CZU 343.7:004.056(477)
DOI https://doi.org/10.52388/2345-1971.2021.e2.11

IMPLEMENTATION OF INTERNATIONAL CYBER SECURITY STANDARDS IN THE NATIONAL LEGISLATION OF UKRAINE

Iulia DERKACHENKO
Doctor of Law, Associate professor,
Higher Educational Institution „Academician Yuriy Bugay International and Scientific Technical University",
Kyiv, Ukraine
e-mail: *derkachenko76@gmail.com*
https://orcid.org/0000-0002-3019-9730

Stanislav KUKHTYK
Doctor of Law, Associate professor,
Higher Educational Institution „Academician Yuriy Bugay International and Scientific Technical University",
Kyiv, Ukraine
e-mail: *stan.kukhtyk@istu.edu.ua*
https://orcid.org/0000-0002-2738-5866

Anna YEMELIANENKO
Doctor of Philosophy, University Professor,
Donbass State Pedagogical University,
Slavyansk, Ukraine
e-mail: *yemelianenkoad@gmail.com*
https://orcid.org/0000-0003-4309-8047

The article is dedicated to the study of the implementation of international norms in the field of cyber security in the national legislation of Ukraine. The information society creates the need to form a new type of intelligence capable of embracing the latest reality of information technology. Technological changes in the 21st century require a change in the unilateral technocratic paradigm. In this context, the topic of the study - the implementation of international standards in the field of cyber security - is relevant. The problems of cyber-attacks are urgent problems for every country in the world through the global digitization of information. These attacks are becoming more frequent. Cybercriminals do not stand still, creating more and more ways to attack and damage cyberspace, improving their viruses and malware. This is especially true for cyber-attacks on the Internet, the consequences of such attacks are unpredictable. Often these consequences are a malfunction of the cyberspace system (internet connection is lost). In the face of external aggression, Ukraine has clear intentions to join Euro-Atlantic and European structures. The multiple threats and dangers are aimed at destabilizing Ukraine. In various countries around the world, the fight against cyber terrorism is the functional responsibility of the intelligence unit and military forces, in order to carry out offensive and defensive actions on the Internet. Cybersecurity issues in the context of global threats lead to the emergence (creation) of new problem-solving mechanisms associated with the invasion of cyberspace on a global scale. The results of the research can be used to further conceptualize the definition of cybersecurity and its impact on Ukrainian law.

Keywords: *cyber security, digitization, cybercrime, cyber sphere, cyber defense, cyber-attack, Internet resource.*

IMPLEMENTAREA NORMELOR INTERNAȚIONALE DE SECURITATE CIBERNETICĂ ÎN LEGISLAȚIA NAȚIONALĂ A UCRAINEI

Articolul este dedicat analizei implementării normelor internaționale în domeniul securității cibernetice în legislația națională a Ucrainei. Societatea informațională creează necesitatea formării unui nou tip de inteligență capabilă să îmbrățișeze cea mai recentă realitate a tehnologiei informației. Schimbările tehnologice din secolul XXI necesită o schimbare a paradigmei tehnocratice unilaterale. În acest context, tema studiului, - implementarea normelor internaționale în domeniul securității cibernetice, - este relevantă. Problemele atacurilor cibernetice sunt actuale pentru fiecare țară din lume prin digitalizarea globală a informațiilor. Aceste atacuri devin din ce în ce mai frecvente. Infractorii cibernetici nu stau pe loc, creând din ce în ce mai multe modalități de a ataca și dăuna spațiul cibernetic, îmbunătățindu-și virușii și programele malware. Acest lucru este valabil mai ales pentru atacurile cibernetice pe Internet. Consecințele unor astfel de atacuri sunt imprevizibile. De cele mai multe ori, aceste consecințe reprezintă o defecțiune a sistemului cyberspațial (conexiunea cu Internetul este pierdută). În condițiile unei agresiuni externe, Ucraina are intenții clare de a se alătura structurilor euroatlantice și europene. Multiplele amenințări și pericole vizează destabilizarea Ucrainei. În diferite țări ale lumii, lupta împotriva terorismului cibernetic este responsabilitatea funcțională a unității de informații și a forțelor militare, cu scopul de a desfășura acțiuni ofensive și defensive pe Internet. Problemele de asigurare a securității cibernetice în contextul amenințărilor globale determină apariția (crearea) de noi mecanisme de soluționare a problemelor asociate cu invazia spațiului cibernetic la scară globală. Rezultatele cercetării pot fi utilizate pentru a conceptualiza în continuare definiția securității cibernetice și impactul acesteia asupra legislației ucrainene.

