Svitlana Mazepa
West Ukrainian National University, Ukraine
ORCID: 0000-0003-1282-9089

Cybercrime as a leading threat to information security: ukrainian experience

Introduction

Since 2020, there has been a significant increase in crimes committed on the Internet. The reason for this is the global trend in the growth of Internet crime and quarantine restrictions. Due to the Covid-19 pandemic, life was almost completely transformed into information space. And crime has also gone online. It is now possible to seize other people's money, threaten, harass, paralyze vital critical infrastructure without leaving home, just by sitting at a computer. The Covid-19 pandemic has forced authorities around the world to take action, including closing borders and quarantining countries. Due to the current situation, the problem of restricting people's rights, including constitutional ones, in order to ensure their security, has become urgent. It is obvious that the restriction of human rights to movement, which is one of the mandatory provisions of quarantine, contradicts the Declaration of Human Rights[1] and, of course, the Constitution of Ukraine[2]. In addition, such a restriction encourages people to spend more time in electronic format. Thus, the whole world was transformed into an information space. Receiving and disseminating information, shopping, working, studying, meeting with friends and many other things that we usually did without direct dependence on the Internet, have now completely gone online. As a result, the number of purchases in online stores, the number of publications and readers and the number of active users of the network has increased significantly. This in turn causes a number of problems in terms of information security in quarantine. One of the important issues is the protection of personal data, because during the pandemic,

[1] Universal declaration of human rights; https://www.un.org/sites/un2.un.org/files/udhr.pdf accessed: 11.11.2021.

[2] Constitution of Ukraine; https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text accessed: 20.11.2021.

people around the world are beginning to actively use unusual software for work and leisure, without even thinking about how safe it is. According to the 2021 report of Europol[3], during the pandemic, Darknet developed, which now has about 500,000 users. In the field of cybersecurity, the coronavirus pandemic has provided hackers and Internet fraudsters with the best opportunity to carry out criminal intent. NATO has recently announced cyberspace as a new dimension of military operations. Cybersecurity and information security in general are an important component of a country's national security. It is proposed to focus on a narrower concept and clarify the issue of cybersecurity.

Overview of threats in the information space and current trends in cybercrime

Two factors had a negative impact on Ukraine's information security in the global sense: the hybrid war with the Russian Federation[4] and the Covid-19 pandemic. The goal of Russia's "hybrid war" against Ukraine is to destabilize Ukraine and control it to achieve its interests, using the threat of armed conflict with Ukraine. An important component is the information component, which is a means of influencing the decisions of the military-political leadership; justification of one's own actions and condemnation of actions on the part of Ukraine; creating the necessary conditions for successful actions of armed groups; motivation for certain behaviors; impact on the functioning of management systems, livelihoods, infrastructure, transport, etc. The results of Russia's information campaigns against Ukraine and the international community, which supports Ukraine, show the complete superiority of the enemy in the information space and insufficient efforts of the state to implement its own information policy and information security. Ukraine has become the object of the largest cyberattacks in the world. The NotPETYA malware attack is currently considered the most destructive cyberattack in history. NotPETYA has destroyed information on hundreds of thousands of computers around the world and caused about $ 10 billion in damage to dozens of organizations, including critical transportation infrastructure and hospitals. Obviously, the attackers' only goal was to harm Ukrainian business and Ukraine as a state, but the attackers did not take into account the lack of borders in cyberspace and the ramifications of business ties that Ukrainian businesses and organizations had around the world. This attack is clear evidence that no country in the world

[3] Internet Organised Crime Threat Assessment (IOCTA) 2021 https://www.europol.europa.eu/cms/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2021.pdf accessed: 1.12.2021.

[4] NATO-2030; https://www.nato.int/nato_static_fl2014/assets/pdf/2020/12/pdf/201201-Reflection-Group-Final-Report-Uni.pdf accessed: 1.12.2021.

can effectively counter such attacks without outside help, and no country is immune to the damage caused by such indiscriminate means, even if the main target is in another hemisphere far beyond its regional and geopolitical interests.

