# WIELOWYMIAROWOŚĆ CYBERBEZPIECZEŃSTWA

pod redakcją
Justyny Żylińskiej, Katarzyny Huczek
i Krzysztofa Borkowskiego

Ministerstwo Nauki i Szkolnictwa Wyższego
Doskonała Nauka
UTH UCZELNIA TECHNICZNO-HANDLOWA im. H. Chodkowskiej w Warszawie

# WIELOWYMIAROWOŚĆ CYBERBEZPIECZEŃSTWA

pod redakcją
Justyny Żylińskiej, Katarzyny Huczek
i Krzysztofa Borkowskiego

**Recenzenci**
dr hab. Mirosław Bednarski, prof. UTH
dr inż. hab. Piotr Wróblewski, prof. UTH
dr inż. Stanisław Krysiński, prof. UTH
dr inż. Ireneusz Fura
dr Tomasz Pajewski
dr Sylwia Skubisz-Ślusarczyk
dr Waldemar Szymański
dr Andrzej Woźniak

**ISBN: 978-83-62250-66-0**
**Wydanie II poprawione i uzupełnione**



**Korekta językowa**
A PROPOS Serwis Wydawniczy Anna Sikorska-Michalak
Bogumił Sieczkowski

**Opracowanie redakcyjne**
Dorota Czernek

**Projekt okładki, skład i łamanie**
Graph-Sign Zuzanna Sandomierska-Moroz

**Grafika na okładce**
Adobe Stock

**Adres wydawcy**
Uczelnia Techniczno-Handlowa im. Heleny Chodkowskiej
ul. Jutrzenki 135, 02-231 Warszawa
tel.: +48 22 262 88 00
www.uth.edu.pl

*Projekt dofinansowany ze środków budżetu państwa, przyznanych przez Ministra Nauki i Szkolnictwa Wyższego w ramach Programu „Doskonała Nauka II”*

Ministerstwo Nauki i Szkolnictwa Wyższego
Doskonała Nauka
UTH UCZELNIA TECHNICZNO-HANDLOWA im. H. Chodkowskiej w Warszawie

# SPIS TREŚCI

WSTĘP ... 11

## CZŁOWIEK A CYBERZAGROŻENIA

**Katarzyna Huczek**
JEDNOSTKA WOBEC CYBERZAGROŻEŃ. PYTANIE O PODMIOTOWOŚĆ CZŁOWIEKA W CYBERŚWIECIE ... 15

**Monika Nowikowska**
TOŻSAMOŚĆ CYFROWA W INTERNECIE – WYZWANIA I ZAGROŻENIA ... 25

**Julia Zorya, Yevhen Kachkar, Marcin Anszczak**
KSZTAŁTOWANIE OSOBOWOŚCI W ZAKRESIEUMIEJĘTNOŚCI KORZYSTANIA Z MEDIÓW: INNOWACYJNE PODEJŚCIE DO CYBERBEZPIECZEŃSTWA W ŚRODOWISKU EDUKACYJNYM ... 39

**Jolanta Grębowiec-Baffoni**
PEDOFILIA I PORNOGRAFIA W INTERNECIE I ICH KONSEKWENCJE W RZECZYWISTOŚCI ... 48

**Nataliya Zagorodna, Ruslan Kozak, Mykola Mytnyk, Taras Lobur**
ANALIZA ZAGROŻEŃ CYBERBEZPIECZEŃSTWA W ŚRODOWISKU OGÓLNOKSZTAŁCĄCEGO SZKOLNICTWA ŚREDNIEGO W UKRAINIE ... 68

**Aleksandra Studzińska**
NIBY WYEDUKOWANI, A JEDNAK NADAL NAIWNI ... 80

## TOŻSAMOŚĆ I SZTUCZNA INTELIGENCJA

**Maria Parlińska, Baiba Rivza, Peteris Rivza, Iveta Leitlante**
MATEMATYKA, SZTUCZNA INTELIGENCJA I CYBERBEZPIECZEŃSTWO ... 97

**Sławomir Cisowski**
IDENTYFIKACJA W PRAKTYCE – ELEMENT ANALOGOWY W CYBERBEZPIECZEŃSTWIE ... 107

**Krzysztof Konopka**
CYBERBEZPIECZEŃSTWO A DOKUMENTY PUBLICZNE ..... 116

**Kamil Szczepaniuk**
TECHNIKI STEGANOGRAFII OBRAZU: PRZEGLĄD ..... 133

**Tomasz Śmiałowski**
SZTUCZNA INTELIGENCJA W CYBERBEZPIECZEŃSTWIE ..... 143

**Kazimierz J. Pawelec**
INFORMACJE ZAWARTE W SYSTEMACH WSPOMAGAJĄCYCH KIERUJĄCEGO I POJAZDACH AUTONOMICZNYCH ORAZ MOŻLIWOŚCI ICH PROCESOWEGO WYKORZYSTANIA W SYSTEMIE CYBERBEZPIECZEŃSTWA. UDOGODNIENIA ORAZ ZAGROŻENIA ..... 157

