MODULE 1
INFORMATION SECURITY THREATS

Theme 1.1 Basic Terms and Definitions in the Information Security Sphere

Information is data about persons, objects, facts, events, phenomena and processes, regardless of the form of their presentation.

Forms of information presentation:

– paper document;

– electronic document;

– physical fields.

Types of information

1. *Publicly available information* is information on the rights, freedoms and legitimate interests of individuals and legal entities and on the procedure for the exercise of rights, freedoms and legitimate interests, etc.

2. *Information of limited distribution* is information about the private life of an individual and personal data, information constituting state secrets, information constituting commercial and professional secrets, etc.

Database is a set of structured and interrelated information, organized according to certain rules on material carriers.

Data bank is an organizational and technical system that includes one or more databases and a management system.

The interconnection between information resources, systems and networks is demonstrated on Figure 1.1.

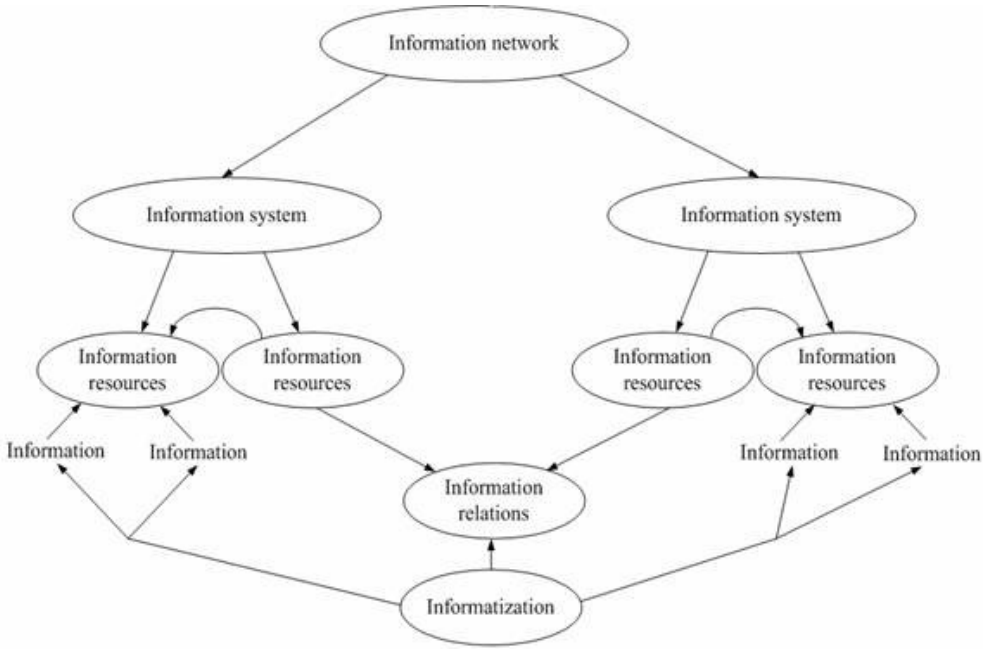

Figure 1.1 – The scheme of interconnection between information resources, systems and networks

Information network is a set of information systems or complexes of software and hardware of the information system that interact via telecommunication networks.

Information system is a set of data banks, information technologies and complex (complexes) of software and hardware.

Information resource is an organized set of documented information, including databases, other sets of interrelated information in information systems.

Information technology is a set of processes, methods of search, receiving, transferring, collecting, processing, storing, distributing and (or) providing information, as well as using information and protecting information.

Informatization is an organizational, socio-economic and scientific-technical process that provides the conditions for the formation and use of information resources and the implementation of information relations.

Information protection is a complex of legal, organizational and technical measures aimed at ensuring integrity, authenticity, security, confidentiality, and accessibility of information.

Confidentiality of information is a requirement not to allow the dissemination and / or provision of information without the consent of its holder or other grounds provided for by legislative acts.

The objectives of information protection are the following.

1. Ensuring national security of the state.

2. Preservation of information on private life of individuals and non-disclosure of personal data contained in information systems.

3. Ensuring the rights of subjects of information relations in the creation, use and operation of information systems and information networks, use of information technology, as well as the formation and use of information resources.

