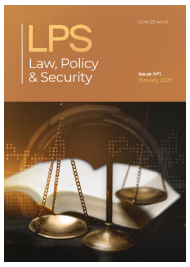

LAW, POLICY AND SECURITY

Journal homepage: https://lpas.com.ua/

***Law, Policy and Security*, 1(1), 4-17**

Received: 28.02.2023 Revised: 18.05.2023 Accepted: 12.06.2023

UDC 342.92

Nataliya Mentukh*

PhD in Legal Sciences, Associate Professor
West Ukrainian National University
46009, 11 Lvivska Str., Ternopil, Ukraine
https://orcid.org/0000-0002-1016-7635

Oksana Shevchuk

PhD in Legal Sciences, Associate Professor
West Ukrainian National University
46009, 11 Lvivska Str., Ternopil, Ukraine
https://orcid.org/0000-0001-6453-355X

Protection of information in electronic registers: Comparative and legal aspect

Abstract. The relevance of the research topic lies in the further development of the theoretical and methodological foundations of information protection in electronic registers based on a comprehensive study of the development of the register system at the current stage of the development of information systems, a thorough study of foreign experience in this field. The purpose of the work was to investigate the analysis of scientific approaches to the definition of the concept of "information security", "information protection" in electronic registers, as well as in a comparative analysis of the main methods and mechanisms of information protection in electronic registers in Ukraine and some foreign countries. The authors studied the main directions of the European information security policy, the protection of information in electronic registers, the main mechanisms of information protection in electronic registers based on a conceptual analysis and a comparative analysis of the legislation on information protection and the main methods of its protection in certain leading foreign countries. Special attention was paid in the article to the features of information security, namely information protection in certain foreign countries for the purpose of studying and introducing the best methods of information security into the practice of our state. The authors proved that the new model of information protection should take into account the development of an effective state policy on the protection of information in electronic registers in accordance with EU legal standards; creation of the Institute of the Commissioner for Information Protection; in accordance with the EU norms, the introduction of specialists in matters of personal data protection at enterprises. Since the modern system of information protection in Ukraine does not guarantee the protection of privacy and personal data of a person and a citizen, the co-authors of the article suggested making appropriate changes to the current legislation in order to bring it into line with EU legal standards. The article also proposes a new model of information protection in Ukraine, taking into account the experience of foreign countries

Keywords: privacy; security; protection; legal regulation; personal data; foreign countries; foreign experience

Suggested Citation:
Mentukh, N., & Shevchuk, O. (2023). Protection of information in electronic registers: Comparative and legal aspect. *Law, Policy & Security*, 1(1), 4-17.

*Corresponding author

INTRODUCTION

Information in society is not only a subject of professional exchanges, a resource for making managerial decisions, a means of ensuring a higher quality of life. Information increasingly functions as an object of criminal encroachment, a means of competitive struggle of business structures, and even a weapon of information wars.

That is, modern society, as noted by O.R. Shevchuk and N.F. Mentukh (2021) is called informational, because information forms the most important element of his vital activity. Information protection is one of the most necessary tasks in the functioning of the entire state and, accordingly, in the activities of individual large or small enterprises. In the 21 century, this fact is considered obvious.

Therefore, the relevance of the chosen research topic lies in the scientific analysis of the theoretical foundations of information protection in electronic registers, a thorough study of foreign experience in this field, in the identification of theoretical and practical problems that arise in the implementation of information protection in electronic registers, as well as in the creation of reasonable proposals and methods solving established problems.

Before starting the analysis, it is necessary to clarify the essence of the main concept in this topic . Therefore, authors consider it appropriately to analyze separate scientific statements regarding the definition of the point of the concept of "information security".

Usually, information security refers to the quality of the object's security, which is most often represented by information, system resources, data, etc. That is, information security, as noted by H. Yarovenko (2020), is a complex concept that covers security at the macro and micro levels, and also includes the legislative framework, bodies that ensure information security, software and hardware security, security policy and field specialists. Therefore, the issue of ensuring information security, according to A.V. Wojcikhovskyi (2020), is quite important at the current stage for the Ukrainian state, which, first of all, is due to the need to resist certain illegal encroachments on the information space of Ukraine.

As noted by some researchers (Ording *et al*., 2022), relevant provisions, legislation and other constitutional norms act as a powerful tool in society and play a vital role in the development of information security both at the national and international levels.

One of the the most pressing problems of modern society is conducting informational wars, protecting information in electronic registers. The main weapon and advantage in such wars, of course, is the possession of information. For these reasons, data protection is becoming a necessity in the world.

