інноваційний сектор; гармонізація діяльності Державної служби фінансового моніторингу та правоохоронних органів у сфері легалізації тіньових капіталів; розробка комплексної теоретико-методичної бази визначення обсягів та протидії кримінальній та тіньовій активності; активізація участі у міжнародній системі протидії іллегалізації економічної діяльності на різних рівнях міжнародного співробітництва [1].

ЛІТЕРАТУРА:

1. *Варналій З. Детінізація економіки як чинник розвитку підприємництва / З. Варналій, З. Живко // Стратегічні пріоритети. – 2013 – № 4 (29).*
2. *Тіньова економіка в Україні: причини та шляхи подолання // Міжнародний центр перспективних досліджень. [Електронний ресурс]. – Режим доступу: http://icps.com.ua/assets/uploads/files/t_novaekonom_kaukra_ni.pdf*
3. *Харазішвілі Ю. Щодо методології комплексного оцінювання складників економічної безпеки держави / Ю. Харазішвілі, А. Сухоруков // Стратегічні пріоритети. – 2014. – № 3 (38). – С. 5-15.*
4. *Friedrich Schneider The Shadow Economy and Work in the Shadow: What Do We (Not) Know? // Discussion Paper No. 6423 March 2015. – Born, 2015.*
5. *World economic outlook April 2017 // IMF Data mapper. [Electronic resource]. – Access: http://www.imf org/external/datamapper/index.php*

UDK 343.33

Farion A.
PhD, Associate Professor of the Department of Economic Security and Financial Investigation, Ternopil National Economic University

CYBER PERPETRATION EXPERIENCED GLOBALLY

Cybercriminal activity is one of the biggest challenges that people faced in this century. Cybercrimes are divided into two groups: cyber dependent crimes and cyber enabled crimes. According to Sean O'Neil … 'Cyber Dependent Crimes … include attacks on computer systems to disrupt IT infrastructure, and stealing data over a network using malware…' and 'Cyber Enabled Crimes' existing crimes that have been transformed in scale or form by their use of the Internet…' [1]. High level of cybercrimes may be explained by theft triangle reasons and all categories of cybercriminals are interconnected with them (fig.1).

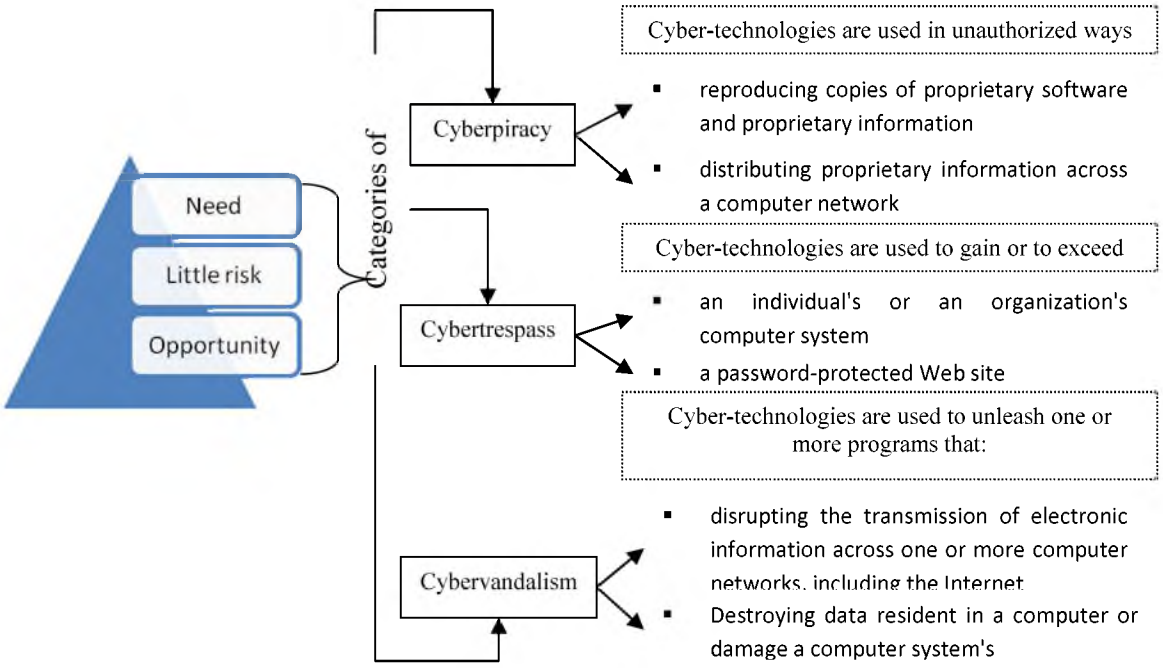

Fig. 1. Theft triangle reasons and categories of cybercrimes that are interconnected with them

Cybercrime is offenses ranging from criminal activity against data to content and copyright infringement[1]. 'Computer and online crime is different from crime in the 'real world'. It's not tangible or visible to most people and hard to resolve…'[2]. Cybercrimes are carried out by criminals using computers, or other devices, with a special requirement – availability of connection to the internet. The probability to be targeted is very big if you use the Internet, devices can become infected within 5 minutes. Because many people download programs to see pictures, hear music, or get other features from web sites but they are not familiar with. The existence of adequate legislation isn't essential for fighting cybercrime. It could be proofed by indicators (fig. 2) [3].

