FINANCIAL ASPECT OF CYBERCRIME: SITUATION IN UKRAINE AND THE WORLD

ASPEKTY FINANSOWE CYBERPRZESTĘPCZOŚCI: STAN W UKRAINIE I ŚWIECIE

ФИНАНСОВЫЙ АСПЕКТ КИБЕРПРЕСТУПНОСТИ: СОСТОЯНИЕ В УКРАИНЕ И МИРЕ

Galina Myskiv
Assistant Professor, Department of Finance and Accounting,
Lviv State University of Internal Affairs
ORCID: https://orcid.org/0000-0001-9315-8859
* Corresponding author: e-mail: galinamyskiv@gmail.com

Olesya Irshak
PhD, Department of banking and insurance business,
Ivan Franko National University of Lviv
ORCID: https://orcid.org/0000-0002-1536-8161
* Corresponding author: e-mail: olesyapetrivska@ukr.net

Abstract
Cybercrime is clearly linked with financial relations: for some it is profit, for others - expenses, and for still others - big losses. The article contains the research of the essence, causes, consequences and counteraction to computer fraud in Ukraine and countries of the world, as well as research of financial flows that accompany these processes. However, the authors tried to analyze quantitatively and qualitatively the dynamics of cybercrimes. It also focuses on bodies that provide cybersecurity and normative legal documents in this area. The authors concluded that cyber security in Ukraine has not been sufficiently developed yet, which requires adopting the experience of cybercrime prevention in the advanced countries of the world and enhanced cooperation between international law enforcement agencies.
Keywords: cybercrime, cybersecurity, fraud, prevention, financial relations

Streszczenie
Cyberprzestępczość jest niewątpliwie związana z relacjami finansowymi: dla niektórych jest to zysk, dla innych - wydatki, a jeszcze dla trzecich są to duże straty. Artykuł obejmuje badanie istoty, przyczyn, konsekwencji i środków zaradczych związanych z oszustwami komputerowym iw Ukrainie i w krajach świata, a także badania przepływów finansowych towarzyszących tym procesom. Jednocześnie autorzy próbowali analizować ilościowo i jakościowo dynamikę cyberprzestępczości. Skupiono się również na organach, zapewniających bezpieczeństwo cybernetyczne i dokumentach regulacyjnych w tej dziedzinie. Autorzy doszli do wniosku, że bezpieczeństwo cybernetyczne w Ukrainie nie jest jeszcze wystarczająco rozwinięte, co wymaga przejęcia doświadczenia w zwalczaniu cyberprzestępczości w zaawansowanych krajach światu i wzmocnionej współpracy między międzynarodowymi organami ścigania.
Słowa kluczowe: cyberprzestępczość, bezpieczeństwo cybernetyczne, oszustwa, przeciwdziałanie, stosunki finansowe

Аннотация
Киберпреступность бесспорно связана с финансовыми отношениями: это получение прибыли, расходы, а также большие убытки. Статья исследует сущность, причины, последствия и меры противодействия компьютерному мошенничеству в Украине и странах мира, а также исследования финансовых потоков, которые сопровождают эти процессы. В то же время, авторы попытались проанализировать количественно и качественно динамику киберпреступности. Также акцентировано на органах, обеспечивающих кибербезопасность и нормативно-правовые документы этой сферы. Авторы пришли к выводу, что в Украине кибербезопасность еще не достаточно развита, что требует перенимать опыт противодействия киберпреступности в передовых стран мира и усиленного сотрудничества с международными правоохранительными органами.
Ключевые слова: киберпреступность, кибербезопасность, мошенничество, противодействие, финансовые отношения

Statement of the problem in general outlook and its connection with important scientific and practical tasks

The development of computer and Internet technologies is an absolute achievement and a preference for modern society: business opportunities are expanding, trade has become global, payments are made through international payment systems, the world has become open and free for communication between people. At the same time, the

Internet has caused the emergence of new types of crime, which before this date did not exist, and made possible the transformation and growth of existing types of crime. The various fraudulent criminal schemes, which are based on fraudulent money takeover of Internet users, are escpecially actively developed and improved.

