Western European Journal of Linguistics and Education
Volume 2, Issue 7, July, 2024
https://westerneuropeanstudies.com/index.php/2
ISSN (E): 2942-190X Open Access| Peer Reviewed

THE ESSENCE AND TASK OF THE PROBLEM OF INFORMATION PROTECTION IN INFORMATION AND TELECOMMUNICATION NETWORKS

Artikova Gulzoda Gulomjonovna
Teacher of TATU Urganch branch
gulzodaartiqova281@gmail.com

The widespread use of computer technologies in automated systems of information processing and management has intensified the problem of protecting information circulating in computer systems from unauthorized access. Information protection in computer systems has a number of specific features related to the fact that information is not strictly connected to mass media, it can be easily and quickly copied and transmitted through communication channels. A large number of threats to information are known, which can be carried out by both external attackers and internal attackers.

Three groups of problems are most relevant in the field of information protection and computer security in general:

1. breaking of confidentiality of information;
2. breaking of the integrity of information;
3. disruption of information and computing systems.

When it comes to state, diplomatic, military, industrial, medical, financial and other confidential information, information protection is becoming the most important problem of state security. Large arrays of such data are stored in electronic archives, processed in information systems and transmitted through telecommunication networks. The main features of this data - confidentiality and integrity must be confirmed by law, legal, as well as organizational, technical and software methods.

Confidentiality of information (Latin confidentialia - confidence) involves the introduction of certain restrictions on the range of persons who have the right to access this information. The level of confidentiality is a certain mark subjectively determined by the owner of the information depending on the content of the unknown information (highly important, top secret, confidential, for official use, not for publication, etc.) is represented by intended for a limited number of people, it is considered a secret when it is disclosed to the public. Naturally, the specified level of confidentiality of data must be maintained during processing in information systems and transmission through telecommunication networks.

Another important feature of information is its integrity (integrity). Information is indispensable if it accurately (adequately) reflects its subject area at any time. The integrity of information in information systems is ensured by timely input of reliable (correct) information, confirmation of the truth of information, protection from corruption and destruction (deletion).

Unauthorized access to information by unauthorized persons, intentional or unintentional errors of operators, users or programs, incorrect changes of information due to equipment failures lead to the violation of these important characteristics of information and make it unusable and even dangerous. Its use can cause material and/or moral damage, so creating an information security system becomes an urgent task. Under information security (information security) understand the security of information from its unwanted disclosure (violation of confidentiality), destruction (violation of integrity), loss or reduction of the level of availability of information, as well as its illegal duplication.

Information security in an information system or telecommunications network is ensured by the ability of this system to maintain its confidentiality during the process of inputting, outputting, transmitting, processing and storing information, as well as to resist its destruction, theft or damage. Information security is ensured by organizing access to it, protecting it from interception, tampering and entry of false information. For this, physical, technical, hardware, firmware and software protection tools are used. The latter occupies a central place in the system of information security in information systems and telecommunication networks.

Security duties:

- protection of information in communication channels and databases by cryptographic methods;
- confirmation of authenticity of data objects and users (authentication of communicating parties);
- detection of violations of the integrity of data objects;

to provide protection against electronic devices installed for obtaining information;

- to ensure protection of software products and computer equipment from introducing software viruses and bookmarks into them;
- protection against unauthorized actions in the communication channel of persons who are not allowed to use encryption tools, but who aim to destroy confidential information and disrupt the work of subscriber stations;
- organizational and technical measures aimed at ensuring the preservation of confidential information.

Fixed Broadband Radio Access System

An analysis of the evolution of user access technologies in the last decade shows that there is now a wide range of wireless user access technologies for providing multimedia services. Modern radio communication systems are built according to the following standards:

- HyperLAN 2;
- MMDS;
- WLL;
- FBWA (IEEE 802.11/b/g series).