It is worth noting that today's military practice clearly demonstrates that information is a weapon of "mass destruction". Therefore, it is necessary to create an effective mechanism by which it is possible to ensure state information security and respect for human rights, and, at the same time, to provide an opportunity for people not to feel invasion on freedom and democracy.

The organizational and legal mechanism of the state policy of information security, as noted by V. Panchenko (2020) is an ordered set of state bodies that are involved in the process of forming, ensuring and implementing informational security policy, as well as internal and external social relations regulated by the system of legal norms and principles in the information field.

The article examines the issues of information protection in electronic registers, as well as countries that have managed to establish themselves as information states. The degree of protection of information in electronic registers of Ukraine is compared with other countries.

The purpose of the scientific research is to analyze scientific approaches to the definition of the concept of "information security", "information protection" in electronic registers, as well as a comparative analysis of the main methods and mechanisms of information protection in electronic registers in Ukraine and some foreign countries.

This research is based on two hypotheses, which are as follows:

1) the modern system of information protection in Ukraine needs to be adjusted with EU legal standards, in particular, the introduction of foreign experience, as well as the introduction of the position of the Ombudsman for the protection of personal data;

2) in Ukraine, it is necessary to develop and implement (taking into account the experience of foreign countries) a new model of information protection, which would include: development of an effective state policy on information protection in electronic registers in accordance with EU legal standards; introduction of the Institute of the Commissioner for Information Protection; in accordance with EU norms, introduction specialists on personal data protection.

LITERATURE REVIEW

The concept of "information security" is currently one of the basic concepts in information law. As noted by some researchers (Alrebdi *et al*., 2022), it is a set of measures, including organizational and technical ones, that are taken to ensure a number of necessary requirements: protection, integrity, availability and manageability of information arrays. Correct and reliable data protection strengthens the sovereignty, defense capability, position of the state in the world, provides reliable support for the preservation of state secrets.

Studies of D. Bell (1980) are devoted to this problem, in which he examines social section of the information

society and perspectives of its dynamics. A. Duff (1998) became a follower of D. Bell's scientific research, continuing his research on the social structure of the information society. D. Lyon (1986) in his scientific work highlights new social transformations from "post-industrialism" to "information society", Y. Masuda (1981) studied the information society, considering it as a post-industrial society, A. Toffler (1980), D. Herrmann & H. Pridöh (2020) explored fundamental concepts and models of cyber security.

In their works, these authors investigated the concept of "information security" and its essential meaning. In their opinion, the emergence and scientific consolidation of the definition of "information security" is directly related to the understanding of the phenomenon of informatization and the study of the content of the process of forming an information society. That is, information security is a multifaceted and multi-directional field of activity, success in which can only be achieved by the use of systematic and complex approaches in its analysis.

It is worth noting that in 1991, European countries developed the "Information Technology Security Evaluation Criteria"[1], which, in particular, define the tasks of ensuring information security. So, in order to ensure the confidentiality and integrity of information resources, the issues of ensuring the protection of information resources from unauthorized modification or destruction, from unauthorized access, as well as the issue of ensuring by means of countering the threats of denial of service of systems are defined.

In 1996, European information security standards were established in the "Common Criteria for Information Technology Security Evaluation"[2], according to which the CIA TRIAD model is used to characterize the main criteria of information security, which provides for three main features of information security, namely: confidentiality, availability and integrity.

In 2001, the European Commission presented the document "Communication from the European Commission: Network and Information Security: Proposal for a European Policy Approach"[3], which marked the current approach of the EU to the problem of information security. This document uses the term "network and information security", which is interpreted as "the ability of a network or information system to resist accidental events or malicious actions that threaten the availability, authenticity, integrity and confidentiality of data stored or transmitted, as well as services, provided through these networks and systems.

European standards of information activity of public authorities provide for issues of maximum information openness, with the exception of restrictions related to issues of information confidentiality (first of all, ensuring the security and protection of personal data). The main document regulating the right of EU citizens to the protection of personal data is Directive 95/46/EU "On the protection of natural persons during the processing of personal data and on the free movement of such data"[4]. Among these norms, we can also note "Principle of Guaranteed Security No. 11"[5], which enshrines the requirement that "personal data shall be protected by reasonable security measures against threats such as loss or unauthorized access, destruction, use, modification or disclosure". Approved on April 14, 2014, new personal data protection regulations (GDPR) entered into force in 2018[6]. The innovations include the introduction of a more severe punishment for late notification of information about a data leak. The need to obtain users' consent to the processing of their personal data, which must be free, conscious and specific, and can also be revoked at any time, is provided by the directive. In his work R.Yu. Prav (2019) notes that given the importance of information for modern people, societies, states and the international community, there is no doubt that, in addition to the obvious benefits that information can bring, it can also be exposed to threats arising from various factors.