4. Non-admission of illegal access, destruction, modification (modification), copying, distribution and (or) provision of information, blocking of lawful access to information, as well as other illegal actions.

Directions of information protection:

– physical protection.

– information hiding.

– special check.

– control access in information networks.

– cryptographic protection.

– security of information networks.

Information security is a state of protection of balanced interests of the individual, society and the state against external and internal threats in the information sphere.

Theme 1.2 Information Security Threats Classification

Information security threat is possible impacts on the information resource leading to damage.

Classification signs of information security threats:

– kind;

– source;

– character.

Depending on the kind of threat are divided into:

– threats to confidentiality;

– threats of integrity;

– threats to accessibility.

The threat of confidentiality is the destruction of property of information to be known only to certain subjects.

The threat of integrity is unauthorized change, distortion, destruction of information.

The threat of accessibility is a nonobservance of access to information, the operability of the resource as a result of the attack on the attacker.

The source of information security threats could be:

– people;

– external environment;

– technical means;

– software.

Information security threats realized by the people are based on the methods of social engineering (see Theme 4).

Information security threats going from external environment are connected with fires, earthquakes, floods etc.

The example of information security threat realization with use of technical means is presented on movie https://www.youtube.com/watch?v=BpNP9b3aIfY.

The example of information security threat realization with use of software is presented on movie https://www.youtube.com/watch?v=MHYweIZi6Ws.

The source could be external or internal (Figure 1.2).

The character of the threat could be:

– intentional;

– random.

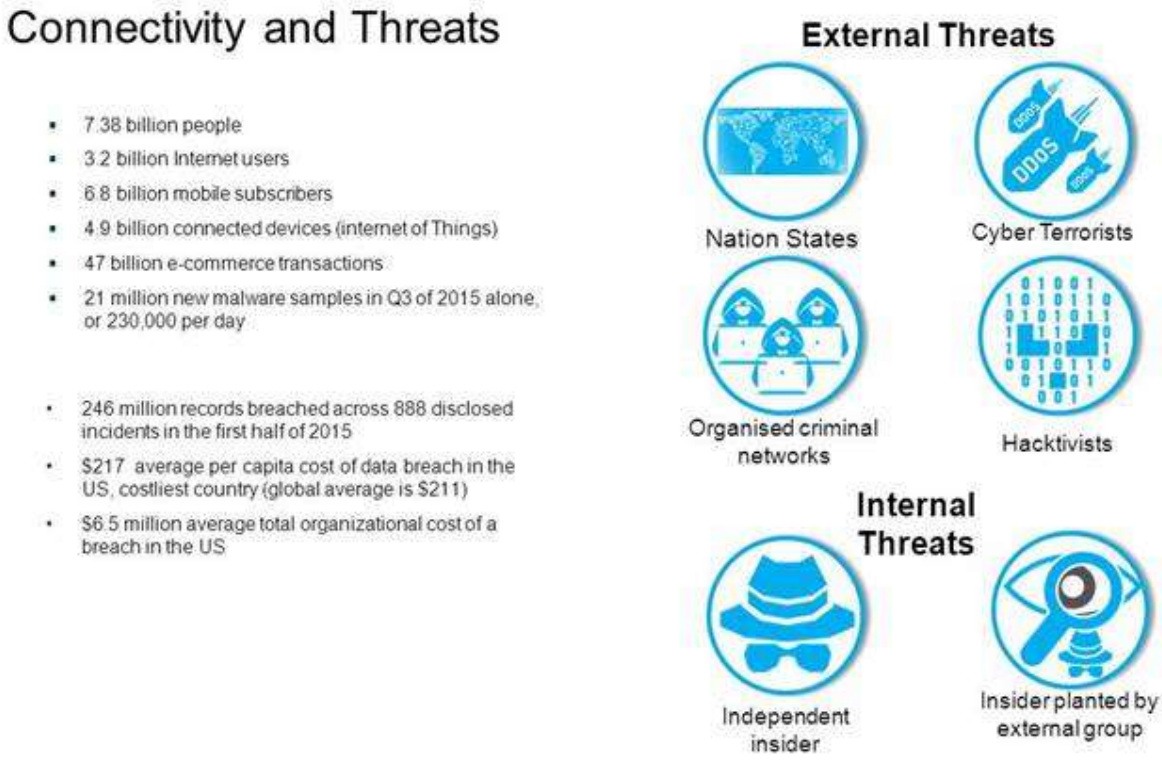

Figure 1.2 – The features of external and internal threats

Theme 1.3 Information Security Breakers Categories

From the point of view of access to the information system, information security breakers are divided into the following categories.

