https://doi.org/10.33271/nvngu/2024-1/167

B. Melnychenko[*1],
orcid.org/0000-0003-1514-8131,
I. Khomyshyn[1],
orcid.org/0000-0002-6180-3478,
M. Sirant[1],
orcid.org/0000-0002-9393-2397,
S. Tsebenko[1],
orcid.org/0000-0002-9247-1867,
S. Yesimov[2],
orcid.org/0000-0002-9327-0071

1 – Lviv Polytechnic National University, Lviv, Ukraine
2 – Lviv State University of Internal Affairs, Lviv, Ukraine
* Corresponding author e-mail: bohdana.b.melnychenko@lpnu.ua

ORGANIZATIONAL AND LEGAL PRINCIPLES OF INFORMATION SECURITY OF ENTERPRISES IN THE CONDITIONS OF MARTIAL LAW IN UKRAINE

Purpose. To investigate the peculiarities of organizational and legal provision of information security (IS) in the conditions of martial law (ML). To propose changes to legislative provisions to improve legal regulation in this area. To develop systematic measures to balance the rights and obligations of individuals and legal entities in the field of IS in the conditions of ML.

Methodology. The general scientific and special legal methods of cognition are used: hermeneutic method allowed us to substantiate expansion of IS field; content analysis – to determine organizational principles of IS of enterprises in conditions of ML; structural and legal – to propose indicator conditions for legal norms; special-legal – to propose system of local regulatory acts for the legal provision of IS; comparative legal – to propose special legal regime for IS of enterprises.

Findings. It is indicated that during the state of war, the IS field of enterprise expands significantly and becomes an element of the national security system. The peculiarities of organizational and legal support and the basic organizational principles of IS of enterprises in the conditions of ML are determined. It is proposed to introduce a special legal regime for implementation of IS of enterprises in conditions of ML and use of the state's capabilities in this area under specified legal regime. Amendments to the articles of Special Part of Code of Ukraine on administrative offenses are proposed for effective regulatory support of the special legal regime for implementation of IS of enterprises

Originality. A legal tool is proposed to limit dissemination of information about a company's activities – the introduction of local law documents to classify information about the company's activities during ML into category "with limited access". Indicator conditions and additions to legislative norms are proposed.

Practical value. The developed proposals, indicator conditions and additions to legislative norms will contribute to strengthening the IS of enterprises.

Keywords: *information security of enterprises, martial law, legal principles, special legal regime, local regulations*

Introduction. A significant level of threats to the business and production activities of enterprises and, most importantly, the need to organize their uninterrupted functioning in conditions of martial law to fulfill urgent tasks of the economy, supply products to the troops and ensure the livelihood of the country's population require appropriate organizational and legal tools for the implementation of information security systems of enterprises.

In peacetime, the organizational and legal measures of information security of enterprises were mainly intended to counter industrial espionage and cyber-crime, but the war began to demand a fight against the aggressor's information forces, to counter subversive and terrorist threats. At the same time, the effectiveness of enterprise management actions in this area is reduced due, in particular, to the complexity of the legal structure of enterprise information security. The specified complexity is caused, in particular, by a significant number of subjects of economic, social, and legal relations in this sphere, which increases significantly under conditions of war, by the fact that the differentiation of subjects of social and economic relations in the information field is not sufficiently taken into account in the regulatory and legal field of Ukraine, the legal norms of direct action regarding the information security of legal entities, enterprises, and organizations are not sufficiently applied.

The above, in particular, leads to an insufficient provision of the balance of rights, obligations, and interests of the parties of social relations in the information sphere, and also creates gaps in the protection of national security, since the issues of information security of the enterprise under the conditions of military age intersect with issues of national security, especially if the specified enterprise is important for the economy and defense of the country and/or has a wide range of economic and social ties.

The above determines the urgency of researching the peculiarities of the organizational and legal provision of information security in the conditions of martial law and the development of proposals for the improvement of this area.

Literature review. The wide range of information security problems is evidenced by the number of aspects to which scientists who have devoted their research to this issue pay attention. The specifics of the organization of the basis of information security are determined by the tasks that must be solved by the information security of the enterprise. Thus, in the article by Yepifanova, et al. [1] the goal of information security is economic security. At the same time, Yepifanova, et al. [1] indicated the complex nature of threats caused by the state of war, which include "financial, legal, informational, technological" aspects, but information security is interpreted only as security of information- in accordance with the current regulatory acts on the factors of "availability, integrity, confidentiality" [1]. Perun [2] analyzed the state of "administrative and legal provision of information security of business entities" and proposed improvements to the legal basis for preserving commercial secrets, for which, in particular, it is proposed to conclude an addendum to the employment contract with the employee – a "non-disclosure agreement". It is noted that in the legal field there is "insufficient determination of the concept of "business information security", which increases the level of threats in the information war.

Bodunova's article [3] is devoted to the legal principles of combating cybercrime and it is determined that a significant gap in the regulatory and legal field of Ukraine in the conditions of a hybrid war is that it lacks a separate legal act dedicated to crimes in the IT sphere. The need for legal formation of factors for preventing threats in the specified area is also indicated.

Kovaliv, et al. [4] study the theoretical and legal foundations of the legal provision of cyber security. A systematic approach to the specified problem was applied, in particular, with an expanded interpretation of the concept of "critical information infrastructure of Ukraine" which includes "natural and legal entities" that form the "process of information relations". The need to identify the objects of this structure, their information audit to solve the security problems of these objects is indicated. The thesis that information security is more reliable under the conditions of integrated confrontation using state capabilities is developed in the presented article.

Borsukovskyi [5] "formulated basic requirements for the formation of the concept of information security in conditions of hybrid threats". These requirements determine the peculiarities of the organizational and legal regulation of information security under martial law. The main requirement is the promotion of flexible preventive measures in the specified area and the formation of an information security strategy in conditions of hybrid threats in order to ensure the effectiveness of the functioning of security systems. Borsukovskyi [5] indicates that information security measures of enterprises in the conditions of increased threats should not be financed by a left-over principle The lack of enterprise resources for the organization of information security is considered in the presented article.