In addition to the fact that the problem of information security attracts the attention of a significant number of scientists, today there is a lack of a unified and systematic scientific study of the issue of improving the protection of information in electronic registers in comparison, including international experience.

MATERIALS AND METHODS

Because the focus of the research is concept of protection of information in electronic registers, the main mechanisms of information protection in electronic

[1]Information Technology Security Evaluation Criteria. (1991). Retrieved from https://www.ssi.gouv.fr/uploads/2015/01/ITSEC-uk.pdf.
[2]Common Criteria for Information Technology Security Evaluation. (2012). Retrieved from http://www.commoncriteriaportal.org/files/ccfiles/CCPART2V3.1R4.pdf.
[3]Communication from the European Commission: Network and Information Security: Proposal for a European Policy Approach. COM. (2001). Retrieved from http://ec.europa.eu/information_society/eeurope/2002/news_library/pdf_files/netsec_en.pdf.
[4]Directive 95/46/EU of the European Parliament and the Council "On the Protection of Natural Persons During the Processing of Personal Data and on the Free Movement of Such Data". (1995, October). Retrieved from http://zakon2.rada.gov.ua/laws/show/ 994_242
[5]Interpreting the Security Principle. (2007, March). Retrieved from http://www.cyberlawcentre.org/ipp/wp/WP1%20Security.pdf.
[6]Statement by Vice-President Ansip and Commissioner Jourová ahead of the entry into application of the General Data Protection Regulation. Regulation (EU) No. 2018/1725. (2018). Retrieved from https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_18_3889.

registers were investigated with the help of conceptual analysis.

The logical-semantic method was used in the formulation of the categorical apparatus, in the process of researching and structuring the main tasks of information protection, as well as for the empirical analysis of the main means of countering information security threats in computer systems.

The authors applied sociological methods (content analysis, synthesis, discourse analysis, statistical arrangement) of accumulation, rethinking and systematization of information.

The use of the comparative-historical method, in particular the retrospective-chronological method, made it possible to identify and compare the history of the creation of electronic registers in Ukraine and certain foreign countries; cross-national analysis made it possible to distinguish such important and fundamental categories as information security and information protection; cross-temporal analysis was used to form information protection mechanisms in electronic registers in the period of threats.

A previous search of the results found many cases of erroneous results, so the search needed to be refined. For example, specific search results related to other aspects of information security in general, rather than the issue of information protection in electronic registries.

Although, the diversity of research is explained by the fact that there are different comparative forms of research (case studies, binary studies, cross-temporal and cross-regional studies), as well as various research strategies – oriented to theoretical data and oriented to empirical data , which differ in both methodological and empirical effectiveness and are used in the comparative analysis of forms and methods of information protection.

The research was carried out in three stages.

At the first stage of the research, with the help of special scientific methods (comparative analysis, analysis of expert positions), information is collected and processed about the most effective practices of information protection in electronic registers.

Atthe second stage, the study of the correlational impact of the level of information protection in electronic registers and the introduction of the position of the Ombudsman for the protection of personal data will be carried out.

At the third stage, a model of information protection in electronic registers was formed on the basis of the conducted research.

RESULTS AND DISCUSSION

The content of the phenomenon of information protection

Today, the informatization process of the modern world determines the level of information security, based on the need for multifaceted protection of information, regardless of the location of its carriers.

Information security is the state of data security, which ensures their availability, confidentiality and integrity. In this case, the availability of data refers to their property, which determines the possibility of obtaining it and further use at the request of authorized persons, under confidentiality – the property related to the fact that that data will not become available to third parties without the consent of authorized persons, and under integrity – immutability of information in the process of storage or transmission. In other words, to protect information, it must be:

1) sufficiently protected against hacking from the outside;

2) operated by a sufficiently educated person;

3) inaccessible to unauthorized persons.

Information protection is a set of measures aimed at ensuring information security.

In their work the researchers (Degtyareva & Miroshnykova, 2018) note that the widespread use of specialized and global information systems (IS) in government bodies, in transport, in health care structures and in the field of state-building gives the ability to accumulate and transfer huge amounts of valuable information. At the same time, the widespread use of IS makes system data vulnerable to uncontrolled access to protected information, increasing the risks and dangers of unauthorized influences on information in these systems.

The factors of IS vulnerabilities include a relatively large amount of the danger of internal information threats, the widespread use by criminal structures of devices for secretly obtaining information, and the increase in the number of crimes in the field of computer information. Regarding the protection of information, the following definitions are the most successful.