Cuvinte-cheie: *securitate cibernetică, digitalizare, criminalitate cibernetică, sferă cibernetică, apărare cibernetică, atac cibernetic, resursă Internet.*

MISE EN ŒUVRE DES NORMES INTERNATIONALES DE CYBERSÉCURITÉ DANS LA LÉGISLATION NATIONALE DE L’UKRAINE

L’article est consacré à l’étude de la mise en œuvre des normes internationales dans le domaine de la cybersécurité dans la législation nationale de l’Ukraine. La société de l’information crée le besoin de formation d’un nouveau type d’intelligence capable d’embrasser la dernière réalité des technologies de l’information. Le changement technologique au 21e siècle nécessite un changement de paradigme technocratique unilatéral. Dans ce contexte, le sujet de l’étude, - la mise en œuvre des normes internationales dans le domaine de la cybersécurité, - est pertinent. Les problèmes des cyberattaques sont des problèmes urgents pour tous les pays du monde grâce à la numérisation mondiale de l’information. Ces attaques sont de plus en plus fréquentes. Les cybercriminels ne s’arrêtent pas, créant de plus en plus de moyens d’attaquer et de nuire au cyberespace, améliorant ainsi leurs virus et logiciels malveillants. Cela est particulièrement vrai pour les cyberattaques sur Internet. les conséquences de telles attaques sont imprévisibles. Le plus souvent, ces conséquences sont un dysfonctionnement du système du cyberespace (la connexion à Internet est perdue). Dans des conditions d’agression extérieure, l’Ukraine a clairement l’intention de rejoindre les structures euro-atlantiques et européennes. De multiples menaces et dangers visent à déstabiliser l’Ukraine. Dans différents pays du monde, la lutte contre le cyber-terrorisme relève de la responsabilité fonctionnelle de l’Unité de renseignement et des forces militaires dans le but de mener des actions offensives et défensives sur Internet. Les problèmes de cybersécurité dans le contexte des menaces mondiales déterminent l’émergence (création) de nouveaux mécanismes pour résoudre les problèmes liés à l’invasion du cyberespace à l’échelle mondiale. Les résultats de la recherche peuvent être utilisés pour conceptualiser davantage la définition de la cybersécurité et son impact sur la législation ukrainienne.

Mots-clés: *cybersécurité, digitalisation, cybercriminalité, cyber sphère, cyber défense, cyber attaque, ressource Internet.*

ИМПЛЕМЕНТАЦИЯ МЕЖДУНАРОДНЫХ НОРМ В СФЕРЕ КИБЕРБЕЗОПАСНОСТИ В НАЦИОНАЛЬНОЕ ЗАКОНОДАТЕЛЬСТВО УКРАИНЫ

Статья посвящена исследованию имплементации международных норм в сфере кибербезопасности в национальное законодательство Украины. Информационное общество создает необходимость формирования нового типа интеллекта, способного охватить новейшую информационно-техническую действительность. Технологические сдвиги XXI века обуславливают необходимость смены односторонней технократической парадигмы. В этом контексте, тема исследования имплементации международных норм в сфере кибербезопасности актуальна. Проблемы кибератак и кибернападений – неотложные вопросы для каждой страны мира через глобальную цифровизацию информации. Количество подобных атак со временем увеличивается. Киберпреступники не стоят на месте, создавая все новые и новые способы совершения нападения и нанесения вреда киберпространству, совершенствуя свои вирусы и вредоносные ПО. Особенно это касается кибердаров по сети Интернет. Результаты таких нападений непредсказуемы. Чаще всего, последствиями нападений становится сбой в системе киберпространства (теряется связь с сетью Интернет). В условиях противостояния внешней агрессии, Украина имеет четкие намерения вступить в евроатлантические и европейские структуры. Количество и качество угроз и опасностей направлены на дестабилизацию Украины. В разных странах мира борьба с кибертерроризмом – функциональные обязанности подразделений информационно-военных сил, имеющих целью проведение наступательных и оборонительных действий в сети Интернет. Проблемы обеспечения кибербезопасности в контексте глобальных угроз обуславливают появление (создание) новых механизмов решения проблем глобального масштаба, связанных с вторжением в киберпространство. Результаты исследования могут быть использованы в дальнейшей концептуализации определения кибербезопасности и ее влияния на законодательство Украины.

