This paper presented encryption model of transmission medical data and rules and facts of attacks related to subjective deliberate threats. This model is the construction and design of expert systems for telemedicine networks and medical data leakage channel. System algorithm rules and facts of attacks related to subjective deliberate threats are based on theoretical and practical facts.

References

1. Review of ICT development in Uzbekistan 2006-2008, ICTP_Review_2008_RU_part_07.

2. Fundamentals of Information Security. Textbook for universities/ E.B.Belov, V.P.Los, Mesch R.V. Mershyakov, A.A. Shelupanov. -M.: 2006. - 544

3. S.V. Vikhorev, R.Y. Kobtsev "How to identify the sources of threats ?" / / Open Systems 7-8/2002, number. http://www.elvis.ru/files/howto.pdf.

4. "ENCODINGS OF MEDICAL DATA BY SOFTWARE TRANSMISSION TO OPEN COMMUNICATION LINKS OF VIPNET", Collection:- Mathematics, science, science in the economy and in society "(MIESEKO 2014), Moscow December 31, 2014.

5. www.mednet.ru. 6. www.wikipedia.org/wiki/IPv6.

6. Hopgood, Adrian A. Intelligent systems for engineers and scientists / Adrian A. Hopgood.--2nd ed. CRC Press Boca Raton London New York Washington, D.C.2000, 34- 49 pp.

D. Nurjabova

APPLICATION OF NEW METHODS AND METHODS CYBER CRIMINALISTICS

(Tashkent University of Information Technologies Karshi brnach,department"Software Engineering"
Shukurova Markhabo Tashkent University of Information Technologies Karshi brnach,department"Information technologies")

Abstract. This article is devoted to application of new methods and methods cyber criminalistics. Problems of cybercrime are considered in this article and given new methods .

Key words: cyber, criminalistics, cybercrime.

We live in the information space. I can not say exactly how this information closer to reality or engage in fraud on the Internet, hacking passwords large company sites or e-mail to threaten a person's life on the Internet, engage in hacking and other place around us every second growing cybercrime. What is cybercrime, and when there was this term in the Criminal Code. Computer security experts are well aware of the term and know what kinds of threats are struggling with them and define the concept of cybercrime.

Cybercrime- crimes committed by people using information technologies for criminal purposes. In foreign countries, particularly the United States, have become widespread fraud related to the sale of domain names made a mass mailing e-mail messages in which, for example, the report attempts to unknown persons register domain names similar to addresses belonging to the recipients and site owners are invited to register unnecessary their domain name to get ahead of these persons. So, shortly after the attacks of September 11, 2001 US Federal Trade Commission said the fact the mass sale of domain names zone "usa". This group of infringements are a special part of the institution of criminal law, the responsibility for these acts can not accommodate the Criminal Code of the Republic of Uzbekistan. As an independent institution for the first time not isolated and requires special adopted article which refers to sub institute "Crimes against public safety and public order." Kinds of objects are considered crimes of public relations related to security of information and information processing systems by a computer.

Cybercrime information are: illegal access to computer information, creation, use and distribution of malicious computer programs.

Violation of the rights of information and unauthorized access to information remains a mystery sometimes, about the concept of cybercrime identified which is studying science Cybercrime happening crime with information technology.

Fighting to cybercrime requires international co-operation, etc. This adoption of the Convention of the Council of Europe.

Council of Europe Convention on Cybercrime, cyber crime divides into four groups.

• The first group of offenses against the confidentiality, integrity and availability of computer data and systems are: illegal access (Art. 2), illegal interception (v. 3), the impact on computer data (wrongful intentional damage, deletion, deterioration, alteration or suppression of computer data) (Art. 4) or the system (Art. 5). Also in this group of crimes included illegal use of special technical devices (v. 6) - software designed or adapted for the commission of offenses set forth in Art. 2 - 5, as well as computer passwords, access codes, their analogues, by which can be accessed by the computer system as a whole or any part thereof). Rates Art. 6 apply only if the use of (distribution) of special technical devices aimed at the commission of unlawful acts.

• The second group consists of crimes associated with the use of computer tools. These include fraud, forgery and use of computer technologies (Art. 7 - 8). Forgery using computer technology includes malicious and unlawful entry, modification, deletion or suppression of computer data, entailing inauthentic data with the intent that it be considered or acted upon for legal purposes as authentic.

• The third group of production (for distribution through a computer system), supply and (or) provision for the use, distribution and purchase of child pornography and possession of child pornography in a computer memory (v. 9).

• The fourth group consists of offenses related to infringements of copyright and related rights.

Under the Convention, each State Party is required to create the necessary legal conditions for the provision of the following rights and duties of the competent authorities to combat cybercrime: seizure of a computer system or part of the carrier; manufacturing and confiscation of copies of computer data; ensure the integrity and preservation of stored computer data relating to the case; destruction or suppression of computer data in a computer system.

The Convention also requires the necessary legal conditions for a touch of Internet providers to collect and fixing or intercept the information you need with the help of available technology, and promote the law enforcement agencies. It is recommended to oblige providers to maintain absolute confidentiality about the facts of this cooperation.

In early 2002, was admitted to Protocol N 1 of the Convention on Cybercrime, which adds to the list of crimes of dissemination of racist and other nature, inciting to violence, hatred or discrimination against a person or group of persons based on the racial, ethnic, religious or ethnic affiliation .

The next step interaction with the subject is a subject of authentication. Authentication of the subject - is the subject of authentication with the ID. The authentication procedure determines whether the subject is what he himself declared.

