UR JOURNAL OF HUMANITIES AND SOCIAL SCIENCES
NR 1(6)/2018 ISSN 2543-8379
ARTYKUŁY DOI: 10.15584/johass.2018.1.6

Nataliia Karpchuk[1]

European Union information security practice: a ukrainian prospect

Abstract

Information technologies are developing at a rapid pace, bringing great benefits to mankind, but at the same time provoking huge dangers. Access to personal information, the impact of negative content on children, the modification and stealing of information, damage to information systems, cybercrime, etc. are signs of the use of information and communication technologies to undermine information security. Naturally, both states and organizations develop a number of mechanisms to prevent/overcome destructive information influences.

The purpose of the article is to analyze how the EU experience in the field of information/cybersecurity has been/could be applicable in Ukraine. Since the early 21st century the EU has adopted a number of regulations, has created necessary empowered bodies and has developed strategies to eliminate threats in the information sphere. Legislation of the EU is being constantly improved. EU legal framework regulates access to personal data, public information, counterfeit payment issues, issues of online sexual exploitation of children, protection of classified information, prevention of attacks on information systems, protection of national information infrastructures.

Trying to adapt its legal frameworks to the norms of the EU legislation, Ukraine adopted the law on "Processing personal data", the law on "Access to public information", "the Cybersecurity Strategy of Ukraine", and the law on "Basic principles of providing cybersecurity of Ukraine"; established respective cybersecurity structures, specifically the National Coordination Center for Cyber Security, Cyberpolice, CERT-UA. In the article the author considers some challenges provoked by the mentioned legislation and offers personal ideas concerning the improvement of some cybersecurity aspects in Ukraine.

Key words: cybersecurity, information and communication technologies (ICTs), information systems, personal data, information threats

[1] Dr Nataliia Karpchuk, International Communications and Political Analysis Department, Lesya Ukrainka Eastern European National University, Lutsk, Vynnychenko St. 28/6, e-mail: karpchuknata@gmail.com

Introduction

The notion of “information security” arose with the emergence of the first means of information communications between people when they understood that some of their interests could be damaged by influencing information communications. On the international level the issue of “information security” has been on the agenda since the Russian Federation in 1998 first introduced a draft resolution in the First Committee of the UN General

Assembly. It was recognized that few technologies had been as powerful as information and communication technologies in reshaping economies, societies and international relations; cyberspace touched every aspect of people’s lives; the benefits were huge, but the challenges and threats were enormous as well. Making cyberspace stable and secure can only be achieved through international cooperation.

In numerous scientific investigations the concept of information security is understood as a state, a process, activity, property, function, system of safeguards. Since modern information security is associated with threats and dangers of Information Communication Technologies (ICTs), the term “cybersecurity” has been synonimously used (though Ukrainian academic circles have vigorous disputes as to the differences/similiarities of these terms. In any case, this problem is not relevant to the present article).

However, in the paper we will use the definition offered by the European Union Agency for Network and Information Security (ENISA) as one of possible treatment of information/ cybersecurity: “the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user’s assets. Organization and user’s assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment” (Definition of Cybersecurity).

The whole world is interconnected and interdependent through ICTs; they facilitate the work of different institutions (including the EU) and pose grave threats. In order to prevent/ overcome such threats the EU developed appropriate legislation and strategies, and established the relevant structures. The practice of the EU could be beneficial for Ukraine in its attempt to regulate the sphere of information/ cybersecurity.

EU Legislation on Information Security

“Regulation (EC) No 45/2001 on the Protection of Individuals with Regard to the Processing of Personal Data by the Community Institutions and Bodies and on the Free Movement of Such Data” (Regulation (EC) No 45/2001) imposes a set of obligations on data controllers within EU institutions and agencies with regard to handling the personal data of employees and other affected data subjects in order to protect the privacy of these data subjects. The Regulation stipulates that EU institutions and bodies are only allowed to collect personal data that serve specified, explicit and legitimate purposes.

“Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents” (Regulation (EC) No 1049/2001) defines the principles, conditions and limits governing the right of access to European Commission, Council and European Parliament documents. The Regulation stipulates that EU documents are to be made accessible to the public in electronic form or through a register.

