DOI https://doi.org/10.30525/978-9934-26-442-9-9

GUARANTEEING INFORMATION SECURITY DURING CROSS-BORDER COOPERATION OF TERRITORIAL COMMUNITIES, TAKING INTO ACCOUNT THE RISKS OF MARTIAL LAW

Mendzhul M. V., Mulesa O. Yu.

INTRODUCTION

The war in Ukraine showed how information in the modern world can be used as a tool of struggle and is an integral component of the so-called "hybrid wars". At the same time, scientists rightly point out the importance of guaranteeing military security, which is not possible without the support of such a level of defense capability of the state that, on the one hand, can prevent a military conflict, and on the other hand, give an adequate response to a military attack. The above in combination allows to ensure regional and global stability. At the same time, scientists also note those hybrid tools of warfare related to information and information security with the aim of creating "controlled information chaos" with the help of hacker attacks, spreading false information through the mass media.[1] We agree with this approach, moreover, with the help of the Internet, information is instantly disseminated on a globalized scale, and the use of artificial intelligence allows to change, modify and create information that may not correspond to reality and be used for manipulation and disinformation.

Under such conditions, it is extremely important to study both the concept of information security and those tools of the protective mechanism, which would, on the one hand, contribute to the protection of personal data, and on the other hand, be the basis for regional, national and international security. As part of this study, we will dwell on various aspects of the concept of information security, identify threats to it, find out the legal basis for guaranteeing information security, as well as what changes have taken place under martial law, how digitization and protection of information security are taken into account in the case of cross-border cooperation territorial communities.

[1] Смотрич Д.В., Браілко Л. Інформаційна безпека в умовах воєнного стану. Науковий вісник Ужгородського Національного Університету. Серія ПРАВО. 2023. Випуск 77: частина 2. С. 122.

1. The concept of information security and threats to it in the conditions of martial law

In the modern scientific literature of Ukraine, you can find various terms, in particular "information security" and "information-military security", which are considered as an element of national security[2]. In our opinion, it is more correct to use the term "information security", which definitely in the conditions of war requires increased attention and special guarantee tools, as well as prevention of the use of information as a weapon.

Gbur Z. V. believes that "information security is such a state of protection of the state from information that is illegal and hinders the sustainable development of the state," while the scientist adds that ensuring information security is not possible without such basic principles as systematicity, strength, multi-level protection, continuity, prudence[3]. We agree with this approach, as it takes into account that information security directly affects sustainable development. At the same time, the proposed principles of the scientist are not complete, they should definitely be added, such as reliability and verifiability.

Nashinets-Naumova A. Yu. substantiates that information security is such a "set of vital conditions for the functioning of certain subjects (individuals, society, the state) in the information sphere and subjective possibilities of awareness and control (legal, political, informational, scientific, operational and investigative)"[4]. In this approach, it is important to take into account subjects to guarantee information security, as well as control elements. At the same time, the author does not consider communities as important subjects for ensuring information security.

One can also meet the approach that information security should be considered as "a system that unites state authorities that implement their tasks on the basis of the law with the constant control of the judiciary for the purpose of diagnosis, forecasting of information threats and risks that may affect the state of those public interests, which are vital, the implementation of a number of long-term measures that can prevent

[2] Артемов В. Ю., Хорошко В. О., Хохлачова Ю. Є., Погорелов В. В. Інформайційно-воєнна безпека як елемент національної безпеки України. Захист інформації. 2022. Т. 24, № 1. С. 21-29.

[3] Гбур З. В.Основи інформаційної безпеки держави в умовах війни. / The Russian-Ukrainian war (2014–2022): historical, political, cultural-educational, religious, economic, and legal aspects : Scientific monograph. Riga, Latvia : “Baltija Publishing”, 2022. 1421 p. 870 http://baltijapublishing.lv/omp/index.php/bp/catalog/view/237/6325/13361-1

[4] Нашинець-Наумова А.Ю. Інформаційна безпека: питання правового регулювання: монографія / А.Ю. Нашинець-Наумова. – Київ: Видавничий дім «Гельветика», 2017. С. 10

relevant threats, support the readiness to ensure information security"[5]. In general, one should agree with the indicated approach, the only thing it does not take into account local self-government bodies, the public, which play an important role in ensuring information security at various levels.

