33

Presentation date: July, 2019
Date of acceptance: September 2019
Publication date: October, 2019

A VARIETY
OF INFORMATION SECURITY THREATS
UNA VARIEDAD DE AMENAZAS DE SEGURIDAD DE LA INFORMACIÓN

Kseniya E. Kovalenko[1]
E-mail: kovalenko1288@mail.ru
ORCID: https://orcid.org/0000-0001-6017-8933
Natalia E. Kovalenko[1]
E-mail: kke@email.asu.ru
ORCID: https://orcid.org/0000-0003-4961-9480
Jorge Luis León González[2]
E-mail: jlleon@ucf.edu.cu
ORCID: https://orcid.org/0000-0003-2092-4924
[1] Altai State University. Barnaul. Russian Federation.
[2] Universidad de Cienfuegos "Carlos Rafael Rodríguez". Cuba.

Suggested citation (APA, sixth edition):

Kovalenko, K. E., Kovalenko, N. E., & León González, J. L. (2019). A variety of information security threats. *Universidad y Sociedad*, 11(5), 256-261. Retrieved from http://rus.ucf.edu.cu/index.php/rus

ABSTRACT

In recent years, computer technology has been closely integrated into our lives. The life of modern society is inconceivable without modern information technologies. Computers serve banking systems, control the operation of nuclear reactors, distribute energy, monitor the schedule of trains, control spacecraft, etc. Computer networks and telecommunications predetermine the reliability and strength of the country's defense and security systems. Computers provide storage of information, its processing and provision to consumers, thereby realizing information technology. The availability and wide dissemination of information technologies, computers make them extremely vulnerable to destructive influences. Thus, the threat to information security is one of the most important problems of modern human life and we need to know where it comes from and how we can protect ourselves.

Keywords: Information technologies, threat, computers, telecommunications systems.

RESUMEN

En los últimos años, la tecnología informática se ha integrado estrechamente en nuestras vidas. La vida de la sociedad moderna es inconcebible sin las modernas tecnologías de la información. Las computadoras sirven a los sistemas bancarios, controlan la operación de reactores nucleares, distribuyen energía, monitorean el cronograma de trenes, aviones de control y naves espaciales. Las redes de computadoras y las telecomunicaciones predeterminan la fiabilidad y la fortaleza de los sistemas de defensa y seguridad del país. Las computadoras proporcionan almacenamiento de información, su procesamiento y provisión a los consumidores, y de esta forma se dan cuenta de la tecnología de la información. Sin embargo, es el alto grado de automatización que genera el riesgo de reducir la seguridad (personal, información, estado, etc.). La disponibilidad y amplia difusión de las tecnologías de la información y las computadoras las hacen extremadamente vulnerables a las influencias destructivas. Por lo tanto, la amenaza a la seguridad de la información es uno de los problemas más importantes de la vida humana moderna y necesitamos saber de dónde viene y cómo podemos protegernos.

Palabras clave: Tecnologías de la información, amenazas, computadoras, sistemas de telecomunicaciones.

INTRODUCTION

The Internet makes communication easier and breaks language barriers, now even if your friend lives thousands of kilometers away from you in another city or even in another country, you can communicate with him, if desired, even for whole days (León González, Socorro Castro & Espinosa Cordero, 2017).

But with all the advantages of the Internet, it contains a host of dangers. First of all, these are threats to personal and state security. The Internet is a free space where it is easy to steal personal data, bank card data, information wars are being fought, information conflicts are generated (Castells, 1997).

Thus, the threat to information security is one of the most important problems of modern human life and we need to know where it comes from and how we can protect ourselves.

The information sphere has now become a system-forming factor in the life of society (Kovalenko, Kovalenko & Gribanov, 2018) and the more active this sphere of social relations develops, the more political, economic, defense and other components of the national security of any state will depend on information security, and in the course of the development of technological progress this dependence will be all increase more.

When changing the way information is stored from paper to digital, the main question is how to protect this information, because a very large number of factors affect the preservation of confidential data. In order to organize secure storage of data, the first thing to do is to analyze threats, for the correct design of information security schemes.

The threats to information security are divided into two main types: natural and artificial threats. Let us dwell on natural threats and try to identify the main ones. Natural hazards include fires, floods, hurricanes, lightning strikes and other natural disasters and phenomena that do not depend on a person. The most frequent among these threats are fires. To ensure the security of information, it is necessary to equip the premises in which the system elements (digital media, servers, archives, etc.) are located, fire sensors, the appointment of those responsible for fire safety and the availability of firefighting equipment. Compliance with all these rules will minimize the risk of information loss from a fire.

