AMERICAN JOURNALS
Open Access, Peer Reviewed Journals

American Journal of Technology and Applied Sciences
ISSN (E): 2832-1766| Volume 13, | June, 2023

METHODS AND PRINCIPLES OF INFORMATION SECURITY IN DIGITAL TECHNOLOGIES

Bobobekova Xulkar Rasulberdiyevna,
Radjabova Mashhura Rustamovna
Samarkand branch of TATU named after Muhammad al-Khorazmi

A B S T R A C T

The concept of "information" is used very widely today. A large amount of information literally overwhelms people. Scientific knowledge, for example, according to experts, increases by 2 times every five years. Information has consumer qualities, as well as its owners. It is very important for the owner to keep secret commercially important information that allows him to successfully compete in the production market. This requires certain actions aimed at protecting confidential information.

K E Y W O R D S

Information security, security threat, information threat, espionage, cryptography, unauthorized access, risk, vulnerability.

Introduction

Information security (information security) is understood as the state of protection of the information itself and its carriers (a person, systems and means, bodies that provide the receipt, processing, storage, transmission and use of information) from various types of threats. Information security can be ensured by various methods and means of both organizational and engineering nature. The information security system includes a set of organizational measures, technical, software and other methods and means of ensuring information security.

In the Republic of Uzbekistan, the Concept of Information Security is being created as an integral part of the national security of the Russian Federation. Within the framework of the draft of this Concept, the main provisions of the state policy for ensuring information security are formulated:

– the state is developing the Federal Information Security Program, which unites the efforts of state organizations and commercial structures in creating a unified information security system in Russia;

- the state forms a legal framework that regulates the rights, duties and responsibilities of all entities operating in the information sphere;

- restriction of access to information is an exception to the general principle of openness of information and is carried out only on the basis of legislation;

- access to any information, as well as the imposed restrictions on access, are carried out taking into account the property rights to this information determined by law;

- responsibility for the safety, classification and declassification of information is personified;

- legal entities and individuals collecting, accumulating and processing personal data and confidential information are liable before the law for their safety and use;

- the state exercises control over the creation and use of information security tools through their mandatory certification and licensing of enterprises and organizations in the field of information security;
- the state pursues a protectionist policy that supports the activities of domestic manufacturers of informatization and information protection tools, and takes measures to protect the domestic market from the penetration of low-quality informatization tools and information products into it;
- the state wants to abandon foreign information technologies for the informatization of public authorities and administration as competitive domestic information technologies and informatization tools are created;
- the state by legal means ensures the protection of society from false, distorted and unreliable information coming through the media;
- the state contributes to providing citizens with access to world information resources, global information networks;

The above provisions of the state policy for ensuring information security require the development of appropriate scientific, technical, organizational and legal support for information security. Today, a lot of money is spent on protecting information. And it's worth it, because today information means a lot and can become quite a serious weapon. Hacking information, as well as its protection, is quite expensive, but, as a rule, those who are ready to spend money on the implementation of this protection need information protection. The importance of information is directly proportional to the money it costs to protect that information. It is up to the owner of the information to decide whether the method of implementing the protection of information is worth the money that is requested for it.

The most expensive and most functional means of protection are electronic security keys and smart cards. The protection system in such programs is quite flexible, which allows you to reprogram data for a specific user. Electronic security keys are developed to order on an individual basis, so the scheme for breaking them is much more complicated than, say, in smart cards. A more complex organization of the protection method itself causes a high price for the program. If we talk about the cost of programs that provide information protection, it is worth noting that the price of some of them is commensurate with the price of hacking these same systems. Therefore, it is highly impractical to purchase such programs - after all, hacking such programs is hardly more difficult and more expensive than installing them. For example, the cost of hacking a smart card is about $50,000, and development labs do not guarantee protection against hacking.

