Cybercrimes, Cyber Law and Computer Programs for Security

Antonina Farion[1], Valentyna Panasyuk[2]

1. Department of Economical Security and Financial Investigation, Ternopil National Economic University, UKRAINE, Ternopil, 46 A Mykulynetska str., email: secretmail_antonina@ukr.net

2. Department of accounting in the industrial sphere, Ternopil National Economic University, UKRAINE, Ternopil, Peremohy Square 3, email: Tina.panasjuk@gmail.com

Abstract: **In this document we describe the situation that was formed at the information market colligates with the increasing the level of cybercrimes. Law regulation of this sphere can't follow the development of information technology that exacerbates the problems of cybercrime. At the individuals' level cybercrime is associated with the using of pirated software: malicious people can access the user's personal date**.

Keywords: **information technology, cyberspace, intellectual property, cyber security, antivirus and protection**.

I. Introduction

Law and Information Technology are parallel objects and many scientists prove that they complement each other. A lot of lawyers complain that law is always running behind the process of developing information technology.

II. Theoretical Basis

R. M. Kamble underlines that information technology deals with information system, data storage, access, retrieval, analysis and intelligent decision making. Information technology refers to the creation, gathering, processing, storage, presentation and dissemination of information and also the processes and devices that enable all this to be done[1]. And computers become inalienable part of our life. Cybercrime is defined as crimes committed on the internet using the computer as either a tool or a targeted victim. Cybercrimes involve both the computer and the person behind it as victims; it just depends on which of the two is the main target[2]. So cyberspace spreads and become more dangerous because many people can be involved in it. Criminals roam freely in cyberspace than in other environment.

III. Practice

Cybercriminal activity is one of the biggest challenges that humanity will face in the next two decades[3]. 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.1).

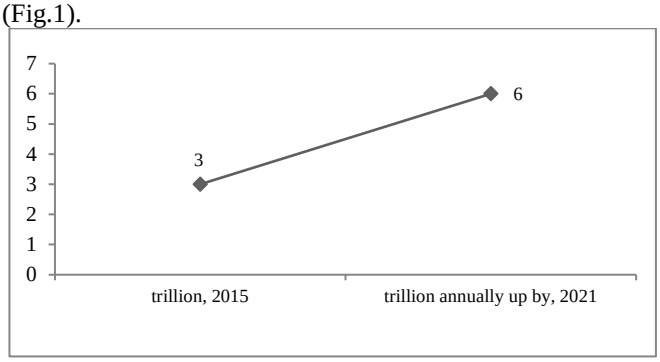

Fig. 1. Prediction for increasing of cybercrimes cost from 2015 annually by 2021

It is direct connection of changing amount of internet users: 100000 in 1990 and 500 million people in 2013. These date rapidly changed (Fig. 2).

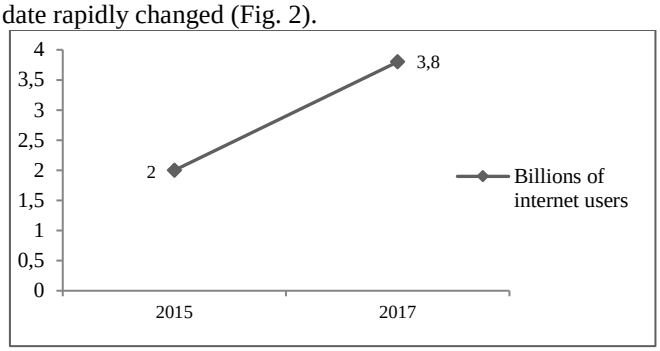

Fig. 2. Quantity of internet users changing (2015-2017)

Cybercrimes have unique structure that is connected with information technologies (Fig.3).

Many crimes that involve the use of cyber-technology are not genuine cybercrimes. Cyber-*related* crimes could be further divided into two sub-categories:

- cyber-exacerbated crimes;
- cyber-assisted crimes.

Crimes involving cybertechnology could be classified in one of three ways: cyber-specific crimes genuine cybercrimes); cyber-exacerbated crimes; cyber-assisted crimes.

