Petrushka O.V., Ph.D. in Economics,

Associate Professor of Department of Finance named after S. I. Yuriy

Ternopil National Economic University, Ternopil

**CYBER CRIMES AS A TYPE OF FINANCIAL SCAM:**

**CONSEQUENCES FOR THE STATE**

Modern life cannot be imagined without the use of computer systems and the Internet. Any activity of the person, enterprise and the state is connected with the use of computer equipment, various means of communication, and other technical means which on the one hand have considerably simplified a life of mankind as they have created preconditions for formation of the only information space in which everyone who wishes can get an access to any information in a few seconds, the ability to manage assets remotely and to carry out all business transactions regardless of its location, and on the other hand – they have created the preconditions for the development of crimes in the same information space, in addition, these crimes began to acquiring features of anonymity. The biggest threat is that these crimes are becoming global and causing huge losses.

Thus, theft of payment card data (bank accounts) or data on access to the Internet banking system in order to seize the funds of bank customers, theft of personal data and commercial information from private computers or servers, intentional damage to information systems or communications to create losses to companies is not a complete list of such threats posed by the rapid development of modern information technology, and accordingly stands out in such a concept as cybercrime [1].

Cybercrime is a type of financial crime committed by an individual or organized groups of individuals and is the theft of funds and other assets using modern technology.

Recognizing the need of cooperation between states and private enterprises to combat cybercrime and the need to protect legitimate interests in the use and development of information technology, on September 7, 2005 Ukraine ratified the Convention on Cybercrime [2], the ratification of which was necessary for the latter, as it is obvious that our state is not an isolated country and its economy is part of the world economy. That is why any cybercrime will affect the entire world economy and each country in particular.

Ukraine, like all countries in the world, faces daily challenges in the field of cybersecurity. During the last few years, government agencies have been repeatedly attacked from cyberspace. One of such attacks was the launch of the virus type of Petya on June 27, 2017, which caused disruption of Ukrainian state-owned enterprises, institutions, banks, media and others. As a result of the attack, the activities of such enterprises as Boryspil Airport, ChNPP, Ukrtelecom, Ukrposhta, Oschadbank, Ukrzaliznytsia, etc. were blocked. In addition, the information systems of the Ministry of Infrastructure, the Cabinet of Ministers, the websites of the Lviv City Council, the Kyiv City State Administration, the cyberpolice and the special services of Ukraine were infected [3].

During 2018, the police discovered 6,000 crimes committed in the field of high information technology. If to analyze that in terms of types, the great share of cybercrime falls on crimes in the field of payment systems, in 2018 the number of such crimes was 2398. As for cybersecurity and e-commerce, the number of crimes in 2018 was 1325 and 1598, respectively. Also, about 700 crimes were registered in the field of illegal content [4].

It should be noted that to establish the real financial losses from the actions of cybercriminals is extremely difficult and almost impossible. This is due to the fact that some companies that have suffered from hacking may partially hide the damage, and to the fact that they often estimate the value of data that has been stolen. In addition, the losses of companies should also include costs associated with the elimination of the consequences of cybercrime, disruption of the smooth operation of IT systems, loss of intellectual property, etc.

Thus, today cybercrime as a type of financial fraud is rapidly developing both in Ukraine and around the world. Victims of cybercrime can be individuals and companies, states. The most dangerous thing about the development of cybercrime is that a virus that can be run from a single computer can easily paralyze the work of any company, group of companies, individual state, union of states, or the world economy as a whole. All this leads to significant financial losses, and on a global scale may even lead to the beginning of the economic crisis.

**References:**

1. Cybercrime and money laundering. Department of Financial Investigations. State Financial Monitoring Service of Ukraine. URL: https://Users/User/Downloads/tipolog2013.pdf (access date: 07.07.2020).

2. Convention on Cybercrime of September 7, 2005 №994-575. URL: https://zakon.rada.gov.ua/laws/show/994\_575#Text (access date 06.07.2020).

3. Niculesco D. Cybersecurity: vulnerabilities. *Legal newspaper Online*. 2019. URL: https://yur-gazeta.com/publications/practice/inshe/kiberbezpeka-vrazlivi-momenti.html (access date: 07.07.2020).

4. Official site of the cyberpolice of Ukraine. URL: https://cyberpolice.gov.ua/ (access date: 07.07.2020).