If premises with media of valuable information are located in close proximity to water bodies, then they are subject to the threat of information loss due to flooding. The only thing that can be done in this situation is to exclude the storage of media on the first floors of the building, which are subject to flooding.

To external premeditated threats include threats of hacker attacks. If the information system is connected to the global Internet network, then to prevent hacker attacks you need to use a firewall (the so-called firewall), which can be either integrated into the hardware or implemented programmatically.

DEVELOPMENT

The integrity of informational data means the ability of information to retain the original appearance and structure, both during storage and after repeated transmission. Only the owner or user with legal access to data has the right to make changes, delete or supplement information.

Confidentiality is a characteristic that indicates the need to restrict access to information resources for a certain circle of people. In the course of actions and operations information becomes available only to users, which are included in information systems and successfully passed identification.

The availability of information resources means that information that is freely available should be provided to full users of resources in a timely and smooth manner.

Reliability indicates that the information belongs to the trustee or owner, who also acts as a source of information.

Ensuring and maintaining information security includes a set of diverse measures that prevent, monitor and eliminate unauthorized access by third parties. Information security measures are also aimed at protecting against damage, distortion, blocking or copying information. In principle, so that all tasks are solved simultaneously, only then full, reliable protection is provided.

Especially acute are the main questions about the information protection method, when a hack or theft with a distortion of information will lead to a number of serious consequences, financial damages.

In the early 80-ies of XX century information protection was effectively provided with specially developed organizational measures and software and hardware encryption. With the advent of local and global networks, satellite communication channels, the issue of information security has become more acute.

The specificity of the Internet as an information network is based on the realization of the right to information.

In Germany, we found a different approach that does not involve the violation of human rights. Here, access to illegal information is limited based on court decisions.

To the general conditions of legal regulation in the Internet sphere, many authors attribute the following principles: 1) definition of the concept of the right to information; 2) development at the international level of general requirements for information accessible via the Internet; 3) the introduction of uniform standards for the legality of information, as well as the definition of responsibility for the creation, dissemination and provision of access to illegal information; 4) the absence of any kind of censorship of the contents of information transmitted via the Internet; 5) the right to respect for private life, including public figures, etc.

Legal problems that need to be addressed in connection with the development of the Internet in Russia are at the center of attention of the State Duma of the Federal Assembly of the Russian Federation on Information Policy.

In recent years, the Russian Federation has implemented a certain set of practical measures to strengthen the information security of the country. Thus, the formation of a regulatory legal framework for ensuring information security has begun. Currently, it includes more than 80 laws and over 200 other regulatory legal acts.

The work to create a secure information and telecommunications system for special purposes in the interests of public authorities has been launched. State systems for the protection of state secrets and information, a system for licensing the activities of organizations in the field of information protection, and a system for certification of information security tools have been created.

At the same time, an analysis of the state of information security of the Russian Federation shows that its level does not fully correspond to the contemporary needs of society and the state. First of all, the regulatory legal framework for ensuring information security does not cover the whole range of problems in this area, and in some cases is simply contradictory. In order to improve it, an appropriate interdepartmental working group was established by the order of the Secretary of the Security Council of the Russian Federation under the staff of the Security Council of the Russian Federation.

Within its framework, a draft Concept for improving the legal provision of information security has already been developed, which was generally approved at the meeting of the Interdepartmental Commission on September 21, 1999. However, there is currently no single integrated federal law regulating legal relations in the field of information security. In 2000, the Doctrine of Information Security of the Russian Federation was adopted, which is a set of official views on the goals, objectives, principles and main directions of ensuring the information security of the Russian Federation. The doctrine serves as a basis for: the formation of state policy in the field of ensuring information security of the Russian Federation; preparation of proposals for improving the legal, methodological, scientific, technical and organizational support for the information security of the Russian Federation; development of targeted programs to ensure information security of the Russian Federation. This Doctrine develops the Concept of National Security of the Russian Federation in relation to the information sphere.

The Doctrine of the Russian Defense Information Agency contains a more strategic vision on security issues in modern telecommunications systems. However, "information security is a social, not a purely technical phenomenon.

It cannot be identified with the use of special technical means and methods to protect information from unauthorized access, abduction, destruction, etc. Ensuring information security is not only the protection of information, but also organizational, legal and other measures aimed at ensuring a stable, stable development of society and the state.

In contrast to the views of the US government, the Doctrine of the Information Security of the Russian Federation contains paragraphs on the provision of information security in the information and psychological sphere. It is impossible not to notice that the concept itself is absent, there are only its components, it is also necessary to emphasize that "an important aspect of the existence of the information and psychological sphere are" traditional media that act as a factor of mastering reality for the majority of the population".

