Date: 23rd June-2025

INFORMATION SECURITY IN COMPUTER TECHNOLOGIES

Matchonov Akmal
Teacher of public health technical college named after
Republic No. 1 Abu Ali Ibn Sina

Annotation: Information security is the practice of preventing unauthorized access, use, disclosure, alteration, modification, retrieval, recording, or destruction of information. This universal concept applies regardless of the form in which the information is stored. The primary goal of information security is to protect the confidentiality, integrity, and availability of information in a manner that is balanced with the appropriateness of its use and without causing any harm to the organization's operations.

Keywords: information, critical, situation, electronic, computer, security, calculator, product, rapid.

At the heart of information security is the activity of protecting information - ensuring its confidentiality, availability and integrity, as well as preventing any compromise in critical situations. Such situations include natural, man-made and social disasters, computer failures, physical theft, etc. Although the work processes of most organizations in the world are still based on paper-based documents and require appropriate information security measures, the number of initiatives to introduce digital technologies in enterprises is steadily growing. This requires the involvement of information technology (IT) security specialists to protect information. These specialists provide information security technology (in most cases, a type of computer systems). In this context, a computer refers not only to a household personal computer, but also to digital devices of any complexity and purpose, from primitive and isolated ones such as electronic calculators and household appliances to supercomputers connected via industrial control systems and computer networks. Due to the vital importance and value of information to their business, large enterprises and organizations, as a rule, hire information security specialists on their staff. Their task is to protect all technologies from malicious cyberattacks aimed at stealing confidential information or controlling the organization's internal systems.

Information security as a field of employment has developed and grown significantly in recent years. It has created many professional specialties, such as network and related infrastructure security, software and database protection, information systems auditing, business continuity planning, electronic records detection, and computer forensics. Information security specialists have high stable employment and high demand in the labor market. A large-scale study conducted by a number of organizations $(ISC)^2$ found that in 2017, 66% of information security leaders acknowledged a critical workforce shortage in their departments, and predicted that by 2022, the shortage of specialists in this field will reach 1,800,000 people worldwide.

Threats to information security can take many forms. The most serious threats for 2018 were “Crime-as-a-Service”, threats related to the complexity of Internet products, supply chains and regulatory requirements. “Crime-as-a-Service” is an example of a darknet market where large criminal communities offer a package of criminal services to emerging cybercriminals at low prices. This allows them to carry out hacking attacks that were previously inaccessible due to high technical complexity or high cost. This makes cybercrime a mass phenomenon. Many organizations are actively implementing Internet products. Since these devices are often designed without security requirements, they create additional opportunities for cyberattacks. In addition, the rapid development and complexity of Internet services reduces its transparency, which, combined with unclear legal rules and conditions, allows organizations to use personal data collected by devices without their knowledge at their discretion. In addition, it is difficult for organizations themselves to track which data collected by IoT devices is transmitted externally. The threat to supply chains is that organizations exchange a variety of valuable and sensitive data with their suppliers, as a result of which direct control over them is lost. Thus, the risk of compromising the confidentiality, integrity or availability of this data increases significantly. Today, an increasing number of new requirements from regulators significantly complicate the management of organizations' vital information assets. For example, the General Data Protection Regulation (GDPR), adopted in the European Union in 2018, requires any organization to disclose at any time the content of personal data held by it or any part of its supply chain, how it is processed, how it is stored and protected, and for what purposes it is used. In addition, this information must be provided not only during inspections by competent authorities, but also upon first request by the owner of the data. Compliance with such compliance requires significant budget and resources to be diverted from other information security tasks of the organization. While streamlining the processing of personal data implies improving information security in the long term, in the short term the risks to the organization increase significantly. Most people are exposed to information security threats in one way or another. For example, they become victims of malware (viruses and worms, Trojan horses (computer viruses) and scams), phishing or identity theft. Phishing is a fraudulent attempt to obtain confidential information (such as account, password, or credit card information). Typically, they try to lure an Internet user to a fake website that is indistinguishable from the real website of any organization (bank, online store, social network, etc.). As a rule, such attempts are carried out by mass sending of fake e-mail messages on behalf of the organization containing links to fake websites. The user opens such a link in the browser and enters his account information, becoming a prey to fraudsters. In 1964, the term "Identity theft" was introduced into the English language, in which someone's personal information (such as a name, bank account, or credit card number, often obtained through phishing) is used to commit fraud and other crimes. A person who receives illegal financial benefits, borrows money, or commits other crimes on behalf of criminals often becomes the accused himself, which can lead to serious