Ключевые слова: *кибербезопасность, цифровизация, киберпреступления, киберсфера, кибербезопасность, кибератака, Интернет-ресурс.*

Introduction

The legislation of Ukraine in the field of cybersecurity is developing, first of all, through the European integration aspirations of Ukraine, the development of legal regulation of e-commerce within the WTO.

Technological progress does not stand still, so cyberspace is now a new and no less important territory, for leadership in which states around the world are trying to take measures to ensure their own interests, national benefits. At the same time, cyberspace attracts international terrorist groups, transnational organized criminals who want to benefit from stealing information and interfering with the functioning of national systems.

Unfortunately, there is a narrow list of international legal acts that could regulate the relations of subjects of international law in cyberspace.

The principles of cooperation between states within the framework of cyberspace were laid down in 1998 by the Resolution of the UN General Assembly UNGA 53/70. The rapid development of technologies that can be applied in the civil and military fields, allows them to be used for incompatible processes between different countries. It should be noted that now it is necessary to take more and more effective modern measures for safe and stable work in the digital space. Only such a policy on the part of different countries of the world can have a positive impact on the sustainable development of the economy.

The UNGA resolution helps member states to cooperate in considering possible threats to information security, hacker threats. It defines the main concepts that affect the sphere of information security. Each country, in order to increase the level of cybersecurity at

the global level, should inform the Secretary General of the advisability of developing and implementing international principles. Such measures will contribute to the fight against information terrorism and crime [12]. Such actions entail a trend towards the annual presentation of proposals from different states, the preparation by the General Assembly of resolutions on the achievements of digitalization, the telecommunications sector, taking into account international security trends.

The UN General Assembly during 2000-2001 prepared two Resolutions numbered 55/63 and 56/121. They directly relate to the issues of combating the criminal use of information technology. These Resolutions allow states to exchange information, resources of professionals capable of implementing norms that affect the effective fight against the criminal use of information technologies. They help to achieve cooperation on equal terms between the investigating authorities of different states [13].

Resolution 57/239 of 2003 “Creating a global culture of cybersecurity” the UN General Assembly notes the importance of using modern digitalization opportunities (information telecommunication systems) for social development in different countries. It emphasizes that national governments, business activities, the functioning of public organizations and individual users of the Internet must have a clear understanding of the possible risks. Awareness of possible cybercrimes and hacker attacks allows you to take all measures that increase the overall level of electronic information security. Therefore, the Assembly proposes elements that would influence the creation of a global culture of cybersecurity [14].

Research methodology. The article used a comparative historical method, as well as methods developed within the framework of legal phenomenology and hermeneutics. The basic method was a comprehensive systematic approach to the analysis of the problems of the internal legislation of Ukraine. Descriptive, logical, systematic, historical methods are used as the most suitable for studying the problem in time and its connection with related scientific and practical issues.

Review of scientific literature in the direction of research. The theoretical basis of the article was the works of G.M. Danilenko, G.V. Ignatenko, I.I. Lukashuka, S.Yu. Marochkina, T.N. Neshataeva, A.N. Talalaeva, O.I. Tiunova, G.I. Tunkina, E.T. Usenko and other lawyers, who analyze the implementation of international norms in the field of cybersecurity in the national legislation of Ukraine. When studying this problem, the works of such foreign scientists as Martijn van Empel, Marianne de Jong, Sean Murphy, Frederic Kirgis, César Landa, Julio Ramón Garcia Vilchez, Adam Banaszkiewicz and others were used.