Lutsenko, et al. [6] investigated the issue of criminal law enforcement of information security during armed aggression. It is indicated that "along with the strengthening of criminal law protection of the information sphere, the need to improve those normative acts containing blanket norms that define the subject of criminal offenses in the information sphere has increased". The need for codification of information legislation is also indicated. Ways to solve these problems are researched in the presented article.

Skochylias-Pavliv [7] analyzed the challenges to various aspects of information security in the conditions of martial law, in particular, pointed out new threats to the "industrial sphere" in view of the fact that "the need for constant updating of information security systems" is indicated. Issues of operational adaptation of organizational and legal conditions of information security, which were emphasized by Skochylias-Pavliv [7], are investigated in the presented article.

Lehominova, et al. [8] indicated the need for "special legal mechanisms in the conditions of hybrid war" which should "be aimed at preventing and countering the use of information technologies to carry out aggression, as well as at protection against new forms of threats to information security. Such mechanisms must be dynamic, i.e. quickly adapt to changing conditions and threats". This approach is expanded in the presented article.

In the article by Nashynets-Naumova [9], the world experience of "legislative regulation of confidential information regimes" is analyzed. Nashynets-Naumova [9] considers the EU's experience in this field to be "the most promising". It is also noted that in Ukrainian law "processes of unification ... only partially affect the category of confidential information". This issue is investigated in the presented article for the legal provision of information security.

Pravdiuk [10] points out that the legal and organizational foundations of information security in the conditions of war are much broader than the technical and technological aspects of the protection of enterprises, organizations, and the country. The urgent need for "the creation of a comprehensive system for ensuring cyber security and information security" is indicated. It is noted that legislators should act in advance and respond promptly to dynamic changes in the field of information security.

In the article by Moroz [11], it is indicated that a comprehensive normative regulation of administrative legislation in the field of information security is needed through the introduction of a special normative legal act. The need for constant monitoring of the compliance of the legal framework of information security with threats under martial law is indicated.

Sopilko [12] pointed out that "during external threats, especially information war ... enterprises and organizations need to develop and implement special policies and procedures for handling information resources", establish organizational "rules of operation in the company's information system". It is also noted that information threats "can cause irreparable damage... not only to an individual enterprise, but also to entire structures". The specified provisions, in particular, regarding the expansion of information security measures beyond the boundaries of a separate enterprise, are used in the presented study.

Zakharenko [13] points to the uncertainty of the concept of "information security" due to its multifunctionality and structural complexity, although the need for changes in the regulatory legal field in this area is indicated at the legislative level. Therefore, according to Zakharenko [13], nowadays there is a need to introduce a codification legal act that would regulate information security issues.

A review of literary sources shows that due to the significant increase in the level of threats to information security under martial law, organizational and legal support in this area needs improvement, and the organizational and legal principles of information security of enterprises under martial law must be defined.

Purpose. To investigate the peculiarities of organizational and legal provision of information security in the conditions of martial law. To propose changes to legislative provisions to improve legal regulation in this area. To develop systematic measures to balance the rights and obligations of individuals and legal entities in the field of information security in the conditions of martial law.

Methods. When performing scientific research, general scientific and special legal methods of cognition are applied.

By using the hermeneutic method, the need to expand the field of information security of the enterprise in the conditions of war is substantiated.

The method of content analysis made it possible to determine the main organizational principles of information security of enterprises in the conditions of martial law.

Structural-legal and formal-logical methods made it possible to analyze approaches to the phenomenon of information security and to propose indicator conditions and additions to legal norms in this area.

The application of the formal legal method made it possible to establish the need to apply the norms of the Criminal Code of Ukraine for the legal assessment of the dissemination of information due to the failure to take appropriate measures to protect it.

The special legal method made it possible to establish that for the legal provision of information security, enterprises should use a coordinated system of local regulatory acts.

The comparative legal method made it possible to assess the need for a special legal regime for the implementation of information security of enterprises and to propose changes to the articles of the Special Part of the Code of Ukraine on administrative offenses for this purpose.

Results. Information security is a set of organizational, technical and legal measures aimed at protecting vital information. Ensuring the information security of the enterprise is a purposeful organizational activity using legal, organizational and technical tools to protect the information environment for the purpose of sustainable functioning of the enterprise. The object of information security is information, information infrastructure and actions of subjects related to information.

Organizational and legal principles of information security of enterprises are formed by regulatory and legal acts regulating the business and production activities of enterprises and corporations related to the processing, collection, transmission and/or use of information. Accordingly, economic, social and other relations that accompany actions with information, primarily confidential information and information with limited access, become the object of legal regulation.

Subjects of legal regulation in the field of "enterprise information security" are natural and/or legal entities, society and the state.

In view of the above, "enterprise information security" as a legal category is much broader than its traditional attribution to issues exclusively related to information technologies. This is also evidenced by the conclusions of other scientists' research in this field. In particular, Koterlin [14] indicated that an effective system of information security should be based on: technical, political, legal ("formulation of all related elements into high-quality regulatory and legal acts" [14]) components.

This category is related to the restriction of information actions in an illegal manner, the consequences of which may be damage to the property interests or safety of a person, enterprise, organization, society, state. Therefore, the following definition is proposed for use in the regulatory and legal field: "Information security of the enterprise, as a legal category, is a set of corporate, economic and social relations that are implemented in the regulatory and legal field of Ukraine and are aimed at countering threats to the sustainable functioning of the information environment of the enterprise".

If in peacetime the legal principles of information security should provide, first of all, motivational and social control functions to prevent the subjects of social, economic and legal relations in this area from going beyond the legal field, then under conditions of martial law they should be aimed at neutralization targeted threats to the information infrastructure and ensuring reliable management of the enterprise.