Analysis of latest research where the solution of the problem was initiated
The problem of cybercrime and the growing range of its threats undeniably has an economic background and financial motivation. This requires reaction and cohesiveness of the governments of all countries and cyberpolice units to prevent and minimize harm from cyber attacks. Hence, the theoretical and practical aspects of cybercrime and the areas of counteraction to it are best investigated by national cybercrime bodies and outlined in national strategies and doctrines: Cyber security Doctrine of the Republic of Poland' (National Security Bureau, 2009), Cyber Security Strategy for Germany (Federal Ministry of the Interior, 2011), Cyberspace Protection Policy of the Republic of Poland (Ministry of Administration and Digitisation, Internal Security Agency, 2013), Strategia cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2016-2020' (Ministry of Digital Affairs International Strategy for Cyberspace, 2016), Prosperity, Security, and Openness in a Networked (Washington, 2011), National Cyber Security Policy (New Delphi, 2013) and others.
In Ukraine, a separate department of the National Police, which publishes all statistical information (Official site of the National Police), deals with the problem of cyber security. Among the scholars who are investigating the current state and directions of combating cybercrime in Ukraine, it is worth highlighting O.S. Bondarenko (Bondarenko O.S., 2018), M. Kravtsova (Kravtsova M., 2018), L. Kovtun (Kovtun L.Yu, 2015) and others. However, the over-rapid development of information technology generates new types of cybercrime, which makes a permanent study of this topic relevant and requires constant resistance to cyber attacks for consumer safety.

Aims of paper. **Methods**
The purpose of the paper is to investigate the financial component of cybercrime as a huge cash flow that has mobilized through illegal activities and has pointed to a real financial sector that directly affects the criminal situation and financial security of countries and violates their national security.
In the process of conducting the study, it is necessary to use a set of statistical data on the main indicators, which provide a chance to make a global assessment of the state of financial impact of cybercrime on the national financial systems. For this purpose it is necessary to analyze the losses of the world economy from cybercrime and the annual expenses of the countries to fight against virtual criminals. It's also worth investigating the change in the share of these indicators relative to the indicators of global GDP and GDP of the countries. Thus, the use of economic and statistical methods will allow us to draw conclusions about the current state of financial risks caused by cybercrime and to identify existing problems in the information environment in order to develop advanced security areas.

Exposition of main material of research with complete substantiation of obtained scientific results. **Discussion**
All crimes committed in the information space with the use of computers, information technologies and global networks are generalized under the name "cybercrime".
Cybercrime has become a problem in the twenty-first century in connection with the lively modernization of technology and society, and its evolution has been rapidly developing. Every day the criminals find creative ways of programming devastating viruses, theft of intellectual property, theft of personal data, access to financial information and the closure of corporate computer systems.
The development of cybercrime is directly related to the development of global computer networks and covers all sectors of social existence:
- public and political activity (stealing important information to attract attention or increase social pressure on someone, or to suspend someone's activity);
- the activities of state institutions (espionage of hackers - cyber-espionage);
- financial sector (illegal receipt of funds from bank accounts (phishing) and crimes with financial instruments);
- the information technologies sector (stealing personal data, the creation of harmfull or virus programs for use in cyberattacks);
- national security (cyberterrorism), etc.

All this raises the price of cybersecurity for the state and business, which overcomes the effects of breaks much more expensive than their warning. Billions of dollars are lost annually, repairing systems that have been hit by

cybercrime attacks. Some cyberattacks against vital systems sometimes disconnect the operation of hospitals, banks and rescue services throughout the country.

According to IBM Security and Ponemon Institute, the average price of even a small leak of information (from 2500 to 100 thousand accounts) is 3.87 million USD, and a high leak costs at least 40 million USD (IBM. Detect and advanced persistent security threats, 2018).

Changes in legislation cause increase in the price of information leak - according to the new European General Data Protection Regulation (GDPR), there is a fine for each case of leak (regardless of the reasons). Therefore, according to Gartner, world cybersecurity costs in 2018 amounted to 114 billion USD, and in 2019 - 124 billion USD (through risk management and increased attention to the protection of personal data) (Re-Hashed: 2018 Cybercrime Statistics).

The main reason for the development of cybercrime is the high profitability. Existing research shows that cybercrime ranks third after trafficking in weapons and drugs by enrichment. For example, according to estimates of the Accounting Chamber of the United States, the annual income of criminals only from the theft and fraud committed through the use of computer technology through the Internet, reaches 5 billion USD (Bondarenko O., 2018).

Such facts require the study of the financial component of cybercrime, since huge cash flows are mobilized through illegal actions and directed to a real financial sector, which directly affects the criminal situation and financial security of the states and violates their national security.