## CYBERBEZPIECZEŃSTWO DANYCH

**Pietro Pavone, Francesco Zappia**
PRZYSZŁE TRENDY W BEZPIECZEŃSTWIE DUŻYCH ZBIORÓW DANYCH: PERSPEKTYWA ZARZĄDZANIA PUBLICZNEGO ..... 177

**Mariusz Gorustowicz, Andrzej Woźniak**
BEZPIECZEŃSTWO DANYCH NA URZĄDZENIACH MOBILNYCH ..... 187

**Dominika Liszkowska**
CYFRYZACJA PROCESU WYBORCZEGO W POLSCE I JEJ WPŁYW NA BEZPIECZEŃSTWO WYBORÓW PARLAMENTARNYCH W 2023 ROKU ..... 197

**Marta Stanisławska, Anna Kasperowicz, Robert Piechota**
BEZPIECZEŃSTWO FINANSOWE W DOBIE CYBERZAGROŻEŃ: WZROST LICZBY INCYDENTÓW PHISHINGU PODATKOWEGO W POLSCE ..... 210

**Agnieszka Zwolenik**
CYFRYZACJA W DOBIE OBCIĄŻEŃ FISKALNYCH – WYKORZYSTANIE NARZĘDZI INFORMATYCZNYCH W ROZLICZENIACH Z INSTYTUCJAMI PUBLICZNYMI ..... 223

**Taras Lechachenko, Volodymyr Hutsaylyuk, Bogdan Kovalyuk, Mykhailo Blavitskyi, Yuriy Skorenkyy, Liudmyla Moroz**
WIELOKRYTERIALNA ANALIZA ZAGROŻEŃ CYBERBEZPIECZEŃSTWA I DZIAŁAŃ MITYGUJĄCYCH DLA PRZEDSIĘBIORSTW PRZEMYSŁU 4.0 ..... 237

**Sylwia Szybowska**
ŚRODKI ZARZĄDZANIA RYZYKIEM W CYBERBEZPIECZEŃSTWIE W POLITYCE BEZPIECZEŃSTWA ICT I WYZWANIACH PRAWNYCH ..... 252

**Paweł Romaniuk**
WYBRANE AKSJOMATY OCHRONY INFORMACJI W STRUKTURZE BEZPIECZEŃSTWA PAŃSTWA ..... 268

**Sebastian Jarzębowski, Mykola Melnyk**
ESKALACJA CYBERWOJNY: ANALIZA ROLI CYBERATAKÓW W KONFLIKCIE W UKRAINIE I IMPLIKACJE DLA GLOBALNEGO BEZPIECZEŃSTWA. WPŁYW NA GOSPODARKĘ ..... 282

**Volodymyr Hutsaylyuk, Valeriy Lazaryuk, mgr Mykhailo Blavitskyi**
STAN CYBERBEZPIECZEŃSTWA UKRAINY W OBLICZU KONFLIKTU ZBROJNEGO: WYZWANIA I PERSPEKTYWY OCHRONY ..... 297

**Mykola Karchevskyi, Taras Sozanskyi, Vasyl Franchuk**
GŁÓWNE PROBLEMY PRAWNOKARNEJ OCHRONY BEZPIECZEŃSTWA INFORMACJI W UKRAINIE ..... 311

**Viktoriia Shpiliarevych**
MIEJSCE I ROLA CYBERBEZPIECZEŃSTWA W SYSTEMIE ZAPEWNIENIA BEZPIECZEŃSTWA NARODOWEGO UKRAINY ..... 339

# CONTENTS

## HUMAN AND CYBER THREAT

**Katarzyna Huczek**
THE INDIVIDUAL IN THE FACE OF CYBER THREATS.
THE QUESTION OF HUMAN SUBJECTIVITY IN THE CYBER WORLD ..... 15

**Monika Nowikowska**
DIGITAL IDENTITY ON THE INTERNET – CHALLENGES AND THREATS ..... 25

**Julia Zorya, Yevhen Kachkar, Marcin Anszczak**
FORMATION OF A MEDIA LITERACY PERSONALITY:
AN INNOVATIVE APPROACH TO CYBERSECURITY
IN THE EDUCATIONAL ENVIRONMENT ..... 39