Shinkarenko I. R. and Shinkarenko I. I. believe that the formation of information security during war is "such a system of political, legal and technical actions of authorized bodies that aim to protect citizens, society and the state", and the development of normative and legal the basis for managing national security should be through the development of relevant legal acts, concepts, strategies and programs, etc.[6]. At the same time, the specified definition did not foresee the peculiarities of the action of the protective mechanism to guarantee information security in the conditions of martial law.

According to Thayer Amro, in the conditions of war, the methods of ensuring information security are important, in particular: cyber security guarantee tools (protection of computer systems against unauthorized access, virus attacks, etc.); ensuring physical security of information; guaranteeing effective public control in the management mechanism; guaranteeing the security of the information space, management of information that is confidential, proper interaction between various state structures, military units and the public, development of the system of public information, mass communication; proper monitoring and analysis of information[7]. All of these components of ensuring information security during wartime are important, but at the same time, the use of artificial intelligence tools to combat disinformation generated by artificial intelligence itself is lacking.

Regarding clear tools for guaranteeing information security, here we agree with the position of Skochilyas-Pavliv O. V., who believes that "only a state approach to solving the problem of protection and protection of information in information systems and telecommunications networks can guarantee the conditions for properly countering the increase threats in the information field, in particular due to the improvement of the information infrastructure at the national level, including electronic mass media, the banking system, communication systems, energy, transport, industry and the

[5] Капля О. М. Правове регулювання інформаційної безпеки громадянина під час дії воєнного стану. Експерт: парадигми юридичних наук і державного управління. 2023. № 6(24). С. 18. https://doi.org/10.32689/2617-9660-2022-6(24)-16-20

[6] Шинкаренко І. Р., Шинкаренко І. І. Інформаційна безпека України в умовах воєнного стану / Сучасні проблеми правового, економічного та соціального розвитку держави: тези доп. XI Міжнар. наук.-практ. конф.(м. Вінниця, 9 груд. 2022 р.). Вінниця, 2022. С. 140.

[7] Амро Т. Взаємозв'язок систем забезпечення інформаційної безпеки та публічного управління в умовах воєнного стану: методи та можливості. Публічне урядування. 2022, № 5 (33). С. 86-87. https://doi.org/10.32689/2617-2224-2022-5(33)-11 86-87

sphere of services, which is constantly supplemented by the Internet, which brings both new opportunities and threats"[8].

In a detailed study of information security, scientists identify the following groups of information and technology threats: 1) information weapons that can affect both the human psyche and the state information and technology infrastructure; 2) use of modern information technologies for the purpose of causing harm (financial fraud, illegal copying of technologies, etc.); 3) through computer systems, the introduction of total control over both human life and the work of public structures and state institutions; 4) the use of information technologies in the political struggle[9]. In our opinion, the specified threats should be supplemented by a fifth one – the use of artificial intelligence to produce disinformation and its maximum distribution via the Internet.

Guaranteeing information security is important at different levels – private (saving information of an individual or a legal entity under private law), at the level of a territorial community, regional, national and international (global) level. Regardless of the level of information security, its basis is compliance with such principles as reliability, availability, guarantee of data integrity, reliable storage, compliance with confidentiality, use and storage exclusively in accordance with regulated regulations.

2. Legal principles of information security at the level of territorial communities

The regional information security policy at the level of individual territorial communities cannot contradict the Information Security Strategy of Ukraine, which was approved even before the full-scale war until 2025[10], and the corresponding Action Plan for its implementation, adopted in March 2023[11].

Despite the fact that the Information Security Strategy of Ukraine was adopted even before the full-scale invasion, a number of its provisions are conceptual and do not require correction, in particular: the understanding of

[8] Скочиляс-Павлів О.В. Сучасні загрози інформаційній безпеці України в умовах правового режиму воєнного стану. Юридичний науковий електронний журнал. 2023. № 9. С. 266.

[9] Свердлов Д.В., Борисенко Т.В. Забезпечення інформаційної безпеки держави в умовах дії правового режиму воєнного стану / Актуальні проблеми превентивної діяльності Національної поліції в умовах воєнного стану : матеріали Всеукр. наук.-практ. семінару (м. Дніпро, 27 квіт. 2022 р.). Дніпро: ДДУВС, 2022. С. 78-80.