According to the joint report by the McAfee Cybersecurity Company and the Center for Strategic and International Studies (CSIS), the global economy losses from cybercrime in 2017 amounted to about 600 billion USD, or 0.8% of global GDP, that 1.35 times exceeded the world losses in 2014 (445 billion USD) (McAfee Labs Threats Report, 2018). In 2018, more than 43% of all enterprises were victims of cybersecurity violation. By 2021, losses from cybercrime will increase to 6 trillion USD a year (6 trillion USD) (21 Terrifying Cyber Crime Statistics, 2018). This testifies to the crazy scale of cybercrime, which target is all countries of the world - both civilized and less civilized.

The global trend of cybercrime is the fraudulent use of mobile devices: 60% of fraud is carried out on mobile devices; 80% - from mobile apps. First of all, cybercriminals through mobile phones have access to mobile banking of victims (deceived).

In the USA, Great Britain and China, Smart Home is becoming the most vulnerable to cybercrime attacks. The USA has 28% of smart home appliances, while the United Kingdom and China - 7%. Since most smart home appliances are connected through a computer network, it makes them vulnerable to cyber attacks, and houses are open to crime (21 Terrifying Cyber Crime Statistics, 2018).

The most popular cybercrime in the world is phishing - a method of Internet fraud, whereby hackers force users to transfer confidential information for its further use for illegal purposes: obtaining loans under a false name, receiving money from a bank account, paying expenses with someone's credit cards, etc. [kovtun]. Nearly 30% of all e-mails, according to the Verigon's 2018 Data Breach Investigations report, are phishing emails Strategy for Cyber Security of Montenegro to 2017), and 12% of users open links and fall into the trap of cyber criminals.

Certainly, in Ukraine, cybercrime does not have such scope as in the highly developed countries. First of all, this is connected with the solvency and wealth of the country's population. However, world trends in this area ado not set aside any country.

If even five years ago the regulations of the Criminal Code (CC) of Ukraine regarding crimes in the use of electronic computing machines (computers), automated systems, computer networks or telecommunication networks were practically not used, now they are becoming more widespread.

The dynamics of the cybercrime level in Ukraine since 2009 has been growing, although in some years there has been a reduction. In 2009, 217 crimes in the computer use were registered in Ukraine, in 2010 - 190, in 2011 - 131, in 2012 - 138, in 2013 - 595, in 2014 - 443 , in 2015 - 598, in 2016 - 865, in 2017 - 2573, in January-August 2018 - 1885 crimes (Kravtsova M., 2018).

Special phishing activity in Ukraine has been observed since 2015. According to the Ukrainian Interbank Association of Payment System Members, the largest number of fraudulent resources was recorded in Ukraine in 2016 - 174 phishing sites; in 2017 - 108, in 2018 - 131.

The number of detected cyber-security crimes in Ukraine increases on the average by 2.5 thousand annually. Therefore, a new unit was created in the structure of the National Police of Ukraine - the Cyber Police Department, which deals with cybercrime, develops a methodology and acquires knowledge from foreign partners.

According to the Department of Cyberpolice of Ukraine, in 2017 there were 3810 of applications for the theft of money from bank cards. It is 70% more than in 2016. In total, for 2017, 670 million UAH was stolen from bank cards, including 510 million UAH due to social engineering methods, and 160 million UAH due to Internet fraud. The scale of theft in 2017 has increased twice compared with 2016 and 8 times compared with 2015 (The National Police, 2018).

In 2017, the Department of Cybercrime Police accompanied about 7 thousand criminal proceedings, 4.5 thousand of which - exclusively cybercrime. In 2017, bills of indictment were directed against 726 persons.

In 2018, the Department of Cyberpolice of the National Police of Ukraine found about 6 thousand of crimes committed in the area of high-tech information technology, including:

- 2398 in the field of payment systems;
- 1 325 - crimes committed in the field of cyber security;
- 1598 in the field of e-commerce;
- 680 - in the field of illegal content.

During 2018 the Cyberpolice of Ukraine was prevented from spreading 4 massive cyberattacks in the territory of the state and suspended activities of more than 40 unauthorized website. Within the framework of international cooperation 8 transnational hacker groups were exposed and more than 30 international operations took place (The National Police, 2018).

The average amount of losses for each Ukrainian user in 2018 amounted to 2478 UAH, and slightly decreased compared to 2017, where those losses amounted to 2 543 UAH, which is 1.8 times more than in 2016, and 3 times more than in 2015 [19] (Fig. 1).