So, P.K. Yeng (2022) notes in his work that "information is data that eliminates the uncertainty that existed for the consumer before receiving it".

Some researchers (Westin & Louis, 1970) note that information is defined as a structured way of presenting raw data after processing, generalization and transformation. Data is processed, stored and exchanged in a certain way, and the system essentially represents it. Through the use of a computer-based information system (CBIS), data is collected, processed, stored, analyzed and transformed in a meaningful way. Information privacy is defined as the right of an individual to personal data who can manage the data and decide to what extent personal data will be shared with others.

In turn, as noted (Fei Wu *et al*., 2020), the development of privacy should go beyond the basic mechanisms of protection of already created personal data,

and instead develop creative ways of directing both individuals and organizations to preventive behavior in various contexts. Viewing privacy from a contextual approach is more complex, but it more accurately reflects the reality of data sharing and privacy management in the 21st century.

However, as the information collected, processed, stored and analyzed by organizations is concerned with information privacy, it is becoming an increasingly serious concern for data security, information privacy and the corresponding compliance status. This collection and storage of information, as scientists D.K. Rath & A. Kumar (2021), caused two main information problems:

a) security problem

b) confidentiality.

In general, in information law (Mantelero & Vaciago, 2022) general and legal properties of information are distinguished. There are also properties of information that characterize its quality for decision-making, that determine the state of information security, etc. (Fig. 1).

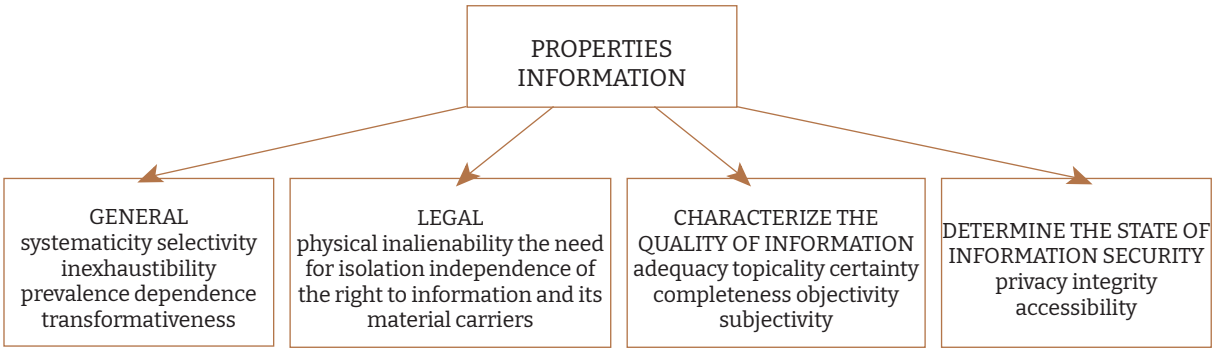

Figure 1. Main properties of information

Also according to S. Carey (2021), such a property of information as observability is sometimes defined, which is becoming more and more vital for software developers who strive to create better and more stable programs. That is, this property is under the control of the protection system all the time (at all stages of processing and transmission).

In his research W.H. Zurek (1990) noted that conventional information theory works mainly with computers and technological communication systems; he is interested not so much in the independent formal definition of "information" as in the exact mathematical expression of the information content of a given message and its deterioration during transmission, processing and storage.

By the protection of information O. Gstrein & A. Beaulieu (2022) understands "activity that involves a complex of legal, organizational and (or) technical measures, as a result of which the risk associated with information causing harm to the individual, society and the state is minimized".

In his work R.M Adelman (2018) writes about the provision of information security as a complex phenomenon that includes a security object, which, in turn, is formed due to the aggregate of the state's needs for information and functions for the implementation of these needs, threats to its security and countermeasures against them, including subjects of countermeasures.

R. Creemers (2022) notes that information protection is one of the most necessary tasks in the functioning of the entire state and, accordingly, the activities of individual large or small companies. In the 21st century, this fact is considered quite obvious.

It should be noted that regarding the concept and problem of information security, the existing positions of scientists reveal both the presence of common visions and different ones, where the specifics of each scientific approach in particular can be traced. From this it emerges that at the expense of coordinated and unified political, organizational, socio-economic, military, legal, informational, special and other measures, it is possible to solve the problems of information security.