In the conditions of war, any information about the company's activities using modern methods of integrated data can give the interested party the opportunity to disorganize work, destroy means and supply networks, acquire information about the location of those to whom the company's products are intended, especially if it concerns military units [15]. At the same time, attempts to differentiate enterprises into those related to critical infrastructure and those not related to it are artificial. References to forms of ownership or industry affiliation of enterprises in this case are not substantiated, since, in particular, according to clause 25, Part 2, Article 15 of the Law of Ukraine No. 389-VIII "On the Legal Regime of Martial Law" (as amended from 12.07.2022) the duties of "production and supply to the military ... of ordered products, services, energy resources" can be assigned by military administrations even to "nterprises and organizations , which are in communal ownership". Military administrations according to item 42, Part 2, Article 15 of the Law of Ukraine No. 389-VIII may involve the involvement of legal entities that are not even communally owned by the respective territorial communities, to meet the urgent needs of the population, primarily in transport and communication. That is, according to the specified legal norms, enterprises and organizations of any form of ownership or industry affiliation under certain circumstances can be classified as "critical infrastructure" and, accordingly, they can become targets for an aggressor in a hybrid war.

Traditional organizational approaches to the implementation of information security measures, which were used by enterprises in peacetime, are insufficient in wartime and do not correspond to the new level, new directions of threats [15]. In particular, the concept of information systems for industrial purposes requires an expanded interpretation due to the lack of legal norms, according to which the specified systems are clearly separated. Such new directions of threats as informational and psychological [16] also need to be countered, when through the use of informational (primarily informational and communicative) means, the enemy disorients and demotivates the personnel of the enterprise and/or its suppliers, contractors, etc.

Under conditions of military operations, enterprises use various methods for reducing the level of threats, in particular, resort to relocation, use workplaces with remote access, etc. The relocation of the enterprise leads to a significant change in logistical connections, which, in turn, results in the need for a significant change in the organizational and legal provision of information security. The wartime expansion of remote access workplaces also increases the vulnerability of enterprise information flows. This, accordingly, forms the peculiarities of the organization of information security in the conditions of martial law, and determines the need for changes in the organizational and legal protection of the specified vulnerable places.

The above also shows that the conditions of military operations lead to the need for a radical revision of approaches to the formation of information security of the enterprise. This is primarily due to the fact that the informational aspect of hybrid warfare allows the aggressor to choose a wide range of directions and objects for attack. The reasons for which the information space of a particular enterprise is attacked can be very different. In a state of war, an enterprise may be affected by a threat even if it is not a direct target of the aggressor's information, sabotage, or espionage units. For example, an attack can be aimed at a wide range of legal entities, which includes the threatened enterprise. The object that is in economic, social, informational relations with the enterprise affected by the attack can also be attacked. Damage to the enterprise can also be a consequence of the use by its divisions of means or channels of information transmission, information resources that have been attacked. This enterprise may be included in the circle of enterprises that are suppliers of military units whose location the information forces of the aggressor want to discover.

Moreover, the enterprise may not be attacked itself, but may cause a threat due to improper use of organizational, technological and other mechanisms of information security. In particular, Arkhypov, et al. [17] indicate that for effective information security of the enterprise, it is necessary to "analyze all possible information threats to the business", including in the absence of their direct impact on the information system of the enterprise.

The above also shows that the information security of any enterprise in the conditions of war should be interpreted more broadly, taking into account the need to form the security of society and the state [18], and, accordingly, needs organizational and legal support.

This leads to the fact that, under the conditions of martial law, organizational information security measures of the enterprise should include the following directions:

- the enterprise must implement a systematic identification, isolation and, if possible, avoidance of activities not determined by production necessity, which contribute to the influence of external or internal threats;
- the enterprise's organizational efforts regarding the formation of information security measures must be involved in all implemented areas of activity;
- the information security system, unlike in peacetime, must protect not only the organizational and inter-structural connections of the enterprise itself, but also cover its external connections.

For this purpose, the following organizational principles of information security of enterprises in the conditions of martial law should be implemented:

- the need for an operational and dynamic change of the enterprise's information security system in view of the dynamic change in threats;
- continuity of organizational activities of the management and authorized persons to improve the information security of

the enterprise, given that in the conditions of war, the means and tools of targeted malicious activity of the aggressor are constantly being improved;

- the need, due to the multiplicative nature of the influence of military threats, to form communication links between different areas of information security for their mutual coordination;

- permanent monitoring of the information environment, identification of likely directions of information leakage for the formation of information security mechanisms and implementation of effective methods, ways, and protection tools;

- avoiding the protection of only the weak points of the information environment and the use of a complex system approach in information security, implementation of a unified information protection strategy;

- introduction of information security measures in all connecting links with the external environment – counterparties, suppliers, consumers, even for the use of own company's resources for this on a contractual basis;

- implementation of the unity of employees and management in the formation of information security of the enterprise.

From these circumstances, the possibility of complex application of threats to information security with a military purpose requires special attention, since in the conditions of a hybrid war, information becomes a means of conducting hostilities to inflict maximum damage on the enemy in all possible directions. The primary targets of attack are enterprises whose products are supplied to the army or, as it can be seen from the targets chosen for missile and bomb attacks, enterprises that are important for the livelihood of the population. For these enterprises, the organizational and legal principles of information security in the conditions of martial law have their own characteristics.

A stricter attitude to the dissemination of information that may be of value to the enemy by all subjects of information relations is the first of these peculiarities. Dissemination of such information in conditions of martial law is subject to the application of Article 114^2, item 2, Section 1 of the Special Part of the Criminal Code (CC) of Ukraine. Therefore, when organizing the information security system, responsible persons of enterprises and corporations should also take into account the fact that the specified Article of the Criminal Code of Ukraine does not have restrictions on unintentional dissemination of information, dissemination of information due to failure to take appropriate measures to protect it, etc.

At the same time, the effect of legal norms regarding the responsibility of subjects entrusted with the responsibility of ensuring the information security of the enterprise should extend only to the horizon of their managerial influence. For this purpose, the norms of direct action must be introduced, which is especially important during martial law.

