DOI: https://doi.org/10.36910/6775-2524-0560-2024-55-41
UDC 004.056:004.7:004.9
Larchenko Oksana, Candidate of Agricultural Sciences, Associate Professor,
ORCID: https://orcid.org/0000-0001-7857-0802
Kherson State Agrarian and Economic University, Kherson, Ukraine

THEORETICAL ASPECTS OF DATA CONFIDENTIALITY IN INFOCOMMUNICATION NETWORKS

Larchenko O. Theoretical Aspects of Data Confidentiality in Infocommunication Networks. Data confidentiality in information and communication networks is a hot topic in the modern digital world. With the development of infocommunications and global information infrastructure, the volumes of transmitted and processed information have acquired an unpredictable scale. In this context, ensuring data privacy becomes a vital concern.

A growing number of cyber threats, including hacking, phishing, data theft and privacy breaches, pose risks to the security and privacy of information transmitted over networks. Known cases of leakage of confidential data, such as personal information, commercial and state secrets, and medical records, demonstrate the need for effective means and methods of protection.

In addition, public awareness regarding data privacy and confidentiality is growing. Users are becoming more aware and aware of the risks associated with storing and transmitting their personal data online. This is driving demands for organizations and companies to ensure strong privacy protections for their customers.

In recent years, there has been a significant increase in the amount of digital data stored and transmitted through information and communication networks, thanks to new technologies such as the Internet of Things, cloud computing, social networks, e-commerce and other digital technologies that have become an integral part of our daily lives. This creates a need to reliably protect these large volumes of data from unauthorized access and malicious activity.

The number of cyber threats is constantly growing, and attackers are constantly developing new methods of attack and cybercrime, which jeopardizes data confidentiality. From hacking attacks, phishing, malware, to identity theft and business disclosure, digital threats are becoming more complex and dangerous. Ensuring data confidentiality is becoming a critical need to avoid financial losses, privacy breaches and other negative consequences.
Keywords: cyber threat, infocommunications, infocommunication networks, confidential information, insider threats.

Ларченко О. Теоретичні аспекти конфіденційності даних в інфокомунікаційних мережах. Конфіденційність даних в інфокомунікаційних мережах є надзвичайно актуальною темою в сучасному цифровому світі. З розвитком інфокомунікацій та глобальної інформаційної інфраструктури, обсяги інформації, що передається та обробляється, набули непередбачуваного масштабу. У цьому контексті забезпечення конфіденційності даних стає життєво важливим завданням.

Зростаюча кількість кіберзагроз, включаючи хакерські атаки, фішинг, крадіжки даних та порушення приватності, створює небезпеку для безпеки та конфіденційності інформації, що передається через мережі. Відомі випадки витоку конфіденційних даних, такі як особисті інформації, комерційні та державні секрети, медичні записи, демонструють потребу в ефективних засобах та методах захисту.

Окрім того, суспільне усвідомлення, щодо приватності та конфіденційності даних росте. Користувачі стають більш обізнаними та свідомими щодо ризиків, пов'язаних зі збереженням та передачею їхніх особистих даних в мережі. Це стимулює вимоги до організацій і компаній забезпечувати надійний захист конфіденційності даних своїх клієнтів.

В останні роки спостерігається значне збільшення кількості цифрових даних, які зберігаються та передаються через інфокомунікаційні мережі, завдяки таким новим технологіям як Інтернет речей, хмарні обчислення, соціальні мережі, електронна комерція та інші цифрові технології, що стали невід'ємною частиною нашого повсякденного життя. Це створює потребу в надійному захисті цих великих обсягів даних від несанкціонованого доступу та зловмисних дій.

Кількість кіберзагроз постійно зростає, зловмисники постійно розвивають нові методи атак та кіберзлочинності, що ставить під загрозу конфіденційність даних. Від атак хакерів, фішингу, шкідливих програм до крадіжок особистих даних та розкриття комерційної інформації - цифрові загрози стають все більш складними та небезпечними. Забезпечення конфіденційності даних стає критичною необхідністю для уникнення фінансових втрат, порушення приватності та інших негативних наслідків.
Ключові слова: кіберзагроза, інфокомунікації, інфокомунікаційні мережі, конфіденційна інформація, інсайдерські загрози.

