colloquium-journal

ISSN 2520-6990

Międzynarodowe czasopismo naukowe

Jurisprudence
Public administration

№14(101) 2021
Część 4

colloquium-journal

ISSN 2520-6990

ISSN 2520-2480

Colloquium-journal №14 (101), 2021

Część 4

(Warszawa, Polska)

«Colloquium-journal»
Wydawca «Interdruk» Poland, Warszawa
Annopol 4, 03-236
E-mail: info@colloquium-journal.org
http://www.colloquium-journal.org/

CONTENTS

PUBLIC ADMINISTRATION

Вергунов Г.А., Антонова Н.Л.
ПОЛИТИКА ГОСУДАРСТВА ПО РАЗВИТИЮ ТВОРЧЕСКИХ СПОСОБНОСТЕЙ ЧЕЛОВЕКА 4
Vergunov G.A., Antonova N.L.
STATE POLICY ON THE DEVELOPMENT OF HUMAN CREATIVITY 4

Сацюков П.А., Васильев В.И.
ТОРГОВАЯ ДЕЯТЕЛЬНОСТЬ КАК ОБЪЕКТ ГОСУДАРСТВЕННОГО РЕГУЛИРОВАНИЯ....9
Satsyukov P.A., Vasiliev V.I.
TRADE ACTIVITY AS AN OBJECT OF GOVERNMENT REGULATION 10

JURISPRUDENCE

Килівник А.
ПРОБЛЕМИ РЕГУЛЮВАННЯ ПРОЦЕДУР БАНКРУТСТВА 12
Kylivnyk A.
PROBLEMS OF REGULATION OF BANKRUPTCY PROCEDURES 12

Baboi A.
CYBERCRIME AS AN INTEGRAL PART OF THE DEVELOPMENT OF THE INFORMATION SOCIETY 14

Baboi V. S., Kovalchuk O. Yu.
CURRENT PROBLEMS AND DEVELOPMENT PROSPECTS ELECTRONIC GOVERNANCE IN UKRAINE 22

Васильева В.С., Малиненко Э.В.
МЕСТО КОНСТИТУЦИОННОГО СУДА В ЗАКОНОДАТЕЛЬНОМ ПРОЦЕССЕ РОССИЙСКОЙ ФЕДЕРАЦИИ 29
Vasilyeva V.S., Malinenko E.V.
THE PLACE OF THE CONSTITUTIONAL COURT IN THE LEGISLATIVE PROCESS OF THE RUSSIAN FEDERATION 29

Дедок Н. М., Шарыпова В. А.
ВИДЫ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, ИСПОЛЬЗУЕМЫХ В ПРАВОВОЙ СФЕРЕ 31
Dedok N. M., Sharypova V.A.
TYPES OF INFORMATION TECHNOLOGIES USED IN THE LEGAL FIELD 31

Желтяк Т. П.
МОМЕНТ ОКОНЧАНИЯ ХИЩЕНИЯ ПРЕДМЕТОВ, ИМЕЮЩИХ ОСОБУЮ ЦЕННОСТЬ....33
Zheltyak T. P.
THE MOMENT OF THE END OF THE THEFT OF ITEMS OF SPECIAL VALUE 33

Желтяк Т. П.
ПРЕДМЕТ И ОБЪЕКТ ХИЩЕНИЯ ПРЕДМЕТОВ, ИМЕЮЩИХ ОСОБУЮ ЦЕННОСТЬ....34
Zheltyak T. P.
SUBJECT AND OBJECT OF THEFT OF ITEMS OF SPECIAL VALUE 34

Желтяк Т. П.
ОБЪЕКТИВНАЯ И СУБЪЕКТИВНАЯ СТОРОНА ХИЩЕНИЯ ПРЕДМЕТОВ, ИМЕЮЩИХ ОСОБУЮ ЦЕННОСТЬ 36
Zheltyak T. P.
THE OBJECTIVE AND SUBJECTIVE SIDE OF THEFT OF ITEMS OF PARTICULAR VALUE 36

Ілляшик К.
ПРОБЛЕМИ СТАНОВЛЕННЯ ПРАВОВОЇ ДЕРЖАВИ В УКРАЇНІ....38
Illiashyk K.
PROBLEMS OF THE FORMATION OF THE RULE OF LAW IN UKRAINE 38

Mangora T.V.
FEATURES OF LEGAL RESPONSIBILITY FOR VIOLATION OF LEGISLATION ON CONSUMER PROTECTION 40

Overkovska T.
LEGAL PROTECTION OF LAND FROM POLLUTION....48

лише практика застосування норм нового кодексу дасть відповідь на питання – чи належним чином захищені права таких кредиторів у процедурі банкрутства та яким чином забезпечені кредитори матимуть можливість реалізувати свої права та захистити охоронювані законом інтереси.

Список літератури

1. Кодекс України з процедур банкрутства від 18 жовтня 2018 року. URL: https://zakon.rada.gov.ua/laws/show/2597-19.

2. Про відновлення платоспроможності боржника або визнання його банкрутом: Закон України від 14 травня 1992 року. URL: https://zakon.rada.gov.ua/laws/show/2343-12.

3. Дайджест судової практики Касаційного господарського суду у складі Верховного Суду у справах про банкрутство. Рішення, внесені до ЄДРСР за період з 18.06.2019 по 15.07.2019 / — Київ, 2019. — Вип. 15. — 12 стор.