In his work S.O. Lysenko (2019) notes that, according to legal researchers, there are methodological differences in the understanding of information security at different levels of social relations (national, regional, state, individual organizations). A separate approach is applied to the legal representation of the protection organization of the Unified State Register of Executive Proceedings of Ukraine. This approach differs from the approach to local network security in an individual company. This makes it necessary to define such uniform methods of regulation, models of protection and protection of information regarding any subject.

The main goal of information security, as noted by some researchers (Orozova *et al.*, 2019) is the protection of data and information from possible harmful malicious actions, such as: unauthorized access, use, disclosure, modification, reading, writing and destruction; and also

to minimize harm in case of such intervention. Information protection includes: risk management practices related to the use, operation, storage and transmission of information; systems and processes used for this.

D.W. Jr Straub & R.W. Collins (1990) claimed, that today, security is a major concern for the protection of individual information. That is, information security means the protection of information from accidental or intentional influences of a natural or artificial nature that threaten to harm the owners or users of information. The protection of information means a set of methods and means that ensure the integrity, confidentiality, reliability, authenticity, and availability of information in the conditions of exposure to threats of a natural or artificial nature.

Foreign experience of information security

Ukraine realized the need for data protection at the state level only relatively recently, while the United States of America adopted the first law on information protection in 1906. Today, after more than a century of long-term formation in this field, the US has approximately five hundred different legislative acts that are directly related to this field. Ukraine, in turn, obviously does not have such a variety of information security laws.

So, for example, as noted by R. Ducato (2020), some laws were fixeted by legislation even before the beginning of the year two thousand: "On Freedom of Information" (1967); "About Secrecy" (1974); "On the Right to Financial Secrecy" (1978).

Researchers (Chernovol & Charskykh, 2020) point out that by its very nature, the information policy of the USA arises on the basis of the national security strategy, foreign policy doctrine, and military doctrine, and they, therefore, differ significantly in the implementation of the political courses of various American presidents. It is worth noting that regardless of the carrier of information, the concept of information protection applies in the USA, and therefore, its protection is carried out on general grounds (as well as material values).

This concept, as Zh.V. Udovenko notes (2020), is implemented through the "CSA" standard, which was adopted in 1996. This standard applies to all NATO member countries and contains a number of the most important principles regarding the regulation of public relations in the field of personal data protection.

In her work N.V. Kushakova (2003) notes that "laws adopted by the American Congress relate to certain specific problems (precedents) arising in the process of active use of information technologies, in particular the Internet, as well as aimed at protecting the right to information or its possible restrictions in connection with the detection of a negative impact on other members of society or society in general". Comparing the normative basis of Ukraine and the USA, it will be neccesery to note that in Ukraine it is more defensive in nature, aimed at preserving sovereignty, state secrets, and strengthening the country's defense.

Great Britain is also a state with one of the most developed information infrastructures in the world. Its authorities realized the importance of developing legislation in the field of ensuring data protection much earlier than other European countries. The strictest concept of information protection organization is currently in full-force in the country. In Great Britain in 1984 the law "On Data Protection" was adopted[1].

In accordance with the Data Protection Act[1] dated 12.07.1984, the Institute of the Representetive for Personal Data operates in Great Britain. This law defines the positions of the Minister, whose competence is assigned to the issue of personal data protection, the Registrar and established the Data Protection Court. That is, this legislative act outlines the legal basis for the protection of personal data. Information security in the UK has its own history and characteristics. Great Britain does not have its own Constitution. However, the British Parliament passed the Human Rights Act in 1998, which gave force of law to the European Convention on Human Rights, which entered into force in October 2000.

Also, in July 1998, the British Parliament adopted the Information Protection Act[2], which brings the similar act of 1984 into compliance with the requirements of the Information Protection Directive adopted by the European Union. The norms of this law are aimed at accounts maintained by state institutions and private companies. Also, this law provides for the imposition of a number of restrictions on access to accounts and the use, on this basis, of personal data.

This act provides for the rules, conditions and procedures for the supervision and protection of information, both in paper and electronic form. In addition, the main rules and principles are fixed in the content of this legislative act, namely: the principle of information security; information must be timely; all information must be legal and reliable; information must be relevant and adequate; information may be used only on legal grounds; information should be provided only at the request of users; must be completed for a certain period of time (not longer than necessary); information can be provided only to those countries that can ensure its adequate protection; information must contain sources.

[1]Data Protection Act. (1984, July). Retrieved from https://www.legislation.gov.uk/ukpga/1984/35/enacted.
[2]Data Protection Act. (1998). Retrieved from https://www.legislation.gov.uk/ukpga/1998/29/contents.

