Єгоров Д., магістр ННІ № 2 Національно академії внутрішніх справ
Консультант з мови: Лопутько О. А.

CYBERCRIMES IN UKRAINE: THE MODERN CHALLENGES AND THE WAYS TO DEAL WITH THEM

At the present stage of social development, cultural and economic relations in our country, Ukraine require special attention to a number of issues in combating cybercrime. Crimes in before mentioned field are demonstrating both quantitative and qualitative growth. These offenses are becoming more complex and increase the level of anti-social orientation. The spread of computer crimes has led to the need of studying this phenomenon, making recommendations how to combat this type of crimes. The widespread introduction of computer technology in all areas of modern life along with the simplicity of access to a global network of personal and industrial devices have not got only positive effects. One of the negative ones is the increasing threat of cybercrime. As modern society becomes more reliant on digital technology, it is also becomes more vulnerable to cyber-attacks such as corporate security breaches, spear phishing attacks and social media fraud. Moreover, the cyber threat has morphed over the last decade. Previous activity

was based on cleverly crafted attacks by skilled individuals. In contrast, modern cybercrime has become industrial in scale and approach: cheap, mass-produced and easily accessible. Hacking communities, discussion groups and online walkthroughs are plentiful and easy to find. [7]

Cybercrime as a phenomenon appeared in the information technology evolution process and nowadays cyber criminals operate remotely, using special kind of software called malware (malicious software). It includes next types of malware:

• Viruses - small pieces of software programs that can replicate itself and come from one computer to another by attaching themselves to other computer files in order to gain access to, steal, modify and/or corrupt information and files from a targeted computer system.

• Worms - programs that seek to damage networks and often deliver payloads which allow remote control of the infected computer by exploiting weaknesses in operating systems. Worms are self-replicating and do not require a program to attach themselves to. Worms continually look for vulnerabilities and report back to the worm author when weaknesses are discovered.

• Spywares/Adware s- programs that by opening attachments, clicking links or downloading infected software, spyware/adware are installed on your computer. Their aims are to take control on your computer and/or to collect personal information without your knowledge.

• Trojan - a software program appears to perform one function (for example, virus removal) but actually acts as something else. It is aiming to create a ‘backdoor’ on computer by which information can be stolen and damage can be caused.

There are also a number of attack vectors available to cyber criminals who allow them to infect computers with malware or to harvest stolen data:

• Phishing - an attempt to acquire users’ information by masquerading as a legitimate entity. Examples include spoof emails and websites.

• Pharming - an attack to redirect a website's traffic to a different, fake website, where the individuals' information is then compromised.

• Drive-by - opportunistic attacks against specific weaknesses within a system.

• MITM ('Man in the middle attack') - where a middleman impersonates each endpoint and is thus able to manipulate both victims.

•Social engineering - exploits the weakness of the individual by making them click malicious links, or by physically gaining access to a computer through deception [8].

As we mentioned above, such criminal activities are operated remotely so they are committed not only in virtual space of particular country, they are international or so-called "transborder" by their nature.

It is worth to be mentioned, that it is easy for qualified offenders to hide the evidence of their activity that is why they become a great threat to Cybersecurity of Critical Infrastructures around the world. Nowadays, financial institutions, transport, medicine are dependent on the reliable operation of computer equipment [1].

That is why cyber police need modern technology to trace hackers and Internet frauds successfully. It was confirmed by the Director of the Ukraine IT Association. "Criminals have very high skills and sufficient resources to commit cybercrimes. The cyber police must have the appropriate technical equipment to be able to fight criminals effectively", said Victor Valeyev. [5]

However, due to the long absence of the forensically important information about computer crimes, cybercrime counteractions were not always systematic. Therefore, the first phase of organizational measures against computer crime is to be informational -analytical work. We ought to create a system of computer crimes registration, statistical reporting, working out on analytical sectors activity order and regulatory legal acts, which regulate activity (cooperation) of specialized cybercrime combating agencies. Obtained during the first phase data should be the basis for a more complete and comprehensive analysis of socially dangerous acts [4]. Since the

cybercrimes mostly have transborder nature from the expert in the field of cyber security both knowledge in the sphere of information technology and language proficiency for cooperation at the international level and quick information uptake from foreign sources are required.