Also a significant reason for the destabilization of the country is the spread of fakes and information propaganda. Analysis of the activities of Russian structures and organizations in the field of information warfare gives grounds to divide their main directions:

- traditional propaganda activities: mass media, visual agitation, rallies, literature, education, art, upbringing (in religious institutions (churches, religious organizations), public organizations);
- influence through the Internet: sites, file sharers, fake sites and organizations "International Group Information on Crimes against the Person" (IGCP) articles, blogs, Instagram;
- social networks: fake pages (photos), moderation groups ("Bots from Olgino") to block anti-Russian bloggers and negative commenting on publications; fake faces ("Spanish dispatcher");
- online media: "Information resistance to the occupiers" (inforesist.org); "Russian Spring" (rusvesna.su); "NEW RUSSIA is ours land!" (novorossiya.info); "News of independent Ukraine" (uafree.ru); "I am Ukrainian" (euromaidanu.net);
- change content on the Internet (online encyclopedia, National Geographic etc);
- impact on the information space of Western countries: street actions (demonstrations), engaged experts, "authoritative" journalists, scientists, RussiaToday TV channel;
- cyber war;
- separate information and psychological operations[5].

Only one-fifth of respondents believe that social networks are used to spread propaganda[6]. A little more - we are convinced that misinformation is an acute problem of the Russian media. Of particular concern is the fact that less than a third of users feel the need for additional knowledge to detect and recognize fakes, and we see this as both a problem and an opportunity.

Informing citizens about threats in cyberspace is extremely important, so we consider it necessary to clarify the nature and danger of these relatively new phe-

[5] D.M. Prysiazhniuk, Zastosuvannia manipuliatyvnykh tekhnolohii z boku Rosii v ZMI Ukrainy (na prykladi Krymu) [Application of manipulative technologies by Russia in the media of Ukraine (on the example of Crimea)] http://vuzlib.com/content/ view/1108/23 accessed: 15.11.2021.

[6] Ukrainian site Stop fake; https://www.stopfake.org/osvedomlennost-i-otnoshenie-k-dezinformatsii-i-propagande-v-smi-otchet-ob-issledovanii-stopfake accessed: 15.11.2021.

nomena, and to highlight ways to counter hostile propaganda[7]. The study of the Russian-speaking segment of the Internet, which was conducted in 2017 by the NATO Center for Strategic Communications Research and presented in the report Virtual Russian World in the Baltics, was interesting. Basic conclusions of the study: Anti-Ukrainian and anti-Western rhetoric dominates Russian-language social networks. At the same time, anti-Ukrainian publications and actions aimed at justifying the occupation of Ukrainian territories dominate even in groups and pages that are aimed at the audience of the Baltic countries. Although the focus of the study was on the Baltic countries, statistical and systematic analysis of publications on Russian-language social networks revealed that anti-Ukrainian issues sometimes account for more than half of all ideologically motivated publications[8].

The study also notes that most propaganda accounts are created or activated in late 2013 and early 2014, and that 10 percent of Russian-speaking social media users generate 90 percent of ideological publications. Another publication in the Centre's regular edition, called Robotrolling, cites research showing an extremely high percentage of anonymous users and "bots" in the Russian-language segment of the Internet compared to the English-language segment. Thus, only 7 percent of active accounts that publish in Russian are identified as real users. The remaining 93 percent are new accounts, bots or anonymous or "fake" accounts. In the English-speaking segment, this ratio is 45 to 65 percent.

In our opinion, this indicates the growing use of the Internet as the main tool of hybrid warfare and the ongoing information aggression against our country.

Detoxification of the national information space and its cleansing from the "fake" component is recognized as one of the most important tasks in most modern developed countries. For Ukraine, this issue is particularly painful, as the security of its citizens from hostile lies and the provision of open strategic communication of national interests are vital conditions for overcoming internal contradictions and consolidating the Ukrainian people in order to carry out reforms; to carry out deoccupation and reintegration of the east of the country and to provide stable internal and external support to the government's actions.

Today it is known that the situation with cybercrime in the world has a steady tendency to worsen. This strengthens the link between cybercrime and organized crime. The Internet is used not only as an aid, but also as a place and the main means

[7] Ukrainian site Stop Fake; https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKEwin6_n7krXcAhXBdpoKHSnRC0kQFggoMAA&url=https%3A%2F%2Fwww.stopfake.org%2Fosvedomlennost-i-otnoshenie-k-dezinformatsii-i-propagande-v-smi-otchet-ob-issledovanii-stopfake%2F&usg=AOvVaw1WneOPcYw0n9pp2rQ09ZWg accessed: 15.11.2021.