Main ideas of the research

The Council of Europe has adopted the main instrument for ensuring cybersecurity - the 2001 Cybercrime Convention, which has been ratified by 49 countries of the world. This document is also known as the Budapest Convention on Cybercrime [13]. In Ukraine, it entered into force on July 1, 2006 [108]. This international treaty guides the public (Internet users) and the international community to protect themselves in the field of cybercrime.

This document defines a list of terms related to cybercrime, questions of actions that are violations of digital technologies. The Cybercrime Convention defines the procedural aspects that force countries that have ratified the document to take on the following obligations:

– creation of domestic legislation, the purpose of which is to strengthen the procedures contained in the Treaty (search for information, capture and interception of data in electronic form);

– cooperation by providing mutual assistance, even without special agreements (on extradition, access to computer data, etc.);

– investigation and prosecution of cybercrime committed in the territory of a ratifying State.

The Convention has an additional protocol that appeared in 2003. In Ukraine, it entered into force on April 1, 2007. It contains a list of extended cybercrimes: distribution of racist material or xenophobic views on the Internet, threats and insults of xenophobic and racist motives distributed through a computer network [8]. The first document among the EU countries regulating cyberspace is Directive 95/46, adopted by the European Parliament and Council on October 24, 1995. The Directive points out the importance of protecting individuals from criminal theft and processing of personal data, on the free movement of personal information. Member States, based on the Directive, must take measures to protect the fundamental rights and freedoms of individuals (their right to privacy, the processing of personal data) [6].

The European Parliament and the European Union are trying to ensure the maximum level of cybersecurity in the territories of EU member states. For this purpose, the European Agency for Network and Information Security was established in 2004. Article 2 of Regulation No. 460/2004 provides, in a number of other objectives, for the following point - the expansion of the European Union's ability to quickly and effectively respond to modern challenges of cyberspace (to solve information security problems). Also, this agency can perform other important functions:

– providing assistance and advice to the Commission and Member States on issues related to network security, confidentiality of information;

– providing assistance to the Commission in the technical preparatory work to update and develop European Union regulations in the field of network and information security [10]. In 2016, an important document among European states for organizing cooperation in the cyber sphere was signed - the EU Network and Information Security (NIS) Directive [5].

Its goal is to achieve a high overall level of security of network and information systems within the Union. The Directive aims to ensure that Member States cooperate in matters of cyber security in a coordinated manner: adopt appropriate national strategies, create interaction groups to support and facilitate cooperation on strategic issues such as cybersecurity, monitor the exchange of information between Member States. An equally important task set before the EU countries by the Directive is the creation of a rapid response team for computer incidents to develop a level of trust between Member States and ensure the effectiveness of cooperation; establishing security requirements for operators providing digital services, etc.

In 2007, Estonia faced such a serious threat as attacks on the cyberspace of the state. Therefore, in 2008, NATO took important steps to overcome the consequences and prevent such incidents - the decision to establish a Center for Advanced Studies in General Cyber Defense CCD COE (*Cooperative Cyber Defense Center of Excellence*). The activities of the center are focused on coordinating actions to ensure cyber defense and creating policies to assist allies in attacks [15, p. 110].

In particular, Estonia is one of the European leaders in cybersecurity. It is in Tallinn

that the NATO Cyber Defense Center is located. Estonia began to actively develop in the field of cybersecurity, attracting as many resources as possible. In June 2011, the Center for the Development of State Information Systems was modified and became the Department of the State Information System, which is engaged in the development of the state information system, considering it as a single entity. In 2018, the Department examined 9,135 cases of Estonian computer networks, of which 348 had a direct impact on the operation of an important administrative service or page [39].

The EU has a unique opportunity to invest in enhancing cooperation, ensuring coordination among EU member states, key EU stakeholders in the field of cybersecurity. In 2016, the European Commission signed a private partnership agreement with the European Cyber Security Organization (ECSO). This move resulted in the structuring and coordination of industrial digital security resources in Europe.