Consider these known radio access systems in the order listed above. HiperLAN 2 is based on a newly developed radio technology developed specifically for LAN communication as part of the broadband project. Radio Introduction Networks (BRAN) implemented by the European Telecommunications Standards Institute (ETSI), radio technology - orthogonal frequency division multiplexing (Orthogonal Frequency Division Multiplexing, OFDM), its implementation is a very serious technical problem.

The most attractive feature of HiperLAN2 is its high speed, which is sometimes incorrectly called 54 Mbit / s. In fact, the nominal radio transmission speed is 54 Mbps, but typical speeds for applications are closer to 20 Mbps. Another feature is QoS support, which is very important for applications such as video and speech. The HiperLAN2 architecture allows for connectivity to a variety of network types, including Ethernet (which will be among the first to be supported), IP, ATM, and PPP. Building networks based on HiperLAN2 technology requires large investments for the following reasons:

- First of all, the single widely used WLAN standard was proposed by IEEE, not ETSI at all.
- Second, IEEE already has several wireless LAN standards, including the 802.11a standard, which provides a transmission speed of 54 Mbit/s.
- Thirdly, none of the companies that supported the HiperLAN2 project are recognized leaders in the field of local networks. This HiperLAN2 technology operates in the 5 GHz band, which is currently unlicensed. In order for HiperLAN2 public networks to provide a truly broadband connection, they must have several access points and several channels that provide freedom of movement in a defined area.

Information protection when using HiperLAN2 technology includes authentication and encryption, which provides temporary cryptographic strength of data transmitted on the communication line against unauthorized disclosure. In addition, the technical implementation of channel multiplexing with orthogonal frequency division increases data security due to the large uncertainty in the selection of carrier frequency parameters.

The MMDS system (Microwave Multipoint Distribution Service - Microwave multipoint distribution systems) has become widespread in recent years as an alternative to classic cable networks, in which the distribution network is built by laying coaxial or optical cables. The ability to combine MMDS systems with high-speed wireless digital data exchange makes it easier to solve the "last" mile problem, providing a broadcast radius limited to the horizon line (about 60 km).

User requested data is transmitted downstream on digital channels using QPSK, 16, 32-, 64-, 128-, or 256-QAM modulation. At the same time, depending on the channel width and the selected signal modulation scheme, one channel with a width of up to 8 MHz provides a data transfer rate of up to 56 Mbit / s. time, which is 1000-1500 times faster than an analog telephone modem (33.6 Kbps), 200-400 times faster than an ISDN line (64 and 128 Kbps). The radius of the service area of the MMDS system is determined by the height of the transmitting antenna, the transmitting power, the number of transmitted channels, losses in the antenna-feeder path, and the gain of the transmitting and receiving antennas. . A number of advantages of the MMDS system were identified during construction and operation. The main disadvantage of the technology is the high cost of the equipment, a large number of employees. The organization of information security in the MMDS system is similar to the previously discussed information security in the HiperLAN2 system.