Formulation of the problem. Data privacy protection has become the subject of strict legislation and regulation. Many countries and regions are establishing new regulations, such as the General Data Protection Regulation (GDPR) in the EU, to regulate the collection, storage, processing and transfer of personal data. Companies must meet these requirements because data breaches can have serious consequences, such as fines and loss of reputation.

Infocommunications is a modern concept that combines telecommunications technologies with information and computer systems. This is an inextricable connection between different elements that ensure the transfer and exchange of information. Infocommunications develops through the convergence of various technologies such as signaling, routing, signal conditioning and programming, ensuring optimal information processing.

Infocommunication networks are a complex set of technical means, including elements of infocommunications, structures and routing systems. They are designed to transmit, receive and exchange various types of signals, messages, text, images and sound through various types of communication systems such as radio, wired and optical.

The global information infrastructure includes networks and infocommunication systems that connect communication nodes, computers and electronic devices to ensure the transfer of a variety of information. It creates the basic infrastructure for organizing various infocommunication services and ensures communication between users around the world.

Given the rapid technological development and growing dependence on information systems, data confidentiality in information and communication networks is becoming increasingly important. The need to protect personal information, business data and other sensitive data requires the development of effective security methods and tools on these networks.

In the modern world of information technology and the Internet, the importance of issues related to data confidentiality is growing. Ensuring data confidentiality is becoming a critical issue for ensuring the privacy of users, businesses and governments in the digital environment.

Research analysis. Scientists and specialists in the field of information security and cryptography are actively researching and developing new methods and algorithms to ensure data confidentiality in information and communication networks. Ongoing efforts are aimed at improving encryption, authentication and access control systems to ensure that information is protected from unauthorized access and malicious activity. The purpose of the article is to study data confidentiality in information and communication networks and analyze the means of ensuring it. The object of the study is data confidentiality in information and communication networks. The subject of the study is ways to ensure data confidentiality in information and communication networks. Including methods of encryption, authentication, access control, threat and risk analysis.

Presentation of the main material and justification of the obtained results. Confidential information is a set of data that is in the possession, use or disposal of individual individuals or legal entities and is distributed at their request.

The basic principles of information security are confidentiality, integrity and availability.

1. Confidentiality: This principle deals with the confidentiality of information, which means that only authorized persons have access to confidential data. Information must be protected from unauthorized access or disclosure. This is achieved through encryption, authentication and access control.

2. Integrity: This principle requires maintaining the integrity of information, i.e. protection against unauthorized changes or modifications. Information must be stored in a permanent state and reliably protected from unauthorized interference. To ensure integrity, data integrity monitoring methods, backups, and intrusion detection mechanisms are used.

3. Availability: This principle means that information and resources should be available to authorized users at the right time. Information systems must be resilient to operational failures, technical problems, or malicious attacks to ensure that information is always available. Measures such as backup, replication and recovery systems are used to ensure availability.

According to Article 21 of the Law of Ukraine «On Information», confidential information, together with official and secret information, refers to information with limited access.

Restricted information is a set of data, access to which is limited only to a certain circle of persons, and its disclosure is prohibited by the information manager by law. Restriction of access to information is carried out for the purpose of national security or protection of the legal rights of individuals and legal entities. It is important to note that access to the information itself is restricted, not the document. Thus, if a document contains both open and restricted information, then the open information can be provided as a separate document to the interested party for review. [1].

According to Article 6 of the Law of Ukraine «On Access to Public Information», information with limited access may be as follows:

1. Confidential information: this is data to which access is limited to an individual or legal entity other than those in authority, and can be disseminated in accordance with their wishes and the conditions determined by them.

2. Secret information: this is data to which access is limited and the disclosure of which could cause harm to a person, society or state. A secret is information that contains state, professional, bank secrets, investigative secrets and other secrets provided for by law.

3. Official information: this is data contained in documents of subjects of power and constituting internal official correspondence, memos, recommendations related to the development of the direction of the institution's activities or the implementation of control and supervisory functions by public authorities, the decision-making process, precedes public discussion or adoption decisions. It may also contain data collected in the process of operational-search, counterintelligence activities and in the field of national defense that are not related to state secrets. [1].

Confidential information owned by the state and in the use of state authorities, local governments, enterprises, institutions and organizations of all forms of ownership does not include information about:

1. State of the environment, quality of food products and household items.

2. Accidents, catastrophes, natural hazards and other emergencies that have occurred or may occur and threaten the safety of citizens.