The partnership includes a wide range of participants, including: manufacturers of equipment, components; operators of basic services, research institutes united under the auspices of ECSO. The European Union has committed to invest about 450 million euros in this partnership [39].

Today, the EU has a problem with the lack of qualified specialists (information and communication technology workers, especially experts in the field of cybersecurity). European Union budget proposals for the period 2021-2027 contain an emphasis on the development of digital skills in the field of cybersecurity.

The European Commission has invested more than 63.5 million euros in four pilot projects: Four pilots: CONCORDIA; ECHO; SPARTA; Cybersec4 Europe.

They laid the foundation for the creation of a European Network of Cybersecurity Centers of Excellence (helping to strengthen cybersecurity research and coordination in the EU).

The pilot projects aim to contribute to the common post-2020 European Cybersecurity and Innovation Roadmap and the European Cybersecurity Strategy for Industry. They were intended to provide EU assistance in defining and testing management models for the European network of specialists in the field of centers of excellence in the field of cybersecurity [39].

The role of cyberspace is constantly growing due to the introduction of global digitalization in the world. Due to the presence of risks of criminal hacker attacks, many countries create personal national legislative norms and introduce new cybersecurity strategies in order to be able to protect themselves from offenses in cybersecurity.

In 2016, by Decrees of the President of Ukraine No. 96/2016 “On the decision of the National Security and Defense Council of Ukraine” dated January 27, 2016, “On the Cyber Security Strategy of Ukraine”, a national cyber security strategy was approved [1]. In 2009, NATO Headquarters adopted a strategically important document, the Framework for Cooperation on Cyber Defense between NATO and Partner Countries. This act laid the foundation for establishing cooperation in the field of cybersecurity between the participating countries (including with the participation of Ukraine) [2]. Article 3 of Annex XVII (Regulatory Approach to Achieving a Full Internal Market Regime in a Specific Sector) states: “Relying on Articles 114, 124, 133 and 139 contained in Chapter 6 “Establishing a Business, Trade in Services and Electronic Commerce”, Chapters 7 “Current payments and capital flows” of Section

IV of this Agreement and Article 2 (1) of this Annex Ukraine implements and implements on a permanent basis in its national legal system (in accordance with Article 2 (2)) of this Annex the provision of the current EU legislation contained in the Additions" [19].

A fairly common practice in the context of cybercrime is the infliction of damage by computer technologies to military and civilian infrastructure, the provision of negative effects on production processes, and the organization of failures in the functioning of national Internet resources. Therefore, cybersecurity issues are becoming more relevant and acute, becoming urgent for many countries, which they consider to be a problem at the national level.

As a result, security in the world requires the expansion of international legal cooperation between the subjects of international law in order to maintain peace, to prevent the resolution of cyber wars that can run in parallel with kinetic ones (may be accompanied by real military conflicts).

In January 2012, the EU reformed legislation (amending personal data protection issues in order to bring legislation in line with the requirements of the "digital age"), wanting to implement the European Digital Single Market Strategy. As a result, 2 documents were adopted: Directive 2016/680 of the European Parliament and of the Council of the EU of April 27, 2016 "On the protection of individuals with regard to the processing of personal data by competent authorities for the purpose of preventing, investigating, detecting or prosecuting criminal offenses or executing criminal penalties" and " On the free movement of such data, as well as repealing Council Framework Decision 2008/977, repealing Directive 95/46/EC (General Data Protection Regulation (GDPR)" [20].