4. Про деякі питання практики застосування Закону України «Про відновлення платоспроможності боржника або визнання його банкрутом»: Рекомендації Вищого господарського суду України від 04.06.2004 р. //Збірник поточного законодавства, нормативних актів, арбітражної та судової практики. – 2004. - No 36

5. Джунь В.В. Процесуальні фігуранти конкурсного процесу у світлі судової практики // Вісник господарського судочинства. – 2005. - N4. – С. 136 – 140

6. Поляков Б.М. Правовые проблемы регулирования несостоятельности (банкротства).: Дис. ...доктора юрид. наук. – К. – 2003. – С. 194

7. Джунь В.В. Інститут неспроможності: світовий досвід розвитку та особливості становлення в Україні. Монографія. – Видання друге, виправлене і доповнене. – К.: Юридическая практика, 2006. – С. 117

8. Н.Теремцова. Бюджетний процес за законодавством України Монографія Бюджетний процес за законодавством України: монографія / –К.: Вид. ТОВ «Інтер Логістик України». 2010. – 240с.

9. Teremtsova N. (2017) The main types understanding to legal liability: the theoretical aspect. European Perspectives (Politics, Economics, Law) 1. 12-18.

10. Teremtsova, N. (2019). The problem of differentiation between private and public law. Journal Transition Studies Review, 26(2), 15-22. Index Scopus 2019 International ISSN: 1614-4007.

11. Kopotun, I. M., Durdynets, M. Y., Teremtsova, N. V., Markina, L. L., & Prisnyakova, L. M. (2020). The Use of Smart Technologies in the Professional Training of Students of the Law Departments for the Development of their Critical Thinking. International Journal of Learning, Teaching and Educational Research, 19(3).Index Scopus 2020 International ISSN: 1694-2116.

12. Н.Теремцова. Актуальне питання визначення принципу єдності бюджету в Україні: теоретико-правовий аспект. Юридична освіта: осмислення, виклики та перспективи (пам'яті Юрія Бондаря). / Редкол. : А. М. Завальний, Ю. В. Кривицький, Н. В. Лазнюк. Київ : НАВС, 2020. 110с.

13. Н.Теремцова. Теоретико-правові основи здійснення контролю за дотриманням бюджетного законодавства. /Редкол.: А.П.Гетьман, М.П. Кучерявенко, Н.Ю. Пришва та ін.. – Київ: Асоціація фінансового права України, 2016. – 300 с. – С. 228-232. URL: http://afl.org.ua/2016/12/10/voronovsbki-chitannya-2016-zbirnik-tez.

УДК 343.2(477)

Baboi Anna
senior lecturer at the Department of Law,
Faculty of Management and Law
Vinnytsia National Agrarian University
DOI: 10.24412/2520-6990-2021-14101-14-22

CYBERCRIME AS AN INTEGRAL PART OF THE DEVELOPMENT OF THE INFORMATION SOCIETY

Abstract.
The article analyzes the history of the formation and spread of cybercrime. The tendency of increasing cybercriminal activity in Ukraine has been investigated. The reasons for the increase in cybercriminal activity have been determined. The positive experience of foreign countries in the fight against cybercrime has been investigated. The advantages and disadvantages of law enforcement in the field of cybercrimes have been investigated. Methods of combating cybercrime activities have been determined.

Keywords: *cybercrime, information society, Internet crime, cyber space, Internet.*

Formulation of the problem. Since the end of the 20th century, the development of information technology has revolutionized the field of communications, which has become a key factor in the rise and growth of the world economy. This phenomenon has enabled people around the world to benefit from the convenience, speed and accessibility of information transfer and digital transactions, but also increased the risk of damage and theft of personal data by cybercrime groups and hackers. The problem of cyber risks at the global level has been officially named one of the five key threats to humanity since 2012. In the proceedings of the World Economic Forum that year, cyber attacks ranked fourth in the ranking of threats. In five years, the report identified new types of cyber threats: data theft and fraud.

Words and phrases that scarcely existed a decade ago are now part of our everyday language, as criminals use new technologies to commit cyberattacks against governments, businesses and individuals. These crimes know no borders, either physical or virtual, cause serious harm and pose very real threats to victims worldwide.

Cybercrime is progressing at an incredibly fast pace, with new trends constantly emerging. Cybercriminals are becoming more agile, exploiting new technologies with lightning speed, tailoring their attacks using new methods, and cooperating with each other in ways we have not seen before. Complex criminal networks operate across the world, coordinating intricate attacks in a matter of minutes. Police must therefore keep pace with new technologies, to understand the possibilities they create for criminals and how they can be used as tools for fighting cybercrime.

Analysis of recent research. There are a number of monographs, scientific articles devoted to the research of cybercrime, but this issue is quite "vague" and needs constant study and improvement. This topic has been studied by many scientists, in particular: N. Akhtyrska, Yu. Baturyn, P. Bilenchuk, O. Botvinkin, V. Golubev, V. Gavlovsky, M. Gutsalyuk, M. Karchevsky, M. Kravtsova, O. Litvinov, Yu. Nizovtsev, O. Parfilo, B. Romanyuk, O. Rosinskaya, T. Tropina and others.

Presentation of the main material. More recently, cybercrime has come to be seen on a par with the world's greatest threats. At first glance, inconspicuous, petty online fraud seems like a petty and inconspicuous threat and does not draw the necessary attention to the problem.

Considering the full potential and threat in full, one could consider the possibility of cyberattacks on critical infrastructure, the theft of millions of dollars from bank accounts, interference with the will of states, and even the hacking of military systems responsible for launching missile launchers. It is necessary to realize that cybercrime is a phenomenon of international importance. The development of cybercrime is proportional to the development of computer technology and poses a threat not only to personal property and non-property rights of people, but also to national security.

With the rapid development of informatization in Ukraine, a potential bridgehead for the use of computer technology for selfish reasons. Therefore, much more attention should be paid to the issue of cybersecurity.