**Jolanta Grębowiec-Baffoni**
PEDOPHILIA AND PORNOGRAPHY ON THE INTERNET
AND THEIR CONSEQUENCES IN REALITY ..... 48

**Nataliya Zagorodna, Ruslan Kozak, Mykola Mytnyk, Taras Lobur**
THE ANALYSIS OF THE CYBERSECURITY THREATS
IN THE GENERAL SECONDARY EDUCATION ENVIRONMENT
IN UKRAINE ..... 68

**Aleksandra Studzińska**
PRESUMABLY EDUCATED, BUT STILL NAIVE ..... 80

## IDENTITY AND ARTIFICIAL INTELLIGENCE

**Maria Parlińska, Baiba Rivza, Peteris Rivza, Iveta Leitlante**
MATHEMATICS, ARTIFICIAL INTELLIGENCE AND CYBERSECURITY ..... 97

**Sławomir Cisowski**
IDENTIFICATION IN PRACTICE – AN ANALOG ELEMENT
IN CYBERSECURITY ..... 107

**Krzysztof Konopka**
CYBERSECURITY AND PUBLIC DOCUMENTS ..... 116

**Kamil Szczepaniuk**
IMAGE STEGANOGRAPHY TECHNIQUES: AN OVERVIEW ..... 133

**Tomasz Śmiałowski**
ARTIFICIAL INTELLIGENCE IN CYBERSECURITY ..... 143

**Kazimierz J. Pawelec**
INFORMATION CONTAINED IN DRIVER ASSISTANCE SYSTEMS AND AUTONOMOUS VEHICLES AND THE POSSIBILITIES OF THEIR PROCESS USE IN THE CYBERSECURITY SYSTEM. AMENITIES AND THREATS ..... 157

## DATA CYBERSECURITY

**Pietro Pavone, Francesco Zappia**
FUTURE TRENDS IN BIG DATA SECURITY: A PUBLIC GOVERNANCE PERSPECTIVE ..... 177

**Mariusz Gorustowicz, Andrzej Woźniak**
DATA SECURITY ON MOBILE DEVICES ..... 187

**Dominika Liszkowska**
DIGITIZATION OF THE ELECTORAL PROCESS IN POLAND AND ITS IMPACT ON THE SECURITY OF THE 2023 PARLIAMENTARY ELECTIONS ..... 197

**Marta Stanisławska, Anna Kasperowicz, Robert Piechota**
FINANCIAL SECURITY IN THE AGE OF CYBER THREATS: THE RISE OF TAX PHISHING INCIDENTS IN POLAND ..... 210

**Agnieszka Zwolenik**
DIGITIZATION IN THE ERA OF FISCAL BURDENS – THE USE OF IT TOOLS IN SETTLEMENTS WITH PUBLIC INSTITUTIONS ..... 223

**Taras Lechachenko, Volodymyr Hutsaylyuk, Bogdan Kovalyuk Mykhailo Blavitskyi, Yuriy Skorenkyy, Liudmyla Moroz**
MULTI-CRITERION ANALYSIS OF CYBERSECURITY RISKS AND MITIGATION ACTIONS FOR INDUSTRY 4.0 ENTERPRISE ..... 237

**Sylwia Szybowska**
CYBERSECURITY RISK MANAGEMENT MEASURES IN ICT SECURITY POLICY AND LEGAL CHALLENGES ..... 252

**Paweł Romaniuk**
SELECTED AXIOMS OF INFORMATION PROTECTION IN THE STATE SECURITY STRUCTURE ..... 268

**Sebastian Jarzębowski, Mykola Melnyk**
CYBER WARFARE ESCALATION: ANALYZING THE ROLE OF CYBER ATTACKS IN THE UKRAINE CONFLICT AND IMPLICATIONS FOR GLOBAL CYBERSECURITY. ECONOMIC IMPACT ..... 282

**Volodymyr Hutsaylyuk, Valeriy Lazaryuk, Mykhailo Blavitskyi**
THE STATE OF UKRAINE'S CYBERSECURITY IN THE FACE OF ARMED CONFLICT: CHALLENGES AND PROSPECTS FOR PROTECTION ..... 297

**Mykola Karchevskyi, Taras Sozanskyi, Prof. Vasyl Franchuk**
THE MAIN PROBLEMS OF CRIMINAL LAW PROTECTION OF INFORMATION SECURITY IN UKRAINE ..... 311

**Viktoriia Shpiliarevych**
THE PLACE AND ROLE OF CYBERSECURITY IN THE SYSTEM OF PROVIDING NATIONAL SECURITY OF UKRAINE ..... 339

**Prof. PhD Viktoriia Shpiliarevych**
Department of Policy in the field of the fight against Crime and Criminal Law,
Vasyl Stefanyk Precarpathian National University, Ukraine
ORCID: 0000-0002-1761-9892