The specificity of viruses, spam and phishing messages is that they do not leave a typical track information, mask harmless software or letters that are capable of self-reproduction and self-distribution, can be modified and changed in the process of existence, independently destroy their traces of existence and, as a rule, are used by remote access.

All of these signs and a significant increase in the volume of payments on the Internet lead to the growth of cybercrime and the growth of its profitability in Ukraine and around the world.

In general, in 2018, the international cybercrime generated more than 1.5 trillion USD in profits (Re-Hashed. Cybercrime Statistics, 2018). Each year, the volume of losses from cybercrime and, accordingly, the level of its profits are increasing. This necessitates the development of a series of measures to counter this criminal activity and develop cyber security tools for all computer users.

Fig. 1. The average amount of fraudulent operation in 2015-2018 in Ukraine, UAH.
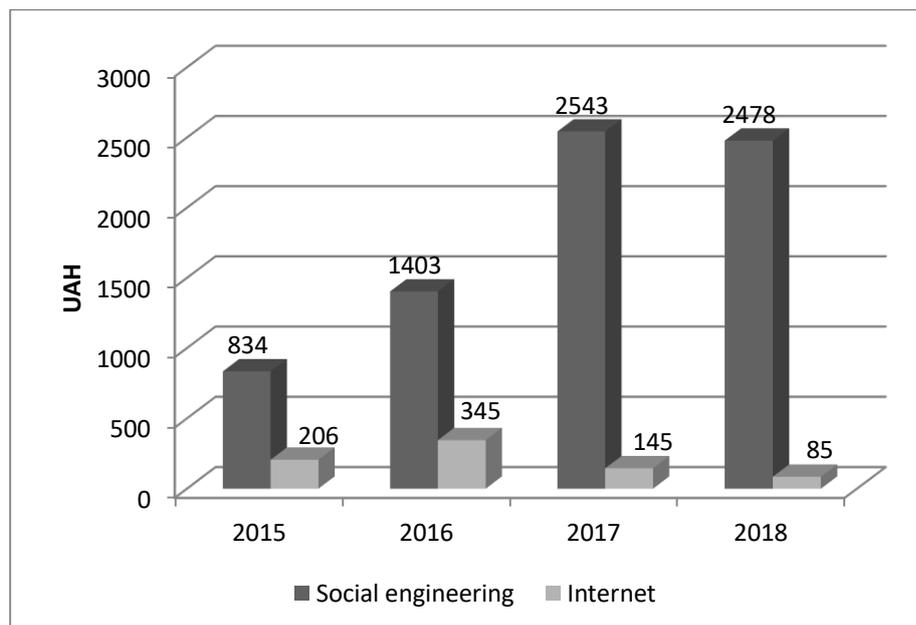
Source: (Bondarenko O., 2018)

The world leader in the fight against cyber threats is the United States of America, which in recent years has created a set of technological and research opportunities and partnership relations for pursuing cyberspace in all continents.

The FBI is the leading federal agency for investigating cyberattacks of criminals and terrorists. The threat is constantly increasing. Cyber intrusions become more common, dangerous and complex. The FBI has significant investigative resources throughout the country and around the world to investigate the infrastructure and agents responsible for these crimes and prosecute and recover the assets.

The FBI anti-cybercrime structure includes:

− Cyber Division at FBI headquarters;

- Specially trained cyber squads at FBI headquarters and in each of the 56 field offices, staffed with "agents and analysts who protect against investigate computer intrusions, theft of intellectual property and personal information, child pornography and exploitation, and online fraud";
- New Cyber Action Teams that "travel around the world on a moment's notice to assist in computer intrusion cases" and that "gather vital intelligence that helps us identify the cybercrimes that are most dangerous to our national security and to our economy;
- Our Computer Crimes Task Forces nationwide that combine state-of-the-art technology and the resources of our federal, state, and local counterparts;
- A growing partnership with other federal agencies—including the Department of Defense, the Department of Homeland Security, and others—which share similar concerns and resolve in combating cybercrime (FBI. Cyber Crime. 2019).

In addition to the FBI, in the USA in 2008, the National Cyber Investigative Joint Task Force (NCIJTF) was established to overcome cybercrime. As a unique multi-agent cybercenter, the NCIJTF has the primary responsibility for coordinating, integrating and sharing information for cyber-threats research, analysis and development of intelligent information for authorities (National Cyber Investigative Joint Task Force, 2019).