Cybercrime involves gaining illegal access to or illegal entry into a computer or illegally interfacing with another through the use of a computer. Some cybercrimes are just a new method for committing old offences against property, such as theft and fraud, or crimes against the person, such as harassment and assault. Other cybercrimes are newly created offences, enacted to respond to the computer's ability to be used as a conduit for unacceptable behaviour, such as phishing and hacking. They are typically legislative responses to behaviour that affects government or large corporate interests: advance fee frauds, cyber fraud (through phishing, malware, scamming and hacking), auction frauds, non-delivery and credit-debit card frauds, identify theft, stock market manipulations, investment and pyramid schemes, digital extortion, cyber-terrorism and industrial sabotage, intellectual property infringement, and unauthorized access.

The COVID-19 pandemic renders individuals and society extremely vulnerable in all respects. During this crisis, we all rely more than ever on computer systems, mobile devices and the Internet to work, communicate, shop, share and receive information and otherwise mitigate the impact of social distancing. There is evidence that malicious actors are exploiting these vulnerabilities to their own advantage. Criminal justice authorities need to engage in full cooperation to detect, investigate, attribute and prosecute the above offences and bring to justice those that exploit the COVID-19 pandemic for their own criminal purposes.

Cybersecurity plays a significant role at the state level. Cyber attacks often target critical infrastructure: energy, transportation, and the banking sector. In most cases, the price of protection is ten times cheaper than the attack itself. Thus cybersecurity must be a priority way for development of legal states.

The definition of "cybercrime" was first provided in 1983 in Paris by a group of experts from the Organisation for Economic Co-operation and Development: cybercrime is any illegal, unethical or unauthorized act involving automated data processing or data transmission. Since then and to this day, the concept of cybercrime is debatable and one of the most discussed in legal circles [1]. With the further development of information technology, along with the concept of "computer crime", the concept of "cybercrime" is gradually beginning to be used. This term is a combination of the words "cybernetics" and "crime". The term "cybercrime" became widespread after the signing of the Cybercrime Convention by member states of the Council of Europe and other states in 2001.

Subsequently, on 21 July 2006, the Additional Protocol to the Convention on the Criminalization of Racist and Xenophobic Acts Committed through Computer Systems was ratified. At the same time, the term "computer crime" is preferred in the domestic legal literature, dissertation research and normative legal acts.

In particular, the Law of Ukraine of June 19, 2003 "On the Fundamentals of National Security of Ukraine" [2] contains the terms "computer crime", "computer terrorism". These concepts are also applied in the Doctrine of Information Security of Ukraine, approved by the Decree of the President of Ukraine of July 8, 2009. Instead, the term "cybercrime" is already present in the National Security Strategy of Ukraine, approved by the Decree of the President of Ukraine of May 26, 2015.

These types of crimes have certain specifics. The crime is carried out from anywhere on Earth, and the victim of the crime can be hundreds and thousands of kilometers away. The convenience of committing such crimes is that in order to commit such a crime you only need to have access to the Internet. With the constant development of technology and the cheapening of computer devices, the development of cybercrime is gaining momentum.

In addition, the detection of such crimes is extremely difficult, and the gathering evidence in the

course of investigative actions is quite difficult, and in many cases - impossible. All these factors are great advantage for cybercriminals.

Regulation of cybercrime in Ukraine lags behind the development of technology, which is an acute problem. Piracy is a favorable condition for the development of cybercrime in Ukraine. Using pirated software, ordinary network users serve as a tool for D-DOS hacker attacks, transmit viruses, and unsuspectingly hand over access to all their personal data to attackers.

That's why its so important to provide a definition of "cybercrime". Cybercrime is a criminal activity committed through computers and the Internet. This includes everything from downloading illegal music files to stealing millions of dollars from online bank accounts. Cybercrime also includes non-monetary crimes, such as creating and spreading viruses on other computers or posting confidential business information on the Internet.

Speaking of cybercrime in the criminal aspect, cybercrime can be understood as a criminally punishable actions aimed at unauthorized interference with the normal operation of computer networks, systems and programs, the purpose of which is to modify or seize computer data. In this case, the subject of the crime is a computer, and the object - information security. In these crimes, the instrument of the crime is a computer, and the purpose of the crime is material gain, infringement of copyright, property, morality and public safety.

The most common and popular crimes in this area are:

- Carding - illegal use of the card (Credit/Debit) by unauthorized people (carder) to buy a product.

- Phishing - fraudulent actions that mislead people in order to obtain the details of stolen payment or virtual cards and passwords.

- Wishing - cybercrimes aimed at obtaining confidential data of the holder, by sending spam with a request to call a certain number, and in a telephone conversation clarifying the confidential data of the cardholder.

- Online fraud - the activities of fake online stores, auctions and other sites that can mislead a person for selfish motives;

- Piracy - illegal distribution of intellectual property on the Internet;

- Card-sharing - providing illegal access to satellite and cable television;

- Social engineering - a technology that involves selfish management of people in the network;

- Malware - development and distribution of malicious software and computer viruses;

- Illegal content - content which main purpose is to promote extremism, terrorism, drug addiction, pornography and the cult of cruelty and violence.

Cybercrimes are characterized by specific features:

- Cybercrime must be committed with an appropriate instrument of crime - using computer technology;

- crimes of this classification are committed in a specific environment - cyberspace.

Cyberspace is a computer-modulated cyberspace that contains data about a person, phenomena, and processes in mathematical, symbolic, or other forms. This information is in the process of moving on local and global computer networks, stored in the memory of any physical or virtual device specifically designed for storage, modification and transmission.

Thus, the object of unlawful encroachment are the relations of all branches of human activity that are represented and function in cyberspace.

The first crimes committed with computers were registered in the early 1960s, and the concept of "computer crime" appeared in the American press. Despite the lack of both forensic and legal grounds, the term began to be used in the media, scientists, law enforcement officers and more.

It should be noted that in the territory of the former Soviet Union, the first computer crime was registered in 1979 in Vilnius (Lithuania), where the theft caused damage amounting to 78,584 rubles.