financial and legal consequences for him. Information security directly affects privacy, and this can be defined differently in different cultures.

Governments, militaries, corporations, financial institutions, medical institutions, and private enterprises constantly collect large amounts of confidential information about their employees, customers, products, research, and financial results. If such information falls into the hands of competitors or cybercriminals, it can lead to extensive legal consequences, irreparable financial, and catastrophic losses for the organization and its customers. From a business perspective, information security must be balanced against costs. The Gordon-Lob[en] economic model describes the mathematical apparatus for solving this problem. According to it, the main methods of combating information security threats or information risks are:

mitigation — implementing security and countermeasures to eliminate vulnerabilities and prevent threats;

transfer — transferring the costs associated with the implementation of threats to third parties: insurance or outsourcing companies;

acceptance — forming financial reserves in the event that the costs of implementing security measures exceed the potential damage from the implementation of the threat;

to renounce — to renounce an extremely dangerous activity.

With the advent of the first means of communication, diplomats and military leaders realized the need to develop mechanisms for protecting secret correspondence and methods for detecting attempts to forge it. For example, the encryption method invented by Julius Caesar in the 50s BC was developed to prevent his secret messages from being read by strangers. Secret messages were coded in such a way that they were protected and stored in special boxes in secure rooms, guarded only by trusted persons.

As a result of the development of the postal service, state organizations began to appear to receive, decrypt, read, and reseal letters. Thus, in England, the “Secret Office” was established for such purposes in 1653. Control of letters in Russia was established during the reign of Peter I, and from 1690 all letters sent abroad were controlled in Smolensk. In the middle of the 18th century, the practice of secretly copying almost all the correspondence of foreign diplomats in “black cabinets” in order to avoid any suspicions from the recipient became systematic. After opening, it was required to conduct a cryptanalysis of the message, and for this, famous mathematicians of his time were involved in the activities of the “black cabinets”. The most amazing results in this regard were achieved by Christian Goldbach. During his six-month work, he managed to open 61 letters from the ministers of Prussia and France. In some cases, even after the letter was successfully encrypted, its content was changed as a result of a man-in-the-middle attack.

In the early 19th century, with the coming to power of Alexander I in Russia, all cryptographic activities were transferred to the Ministry of Foreign Affairs. Since 1803, the famous Russian scientist Pavel Lvovich Schilling was involved in the service of this department. One of the Chancellor's most important achievements was the decoding of Napoleon I's orders and correspondence during the Patriotic War of 1812. In the mid-19th

century, more sophisticated classification systems for classified information emerged, allowing governments to manage information according to its sensitivity. For example, the British government legalized such classification to a certain extent with the publication of the Official Secrets Act in 1889.

During the First World War, multi-level classification and encryption systems were used by all belligerent countries to transmit information. This, in turn, contributed to the emergence and intensive use of encryption and cryptanalysis departments. Thus, by the end of 1914, one of the departments of the British Admiralty, “Room 40”, was formed, which became the leading cryptographic body in Great Britain. On August 26, 1914, the German light cruiser “Magdeburg” ran aground on the rocks near the island of Odensholm at the mouth of the Gulf of Finland. This island belonged to the Russian Empire at that time. The Germans destroyed all secret documents and blew up this ship. However, Russian divers, examining the underwater part, found two copies of the signal book, one of which was handed over to the British. Soon, the British, who received a book of codes for communication between auxiliary ships, as well as foreign naval vessels and enemy ships accompanying them, were able to crack the German naval codes. Breaking the code made it possible to read the enemy's intercepted radio messages. From the end of November 1914, "Room 40" began to systematically decrypt almost all the radiograms of the German fleet, transmitting orders and commands. They first used this decryption on December 16, 1914, during the approach of the German fleet to the British coast.

