Nyrko I., Cadet of the National Academy of Internal Affairs

CYBERCRIME IN UKRAINE

Cybercrime is an action; illegal access; illegal interception; interference with data or system; abuse of devices; fraud; offenses related to child pornography; violation of copyright and related rights; violations of the confidentiality, integrity and availability of computer systems, networks, and computer data, as well as the abuse of such systems, networks, which leads to criminal liability [1].

This is a fast-growing area of crime. Today the cybercrime is one of the most dynamic groups of socially dangerous attacks. The

rapid spread of those crimes and its social danger (which does not have any physical or virtual limits) cause the real threat to people around the world. More and more criminals are exploiting the speed, convenience and anonymity of the Internet to commit a diverse range of criminal activities. However, the Ukrainian legislator pays considerable attention to this problem: new Criminal Code of Ukraine anticipated an independent chapter of these crimes - section XVI "Crimes in usage computers, systems and networks and telecommunication network": twice this section has been changed and supplemented - this indicates the relevance of this problem in society [2]. Cybercrime became more serious than 5 years ago. Despite the effort of law enforcement agencies to fight the cybercrime, the rate of these crimes are not decreasing, but growing.

There are two types of cybercrimes: Traditional crimes, which caused by computer technologies and network: Violation of copyright and related crimes (art. 176); Fraud (art. 190); Illegal actions with documents of transfer, payment cards and other means of access to bank accounts, equipment for its manufacture (art. 200); Evasion of taxes, duties (mandatory payments) (art. 212); Import, production, sale and distribution of pornographic items (art. 301); Illegal collection or usage of information constituting commercial or banking secrets (art. 231) [3]. New crimes, which are committed by latest computer technologies (crimes that provided by section XVI of Criminal Code of Ukraine). New trends in cybercrime are emerging all the time, with estimated costs to the global economy running to billions of dollars. New cybercrimes have divided into other types: Fraud with credit cards; Fake online auctions; Fraud with bank loans; Search and usage of bugs in applications; Spam; Online gambling; Ransom and registration of domain names; Theft of services (telemarketing); Virus creations; Theft of information and personal data; Theft of false new in electronic mass media, etc.

Security Service of Ukraine and National Police, as an agent of cybercrime control, are fighting against hackers. However, it is not enough. If before Ukrainian programmers were writing viruses to hack and steal data from rich Western countries, so nowadays due to

increased security protection level from US and EU, their crimes turned to Ukraine. The laws should respond to current development of technologies. The priority area is to organise the interaction and coordination between legal body, special services, judiciary, and to provide the necessary material and technical base. None of the countries can resist cybercrime on its own. The campaign against these crimes require social efforts from country, citizens and the international community[4].

List of reference:

1. Поняття та сутність кібернетичноїзлочинності. URL: http://legalactivity.com.ua/index.php?option=com_content&view=article&id=1425%3A091216-07&catid=170%3A5-1216&Itemid=211&lang=en.

2. Поняття та зміст кіберзлочинності. URL: http://goal-int.org/ponyattya-ta-zmist-kiberzlochinnosti/.

3. Кіберзлочинність в Україні. URL: https: //www .science -community.org/uk/node/16132.

4. Кіберзлочинність у всіх її проявах: види, наслідки та способи боротьби. URL: https://www.gurt.org.ua/articles/34602/