# THE PLACE AND ROLE OF CYBERSECURITY IN THE SYSTEM OF PROVIDING NATIONAL SECURITY OF UKRAINE

# MIEJSCE I ROLA CYBERBEZPIECZEŃSTWA W SYSTEMIE ZAPEWNIENIA BEZPIECZEŃSTWA NARODOWEGO UKRAINY

## STRESZCZENIE

*Zapewnienie bezpieczeństwa narodowego Ukrainy jest jednym z priorytetowych kierunków jej polityki wewnętrznej jako państwa suwerennego, niezależnego, demokratycznego, społecznego i prawnego. Elementem składowym bezpieczeństwa narodowego Ukrainy jest bezpieczeństwo informacyjne Ukrainy, które obejmuje cyberbezpieczeństwo jako ochronę żywotnych interesów człowieka i obywatela, społeczeństwa i państwa podczas korzystania z cyberprzestrzeni, które zapewnia zrównoważony rozwój społeczeństwa informacyjnego i środowiska komunikacji cyfrowej, terminowe wykrywanie, zapobieganie i neutralizowanie rzeczywistych i potencjalnych zagrożeń dla bezpieczeństwa narodowego Ukrainy w cyberprzestrzeni.*

*Na podstawie wyników badań naukowych autorka stwierdziła, że: 1) istniejące potencjalne lub realne zagrożenia cybernetyczne to takie, które stwarzają poważne zagrożenie dla bezpieczeństwa narodowego Ukrainy podczas korzystania z cyberprzestrzeni; 2) zapewnienie bezpieczeństwa narodowego, w tym cyberbezpieczeństwa Ukrainy jako elementu narodowego bezpieczeństwa informacyjnego Ukrainy, zależy od: a) obowiązywania odpowiednich ram prawnych, które dotyczą odpowiedniej sfery regulacyjnej; b) utworzenia/udoskonalania i efektywnego funkcjonowania instytucji narodowych, których działalność ma na celu zapewnienie bezpieczeństwa narodowego Ukrainy jako całości lub jej poszczególnych elementów, w tym cyberbezpieczeństwa Ukrainy; c) rozwoju współpracy międzynarodowej w celu integracji Ukrainy z bezpieczeństwem międzynarodowym (zbiorowym).*

## SUMMARY

*Ensuring the national security of Ukraine is one of the priority directions of its internal policy as a sovereign, independent, democratic, social and legal state. A constituent element of the national security of Ukraine is the information security of Ukraine, which includes cybersecurity as the protection of the vital interests of a person and citizen, society and the state during the use of cyberspace, which ensures the sustainable development of the information society and digital communication environment, timely detection, prevention and neutralization of real and potential threats to the national security of Ukraine in cyberspace.*

*According to the results of the scientific research, the author found that: 1) the existence of potential or real cyber threats are those that pose a serious danger to the national security of Ukraine when using cyberspace; 2) ensuring national security, including and cybersecurity of Ukraine as a component of the national information security of Ukraine depends on: a) the validity of the appropriate regulatory and legal framework, which concerns the relevant sphere of regulation; b) creation/improvement and effective functioning of national institutions whose activities are aimed at ensuring the national security of Ukraine as a whole or its individual components, including and cybersecurity of Ukraine; c) development of international cooperation with the aim of integrating Ukraine into international (collective) security.*

**Słowa kluczowe:** bezpieczeństwo narodowe, bezpieczeństwo informacyjne, cyberbezpieczeństwo.

**Keywords:** national security, informational security, cybersecurity.

According to the provisions of the Basic Law of Ukraine, "Ukraine is a sovereign and independent, democratic, social, legal state (Article 1), in which a person, his life and health, honor and dignity, inviolability and security are recognized as the highest social value (Article 3). Protecting the sovereignty and territorial integrity of Ukraine, ensuring its economic and informational security are the most important functions of the state, the business of the entire Ukrainian people (Article 17)"[1]. These provisions of the Constitution of Ukraine dated June 28, 1996 No. 254к/96-ВР became the legal basis for the formation and implementation by Ukraine of its state policy in the field of national security, that is, ensuring the protection of state sovereignty, territorial integrity, the democratic constitutional system and other national interests of Ukraine (vital important interests of man, society and the state, the

[1] *Конституція України* (*Constitution of Ukraine* dated June 28, 1996, as amended on December 2, 2019. No. 254к/96-ВР), 1996, https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text [access: 10.03.2024].

implementation of which ensures its progressive democratic development, as well as safe living conditions and the well-being of its citizens) from real and potential threats[2]. At the same time, such threats can be different both in nature and in the consequences of impact directly on the relevant components of the national security of Ukraine. In particular, as stated in the National Security Strategy of Ukraine, approved by the Decree of the President of Ukraine dated September 14, 2020 No. 392/2020 On the Decision of the National Security and Defense Council of Ukraine dated September 14, 2020 "On the National Security Strategy of Ukraine", threats to the national security of Ukraine are[3]:

- climate changes and the growth of man-made load on the surrounding natural environment;
- increase in the number and scale of natural and man-made emergencies;
- the strengthening of the negative impact of biological factors on the population, the emergence and spread of both already known and new infectious diseases, which leads to the deterioration of the living environment, the quality of air, drinking water, and food products and, as a whole, negatively affects life and health people;
- rapid technological changes, primarily in energy and biotechnology, developments in the field of artificial intelligence, etc., which fundamentally transform the economy and society as a whole;
- the growth of challenges to transatlantic and European unity, which can cause the escalation of existing and the emergence of new conflicts (a clear example today is the conduct of military operations by the Russian Federation on the territory of Ukraine);
- strengthening international competition with the use of all instruments of national power (political-diplomatic, military, economic, etc.) by the relevant states;
- spread of international crime;
- lack of proper internal state policy, which inhibits the development of Ukraine as a sovereign and independent, democratic, social, legal state, etc.

---

[2] *Про національну безпеку України* (*About the national security of Ukraine*: Law of Ukraine of June 26, 2018. No. 2469-VIII), 2018, https://zakon.rada.gov.ua/laws/show/2469-19#Text [access: 10.03.2024].

[3] *Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року «Про Стратегію національної безпеки України»* (*On the decision of the National Security and Defense Council of Ukraine dated September 14, 2020 "On the National Security Strategy of Ukraine"*: Decree of the President of Ukraine of September 14, 2020. No. 392/2020), 2020, https://zakon.rada.gov.ua/laws/show/392/2020#Text [access: 10.03.2024].

Based on the analysis of the provisions of the Decree of the President of Ukraine dated December 28, 2021 No. 685/2021 On the Decision of the National Security and Defense Council of Ukraine dated October 15, 2021 "On the Information Security Strategy of Ukraine", one of the constituent elements of the national security of Ukraine is the information security of Ukraine, which also includes cybersecurity[4], the legal basis of which is:

1) **The Constitution of Ukraine** dated June 28, 1996 No. 254k/96-VR, which states that "Ukraine is a sovereign and independent, democratic, social, legal state (Article 1). A person, his life and health, honor and dignity, inviolability and security are recognized as the highest social value in Ukraine (Article 3). Protecting the sovereignty and territorial integrity of Ukraine, ensuring its economic and information security are the most important functions of the state, the business of the entire Ukrainian people (Article 17)"[5];

2) **international treaties** whose binding consent has been given by the Verkhovna Rada of Ukraine:
   - Convention on the Protection of Human Rights and Fundamental Freedoms of November 4, 1950 No. 995_004, ratified by the Verkhovna Rada of Ukraine on the basis of the Law of Ukraine "On the Ratification of the Convention on the Protection of Human Rights and Fundamental Freedoms" of 1950, the First Protocol and Protocols Nos. 2, 4, 7 and 11 to the Convention dated July 17, 1997 No. 475/97-BP[6], which enshrines "everyone's right to freedom of expression. This right includes the freedom to adhere to one's views, to receive and transmit information and ideas without interference from state authorities and regardless of borders (Part 1, Article 10)"[7];

[4] *Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки України»* (*About the Decision of the National Security and Defense Council of Ukraine dated October 15, 2021 "About the Information Security Strategy of Ukraine"*: Decree of the President of Ukraine of December 28, 2021. No. 685/2021), 2021, https://zakon.rada.gov.ua/laws/show/685/2021#n5 [access: 10.03.2024].

[5] *Конституція України…*, *op. cit.*

[6] *Про ратифікацію Конвенції про захист прав людини і основоположних свобод 1950 року, Першого протоколу та протоколів № 2, 4, 7 та 11 до Конвенції* (*On the ratification of the 1950 Convention on the Protection of Human Rights and Fundamental Freedoms, the First Protocol and Protocols Nos. 2, 4, 7 and 11 to the Convention:* Law of Ukraine of July 17, 1997. No. 475/97-BP), 1997, https://zakon.rada.gov.ua/laws/show/475/97-%D0%B2%D1%80#Text [access: 10.03.2024].

[7] *Конвенція про захист прав людини і основоположних свобод* (*Convention on the Protection of Human Rights and Fundamental Freedoms*: International document of November 4, 1950. No. 995_004), 1950, https://zakon.rada.gov.ua/laws/show/995_004#Text [access: 10.03.2024].