“Framework Decision on combating fraud and counterfeiting of non-cash means of payment” (2001) (EU cybersecurity initiatives 2017), which defines the fraudulent behaviours that EU States need to consider as punishable criminal offences. The Commission is assessing the need to revise this Framework Decision to cover new forms of money transmissions like virtual currencies and other aspects.

“Commission Decision of 16 August 2006 C (2006) 3602 concerning the security of information systems used by the European Commission” (Commission Decision of 16 August 2006 C) constitutes the main framework document on security measures and organisational guidelines for the protection of the Commission’s information systems and the information processed therein. The Decision primarily covers the use of encryption technologies, responses in the case of security incidents, and the general security capabilities of information systems.

“European Commission Security Standard on Logging and Monitoring” (2010) (EC Information System Security Policy C(2006) 3602) supplements Commission Decision C (2006) 3602 (mentioned above) and provides mandatory instructions for the procedures to be used for logging and monitoring on all ICT systems that are capable of generating information security-related log events, including but not limited to: servers, workstations, portable PCs, other portable computing devices, such as mobile phones and PDAs, storage devices, and network equipment.

"Directive on combating the sexual exploitation of children online and child pornography" (2011), which better addresses new developments in the online environment, such as grooming (offenders posing as children to lure minors for the purpose of sexual abuse) (EU cybersecurity initiatives 2017).

"Council Decision 2013/488/EU on the Security Rules for Protecting EU Classified Information" (Council Decision 2013/488/EU) sets out the basic principles and minimum standards for protecting EU Classified Information (EUCI), including provisions on processing EUCI through ICTs (Robinson 2014: 26).

"A Directive on attacks against information systems" (2013) (Directive 2013/40/EU) the aim of which is to approximate the criminal law of the Member States in the area of attacks against information systems by establishing minimum rules concerning the definition of criminal offences and the relevant sanctions and to improve cooperation between competent authorities, including the police and other specialised law enforcement services of the Member States, as well as the competent specialised Union agencies and bodies, such as Eurojust, Europol and its European Cyber Crime Centre, and the European Network and Information Security Agency (ENISA).

In December 2015, two new pieces of EU legislation were agreed, namely General Data Protection Regulation and Network and Information Security Directive (came into force in 2016). "General Data Protection Regulation" (GDPR*)* represents a profound reform of data protection law in Europe, shifting the balance of power towards the citizen to whom the personal data belongs, away from organisations that collect, analyse and use such data. "Network and Information Security Directive" (NISD) can be regarded as a complementary law to GDPR, designed to create a focus on the protection of IT systems in European critical national infrastructure (CNI) (EU cybersecurity initiatives 2017).

A number of EU strategies, namely "The e-Commission Initiative 2012 – 2015", "EU Cybersecurity Strategy" (2013), "European Agenda on Security 2015 – 2020", "Digital Single Market Strategy" (2015), "Communication: Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry" (2016) were aimed at increasing the EU cyber resilience and developing the industrial and technological resources for cybersecurity (EU cybersecurity initiatives 2017).

EU Cybersecurity and Privacy Organisations

Directorate-General for Informatics (DIGIT) has a mission to enable the European Commission to effectively and efficiently use ICTs in the course of achieving its organisational and political objectives. Since 2011, DIGIT has been host to a permanent Computer Emergency Response Team (CERT-EU), which is supervised by the Director-General of DIGIT and steered by a group chaired by the Council. CERT-EU's task is to support EU institutions and agencies in their fight against cyber threats. Towards this end, CERT-EU engages in information sharing, threat assessment and awareness-raising activities (CERT - EU). The DIGIT Security Operations Centre (SOC) is managed by a Local Information Security Officer (LISO) who also acts as an advisor to the Information Security Steering Committee. The LISO analyses the security requirements of DIGIT's ICT systems and proposes policies that govern the ICT systems in line with the latter's needs (Robinson 2014:16).

In 2010, the General Secretariat of the Council of the EU launched the Network Defence Centre (NDC) (Network Defence). Its objective is to strengthen the protection of EU sensitive and classified Communication and Information Systems against all forms of technical attacks, including Advanced Persistent Threats, through the development of the capability to detect and respond to security incidents.