The first computer crime in Ukraine was committed in 1990. The program for an electronic computer, which recalculated the Komsomol contributions of workers of one of the industrial enterprises of Lugansk to the current account of the district committee of the Komsomol, was drawn up in such a way that the corresponding money were deducted not only from Komsomol members but also from all other workers. .

Analysis of official statistical reporting data for the last fourteen years in Ukraine makes it possible to record a rapid trend of stable growth of cybercrime. In 2015 the number of registered cybercrimes in Ukraine was 556, compared to 2002, which is 1753.3% more and 33% more than the number of cybercrimes in 2014. During the period 2002-2015, the growth rate of cybercrime was 107.5%. Such statistic shows the opposite of cybercrime levels to the level of common crime in the country. This indicates:

a) the specificity of the complex cycle of cybercrime, in which during 2014-2015 an important role is played by external aggression against Ukraine in cyberspace;

b) the lag of law enforcement capabilities from the current level and the provision of cybercrime activity, in particular, the nature of the fight is catching up, not ahead in terms of preventive and jurisdictional policing.

Taking into account expert assessments and analysis of statistical data, it was found that the level of latency of cybercrimes is about 95%, which allows them to be classified as highly latent. Forming latency factors distinguish several groups: 1) the natural latency of cybercrime, according to which information about the crime is available only to the subject of the crime; 2) factors related to the disinterest of victims and eyewitnesses of the crime and their failure to apply to law enforcement agencies, failure to report the fact of the crime; 3) factors related to the drawbacks of law enforcement agencies in terms of disinterest and rapid response to reports of crimes: a) related to the errors of law enforcement officers in the availability, definition and classification of the composition; b) related to concealment and non-entry in the register of crimes.

The main share in the structure of cybercrime in Ukraine is unauthorized interference in the operation of computers, systems, computer networks or telecommunication networks (56.5%) and unauthorized actions with information processed in electronic computers (computers), automated systems, computer networks or stored on media such information committed by a person who has the right to access it (31.5%). A characteristic feature of the structure of cybercrime is a steady increase in the share of serious crimes, which since 2008 has fluctuated at 45-59%. It was found that the decisive role in restoring the tendency to increase the level of cybercrime in 2015, after a certain decline in 2014, played the crimes under Art. 361 and Art. 361-2 of the Criminal Code of Ukraine. In general, in 2015 there was a positive increase in all components of cybercrime, except for crimes under Art. 362 of the Criminal Code of Ukraine, which is atypical given the traditionally significant share of the latter and their leading role in determining the characteristics of the structure of cybercrime.

Instead, starting from 2013, the growth rate of these crimes slowed down significantly, gaining negative values in 2014 and 2015 (- 51.4% and - 57.7%, respectively). Every tenth cybercrime is committed in the group. Since 2006, there has been a downward trend in the proportion of juveniles who have been completely absent from cybercrime over the past five years. It has been established that only 35–45% of registered cybercrimes are solved. Only 25% of identified persons accused of committing crimes in this category are convicted. Thus, only for every tenth crime committed in cyberspace and registered, the perpetrators are criminally liable. It is believed that this situation is a consequence of systemic dysfunctions in crime units, which are manifested in insufficient scientific, logistical, staffing of the cyberpolice structure and pre-trial investigation bodies [3].

Also, there is a problem of inconsistency of judicial practice regarding the imposition of penalties for cybercrimes of the nature and degree of their public danger. After all, in the vast majority of persons whose guilt is proven, the court is released from criminal liability, punishment or its serving (67%); among the imposed punishments the fine prevails; in half of the cases, a milder punishment is imposed than provided by law; only in a small number of cases does the court impose an additional penalty in the form of confiscation of property (3%).

Since 2015, 4,749 cases have been initiated under Article 361, given that the number of convictions is only 113. In 2016, thousands of Ukrainian companies suffered from the Petya virus, but the number of written statements about lost data to the relevant law enforcement agencies was negligible, and written remain unanswered. This indicates the small percentage of criminals prosecuted under this article and the great difficulty in detecting and investigating such crimes. The increase in the detection of such crimes and the initiation of criminal cases over the past few years can be attributed to the gradual increase in the number of cyber police officers. However, a large number of such cases either do not reach the court or fall apart during the trial due to insufficient evidence. This situation in our country has arisen due to insufficient staffing, lack of literacy and professionalism of investigators and experts who could properly qualify and bring cases of such categories to appropriate punishment.

Preconditions for the development and functioning of cybercrime are created by social factors. After all, there are changes in the social life of society, due to the rapid pace of technical development and scientific modernization. Computerization is taking place and a huge information space is being formed. Many specific areas are moving into cyberspace, creating new relationships in the field of computer networking. And of course, there are other opportunities for cybercrime. We can say that cybercrime is a causal result of technical development and modernization [4].

Political factors include the government's lack of understanding of the dangers of cybercrime and the consequences for the state as a whole. Lack of sufficient funding for research in the field of combating cybercrime. Unconformity of legal support and regulation of the pace of development of the environment of these crimes. The current legislation lags behind the needs of society in the field of cybercrime.

As a rule, the factors involved in the work of the law enforcement system have an impact on the functioning and development of crimes. In particular, the imperfection of criminal and criminal procedure legislation; lack of necessary knowledge in law enforcement agencies, which simply leads to the innocence of crimes in cyberspace; technical difficulty to offer information threats; weak coordination of actions in combating cybercrime between state and law enforcement agencies.

If we take into account the peculiarities of cybercrime in Ukraine depending on geographical conditions, we can find that in the eastern part compared to the western part, crime rates are higher. This is explained by the fact that industrial and technical development prevails in the eastern regions, which is impossible without the involvement of modernized information technologies. Information technology is the environment of cybercrime.

Analyzing the geographical features of individual cybercrimes, we can identify a pattern - some types of violations of the law belong to the place of commission, mainly in large cities. For example, such crimes as: distribution or sale of specialized malware; illegal sale or dissemination of information with limited access; carried out through violation of basic rules for the protection of information and violation of established rules for the use of computer networks or telecommunications networks.