This also requires proper coordination of legal issues in the specified area, introduction of additions and indicator conditions to the current legislative norms. It takes time to complete all legislative procedures, which is unacceptable due to the dynamic change of threats and the rapidity of changing tactics by the aggressor. Therefore, for the effectiveness of organizational actions to ensure information security, it is proposed to use a coordinated system of local regulatory acts of enterprises.

The need for proper coordination of the specified system is due to the fact that organizational tools and security measures must take into account the differences between military, economic, technological, cyber threats, etc. and the dynamic nature of threats, which requires prompt changes to the set of local regulations.

When forming a system of local regulatory acts regarding the protection of enterprise management information, it is also necessary to take into account the fact that information security, as a component, includes information security, or, in an even narrower interpretation, "data protection". Then, for such aspects of the organization of information security as technical, technological, cyber security, local normative acts of enterprises should be based on international ISO/IEC standards for information security management. These documents include international standards: ISO/IEC 17799:2005; ISO/IEC 27000; ISO/IEC 27001; ISO/IEC 17799:2005 ISO/IEC.

The State Standard of Ukraine DSTU ISO/IEC 27001 declares an important characteristic of "Information Security" – its variability over time depending on the value in a specific period of the main properties of information "confidentiality, reliability, non-failure, reliability", etc. and the level of influence and number of external and internal threats.

We should also note that the State Standard of Ukraine DSTU ISO/IEC 17799:2005 provides for protection "against a wide range of threats", i.e. not only technical, technological or cyber threats.

This substantiates the legal possibility of applying the ISO/IEC 27001 standard in the condition of military risks, which, in turn, makes it possible to evaluate the effectiveness of organizational measures of information security according to the methodology of the mentioned standard. For this, in accordance with the specified standard, it is necessary to assess the direction and dynamics of threats. The criterion for such an assessment according to the DSTU ISO/IEC 27001 standard is the security risks of the enterprise, which are comparable to the possible damage which will occur upon the realization of one of the specified threats or their combination. This also allows moving from the assessment of damage to the information itself according to Shannon's well-known approach to social, economic, and industrial damage, which makes it possible to use appropriate legal tools.

Terminological uncertainty and the unreadiness of the current regulatory legal framework to confront wartime threats are significant obstacles to the use of legal tools in the organization of an enterprise's information security system. Therefore, when forming a system of local normative acts of the enterprise, it should be taken into account that the specified international ISO/IEC standards provide a normative basis for a wider application of organizational information security measures than "data protection", which was previously considered the exclusive goal of information security. Thus, according to the DSTU standard ISO/IEC 17799:2005, the goal of information security is protection against threats to ensure the sustainability of business activities. The interpretation of the definition of "business" in the English language extends to the business and production activities of enterprises, which provides a legal basis to use the specified regulatory documents in this area as well.

The EU Legislation has direct action norms aimed at the information security of enterprises. In particular, such norms are contained in EU Directive No. 114 of 2008 "On the identification and designation of European critical infrastructure and assessment of the need to increase the level of its protection". Such norms are also in the national regulatory field of developed countries, for example, in the "Cyber Security Strategy" of Great Britain. Certain steps in this regard have been taken in Ukraine. Thus, the Law of Ukraine No. 2163-VIII "On the basic principles of ensuring cyber security of Ukraine" defined "the powers of ... enterprises, institutions, organizations, individuals and citizens", but, unfortunately, the specified legal norm applies only to those individuals and legal entities that are involved in the field of information communications

Therefore, the approaches of the legislation of developed countries regarding the implementation of direct-action norms aimed at the information security of enterprises should be extended in the regulatory and legal field of Ukraine. In particular, the Resolution of the CMU No. 1126 regarding technical protection of information (TPI) needs to be changed. The definition of "Technical Information Technology", in contrast to the one provided in the mentioned Resolution No. 1126, nowadays extends to state-of-the-art digital technologies, which are especially relevant as information security

tools, including cloud technologies, artificial intelligence, etc. That is why it is especially important to extend the application of CMU Resolution No. 1126 to enterprises and corporations. For this purpose, in the text of Resolution of the CMU No. 1126, enterprises must be included in the list of parties to which this Resolution applies. Therefore, it is proposed to replace the definition of "person" with the indicator condition – "physical and legal entity" in the provision of the Resolution, which enumerates the areas of its application in relation to "person, society and the state". The above will, if necessary, provide a legal basis for the use of the norms of Resolution of the Cabinet of Ministers No. 1126 as a legal basis for the organization of the information security system of enterprises.

In view of the above, indicator conditions should also be introduced to the Law of Ukraine No. 2657-XII "On Information". In particular, Article 3 Part 1 of the provision on "information security of Ukraine" should be replaced by the provision of "information security of citizens, legal entities, society and the state".

Also, to Article 5 Part 1 of the Law of Ukraine No. 2657-XII, which stipulates the right of citizens to information, the condition-indicator "except for the conditions of martial law" should be added. This corresponds to the necessity of restrictions on the rights and freedoms of citizens in the conditions of martial law [19].

Part 2, Article 6. Law of Ukraine No. 2657-XII needs to be supplemented in the paragraph where limitations of the right to information are specified. After the words "other people's rights" the indicator condition "and legal entities" should be given.

These additions will contribute to the effectiveness of legal support of security measures of enterprises and corporations. The above needs appropriate confirmation in the regulatory and legal field of Ukraine, first of all, by the application of direct-action norms in the legislation.

It should also be noted that the interpretation of information security according to DSTU ISO/IEC 17799:2005 and the interpretation provided in clause 3, Part 3 of the Law of Ukraine No. 537-V do not coincide. The definition of information security provided in clause 3, Part 3, of the Law of Ukraine No. 537-V, in its essence, is the legal basis of only "information protection". The necessity of assigning the task of information protection to the sphere of information security is unconditional [20], but these legal definitions should not be equated. Therefore, the specified definition of information security according to the Law of Ukraine No. 537-V is significantly limited for the legal substantiation of the principles of information security of enterprises, especially in the conditions of martial law [21, 22].