The core task of the European Agency for the operational management of large-scale IT systems (1 December 2012) is to ensure the uninterrupted exchange of data between national authorities. However, the Agency is also responsible for adopting and implementing security plans to prevent the unauthorised reading, copying, modification or deletion of personal data during transfers of personal data or transport of data media (Robinson 2014:16).

A European Data Protection Supervisor (EDPS) as well as an Assistant Supervisor and an institutionally independent supporting structure were established in January 2004. The EDPS's mission is to ensure that EU institutions and agencies respect individuals' fundamental rights and freedoms, specifically their right to privacy, when processing personal data or developing new policies (Robinson 2014: 17).

The European Union Agency for Network and Information Security (ENISA) was set up in 2004 to contribute to the overall goal of ensuring a high level of network and information security within the EU. ENISA helps the Commission, the Member States and the business community to address, respond and especially to prevent NIS problems. The main activities run by ENISA include collecting and analysing data on security incidents in Europe and emerging risks; promoting risk assessment and risk management methods to enhance capability to deal with information security threats; running of pan-European cyber exercises; supporting Computer Emergency Response Teams (CERTs) cooperation in the Member States; awareness-raising and cooperation between different actors in the information security field (ENISA). In order to boost the overall level of online security in Europe, each October the agency organises the Cybersecurity Month awareness campaign, with the support of NIS contact points in all Member States.

The Europol's Cybercrime Centre was set up in 2013 as integral part of Europol and has become a focal point in combatting and preventing cross-border cybercrime by serving as the central hub for criminal information and intelligence; supporting Member States' operations and investigations by means of operational analysis, coordination and expertise; providing strategic analysis products; reaching out to cybercrime related law enforcement services, private sector, academia and other non-law enforcement partners (such as internet security companies, the financial sector, computer emergency response teams) to enhance cooperation amongst them, etc. (EU cybersecurity initiatives 2017).

Ukraine' Information Security Experience in the Context of its European Integration

Since the days of EuroMaidan and the annexation of the Crimea, Russia has used cyber attacks as part of its hybrid war against our state. Various special units of the security structures attacked the state information resources and the personal data of individual politicians and public figures. The most known cases of such actions are DDoS attacks on government resources (the Ministry of Foreign Affairs, the site of the President of Ukraine, sites of the security and defence sector), targeted attacks on state agencies through fraudulent e-mails, attempts to disrupt the work of the Central Election Commission during the presidential elections and parliamentary elections of 2014, as well as the functioning of the Uroboros virus, which, with high probability, is identified as Russian. It had all the signs of using the cyber-skirmish campaign against Ukraine, and the web-resources of public authorities (including law enforcement agencies), the media, financial institutions, and large industrial enterprises fell under the influence of the virus.

In the opinion of ESET researchers, the BlackEnergy virus was deliberately targeted against Ukraine aimed at collecting data from hard disks of affected computers, taking screen shots of users, intercepting data entry and much more (ESET Finds Connection 2016). It is estimated that state organizations, business structures and the industrial sector were affected. In addition, the KosmicDuke virus (modification of the Miniduke virus, the purpose of which is theft of information) was used against Ukrainian institutions. There exists data proving the use of FireEye virus for espionage upon Ukrainian officials. Besides there are a number of indirect cyber attacks using social networks with their thousands of "fake" accounts for spreading false information about events in the state and provoking unrest, as well as more traditional attacks with the help of social engineering (Horbulin 2015).

Russian intelligence services used the power of some of Ukraine's largest mobile operators to listen to Ukrainian subscribers' phones, identify their location, and receive all the necessary data concerning the users. This information is used in a variety of ways: from the implementation of psychological pressure and the use of the data obtained to guide the artillery of the aggressor in positions of Ukrainian military in the NATO zone.

June 27, 2017 is known as the "black Tuesday" for the cyber security of our country. Within a day, the computer virus "Ransom: Win32/Petya" attacked the private and public sectors of the Ukrainian economy, in particular banks, airports, state railway companies, television and telecommunication companies, large supermarkets, energy companies, state fiscal services, state authorities and local government, etc. The virus also infected private and state actors of other countries, but experts in this area agree that Ukraine has suffered the most (Грабовий 2017).