There are the following factors that contribute to the spread of cybercrime: low level of control over the reproduction and distribution of computer software; high level of latency of crimes, very low percentage of crimes committed on a computer network become known to law enforcement agencies; low level of theoretical and practical knowledge for the investigation of crimes in the field of computer use, in the system of computer networks and telecommunication networks; the difficulty of opening legal proceedings in this cate-

gory : there are more errors in the investigation of cybercrime than in the investigation of traditional crimes, because this area requires a high level of specialized knowledge. That is, technological developments are taking place, which links the increase in cybercrime crimes, which are not always possible to track.

The Criminal Code of Ukraine provides for criminal liability for cybercrime. These crimes are qualified by articles: Art. 361 of the Criminal Code, Art. 361-2 of the Criminal Code, Art. 362 of the Criminal Code, Art. 363 of the Criminal Code, Art. 363-1 CCU. Liability is provided for crimes such as unlawful interference with computers, various automated systems and computer or communication networks; creation of malicious programs for sale or distribution; if the subject of the crime is engaged in the dissemination or sale of information that has the character of restricted access and is stored in appropriate automated systems or electronic media; illegal actions by a person who has access to information with limited access and is stored on electronic media or in automated systems, computer networks, etc .; when there is a violation of the rules of operation of automated systems, computer networks or telecommunication networks; when computers, automated systems, and telecommunication networks are intentionally disrupted by the dissemination of mass messages [5].

Unfortunately, national legislation does not sufficiently meet the needs of the modern world, because it does not contain concepts that are the starting point in the field of information security infrastructure of the state, which is in the process of formation.

The current CCU provides only part of the criminal acts that are common in cyberspace. Due to the rapid modernization of the information infrastructure, the number of crimes is increasing, changing, but not all are responsible.

Cybercrime is also classified in other articles of the Criminal Code:

- Part 3 of Art. 190 of the Criminal Code - fraud committed through illegal transactions using electronic computers;

- Art. 200 of the Criminal Code - provides for the use of counterfeit electronic means of access to bank accounts;

- Part 4 of Art. 301 of the Criminal Code, provides for the sale and distribution of pornographic items using electronic computers. One of the most common crimes in Ukraine, but unfortunately due to technical impossibility and on the basis of corruption, the disclosure of these types of crimes is low statistics.

After the adoption of the current Criminal Procedure Code of Ukraine, there are many cases of classification of crimes in the field of computer technology under Art. 185 of the Criminal Code, although to a greater extent its content relates to crimes against property [6].

Cybercrime refers to crimes, not misdemeanors. However, this area needs detailed improvement in Ukraine. After all, not all crimes can be classified and immediately attributed to some category of the article of the Criminal Code. The practical sphere is improving at a very fast pace, which requires rapid legal improvement and updating in the current legislation.

The activities of the bodies of the legal system that ensure the fight against cybercrime are characterized by tasks that are specific in nature and the implementation of which should contain objective conclusions and solutions.

For instance:

- to start the activities of law enforcement agencies, there must be a basis, namely information or a message about the commission of an illegal act in the field of computer information, technology or other crime;

- this activity can only be carried out by persons working in law enforcement agencies, have the appropriate education and qualifications;

- the relevant decisions of law enforcement agencies should be based only on legal grounds;

- law enforcement agencies carry out their activities to combat cybercrime only in a procedural form on the basis of the law, any other actions not provided for by law are unacceptable;

- legal decisions made by law enforcement agencies are subject to mandatory execution by all citizens and officials.

Law enforcement agencies, especially the National Police, are of great importance in countering cybercrime. According to the Cybersecurity Strategy of Ukraine, the national police, as a body, refers to the cybersecurity system, whose competence includes ensuring human rights and freedoms, protecting the interests of society and the state from criminal encroachments and facilitating the investigation of such crimes. The structural divisions of the National Police that are available in the allocation are as follows [7]:

- a subdivision of the Department of Cyberpolice, whose specialists are authorized to counteract offenses in the field of the computer network, in the telecommunication network and crimes using electronic computers. Ukraine has ratified provisions of the Council of Europe Convention on Cybercrime, therefore, the units of the Cyber Police Department, therefore, are directly obliged to carry out operational and investigative activities to counter the crimes provided for by the Convention.

The tasks of the "cyberpolice" include the implementation of state policy in the area of countering these crimes, timely informing the population about the development and the emergence of new cybercrimes. And also one of the tasks is to respond to requests from foreign partners that will come.

The Cyber Police Department is an interregional territorial body. It includes structural divisions directly subordinate to the chief on an interregional basis. These units are:

- operational units of the National Police assist in the manner prescribed by the current legislation in the prevention, detection and suppression of cybercrime. First of all, they ensure the receipt of timely information on the commission of the relevant crimes [8]:

- subdivisions of counterintelligence protection of the interests of the state in the field of information security, protection of the national statehood of the Security Service of Ukraine (SSU).

Their tasks are: prevention, disclosure and suppression of crimes related to crimes against peace and security, terrorism and crimes committed in the field of management and economics, posing a threat to the priority interests of Ukraine. These crimes, in the context of modernized technologies, often have a connection with cyberspace, or are committed directly there. Especially with regard to the information sphere, interference in which may pose a threat to the security of the state as a whole.

The SSU has introduced the Department of Special Telecommunication Systems and Information Protection. In this body, regulations require special specialized information protection. The information, the use of which is carried out by departmental automated systems, must be protected from criminal encroachments. That is, the SSU has created groups that are supposed to counter some specific types of cybercrimes.

Sources of information on cybercrime include:

- written and electronic messages with information about the crime;
- inquiries and notifications of the bodies of the legal system of foreign countries;
- materials obtained as a result of verification of communications of citizens with whom secret cooperation was carried out;
- written instructions and orders of investigators;
- other information obtained as a result of operational and search actions.