3. The state of health of the population, its standard of living, including food, clothing, housing, medical care and social security, as well as socio-demographic indicators, the state of law and order, education and culture of the population.

4. The state of affairs with the rights and freedoms of man and citizen, as well as facts of their violations.

5. Illegal actions of state authorities, local governments, their officials and officials.

Activities of state and municipal unitary enterprises, business societies, in the authorized capital of which more than 50 percent of the shares (shares) belong to the state or territorial community, as well as business companies, 50 or more percent of the shares (shares) of which belong to the business company, the share of the state or territorial society in which it is 100 percent, information about these enterprises is subject to mandatory disclosure in accordance with the law.

Other information, access to which in accordance with the laws of Ukraine and international treaties, the consent to be bound by which is provided by the Verkhovna Rada of Ukraine, is limited. These are some alternative formulations for defining confidential and restricted information under Ukrainian law.

Confidential information can be divided into information relating to individuals and information relating to legal entities.

The basis for recognizing information as confidential is the desire of an individual or legal entity to consider certain information about himself or another person in his possession as confidential. The terms «personal data» and «identity information» are used interchangeably. Personal information may concern both individuals and legal entities. However, not all information about a person is confidential unless prohibited by law.

Certain categories of information relating to individuals are not considered restricted information, in particular, income statements of individuals and members of their families who are applying for or already occupy an elected position in government or are civil servants, employees of local government bodies of the first or second category.

Information with limited access also does not include income declarations of persons and members of their families who apply for a position or hold an elected position in government bodies or hold the position of a civil servant, employee of a local government body of the first or second category. This information is publicly available and subject to disclosure to ensure transparency and prevent conflicts of interest.

Declarations of income of persons holding important positions in state or local authorities are an important tool for monitoring the distribution and use of public resources. These declarations contain information about income, property, financial obligations and other important information that helps to check the declarant for the absence of conflicts of interest and possible corrupt behavior.

Such disclosure of information promotes transparency in government structures and helps the public monitor possible inconsistencies and abuses in the sphere of public service. It helps to establish trust in authorities and ensures public control over their activities.

Threats to data confidentiality in information and communication networks. Analyzing the potential threats that arise during the processing of personal data, taking into account the wide range of possibilities for gaining access to information, the following classes of threats can be distinguished:

1. Insider or insider threats arising from the capabilities of internal users. These risks are associated with the possibility of theft or alteration of information by persons who have access to information systems through their official positions or work in a company or government agency.

2. External threats that arise when a threat actor gains unauthorized access to the protected object using the capabilities of public networks.

3. Technical threats that arise when using hardware and programs designed to steal electronic information.

All of these types of threats require serious analysis of personnel who have access to sensitive information, as well as a focus on the technical security of data storage and processing facilities using specialized software, information security management systems (DLP), security event and incident management systems (SIEM)) and other means of protecting information resources. [2].

Threats based on different types of equipment used are also taken into account:

1. Data security threats processed by an employee at his automated workstation (AMW), not connected to the Internet.

2. Threats to information processed by an employee at his workplace connected to the Internet.

3. Threats to information arrays processed in local networks not connected to the Internet.

4. Threats to data arrays processed in local networks of enterprises and organizations connected to the Internet.

5. Security threats to data processed in distributed networks of operators, which may or may not be connected to Internet networks.

In the security threat model, there is also a classification associated with different types of technical means used to access protected amounts of information.

This classification includes:

1. Use of malware, viruses, worms and the like that are created for illegal purposes.

2. Loss of data through technical and physical leakage channels.

3. Other special effects.

Based on the types of security and technical vulnerabilities installed in a particular operator, the threat model identifies the following categories:

– Related to system software vulnerabilities.
– Associated with the use of application software deficiencies.
– Related to the possibilities of using hardware bookmarks.
– Related to the use of communication tools and information transfer protocols.
– Associated with the use of technical data transmission channels, such as telephone networks, power supply networks and others.

This classification allows you to identify different types of threats and vulnerabilities associated with the use of technical means and implement appropriate security measures to prevent them. [3].

It follows from practice that most information leaks from protected areas occur through technical data transmission channels. A signal propagating through a physical environment can be acoustic or electromagnetic, and can be intercepted using embedded devices and other methods. These devices can intercept electromagnetic radiation, acoustic and visual information. Protection against this type of interception due to restricted access to the protected object. Unauthorized access to data from employee owners is very weak and can be completely eliminated.