[8] NATO strategic communications center of excellence; https://www.stratcomcoe.org/download/file/fid/78604 accessed: 15.11.2021.

of committing traditional crimes - fraud, theft, extortion. One of the reasons for increasing the organization of criminal activity on the Internet can be considered that such destructive activities are becoming more profitable than other means of illicit enrichment. Experts point to an alarming trend: in recent years, cybercrime has become more organized and has acquired the characteristics of a business in which profits and gaining new markets are important components. Due to the lack of borders, illegal activities are spreading to new regions around the world. Coordination of criminal activity is carried out at any distance at high speed. National criminal groups are merging with transnational criminal organizations[9]. Strengthening the organization of cybercrime in modern conditions is facilitated by two interrelated components: first, organized crime tries to use cyberspace for its own purposes, and secondly, the complex nature of cybercrime forces people who specialize in committing crimes in the network information space to coordinate their actions. unite and create organized criminal communities. Organized crime groups with complex cross-border structures are increasingly coming to the attention of law enforcement. Not only the organization of criminal groups is growing, but also their secrecy, the number of persons engaged in illegal activities on the Internet on a professional basis is increasing, the specialization of such persons is increasing. Organized crime groups often use the "Darknet" network in their activities.[10], whose websites are not indexed and which cannot be accessed through search engines such as Google or Yahoo. "Darknet" uses cryptographic technologies of network anonymity and online settlements, which have allowed criminals to create a black market where they sell and buy drugs, stolen and counterfeit goods, child pornography, weapons, and more. According to cyberpolice, one of the most popular are the so-called extortion viruses (Ransomware)[11]. Firmware is malicious software that blocks your computer and mobile devices or encrypts your files. When this happens, you cannot access the data until you have paid the ransom.[12] There has been a significant increase in phishing attacks (obtaining valuable data that can be sold or used for malicious purposes). But such attackers target not only large businesses, but also ordinary users who download applications and information related to COVID-19. The intensification of DDOS attacks took place in 2013-2014[13], but even today they cause a lot of damage.

[9] M.V. Hutsaliuk, Suchasni tendentsii orhanizovanoi kiberzlochynnosti, „Informatsiia i pravo" № 1 (2019), p. 118-128; http://nbuv.gov.ua/UJRN/Infpr_2019_1_15 accessed: 15.11.2021.

[10] Internet Organised Crime Threat Assessment (IOCTA) 2021 https://www.europol.europa.eu/cms/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2021.pdf accessed: 1.12.2021.

[11] Official site of cyberpolice of Ukraine; https://cyberpolice.gov.ua/ accessed: 1.12.2021.

[12] No more randsom; https://www.nomoreransom.org/uk/index.html accessed: 6.12.2021.

[13] S. Mazepa; L. Dostálek; O. Sharmar; S. Banakh, «Cybercrime in Ukraine and Cyber Security Game» 2020 10th International conference on advanced computer information technologies (ACIT), Deggendorf, Germany, 2020, p. 787-791, doi: 10.1109/ACIT49673.2020.9208972.

In addition, there are many cases of online fraud that have recently been linked to the fight against and treatment of coronavirus.

Investigation of Cybercrime: challenges and issues

It is also necessary to mention one of the main problems in the investigation of cybercrimes. Issues of criminal liability for cybercrime are mainly regulated in the chapter XVI "Criminal offences against computers, computer systems and networks" of Criminal Code of Ukraine. One of the most often and widespread offences is unauthorized willful interference with the computers and/or computer networks. According to the statistical data obtained from the Ministry of Internal Affairs, the registered number of these crimes has almost tripled in the last 5 years. However, given the fact that most of these crimes remain latent and unreported, the real number of these crimes should be several times more than the number of reported. The specifics of the mechanism of this crime define certain specific complexities in their investigation.

One of the problems is that criminals in most cases use technical resources and online services owned by foreign companies and are physically located outside of the Ukrainian jurisdiction.

Obtaining information and documents of probative value in criminal proceedings in such cases involves the sending of numerous international "mutual legal assistance treaty" requests. The whole process, from the beginning of the preparation of such a request to the receipt of the results, is usually quite lengthy and may take up to a year or more.

The situation is complicated by the fact that the information required to identify the perpetrators of the offences and the log-files of their actions online are in most cases only kept for a limited time.

Additionally, criminals often use special tools and technologies to anonymize their activities online. Examples are, but not limited to: TOR network, anonymous VPN services, e-mail services that publicly declare anonymity policy, process emails only in encrypted form and do not store technical information about the activities of users.