Category I – persons who do not have the right to access the controlled area of the information system.

Category II – persons who have the right of access to the controlled area of the information system.

Potential information security breakers are divided into 2 groups.

External breakers (carrying out attacks from outside the controlled zone of the information system) are persons of category I, as well as persons of category II, who are outside the control zone.

Internal breakers (perform attacks, being within the controlled zone of the information system) are persons of category II.

External breakers from the category I:

– former employees of the industry;

– outsiders trying to access data on an initiative basis;

– representatives of criminal organizations.

Breakers from the category II are divided into 8 groups.

1. Employees of enterprises that are not registered users and not admitted to the information system data, but have authorized access to the controlled area.

2. Registered users of the information system who have limited access to the data of this system from their workstation.

3. Registered users of the information system who have remote access to data over a local or distributed network of enterprises.

4. Registered users of the information system with the authority of the security administrator of the segment of this system.

5. Registered users with the authority of the system administrator of the information system.

6. Registered users of the information system with the authority of the security administrator of this system.

7. Persons from the number of programmers-developers of a third-party organization that are software providers and persons providing its support at the object of information system deployment.

8. The personnel serving the technical means of the information system, as well as the persons providing the delivery, maintenance and repair of such facilities.

When developing the breaker model, the following conditions are taken into account.

1. Data security is provided by means of information protection, as well as the information technologies, technical and software tools that meet them, which meet

the requirements for information protection established in accordance with the legislation.

2. Information security tools consistently operate in conjunction with technical and software tools that can affect compliance with established requirements.

3. Information security means can’t provide data protection from actions performed within the limits of the powers granted to the subject of the information system.

Theme 1.4 The Main Prerequisites of Information Security Threats. Technologies of Crime and Abuse in the Field of Information Security

The main prerequisites of information security threats are associated with the fact that information systems and networks are created and maintained by people. This leads to the fact that the main technologies of crime and abuse in the field of information security are social engineering attacks.

Social engineering is a method of unauthorized access to an information network without the use of technical means, based on the use of weaknesses of the human factor.

The terms «social programming» and «social engineering» should not be confused.

The first term is universal and is used to refer to the process of manipulating a person or people, not only to gain unauthorized access to the information network.

The second term is applicable only to indicate cases of manipulation by a person or people who are part of an information network.

The «father» of the social engineering is Kevin Mitnick (Figure 1.3).

Figure 1.3 – Kevin Mitnick

Social engineering techniques are the following.

1. *Pre-texting*. An action worked out according to a pre-compiled scenario (pretext). As a result, the object of influence must give out certain information or perform a certain action. This type of attack is usually used by phone. This technique requires any preliminary research (for example, personalization) to ensure the trust of the impact object.

2. *Phishing*. An attacker sends an object of influence a letter, forged by an official (for example, from a bank or payment system), in which it is required to "check" certain information or perform certain actions. This email usually contains a link to a fake web page that mimics the official web page, with a corporate logo and content, and contains a form that requires you to enter sensitive information (home address, bank card information, etc.).

3. *Quid pro quo (from Latin – "then for this").* An attacker calls the company, and is represented by a technical support officer asking if there are any technical problems. In case they exist, in the process of "solving" them, the impact object enters commands that allow an attacker to run malicious software.

4. *The Trojan horse*. The technique is based on the curiosity of the target object. An attacker sends an e-mail to the object containing an attachment file representing malicious software. One of the variants of the attachment file name is "critical updates", "information about employee wages", etc.

5. *«Road apple».* This method of attack is an adaptation of the «Trojan Horse» attack and consists in the use of physical media. An attacker flips a CD or USB-flash in a place where the media can be easily found. The carrier is forged under the official one, and accompanied by a signature designed to arouse curiosity.

6. *Reverse social engineering.* The purpose of reverse social engineering is to force the object of influence to independently turn to the attacker for "help". For this purpose, an attacker can use techniques of sabotage and advertising.

Theme 1.5 Software Vulnerabilities

The computing system is an interconnected aggregate of computer hardware (electronic computers) and software intended for information processing.

