works remains controversial, since creativity has so far been recognized only by man.

Scientists from various fields of science are discussing the possibility and probability of creating artificial intelligence, able to create creative objects in the same way as a person. The solution to such a question is compounded by the lack of a unified understanding of the notion of creativity in the field of jurisprudence and other branches, and the content of the definition. If creativity is understood from the point of view of human consciousness, at least as in copyright law, then in such conditions, machines will never be able to achieve it, regardless of their complexity, skills and abilities.

Skeptics of the possibility of creating strong artificial intelligence quoted Adu Lovelace, the daughter of Lord Byron, who worked with Charles Babbage and in 1843 warned against excessive optimism about the potential of the developed analytical mechanism, and recommended avoiding exaggerated ideas about the possible abilities of this mechanism.

Acknowledging the achievements of substantial progress and technological advances since the speech of A. Lovelace, it has not lost its relevance yet. Despite the fact that today's computers are more powerful than their predecessors in terms of memory and data processing, they still rely on people who set the rules on which they are futile. Just as a photographer makes a photo, standing behind the camera, programmers are behind the development of each software and neural network. According to A. Lovelace, people create rules, and artificial intelligence follows them, only acting within certain limits.

Taking into account the above, given the rapid development of technology, the issue of legal regulation of artificial intelligence and the generation of creative objects by computing technology becomes more relevant and requires further research.

MAZURENKO S. V.

National University «Odesa Law Academy»,
Associate Professor of the Department of Intellectual Property Law and Corporate Law, PhD in Law, Associate Professor

LEGAL PROBLEMS OF SUPPLY OF THE CYBER SECURITY

Key words: *cyber security, cybercrime, cyber threat, cyber defense, Internet, website.*

In the Great Explanatory Dictionary of the Ukrainian Language, the terms «cyber» or «cybernetic» are interpreted as referring to the term «cybernetics», which is created and operates on the basis of the principles and methods of cybernetics. And the term «security» describes a state where someone does not threaten anyone, that is, characterizes the absence

of danger [1]. The basis for the introduction of the term "cyber security" was the understanding of the need to address the problem of neutralizing or minimizing the totality of cyber threats. From the technological point of view, cybersecurity is an integral part of information security, since the nature of threats, methods, means and measures is the same and cybersecurity concerns only cyberspace. From another point of view, the term «Cyber Security» is considered as a separate case of information security, the introduction of which is due to the use of computer systems and networks (KSM) and/or telecommunication networks (TCM). «Cyber Security» as the security of information and infrastructure in the digital environment that it provides involves achieving and maintaining security features in the resources of the organization or users aimed at preventing relevant cyber threats. The analysis of the main factors that adversely affect the functioning of computer systems and networks and/or telecommunication networks has shown that there are a number of factors that cause the risks of cyber threats to their functioning and the need for their protection against cyber attacks [2].

O.A. Baranov suggests, under cybersecurity, a separate case of information security, the appearance of which is due to the use of computer systems and / or telecommunication networks. In an expanded state, the author suggests, under this term, to understand «such a state of protection of vital interests of the individual, society and the state in the use of computer systems and / or telecommunication networks, which minimizes the task of harm to them due to: incompleteness, timelessness and unlikelihood of information that used; negative information influence; negative consequences of the functioning of information technologies; unauthorized distribution, use and violation of the integrity, confidentiality and availability of information» [3].

The importance of the problems of cyber security led to the adoption in Ukraine of the Law «On the Basic Principles for the Cybersecurity of Ukraine», which defines the legal and organizational foundations for ensuring the protection of the vital interests of man and citizen, the society and the state, the national interests of Ukraine in cyberspace, the main goals, directions and principles of state policy. in the field of cyber security, the powers of state bodies, enterprises, institutions, organizations, individuals and citizens in this area, the basic principles of coordination of their activities with Cybersecurity. According to Art. 1 of this law, cybersecurity is understood as the protection of the vital interests of man and citizen, the society and the state during the use of cyberspace, which ensures the sustainable development of the information society and the digital communication environment, timely detection, prevention and neutralization of real and potential threats to the national security of Ukraine in cyberspace [4].