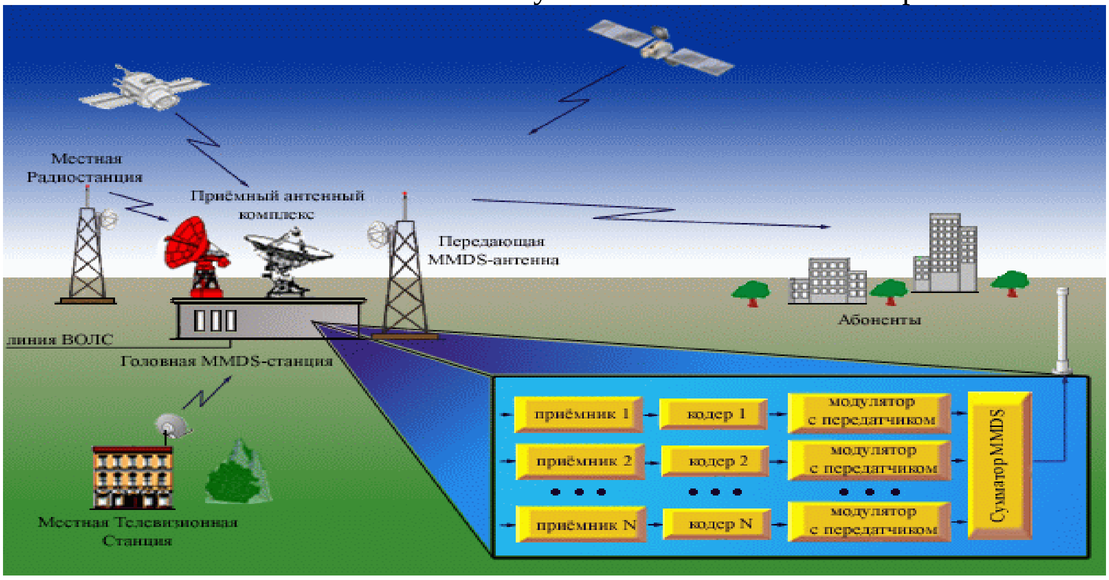

Figure 1. WLL fixed wireless connection systems (WLL -Wireless Local Loop).

In the late 1980s - early 1990s, it was developed to solve a very urgent problem - expanding the service area of automatic telephone exchanges. The name of this class of systems also defines their purpose - to provide traditional telephony services to subscribers located outside the service area.

WLL systems operate in the frequency range of 1.5 to 3.5 GHz, and networks based on WLL systems are built on a cellular basis. WLL systems include:

a central station (CS) that provides connection and control of the entire network;

relay stations (PK) that provide continuous coverage of the service area and expand the service area to several hundred kilometers;

3) terminal stations (TS) installed in service areas;

4) maintenance system implemented as software at the level of management of network elements and installed on a personal computer.

WLL systems provide PSTN services (telephony, fax and data transmission using dial-up modems) to subscribers located tens of kilometers away. The main disadvantages of these systems are the high cost, the complexity of installing and using the equipment.

In the WLL system, information security is achieved by means of specific addressing of the message sent to the user and organizational measures to receive service personnel to the base stations of the network.

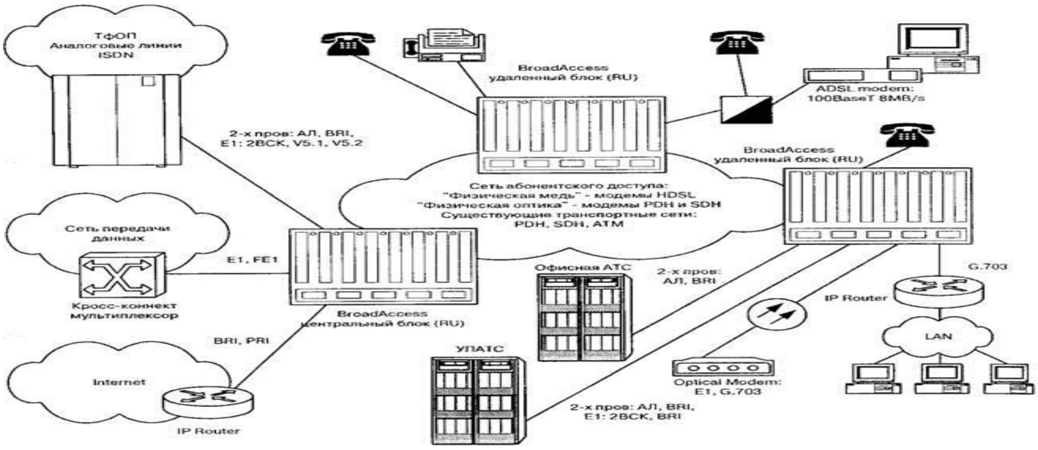

Figure 1.2 Structure of WLL technology

The development of FBWA class systems depends on several factors:

1) almost universal need for information;

2) the emergence of a wide range of high-speed transport technologies;

3) development of the concept of building new generation networks that provide unified management of all types of traffic in multi-service communication networks.