Law of Ukraine No. 537-V also does not provide adequate legal substantiation for the need to prevent methods of hybrid warfare. This, in particular, is due to the fact that the mentioned Law was prepared and approved at its beginning, although, even during the period of less active confrontation in 2014–2018, the aggressor state was already actively using malicious means of information warfare against Ukrainian institutions and Ukrainian enterprises.

Therefore, for legal counteraction to information tools of hybrid warfare, cyber-terrorism, formation of legal grounds and determination of the importance of ensuring information security at the level of enterprises, the specified definition of information security, provided in clause 3, Part 3, Law of Ukraine No. 537-V requires the application of the indicator condition "negative informational influence, intentional actions to cause harm to individuals and/or legal entities, society and the state".

The definition of an information threat in the "Information Security Strategy" put into effect by Decree of the President of Ukraine No. 685/2021 dated 28.12 2021 has a limited application for the legal basis in the organization of information security of enterprises. This definition lacks a significant political, economic and social component that can be targeted by an informational threat – enterprises, legal entities. Therefore, the legal application of this definition for the organization of information security of enterprises is limited to the indirect use of the definition "information influence" [23, 24].

In order to eliminate the terminological uncertainty, the Law of Ukraine No. 1089-IX "On Electronic Communications" in the version dated 07.29.2023 also needs to be clarified, where instead of the definition "information security" the definition "security of networks and services" is used, which, in the essence of the normative provisions of the specified Law, is more aimed at data protection.

Due to the significant and rapid changes in the tasks of information security of enterprises, the uncertainty in the need to introduce information security measures to limit the spread of corporate information during martial law leads to legal conflicts. Plaintiffs in court cases about violation by the management of enterprises and corporations of their right to receive information point out that this right is guaranteed by the Constitution of Ukraine. Thus, although Article 64 of the Constitution of Ukraine indicates that during the state of war or state of emergency, the rights of citizens may be limited, in particular the right to "collect, store, use and disseminate information", at the same time, Article 55 of the Constitution of Ukraine indicates that these rights must be protected by the court.

Therefore, it should be taken into account that during the period of martial law, requests from third parties or organizations, even if they are officially registered, to provide information that is not classified as "with limited access" may be reasonably delayed for publication, making public reasons for postponement according to the provisions of Law of Ukraine No. 2657-XII "About information". Such reasons may include danger to the company's employees due to the provision of relevant information; temporary lack of opportunity to collect information, in particular, due to the lack of employees due to mobilization; due to the temporary impossibility of reliable protection of information channels by employees who have this information but work remotely under martial law conditions; other reasons due to force majeure factors.

Also, the distribution of information by employees of the enterprise should be limited due to possible damage to national interests, corporate interests of counterparties, life, or health of other employees, to prevent the distribution of information obtained confidentially, if the information is classified as "having limited access".

Information can be categorized as "restricted access" documentation, which is regulated by the local law of a legal entity under Article 7 of the Law of Ukraine No. 2939-VI "On access to public information" and may be classified as "confidential information".

As according to Article 21 of the Law of Ukraine No. 2657-XII the publication of information that belongs to the category "with limited access" is prohibited, so one of the primary measures of the information security of the enterprise should be the assignment of information that may pose a threat to the business and production activities of the enterprise or life/health of workers to this category by the managers of corporate information. For this, it is necessary to use legal instruments of local normative regulation: management orders, internal instructions of the enterprise, etc. Employees of the enterprise must be informed about the inadmissibility of granting access to corporate information to persons without the right to access it in conditions of martial law. The employee's notification must be confirmed by his personal signature [25].

It is indicated that, in the case of legal disputes with the plaintiff's reference to Part 2 of Article 200 of the Civil Code of Ukraine, which regulates the rights of relations in the information sphere, the application of Part 1, Article 5. Law of Ukraine No. 2657-XII, according to which the use of the right to information should not lead to violation of the rights of other physical/legal entities, will be allowed.

For this, the legal instruments of local normative regulation – the company's documents must indicate harm to corporate interests in case of dissemination of information that belongs to the "restricted access" category.

For the effective organization of information security measures, during martial law, it is also necessary to temporarily suspend Article 21 "Information with restricted access" of the Law of Ukraine No. 2657-XII, namely, Part 4: according to which the specified information cannot include information about certain categories of legal entities. During the state of war, these provisions may harm citizens and the specified categories of legal entities.

The above-mentioned suspension of clause 2, Part 4, Article 21 ZU No. 2657-XII is due to the need not to give the aggressor the opportunity to adjust his strikes, in particular on the infrastructure of enterprises. Suspension of clause 2, Part 4, Article 21 of ZU No. 2657-XII is due to the necessity of the above-mentioned measures regarding information security of enterprises of all types of ownership, in particular, specified in this subsection of the Law of Ukraine. Suspension of clause 6, Part 4., Article 21 of ZU No. 2657-XII due to the fact that the majority of international treaties of Ukraine, ratified by the Verkhovna Rada of Ukraine, do not provide for the circumstances of military aggression of this level of intensity.

Also, with the specified reasons, an indicator condition should be introduced to clause 1, Part 4, Article 21 of the Law No. 2657-XII, according to which it is impossible to assign information about the state of the environment to data with limited access. The indicator condition should state: "during martial law, if it is related to information about the location of industrial facilities, military purpose or critical infrastructure".

The following indicator condition must be introduced to clause 2, Part 4, Article 21 of the Law of Ukraine No. 2657-XII, according to which it is impossible to assign information about disasters and emergency situations to data with limited access: "if this emergency situation is not a consequence of military actions and the dissemination of information about it in conditions of martial law does not pose an informational threat to individuals or legal entities". The need for this indicator condition is due to the fact that "emergency situations" in the conditions of war can include the consequences of the aggressor's actions regarding the destruction of the infrastructure of enterprises, hindering their production activities, etc. Therefore, the dissemination of such information poses the threat of adjusting the aggressor's fire on the infrastructure of enterprises.