The following methods can be used to harm data:

1. Use of standard software that allows you to access the operating system.

2. Creation of uncontrolled operating conditions that allow the resulting distortions to be used to modify data.

3. Use of malware.

4. Threats related to remote access to the system.

5. Combined threats.

Characteristics of information systems that influence the emergence of new threats and risks include:

1. The volume and content of information contained in the database.

2. System structure and configuration.

3. Connecting the system to public information transmission networks or networks with cross-border communication.

4. Availability and quality of protection systems.

5. Personal data processing mode.

6. Levels of access to data for persons with different powers and tasks.

7. Physical location of technical devices and mode of protection against illegal access.

Among modern cyber threats the following stand out:

1. Social engineering and phishing – the use of manipulative methods to obtain confidential information.

2. Virus software - malicious programs that can damage or hack the system.

3. Using outdated versions of software with known vulnerabilities.

4. Insider threats – threats associated with unauthorized access or use of information by employees of one's own organization.

5. Lack of policies and procedures for handling information resources.

Social engineering. Social engineering is based on exploiting human weaknesses. Through successful psychological manipulation, a sophisticated attacker can gain access to many important aspects of an organization to plan a hack and steal information. These could be physical access control systems, security operating hours, cleaning schedules, location of printers, trash bins, availability of shredders, etc. Preparation for hacking an organization's information system begins with this type of work.

Phishing attacks are a continuation of social engineering and are one of the most common and effective methods of malicious and illegal access to the resources of businesses and organizations of all forms of government. According to various estimates, up to 90% of successful cyber-attacks are related to phishing. This method is quite simple and is based on the use of fragmented electronic sheets that manipulate the victim by running virus programs, for example, under office applications, or by clicking on fragmented messages that lead to forgery of their websites, where you are asked to enter a login and password before shipment or other resources. [4].

Virus software is one of the most important weapons of attackers, against which it is necessary to have an up-to-date version of anti-virus software. There is no universal antivirus software that would provide equally effective protection against all types of viruses. However, practice shows that it is very useful to exchange information between specialists 19 regarding the beginning of attacks and the emergence of new viruses, as well as the use of services for analyzing suspicious files and links to detect worms, Trojans and other malicious software.

Updating your software is key to avoiding cyber threats. *Constantly updating your software* is of great importance, as it will ensure an increased level of security and protection against new vulnerabilities and threats. It is important to consult with staff, make regular updates and make assumptions, and illustrate with specific questions what risks may arise from using an outdated version of the software. [5].

Insider threats are a significant group of threats emanating from one's own employees. This often happens in organizations where there is no high-level control over the provision of access rights and delimitation of access to information resources. The ideal situation would be if there is a systematic assessment of employee loyalty during recruitment, employment and termination. Considering that personnel are always the weak point in the security system, it is important to constantly work on increasing the security consciousness of employees [5].

The lack of policies and procedures for handling information assets creates serious threats. Policies and procedures define the rules for operating an organization's information system, as well as the distribution of roles and responsibilities. The absence of such policies and procedures leads to chaos, possible financial losses due to inefficient use of resources, increased risk of personnel errors, inadvertent disclosure and loss of information. Having the right policies and procedures allows users to make their own decisions and work within clearly defined boundaries. This includes the proper procedure for granting access rights, following basic information security rules, such as limiting access to necessary resources.

With appropriate security policies in place, there are fewer problems with responsibilities, role allocation, resource protection, and there is a clear procedure for reporting cybersecurity incidents and assessing possible business consequences. All this can be predicted ahead of time by conducting a risk assessment procedure and analyzing the consequences of incidents for business [3].

Technical means of ensuring data confidentiality in information communication networks. At the technological level, the information security policy is implemented through the implementation of a complex of modern automated information technologies. [4] Technical means ensure the confidentiality of data in information communication networks by applying various methods of encryption and information protection.

Here are a few such tools:

1. Virtual Private Networks (VPN): VPN provide secure connections and data transfers over unsecured networks by encrypting traffic. They provide data privacy by creating an encrypted tunnel between remote networks or devices.

2. Data Encryption: Encryption uses mathematical algorithms to convert plain text into encrypted text that is unintelligible to unauthorized persons. Various encryption methods are used, such as symmetric encryption (AES, DES) and asymmetric encryption (RSA, ECC).

