Malicious programs.Measures and means of information protection protection.Standards in the field of information security specifications

Prepared by: Pioner Z. Ermukhanova R. Satybaldy M. Karasay A.
Checked by: Suiinbaeva Gulder

Information

Information is derived from the Latin word informatio, which means information about the state of affairs or someone's actions, a statement, or a collection of information about something. However, data cannot be equated with information. The information contains only information that reduces the inaccuracies of the cases in which we are interested.

Information protection is a set of measures aimed at ensuring information security (integrity of information, sources of access, restrictions, use of information and its resources). A system is said to be secure if it is accessible only to a limited number of users using the appropriate information and software. Scope - read, write, create, delete. In general, there are no absolutely safe systems. Here we are talking about reliable systems. The system will be reliable - if it allows a predetermined group of users to process information on the basis of software and information equipment.

Methods of information security

Information

cryptographic

software

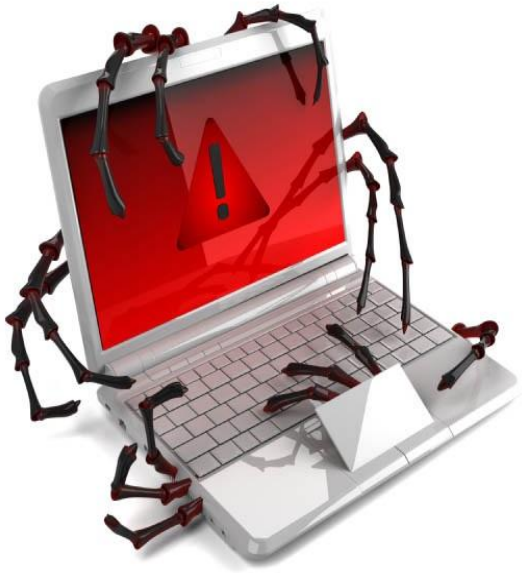
organizational

- The use of hardware methods of protection suggests the use of the following technical means:
- 1. Detector of TRD-800 category radio transmitters and tape recorders, which protects against listening and recording devices;
- 2. Modular numbers that form a hidden video surveillance;
- 3. Schemes of verification of information to ensure the accuracy of information delivery;
- 4. SAFE-400 fax message scramblers for sending confidential documents. Hardware methods of protection require a large expenditure of resources. Software methods recommend the removal of unauthorized use of computing algorithms and programs that restrict access. Software methods perform the following functions:
- 1. Identification, authentication, authorization (via Pin codes, password systems);
- 2. Backup and recovery procedures;
- 3. Active use of anti-virus programs and frequent updating of anti-virus resources; 4. Transaction processing.

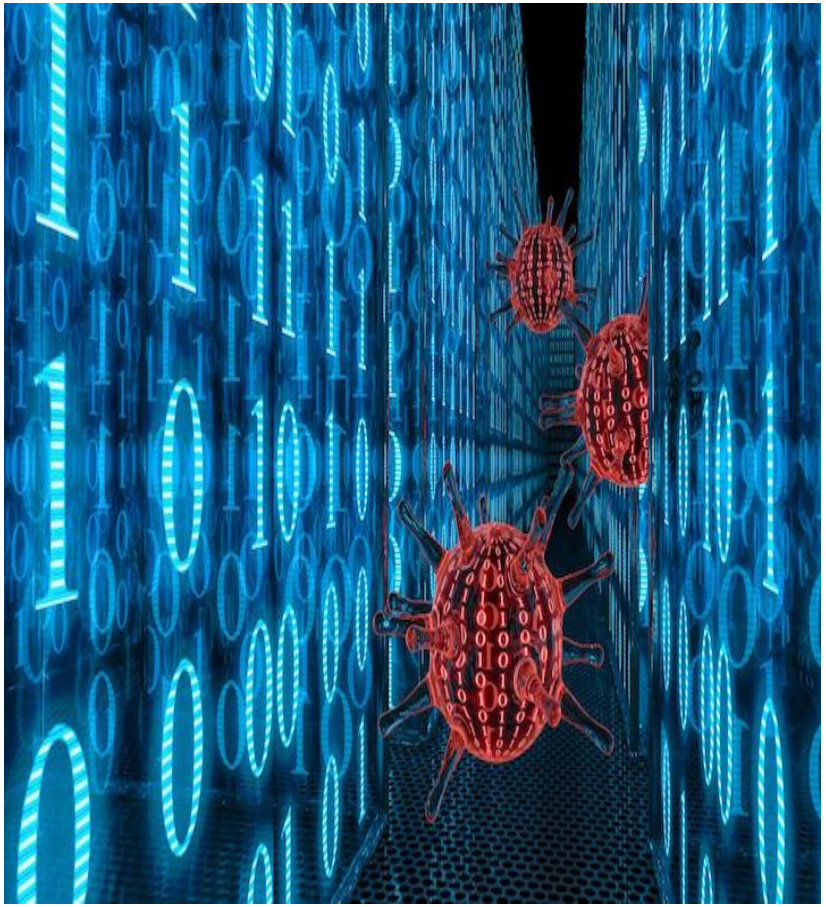
Classification of computer viruses

There are several ways to classify computer viruses:
1 By the environment in which the virus is spread
2 By the method of infection
3 On destructive possibilities
4 On the features of the working algorithm

Malicious software (malware) is software that the developer or sender has malicious intent. While many of the programs and files you install or download are completely harmless, some are designed to further create a hidden agenda, such as deleting files, stealing information, or getting paid. For a long time, malware has used various methods to obtain malware on as many computers as possible. In 1982, the first computer virus called Elk Cloner was discovered on a Mac. In 1986, the first computer malware known as Brain was released.



Malware in the 21st century



The proliferation of exploits (programs used by cybercriminals to exploit system vulnerabilities) led to the explosion of malware delivered to the Internet in the 2000s. Automated SQL injection (a method used to attack data-driven applications) and other types of mass websites increase deployment capabilities. Since then, the number of malware attacks has doubled or more each year.

Information security standards and specifications are implemented in two ways: Assessment standards, classification-oriented information systems and information security obligations; Development of technical specifications, regulations as a means of protection of various aspects. For example, normative information, which is implemented in two ways, is not displayed on the wall of silence. Assessment standards play an important role in the basic perspective of the information system, the aspect of the information system, the architectural specification.