Since Ukraine has officially declared its course to European integration, it is to bring its legal frameworks in accordance with the EU standards. The EU experience in the sphere of cybersecurity is quite positive. In Ukraine some steps have already been taken and some are expected to be implemented.

Until recently, the development of the cyber security sector in Ukraine was rather specific, and sometimes fragmented. The respective norms have been dispersed in a number of different laws and regulations; even the legal (not academic) definition of the term has not been properly elaborated. However, there is the law on state secret (1994), and the law on processing personal data (it coincides with the provisions of the EU "Regulation (EC) No 45/2001 on the Protection of Individuals with Regard to the Processing of Personal Data by the Community Institutions and Bodies and on the Free Movement of Such Data") and the law on access to public information (it contains similar provisions as "Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents") were adopted in 2013. However, the law on processing personal data seems to have a lot of gaps as there are cases of unauthorized usage of private information.

In order to solve this problem to author's opinion, in Ukraine it is necessary to establish the position like the EU European Data Protection Supervisor with the same powers and rights, namely: the right to: give advice to data subjects in the exercise of their rights; make proposals for improving the protection of data subjects; order that requests to exercise certain rights in relation to data be complied with; order the rectification, blocking, erasure or destruction of all personal data that have been processed in breach of the provisions governing the processing of personal data; impose a temporary or definitive ban on the processing of personal data; intervene in actions brought before the Court of Justice.

Since 2011, many attempts have been made to solve the regulation issue at the legislative level, mainly within the framework of the relevant law of Ukraine. The necessity of such a law was regularly discussed at the National Security and Defense Council meetings, but there were still no particular developments in this issue. One of the reasons was the interagency controversies and the difficulty in finding a compromise between government structures. Each institution does not want to give way to its interests and powers, believing that it should become a "key" structure. Often, this discussion was reduced to the need to create a completely new state structure that would deal with the issues of cybersecurity.

On March 16, 2016 the President P. Poroshenko approved "the Cyber security Strategy of Ukraine" (Президент затвердив Стратегію 2016). In the draft discussions the experts and authors claimed to have taken into account the EU strategies on cyber security issues. The Strategy includes a set of measures, priorities and directions for the provision of cybersecurity in Ukraine, in particular, the creation and operational adaptation of the state policy aimed at developing cyberspace and achieving compatibility with relevant EU and NATO standards, forming a competitive environment in the field of electronic communications, providing information security and cybernetic services protection. In addition, the Strategy provides for 1) the involvement of expert potential of scientific institutions, professional and public associations in the preparation of draft conceptual documents in this area; 2) increase of digital literacy of citizens and culture of behavior safety in cyberspace; 3) development of international cooperation and support of international initiatives in the field of cyber security, including deepening Ukraine’s cooperation with the EU and NATO.

In June 2016 the National Coordination Center for Cyber Security was created (its functions remind the respective functions of the EU DIGIT). The main tasks of the Center include the analysis of the condition of cybersecurity; monitoring of the national cybersecurity system; control of the readiness of the subjects concerning providing cybersecurity and counteracting cyber threats; analysis of national legislation fulfillment in the sphere of cyber defense of state electronic information resources and information; collection of data on cyber incidents in relation to state information, etc. (Президент затвердив Положення 2016).

It is necessary to mention that a Cyberpolice as a structural unit of the National Police was created a year before, on October 5, 2015 with the purpose to reform and develop the units of the Ministry of Internal Affairs of Ukraine, to ensure the training and functioning of highly qualified specialists in the expert, operational and investigative units of the police engaged in the fight against cybercrime and capable of applying the latest technology in operational and service activities at the highest professional level. The main tasks of Cyber police are to implement state policy in the field of combating cybercrime; to early inform the population about the emergence of the latest cybercrime; to use software tools for the systematization and analysis of information on cyber incidents, cyber threats and cybercrime; to respond to inquiries of foreign partners received by channels of the National round-the-clock network of contact points; to participate in the training of police officers concerning the use of computer technologies in counteracting crime; to take part in international operations and co-operation in real time; to counteract cybercrime, specifically in the area of using payment systems etc. The Devepopment Strategy claimes the application of methodology elaborated by Europol (Cyberpolice).