FBWA systems are designed to provide modern services to individual and corporate users.

FBWA class solutions currently offered on the telecommunications market almost do not have relay stations, which limits the radius of their service area to the limits of one cell of the cellular system.

FBWA systems use the network principle of building a central station containing several receivers serving each sector, and several radio channels can be organized in each sector.

Terminal stations of FBWA systems provide connection to various services for a wide range of individual and corporate users, including LAN, PBX, Frame networks, etc.

Finally, in addition to providing access services to users, FBWA systems are widely used as wireless metropolitan networks to provide transport services (for example, to connect base stations to mobile network switches).

A comparative assessment of the reliability of information protection in the above systems of access to information resources of local networks shows that when choosing a method of ensuring information security, priority should be given to modern FBWA systems with great prospects for their development and reasonable price. and frequency legitimacy. Therefore, in the thesis, we will pay extra attention to the review of this FBWA system.

Conclusion: Confidentiality involves restricting access to information to authorized individuals, which is crucial for state security and sensitive sectors like military, financial, and medical fields. Integrity ensures that information remains accurate and uncorrupted, reflecting the true state of its subject area. Information security aims to protect data from unauthorized access, destruction, and corruption through a combination of physical, technical, hardware, and software measures.

Wireless communication technologies such as HiperLAN2, MMDS, WLL, and FBWA offer various methods of providing access to information services. Each technology has its own advantages and challenges regarding speed, coverage, and security. HiperLAN2 offers high-speed connectivity and QoS support but requires significant investment and is limited by the need for multiple access points

MMDS provides a viable alternative to cable networks with high data transfer rates but comes with high equipment costs and complex installations. WLL systems are designed for telephony services in areas beyond traditional service ranges but are also costly and complex.

Among these, FBWA systems stand out for their modern, high-speed transport technologies, making them suitable for individual and corporate users. They also serve as efficient wireless metropolitan networks for transport services. FBWA systems, with their promising development prospects and reasonable costs, are recommended for ensuring reliable information protection.

References

1. BenHaddouN.,Ez-zahraouyH.,RachadiA. Implantation of the global dynamic routing scheme in scale-free networks under the shortest path strategy, Phys. Lett. A.,380(2016), pp.2513-2517
2. Matyoqubovich, M. O. (2021). On A Methods Of Using Weighted Simulation Improving Reliability To Redundant Fiber Optic Communication Systems. Turkish Journal of Computer and Mathematics Education (TURCOMAT), 12(5), 1538-1550
3. Olimboy Olimov, Gulzoda Artikova and Mavluda Xatamova 2024. IPERF TO DETERMINE NETWORK SPEED AND FUNCTIONALITY. *Web of Technology: Multidimensional Research Journal*. 2, 3 (Mar. 2024), 94–101.
4. Olimov Olimboy. Gulzoda Artikova (2024). MULTISERVICE NETWORK SERVICES. *Web of Humanities: Journal of Social Science and Humanitarian Research*, *2*(2), 101–104. Retrieved from https://webofjournals.com/index.php/9/article/view/844
5. G'ulomjonovna A. G., Rustamboyevna J. M. ANALYSIS, ADVANTAGES AND DISADVANTAGES OF MICROSCHETS USED IN IOT TECHNOLOGY //INTERNATIONAL SCIENTIFIC CONFERENCES WITH HIGHER EDUCATIONAL INSTITUTIONS. – 2023. – T. 1. – №. 05.05. – C. 478-481.
6. Rustamboyevna, Jumaboyeva Marhabo, and Artikova Gulzoda G'ulomjonovna. "PRINCIPLES AND TECHNOLOGIES OF SMART CITY BUILDING." *INTERNATIONAL SCIENTIFIC CONFERENCES WITH HIGHER EDUCATIONAL INSTITUTIONS*. Vol. 1. No. 05.05. 2023.