- Convention on Cybercrime dated November 23, 2001 No. 994_575, ratified by the Verkhovna Rada of Ukraine on the basis of the Law of Ukraine "On the Ratification of the Convention on Cybercrime" dated September 7, 2005 No. 2824-IV[8], which provides for measures to be carried out on the national levels for the purpose of countering cybercrime, namely establishing criminal liability for[9]:
  - Offenses against the confidentiality, integrity and availability of computer data and systems (illegal access to the entire computer system or its part without the right to do so; illegal interception by technical means without the right to do so; transfer of computer data not intended for public use and conducted from, on or within a computer system, including electromagnetic radiation from a computer system containing such computer data; data interference: intentional damage, destruction, deterioration, alteration or concealment of computer information without the right to do so; tampering with the system: intentionally seriously interfering with the functioning of a computer system by entering, transmitting, damaging, destroying, degrading, replacing or concealing computer data without the right to do so; misuse of devices without the right to: manufacture, sell, acquire for use, distribute or otherwise make available for use devices, including computer programs, created or adapted primarily for the purpose of committing any of the crimes listed above, computer passwords, access codes or similar data, with the help of which it is possible to gain access to all or part of a computer system with the intention of using it to commit any of the crimes listed above, as well as possessing the items specified above with the purpose of using them to commit any of the crimes listed above).
  - Computer-related offenses (forgery related to computers, committed intentionally without the right to do so: entering, changing, destroying or concealing computer data that results in the creation of invalid data with the purpose of they would be considered or legally acted upon as valid, whether or not such data can be directly read and understood; computer fraud: intentionally committing, without the right to do so, actions that lead to the loss of another person's property by any input, change, destruction or concealment of computer data or any interference in the

[8] *Про ратифікацію Конвенції про кіберзлочинність* (*On the ratification of the Convention on Cybercrime*: Law of Ukraine of September 7, 2005. No. 2824-IV), 2005, https://zakon.rada.gov.ua/laws/show/2824-15#Text [access: 10.03.2024].

[9] *Конвенція про кіберзлочинність* (*Convention on cybercrime*: International document of November 21, 2001. No. 994_575), 2001, https://zakon.rada.gov.ua/laws/show/994_575 [access: 10.03.2024].

functioning of a computer system with the fraudulent or dishonest purpose of obtaining economic advantages for yourself or another person).
- Offenses related to the content (offenses related to child pornography, in particular, the intentional commission without the right to do so of the following actions: production of child pornography for the purpose of its distribution using computer systems; offering or providing access to child pornography for using computer systems; distribution or transmission of child pornography using computer systems; obtaining child pornography using computer systems for oneself or another person; possession of child pornography in a computer system or on a computer storage medium).
- Offenses related to the violation of copyright and related rights.

3) **other normative legal acts** of Ukraine:
- the Law of Ukraine "On the National Security of Ukraine" of June 26, 2018 No. 2469-VIII, which defines and delimits the powers of state bodies in the spheres of national security and defense, creates a basis for the integration of policies and procedures of state authorities, other state bodies whose functions concern of national security and defense, security forces and defense forces, a system of command, control and coordination of operations of security forces and defense forces is defined, a comprehensive approach to planning in the spheres of national security and defense is introduced, thus ensuring democratic civilian control over the bodies and formations of the security sector and defense[10];
- the Law of Ukraine "On the Basic Principles of Ensuring Cybersecurity of Ukraine" dated October 5, 2017 No. 2163-VIII, which defines the legal and organizational foundations for ensuring the protection of the vital interests of a person and citizen, society and the state, national interests of Ukraine in cyberspace, the main goals, directions and principles of state policy in the field of cybersecurity, powers of state bodies, enterprises, institutions, organizations, individuals and citizens in this area, basic principles of coordination of their activities to ensure cybersecurity[11];

[10] *Про національну безпеку України* (*About the national…*, *op. cit.*

[11] *Про основні засади забезпечення кібербезпеки України* (*About the main principles of ensuring cybersecurity of Ukraine*: Law of Ukraine of October 5, 2017. No. 2163-VIII), 2017, https://zakon.rada.gov.ua/laws/show/2163-19#Text [access: 10.03.2024].

- Decree of the President of Ukraine dated September 14, 2020 No. 392/2020 On the decision of the National Security and Defense Council of Ukraine dated September 14, 2020 "On the National Security Strategy of Ukraine"[12];
- Decree of the President of Ukraine dated August 26, 2021 No. 447/2021 On the decision of the National Security and Defense Council of Ukraine dated May 14, 2021 "On the Cybersecurity Strategy of Ukraine"[13];
- Decree of the President of Ukraine dated December 28, 2021 No. 685/2021 On the Decision of the National Security and Defense Council of Ukraine dated October 15, 2021 "On the Information Security Strategy of Ukraine"[14].