After identification and authentication of the subject of the authorization procedure is performed. Under the threat of information security in computer network (COP) to understand an event or action that may cause a change in the functioning of the COP related to violation of protection of the processed information in it. Vulnerability information - is the possibility of such a state in which the conditions for the implementation of information security threats.

The attack on the Constitutional Court referred to the action taken by the infringer, which is to search for and use of a particular vulnerability. In other words, an attack on the COP is the implementation of information security threats in it.

Problems arising from the security information transmission when the computer networks can be divided into three main types:

• interception of information - data integrity is preserved, but her privacy violated;

• modification of information - the original message is changed or completely replaced by others, and sent to the addressee;

• substitution of the authorship information. This problem can have serious consequences.

The specifics of computer networks, in terms of their vulnerability, mainly associated with the presence of an intense information exchange between geographically dispersed and diverse (heterogeneous) elements.

Vulnerable are literally all the main structural and functional elements of the CS: workstations, servers (Host-machine), bridging (gateways, switching centers), communication channels, etc.

A large number of diverse security threat information from various sources. In literature there are many different classifications, where the dividing criteria used types of

dangers posed by the degree of malice, source of the threats, etc. One of the most basic classifications is shown in Fig. 1.

Natural threat - the threat is caused by exposure to the elements of the COP and its objective physical or natural processes of nature, beyond the control of man.

Artificial threat - a threat to the COP caused by human activity. Among them, based on the motivation of actions can be distinguished:

- unintended (inadvertent, accidental) threats caused by errors in the design of the COP and its components, software errors, errors in the actions of personnel, etc .;
- deliberate (intentional) threats associated with selfish aspirations of the people (hackers).

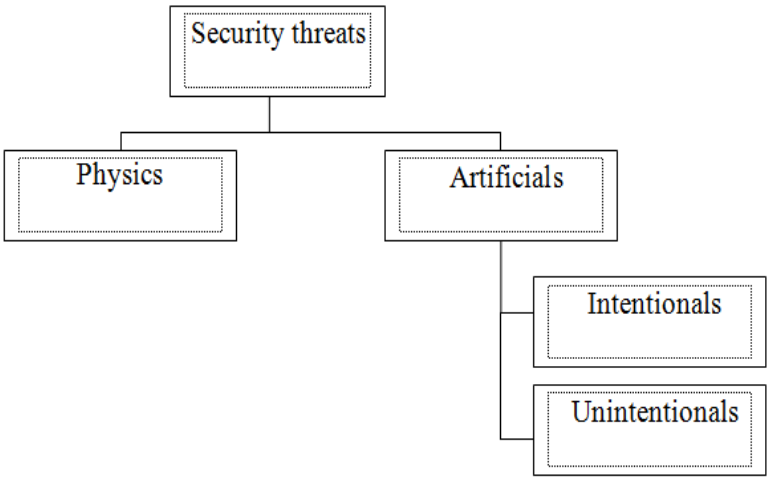

Fig. 1. General classification of security threats

According to international standard GOST R ISO / IEC 17799-2005, the information security policy should establish the responsibility of management, as well as to present the organization's approach to managing information security. In accordance with this standard requires that the information security policy of the enterprise as a minimum, include:

- definition of information security, its overall objectives and scope, as well as disclosure of the importance of security as a tool that provides the ability to share information;
- presentation of the purposes and principles of information security formulated by the leadership;
- summary of the most important for the organization of security policies, guidelines, rules and regulations, such as:
- comply with legal requirements and contractual obligations;
- requirements for security training;
- prevention and detection of viruses and other malicious software;
- business continuity management;
- responsibility for violations of security policy.

- definition of general and specific obligations of employees in the management of information security, including information on incidents of violation of information security;
- links to documents that complement the information security policy, for example, more detailed policies and procedures for specific information systems, as well as the safety rules to be followed by users.

Information Security Policy of the company must be approved by management, published and communicated to all employees in an accessible and understandable form.

References

1. The Council of Europe Convention-11.12.2008, www.coe.int
2. Fundamentals of Information Security. Textbook for high schools / EB Belov, VP Moose, RV Meshcheryakov AA Shelupanov. -M.: 2006 - 544
3. Vikhorev SV Kobtsev RY How to determine the sources of threats? // Open systems №7-8 / 2002. http://www.elvis.ru/files/howto.pdf.
4. GOST R ISO / IEC 17799-2005.
5. ISO / IEC 17799: 2000 (BS 7799-1: 2000).

D.M. Umurzakova

INFORMATION SECURITY AND DATA PROTECTION

(TUIT Fergana branch, Uzbekistan)

The emergence of new information technologies and the development of powerful computer storage and information processing systems increased the levels of information security and necessitated that the effectiveness of information security grow along with the complexity of the data storage architecture. So gradually the protection of economic information becomes mandatory: all kinds of documents for the protection of information are being developed; the recommendations on information protection are formed; even carried out a federal law on information protection, which deals with the protection of information and the task of protecting information, and also solves some unique issues of information protection.

This, the threat of information security has made the means of ensuring information security one of the mandatory characteristics of the information system.

The phrase "threats to the security of information systems" refers to real or potentially possible actions or events that are capable of distorting data stored in the information system, destroy them or use them for any purposes not provided for by the rules in advance.

Protection of information from computer viruses (protection of information in information systems) involves means of protecting information on the network, or more specifically, software-based information security that prevents the unauthorized execution of malicious programs that attempt to seize data and send them to an attacker, or destroy database information, but protection information from computer