Government Cyber Security Strategy for 2022-2030[1] pursues the main goal – by 2025, critical government functions must be significantly protected from cyber attacks, and all government organizations throughout the public sector will be resilient to known vulnerabilities and attack methods by 2030 at the latest.

The policy for the protection of state secret information in Great Britain is defined by the Security policy framework (SPF)[2]. The SPF contains key security policy principles and guidance on security and risk management for UK government agencies and relevant authorities. The SPF contains about 70 recommendations, which are grouped into 7 sections, in the field of information security policy:

1) personnel responsible for security information;
2) risk management;
3) ensuring information security;
4) access control and information classification;
5) physical protection;
6) business continuity;
7) anti-terrorist activity.

In 2018, the Data Protection Act 2018 was adopted[3]. The Data Protection Act 2018 is the UK's implementation of the General Data Protection Regulation (GDPR).

However, as noted by some researchers (Addis & Kutar, 2018) GDPR is an extremely complex piece of legislation whose importance and implications are not yet fully understood by most UK organisations. Anyone responsible for the use of personal data must follow strict rules called "data protection principles". They must ensure that the information:

- be used fairly, lawfully and transparently;
- is used for specific, clear purposes;
- is used in a way that is adequate, relevant and limited to what is necessary;
- accurate and, where necessary, updated;
- stored no longer than necessary;
- processed in a manner that ensures adequate security, including protection against unlawful or unauthorized processing, access, loss, destruction or damage.

There are stronger legal protections for more sensitive information such as: ethnic origin, political views, religious beliefs, trade union membership, genetics, biometrics (if used for identification), health, sex life or orientation.

There are separate safeguards for personal data related to convictions and offences. Any organization in Great Britain must independently take care of the protection of its own commercial secrets, in connection with which large companies are forming their own security services. The state organization for ensuring the security of the country is built based on the definition of information warfare as operations capable of causing significant damage to the information system of the enemy, while protecting one's own systems, which can be called the optimal tactic.

Germany, without a doubt, can be called the undisputed leader among European countries in the field of regulation of the protection of personal information, its submission at the legislative level. To this day, Germany is considered one of the world leaders in the field of privacy and personal data protection. Starting from the middle of the 20th century. legislation on the protection of personal data began to take shape in Germany. Thus, in 1970, the first normative act in the world was adopted, which regulated issues of personal data protection. This regulatory act was proposed by the federal state of Hesse, and later by other federal states.

It is worth noting that the German federal law "On Data Protection" of 1977[4] provided for two main tasks, which were as follows: on the one hand, using new information technology to prevent interference in the private sphere of German citizens; on the other hand, in connection with the emergence of "informational advantages" of executive authorities over parliamentary bodies, to prevent changes defined in the Constitution of the state concerning the distribution of their powers.

German citizens have the right to make their own decisions about the disclosure of their personal data, and an independent personal data protection officer protects their rights in this matter. Today, the protection of personal data in the state is carried out in accordance with the provisions of the federal law "On Further Development Of Data Processing And Protection" dated 12.20.1990[5]. According to this legislation, personal data are protected only if they perform a certain public or economic function of life and are used in private life.

It should be noted that today this law is considered one of the strictest data protection laws in the European Union. The final version of the review took place in August 2002, in order to bring German legislation into line with EU requirements. The general purpose of this law is the following – "protection of individuals from violation of their personal rights".

[1]Government Cyber Security Strategy 2022-2030. (n.d.). Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1049825/government-cyber-security-strategy.pdf.
[2]Security policy framework (SPF). (2022, December). Retrieved from https://www.gov.uk/government/publications/security-policy-framework/hmg-security-policy-framework.
[3]Data Protection Act. (2018). Retrieved from https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted.
[4]German Data Protection Act of 1977. (1977, February). Retrieved from https://www.datenschutz-wiki.de/BDSG_1977.
[5]Law "On Further Development of Data Processing and Protection". (1990, December). Retrieved from https://www.iuscomp.org/gla/statutes/BDSG.htm.

So, in Germany, the protection of personal data is clearly regulated at the legislative level and is really ensured in practical activities and life in general. Equally important is the fact that in this country the legislation on the protection of personal data is based on provisions arising from the principle of informational self-determination, while providing the opportunity for each citizen to manage his personal data independently. However, under the condition that he must disclose this information in the interests of the state, the questions of state institutions regarding him should be limited to the necessary minimum, such as paying taxes, etc. The use of personal data of citizens is also prohibited in Germany, although in cases established by law, permission to collect and use this data is possible.