Cybersecurity of Ukraine is the protection of the vital interests of a person and citizen, society and the state during the use of cyberspace, which ensures the sustainable development of the information society and digital communication environment, timely detection, prevention and neutralization of real and potential threats to the national security of Ukraine in cyberspace[15]. That is, if we determine the peculiarities of cybersecurity of Ukraine and its place and role in ensuring national security as one of the priority directions of the internal policy of Ukraine as a sovereign, independent, democratic, social and legal state, then it is worth, first of all, to pay attention to the following:

- cybersecurity of Ukraine is aimed at ensuring the protection of the vital interests of a person and citizen, society and the state precisely during the use of cyberspace, i.e. "the environment (virtual space) that provides opportunities for communication and/or the implementation of social relations, formed as a result of the functioning of compatible (with "united") communication systems and provision of electronic communications using the Internet and/or other global data transmission networks"[16];
- cybersecurity of Ukraine is aimed at:

---

[12] *Про рішення Ради національної безпеки і оборони України від 14 вересня…*, *op.cit.*

[13] *Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України»* (*On the decision of the National Security and Defense Council of Ukraine dated May 14, 2021 "On the Cybersecurity Strategy of Ukraine"*: Decree of the President of Ukraine of August 26, 2021. No. 447/2021), 2021, https://zakon.rada.gov.ua/laws/show/447/2021#Text [access: 10.03.2024].

[14] *Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки України»* (*About the Decision of the National Security and Defense Council of Ukraine dated October 15, 2021 "About the Information Security Strategy of Ukraine"*: Decree of the President of Ukraine of December 28, 2021. No. 685/2021), 2021, https://zakon.rada.gov.ua/laws/show/685/2021#n5 [access: 10.03.2024].

[15] *Про основні засади забезпечення…*, *op. cit.*

[16] *Ibidem*.

– ensuring the sustainable development of the information society and digital communication environment;
– timely detection, prevention and neutralization of real and potential threats to the national security of Ukraine in cyberspace, i.e. cyber threats – "existing and potentially possible phenomena and factors that pose a danger to the vital national interests of Ukraine in cyberspace, have a negative impact on the state of cybersecurity of the state, cybersecurity and cyber protection of its objects"[17].

In particular, as directly stated in the Decree of the President of Ukraine dated August 26, 2021 No. 447/2021 On the decision of the National Security and Defense Council of Ukraine dated May 14, 2021 "On the Cybersecurity Strategy of Ukraine", the following threats to Ukraine's cybersecurity are[18]:

- **war in cyberspace** - increasing the arsenal of offensive cyber weapons, the use of which can cause irreparable, irreversible destructive consequences. We are talking about cyberattacks aimed, first of all, at information and communication systems of state bodies of Ukraine and objects of critical information infrastructure with the aim of disabling them (cyber sabotage), obtaining covert access and control, carrying out intelligence and intelligence-subversive activities, or for the purpose of manipulative influence on the population, interference in election processes and discrediting Ukrainian statehood;
- **cybercrime** - the use of cyberspace to commit crimes against the foundations of national security of Ukraine, as well as criminal offenses related to the legalization of proceeds of crime, human trafficking, illegal handling of weapons, ammunition or explosives, illegal trafficking in narcotic drugs, psychotropic substances, their analogues or precursors and other objects and substances that threaten the life and health of people, etc.;
- **cyberespionage** - cyberattacks related to the theft of information with limited access for political, economic or military purposes (cyberespionage) and the implementation of intelligence and subversive activities against Ukraine;
- **cyber terrorism** - the priority targets of which remain nuclear energy facilities, electricity and water supply, the spheres of electronic communications, financial and banking spheres, air and railway transport, warehouses of strategic types of raw materials, chemical and biological facilities, etc.

[17] *Ibidem.*

[18] *Про рішення Ради національної безпеки і оборони України від 14 травня…, op. cit.*

It should be noted that cyber threats are dynamic phenomena. And this means that they are constantly changing, depending on the appearance of relevant new challenges before the world community in general or Ukraine in particular. In this regard, some of them may recede into the background, while others, on the contrary, become dominant in cyberspace. So, for example, as of today, the cyber threat associated with the spread of the COVID-19 pandemic, which at one time caused a rapid transformation and organization of a significant segment of social relations in remote mode with the wide use of electronic services and information and communication systems, has somewhat receded into the background[19]. Instead, an actual external threat to the cybersecurity of Ukraine is the conduct of hybrid aggression by the Russian Federation against Ukraine in cyberspace, because, as Yu. P. Lisovska points out, the special services of the Russian Federation conduct such information operations that are directly aimed at undermining the national security of Ukraine, its national interests, liquidation of Ukrainian statehood and destruction of Ukrainian identity, provoking manifestations of extremism and panic in society, which weaken and destabilize socio-political and socio-economic conditions in Ukraine[20]. Unpredictable cyber threats for Ukraine remain the rapid development of artificial intelligence technologies and the introduction of 5G communication technology in Ukraine on the basis of a pilot project, the effective and safe functioning of which will significantly depend on the correct operation of the software. And many such examples can be cited.