[10] Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року "Про Стратегію інформаційної безпеки": Указ Президента України; Стратегія від 28.12.2021 № 685/2021. URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text

[11] Про затвердження плану заходів з реалізації Стратегії інформаційної безпеки на період до 2025 року: Розпорядження Кабінету Міністрів України від 30 березня 2023 р. № 272-р. URL: https://www.kmu.gov.ua/npas/pro-zatverdzhennia-planu-zakhodiv-z-realizatsii-str-a272r

information security as part of national security and, accordingly, that the Strategy should contain goals and objectives, which are aimed at counteracting national security risks, protecting a person's right to information and his personal data; provision of an effective system of protection and countermeasures against harm caused by negative information influences (coordinated releases of unreliable information, destructive propaganda, other information operations, unauthorized dissemination of information, violation of the integrity of information that has limited access); definition of the concepts "information threat", "information measures of state defense", "anti-crisis communications", "crisis communications", "strategic communications", "strategic narrative", "government communications"; highlighting global challenges and threats (increasing number of disinformation campaigns of a global level, recognition of information policy of the Russian Federation as a threat both to Ukraine and to other states; use of social networks as a subject of information influence; insufficient media literacy in combination with the rapid development of digitalization) and national challenges and threats (the informational influence of the Russian Federation on the Ukrainian population, as well as their dominance in the temporarily occupied territories, insufficient opportunities to influence disinformation, the absence of a strategic communication system, improper regulation of information relations, as well as the protection of journalists, an attempt to manipulate influences on issues of European and Euro-Atlantic integration, guaranteeing the availability of information at the community level, lack of media literacy); seven strategic goals were defined (countering disinformation and information attacks, including those of the Russian Federation, which aim to eliminate the independence of Ukraine, violate sovereignty and territorial integrity, promote violence, war, enmity; ensure comprehensive development of Ukrainian culture, affirm Ukrainian civic identity; increase the level media culture, media literacy; to ensure compliance with the right of individuals to collect, store, and distribute information, as well as to protect journalists and their safety, to counter the spread of illegal content; and informational reintegration of those citizens living in the temporarily occupied territories and adjacent to them communities; to create an effective system of strategic communication; to promote the development of information society, cultural dialogues), which include clear measures to achieve; mechanisms for implementing tasks and expected results are defined[12]. Considering that the hybrid war against

[12] Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року "Про Стратегію інформаційної безпеки": Указ Президента України; Стратегія від 28.12.2021 № 685/2021. URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text

Ukraine was launched by Russia many years ago, and the first invasion, military operations and occupation of part of the territory began in 2014, the Information Security Strategy for the period until 2025 contains goals and clear tasks for their implementation, already taking into account aggression from Russian Federation At the same time, it pays little attention to information security at the international level (there are constant disinformation campaigns that harm the national security of Ukraine), as well as the issue of information policy implementation at the local level. Among the problems, the involvement of local media and limited access to the Internet in certain communities is indicated, and the need to establish communication, including with the participation of local self-government bodies, which should also be involved in the strategic communication system, is noted. In our opinion, the next Information Security Strategy should pay more attention to the role of guaranteeing information security at the level of each community, from the implementation of technical solutions to guarantee free access to the Internet, to media and information education of the population, as well as training in the basics of information security for employees of local self-government bodies.

Separately, it is worth dwelling on the provisions of the Action Plan for the Implementation of the Information Security Strategy for the period up to 2025, adopted in March 2023. If the Strategy mentions hybrid war and hybrid threats once, the plan describes steps to prevent hybrid threats already in six points. As for the tasks planned for the implementation of strategic goals at the community level, only the following are indicated: ensuring effective interaction between state and local self-government bodies, civil society institutions both during planning and implementation of information policy; local self-government bodies are entrusted with the responsibility of raising the level of public awareness through briefings and other events; the development of programs to improve the qualifications of public servants of local self-government in information security, including issues of hybrid threats, countering disinformation, manipulative content, as well as strategic communication, organization of appropriate training and some other[13]. Obviously, after the adoption of the new Information Strategy, the plan of measures for its implementation should also be more focused on overcoming information security threats at the level of individual communities.