Principles of computing systems construction.

1. The principle of digital representation of data (a set of bits).

2. The principle of addressability of data (all data is stored in memory cells with a specific address).

3. The principle of program management (control of the computing process is realized with the help of programs stored in the memory of an electronic computer).

Software for computer systems is divided into two groups:

general (system) software;

special software.

General software is divided into the following types:

– software tools for managing data processing, including operating systems;

– service (utility) programs (utilities);

– software tools.

Special software is divided into the following types:

– application programs of general purpose;

– user applications.

The operating system is a kind of common software, through which:

– control hardware of computing equipment;

– organization of work with files;

– use of special software;

– input and output of data.

Currently, the most common operating systems are as following:

– Windows;

– Linux-kernel;

– MacOs;

– IOs;

– Android.

The main vulnerabilities of operating systems are its following functional defects.

1. Identification. Each resource in the system must be assigned a unique name – an identifier. In many systems, users do not have the opportunity to make sure that the resources they use really belong to the system.

2. Passwords. Most users choose simple password words that are easy to pick up or guess.

3. List of passwords. Keeping a list of password words in plaintext allows it to be compromised with subsequent unauthorized access to data that is protected with such password words.

4. Threshold values. To prevent unauthorized access attempts by selecting a password, you must limit the number of such attempts that some operating systems do not provide.

5. Implied trust. In many cases, operating system programs feel that other programs are working correctly.

6. Common memory. When shared memory is used, parts of RAM are not always cleaned after programs are run.

7. Break the connection. In the event of a disconnection, the operating system should not always terminate the session with the user or repeatedly request the input of the password.

8. Passing parameters by reference, not by value. When passing parameters by reference, it is possible to save parameters in RAM. After checking their correctness, the intruder can change this data before using it.

9. Difference of privileges. The operating system can contain many programs with different usage privileges.

Theme 1.6 Information Networks Security Threats

Information networks classification. Classification characteristics of information networks are the following.

1. Categories of subscribers:
– public networks;
– departmental networks.
2. Message rate:
– narrowband networks (unto 2048 kb/s)
– wideband networks (more than 2048 kb/s).
3. Scale:
– local computing network;
– corporate or regional network;
– global network.
4. Topology (switching method):
– linear network (Figure 1.4, a);
– ring network (Figure 1.4, b);
– network “star” (Figure 1.4, c);
– network “tree” (Figure 1.4, d).