[1] R. M. Kamble. Cyber law and information technology. International Journal of Scientific & Engineering Research, Volume 4, Issue 5, May-2013

[2] Computer Crime Research Center. Cybercrime definition. Electronic access: http://www.crime-research.org/articles/joseph06

[3] Steve Morgan, Editor-in-Chief Cybersecurity Ventures. 2017 Cybercrime Report. Herjavec group. Electronic access: https://cybersecurityventures.com/2015-wp/wp-content/uploads/2017/10/2017-Cybercrime-Report.pdf

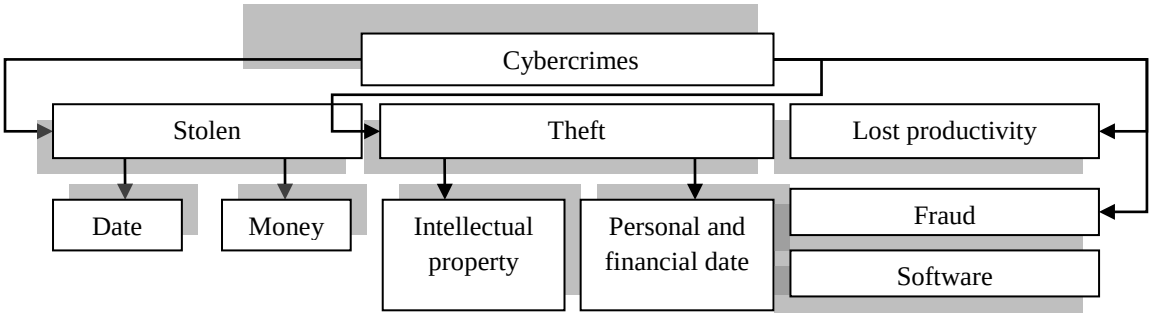

Fig. 3. Cybercrimes that connect with information technologies.

Like other kinds of crime, which historically grew in relation to population growth, cybercrimes grow in proportion to digital targets. And cybercrimes are more dangerous than the others because criminals can operate anonymously over the computer networks. The difference between crimes is the hackers steal intellectual property. Law that connects with cybercrimes must cover IT area (Fig. 4).

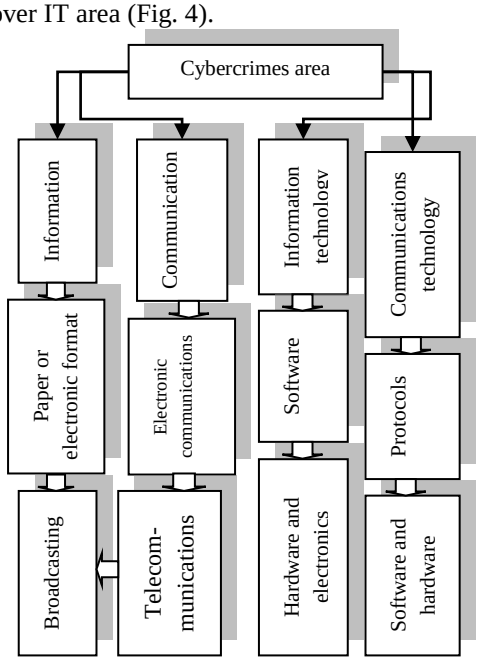

Fig. 4. Definition of cybercrimes area.

During last 20 years many security software were invited for electronic date protection because in the world's practice there is not the single law that can regulate all IT relations.

There is a field of law that comprises elements of various branches of the law[4] (Fig. 5).

But even these parts of law are not enough to control cyberspace. Cybercrimes develop more quickly than others crimes (Fig. 6) [1]-[6]. Many countries have very few laws addressing cybercrime.

- Love Bug Virus;
- VB script that spread via email and corrupted many different file types;
- FBI traced the virus to the Philippines.

[4] What is IT law, ICT law or Cyber law? Michalsons. Electronic access: https://www.michalsons.com/blog/what-is-it-law-ict-law-or-cyber-law/286

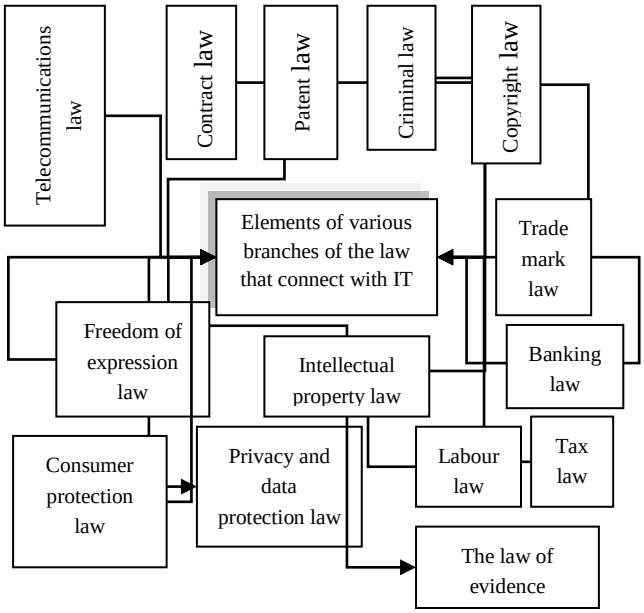

Fig. 5. Elements of various branches of the law that connect with IT for creation the unique law for protection internet users' property.