Next important issue is related to the procedural difficulties with collection of information from transport telecommunication networks.

According to the art. 263 of Criminal Procedure Code of Ukraine, collection of information from transport telecommunication networks (networks which provide transmitting of any signs, signals, written texts, images and sounds or messages between telecommunication access networks connected) is a variety of interference in private communication conducted without the knowledge of individuals who use telecommunication facility for transmitting information based on the ruling rendered by the investigating judge, if there is possibility to substantiate the facts during its conducting, which have the importance for criminal proceedings. However, according to p. 1.11. of the Instruction of covert investigation (joint order of General Prosecutor's Office of Ukraine, Security Service of Ukraine, Ministry of internal affairs, № 114/1042/516/1199/936/1687/5 dated 16.11.2012[14]) collecting information from transport telecommunication networks is only possible in investigations of grave offenses, or special grave offenses. However, p.1 of the art. 361 of Criminal Code of Ukraine "Unauthorized willful interference with the operation of computers, computer systems and networks" is not considered to be a grave offense, therefore evidence cannot be technically gathered.

The recent reform of criminal law requires an appeal to the Legal Reform Commission. As the main goal of this reform is to create new criminal and criminal procedure codes, we propose amend part 1 of Art. 361 of Criminal Code of Ukraine[15] in order to attribute it to the grave crimes; and further develop international and legal mechanisms for the effective investigation of Cybercrime, including the provisions for the direct contacts between law enforcement and private online services operators.

Development of cybersecurity legislation

In 2016, there was an attack by BlackEnergy, which caused a massive power outage in the western regions of Ukraine, which could lead to a large-scale man-made disaster and casualties. In 2017, this was the attack of the NotPETYA virus, which was recognized as the largest and caused multibillion-dollar losses. During this period, the concept of "cybercrime" did not even exist in the current Ukrainian legislation. Only in 2018, the Law of Ukraine "On Basic Principles of Ensuring Cyber Security of Ukraine"[16] came into force, which defines that cybercrime (computer crime) is a socially dangerous crime in cyberspace and / or its use, for which the law of Ukraine on criminal liability and / or recognized as a crime by international treaties of Ukraine, and cybercrime - a set of cybercrimes. At the same time, a complete list of crimes under the Criminal Code of Ukraine that should be considered cybercrimes does not yet exist. This entails a lack of

[14] Order of General Prosecutor's Office of Ukraine, Security Service of Ukraine, Ministry of internal affairs, № 114/1042/516/1199/936/1687/5 dated 16.11.2012; https://ips.ligazakon.net/document/view/gp12042?an=1 accessed: 6.12.2021.

[15] Criminal Code of Ukraine; https://zakon.rada.gov.ua/laws/show/2341-14#Text accessed: 8.12.2021.

[16] Закон України Про основні засади забезпечення кібербезпеки України (the Law of Ukraine "On Basic Principles of Ensuring Cyber Security of Ukraine"); https://zakon.rada.gov.ua/laws/show/2163-19#Text accessed: 8.12.2021.

accurate statistics on cybercrime committed for a full analysis of cybercrime as a threat to information security. Basically, there are figures that relate only to crimes limited to Section XVI of the Criminal Code of Ukraine. Identify the number of other cybercrimes, such as cyber fraud, online drug trafficking, child pornography, payment card fraud, piracy, phishing, etc., as they are contained in other sections and combined into common statistics on specific section crimes. In addition, this type of criminal activity is characterized by a high level of latency. Thus, in terms of the level of cybercrime, as of 2014 it amounted to 443 registered crimes, where 207 people were notified of suspicion, and as of 2021 3310 crimes were registered, of which 2435 people were served as suspects[17]. You can see a significant increase in the dynamics of the studied type of crime in Ukraine over the past 7 years. Compared to 2014, the number of detected crimes has increased sevenfold.

Also, the lack of the concept of cryptocurrency in the current legislation makes it difficult to prosecute individuals for committing criminal acts with their use.

Ukrainian experts are actively studying IOCTA reports prepared by a group of Europol's strategic analysts. These analytical assessments are based on materials from EU Member States and the SOCTA group in the form of structured studies. This has been enhanced with open source research and input from the private sector, including EC3's advisory groups, Eurojust, ENISA, CERT-EU, the EBF and the CSIRT community. These contributions have been essential to the production of the report. Each year, Europol's European Cybercrime Centre (EC3) publishes the Internet Organized Crime Threat Assessment (IOCTA), its flagship strategic report on key findings and emerging threats and developments in cybercrime — threats that impact governments, businesses and citizens in the EU[18]. The IOCTA provides key recommendations to law enforcement, policy makers and regulators to allow them to respond to cybercrime in an effective and concerted manner. Unfortunately, as of today, no such study has been conducted in Ukraine.