Another problem is connected with the backlog of domestic information and telecommunication technologies, which compels public authorities to create information systems in the way of purchasing imported equipment and attracting foreign firms. As a consequence, the likelihood of unauthorized access to processed information increases and Russia's dependence on foreign computer and telecommunications equipment manufacturers is growing. At the same time, due to the lack of necessary funding, the pace of work to create a secure information and telecommunications system for special purposes in the interests of public authorities is not sufficient, production of certified information protection equipment, including domestic protected operating systems and application software, is not provided in the required volumes.

Regional problems are also insufficiently worked out, Shestyuk, in the field of information security, the lack of the necessary coordination of the activities of federal and regional public authorities, state and non-governmental

organizations in this field. It should be noted that the regions themselves were the first to sense this and realized themselves, and some of them have recently begun to take certain practical steps in this direction.

Thus, in St. Petersburg, with the regional Security Council, an Interdepartmental Commission for Information Security has been established and is successfully functioning. In the Sverdlovsk region, a draft of the foundations of a federal policy in the field of information security of the regions was developed. In the Novgorod region, a council for information security and information protection was set up under the Governor, a working group was established to coordinate the use of information resources of the region. The Resolution of the Head of Administration of the Khabarovsk Territory approved the Concept of Information Security of the Territory. In the Voronezh Region, the Head of the Administration of the Region has developed and approved the Regulations on the Council for Protection of Information, the Regulations on the Regional Information Security System, the Regulations on the Security Department, the Protection of State Secrets and Information. This is far from a complete list of positive examples, but these actions are still being implemented without proper coordination.

Nevertheless, Russian legislation is able to resolve legal issues arising in connection with the use of the Internet in various areas of life. At the same time, a legal solution awaits the problem of e-commerce, the creation of a legal regime for electronic digital signature and the distribution of the domain space: free access to official information via the Internet, the settlement of the use of cryptography and encryption, and Internet-based operational search activities. The first priority for Russia is the development of a state policy for the use and development of the Internet.

In a number of publications, issues of legal provision of information security on the Internet are investigated. Thus, in the opinion of lawyers, it is necessary to adopt criminal law norms regulating relations in connection with the global network: to determine the legal regime of information (ie, different types of information objects), the procedure for their recording and evaluation; Adopt the rules governing the main types of civil law contracts on the Internet; to regulate electronic commerce and the use of electronic digital signatures in business turnover.

Among the universal norms of international law in this area are, first of all, norms related to human rights and freedoms: the preservation of his life and health; privacy inviolability; freedom of thought, belief and following one's beliefs; freedom of participation in cultural life; protection of interests related to the use of intellectual activity by another person; restrictions on freedom of expression. The author believes that it is very important to ensure the development of norms of customary international law regulating relations in the field of the functioning of the information infrastructure of the world community. The decisions of the 55th session of the UN General Assembly relating to advances in the field of information and telecommunications in the context of international security will contribute to strengthening Russia's information security.

Varieties of Information Security Threats. Information threat refers to the potential impact or impact on an automated system, followed by causing damage to someone's needs.

Today there are more than 100 positions and types of threats to the information system. It is important to analyze all risks using different diagnostic methods. On the basis of the analyzed indicators with their detailing, you can competently build a system of protection against threats in the information space.

Security vulnerability classification. Information security threats do not manifest themselves, but through possible interaction with the weakest links of the protection system, that is, through factors of vulnerability. The threat leads to disruption of the systems on a particular object carrier.

The main vulnerabilities are caused by the following factors:

- Imperfection of software, hardware platform.
- Different characteristics of the structure of automated systems in the information flow.
- Part of the processes of functioning of the systems is inadequate.
- Inaccuracy of communication protocols and interface.
- Difficult operating conditions and location information.

Most often, the threat sources are launched with the aim of obtaining illegal benefits due to the prejudice of information. But it is possible and accidental action of threats due to insufficient protection and the massive action of a threatening factor.

There is a division of vulnerabilities into classes, they can be: objective, random; and subjective.

Objective vulnerabilities. This type directly depends on the technical construction of the equipment at the facility, which requires protection, and its characteristics. Full elimination of these factors is impossible, but their partial elimination is achieved using engineering techniques in the following ways:

1. Associated with the technical means of radiation:

- Electromagnetic techniques (side variants of radiation and signals from cable lines, elements of technical equipment).
- Sound options (acoustic or with the addition of vibrosignals).
- Electrical (slippage of signals in chains of the electrical network, on line pickups and conductors, on the uneven distribution of current).