It should be noted that with regard to Internet security and information protection, such actions as:

- transfer of greater responsibility in the creation of the information society to business;
- government uses all legal means to prevent the spread of xenophobia, anti-Semitic and neo-Nazi ideas on the Internet;
- in order to develop preventive security measures and increase the ability to resist threats, it is envisaged to create "computer emergency response teams" (Computer Emergency Response Teams, CERT) in federal authorities;
- an information support organization named "Renewal of Germany" (Deutschland erneuern) is aimed at more active use of the Internet as a means of disseminating information and expanding relations with the public. In turn, the Deutschland portal will give German and foreign users access to information about Germany, including the provision of information about the government and public administration bodies, as well as about culture, business, science and education, and tourism[1].

German legislation establishes the obligation to observe the regime of confidentiality of information by officials of state control bodies and provides for liability for its disclosure, up to criminal liability. As noted A. Mantelero & G. Vaciago (2017). German procedural law provides for guarantees of confidentiality of know-how in the judicial process.

The German understanding of information protection and information warfare is as follows: the offensive and defensive components are combined into a single whole, and foreign states are separated from non-state organizations, being considered separately.

It seems appropriate to draw attention to the experience of France, where the Institute of the Commissioner for the Protection of Personal ("Nominative") Data functions on the basis of the Law "On Informatics, File Archives and Freedoms" dated November 6, 1978[2].

In France, the protection of confidential information forms the basis of the application of general norms of civil, labor and criminal law.

French legislation, as noted A. Mantelero & G. Vaciago (2017), includes the following areas of protection:

1) within the limits of labor relations, the employee is obliged to maintain the regime of information confidentiality, the employee has no right to compete with the employer after dismissal;

2) provided for civil liability for "breach of trust", i.e. for the disclosure of a commercial secret by a person entrusted with it by the owner;

3) criminal liability is provided for state officials and officials of control bodies for disclosing confidential information.

Issues of information security in France are dealt with both by state structures, and non-governmental organizations participate in this process. Each French police department has its own dedicated information crime unit in each region.

Three information security services operate under the leadership of the French Ministry of Defense: the General Directorate of External Security (1982), the Office of Military Intelligence (1992) and the Office of Military Counter intelligence (1981). The total composition of the French intelligence community is approximately equal to 12,779 employees.

It is worth noting that this was also connected with local events, due to which the French government developed a project of a single registry of citizens' data for social insurance. With the help of automated programs, it was planned to process all this information. In connection with this, the newspaper Le Monde published an article "SAFARI ou la chasse aux Français" ("Safari or the hunt for the French") (Safari et la (nouvelle)...2010), which criticized this kind of intention on the part of the state. Public pressure also contributed to the adoption of the aforementioned act.

In France, the main elements of the personal protection system include the following:

- issuance of an order on violation, warning and appeal to the prosecutor's office, appeal of illegal actions in court (Articles 21, 35 of the Law of 1978);
- supervision and control (verification of applications, complaints, etc.) on compliance with data protection requirements (Chapter II of the 1978 Act), document verification (Article 21 of the 1978 Act);

[1]The Portal of the Federal Government. (n.d.). Retrieved from https://www.bundesregierung.de/breg-en.
[2]The French Law "On Informatics, File Archives and Freedoms". (1978, November). Retrieved from https://www.legifrance.gouv.fr/loda/id/LEGISCTA000006095896.

► granting permission for access to the National Register and processing of personal data (Articles 18, 19 of the Law of 1978), for the transfer of data abroad (Article 24 of the Law of 1978);

► maintenance of the National Register of Identification of Individuals (Decree of January 22, 1982 No. 82-103)[1], which is carried out by the National Institute of Statistics and Economic Research. Such information as: first name, last name, gender, date and place of birth, date and place of death, the last name of the closest relative on the male line, numbers of birth and death certificates are entered into the Register to identify people with the same surname. In addition, notations about a change in a person's marital status are made to the Register; the number given to each person, and certain indicators are entered for data search.

It is worth noting that persons guilty of violating personal data protection issues are subject to administrative and criminal (chapter 4 of the 1978 Law) liability. Also, French legislation on information protection is being improved every year, especially at the beginning of the 21st century after the creation of the EU, since the legislation on information protection applies to all EU countries, including France. In Poland the law "On Protection of Personal Data" was adopted, which was approved in October 1997 and entered into force in April 1998[2]. This Law is based on the EU Directive on the protection of personal data.

It is worth noting that the Ministry of Internal Affairs and administrations issued a resolution in 1998 establishing security standards for information systems containing personal information. In August 2001, this Law was changed in order to bring it into full compliance with the requirements of the EU Directive on the protection of personal data. The rules regarding the automated processing of personal data, definition of personal data, provisions on the legality of information processing, etc. were also changed.