In addition, Ukraine's positive steps to strengthen cybersecurity should be highlighted. Thus, in August 2021, Ukraine approved a new version of the State Cyber Security Strategy[19]. The need to reconsider the approach to cyber defense in Ukraine was also discussed during the international forum "Cybersecurity - let's protect business, let's protect the state." In early November 2021, it took place in Kyiv. Yuri Shchigol, head of the State Special Service, had a speech about launch of

[17] General prosecutor's office of Ukraine; https://gp.gov.ua/ua/posts/pro-zareyestrovani-kriminalni-pravoporushennya-ta-rezultati-yih-dosudovogo-rozsliduvannya-2 accessed: 9.01.2022.

[18] Internet Organised Crime Threat Assessment (IOCTA) 2021 https://www.europol.europa.eu/cms/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2021.pdf accessed: 1.12.2021.

[19] Strategy of cybersecurity of Ukraine; https://www.president.gov.ua/documents/4472021-40013 accessed: 1.12.2021.

national center for reserving state information resources, "the Swiss Bank of Our Registers", he said[20]. But since cybersecurity is a process, not a state, and it is simply impossible to create an effective protection system once and for all, the work of international organizations and the exchange of experience is very important.

In particular, the Strategy clearly identifies threats to Ukraine's cybersecurity:

- hybrid aggression of the Russian Federation against Ukraine in cyberspace. The aggressor state is constantly increasing the arsenal of offensive cyber weapons, the use of which can cause irreparable, irreversible destructive consequences. Cyberattacks of the Russian Federation are aimed primarily at information and communication systems of state bodies of Ukraine and critical information infrastructure in order to disable them (cyber diversion), gain covert access and control, intelligence and intelligence activities. Cyberattacks are also actively used by the aggressor state as an element of special information operations aimed at manipulating the population, interfering in electoral processes and discrediting Ukrainian statehood;
- cybercrime, which damages information resources, social processes, personally citizens, reduces public confidence in information technology and leads to significant material losses. The use of cyberspace to commit crimes against the national security of Ukraine, as well as criminal offenses related to money laundering, trafficking in human beings, illicit handling of weapons, ammunition or explosives, illicit trafficking in narcotic drugs and psychotropic substances is becoming widespread., their analogues or precursors and other objects and substances that threaten human life and health, etc .;
- cyberattacks organized and sponsored by other governments in connection with the theft of sensitive information for political, economic or military purposes (cyber espionage) and intelligence and subversive activities. Features of such cyberattacks are their duration, complexity and hidden nature, which complicates their prevention, detection and neutralization;
- use of cyberspace by terrorist organizations to commit acts of cyberterrorism, financial and other support for terrorist activities.

Given the challenges and threats facing Ukraine in cyberspace, the role of cybersecurity in the process of digital transformation of the state is growing critically[21].

[20] State forum of cybersecurity; https://cybersecurity-2021.ciseventsgroup.com/ accessed: 1.12.2021.

[21] Strategy of cybersecurity of Ukraine; https://www.president.gov.ua/documents/4472021-40013 accessed: 1.12.2021.

Conclusions

An overview of the situation in the cyberspace of Ukraine as a result of the hybrid war and the COVID-19 pandemic allows us to conclude that combating cybercrime at the present stage of development of the information society is not possible in an isolated, separate field: military, political, legal, economic, technical etc. The current situation requires the combination of knowledge and efforts of specialists in various fields to create a comprehensive approach to combating this socially dangerous phenomenon. The main features of cybercrime as the main threat to Ukraine's information security are outlined.

Information and communication technologies are being implemented and developed much faster than legislators and law enforcement agencies can respond. The number of cybercrimes is growing every year, seven times in the last seven years. We should not forget that cybercrime is characterized by high latency and the real figure will be at least twice as high. Therefore, the fight against cybercrime is one of the most pressing issues facing the entire world community, including Ukraine. New technologies make life easier and provide significant benefits to humanity, but at the same time create new forms of crime. Cybercrime is becoming increasingly organized. Organized cybercrime is constantly transforming, which poses new threats and challenges that require various measures, including organizational, legal and technical, in order to adequately prevent the protection of both cyberspace users and critical infrastructure, banking system, etc.