But can legislation stop cyber crime. Research shows that the costs of cyber crime for companies in financial services and utilities and energy have the highest annualized cost. The most expensive attacks are malicious insiders, denial of service and Web-based attacks [7]. In last 2017 year in the world the new kinds of cybercrimes appeared – machine learning accelerates social engineering attacks or cloud computing providers' infection. But the necessary sections in the law that provide security from cybercrimes are not adopted so quickly. So, cybersecurity is the main instrument in securing date from threats (Fig.7).

Many computer criminals have been company employees, who were formerly loyal and trustworthy and who did not necessarily possess great computer expertise. To prevent increasing in cybercrimes activity it is important to identify career criminals, including those involved in organized crime, who are now using cyberspace to conduct many of their criminal activities. Some cyber-related crimes can be carried out by professional's offenders and might be undetected because professional criminals do not typically make the same kinds of mistakes as hackers, who often tend to be amateurs.

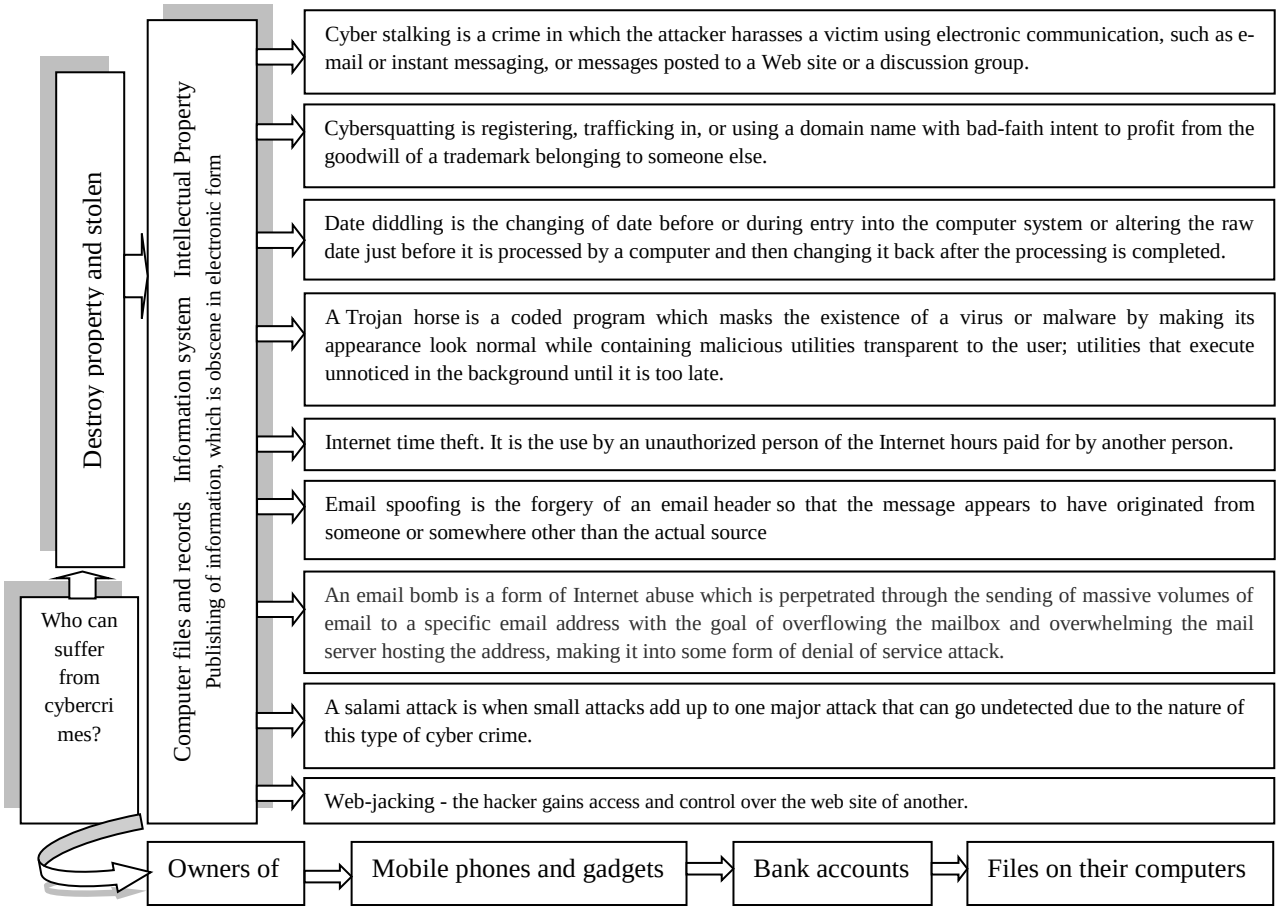

Fig. 6. Classification of Cyber Crimes and people who are affected by them.

Information age is so called because our life is codified by date: almost everything we do or buy, and everything we depend on, involves data and the technology that uses it. Cyber criminals are building so called “an army of things” that has the potential to impact the future of the digital economy [9]. Impact of a cyber attack could include substantial loss of revenue and margin, of valuable data, and of other company assets. Quantity of cybercriminals increases quickly around the world. Now cybercrimes are connected international serious organized crime groups, smaller-scale, domestic criminals and hacktivists.