Law enforcement agencies can identify cybercrimes during the investigation of other qualifications of the crime [9].

After analyzing the legal system of Ukraine, we can conclude that the system of bodies whose powers include the fight against cybercrime is functioning. But if we compare with the systems of other developed countries, then we do not have a structured mechanism of activity in the fight against cybercrime, and also there is no implemented specialized technology.

Our state needs a gradual transformation of the current model to the newest human rights body. Which, thanks to its technological capabilities, facilitate an instant response to cyber threats.

And also it is necessary to develop cooperation to combat transnational groups in cyberspace.

International cooperation is an important element in the fight against cybercrime. After all, counteracting at the level of individual states is very difficult and does not reach the expected level of success. Therefore, there is a need for organizational, scientific and legal support in the use of computer technologies at the international level [10].

Improvement of Ukrainian legislation should be based on analysis and research of international experience in countering cybercrime.

The experience of combating cybercrime in foreign countries is much greater, because in developed countries the technology sector is ahead of Ukraine, that is, the development and spread of various crimes is very characteristic [6].

This issue is under the control and focus of such international institutions and bodies as the United Nations, in particular the General Assembly, the Economic and Social Council, the Commission on Crime Prevention and Criminal Justice. After all, it has been determined that these crimes pose a threat to the security of each state, especially with regard to the information sphere. The first international document to combat cybercrime was adopted in 1990 at the European Committee on Crime Problems of the Council of Europe and was called the "Minimum List", and provided for such crimes as: computer forgery, fraud, illegal copying of protected computer programs and making various topographic copies, interception of information other. Later, this classification of crimes was amended by the 2001 Cybercrime Convention [11].

Since 1991, in order to coordinate the activities of law enforcement agencies, these crimes have been identified according to the classifier of the international criminal police and integrated into the search system, which is automated and accessible to the units of the National Central Bureaux of Interpol in most countries.

Among the international documents that are universal in nature, they distinguish the UN Handbook on the Prevention and Control of Computer-related Crime, adopted in 1995; Ten principles for combating high-tech crime, which were adopted in 1997.

Having studied the experience of foreign countries, it should be noted that the provision of countering cybercrime is entrusted to the existing units of law enforcement agencies, in particular to the police, or, nevertheless, special units are created.

In countries such as Belarus, Austria, Poland, USA, India, Norway, Shvets, Belgium, etc., the creation of special units to combat cybercrime is practiced. The main functions of the work of these departments will be highlighted:

- carrying out operational-search and reconnaissance operations
- constant monitoring to detect crimes, viruses or dangerous software

The European Union has made a lot of efforts to harmonize legislation to combat cybercrime in the territory of the member states. In 2002. The law on computer and computer-related crimes was passed, thanks to which the improvement of legislation and joint cooperation in countering cybercrime among the member states should take place.

In 2013, the European Union's Directive on countering cyber attacks on information systems was adopted.

In 2017, the European Commission adopted a directive against fraud and other financial crimes on the Internet.

The European Union pays special attention to the timely response to cybercrime.

A special action plan has been developed to identify, block and eliminate cyberattacks, as well as eliminate the resulting consequences. This strategy is being implemented by the European Agency for Network and Information Security. It is a structure that detects attacks thanks to a special technical system installed to access servers on subscriber lines. Information about detected cybercrimes is sent to the European Center for Cybercrime Investigation, which in turn, depending on

the type of crime, informs the European Defense Agency or the European Service outside of affairs [12]. That is, the European Union clearly demonstrates a structured approach to investigation and proactive response.

Also, the regulatory legal documents for the legal support of the sphere of cybercrime were destroyed, in particular: Directive No 2000/31 / EC of the European Parliament and of the Council on certain legal aspects of information society services, such as electronic commerce in the internal market, framework decision of the Council of the European Union 2000/41 / JHA on combating fraud and falsification of non-cash means of payment. Considering the experience of Canada, we can single out one of the most important areas of police activity - the fight against telecommuting and computer crimes.

These crimes are handled by a police unit - the Royal Canadian Mounted Police. The unit relies on information from the Canadian Clearing House and works with other countries to do its work. Their work is aimed at investigating and solving crimes related to computers and telecommunications. There is also a section for the protection of information technology, it is engaged in the protection of federal state computer centers, consulting and training personnel to work with the implementation of computer protection, and also helps law enforcement agencies in carrying out crimes in the field of the computer system.

There are 1,285 police departments and 1,180 specialized units in Canada. That is, sufficient staff to conduct quality investigations.

If we take into account the experience of the United States, then the system has a more ramified character. In 2007, the implementation of the Trusted Internet Connections program was launched, thanks to which it was planned to cybersecurity a significant part of the information system of federal authorities and departments.

The main actors in countering cybercrime in the US government system are the National Cybersecurity and Communications Integration Center and the National Communications Coordination Center [13]. Upon detecting a cyberattack at the facilities of federal authorities, security administrators of information systems are immediately warned and work begins to restore federal information systems. The experience of the United States is also interesting, about the work of the National Institute of Science and Technology, which occupies an important place in the fight against these crimes. The main functions of which are the development of methodological recommendations on cyber security and cyber security, as well as the consideration of technical standards for cyber security.

So, having studied the experience of foreign countries, it can be noted that the experience of the European Union and the United States in the development of the sphere of cyber defense is the most useful for Ukraine. First of all, attention should be paid to the structure of the bodies for rapid response and investigation [14].

Due to the rapid spread of cybercrime and the low rate of disclosure of these crimes, it is necessary to implement clear and effective measures to prevent the spread of cybercrime.

The prevention of these crimes is possible by measures that are aimed at reducing the risk of the implementation of crimes and neutralizing the harmful consequences for society. Prevention of the spread of cybercrime should be ensured by a complex of organizational, technical, informational and technical measures [15].