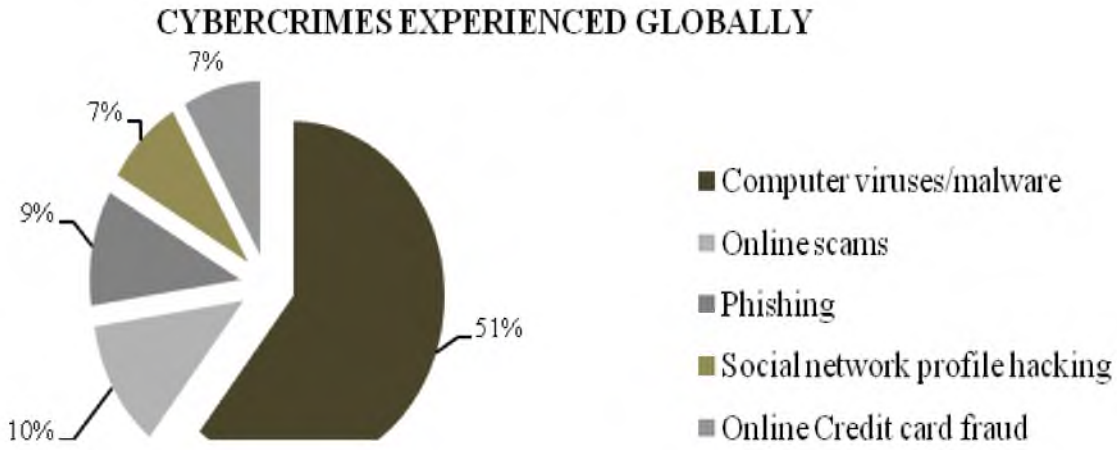

Fig. 2. Cybercrimes experienced globally

[1] Council of Europe's CC Treaty
[2] Anne Collier, Editor of NetFamilyNews.org & Co-chair of the Online Safety & Technology Working Group and Report collaborator

Most of criminals are faceless that causes the main problems in their searching (fig. 3) [3].

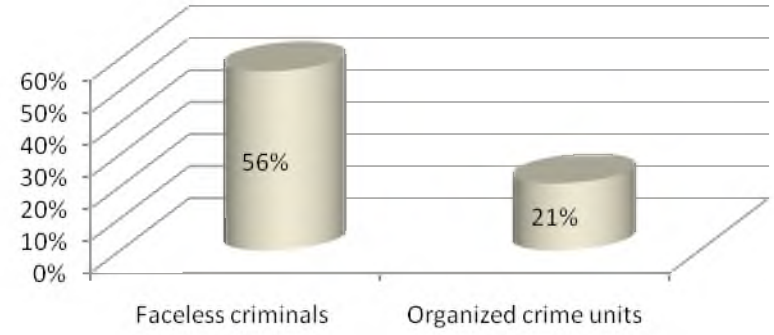

Fig. 3. The proportion of unknown and organized criminals units that are involved in cybercrimes acts

The cybercrime statistics proof that 2016 and 2017 were defined in rapid growth in mischievous and harmful online criminality, as well as rapid increasing of digital crimes [5]. Cybercrime was the 2-nd most reported crime in 2016 and it cost the global economy over $ 450 billion. It is predicted that cybercrime will cost the world $6 trillion annually by 2021. This increasing are based on hundreds of major media outlets, universities and colleges, senior government officials, associations, industry experts, the largest technology and cybersecurity companies, and cybercrime fighters globally (fig. 4) [6]. The cost of cybercrime will continue to increase in the future as more and more business functions move online and as more companies and consumers around the world connect to the Internet

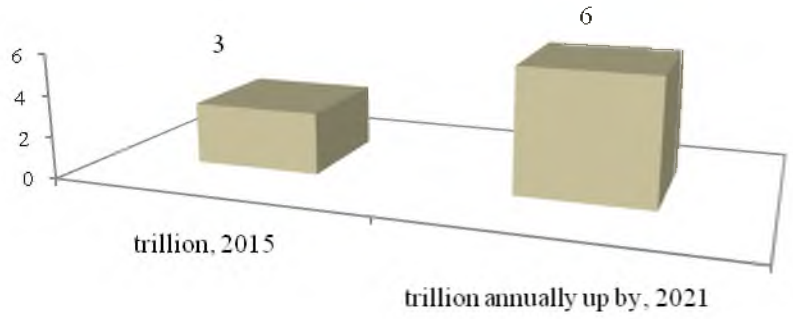

Fig. 4. Prediction for increasing of cybercrimes cost from annually by 2021

In the global economy it's indicating by tendency that four main industries are under the big danger of cyberattack: healthcare, financial service, manufacturing and government.