In addition, in the context of the protection of information on the Internet, it is also worth mentioning the Cybersecurity Strategy of Ukraine, which does not

[13] Про затвердження плану заходів з реалізації Стратегії інформаційної безпеки на період до 2025 року: Розпорядження Кабінету Міністрів України від 30 березня 2023 р. № 272-р. URL: https://www.kmu.gov.ua/npas/pro-zatverdzhennia-planu-zakhodiv-z-realizatsii-str-a272r

even once mention communities and local self-government bodies[14]. Obviously, the specified act also needs to be revised and updated, because the issue of cyber security is key to national security and its guarantee is not possible without the implementation of countermeasures on the ground.

The introduction of a number of changes to the legislation of Ukraine after the full-scale invasion of the Russian Federation into the territory of our state became quite important for minimizing information security risks at the level of territorial communities. Amendments to legal acts became necessary to regulate the limitation of the dissemination of information necessary for the protection of national security and defense, to prevent the leakage of defense and related information, to regulate the technical aspects of information collection for possible future use as evidence, and to bring guilty parties to justice for illegal dissemination of information.

After February 24, 2022, as of April 2024, that is, in two years and two months, the parliament adopted 26 laws on amendments to the Criminal Code of Ukraine [15], the vast majority of norms concerned the strengthening of criminal liability for crimes against national security, as well as those actions that would contribute to the enemy during a full-scale war, in particular, amendments were made to the following articles of the Criminal Code of Ukraine: Art. 43-1 to guarantee combat; Art. 84-1, which provides for exemption from liability for the transfer of a prisoner for exchange; articles 111 and 113 to strengthen responsibility for crimes against national security; Art. 111-1 and Art. 111-2 for the provision and strengthening of criminal liability for collaborative activity; Articles 161 and 435-1; Article 127 to reform approaches to accountability for torture; articles 185-187, 189 and 191 to refer responsibility for looting; to articles 201-1, 201-3, 201-4 on the criminalization of smuggling of certain goods; to Article 201-2 to counter the misuse of humanitarian aid; Articles 336 and 337 regarding the change of liability for evasion of military service; Articles 258-4 and 258-6 regarding increased responsibility for terrorism; Article 263 for the purpose of exemption from responsibility for voluntary surrender of weapons; Art. 270 on strengthening man-made security; Art. 212 with the aim of stimulating the detinization of incomes; Articles 45-48, 69, 74, 75, 79, 81 and 82, 86 and 87, 366-2 regarding criminal offenses related to corruption; Articles 114-2, 161 and 435-1 to increase liability for dissemination of unauthorized or prohibited information; Article 361 on improving countermeasures against cybercrime; to Article 367 for changes

[14] Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України»: Указ Президента України; Стратегія від 26.08.2021 № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#n12

[15] Кримінальний кодекс України від 05.04.2001 № 2341-III. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text

in liability for official negligence; of Chapter II "Final and Transitional Provisions" for the purpose of enabling the participation of civilians in defense, etc. Of the specified changes, in 7 cases changes were made exclusively to the Criminal Code of Ukraine, and in 19 cases, complex legislative changes were adopted that reformed individual institutions, for example, on the issue of military service, or supplemented criminal law, administrative law, and criminal law. – procedural or other norms.

As for the introduced changes, only a number of laws were aimed at protecting information security. For example: Law of Ukraine dated March 3, 2022 No. 2110-IX increased responsibility for the production or distribution of such information products, which are prohibited, namely, it provided for responsibility for inciting regional enmity or hatred (Article 161 of the Criminal Code of Ukraine), as well as for the use of materials, insulting military personnel or their relatives (Article 435-1 of the Criminal Code of Ukraine)[16]; The Law of Ukraine dated March 24, 2022 No. 2149-IX improved responsibility for taking actions on unauthorized interference in the work of information (automated), electronic communication, information and communication system, electronic communication network[17]; Laws of Ukraine dated March 24, 2022 No. 2160-IX and dated April 1, 2022 No. 2178-IX provided for and improved criminal liability in order to prevent unauthorized dissemination of information about the transfer of weapons, the transfer or placement of the Armed Forces of Ukraine or other military formations (114-2 of the Criminal Code of Ukraine)[18,19]. Other acts are indirectly related to information security through increased liability for treason[20], as well as