The Strategy and Agenda were published in the spring of 2015. Already in July 2016, the European Commission presented "Additional measures to promote the development of the cyber defense industry". On July 6, 2016, the EU Directive on measures to ensure a high overall level of security of network and information systems throughout the European Union (DIRECTIVE (EU) 2016/1148 - NISDirective) was adopted. The Directive contains uniform rules that allow each EU member state to exercise the right to independently take its own measures to implement the norms of this Directive into national legislation [21]. The purpose of the Directive is to ensure a high level of network and information security in the EU. To achieve this goal, it is necessary to take measures immediately in 3 directions:

– *increasing by each member country at the national level the capacity of the cybersecurity system;*

– *increasing the level of cooperation between the EU countries;*

– *introduction of a risk management system, the obligation of member governments to notify basic web service operators (digital service providers) of all cyber incidents.*

For further success in the development of regulation in the field of cybersecurity at the legislative level, there is Council Directive 2008/114 / EC of December 8, 2008, which identifies and defines critical infrastructures in Europe, conducts an assessment analysis to develop the necessary measures to improve their protection and protection. It is important to understand the need to take into account the provisions of this document when developing a national regulatory act, as well as local acts of business entities.

Of particular note are the Cross-Cutting Criteria for EQI Evaluation defined in Directive 2008/114/EC (refer to paragraph 1). They consist of the following criteria:

– *accident criterion - an assessment of the potential number of deaths or injuries received by employees;*

– *criterion of economic results - analysis of the significance of economic costs and / or deterioration of products, services provided, including potential consequences for the environment;*

– *criterion of public consequences - assessment of the impact on public confidence, physical suffering, disruption of everyday life (including the failure to provide citizens with basic services).*

Cross-cutting criteria have limiting values, the establishment of which is directly influenced by consideration of the severity of the consequences caused by damage or destruction of a particular infrastructure. Member States are responsible for the accuracy of the endpoints of the cross-cutting criteria (they differ for certain critical infrastructures). Each case is considered separately.

Each EU Member State informs the Commission annually of the number of infrastructures in each sector for which the discussion and determination of the limit values of the cross-cutting criteria took place. Sectoral criteria should take into account other indicators - the characteristics of individual sectors of a single critical infrastructure (hereinafter - ECI).

In doing so, each Member State should verify the existence of an Operator Security Plan (OSP) or similar instruments that are intended to address issues in each specific ECI located on its territory.

In Ukraine, the initial stage of creating a legislative regulation of cyber defense is currently underway. However, the most difficult stage has already been passed, and Ukraine is moving according to the planned strategy of the state policy to ensure cyber defense.

Of course, ahead in Ukraine is the need to overcome many challenges, to consider and solve problems of cyber defense. Currently, the organization of public-private interaction remains an urgent unresolved issue; it is also necessary to form a list of critical infrastructure facilities, as well as develop approaches to cyber defense. For the functioning of the legal regulation in the field of cybersecurity in Ukraine, it is necessary to perform a large amount of work.

Today, an information war is taking place between Russia and Ukraine, which implies not only a real military conflict with losses in the form of casualties, but also the conduct of information and psychological operations to destabilize the civilian population and conduct cyber-attacks. Therefore, an urgent issue for Ukraine is the creation of a clear, understandable and logical Strategy (the formation of a regulatory framework for ensuring cybersecurity).

Conclusions

The legal framework for cybersecurity in Ukraine contains international obligations and elements of national legislation. With regard to international experience, the Budapest Convention and the Directive on Network and Information Security (NIS) should be highlighted.

National legislation should contain the following:

– *obligations that Ukraine must fulfill after signing international agreements and conventions;*

– *especially that Ukraine will have to make commitments if it continues to demonstrate its desire to join the European Union.*

In Ukrainian legislation, problems also arise due to the uncertainty of the issues of distribution of powers between various pu-

blic and private institutions in the field of cyber defense, as well as the lack of legally regulated and financial security of the strategy of public and private partnership, the unresolved large number of procedural issues of the actions of control bodies and law enforcement officers; insufficient attention when considering the problems of general cybersecurity education, awareness raising and capacity building. All these moments significantly increase Ukraine's vulnerability to cyber incidents and cyber-attacks.

Ukraine cannot do without the need for a legislative settlement of the listed problematic issues that negatively affect the transparency of the legislative process, the fruitfulness of cooperation between Ukrainian and international stakeholders, and the promotion of increased trust between them.

