Radkovich Maria
Magister,
Scientific supervisor: **Sapun A.L.**,
Phd pedagogical science
Chief of information technology and modeling of economical process
Belarusian State Agrarian Technical University,
Minsk, Belarus

APPLICATION OF INFORMATION TECHNOLOGIES IN ECONOMIC OFFENSES

Currently, you can notice the intensive development of information technology. Computers are an integral part of modern society. Computers help us in many tasks. However, the experience of developed foreign countries suggests that computers can also be used to commit crimes.

Information is subject to legal regulation. Information is not a material object, but it is fixed on material carriers. Initially, information is stored in a person's memory, and then it is alienated and transferred to tangible media: books, discs, tapes, and other drives designed to store information. As a result, information can be replicated by distributing the material carrier. The transfer of such a material carrier from the owner-subject that creates specific information to the user-subject entails the loss of ownership of the information owner.

Until recently, it was believed that computer crime exists only in foreign capitalist countries, and in the CIS countries, in particular, the Republic f Belarus, due to weak computerization, is absent altogether. In our opinion, it is this circumstance that led to the insufficient study of this problem. The very emergence of computer crime in our country leads to the conclusion that this phenomenon is characteristic of all states that, due to their scientific progress, are entering a period of widespread computerization of their activities [1].

The method of committing a crime is made up of a complex of specific actions of the offender in preparing, committing and disguising a crime. Usually, the criminals, by committing these actions, leave certain traces, which later allow to restore the picture of what happened, to get an idea about the originality of the criminal behavior of the offender, about his personal data. Domestic forensic science began to seriously address the issue of characterizing methods of committing computer crimes only in the early 90s. In this regard, we are almost 20 years behind foreign researchers. In my opinion, our researchers need to use the experience of foreign colleagues.

Currently, there are over 20 basic methods of committing computer crimes and about 40 of their varieties. And their number is constantly growing. I will highlight 6 main groups of methods of committing computer crimes. Classifying sign - the method of use by the offender of those or other actions aimed at gaining access to the means of computer equipment with different intentions:

- withdrawal of computer equipment;
- interception of information;
- direct interception;
- electronic interception;
- audio interception;
- video interception.

Effective protection of the rights and interests of citizens can only be ensured by applying the full range of measures, both organizational and technical, and legal. In the republic, at present, objectively the grounds have been laid for the criminalization of such offenses - crimes against information security, which requires the introduction of appropriate amendments and additions to the current legislation.

Almost all types of computer crimes can be somehow prevented. World experience suggests that law enforcement agencies must use various preventive measures to accomplish this task. In this case, preventive measures should be understood as activities aimed at identifying and eliminating the causes of crime, and the conditions conducive to their commission. There are three main groups of measures to prevent computer crimes:

1) legal;

2) organizational and technical;

3) forensic.

Economic crimes are the most common, carried out with mercenary purposes (fraud; theft of programs, services, computer time; economic espionage). Crimes against personal rights and the private sphere (collection of compromising data on individuals; disclosure of banking, medical and other private information; obtaining data on income or expenses).

Descending from the results of the study of foreign researchers on this issue, it is now possible to highlight the five most common motives for committing computer crimes, presented in the following diagram:

As a rule, 52% of crimes are related to the theft of money; 16% - with the destruction and destruction of computer equipment; 12% - data substitution; 10% - with theft of information and software; 10% - due to the theft of services [2].

The experience of operating existing computer systems for processing economic information shows that the problem of ensuring security is still far from being resolved, and the remedies offered by the manufacturers of various systems vary greatly in both the tasks and methods used and the results achieved.

This determines the urgency of the problem of building secure systems for the processing of economic information, the solution of which should begin with an analysis of the causes of the situation.

References

1. Denisevich, A.V. Theoretical foundations of building a system of ensuring the economic security of the Republic of Belarus / A.V. Denisevich // Problems of management. - 2014. - N11. - P. 121 - 124.

2. Vasilenko N.A. Crimes in the sphere of information technology (cyberpress) // Start in science. - 2016. - № 5. - p. 31-34. URL: http://science-start.ru/ru/article/view?id=428 (appeal date: 03/14/2019).