[16] Про внесення змін до деяких законодавчих актів України щодо посилення кримінальної відповідальності за виготовлення та поширення забороненої інформаційної продукції : Закон України від 03.03.2022 № 2110-IX. URL: https://zakon.rada.gov.ua/laws/show/2110-20#n6

[17] Про внесення змін до Кримінального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану: Закон України від 24.03.2022 № 2149-IX. URL: https://zakon.rada.gov.ua/laws/show/2149-20#n2

[18] Про внесення змін до статті 114-2 Кримінального кодексу України щодо удосконалення відповідальності за несанкціоноване розповсюдження інформації про засоби протидії збройній агресії Російської Федерації: Закон України від 01.04.2022 № 2178-IX. URL: https://zakon.rada.gov.ua/laws/show/2178-20#n2

[19] Про внесення змін до Кримінального та Кримінального процесуального кодексів України щодо забезпечення протидії несанкціонованому поширенню інформації про направлення, переміщення зброї, озброєння та бойових припасів в Україну, рух, переміщення або розміщення Збройних Сил України чи інших утворених відповідно до законів України військових формувань, вчиненому в умовах воєнного або надзвичайного стану: Закон України від 24.03.2022 № 2160-IX. URL: https://zakon.rada.gov.ua/laws/show/2160-20#n6

[20] Про внесення змін до Кримінального кодексу України щодо посилення відповідальності за злочини проти основ національної безпеки України в умовах дії режиму воєнного стану: Закон України від 03.03.2022 № 2113-IX. URL: https://zakon.rada.gov.ua/laws/show/2113-20#n7

collaborative activities[21], as well as protection of information contained in intellectual property objects[22].

Amendments to criminal, administrative, and criminal procedural legislation were primarily intended to introduce strengthened tools to counter the leakage, unauthorized collection, and use of information of value to the protection of national security. Thus, the tools for countering the use of information as a means of hybrid warfare were improved. At first glance, it seems that such tools are national, at the same time, they are also effective for guaranteeing information security at the level of territorial communities.

3. Cross-border cooperation of territorial communities and information security

In the conditions of the implementation of cross-border cooperation projects, it is extremely important to guarantee information security, especially when the participants of such projects are territorial communities. Zakarpattia, Lviv, Chernivtsi, and Ivano-Frankivsk regions are quite actively involved through various entities in the implementation of cross-border cooperation projects. We analyzed projects within the framework of two programs "Hungary-Slovakia-Romania-Ukraine ENPI Cross-border Cooperation Program 2007-2013" and "Hungary-Slovakia-Romania-Ukraine ENI CBC Program 2014-2020". The conducted research showed that within the framework of the program "Hungary-Slovakia-Romania-Ukraine ENPI Cross-border Cooperation Program 2007-2013" 31 projects were supported with the participation of various communities from the Zakarpattia region. The program "Hungary-Slovakia-Romania-Ukraine ENI CBC Program 2014-2020" provided for three rounds of tenders, projects in the last round completed the implementation of projects no later than the fall of 2023. The conducted analysis showed that only four projects were selected in the first round of the program "Hungary-Slovakia-Romania-Ukraine ENI CBC Program 2014-2020", in the second round – 46 projects, in the third competition of the program – 30 supported projects[23].

---

[21] Про внесення змін до Кримінального та Кримінального процесуального кодексів України щодо удосконалення відповідальності за колабораційну діяльність та особливостей застосування запобіжних заходів за вчинення злочинів проти основ національної та громадської безпеки: Закон України від 14.04.2022 № 2198-IX. URL: https://zakon.rada.gov.ua/laws/show/2198-20#n6

[22] Про внесення змін до Кодексу України про адміністративні правопорушення та Кримінального кодексу України щодо відповідальності за порушення авторського права і (або) суміжних прав: Закон України від 01.12.2022 № 2803-IX. URL: https://zakon.rada.gov.ua/laws/show/2803-20#n3

[23] The 3rd Call for Proposals of the Hungary-Slovakia-Romania-Ukraine ENI CBC Programme 2014-2020. URL: https://huskroua-cbc.eu/calls/3rd-call-for-proposals

The analysis of four competitions within the framework of the programs "Hungary-Slovakia-Romania-Ukraine ENPI Cross-border Cooperation Program 2007–2013" and "Hungary-Slovakia-Romania-Ukraine ENI CBC Program 2014–2020" showed a positive trend in increasing the number of implemented successful projects in various communities of the border areas. At the same time, there are no projects that would be implemented exclusively by municipalities, as a rule, even if the municipality of a certain community joins as a partner, other partners include public institutions, higher educational institutions, hospitals, scientific institutions, and communal facilities.