Highlight the measures that must be implemented by law enforcement agencies, especially the Cyber Police Department:

- development of a clear program of action to combat cybercrime;
- carrying out criminal preventive activities;
- strengthening of criminal responsibility for committing crimes;
- carrying out inspections by law enforcement agencies of enterprises engaged in activities directly related to the use of computer technology;
- provision of information services in order to expose the use of illegal software;
- the establishment of a strict system of control over the circulation of specialized technical devices that are prohibited for use in free circulation or are restricted in use;
- continuous professional development of employees of the "cyberpolice";
- participation of workers in this area in international seminars, conferences dedicated to the exploration of problems in this area;
- implementation of government policy in the field of cybercrime prevention;
- introduction of special software for systematization of cyber-incidents;
- informing the public about the emergence of new types of cybercrimes, which will help to reduce the number of victims of cybercrime, since they were not aware of such a possibility of such incidents;
- Amendments to the legislation of Ukraine, especially in terms of such as the legalization of electronic evidence, which is most typical for crimes in this area;
- provision of appropriate professional training of judges, law enforcement agencies with powers, which include investigation and consideration of crimes in this area.

One of the ways to prevent the spread of cybercrime should be the identification of persons who are inclined to commit these crimes or have already committed similar crimes. The classifier of their behavior is overwriting data without the need to change or delete data, make fake records, when there are constant complaints from database users about system delays and errors. Often, the beginning of the commission of crimes is the allegedly typical behavior of the employee, for example, overtime, without objective grounds, the work of the operator.

Necessary aspects of improving preventive activity are:

a) the embodiment of the experience of the bodies of the legal system of foreign countries in this area;

b) active participation in international cooperation in solving crimes;

c) creation of comprehensive means of protection against cyberattacks of the information resources of state power corresponding to modern conditions, because cybercrimes can pose a threat to national security.

Some scholars point out that Ukraine needs to develop an effective strategy to combat cybercrime. The development of this Strategy would be most expedient by the bodies of the Ministry of Internal Affairs and the bodies of the National Police. Its main content should include criminological forecasts, processing information about the tendency of cybercrime, developed strategies of action for the timely identification of these evil-doers and elimination of their consequences.

Based on the above, it should be noted that it is necessary to improve and introduce a mechanism for a significant number of measures that will help reduce the spread of cybercrime.

Conclusions. Cyberspace crime is one of the most dynamic groups of extremely dangerous attacks today.

After analyzing international experience, we see that in Ukraine the law enforcement system in the field of combating cybercrime does not meet modern requirements. To eliminate this deficiency, it is necessary to improve the system of legal bodies, using the experience of developed countries. After all, artificially creating bodies whose specialists do not have the appropriate modern technological devices for the timely detection of crimes cannot give positive dynamics. It is also necessary to immediately improve legislation, since in the virtual space there are already crimes that do not even have an appropriate theoretical classification. Then we generally cannot talk about identifying and investigating these crimes.

Unfortunately, in modern society there is the possibility of developing and distributing information weapons, which can lead to cyber terrorism and information warfare. And the consequences of such an information war are unpredictable.

For Ukraine at this stage, the most typical manifestations of cybercrime in such areas as banking, credit and financial.

The tendency to counteract this type of crime in our country has been not positive for a long time. First of all, there is a lack of a modernized legislative framework and passivity on the part of the government. Previously, due attention was not paid to this area at all.

The modern world is increasingly moving into a virtual space, convenient for public life, and, accordingly, a cyberspace is created with the data of both one person and the data of multimillion-dollar companies that keep their information in electronic databases.

This topic is imperfectly studied in the scientific literature, therefore, it requires constant updating and improvement.

The relevance of this study lies in the absence of a structured system of measures of pro-military bodies, and a corresponding system of law enforcement agencies with a clear delineation of powers for the early identification and mitigation of the consequences of crimes in cyberspace. Therefore, conducting research on the schemes and methods of committing crimes in this area is especially important.

With the development of the information society, cybercrime also appears as an integral component. Therefore, in order to improve the public safety of the state, it is necessary to immediately begin work on improving the sphere of countering cybercrime.

References:

1. OON stavyt kyberprestupnost v odyn riad s mezhdunarodnym terroryzmom [OUN puts cybercrime on a par with international terrorism]. URL: http://www.ifap.ru/pr/2005 /050427b.htm (date of the beast 10.04.2021)

2. Zakon Ukrainy «Pro natsionalnu bezpeku» № 2469-VIII vid 21 chervnia 2018 roku [Law of Ukraine "About National Security" № 2469-VIII of June 21, 2018]. URL : https://zakon.rada.gov.ua/laws/show/2469-19#Text (date of the beast 17.04.2021).

3. V. Markov Statystychne doslidzhennia pokaznykiv kiberzlochynnosti: metodolohichnyi aspekt [Statistical study of cybercrime indicators: methodological aspect] Pravo i bezpeka [Law and Security]. 2013. № 2. P. 136-140.

4. Problemy Ukrainskoho suspilstva: kiberzlochynnist [Problems of Ukrainian society: cybercrime]. Materialy VII rehionalnoi mizhvuzivskoi studenskoi naukovo-praktychnoi konferentsii [Proceedings of the VII regional interuniversity student scientific-practical conference.]. Rivne, 2017. P. 56-62. URL: http://progrdak.16mb.com/wpcontent/uploads/2017/04/kiberzlochunu.pdf. (date of the beast 11.03.2021).

5. Vitvytskyi V. V. Kryminolohichni aspekty zapobihannia rozpovsiudzhenniu dytiachoi ponohrafii zasobamy Internetu. Borotba z internet zlochynnistiu : materialy mizhnar. nauk.-prakt. konf. (Donetsk, 12–13 cherv. 2013 r.). [Criminological aspects of preventing the spread of child pornography through the Internet. The fight against cybercrime: materials intern. scientific-practical conf., Donetsk, June, 12–13, 2013).. Donetsk : Donets. yuryd. in-t, 2013. p. 70-73.