The adoption of the Law of Ukraine dated March 24, 2022 No. 2149-XX promotes the strengthening of the imperative of the legal foundations of information security of enterprises.

At the same time, it is expedient to increase the level of imperativeness of the legal principles of information security of enterprises under martial law by adding to paragraph 1, Article 1142, Section 1 of the Special Part of the Criminal Code of Ukraine "Crimes against the foundations of the national security of Ukraine" the supplement of the following content: "Dissemination of information on the direction, movement of weapons, armaments, munitions, raw materials, components for the production of weapons, munitions, dual purpose products and products to ensure the military needs and livelihood of the population to Ukraine".

Paragraph 2, Article 1142, Section 1 of the Special Part of the Criminal Code needs to be supplemented by: "Dissemination of information on the movement, movement or location of the Armed Forces ... weapons, munitions, as well as raw materials, components for the production of weapons, munitions, dual-purpose products and products to ensure military needs and the population's livelihood". The specified changes will extend the effect of the specified legal norms to a wide range of legal entities.

If in peacetime the information security of enterprises was a self-regulated system, the formation and functioning of which took place according to narrow corporate interests and according to changes in the directions and technologies of the formation of information threats, which did not require regulatory influence, then in the state of war, the information security of the enterprise should become an element of the national security system. Enterprises, corporations, and legal entities in wartime need agreed regulatory conditions for the use of information security mechanisms, as this will contribute not only to the settlement of corporate conflicts in the event of overlapping security spheres, reliable legal protection in the event of lawsuits related to the information support of business and economic activities of enterprises in a special period, but also to strengthening national security. The specified regulatory conditions must take into account the circumstances and capabilities of enterprises to implement information security tasks fully independently to protect key components of the country's economy. This can be found out when conducting an information audit of enterprises, assessing the state of their information security and their importance for the economy and defense, which necessitates the introduction of relevant legal acts.

When researching issues of organizational and legal regulation of information security of enterprises, we established that the sphere that needs regulation and legal consideration is much wider than the narrow corporate framework. This expands the need for the introduction of norms of direct action and separation for this purpose of the sub-branch of information security of individuals and legal entities, society, and the state in information law. The prerequisite for the specified separation may also be the need for legislative consolidation of special legal constructions, basic definitions of information security through the approval of the relevant Law. This will provide opportunities not only for a comprehensive assessment of proper/improper provision of information security during the consideration of relevant court cases, but also for systematization of legislative norms in the field of information security, identification and elimination of contradictions between them.

In the conditions of a hybrid war, the information security organization of the enterprise must take into account that using a powerful targeted attack, in most cases, the aggressor's actions will be successful. Under such circumstances, it becomes expedient to detect an act of informational aggression in a timely manner, assess its direction and consequences. This should be taken into account not only when organizing the protection of purely informational infrastructure, but also when forming the enterprise's production and business processes, for which many enterprises in wartime will lack their own resources.

Therefore, in order to actively counter threats to information security in the conditions of the use of modern information tools to neutralize the information security systems of enterprises that, due to the unequal personnel, resource, and technical capabilities of the aggressor state and individual enterprises or corporations, cannot provide legal entities of Ukraine with the appropriate level of protection, it is proposed to introduce a special legal regime for the implementation of information security of the country's leading enterprises and the use of state opportunities for this.

Certain elements of complex approaches in this direction are already available today. In particular, state structures implement measures to protect information and telecommunication systems, and although, to a greater extent, these systems are outside the sphere of influence of the protection services of individual enterprises, they play a significant role in shaping the level of their information security. So according to paragraph 11 Part 1 of Article 8 of Law of Ukraine No. 389-VIII "On the Legal Regime of Martial Law" as amended in accordance with Laws No. 1089-IX dated 16.12.2020, No. 1702-IX dated 16.07.2021 – came into force on 01.01.2022, the military command along with by military administrations has the right

to "regulate ... the transfer of information through computer networks", which is already one of the legal bases of the special legal regime for the implementation of information security of leading enterprises.

Also, in the conditions of war, the organizational and legal principles of information security of enterprises extend beyond the boundaries of information law and should rely more on the imperative norms of administrative and criminal law. Therefore, the special legal regime proposed above for the implementation of information security of the country's leading enterprises should be based on the expansion of the norms of Administrative Law regarding the provision of information security of legal entities.

For this purpose, it is proposed to introduce changes to the articles of the Special Part of the Code of Ukraine on Administrative Offenses (CUAO):

1. Article 172-8: "The subjects of offenses in Part 1 of this article are the persons specified in paragraph ... as well as the subjects specified in Part 4 of the Law of Ukraine No. 2657-XII "On Information".

2. Article 188-31: "which also includes information with limited access of legal entities".

3. Article 212-5: "in the field of economy during wartime, including the activities of enterprises, as well as in the field of defense of the country".

4. Article 212-6: "Illegal access to information of information (automated) systems, including enterprise systems". But "the same actions committed in a special period entail responsibility according to Article 114^2, clause 2. Chapter 1 of the Special Part of the Criminal Code of Ukraine".

The proposed changes to the Code of Administrative Offenses under the conditions of martial law in Ukraine will increase the responsibility of enterprises and corporations, will contribute to increasing the level of organization of their information security and will allow using the legal tools provided by them for this purpose effectively.

Conclusions. The interpretation of legal definitions of information security of enterprises, which excludes uncertainty in the application of legal norms in this area, is proposed and substantiated. It is noted that attempts to differentiate enterprises into those belonging to critical infrastructure and those not belonging to it are artificial.

It is indicated that the concept of information systems for industrial use needs an expanded legal interpretation due to the lack of norms in the legislation of Ukraine, according to which the specified systems are clearly separated. It is noted that the information security of the enterprise in the conditions of war should be interpreted more broadly.

During martial law, it is proposed to spread the organizational and legal principles of information security of enterprises beyond the limits of information law and the use of imperative norms of administrative and criminal law. In order to increase the imperativeness of legal norms under martial law, supplements to the articles of the Special Part of the Criminal Code of Ukraine are proposed.