Among the main directions for further improvement of existing and development of new approaches to combating cybercrime is the need to prepare an IOCTA analytical report in Ukraine, which would be important for the implementation of the Europol-Ukraine Strategic Cooperation Agreement and promote effective implementation of the Cyber Security Strategy; introduction of changes in the current criminal legislation to change the severity of computer crimes (in the context of the addition of qualifying features), which will provide an opportunity to conduct covert investigative (investigative) measures that will facilitate documentation; timely introduction of scientifically sound concepts and definitions, such as "cryptocurrency", which will make it possible to prosecute individuals for committing criminal acts with their use. The issue of establishing legal liability for intentional mass distribution of fake news should also be raised.

It is clear that it is not possible to investigate all the issues that have existed and been exacerbated by the COVID-19 pandemic in a single publication. However, this contribution is the basis for further discussions and legislative initiatives.

* * *

Cybercrime as a leading threat to information security: ukrainian experience

(summary)

Since 2020, there has been a significant increase in crimes committed on the Internet. The reason for this is the global trend in the growth of Internet crime and quarantine restrictions. Due to the Covid-19 pandemic, life was almost completely transformed into information space. And crime has also gone online. It is now possible to seize other people's money, threaten, harass, paralyze vital critical infrastructure without leaving home, just by sitting at a computer. The dynamics of cybercrime in Ukraine and the world is analyzed. Ways to improve state information security have been identified.

Bibliography

Constitution of Ukraine; https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text accessed: 20.11.2021.

Criminal Code of Ukraine; https://zakon.rada.gov.ua/laws/show/2341-14#Text accessed: 8.12.2021.

Hutsaliuk M.V., Suchasni tendentsii orhanizovanoi kiberzlochynnosti, „Informatsiia i pravo" № 1 (2019), p. 118-128; http://nbuv.gov.ua/UJRN/Infpr_2019_1_15.

Internet Organised Crime Threat Assessment (IOCTA) 2021 https://www.europol.europa.eu/cms/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2021.pdf accessed: 1.12.2021.

Mazepa S., Dostálek L., Sharmar O., Banakh S., «Cybercrime in Ukraine and Cyber Security Game» 2020 10th International conference on advanced computer information technologies (ACIT), Deggendorf, Germany, 2020, pp.787-791 doi: 10.1109/ACIT49673.2020.9208972.

Murray A., Information Technology Law: The Law and Society (4th edn) Oxford University Press https://doi.org/10.1093/he/9780198804727.001.0001.

NATO-2030; https://www.nato.int/nato_static_fl2014/assets/pdf/2020/12/pdf/201201-Reflection-Group-Final-Report-Uni.pdf accessed: 1.12.2021.

NATO strategic communications center of excellence; https://www.stratcomcoe.org/download/file/fid/78604 accessed: 15.11.2021.

Order of General Prosecutor's Office of Ukraine, Security Service of Ukraine, Ministry of internal affairs, № 114/1042/516/1199/936/1687/5 dated 16.11.2012; https://ips.ligazakon.net/document/view/gp12042?an=1 accessed: 6.12.2021.

Prysiazhniuk D.M., Zastosuvannia manipuliatyvnykh tekhnolohii z boku Rosii v ZMI Ukrainy (na prykladi Krymu) [Application of manipulative technologies by Russia in the media of Ukraine (on the example of Crimea)] http://vuzlib.com/content/ view/1108/23 accessed: 15.11.2021.

Ukrainian site Stop fake; https://www.stopfake.org/osvedomlennost-i-otnoshenie-k-dezinformatsii-i-propagande-v-smi-otchet-ob-issledovanii-stopfake accessed: 15.11.2021.

Universal declaration of human rights; https://www.un.org/sites/un2.un.org/files/udhr.pdf accessed: 11.11.2021.

Закон України Про основні засади забезпечення кібербезпеки України (the Law of Ukraine "On Basic Principles of Ensuring Cyber Security of Ukraine");; https://zakon.rada.gov.ua/laws/show/2163-19#Text accessed: 8.12.2021.

https://cyberpolice.gov.ua/ accessed: 1.12.2021.

https://www.nomoreransom.org/uk/index.html accessed: 6.12.2021.