The law also defines terms such as: «cyber threats» – the existing and potentially possible phenomena and factors that pose a threat to the vital national interests of Ukraine in cyberspace, have a negative impact on the state of cybersecurity of the state, cybersecurity and cyber defense of its objects; «cyber defense» – a set of organizational, legal, engineering and

technical measures, as well as measures of cryptographic and technical protection of information aimed at preventing cyber incidents, detecting and protecting against cyber attacks, eliminating their consequences, restoring the sustainability and reliability of the functioning of communication and technological systems; «cybercrime» (computer crime) is a socially dangerous offense in cyberspace and / or its use, liability for which is provided for by the law of Ukraine on criminal liability and / or recognized as a crime by international treaties of Ukraine.

In paragraph 14 of the report of the Committee of the 2nd Tenth United Nations Congress of 2000 on the Prevention of Crime and the Treatment of Offenders, it is noted that there are two categories of information crimes: cybercrime in the narrow sense («computer» crimes) – any unlawful act committed by way of electronic operations, the purpose of which is to overcome the protection of computer systems and data processed by them; cybercrime in the broadest sense (computer-related crime) is any unlawful act committed by or in connection with a computer system or network, including such offenses as unlawful storage, offering or distribution information through computer systems or networks [5].

According to N.M. Dimitrova, in contrast to the traditional types of crimes, whose history includes centuries, such as murder or theft, cybercrime phenomenon is relatively young and new, which arose with the advent of the Internet. The specificity of this type of crime lies in the fact that the preparation and commission of a crime is carried out almost without leaving the «workplace», the crimes are accessible, since computer technology is constantly cheaper, crimes can be committed from anywhere in the world, which settlement, and objects of criminal encroachment may be thousands of miles away from the perpetrator. In addition, it is rather difficult to detect, capture and remove forensic-meaningful information when conducting investigative actions to use it as evidence of material [6].

The main types of cybercrime NM Dimitrov considers: violation of copyright and related rights; fraud; avoidance of taxes, duties (mandatory payments); illegal actions with transfer documents, payment cards and other means of access to bank accounts, equipment for their production; import, manufacture, sale and distribution of pornographic items; illegal collection for the purpose of using or using information constituting commercial or banking secrets.

In general, one can identify the following main features that distinguish cybercrime from other criminal offenses: the commission of such crimes does not require the physical rapprochement of the subject of crime and victim; Thanks to automation, the number of objects of a crime can be measured by thousands, as a result of one criminal act; such crimes are committed «instantaneously», so a quick reaction of the relevant authorities is required; lack of a stable algorithm for committing actions that lead to unlawful consequences, due to insufficient research.

To date, the terminology of cybercrime and crime in the Internet network should not be considered. Scope of Internet crime – the so-called virtual space, which can be defined as computer-simulated informational space, which

contains information about individuals, objects, facts, events, phenomena and processes presented in mathematical, symbolic or any other and are in the process of moving on local and global computer networks, or information stored in the memory of any physical or virtual device, as well as another medium specially designed for their storage, processing and before chi.

The specificity of crime on the Internet is as follows: relative comfort, that is, cooking and committing a crime is carried out practically without leaving the «workplace»; availability – in connection with the tendency of constant decrease of prices for computer equipment; wide geography of crimes, but given the fact that the majority of computers are located in large settlements, it is precisely for them that the «lion's share» of crime; the distance of the object of criminal encroachment – it can be thousands of kilometers from the place of the crime; the complexity of detecting, fixing and extracting forensic-meaningful information (the trace of a crime) in carrying out investigative actions for using it as evidence of evidence, etc., etc .; wide use of criminals of information encryption tools [7].