However the most important cost of cybercrime comes from its damage to company performance and to national economies. Cybercrime cost $600 billion to the businesses in 2017 that is equated to 0.8% of global GDP. Also it could be proof that the countries with higher losses from cybercrimes are the richest ones. And cybersecurity law cannot protect appropriately all parts of cyberspace. Problems must be decided onto micro level, companies must pay considerable attention to a set of managerial improvements (fig. 5).

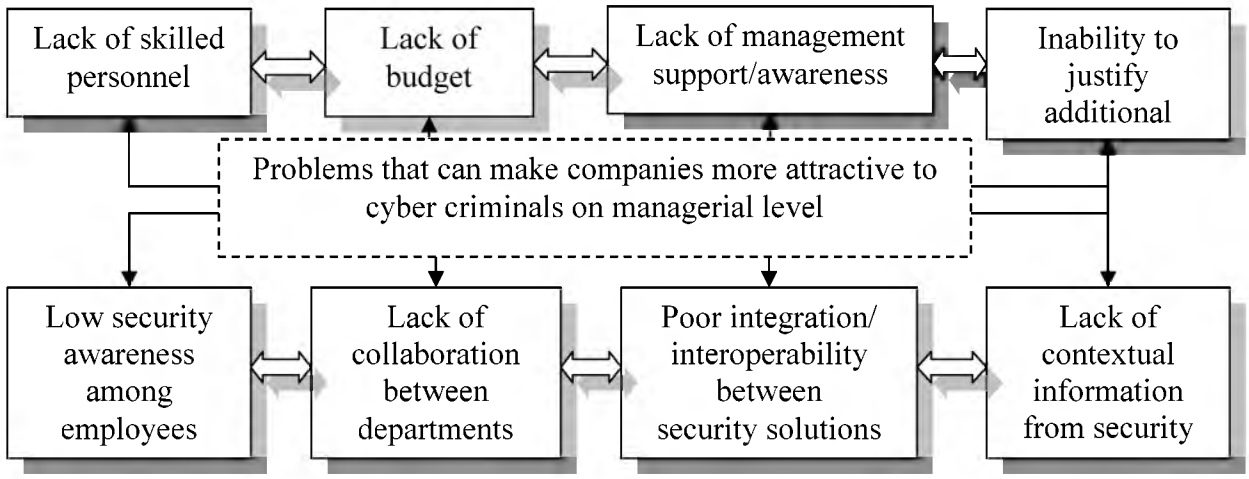

Fig. 5. Set of problems that make companies more attractive to cyber criminals

Last scientific investigation shows that the best methods of fighting with cybercrimes are high quality professionals and appropriate IT protection system.

REFERENCES:

1. Sean O'Neil Tackling Cyber threats together. [Electronic resource]. – Access: http://webcache.googleusercontent.com/search?q=cache:DH7g10QapPQJ: www.localinstitutes.cii.co.uk/media/8787/cyber-protect-may-17-law-society-presentation.pptx+&cd=2&hl=uk&ct=clnk&gl=ua&client=aff-maxthon-maxthon4

2. Introduction to Cybercrime. [Electronic resource]. – Access: http://webcache.googleusercontent.com/search?q=cache:yE_YX-YVPxEJ:www.personal.utulsa.edu/~james-childress/cs5493/Resources/Abstracts/NienhausCybercrime.ppt+&cd=6&hl=uk&ct=clnk&gl=ua&client=aff-maxthon-maxthon4

3. Norton cybercrime report. The Human Impact. [Electronic resource]. – Access: https://www.symantec.com/content/en/us/home_homeoffice/media/pdf/ cybercrime_report/Norton_USA-Human%20Impact-A4_Aug4-2.pdf

4. Comparitech 100+ Terrifying Cybercrime and Cybersecurity Statistics & Trends [2018 Edition]. [Electronic resource]. – Access: https://www.comparitech.com/vpn/cybersecurity-cyber-crime-statistics-facts-trends/

5. PWC. Pulling fraud out of the shadows. Global Economic Crime and Fraud Survey 2018. [Electronic resource]. – Access: https://www.pwc.com/gx/en/forensics/global-economic-crime-and-fraud-survey-2018.pdf

6. Cybersecurity ventures. Cybercrime report. [Electronic resource]. – Access: https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/