3. Firewalls: Firewalls are the first level of network protection and control traffic passing through network nodes. They set traffic filtering rules that allow or block certain types of connections and communications based on predefined security rules.

4. Identification and authentication: Technical means, such as access control systems, two-factor authentication (2FA), biometric systems, ensure the identification of users and ensure their authenticity before providing access to confidential data.

5. Integrated Security Systems: These are comprehensive solutions that combine several technical tools, such as intrusion detection systems (IDS), intrusion prevention systems (IPS), antivirus programs, access control systems and others, to provide comprehensive network and data protection.

6. Link Encryption (SSL/TLS): Link encryption is used to protect data transmitted between a client and a server over the Internet. The SSL (Secure Sockets Layer) and TLS (Transport Layer Security) protocols encrypt data and provide server authentication, which avoids data interception and hacking.

7. Other technologies: Other technical means of data privacy protection include access control systems to network resources, file and folder encryption systems, data backup and recovery systems, and others.

These technical means are used to ensure data confidentiality in information communication networks and reduce the risk of unauthorized access to valuable information. A combination of several tools and proper configuration help ensure a high level of data security. [4]

Conclusions and prospects for further research. The article examined the theoretical aspects of data confidentiality in infocommunication networks. The study began with a definition of data privacy, which points to the importance of protecting information in today's digital world. The threats to data confidentiality encountered in information and communication networks are also analyzed. This includes data interception, unauthorized access, password cracking, network protocol vulnerabilities and others.

Understanding these threats allows you to identify the main attack vectors and take effective measures to prevent them.

Technical means to ensure data confidentiality, such as encryption, access control and authentication, are also presented. Virtual private networks (VPN) have been studied as an effective means of ensuring data confidentiality. Various protocols for ensuring data confidentiality and their suitability for use in information communication networks are analyzed. The advantages and disadvantages of existing methods for ensuring data confidentiality and recommendations for their practical application are identified.

Overall, research in the field of data privacy in information communication networks has great potential for improving information security and protecting user privacy. With the advancement of technology and the challenges of the digital age, further research and development in this area is essential.

References

1. Dokument: Zakon Ukrayiny «Pro zakhyst personal′nykh danykh» № 2297-VI. URL: https://www.president.gov.ua/documents/2297vi-11567 [in Ukrainian]
2. Lahun A. E. (2019) Kryptohrafichni systemy ta protokoly: nav. posibnyk L′viv: Vydavnytstvo L′vivs′koyi politekhniky. [in Ukrainian]
3. Hryhorenko O.H., Holub O.S. (2021) Konfidentsiynist′ danykh v infokomunikatsiynykh merezhakh ta zasoby yiyi zabezpechennya. Zbirnyk «Perspektyvy telekomunikatsiy» PT-2023. K.: KPI im. Ihorya Sikors′koho. [in Ukrainian].
4. Konakhovych H.F., Klymchuk V.P., Pauk S.M., Potapov V.H., Chuprin V.M., Horbunov O.O. (2009) Zakhyst informatsiyi v telekomunikatsiynykh systemakh: Navchal′nyy posibnyk. Kyyiv: NAU. [in Ukrainian]
5. Seniv M . M., V.S. Yakovyna. (2019) Bezpeka prohram ta danykh: navch. posibnyk. L′viv: Vydavnytstvo L′vivs′koyi politekhniky. [in Ukrainian]

Список бібліографічного опису

1. Документ: Закон України «Про захист персональних даних» № 2297-VI.
URL: https://www.president.gov.ua/documents/2297vi-11567
2. Лагун А. Е. (2019) Криптографічні системи та протоколи: нав. посібник Львів: Видавництво Львівської політехніки.
3. Григоренко О.Г., Голуб О.С. (2021) Конфіденційність даних в інфокомунікаційних мережах і засоби її забезпечення. Збірник «Перспективи телекомунікацій» ПТ-2023. К.: КПІ ім. Ігоря Сікорського.
4. Конахович Г.Ф., Климчук В.П., Паук С.М., Потапов В.Г., Чуприн В.М., Горбунов О.О. (2009) Захист інформації в телекомунікаційних системах: Навчальний посібник. Київ: НАУ.
5. Сенів М. М., В.С. Яковина. (2019) Безпека програм та даних: навч. посібник. Львів: Видавництво Львівської політехніки