The main condition for the termination of offenses committed with the use of the Internet is the establishment of the offender. After establishing contact with the offender and obtaining an unlawful offer, the technical capabilities of the network establishes his place of residence and the computer he used.

Thus, the establishment of an attacker's person, after receiving information about the illegal activity on the Internet, is directly related to the installation: the IP address under which the computer worked on the Internet; Internet Service Provider, whose network belongs to the IP address, which used the unlawful implementation of pornographic products; Establishing the location of a personal computer that had access to the Internet at a specified time under the installed IP address.

Thus, the information on the distribution or sale of pornographic items contained on the relevant website is physically located on computer equipment, which, while working on the Internet, uses a universal IP address – an identifier. In addition, a website that hosts similar information, in addition to the IP address, has a web address, an alphanumeric designation called a domain name and also unique to the Internet.

Thus, in recent years, the issue of cyber security has become particularly relevant to Ukraine. The spread of cyber-threats led to the activation of the legislator in this area, which resulted in the adoption of a number of regulations, clarifying terms, forming the system of bodies responsible for such security, increasing the responsibility for cybercrime. Today, cybercrime is to mean a socially dangerous act in cyberspace and/or its use, the responsibility for which is provided for by the law of Ukraine on criminal liability and/or recognized as a crime by international treaties of Ukraine, and under cybersecurity – the protection of vital interests of man and citizen, society and the state during the use of cyberspace, which ensures the sustainable development of the information society and digital communication environment, is timely discovered prevention, and neutralization of real and potential threats to the national security of Ukraine in cyberspace.

References:

1. Бусел В.Т. Великий тлумачний словник сучасної української мови. – К.: ВТФ «Перун», 2003. С. 106, 306.
2. Бистрова Б. Основні поняття дослідження та концептуальні засади професійної підготовки фахівців із кібербезпеки // Педагогічні науки: теорія, історія, інноваційні технології. – 2017. – № 8. – С. 60.
3. Баранов О.А. Про тлумачення та визначення поняття «кібербезпека» // Правова інформатика. – 2014. – № 2. – С. 61.
4. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163 -VIII // Відомості Верховної Ради України. – 2017. – № 45. – Ст. 403.
5. Європіна І.В. види протиправних діянь у сфері новітніх інформаційних технологій // Вісник академії адвокатури України. – 2010. – № 3. – С. 129.
6. Дімітрова Н. М., Н. М. Білик Основні види кіберзлочинів та причини, що їх породжують // Соціально-гуманітарний вісник. – 2018. – Вип. 22. – С. 50.
7. Кіпа О.О. Правопорушення в мережі Інтернет // Часопис Київського університету права. – 2010. – № 4. – С. 347.

NEKIT K. G.

National University «Odesa Law Academy»,
Associate Professor at the Department of Civil Law,
PhD in Law, Associate Professor

THE IMPLEMENTATION OF INFORMATION SECURITY AND PERSONAL DATA PROTECTION IN THE FIELD OF THE INTERNET OF THINGS

Key words: *personal data, European Union, GDPR, software.*

At the end of the twentieth century, the history of humankind was divided into two eras due to the emergence of the Internet. And the speed in the development of technology is gaining so fast, that today, at the beginning of the XXI century, we can talk confidently about a new era in our history – the era of the Internet of things. The number of devices connected to the Internet was 500 million in 2003, by 2010 their number had increased to 12.5 billion, and by 2020, according to various sources, Internet connections from 26 to 50 billion devices are predicted [1]. On the one hand, it opens up tremendous prospects for the development of society, but on the other hand, like any other new phenomenon, it gives rise to a number of issues. There are some issues in the legal sphere as well, because today we have no comprehensive solution regarding the legal regulation of relations in the field of the Internet of Things.

One of the most important issues in the field of the Internet of Things is the issue of personal data protection.

In order to ensure the personal data protection in the European Union, new rules for the processing of personal data were developed and the