be used to improve the effectiveness of security monitoring and analysis); growing use of cloud technologies (they can be used to centralize security monitoring and analysis).

Another important mechanism is that data backup and recovery are important processes that help organizations protect their information and assets from loss or damage. Backup is the process of creating a copy of data that can be used for recovery in case the originals are lost or damaged. Restoration is the process of restoring data from a backup copy. The purpose of data backup and recovery is to ensure that an organization can recover its data in the event of loss or damage. This can be important for many reasons, for example if: cyber attack – can lead to data loss or corruption; тatural disasters, such as fires or floods, can lead to data loss or corruption; failure to do so, such as late software updates, can result in data loss or corruption.

Regulatory standards and requirements for information protection are sets of rules and procedures that establish minimum information security requirements for organizations under their jurisdiction [9, p. 34]. Regulatory standards and requirements for information protection are developed to protect the confidentiality, integrity and availability of information. There are many different regulatory standards and information protection requirements. Some of the more common types include laws and regulations that establish mandatory information protection requirements for organizations under their jurisdiction. For example, the EU Personal Data Protection Act (GDPR) establishes requirements for personal data protection for organizations processing personal data of EU citizens [10, p. 40]. They are also non-binding guidelines and recommendations, but are often used by organizations to develop their own security policies and procedures. For example, the International Organization for Standardization (ISO) has developed a number of information security standards [5, p. 82], which are widely used by organizations around the world. And internal security policies and procedures

are sets of rules and procedures that organizations develop to protect their information. Internal security policies and procedures must meet the requirements of any relevant regulatory standards and requirements. Regulatory standards and requirements for information protection are an important tool for information protection. They help organizations prevent the leakage or damage of information, which can lead to financial losses, privacy violations or other negative consequences [11, p. 50]. Organizations subject to regulatory standards and information protection requirements must develop and implement effective security programs that meet those standards and requirements.

Security programs should include such elements as: security policies and procedures; education and training; control and monitoring.

Conclusions. Implementation, demonstration and observance of principles information security to everyone (at home, at work, etc.) should be effective and able to protect information/data (work, personal, etc.) from unauthorized access, modification, disclosure or destruction. All of these play a key role in preventing data leakage or corruption that could lead to financial losses or privacy breaches. Encryption, authentication and access control are the main security tools that help protect information. Organizations must develop and maintain these mechanisms, as well as constantly improve their systems, taking into account new challenges, such as the rapid development of technology and the increase in cyber threats.

References

1. Parkhuts′ Yu.L. (2011). Kryptohrafichni mekhanizmy zakhystu informatsiyi v mobil′nomu zv'yazku. [Cryptographic mechanisms of information protection in mobile communication]. Natsional′nyy universytet «L′vivs′ka politekhnika» [in Ukrainian].
2. Mykhaylov A.O. (2021). Doslidzhennya modeley ta metodiv kontrolyu dostupu do informatsiynoyi systemy: poyasnyuval′na zapyska do atestatsiynoyi roboty zdobuvacha vyshchoyi osvity na druhomu (mahisters′komu) rivni, spetsial′nist′ 121 - Inzheneriya prohramnoho zabezpechennya. [Study of models and methods of information system access control: explanatory note to the attestation work of a higher education applicant at the second (master's) level, specialty 121 - Software engineering]. M-vo osvity i nauky Ukrayiny, Nats. un-t radioelektroniky. Kharkiv [in Ukrainian].