During a meaningful analysis of cross-border cooperation projects, it was found that none of the involved projects dealt with the issue of guaranteeing information security at the level of border territories. At the same time, digitalization processes and the development of information technologies create conditions for proper organizational and technical support for the implementation of cross-border cooperation projects.

First, the COVID-19 pandemic, and then a full-scale war in our country limited the mobility of various project participants (main executors, experts, beneficiaries, etc.). At the same time, it was the Internet, the use of various digital tools, including platforms and services for online collective communication, holding seminars and other events, that made it possible to successfully implement the specified projects. For example, the project "Introduction of new standards and technologies of surgical treatment of diseases of the central nervous system in the cross-border region "NSDNeuro" (budget 763,757.64 euros) involved joint training for neurosurgeons using innovative neuronavigation systems purchased from within the framework of the project, conducting trainings for student and teaching youth, health care specialists, conducting exchange visits, forming new standards of medical care, improving the material and technical base of both project participants (the Department of Neurosurgery of the University of Debrecen and the Regional Clinical Center of Neurosurgery and Neurology in Uzhhorod)[24]. In the project "Energy Recovery from Municipal Solid Waste by Thermal Conversion Technologies in Cross-Border Region", which was carried out by partners from Romania (North University Center of Baia Mare), Ukraine (Ivano-Frankivsk Technical University of Oil and Gas) and Slovakia (Technical University of Košice) from November 1, 2019 to October 31, 2020, specialists were brought together to study the processes of solid household waste management through the thermal treatment method, and a database with waste

[24] Впровадження нових стандартів та технологій хірургічного лікування захворювань центральної нервової системи в транскор-донному регіоні. URL: https://www.uzhnu.edu.ua/uk/cat/projects-nsdneuro

characteristics was created, the software application "Electronic Monitoring Platform" was developed to manage data related to the administration of heat treatment of waste[25].

At the same time, a meaningful analysis showed that no project was aimed at the development of information security in border areas, including both within the framework of cross-border cooperation and as an additional task in the implementation of other goals and tasks. At the same time, the latest digital technologies became tools for the implementation of individual projects (creation of platforms, sites, promotion of events, etc.), and also helped in the organizational aspects of project implementation, first during the COVID-19 pandemic, and later in the war in Ukraine.

CONCLUSIONS

Modern risks caused by possible pandemics, hostilities, and other emergency situations cause, on the one hand, the activation of digitalization and the use of information tools in cross-border cooperation, and on the other hand, they increase the need to guarantee information security during such cooperation.

Information security in cross-border cooperation is an important element of guaranteeing both national and international security. Problems with disinformation, the use of false reports, incorrect or distorted translation of news are not only a violation of the right to information, but can become the basis for hostility and increased tension in the border areas. In view of this, in matters of cross-border cooperation, the guarantee of information security plays an important role.

To build an effective information security system in cross-border cooperation, it is necessary that the security components of the protection system:

– were applied based on the norms of international law, the principle of the rule of law, were oriented towards respect for human rights, as well as the sovereignty and territorial integrity of states;

– proportionally implemented by all subjects and participants of cross-border cooperation, who were responsible for their application;

– included appropriate technical and digital tools for preventing threats to information security and eliminating consequences in the event of their occurrence;

– were focused on the protection of personal data and confidential information, as well as other information with limited access.

[25] Energy recovery from municipal solid waste by thermal conversion technologies in cross-border region. URL: https://huskroua-cbc.eu/projects/financed-projects-database/energy-recovery-from-municipal-solid-waste-by-thermal-conversion-technologies-in-cross-border-region

In addition, it is important to develop a separate international agreement that would regulate the protection of information, the possibility of using various security tools in the implementation of cross-border cooperation. This agreement can be the basis for the development of the Information Security Strategy in cross-border cooperation, taking into account cyber security.