In conclusion, we note that cybercrimes are cross-border in nature, using servers and technical platforms from different countries. Currently, there is a need to develop cooperation at the interstate level. While there are attempts to explain their own political hardships, accusations are heard from the Euro-Atlantic side about "Russian interference" with the help of information and communication processes, which will in no way contribute to resolving mature contradictions in the field of cybersecurity. Ukraine, in the case of UN membership, has every chance to become one of the initiators of a large-scale international treaty on the issues of "non-proliferation" of digital information weapons, the fight against cyberterrorism and during espionage by hackers.

In order to improve cybersecurity measures aimed at counteracting cyber terror and cybercrime, it is necessary to study in detail the experience of foreign countries and implement it in Ukraine.

Biliography

1. Выводы и рекомендации по внесению изменений в Закон Украины "Об основах национальной безопасности Украины": аналит. записка Нац. Ин-ту стратегических исследований при Президенте Украины. URL: http://www.niss. gov.ua/articles/1775/ (дата посещения: 10.02.18)

2. Всемирное исследование экономических преступлений и мошенничества 2018: результаты опроса украинских организаций. Вывод мошенничества из тени URL:https://www.pwc.com/ru/ru/survey/2018/pwc-gecs-2018-ukr.pdf (дата посещения: 12.03.19)

3. ГНАТЮК, С. Л. *Актуальные вопросы развития государственно-частного взаимодействия в сфере обеспечения кибербезопасности в Украине*. Аналитическая записка. URL:http://www.niss.gov.ua/content/articles/files/kiberbezpek-d3e61.pdf (дата посещения: 16.11.18).

4. ГНАТЮК, С. Л. *Кибербезопасность в условиях развертывания четвертой промышленной революции (industry 4.0): вызовы и возможности для Украины*. Аналитические материалы. URL:https://www.niss.gov.ua/doslidzhennya/analitichni-материалы/информационные-стратегии/кибербезпека-в-умования-разгортания (дата посещения: 12.01.19).

5. Правительство (ЕС) No.460/2004 of European Parliamentandof the Councilof 10 March2 004 establishing the European Network and Information Security Agency. (2004). Official Journal L077,13/03/2004,0001-0011.

6. Регулировка Международного сообщества электроизвестку. (2012). Материалы Всемирной конференции электропередачи МСЭ, Женева.

7. Стратегическое планирование в сфере государственного управления: концептуальные подходы. Государственное управление и местное самоуправление: сб. наук. пр. Днепропетровск: Изд-во ДРИ НАДУ, 2013. №3(18).

8. Additional Protocol to the Conventionon Cybercrime, concerning the criminalization of act sof racist and xenophobic nature committed via cyber systems, CETS No. 189. (2006). The Councilof Europe.conventions.coe.int.Retrieved-

fromhttp://conventions.coe.int/Treaty/en/Treaties/Html/189.htm.

9. Convention on Cybercrime. (2016). Chart of signature sand ratifications of Treaty 185. Status as of 28.09.2016. Retrieved fromhttps://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=yvTbDHWU.

10. Directive 95/46/E Cof the European Parliamentand of the Council on the Protection of Individuals Personal Data and on Free Movement of Such Data.(1995).OfficialJournaloftheEuropeanCommunities,No.L281/31,24Octo

11. Konventsiyaprokiberzlochynnist'.(2007). Ofitsiynyyvisnyk Ukrayinyvid 10.09.2007, No.65,107.

12. Resolution Adopted by General Assembly 53/70. (1999). Разработки в области информации и телекоммуникации в контексте Международной безопасности. ccdcoe.org. Retrievedfromhttps://ccdcoe.org/sites/default/files/documents/UN-981204-ITIS.pdf

13. Resolution adopted by the General Asembly 55/63.(2001). Combating the criminal misuse of informationtechnologies.ccdcoe.org.Retrievedfromhttps://ccdcoe.org/sites/default/files/documents/UN-001204-Cripdf

14. Resolution Adopted by the General Assembly 57/239. (2003).Creationofaglobalculture ofcybersecurity.ccdcoe.org.Retrievedfromhttps://ccdcoe.org/sites/default/files/documents/UN-021220-CultureOf

15. SCHREIER, Fred. (2015). *On Cyberwarfare.*DCAFHORIZON. Workingpaper No.7.