Indicator conditions and supplements to the Laws of Ukraine are proposed.

It is indicated that the legal sphere of information security of enterprises under martial law, which requires regulation, is much wider than the narrow corporate framework, therefore this determines the need for the introduction of direct-action norms and for this purpose, the sub-branch of information security in information law.

It is proposed to introduce a special legal regime for the implementation of information security of the country's leading enterprises in the conditions of martial law and to use the state's capabilities in this area under the specified legal regime. For the effective regulatory support of the special legal regime for the implementation of information security of enterprises, amendments to the articles of the Special Part of the Code of Ukraine on administrative offenses are proposed.

The following organizational measures are proposed to strengthen the information security of enterprises during martial law:

- the enterprise must implement systematic detection, isolation and, if possible, avoidance of activities not determined by production necessity, which contribute to the influence of external or internal information threats;
- organizational efforts of the enterprise to form information security measures should be involved in all areas of activity;
- the information security system, unlike in peacetime, must protect not only organizational and inter-structural connections of the enterprise itself, but also cover its external connections;
- it is necessary to organize an operational change of the information security system of the enterprise in accordance with the dynamic change of threats;
- strengthening of communication links between different areas of information security for their mutual coordination;
- permanent monitoring of information flows of the enterprise, identification of probable directions of information leakage for the organization of security measures;
- avoiding the protection of only the weak points of the information environment and the use of a complex system approach in information security, implementation of a unified information protection strategy;
- organization of countermeasures against information and psychological threats.

The following legal measures to strengthen the information security of enterprises during martial law are proposed:

- application of Article 114^2, Part 2, paragraph1 of the special part of the Criminal Code of Ukraine on the dissemination of information (including its unintentional dissemination) that may represent value for the enemy, by all subjects of information relations;
- limiting the effect of legal norms regarding the responsibility of subjects entrusted with the responsibility of ensuring the information security of the enterprise by the horizon of their managerial influence;
- the use of an agreed system of local normative acts of the enterprise for information security tasks, in particular, regarding the classification of corporate information into the categories of "confidential" and "restricted access";
- legal substantiation for the narrowing of the provision of information by the employees of the enterprise at the request of individuals during the martial law is proposed, which will allow resolving legal disputes on these issues.

Prospects for further research in this direction consist in detailing the legal support of a special regime for the implementation of information security of enterprises in the conditions of martial law.

References.

1. Yepifanova, I., Dzhedzhula, V., & Shevchuk, Y. (2023). Factors influencing the process of managing economic security of enterprises in conditions of military condition. *Innovation and Sustainability*, *2*, 120-125. https://doi.org/10.31649/ins.2023.2.120.125.

2. Perun, T. S. (2020). Information security of business entities: new threats and prospects of development. *Academic notes of TNU named after V. I. Vernadskyi. Series: legal sciences, 31*(70/3), 138-143. https://doi.org/10.32838/TNU-2707-0581/2020.3/24.

3. Bodunova, O. M. (2023). Prevention of crime in the field of information technologies in the conditions of martial law in Ukraine. *Scientific Bulletin of the Uzhhorod National University*, *75*(2), 83-87. https://doi.org/10.24144/2307-3322.2022.75.2.13.

4. Kovaliv, M., Skrynkovskyy, R., Nazar, Y., Yesimov, S., Krasnytskyi, I., Khrystyna, K., Kniaz, S., & Kemska, Y. (2021). Legal Support of Cybersecurity of Critical Information Infrastructure of Ukraine. *Path of Science, 7*(4), 2011-2018. https://doi.org/10.22178/pos.69-12.

5. Borsukovskyi, Y. V. (2019). Defining requirements to develop information security concept in hybrid threats conditions. *Cyber security: education, science, technology, 1*, 61-72. https://doi.org/10.28925/2663-4023.2019.5.6172.