In the interwar period, encryption systems became increasingly complex. Therefore, special machines began to be used to encrypt secret messages. The most famous of them was the "Enigma" created by German engineers in the 1920s. In 1932, the Polish intelligence cryptography bureau managed to break the "Enigma" cipher by reverse engineering.

During World War II, the volume of information exchanged between the countries of the anti-Hitler coalition required the formal coordination of national classification systems and control and management procedures. Given the emergence of sophisticated safes and warehouses, a set of secrecy labels was developed that determined who could handle documents (usually officers, not soldiers) and where they should be stored, which were accessible only to those who handled the documents. The belligerents developed procedures for the guaranteed destruction of secret documents. Sometimes violations of such procedures led to significant intelligence gains throughout the war. For example, the crew of the German submarine U-570 failed to destroy many secret documents captured by the British. A vivid example of the use of information security tools is the aforementioned "Enigma", a sophisticated version of which appeared in 1938 and was widely used by the Wehrmacht and other services of Nazi Germany. In Great Britain, the cryptanalysis of enemy messages encrypted with the help of the Enigma was successfully carried out by a group led by Alan Turing. The Turing Bombe (from the English — “Turing bomb”) developed by them greatly helped the anti-Hitler coalition and sometimes played a decisive role in the victory of the Allies. In the United States, in the Pacific theater of operations,

signalmen were recruited from the Navajo Indian tribe, which was unknown to anyone outside the United States, to encrypt radio communications. The Japanese never managed to find the key to this exotic method of protecting information. Since the 1930s, in the USSR, in order to protect the telephone conversations of the country's highest authorities (including the Supreme Command Headquarters) from eavesdropping, a special communication system based on the sound modulation of high-frequency signals and their subsequent scrambling was used. However, the lack of cryptographic protection made it possible to reconstruct messages in the signal intercepted using a spectrometer.

The second half of the 21st century and the beginning of the 20th century were characterized by the rapid development of telecommunications, computer hardware and software, as well as data encryption. The emergence of compact, powerful and inexpensive computing equipment made electronic data processing accessible to small businesses and home users. It became easier to connect computers to the Internet, which led to the rapid development of electronic business. All this, together with the increase in cybercrime and numerous cases of international terrorism, created the need for better ways to protect computers and the information they store, process and transmit. As a result, scientific disciplines such as "Computer Security" and "Information Security Engineering" emerged, as well as many professional organizations with the common goal of ensuring the security and reliability of information systems.

REFERENCES:

1. Andress, J.. The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice. Syngress, 2014. ISBN 9780128008126.
2. Stewart, James Michael; Mike, Chapple; Darril, Gibson. CISSP® Certified Information Systems Security Professional Study Guide. Canada: Seventh Edition,John Wiley & Sons, Inc., 2015. ISBN 978-1-119-04271-6.
3. Moore, Robert. Cybercrime Investigating High Technology Computer Crime. Boston: 2nd ed., 2011. ISBN 9781437755824.
4. Ramzan, Zulfikar. Handbook of Information and Communication Security. L.: Springer Science & Business Media, 2010. ISBN 978-3-642-04117-4.
5. Johnson, John. The Evolution of British Sigint 1653–1939. Her Majesty's Stationary Office, 1998.
6. Соболева, Т. А.. Введение. История шифровального дела в России. М.: ОЛМА-Пресс, 2002. ISBN 5224036348.
7. Spies, Wiretaps, and Secret Operations An Encyclopedia of American Espionage. Santa Barbara, CA, USA: ABC-CLIO, LLC, 2011. ISBN 978-1-85109-807-1.