In 2013, Europol established the European Center for Cybercrime (ECC) to strengthen the response of law enforcement agencies to cybercrime in the EU to protect European citizens, business and governments from crime on the Internet (European cybercrime center, 2018). The main strategic product of ECC in the fight against cybercrime is IOCTA (Internet organised crime threat assessment), which provides a unique oriented police assessment of new threats and key events in cybercrime during the year.

At the same time, every country in Europe is trying to fight against cybercrime and prevent such Internet crimes.

In particular, in Poland, three main strategic documents have been developed and implemented, which are entirely devoted to cybersecurity, its goals and organizational structure:

- Policies to protect the cyberspace of the Republic of Poland, published in June 2013 (Ministerstwo Administracii i Cyfryzacji, MAC and Agencja Bezpieczeństwa Wewnętrznego, ABW);
- The Cyber Security Doctrine of the Republic of Poland, published in January 2015 (Biuro Bezpieczeństwa Narodowego, BBN).
- The Cybersecurity Strategy of Poland for 2016-2020 (Ministry of Digital. Strategia cyberbezpieczeństwa RP, 2016).

In addition, since 2014 Poland has implemented the Strategy of National Security of the Republic of Poland (Strategia Bezpieczeństwa Narodowego Rzeczpospolitej Polskiej, SBNRP), which states that "ensuring Polish security in cyberspace, including the security of the cyberspace of the Republic of Poland, is one of the main targets related to the security of the state". The document identifies a set of actions and preventive measures to overcome the threats in cyberspace.

Similar documents have been approved and implemented in many countries of Europe and the world:

- Cyber Security Strategy for Germany, 2011 (Federal Ministry of the Interior. Cyber Security Strategy for Germany, 2011);
- National Cyber Security Strategy of Hungary, 2013 (Prime Minister's Office. National Cyber Security Strategy of Hungary, 2013);
- Strategy on Cyber Security of Montenegro to 2017 (Strategy for Cyber Security of Montenegro to 2017, 2013);
- The concept of cyber security of India (National Cyber Security Policy) (National Cyber Security Policy, 2013);
- International Strategy for Cyberspace. Prosperity, Security, and Openness in a Networked World (International Strategy for Cyberspace, 2011);
- Action Plan 2010-2015 for Canada's Cyber Security Strategy (Government of Canada's. Action Plan 2010-2015 for Canada's Cyber Security Strategy, 2013), etc.

Unfortunately, in Ukraine, cybersecurity is not sufficiently developed, which requires adopting the experience of cybercrime prevention in the advanced countries of the world. In particular, the OSCE helps the country overcome the threat of cybercrime, which includes support for the development of a new cyberpolice, promotion of international cooperation between different authorities in combating crimes committed using information technologies, training of specialists in cybersecurity areas, etc.

At the same time, the cyber security of Ukraine requires more and strengthened cooperation between international law enforcement agencies, private sector companies, academia and other relevant concerned parties.

It is very important that law enforcement agencies could cooperate with the Internet security industry to restrict criminal activity and source of its income from information crimes.

Law enforcement agencies should continue to explore the possibility of investigations, analytics and police emerging from new technologies such as artificial intelligence (AI) and machine learning. Such tools will be invaluable for combating modern crime and for intelligence police.

Conclusions

Thus, having studied the problem of cybercrime and the range of its threats, we have reached the conclusion of the economic background and financial motivation of all crimes in computer technology. Cybercrime brings significant financial benefits, while in terms of profitability it ranks third in the world after trafficking in drugs and weapons - its profit is estimated at 1.5 trillion USD. At the same time, the losses caused by this criminal hacking activity grow annually and are forecasted at the level of 6 trillion USD in 2021! This confirms the presence of the financial aspect in cybercrime and requires the counteraction and cohesiveness of governments of all countries and cyberpolice units to prevent and minimize harm from cyber attacks.