6. Lutsenko, Yu. V., & Denysenko, M. M. (2022). Combating crime under martial law: theoretical and legal problems. *Carpathian Legal Bulletin, 3(*44), 70-75. https://doi.org/10.32782/pyuv.v3.2022.16.
7. Skochylias-Pavliv, O. V. (2023). Current threats to the information security of Ukraine in the conditions of the legal regime of the martial state. *Legal scientific electronic journal, 9*(65), 263-266. https://doi.org/10.32782/2524-0374/2023-9/65.
8. Lehominova, S. V., Shchavinskyy, Y. V., Muzhanova, T. M., Dzyuba, T. M., & Rabchun, D. I. (2023). Legal mechanisms for ensuring information security in Ukraine in the conditions of hybrid war. *Telecommunications and information technologies, 1*(78), 101-110. https://doi.org/10.31673/2412-4338.2023.0101111.
9. Moroz, V. (2021). Features of information security in martial law. *Legal Bulletin*, *2*(59), 94-101. https://doi.org/10.18372/2307-9061.59.15600.
10. Nashynets-Naumova, A. (2019). Global experience of legislative regulation of regimes confidential information. *Entrepreneurship, economy and law, 4*, 166-170. Retrieved from https://elibrary.kubg.edu.ua/id/eprint/27354/1/A_Nashynets_Naumova_PGP_4_2019_FPMV.pdf.
11. Pravdiuk, A. (2023). Information security of Ukraine: information influence and information wars. *European Political and Law Discourse, 10*(1), 111-121. https://doi.org/10.46340/eppd. 2023.10. 1.6.
12. Sopilko, I. (2021). Peculiarities of countering cyber threats by legal methods and means. *Legal Bulletin*, *4*(61), 106-110. https://doi.org/10.18372/2307-9061.61.16356.
13. Zakharenko, K. (2019). The category of information security in the national philosophical and political discourse. *Bulletin of Lviv University, 23*, 158-165. https://doi.org/10.30839/2072-7941.2018.130531.
14. Koterlin, I. B. (2022). Information security in martial law in terms of ensuring information rights and freedoms. *Actual problems of domestic jurisprudence*, *1*, 150-155. https://doi.org/10.32782/392257.
15. Zaporozhets, S. A. (2019). Information security of Ukraine in the conditions of the hybrid war. *Problems of creation, testing, application and operation of complex information systems, 17*, 52-63. https://doi.org/10.46972/2076-1546.2019.17.05.
16. Barabash, O., & Hryshchuk, A. (2022). Provision of information security in the context of protection against destructive informational influence. *Law journal of Donbass, 4*(81/1), 55-60. https://doi.org/10.32782/2523-4269-2022-81-4-1-55-60.
17. Arkhypov, O., & Teplytska, T. (2019). Adaptive approach to information security management. *Young scientist, 11*(75), 668-672. https://doi.org/10.32839/2304-5809/2019-11-75-142.
18. Fedchenko, O. (2022). Analysis of factors and modern threats to the information security of the state in the context of ensuring the national security of Ukraine. *Journal of Scientific Papers "Social Development and Security"*, *12*(3), 128-134. https://doi.org/10.33445/sds.2022.12.3.11.
19. Kaplia, O. M. (2023). Legal regulation of citizen's information security during martial law. *Expert: paradigms of legal sciences and public administration*, *6*(24), 16-20. https://doi.org/10.32689/2617-9660-2022-6(24)-16-20.
20. Smotrych, D., & Brailko, L. (2023). Information security under martial law. *Scientific Bulletin of the Uzhhorod National University*, *77*(2), 121-127. https://doi.org/10.24144/2307-3322.2023.77.2.20.
21. Melnyk, D. S., Parfylo, O. A., Butenko, O. V., Tykhonova, O. V., & Zarosylo, V. O. (2022). Practice of the member states of the European Union in the field of anti-corruption regulation. *Journal of Financial Crime*, *29*(3), 853-863. https://doi.org/10.1108/JFC-03-2021-0050.
22. Kalina, I., Khurdei, V., Shevchuk, V., Vlasiuk, T., & Leonidov, I. (2022). Introduction of a corporate security risk management system: The experience of Poland. *Journal of Risk and Financial Management*, *15*(8). https://doi.org/10.3390/jrfm15080335.
23. Semenets-Orlova, I., Rodchenko, L., Chernenko, I., Druz, O., Rudenko, M., & Poliuliakh, R. (2022). Requests for Public Information in the State Administration in Situations of Military Operations. *Anuario De La Facultad De Derecho.Universidad De Extremadura*, *38*, 249-270. https://doi.org/10.17398/2695-7728.38.249.
24. Nitsenko, V., Mardani, A., Streimikis, J., Ishchenko, M., Chaikovsky, M., Stoyanova-Koval, S., & Arutiunian, R. (2019). Automatic Information System of Risk Assessment for Agricultural Enterprises of Ukraine. *Montenegrin Journal of Economics*, *15*(2), 139-152. https://doi.org/10.14254/1800-5845/2019.15-2.11.
25. Semenets-Orlova, I., Shevchuk, R., Plish, B., Moshnin, A., Chmyr, Y., & Poliuliakh, R. (2022). Human-centered approach in new development tendencies of value-oriented public administration: Potential of education. *Economic Affairs*, *67*(5), 899-906. https://doi.org/10.46852/0424-2513.5.2022.25.

Організаційні та правові засади інформаційної безпеки підприємств в умовах воєнного стану в Україні

Б. Б. Мельниченко[*1], *І. Ю. Хомишин*[1], *М. М. Сірант*[1], *С. Б. Цебенко*[1], *С. С. Єсімов*[2]

1 – Національний університет «Львівська політехніка», м. Львів, Україна
2 – Львівський державний університет внутрішніх справ, м. Львів, Україна
* Автор-кореспондент e-mail: bohdana.b.melnychenko@lpnu.ua

Мета. Дослідити особливості організаційно-правового забезпечення інформаційної безпеки в умовах воєнного стану. Запропонувати зміни законодавчих положень для вдосконалення правого регулювання у цій сфері. Розробити системні заходи балансування прав і обов'язків фізичних і юридичних осіб у сфері інформаційної безпеки в умовах воєнного стану.

Методика. Використані загальнонаукові та спеціально-правові методи пізнання: герменевтичний – дозволив обгрунтувати розширення сфери інформаційної безпеки підприємства; контент-аналізу – визначити організаційні засади інформаційної безпеки підприємств в умовах воєнного стану; структурно-правовий – запропонувати умови-індикатори до правових норм; спеціально-юридичний – запропонувати для правового забезпечення інформаційної безпеки систему локальних нормативних актів; компаратив но-правовий – запропоновати спеціальний правовий режим інформаційної безпеки підприємств.

Результати. Указано, що за воєнного стану сфера інформаційної безпеки підприємства значно розширюється та стає елементом системи національної безпеки. Визначені особливості організаційно-правового забезпечення та основні організаційні засади інформаційної безпеки підприємств в умовах воєнного стану. Запропоноване введення спеціального правового режиму реалізації інформаційної безпеки підприємств країни в умовах воєнного стану й використання у цій сфері за вказаного правового режиму можливостей держави. Для ефективного нормативного забезпечення спеціального правового режиму реалізації інформаційної безпеки підприємств запропоновані зміни до статей Особливої частини Кодексу України про адміністративні правопорушення.

Наукова новизна. Запропоновано правовий інструмент для обмеження поширення інформації про діяльність підприємства – запровадження документів локального права для віднесення інформації щодо діяльності підприємства на час воєнного стану до категорії «з обмеженим доступом». Запропоновані умови-індикатори й доповнення законодавчих норм.

Практична значимість. Розроблені пропозиції, умови-індикатори й доповнення законодавчих норм сприятимуть посиленню інформаційної безпеки підприємств і національній безпеці.

Ключові слова: *інформаційна безпека підприємств, воєнний стан, правові засади, спеціальний правовий режим, локальні нормативні акти*

Дата надходження рукопису 05.09.23.