On October 5, 2017 the law on “Basic principles of providing cybersecurity of Ukraine” was adopted being based on national legislation and Convention on cybersecurity. Coordination of activities in the sphere of cybersecurity as a component of national security of Ukraine is carried out by the President of Ukraine through the Council of National Security and Defense of Ukraine headed by him. The National Cybersecurity Coordination Center, as the working body of the National Security and Defense Council of Ukraine, coordinates and monitors the activity of the security and defense sector, which provides cybersecurity, makes proposals to the President of Ukraine on the formation and refinement of the Cybersecurity Strategy of Ukraine. The Cabinet of Ministers of Ukraine shall ensure the formation and implementation of state policy in the field of cybersecurity, protection of human and civil rights and freedoms, national interests of Ukraine in cyberspace, fight against cybercrime; organizes and provides the necessary forces, instruments and resources for the functioning of the national cybersecurity system; establishes requirements and ensures the functioning of the information security audit system at the objects of critical infrastructure (Про основні засади забезпечення кібербезпеки України, 2017).

The Law underlines that the functioning of the national cybersecurity system is provided by development and operational adaptation of the state policy on cybersecurity aimed at developing cyberspace, achieving compatibility with the relevant standards of the European Union and NATO; deepening Ukraine's cooperation with the European Union and NATO in order to strengthen Ukraine's cyber security capacity, participating in confidence-building measures in the use of cyberspace, held under the auspices of the Organization for Security and Cooperation in Europe.

Governmental Response Team for Computer Emergencies of Ukraine CERT-UA, established under the support of the ENISA, is responsible for the accumulation and analysis of data on cyber incidents, keeping the state register of cyber incidents; providing owners of cyber defense objects with practical help in preventing, detecting and eliminating the effects of cyber incidents on these objects; organizing and conducting practical seminars on cyber defense issues for subjects of the national system of cybersecurity and owners of objects of cyber defense; preparing and publishing on its official website recommendations on the counteraction to modern types of cyber attacks and cyber threats; interaction with law enforcement agencies, ensuring their timely information on cyber attacks etc. (CERT – EU).

In spite of general positive perception of the law, it contains a number of provisions that may create conditions for abuse in the future and will provide the government with the tools the officials might use to put pressure on businessmen and at the same time it could hinder raising the level of cybersecurity of Ukraine to the corresponding world level. The law does not define a single body, which carries out operational command of the subjects of cybersecurity in peacetime. The National Security and Defense Council of Ukraine, and the President carry out only coordination and strategic management. Ministry of Defense of Ukraine and General Staff of the Armed Forces of Ukraine perform operational management in the relevant period. In practice, cyber attack and cyber warfare are never declared or stopped. Some experts are concerned about the power of the Security Service of Ukraine (granted by the Law) which has the right to carry out secret inspections of cybersecurity of all objects of critical infrastructure. This, in essence, gives the Service the right to attack a private business (Грабовий 2017).

The EU supports its IT professionals. Ukraine as well is not lagging behind in the sphere of IT specialists' education as in this state annually several thousands of IT professionals graduate from Universities, the level of training of many is consistent with the world standards. Ukrainian IT specialists have the ability to work quickly and efficiently and posses a high motivation to confront external aggression. Ukrainian engineers and programmers create fully competitive software and hardware products that can be used to enhance the cybersecurity of the state. However, the biggest problem is financing. Unfortunately, the state does not offer salaries of the world standard to the highly qualitative specialists. As the result, we face the outflow of brains.

In the condition of a hybrid warfare, the state must rely not only on defensive, but also on offensive technologies, including – cybersecurity. The rival should know that, trying to use cyberspace to the detriment of Ukraine's national interests, he may face a large-scale cyber response. This proposal obviously contradicts all peacekeeping measures being taken at the global level with the demilitarization of cyberspace, but we can no longer pretend that we do not notice reality in this area, replacing it with ineffective talks. We are asking our Western partners for conventional weapon assistance being able to create cyber weapons on our own.

One of the latest coordination steps between Ukraine and the EU was taken on March 12, 2018 when President of Ukraine P. Poroshenko agreed with the High Representative of the EU on Foreign Affairs and Security Policy - Vice President of the European Commission F. Mogherini to strengthen cooperation in combating fake news and cyber attacks (Порошенко і Могеріні домовилися 2018).