2. Activated:

- Malware, illegal programs, technological exits from programs, which is combined by the term "software bookmarks".
- Equipment bookmarks are factors that are embedded directly into telephone lines, into electrical networks, or simply into premises.

3. Those that are created by the features of the object under protection:

- The location of the object (visibility and absence of a controlled area around the information object, the presence of vibration or sound reflecting elements around the object, the presence of remote elements of the object).
- The organization of channels for the exchange of information (the use of radio channels, the rental of frequencies or the use of universal networks).

4. Those that depend on the characteristics of the carrier elements:

- Parts with electro-acoustic modifications (transformers, telephone devices, microphones and loudspeakers, inductors).
- Things that are influenced by the electromagnetic field (carriers, chips and other elements).

Random vulnerabilities. These factors depend on unforeseen circumstances and peculiarities of the environment of the information environment. They are almost impossible to predict in the information space, but it is important to be ready for their quick elimination. Such problems can be resolved by conducting an engineering review and retaliation caused by the threat of information security:

1. Failures and failures of the systems:

- Due to malfunction of technical equipment at different levels of processing and storage of information (including those responsible for the performance of the system and for controlling access to it).
- Malfunctions and obsolescence of individual elements (demagnetization of data carriers, such as diskettes, cables, connecting lines and microcircuits).
- Failures of various software that supports all links in the chain of information storage and processing (antiviruses, application and service programs).
- Interruptions in the work of auxiliary equipment of information systems (problems at the level of power transmission).

2. Factors weakening information security:

- Damage to communications such as water supply or electricity, as well as ventilation, sewage.
- Malfunctions in the work of protecting devices (fences, floors in the building, equipment enclosures where information is stored).

Subjective vulnerabilities. This subspecies in most cases is the result of improper actions of employees at the level of developing storage systems and protecting information. Therefore, the elimination of such factors is possible with the help of techniques using hardware and software:

1. Inaccuracies and gross errors that violate information security:

- At the stage of downloading the finished software or preliminary development of algorithms, as well as at the time of its use (possibly during daily operation, during data entry).
- At the stage of managing programs and information systems (difficulties in learning how to work with the system, setting up services on an individual basis, during manipulations with information flows).
- During the use of technical equipment (at the stage of switching on or off, operating devices for transmitting or receiving information).

2. Disruption of the systems in the information space:

Personal data protection mode (the problem is created by dismissed workers or existing employees during off-hours, they get unauthorized access to the system).

security mode and security (during access to the object or to technical devices).

while working with technical devices (possible violations in energy saving or provision of equipment).

while working with data (transformation of information, its storage, search and destruction of data, elimination of defects and inaccuracies).

CONCLUSIONS

In modern conditions, information security is becoming an increasingly important factor in ensuring national security. This necessitates a more detailed study of issues related to the study of this phenomenon in the aspect of

legal regulation. It is necessary to adopt a comprehensive federal legal act regulating the relevant social relations.

Unauthorized access can be the result of errors of users, administrators, operating and maintenance personnel, as well as the shortcomings of the adopted information processing technology, etc.

The definition of specific values of the characteristics of potential violators is largely subjective. The intruder model, constructed taking into account the peculiarities of a particular subject area and information processing technology, can be represented by enumerating several variants of its appearance. Each category of violators should be characterized by the values of the characteristics. For each of them you can give an estimate of the number of employees of the organization falling into this category of violators.

Vulnerable are literally all the basic structural and functional elements of modern distributed computers: workstations, servers (Host-machines), gateways (gateways, switching centers), communication channels.

To protect computer components is necessary from all kinds of impacts: natural disasters and accidents, failures and failures of technical means, personnel and user errors, program errors and deliberate actions by intruders.

There is a wide range of options for deliberate or accidental unauthorized access to data and interference in information processing and exchange processes (including managing the coordinated functioning of various network components and differentiating responsibility for the transformation and further transfer of information).

Correctly constructed (adequate to reality) model of the violator, which reflects its practical and theoretical capabilities, a priori knowledge, time and place of action, etc. characteristics - an important component of the successful conduct of risk analysis and the definition of requirements for the composition and characteristics of the protection system.

BIBLIOGRAPHIC REFERENCES

Castells, M. (1997). ***La era de la información. Economía, sociedad y cultura.*** Madrid: Alianza.

Kovalenko, K. E., Kovalenko, N. E., & Gribanov, D. V., (2018). The development of the information society. ***Universidad y Sociedad***, 10(3). Retrieved from http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S2218-36202018000300365

León González, J. L., Socorro Castro, A. R., & Espinosa Cordero, C. X. (2017). Uso de la Información Científica Tecnológica en la Investigación y la Innovación. Cienfuegos: Universo Sur.