The cybercrime investigation at the present conditions of international computer networks is complicated for the following reasons:

- Criminal acts may take place in cyberspace. To identify and investigate computer crimes, that mean any crimes committed by using computer or telecommunications network, special knowledge of investigative procedures and appropriate legal powers are required;

- International computer network such as the Internet is an open environment that allows users to do certain actions outside the borders of the states in which they reside. At the same time, investigatory-operative measures of law enforcement agencies are limited to the territory of their own countries. This means that the fight against crimes in open computer networks cannot be made without adequate international cooperation;

- Openness of global information networks allows users of those countries, in which the actions are spent in a cyberspace not to be pursued by the law. Such countries create possibilities to avoid punishment for persons from those countries where such actions, according to the internal legislation fall under criminal responsibility.

Given the importance of these issues, the Council of Europe adopted Convention on Cybercrime.

The Convention on Cybercrime, also known as the Budapest Convention on Cybercrime or the Budapest Convention, is the first international treaty seeking to address Internet and computer crimes by harmonizing national laws, improving investigative techniques, and increasing cooperation among nations [3]. It was drawn up by the Council of Europe in Strasbourg, France, with the active participation of the Council of Europe's observer states Canada, Japan, South Africa and the United States.

It was opened for signature in Budapest, on 23 November 2001 and it entered into force on 1 July 2004. On September 2015,

47 states have ratified the convention, while a further seven states had signed the convention but not ratified its [1].

The Convention is the first international treaty on crimes committed via the Internet and other computer networks, dealing particularly with infringements of copyright, computer-related fraud, child pornography, hate crimes, and violations of network security. It also contains a series of powers and procedures such as the search of computer networks and lawful interception.[3]. By the 7 of September 2005 this convention has been fully ratified by our country. [6].

However, since no state can protect itself by taking action only at national level for effective counteraction of cyber criminality the following steps are necessary:

- Harmonizing the domestic criminal substantive law elements of offences and connected provisions in the area of cyber-crime;
- Providing for domestic criminal procedural law powers necessary for the investigation and prosecution of such offences as well as other offences committed by means of a computer system or evidence in relation to which is in electronic form;
- Setting up a fast and effective regime of international cooperation;
- Establishing a mechanism for resolving jurisdictional issues in cyberspace.

As to the conclusion we may say, that international cooperation is crucial in eliminating the legal vacuum existing between the development of information technology and legislation response. The process of acting at the international level, as the experience itself is a complex problem. But there is no other way to ensure the safety of users and the state from electronic attacks and to provide effective means of investigation and cybercrime prevention.

Список використаних джерел:

1. Гуцалюк М. Перший міжнародний стратегічний конгрес «E-CRIME 2002» / М. Гуцалюк // Крок. - 2002. - №° 24.

2. Бутузов В. М. Злочини із застосуванням сучасних інформаційних технологій // Науково-практичний журнал

“Боротьба з організованою злочинністю і корупцією” - 2003. - № 7.

3. Convention on Cybercrime/ [Електронний ресурс] - Режим доступу: https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561.

4. Бутузов В.М. “Особливості планування заходів по запобіганню та протидії злочинам у сфері високих технологій” Матеріали міжвузівської науково-практичної конференції 14 грудня 2007 року: Боротьба зі злочинами у сфері комп’ютерної інформації: проблеми та шляхи їх вирішення - Донецьк: ДЮІ ЛУНВС, 2007.

5. Урядовий кур’єр [Електронний ресурс]. - Режим доступу : http://ukurier.gov.ua/uk/artides/kiberpolicejski-reaguvatimut-na-zlochini-c ilo dob ov/

6. Про ратифікацію Конвенції про кіберзлочинність: закон України від 7 верес. 2005 р. № 2824-IV.// Відомості Верховної Ради України. - 2006. - № 5-6.

7. Andy Thomas. How cybercrime became industrial-scale [Електронний ресурс] - Режим доступу: http://www.information- age. com/how-cybercrime-became-industrial-scale-123461446/

8. Anderson K. Virtual Hostage: Cyber terrorism and politically motivated computer crime [Електронний ресурс] / Kent Anderson. Cyber terrorism and politically motivated computer crime // The Prague Post. - 2010.