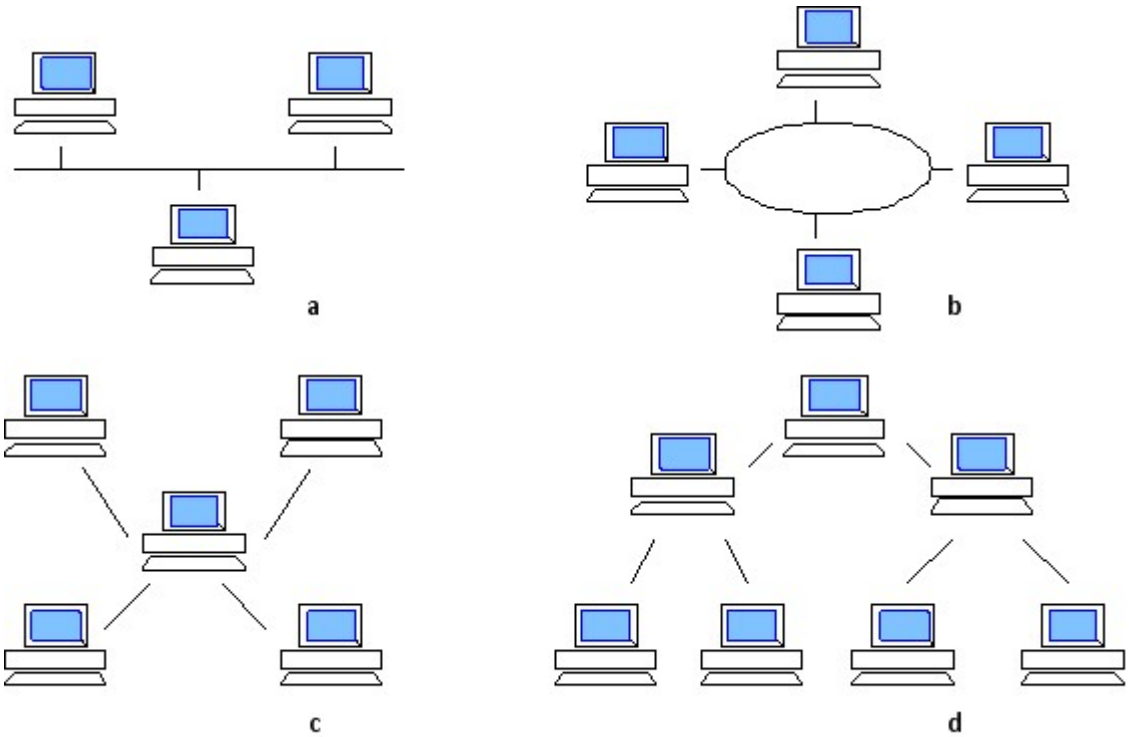

Figure 1.4 – Information networks with different topologies

5. Priority:
– peer-to-peer networks;
– client-server networks.

For client-server networks, access requirements and information security systems are increased.

Building and operating principles of wireless information networks. Wireless information networks are information networks constructed in accordance with the requirements of the IEEE 802.11 standard, in which high frequency radio waves are used for communication and data transfer between nodes, and the transmission medium is airspace.

The terms wireless information networks and Wi-Fi networks are not identical.

Wi-Fi is the name of the brand of equipment manufactured by the Wi-Fi Alliance (since 2002 – the Wireless Ethernet Compatibility Alliance), which can be used to receive and transmit information in wireless information networks.

The full name of the trademark is Wi-Fi CERTIFIED Miracast™ (derived from two English words Wireless Fidelity – «wireless reliability»).

Ways of using of wireless information networks:

– as a section of a wired information network (for connecting two remote segments of the network);

– as an independent local information network in cases where the organization of a wired network is difficult or the cost of building such a network is less than the cost of organizing a wired network.

According to the IEEE 802.11 standard:

– the transmission of information should be realized through frequency channels in the spectra of 2.4 GHz and 5 GHz;

– the provided information transfer rate is about 430 Mbps;

– the modulation is MIMO (Multiple Input Multiple Output) is used; this modulation is based on the use of multiple antennas, respectively, creating a lot of information flows, which increases the data transfer speed.

Frequency distribution by channels is demonstrated on Figure 1.5.

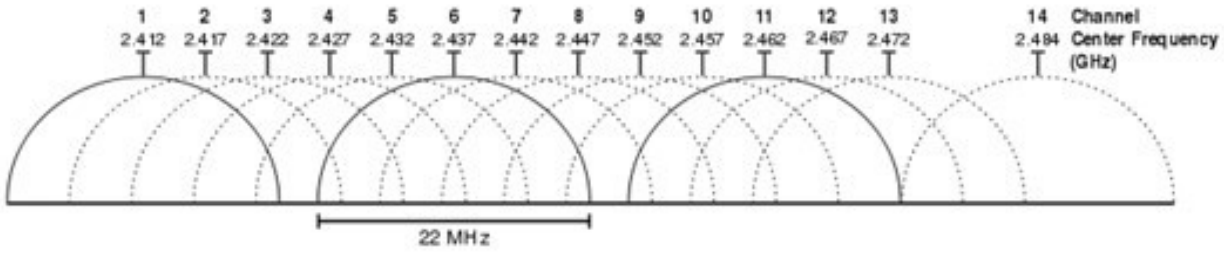

Figure 1.5 – Frequency distribution by channels

2 modes of operation of wireless information networks defined by the IEEE 802.11 standard.

1. Ad-hoc mode (“point-point”) is a network, the communication in which between client stations is established directly, without using an additional access point.

2. “Client-server” mode. It consists of several access points connected to a wired network, and a set of wireless stations (clients). Due to the fact that the network provides access to the file server, database server, printer and other devices, this mode is most often used.

Depending on the range of operation the wireless information networks are divided into the following types.

1. WPAN (Wireless Personal Area Network): the range of operation is up to 100 m. They are serviced by the user or by the system administrator (telecommunications operator is not involved). The most popular among WPAN-networks is Bluetooth.

