A. Omelyanovich
Research supervisor: I. G. Kopytich
Senior Lecturer,
Baranovichi State University
Language tutor: I. G. Kopytich

CYBERCRIME

Since the use of protective measures or measures to combat any phenomenon is impossible without understanding the essence of this phenomenon, scientists, researchers and legislators all around the world have attempted to define the concept of "cybercrime" and to formulate criteria for its separation from other illegal acts.

Cybercrime is any crime in the electronic sphere committed with the help of a computer system or a network or against it."

Features of this type of crimes:

– extreme secrecy of acts achieved through the use of anonymity and encryption;

– cross-borderness, the criminal and the victim can be separated by thousands of kilometers, borders of several countries;

– non-standard ways of committing;

– automated mode [1].

The Council of Europe Convention organize all the types of cybercrime into five groups.

1) All computer crimes against computer data and systems (e.g. illegal access, interference with data or system in general).

2) Illegal acts related to the use of technologies (forgery, extraction, blocking or modification of data, obtaining economic benefits by other means.

3) Offences relating to the contents if the data or content.

4) Violation of copyright, the allocation of certain types of crimes attributed to the legislation of specific states.

5) Cyberterrorism and the use of virtual space for committing acts of violence, as well as other acts that infringe on public security [2].

The number of cybercrime is steadily increasing, over the past five years, their number ranges from 8 thousand to 17 thousand.

The legislation of most countries of the world assumes criminal liability for the commission of crimes of this type. Effective counteraction is possible only at the level of international cooperation. Carrying out preventive work with the population, representatives of business structures plays an important role in the fight against crime. The security of cyberspace in general and their personal data and funds in particular also depends on citizens in many respects.

Here are some specific recommendations:

– ignore phone calls, text messages, messages on winnings from unfamiliar numbers, never call back to them, don't send any messages;

– don't tell anyone the details of your plastic card; with all the questions you have, contact directly to the Bank branch;

– install a reliable anti-virus on your gadgets and regularly conduct a full system scan. Here you can learn what to do when you were charged with creating a virus;

– buy only licensed software.

References

1. Киберпреступления [Electronic resource]. – Режим доступа: https: //urist.one/dolzhnostnye-prestupleniya/ kiberprestuplenie.html – Date of access: 21.03.2018.

2. Cybercrime [Electronic resource]. – Режим доступа: https://www.interpol.int/Crime-areas/Cybercrime/Cybercrime – Date of access: 24.03.2018.