Conclusion

The European Union has developed a powerful base for counteracting the threats and challenges that have been provoked by the widespread use of ICTs in all areas of society's life. Information technologies are improving, the negative influences also become more "sophisticated", but the EU is constantly improving its regulatory framework as well, creating new structures for counteracting information threats, trying not only to eliminate dangers, but to prevent them. It should be noted that the EU pays great attention to the protection of the personal data of ordinary citizens, to combating fraud and to the development of security standards.

Having suffered from cyber attacks, being under the influence of hybrid warfare, Ukraine developed some cybersecurity and related legislation, established some cybersecurity structures following the EU experience. However, we are at the beginning of the process, so Ukraine is sure to need the EU assistance in this activity, specifically in the field of cyber defense skills and capabilities development; cyber security policy, legislation and strategy development; and material and technical assistance.

Literature

CERT – EU, https://www.enisa.europa.eu/topics/csirts-in-europe/capacity-building /european-initiatives/cert-eu (access: 06.01.2018).

Commission Decision of 16 August 2006 C (2006) 3602 concerning the security of information systems used by the European Commission, http://ec.europa.eu/ internal_market/imi-net/docs/decision_3602_2006_en.pdf (access: 07.01.2018).

Communication: Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry, https://ec.europa.eu/digital-single-market/en/news/communication-strenghtening-europes-cyber-resilience-system-and-fostering-competitive-and (access: 07.01.2018).

Council Decision 2013/488/EU on the Security Rules for Protecting EU Classified Information, https://publications.europa.eu/en/publication-detail/-/publication/d43-001e3-356d-11e3-806a-01aa75ed71a1/ language-en (access: 06.01.2018).

Cyberpolice, https://cyberpolice.gov.ua/ (access: 07.01.2018).

Cybersecurity Strategy of Ukraine, 2016, https://www.thegfce.com/news/news/2017/ 05/31/cybersecurity-in-ukraine (access: 06.01.2018).

Definition of Cybersecurity – Gaps and overlaps in standardization, December 2015, https://www.enisa.europa.eu/publications/definition-of-cybersecurity (access: 07.01. 2018).

Developments in the field of information and telecommunications in the context of international security, https://www.un.org/disarmament/topics/informationsecurity/ (access: 06.01.2018).

Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri= CELEX: 32013L0040& from=EN (access: 07.01.2018).

ESET Finds Connection Between Cyber Espionage and Electricity Outage in Ukraine, January 3, 2016, https://www.eset.com/int/about/newsroom/press-releases/research /eset-finds-connection-between-cyber-espionage-and-electricity-outage-in-ukraine/ (access: 17.03.2018).

EU cybersecurity initiatives: working towards a more secure online environment, January 2017, http://ec.europa.eu/information_society/newsroom/image/document/ 2017 (access: 07.01.2018).

European Agenda on Security 2015–2020, https://ec.europa.eu/home-affairs/what-we-do/policies/european-agenda-security_en (access: 07.01.2018).

European Commission Information System Security Policy C(2006) 3602, Standard on Logging and Monitoring, https://www.eba.europa.eu/documents/10180/21209/7--Annex-2---logging_monitoring_standard.pdf (access: 07.01.2018).

European Union Agency for Network and Information Security (ENISA), https://europa.eu/european-union/about-eu/agencies/enisa_en (access: 07.01.2018).

Network Defence Operational Centre of the General Secretariat of the Council of the European Union, https://www.trusted-introducer.org/directory/teams/gsc-ndc-oc.html (access: 07.01.2018).

New European cyber laws GDPR and NISD, https://www.cgi-group.co.uk/systems-integration-services/cyber-security/nisdandgdpr (access: 07.01.2018).

Regulation (EC) No 45/2001 on the Protection of Individuals with Regard to the Processing of Personal Data by the Community Institutions and Bodies and on the Free Movement of Such Data, http://eur-lex.europa.eu/legal-content/EN/TXT/ PDF/?uri= CELEX:32001R0045&from=EN (access: 06.01.2018).

Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents, http://www.europarl.europa.eu/RegData/PDF/r1049_en.pdf (access: 06.01.2018).

Robinson N., Gaspers J., 2014, *Information Security and Data Protection Legal and Policy Frameworks Applicable to European Union Institutions and Agencies,* https://www.rand.org/pubs/research_reports/RR557.html (access: 06.01.2018).

Горбулін В., 2015, *У пошуках асиметричних відповідей: кіберпростір у гібридній війні,* https://dt.ua/internal/u-poshukah-asimetrichnih-vidpovidey-kiberprostir-u-gibridniy-viyni.html (access: 16.03.2018).

Грабовий А., 2017, *Закон про кібербезпеку та стратегія кібербезпеки України,* http://uz.ligazakon.ua/ua/magazine_article/EA010553 (access: 16.03.2018).

Закон України «*Про основні засади забезпечення кібербезпеки України*», 2017, http://zakon2.rada.gov.ua/laws/show/2163-19 (access: 16.03.2018).

Порошенко і Могеріні домовилися посилити боротьбу з рейковими новинами, 2018, https://www.ukrinform.ua/rubric-polytics/2419794-porosenko-i-mogerini-domovilis -posiliti-borotbu-z-fejkovimi-novinami.html (access: 16.03.2018).

*Президент затвердив Положення про Національний координаційний центр кібербезпеки***,** 2016, http://www.president.gov.ua/news/prezident-zatverdiv-polozhennya-pro-nacionalnij-koordinacijn-37329

Президент затвердив Стратегію кібербезпеки України, 2016, https://dt.ua/POLITICS/prezident-zatverdiv-strategiyu-kiberbezpeki-ukrayini-202619_.html (access: 16.03.2018).

Działalność Unii Europejskiej w dziedzinie bezpieczeństwa informacyjnego: ukraińska perspektywa

Streszczenie

Informacyjne technologie rozwijają się w bardzo szybkim tempie, co przynosi wiele korzyści dla ludzkości, lecz jednocześnie prowokuje ogromne niebezpieczeństwo. Dostęp do osobistej informacji, wpływ negatywnych treści na dzieci, sabotaż i wykradanie informacji, uszkodzenia informacyjnych systemów, cyberprzestępczość i tym podobne – oto oznaki użycia informacyjnych i komunikacyjnych technologii dla zniszczenia informacyjnego bezpieczeństwa. Naturalnie zarówno państwa, jak i organizacje opracowują szereg mechanizmów zapobiegania i przezwyciężenia destruktywnych informacyjnych wpływów.

Celem artykułu jest przeanalizowanie, w jaki sposób doświadczenie UE w zakresie informacyjnego cyberbezpieczeństwa może być zastosowane w Ukrainie. Na początku XXI stulecia UE opracowała szereg normatywnych reguł, stworzyła konieczne organy i uruchomiła strategie zorientowane na usunięcie zagrożeń w sferze informacyjnej. Ustawodawstwo UE stale jest doskonalone. Prawna baza UE reguluje dostęp do osobistych danych, społeczną informację, problemy podrabiania spłat, problemy seksualnej eksploatacji dzieci w Internecie, ochronę informacji niejawnych, zapobieganie atakom na informacyjne systemy, obronę narodowych informacyjnych infrastruktur.

Próbując adaptować swoje prawne ramy do norm ustawodawstwa UE, Ukraina uchwaliła ustawę „O obróbce osobistych danych”, ustawę „O dostępie do publicznej informacji”, „Strategię cyberbezpieczeństwa Ukrainy” i prawo „O głównych zasadach zabezpieczenia cyberbezpieczeństwa Ukrainy”; stworzono odpowiednie struktury cyberbezpieczeństwa, w szczególności Narodowe Koordynacyjne Centrum do spraw Cyberbezpieczeństwa, cyberpolicję, CERT-UA.

W artykule rozpatrzono niektóre problemy związane z wymienionym ustawodawstwem i zaproponowano pomysły na polepszanie aspektów cyberbezpieczeństwa na Ukrainie.

Słowa kluczowe: cyberbezpieczeństwo, technologie informacyjne i komunikacyjne, systemy informacyjne, dane osobowe, zagrożenia informacyjne