PCDST, flash drives and USB tokens are in second place in terms of value. These security tools are sold separately from the program that needs data protection, which in principle prevents information from being hacked, since there are no general schemes for hacking. Flash drives and USB tokens are personal security devices, so in order to access information, you need to access the security device directly. As a rule, the cost of such protective devices is adequate to their reliability and functionality. Against the background of the rest, software protection methods are cheaper. This is because the initial data for the program are set immediately, cannot be changed, and are part of the program itself. Protection is installed according to the same schemes and takes up memory on the hard drive, the user does not pay for information protection directly, he pays for the information itself. Also, the relatively low cost of software protection methods is explained by the ease of breakage and / or hacking. For all methods, there are the same schemes by which protection is configured. It is enough just to know such a scheme, and cracking the protection will not be difficult for a good programmer. LCDs cost a little

more due to the flexibility of the internal security system, but are also more of a proprietary security tool and don't cost much more than flash drives given their functionality.

Software protection is the most common type of protection, which is facilitated by such positive properties of this tool as versatility, flexibility, ease of implementation, almost unlimited possibilities for change and development. Another widely used protection method is secure flash drives. They are available to any user, easy to use and do not require any special knowledge to use. Only now, hacking such flash drives is quite easy. Electronic security keys, secure flash drives, smart cards and USB tokens are security tools common both among private users and among office devices such as payment terminals, bank machines, cash registers and others. Flash drives and USB tokens are easily used to protect software, and their relatively inexpensive cost allows them to be widely adopted. Electronic security keys are used when working with devices that contain information not of a specific user, but information about the entire system. Such data, as a rule, needs additional protection, because it affects both the system itself and many of its users. A system that allows programming options in smart cards and keys allows you to expand their scope by customizing the protection system for an existing operating system. For example, private clubs use keys to protect private information that is not subject to information.

Company funds, flash drives, PCDST or tokens are most prone to breakage, often due to the user's fault due to improper operation. Hacking such systems is carried out only when the carrier is physically stolen, which makes it difficult for a hacker to work. As a rule, each medium has a kernel that directly provides the protection itself. Cracking the code to such media or to its core costs about the same as the media itself, for a skilled specialist, hacking medium-protected media is not particularly difficult, so the developers are currently working not on expanding the functionality of such protection systems, but on protection from hacking. For example, the developers of the SHIPKA PCDST have a whole team that has been dealing only with the issues of protection against hacking for about two years. I must say that they succeeded in this matter. The core of the system is protected as physically and at the programming level. To get to it, you need to overcome a two-stage additional protection. However, such a system is not widely used due to the high cost of the production process of such carriers.

Software methods for ensuring information protection are also subject to hacking. Written according to the same algorithm, they also have the same hacking algorithm, which is successfully used by virus creators. In such cases, hacking can be prevented only by creating multi-stage or additional protection. As for the breakdown, here the probability that the algorithm will fail and the method will stop working is determined only by the introduction of a virus, that is, by breaking the algorithm. Physically, software methods of protecting information cannot fail, of course, therefore, it is possible to prevent the occurrence of malfunctions only by preventing the algorithm from being hacked. Smart cards have been presented as suitable for identity verification tasks because they are resistant to tampering. The embedded smart card chip usually uses some cryptographic algorithm. However, there are methods for restoring some internal states. Smart cards can be physically damaged by chemicals or technical means in such a way that the chip containing the information can be directly accessed. Although such methods may damage the chip itself, they allow access to more detailed information (for example, a micrograph of the encryption device). Naturally, there are also differences in smart cards, and depending on the developer and the price at which the smart card is distributed, the security against hacking can be different. But in each card there is still a specially developed unique code, which greatly complicates access to information.

There are smart cards that are easy to hack. But there are also cards that can only be hacked if there is special data available only to developers. At the same time, this does not mean at all that the more expensive the means of protection, the better it is. But it is impossible to judge the efficiency of even security systems of the same type, for example, about all electronic keys taken together, without considering the features of the work.

References

1. Yarochkin V. I. Information security, a textbook for universities.
2. Technical means and methods of information protection: Textbook for universities / Zaitsev A.P., Shelupanov A.A., Meshcheryakov R.V. and etc.; ed. A.P. Zaitsev and A.A. Shelupanov. - M.: Mashinostroenie Publishing House LLC
3. The Law of the Russian Federation "On State Secrets", the Civil Code of the Russian Federation of 1994, the Law of the Russian Federation "On Information, Informatization and Information Protection".
4. Galatenko V.A. Fundamentals of information security
5. Melnikov VV. Textbook for the course Methods and means of information protection.
6. Melnikov, V. V. Information protection in computer systems.