Thus, summarizing all of the above, the following should be stated:

- the existence of potential or real cyberthreats is such that it poses a serious danger to the national security of Ukraine, as it indicates a probable or actual encroachment on the vital interests of a person and citizen, society and the state during the use of cyberspace;
- ensuring national security, including and cybersecurity of Ukraine as a component of the national information security of Ukraine is one of the main directions of the state policy of Ukraine, the effectiveness of which depends on a number of factors, in particular:
  - the validity of the appropriate regulatory and legal framework, which concerns the relevant sphere of regulation;
  - creation/improvement and proper functioning of national institutions whose activities are aimed at ensuring the national security of Ukraine as a whole or its individual components, including and cybersecurity of Ukraine;

[19] *Про рішення Ради національної безпеки і оборони України від 14 травня…*, *op. cit.*

[20] Yu. P. Lisovska, *Information security of Ukraine*: academic. manual, Kyiv: Condor, 2018, p. 117–118.

– development of international cooperation with the aim of integrating Ukraine into international (collective) security.

All of this together will be able to guarantee the protection of state sovereignty, territorial integrity, democratic constitutional system and other national interests of Ukraine from any real and potential threats. And the absence of cyber threats will testify to the safe functioning of cyberspace, which will provide new opportunities for unimpeded digital transformation of all spheres of public life in Ukraine.

## REFERENCES

**Legal Act**

*Конституція України* (*Constitution of Ukraine* dated June 28, 1996, as amended on December 2, 2019. No. 254к/96-ВР), 1996, https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text.

*Конвенція про захист прав людини і основоположних свобод* (*Convention on the Protection of Human Rights and Fundamental Freedoms*: International document of November 4, 1950. No. 995_004), 1950, https://zakon.rada.gov.ua/laws/show/995_004#Text.

*Конвенція про кіберзлочинність* (*Convention on cybercrime*: International document of November 21, 2001. No. 994_575), 2001, https://zakon.rada.gov.ua/laws/show/994_575.

*Про національну безпеку України* (*About the national security of Ukraine*: Law of Ukraine of June 26, 2018. No. 2469-VIII), 2018, https://zakon.rada.gov.ua/laws/show/2469-19#Text.

*Про основні засади забезпечення кібербезпеки України* (*About the main principles of ensuring cyber security of Ukraine*: Law of Ukraine of October 5, 2017. No. 2163-VIII), 2017, https://zakon.rada.gov.ua/laws/show/2163-19#Text.

*Про ратифікацію Конвенції про захист прав людини і основоположних свобод 1950 року, Першого протоколу та протоколів № 2, 4, 7 та 11 до Конвенції* (*On the ratification of the 1950 Convention on the Protection of Human Rights and Fundamental Freedoms, the First Protocol and Protocols Nos. 2, 4, 7 and 11 to the Convention:* Law of Ukraine of July 17, 1997. No. 475/97-ВР), 1997, https://zakon.rada.gov.ua/laws/show/475/97-%D0%B2%D1%80#Text.

*Про ратифікацію Конвенції про кіберзлочинність* (*On the ratification of the Convention on Cybercrime*: Law of Ukraine of September 7, 2005. No. 2824-IV), 2005, https://zakon.rada.gov.ua/laws/show/2824-15#Text.

*Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року «Про Стратегію національної безпеки України»* (*On the decision of the National*

*Security and Defense Council of Ukraine dated September 14, 2020 "On the National Security Strategy of Ukraine"*: Decree of the President of Ukraine of September 14, 2020. No. 392/2020), 2020, https://zakon.rada.gov.ua/laws/show/392/2020#Text.

*Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України»* (*On the decision of the National Security and Defense Council of Ukraine dated May 14, 2021 "On the Cybersecurity Strategy of Ukraine"*: Decree of the President of Ukraine of August 26, 2021. No. 447/2021), 2021, https://zakon.rada.gov.ua/laws/show/447/2021#Text.

*Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки України»* (*About the Decision of the National Security and Defense Council of Ukraine dated October 15, 2021 "About the Information Security Strategy of Ukraine"*: Decree of the President of Ukraine of December 28, 2021. No. 685/2021), 2021, https://zakon.rada.gov.ua/laws/show/685/2021#n5.

**Literature**

Lisovska Yu. P., Information security of Ukraine: academic. manual, Kyiv, Condor, 2018.

**Uczelnia Techniczno-Handlowa im. Heleny Chodkowskiej**
**ul. Jutrzenki 135, 02-231 Warszawa**
**tel.: +48 22 262 88 00**
**www.uth.edu.pl**