2. WLAN (Wireless Local Area Network): range of operation – from 100 to 300 m. Can be used within one or more adjacent rooms. One of the types of equipment used to build such networks is equipment manufactured by the Wi-Fi Alliance (Wi-Fi equipment).

3. WMAN (Wireless Metropolitan Area Networks): range of action is up to 50 km (distributed information networks of urban scale). Purpose – the addition or replacement of the infrastructure of cable city information networks (“last mile”), used for high-speed Internet access and telephony. An example is WiMAX (Worldwide Interoperability for Microwave Access – Worldwide Networking for Microwave Access).

There are following types of wireless networks:

– network on the radio modem;

– network on a cellular modem;

– infrared systems;

– system VSAT (Very Small Aperture Terminal);

– system using low-orbit satellites;

– radio relay systems;

– laser communication systems.

Information security threats in wired information networks. The result of the implementation of threats to the security of data in information networks is unauthorized access to this data.

Unauthorized access is the user's access to an object for which he does not have permission in accordance with the organization's security policy**.**

Methods of implementing unauthorized access:

– interception of secondary electromagnetic emissions from information network equipment;

– attacks using algorithmic and program errors of information networks («hidden channels», «masquerade», «garbage collection», «hatch»);

– attacks using malicious software («Virus», «Worm», «Trojan Horse»).

Attacks using algorithmic and program errors in information networks.

1. «Hidden channels» attack. In an access-sharing information network, the user may not be allowed to read and / or modify the data of interest, but may use indirect paths for this.

2. Attack of the “masquerade”. Performing any action by one network user on behalf of another user. In this case, such actions may be allowed to another user. The violation consists in the assignment of rights and privileges.

3. Attack “garbage collection”. After the end of the work, the information being processed is not completely deleted from the memory. Part of the data can remain in the RAM. With the use of special software and equipment, an attacker can restore the information being processed.

4. Attack of the “hatch”. “Hatch” is a hidden undocumented entry point to the program module that is built into the program at the stage of its debugging. In the event that the programmer has not removed the “hatch”, the attacker can use this point to unauthorized access to the data.

Attacks using malicious software (malware). Depending on the algorithm of work, malware is divided into the following types:

– “virus”;
– “worm”;
– “Trojan horse”;
– rootkit;
– backdoor;
– “loader”.

“Virus” is a self-replicating program code that is embedded in the installed programs without the user's consent and damage the operating system.

Polymorphic “virus” is a kind of “viruses” that modify their code in infected programs in such a way that two instances of the same “virus” may not coincide in any bit. Such «viruses» encrypt their code.

“Worm” is a type of malware that distributes as files through local or global networks, leaving its copy on storage media for long-term storage. In the algorithms of its operation, information network scanning engines are used to determine the host on which a malicious file can be transmitted.

“Trojan horse” is a type of malware that is activated when a certain triggering condition occurs. Usually it is masked for useful utilities, game or entertainment programs.

“Rootkit” is a type of malware, in the algorithm of which it is provided to hide the malicious code and its actions from the user and antivirus software due to faster loading than the operating system.

"Backdoor" or RAT (Remote Administration Tool) is a type of malware used by an attacker to remotely manage an information system.

"Loader" is part of the malware code used for its further implementation into the information system by downloading from a remote server.

Information Security Threats in Wireless Information Networks. The main security threats in wireless information networks:

– unauthorized access;

– denial of service;

– passive monitoring.

Unauthorized access. By connecting to a wireless information network, an attacker can access data stored on other devices connected to the network. Connection is realized through a unauthorized access point, which does not provide encryption and through which it is possible to access the network without going through the authentication procedure.

Denial of service:

– mass distribution of packets, for which all network resources are involved, as a result of which it ceases to function; the distribution is realized using special software available for downloading on the Internet;

– carrier sense access: translation of a powerful radio signal whose amplitude exceeds the amplitude of the carrier signals used to transmit data in the wireless information network; this leads to the deactivation of access points;

– installation of metal shields near the access points of wireless information networks, which will lead either to a decrease in the amplitude of the carrier and modulated signals, or to the appearance of interference signals.

Passive monitoring. Using the programs AirMagnet and AiroPeek, an attacker, connecting to a wireless information network, can disclose the contents of packets transmitted over this network.