SUMMARY

An analysis of the problems of guaranteeing information security during cross-border cooperation of territorial communities was carried out, taking into account the risks of martial law. The risks of using information as a tool of hybrid wars on the example of a full-scale war in Ukraine are revealed. The concept of information security, the tools of the protective mechanism, which would on the one hand contribute to the protection of personal data, and on the other hand be the basis for regional, national and international security, were analyzed, threats to information security were identified, and the existing approaches were supplemented by the need to take into account the technology of artificial intelligence. In addition, the article analyzes the legal principles of guaranteeing information security, as well as what changes have taken place under the conditions of martial law in Ukraine. The main provisions of the Information Security Strategy of Ukraine, which was approved even before the full-scale war until 2025, and the Action Plan for its implementation, adopted in March 2023, were analyzed. All positive changes regarding increased responsibility for threats to information security have been identified. Particular importance is given to finding out how digitization and protection of information security is taken into account in cases of cross-border cooperation of territorial communities. The results of two programs "Hungary-Slovakia-Romania-Ukraine ENPI Cross-border Cooperation Program 2007-2013" and "Hungary-Slovakia-Romania-Ukraine ENI CBC Program 2014-2020" were taken for analysis. As a result of the study, it was proved that information security in cross-border cooperation is an important element of guaranteeing both national and international security. Problems with disinformation, the use of false reports, incorrect or distorted translation of news are not only a violation of the right to information, but can become the basis for hostility and increased tension in the border areas. Clear recommendations regarding a protective mechanism to guarantee information security in cross-border cooperation are offered.

REFERENCES

1. Смотрич Д.В., Браілко Л. Інформаційна безпека в умовах воєнного стану. *Науковий вісник Ужгородського Національного Університету. Серія ПРАВО.* 2023. Випуск 77: частина 2. С. 121-127.

2. Артемов В. Ю., Хорошко В. О., Хохлачова Ю. Є., Погорелов В. В. Інформайційно-воєнна безпека як елемент національної безпеки України. *Захист інформації*. 2022. Т. 24, № 1. С. 21-29.

3. Гбур З. В.Основи інформаційної безпеки держави в умовах війни. / The Russian-Ukrainian war (2014–2022): historical, political, cultural-educational, religious, economic, and legal aspects : Scientific monograph. Riga, Latvia : "Baltija Publishing", 2022. 1421 p. 868-872. URL: http://baltijapublishing.lv/omp/index.php/bp/catalog/view/237/6325/13361-1

4. Нашинець-Наумова А.Ю. Інформаційна безпека: питання правового регулювання: монографія. Київ: Видавничий дім «Гельветика», 2017. 168 с.

5. Капля О. М. Правове регулювання інформаційної безпеки громадянина під час дії воєнного стану. *Експерт: парадигми юридичних наук і державного управління*. 2023. № 6(24). С. 16-20. https://doi.org/10.32689/2617-9660-2022-6(24)-16-20

6. Шинкаренко І. Р., Шинкаренко І. І. Інформаційна безпека України в умовах воєнного стану / Сучасні проблеми правового, економічного та соціального розвитку держави: тези доп. XI Міжнар. наук.-практ. конф.(м. Вінниця, 9 груд. 2022 р.). Вінниця, 2022. С. 139-140.

7. Амро Т. Взаємозв'язок систем забезпечення інформаційної безпеки та публічного управління в умовах воєнного стану: методи та можливості. *Публічне урядування.* 2022, № 5 (33). С. 83-88. https://doi.org/10.32689/2617-2224-2022-5(33)-11

8. Скочиляс-Павлів О.В. Сучасні загрози інформаційній безпеці України в умовах правового режиму воєнного стану. *Юридичний науковий електронний журнал*. 2023. № 9. 263-266.

9. Свердлов Д.В., Борисенко Т.В. Забезпечення інформаційної безпеки держави в умовах дії правового режиму воєнного стану / Актуальні проблеми превентивної діяльності Національної поліції в умовах воєнного стану : матеріали Всеукр. наук.-практ. семінару (м. Дніпро, 27 квіт. 2022 р.). Дніпро: ДДУВС, 2022. С. 78-80.

10. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року "Про Стратегію інформаційної безпеки": Указ Президента України; Стратегія від 28.12.2021 № 685/2021. URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text

11. Про затвердження плану заходів з реалізації Стратегії інформаційної безпеки на період до 2025 року: Розпорядження Кабінету Міністрів України від 30 березня 2023 р. № 272-р. URL: https://www.kmu.gov.ua/npas/pro-zatverdzhennia-planu-zakhodiv-z-realizatsii-str-a272r

12. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України": Указ Президента України; Стратегія від 26.08.2021 № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#n12
13. Кримінальний кодекс України від 05.04.2001 № 2341-III. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text
14. Про внесення змін до деяких законодавчих актів України щодо посилення кримінальної відповідальності за виготовлення та поширення забороненої інформаційної продукції : Закон України від 03.03.2022 № 2110-IX. URL: https://zakon.rada.gov.ua/laws/show/2110-20#n6
15. Про внесення змін до Кримінального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану: Закон України від 24.03.2022 № 2149-IX. URL: https://zakon.rada.gov.ua/laws/show/2149-20#n2
16. Про внесення змін до статті 114-2 Кримінального кодексу України щодо удосконалення відповідальності за несанкціоноване розповсюдження інформації про засоби протидії збройній агресії Російської Федерації: Закон України від 01.04.2022 № 2178-IX. URL: https://zakon.rada.gov.ua/laws/show/2178-20#n2
17. Про внесення змін до Кримінального та Кримінального процесуального кодексів України щодо забезпечення протидії несанкціонованому поширенню інформації про направлення, переміщення зброї, озброєння та бойових припасів в Україну, рух, переміщення або розміщення Збройних Сил України чи інших утворених відповідно до законів України військових формувань, вчиненому в умовах воєнного або надзвичайного стану: Закон України від 24.03.2022 № 2160-IX. URL: https://zakon.rada.gov.ua/laws/show/2160-20#n6
18. Про внесення змін до Кримінального кодексу України щодо посилення відповідальності за злочини проти основ національної безпеки України в умовах дії режиму воєнного стану: Закон України від 03.03.2022 № 2113-IX. URL: https://zakon.rada.gov.ua/laws/show/2113-20#n7
19. Про внесення змін до Кримінального та Кримінального процесуального кодексів України щодо удосконалення відповідальності за колабораційну діяльність та особливостей застосування запобіжних заходів за вчинення злочинів проти основ національної та громадської безпеки: Закон України від 14.04.2022 № 2198-IX. URL: https://zakon.rada.gov.ua/laws/show/2198-20#n6
20. Про внесення змін до Кодексу України про адміністративні правопорушення та Кримінального кодексу України щодо

відповідальності за порушення авторського права і (або) суміжних прав: Закон України від 01.12.2022 № 2803-IX. URL: https://zakon.rada.gov.ua/laws/show/2803-20#n3

21. The 3rd Call for Proposals of the Hungary-Slovakia-Romania-Ukraine ENI CBC Programme 2014-2020. URL: https://huskroua-cbc.eu/calls/3rd-call-for-proposals

22. Впровадження нових стандартів та технологій хірургічного лікування захворювань центральної нервової системи в транскордонному регіоні. URL: https://www.uzhnu.edu.ua/uk/cat/projects-nsdneuro

23. Energy recovery from municipal solid waste by thermal conversion technologies in cross-border region. URL: https://huskroua-cbc.eu/projects/financed-projects-database/energy-recovery-from-municipal-solid-waste-by-thermal-conversion-technologies-in-cross-border-region

Information about the authors:
Mendzhul Marija Vasylivna,
Doctor of Science of Law,
Professor of the Department of Civil Law and Procedure,
Uzhhorod National University
26, Kapitulna st., Uzhhorod, 88000, Ukraine
https://orcid.org/0000-0002-3893-4402

Mulesa Oksana Yuriivna,
Doctor of Technical Science,
Professor of Software System Department,
Uzhhorod National University
26, Kapitulna st., Uzhhorod, 88000, Ukraine
https://orcid.org/0000-0002-6117-5846