Although the most serious threat comes, directly or indirectly, from international crime groups, the majority of cyber criminals have relatively low technical capability. Their attacks are increasingly enabled by the growing online criminal marketplace, which provides easy access to sophisticated and bespoke tools and expertise, allowing these less cyber criminals to exploit a wide range of vulnerabilities [10]. There is also situation when companies’ websites were subject to the criminal access of a customer records database, followed by a ransom demand asking for payment in exchange for the return of stolen data. The wearables are rapidly gaining popularity with smartwatches. Wearables are tracking all sorts of personal information including GPS location, blood pressure, heart rate, and anything else you feed them such as weight or diet. Such personally identifiable information could be used as a base to target you for spear-phishing, or aid in identity theft. But the real opportunity is these devices linking to your smartphone, where phone numbers, more personally identifiable information, emails, web logins etc. could theoretically be compromised [10].

Cybercrime activity is spreading around the world. For decreasing the cybercrimes in Europe, Cooperation Group, the Commission, the European Union Agency for Network and Information Security should be established to support information security within the EU countries [12]. According to Directive (EU) 2016/1148 the certain sectors of the economy are already regulated or may be regulated in the future by sector-specific Union legal acts that include rules related to the security of network and information systems. Each Member State shall designate one or more national competent authorities on the security of network and information systems.

Member States shall ensure that digital service providers identify and take appropriate and proportionate technical and organizational measures to manage the risks posed to the security of network and information systems which they use in the context of offering services referred to in Annex III within the Union. Having regard to the state of the art, those measures shall ensure a level of security of network and information systems appropriate to the risk posed, and shall take into account the following elements: the security of systems and facilities, incident handling, business continuity management, monitoring, auditing and testing [12].