3. Shevchuk D.T. (2022). Metody autentyfikatsiyi ta avtoryzatsiyi u mobil′nykh ta veb-dodatkakh. [Methods of authentication and authorization in mobile and web applications]. Mizhnarodna naukova internet-konferentsiya: «Informatsiyne suspil′stvo: tekhnolohichni, ekonomichni ta tekhnichni aspekty stanovlennya [in Ukrainian].
4. Skrypka M.V. (2021). Systema kontrolyu dostupu do personal′nykh danykh. [Personal data access control system] [in Ukrainian].
5. Tivets′ka A.V., Nevmerzhyts′ka S.M. (2015). Udoskonalennya systemy upravlinnya personalom orhanizatsiyi z vrakhuvannyam vymoh mizhnarodnykh standartiv ISO. [Improvement of the personnel management system of the organization taking into account the requirements of international ISO standards]. Visnyk Kyyivs′koho natsional′noho universytetu tekhnolohiy ta dyzaynu. Seriya «Ekonomika i vyshcha osvita» [in Ukrainian].
6. Hovorushchenko T.O., Mevsha A.V., Krys′kov V.A. (2014). Klasyfikatsiya vidmov ta vrazlyvostey systemnoho prohramnoho zabezpechennya. [Classification of System Software Failures and Vulnerabilities] [in Ukrainian].
7. Oleshko I.V. (2014). Modeli ta metody otsinky zakhyshchenosti mekhanizmiv bahatofaktornoyi avtentyfikatsiyi vid nesanktsionovanoho dostupu. [Models and methods for assessing the security of multifactor authentication mechanisms against unauthorized access] [in Ukrainian].
8. Shevchenko Svitlana, Skladannyi Pavlo, Martseniuk Maksym. (2019). Analiz ta doslidzhennya kharakterystyk antyvirusnoho prohramnoho zabezpechennya, standartyzovanoho v Ukrayini. [Analysis and study of the characteristics of antivirus software standardized in Ukraine. Electronic professional scientific publication]. Elektronne fakhove naukove vydannya «Kiberbezpeka: osvita, nauka, tekhnika». 4.4: pp. 62-71 [in Ukrainian].
9. Blyznyuk Ihor, Shoroshev Vyacheslav. (2002). Osnovy normatyvno-pravovoho zabezpechennya zakhystu informatsiyi v komp″yuternykh systemakh derzhavnykh orhaniv Ukrayiny. [Basics of regulatory and legal provision of information protection in computer systems of state bodies of Ukraine] [in Ukrainian].
10. Lehka O.V. (2023). Implementatsiya mizhnarodnykh standartiv shchodo zakhystu prava na dostup do informatsiyi v Ukrayini. [Implementation of international standards on protection of the right to access to information in Ukraine] [in Ukrainian].

11. Chunarʹova Anna. (2012). Systema upravlinnya informatsiynoyu bezpekoyu na bazi mizhnarodnykh standartiv seriyi ISO. [Information security management system based on international standards of the ISO series] [in Ukrainian].
12. Fedorenko R.M. (2015). Kontent-monitorynh informatsiynoho prostoru yak chynnyk zabezpechennya informatsiynoyi bezpeky derzhavy u voyenniy sferi. [Content monitoring of the information space as a factor in ensuring the information security of the state in the military sphere]. Suchasnyy zakhyst informatsiyi. 2: pp. 21-25 [in Ukrainian].
13. Oksiyuk O.H., Shestak Ya.V. (2015). Metodolohiya rozrobky kompleksnykh system zakhystu informatsiyi v suchasnykh informatsiyno-telekomunikatsiynykh systemakh. [Methodology of development of complex information protection systems in modern information and telecommunication systems]. Zbirnyk naukovykh pratsʹ Viysʹkovoho instytutu Kyyivsʹkoho natsionalʹnoho universytetu imeni Tarasa Shevchenka. 50: pp. 236-243 [in Ukrainian].
14. Zinchenko D.A., Makarova O.P. (2021). Analiz ryzykiv i stratehiy zakhystu vid kiberatak u suchasnomu tsyfrovomu sviti. [Analysis of risks and defense strategies against cyber attacks in today's digital world] [in Ukrainian].
15. Dumansʹka N.O. (2020). Shyfruvannya danykh v informatsiynykh systemakh. [Data encryption in information systems]. Tezy dopovidey V student·sʹkoyi vuzivsʹkoyi naukovoyi konferentsiyi «Matematychni metody, modeli ta informatsiyni tekhnolohiyi v upravlinni pidpryyemstvom». pp. 23-25 [in Ukrainian].
16. Lubko D., Sharov S., Strokan O. (2019). Software development for the security of TCP-connections. Modern development paths of agricultural production: trends and innovations. Cham: Springer international publishing. pp. 99-109 [in Ukrainian].
17. Lubko D.V., Miroshnychenko M.Yu. (2024). Analiz suchasnykh pidkhodiv ta metodyk v oblasti zakhystu informatsiyi ta danykh. [Analysis of modern approaches and methods in the field of information and data protection]. Visnyk Khersonsʹkoho natsionalʹnoho tekhnichnoho universytetu. No1(88). pp. 231-236 [in Ukrainian].