6. Kravtsova M. O., Lytvynov O. M. Zapobihannia kiberzlochynnosti v Ukraini : monohrafiia [Prevention of cybercrime in Ukraine: monography]. Kharkiv : Panov, 2016. 212 p.

7. Burda S. Ya., Yosypiv A.O.Okremi pytannia kryminalnoi vidpovidalnosti za posiahannia u sferi informatsiinoi bezpeky Protydiia kiberzlochynnosti v finansovo-bankivskii sferi : materialy Vseukr. nauk.-prakt. konf. [Some issues of criminal liability for encroachment in the field of information security Countering cybercrime in the financial and banking sector: materials All-Ukrainian. scientific-practical conf], Kharkiv, 23 kvit. 2013.

8. Batiuk O. V. Kryminalno-pravova kharakterystyka obiekta zlochyniv u sferi kompiuternoi informatsii. Aktualni pytannia reformuvannia pravovoi systemy Ukrainy. [Criminal and legal characteristics of the object of crimes in the field of computer information. Current issues of reforming the legal system of Ukraine.] Lutsk, 2008. p. 428-431.

9. Kryminalnyi protsesualnyi kodeks Ukrainy : zakon Ukrainy № 4651-VI vid 13 kvitnia 2012 roku [Criminal Procedure Code of Ukraine : Law of Ukraine of 13 April, 2012]. URL : https://zakon.rada.gov.ua/laws/show/4651-17#Text. (date of the beast 28.04.2021).

10. Zynyna U. V. Mezhdunarodnoe sotrudnychestvo v sfere borby s kompiuternymy prestuplenyiamy. Pravo i bezopasnost. [International cooperation in the field of combating computer crimes. Law and security] 2005. №3. URL: http://www.dpr.ru/pravo_16_19.htm. (date of the beast 2.04.2021).

11. Konventsiia pro kiberzlochynnist : mizhnarodnyi dokument vid 23.11.2001 [Convention on Cybercrime: International Document of 23.11.2001]. URL: http://zakon.rada.gov.ua/laws/show/994_575. (date of the beast 2.05.2021).

12. Lipkan V. A. Maksymenko Yu.A., Zhelikhovskyi V. M. Informatsiina bezpeka Ukrainy v umovakh yevrointehratsii : navch. posib. [Information security of Ukraine in the conditions of European integration: textbook]. Kyiv: KNT, 2006. 280 p. (Seriia: Nats. i mizhnar. bezpeka).

13. Mishchuk N. Kiberzlochynnist yak zahroza informatsiinomu suspilstvu. [Cybercrime as a threat to the information society.] Visnyk Lvivskoho universytetu. Seriia ekonomichna. 2014. Vypusk 51. p. 173-179.

14. Kiikov V. M. Skiminh: shliakhy zapobihannia. Protydiia kiberzlochynnosti v finansovo-bankivskii sferi : materialy Vseukr. nauk.-prakt. konf. [Skimming: ways to prevent countering cybercrime in the financial and banking sector: materials All-Ukrainian. scientific-practical conf.], Kharkiv, 23 kvit. 2013 r. Kharkiv : KhNUVS, 2013. P. 125-128.

15. Zakon Ukrainy «Pro ratyfikatsiiu Konventsii pro kiberzlochynnist vid 7 veresnia 2005 roku. № 2824-IV. [Law of Ukraine "On ratification of the Convention on Cybercrime" № 2824-IV of September 7, 2005]. URL : https://zakon.rada.gov.ua/laws/show/2824-15#Text (date of the beast 27.04.2021).

УДК 35.077.2

Baboi V. S.,
assistant Department of Law,
Faculty of Management and Law
Vinnytsia National Agrarian University
Kovalchuk O. Yu.
4-year student
Department of Law,
Faculty of Management and Law,
Vinnytsia National Agrarian University
DOI: 10.24412/2520-6990-2021-14101-22-29

CURRENT PROBLEMS AND DEVELOPMENT PROSPECTS ELECTRONIC GOVERNANCE IN UKRAINE

Abstract.

The article considers the trends and directions of e-government development of Ukraine and the advantages of its deployment. The main problems that arise at this and subsequent stages of e-government implementation are analyzed. A comparative analysis with the leading countries in this area is done. "Narrow" months of e-government in Ukraine were identified according to the UN E-Government Survey 2018. An assessment of the level of e-government development in public authorities was made. The principle of a "single window" - the Unified State Portal of Administrative Services (poslugy.gov.ua) is considered.

The importance of implementing e-government at the local level is noted. Different approaches to the implementation of e-government at the local level are described, which are outlined in terms of "smart city" (smart city), "e-city" and "e-region". The methodology of the Civil Society Institute for evaluating the websites of local governments is considered. It is determined that the quality of information content and functionality of the website are mandatory and necessary requirements for the development of e-government in Ukraine. The main shortcomings of the official websites of public authorities and local governments and their search engines have been identified. It was found that the priority of e-government development is to complete the transition to electronic document management in the process of document preparation by ministries and interagency cooperation. Indicators of the level of e-government in different countries in accordance with the results of the UN E-Government Survey.

Possible ways to overcome the problematic issues of e-government in Ukraine are identified: improvement of the regulatory framework and systematization of information legislation, expansion and modernization of the existing infrastructure of public authorities, namely computer fleet and structured cable networks.

Keywords*: administrative(management) services; information society; authorities being open; Electric Town; e-government.*

Relevance and formulation of the problem. Development of e-government in Ukraine is one of the most important aspects to improve the country, because it lets you not only to hugely optimize budget expenditures, but also to increase the speed of making manage-