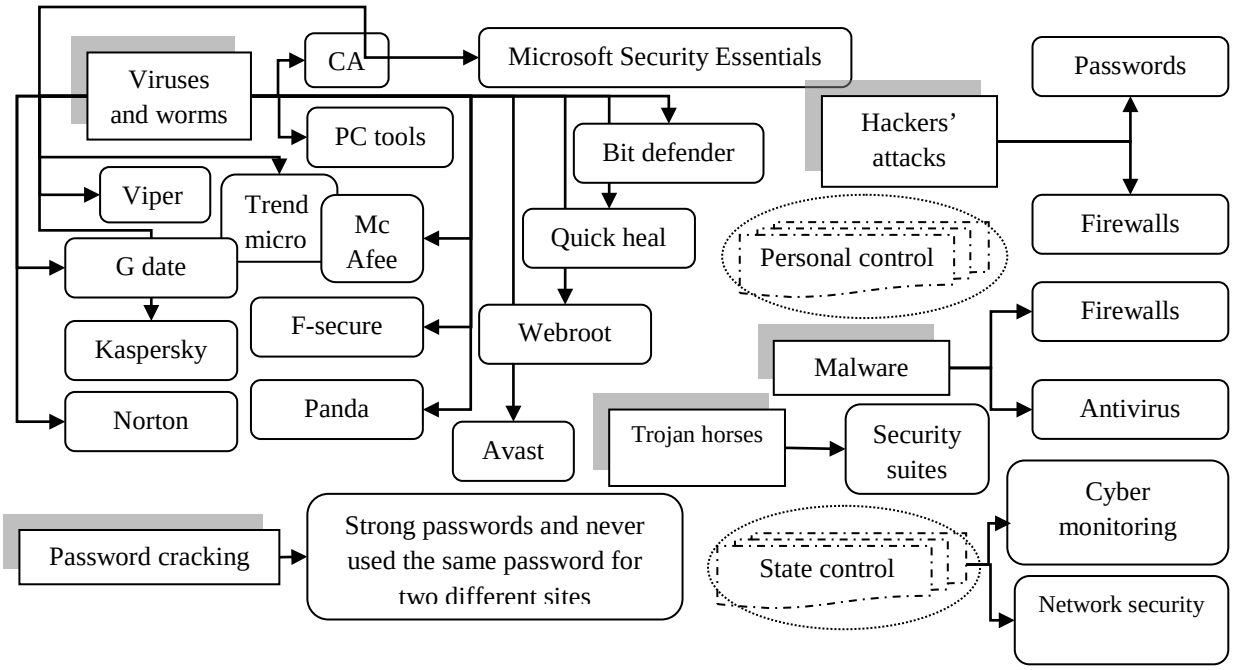

Fig. 7. Types of security in the network space.

The top industries at the greatest risk of cyber attack (Fig. 8) [11].

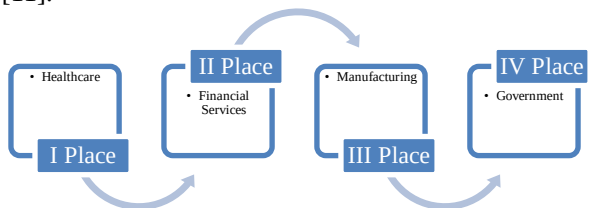

Fig. 8. The top 4 industries at the greatest risk of cyber attack.

IV. Conclusion

Cyber crimes are intrinsically challenging for business companies and governments. Security has to be developed quicker then types of cyber crimes because solutions that may have worked last year may not necessarily work this year or next.

References

[1] Cyber stalking. Available at: http://searchsecurity.techtarget.com/definition/cyberstalking

[2] Cybersquatting. Available at: http://searchmicroservices.techtarget.com/definition/cybersquatting

[3] E-mail spoofing. Available at: http://searchsecurity.techtarget.com/definition/email-spoofing

[4] What is a Trojan Horse Virus? - Definition, Examples & Removal Options. Available at: https://study.com/academy/lesson/what-is-a-trojan-horse-virus-definition-examples-removal-options.html

[5] Aj. Maurya. What is a salami attack? Available at: https://ajmaurya.wordpress.com/2014/03/27/what-is-a-salami-attack/

[6] Email Bomb. Electronic access: https://www.techopedia.com/definition/1655/email-bomb

[7] Cost of cyber crime study. Insights on the security investments that make a difference. Independently conducted by Ponemon Institute LLCand jointly developed by Accenture. Available at: https://www.accenture.com/t20170926T072837Z__w__/us-en/_acnmedia/PDF-61/Accenture-2017-CostCyberCrimeStudy.pdf

[8] Cyber security. Available at: https://www.slideshare.net/Siblu28/cyber-security-36922359

[9] Cyber criminals a growing threat to digital economy. Available at: https://www.gtnews.com/2017/03/29/cyber-criminals-a-growing-threat-to-digital-economy/

[10] NCA Strategic Cyber Industry Group. Cyber Crime Assessment 2016. Need for a stronger law enforcement and business partnership to fight cyber crime. Available at: http://www.nationalcrimeagency.gov.uk/publications/709-cyber-crime-assessment-2016/file

[11] 5 industries that top the hit list of cyber criminals in 2017. Available at: http://www.infoguardsecurity.com/5-industries-top-hit-list-cyber-criminals-2017/

[12] EUR-lex. Directive (EU) 2016/1148 of the European Parliament and of the Council. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?toc=OJ%3AL%3A2016%3A194%3ATOC&uri=uriserv%3AOJ.L_.2016.194.01.0001.01.ENG