References:

1. 21 Terrifying Cyber Crime Statistics. Retrieved April 5, 2019 from: https://www.vpngeeks.com/21-terrifying-cyber-crime-statistics-in-2018/
2. Action Plan 2010-2015 for Canada's Cyber Security Strategy (2013). Government of Canada. Retrieved from: http://www.securitepublique.gc.ca/cnt/rsrcs/pblctns/ctn-pln-cbr- scrt/ctn-pln-cbr-scrt-eng.pdf
3. Bondarenko O.S. *Cybercrime in Ukraine: causes, characteristic features and counteraction measures,* «Comparative and Analytical Law», 2018 No.1, pp.246-248
4. *Cyber Crime. FBI official website*. Retrieved April 9, 2019 from: https://www.fbi.gov/investigate/cyber
5. Cyber security Doctrine of the Republic of Poland. National Security Bureau. Retrieved April 20, 2019 from: http://en.bbn.gov.pl/en/news/400,Cybersecurity-Doctrine-of-the-Republic-of-Poland.html.
6. Cyber Security Strategy for Germany (2011). Federal Ministry of the Interior. Retrieved March 28, 2019 from: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/ Publications/CyberSecurity/Cyber_Security_Strategy_for_Germany. pdf?__blob =publicationFile
7. Cyberspace Protection Policy of the Republic of Poland (2013). Ministry of Administration and Digitisation, Internal Security Agency. Retrieved April 14, 2019 from: https://www.enisa.europa.eu/ activities/Resilience-and-CIIP/national-cyber-securitystrategies-ncsss/copy_of_PO_NCSS.pdf.
8. European cybercrime center – EC3. Retrieved March 20, 2019 from: https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3
9. International Strategy for Cyberspace (2011). Prosperity, Security, and Openness in a Networked World. Retrieved April 17, 2019 from: https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf
10. Internet organized crime threat assessment 2018. Retrieved April 11, 2019 from: https://www.europol.europa.eu/internet-organised-crime-threat-assessment-2018
11. Świątkowska Joanna, Albrycht Izabela, Skokowski Dominik (2017). National Cyber Security Organization. Retrieved March 14, 2019 from: https://ccdcoe.org/uploads/2018/10/NCSO_Poland_2017-2.pdf
12. Kovtun L.Yu. *Phishing as one of the forms of fraud on the Internet* (2017). «Actual jurisprudence. Materials of the conference». Retrieved April 10, 2019 from::http://www.legalactivity.com.ua/index.php?option=com_content&view=article&id=1075%3a2015-09-15-06-47-15&catid=131%3a5-0915&itemid=161&lang=ru
13. Kravtsova M. *The Current State and Directions of Countering Cybercrime in Ukraine* «Bulletin of the Criminological Association of Ukraine», 2018. No. 2 (19), pp.155-165.
14. McAfee Labs Threats Report December 2018. Retrieved March 24, 2019 from: https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-dec-2018.pdf
15. National Cyber Investigative Joint Task Force. Retrieved March 24, 2019 from: https://www.fbi.gov/investigate/cyber/national-cyber-investigative-joint-task-force
16. National Cyber Security Policy (2013). Retrieved March 29, 2019 from: http://deity.gov.in/content/national-cyber-securitypolicy-2013-1
17. National Cyber Security Strategy of Hungary (2013). Prime Minister's Office. Retrieved March 30, 2019 from: https://www.enisa.europa.eu/ activities / Resilience-and-CIIP / national-cyber-securitystrategies-ncsss / HU_NCSS.pdf
18. Official site of IBM. Detect and advanced persistent security threats. Retrieved April 24, 2019 from: https://www.ibm.com/security/solutions/detect-advanced-persistent-threats
19. Official site of the National Police. Retrieved April 8, 2019 from: https://www.npu.gov.ua/news/kiberzlochini/u-2018-roczi-naczpolicziya-vikrila-tisyachu-zlochiniv-u-sferi-kiberbezpeki/
20. Official site of the Ukrainian Interbank Association of Payment System Members (EMA Association Retrieved April 24, 2019 from: https://www.association-secure-transactions.eu/tag/ema/
21. Re-Hashed: 2018 Cybercrime Statistics: A closer look at the "Web of Profit" Retrieved April 16, 2019 from: https://www.thesslstore.com/blog/2018-cybercrime-statistics/
22. Strategia cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2016-2020' (2016). Ministry of Digital Affairs. Retrieved April 8, 2019 from: https://mc.gov.pl/files/strategia_v_29_09_2016.pdf.
23. Strategy for Cyber Security of Montenegro to 2017 (2013). Retrieved April 11, 2019 from: https://www.enisa.europa.eu/activities/ Resilience-and-CIIP/national-cyber-securitystrategies-ncsss/CyberSecurityStrategyforMontenegro.pdf .

24. Verizon 2018 Data Breach Investigations Report. Tales of dirty deeds and unscrupulous activities. Retrieved April 14, 2019 from: https://enterprise.verizon.com/resources/reports/dbir/