Control over the implementation of the Law "On Personal Data Protection" is entrusted to the office of the Inspector General for Personal Data Protection. In addition, in January 1999, the Law "On the Protection of Confidential Information" entered into force[3], the adoption of which is connected with the condition of Poland's accession to NATO. The provisions of this law apply to classified information and data collected by state structures, "the disclosure of which may harm state or public interests, or the interests of citizens or organizations protected by law".

Parliament of Hungary in November 1992 was accepted Law "On Protection of Personal Information and Access to Information of Public Interest"[4].

In accordance with the Law "On the Protection of Data of Individuals"[5], adopted by the Seimas on June 21, 2018, the issue of information protection is being handled in Latvia. This law regulates issues related to the protection of personal data.

Processing of personal data is allowed only in the case when the law does not provide otherwise, and due to the existence of one of the following conditions: data processing results from the contractual obligations of contractual data subjects; consent of the data subject; data processing is necessary to protect the vital interests of the data subject, including life and health, etc. This law regulates the protection of the personal data processing system.

Also in Denmark in order to implement Directive 95/46/EU on the protection of personal data and the free movement of such data, the "Law on the Protection and Processing of Personal Data was adopted in 2000, which came into force on July 1, 2000, enabling people to access[6] their records, which are in the possession of private organizations and state institutions. Datatilsynet (Data Protection Agency) enforces the law, which was amended in 2007. At the legislative level, the basic principles of information protection are established and it is determined which data must remain classified and which can be made available to the general public.

Regarding the storage and protection of personal data, as well as reliable electronic identification of a person, the experience of Denmark may be relevant for solving these problems in Ukraine.

In the context of the above, the experience of some researched and other European countries regarding the construction of a personal data protection system, shown in Table 1, seems interesting.

[1]Decree No. 82-103 relating to the national directory for the identification of natural persons. (1982, January). Retrieved from https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000520382.
[2]Act "On the Protection of Personal Data". (1997, August). Retrieved from http://fra.europa.eu/en/law-reference/act-august-29-1997-protection-personal-data.
[3]Act "On the Protection of Classified Information". (2010, August). Retrieved from https://www.global-regulation.com/translation/poland/2986485/the-law-of-5-august-2010-for-the-protection-of-classified-information.html.
[4]Hungarian Law "On the Protection of Personal Information and Access to Information of Public Interest". (1992, November). Retrieved from https://mkogy.jogtar.hu/jogszabaly?docid=99200063.TV.
[5]The Law "On the Protection of Personal Data", adopted by the Latvian Seimas. (2018, June). Retrieved from https://www.dk.lv/rus/news/26504/.
[6]The Danish Act "The Act on Processing of Personal Data". (2000, July, May). Retrieved from https://www.retsinformation.dk/eli/lta/2000/429.

Table 1. Organization of information protection in the studied and other European countries

Country	Name of the law, date of adoption	Availability of electronic registers, database registration	Authorities authorized to protect information
Great Britain	"About Data Protection", 12.07.1984	all data	Minister for Data Protection. The Information Representetive (Data Protection Registrar) – heads the Data Protection Bureau and information law regulator in the UK and Data Protection Court
Denmark	"About Data Registers", "About Data Protection", 06.08.1982	some data	The Data Supervisory Authority (consists of the Council and the Secretariat). Accountable to the Parliament
Spain	"On Regulation of Automated Processing of Personal Data", 29.10.1982	all data	Commissions of the Parliament and Data protection ombudsmen. Accountable to the Parliament
Italy	"On the Protection of Persons in Connection with the Automated Processing of Personal Data", 01.021982	some data	Data protection ombudsmen
Latvia	"About Security Physical Data People", 2000	some data	Data Protection Inspectorate
Germany	Federal laws: "On Data Protection", (1978); "On the Further Development of Data Processing", 20.12.1990	all data	The Federal Data Protection Commission of the Bundestag and The Data Protection Commissioner is the head of the Institute of the Commissioner for Personal Data Protection. An elected public office, established by the Law, has the rights of sole authority and complete independence from power structures. Has the right to supervise the activities of any bodies related to the processing of personal data. Accountable to the Bundestag. Cooperates with the Minister of Police in order to carry out inspections and stop offenses in organizations and enterprises.
Poland	"On Personal Data Protection", adopted in October 1997 and entered into force in April 1998	some data	Inspector General of Personal Data Protection
Portugal	"About Protection of Personal Data", 29.04.1991	all data	National Commission and Personal data protection ombudsman
Hungary	"On Data Protection and Access to Information of Public Interest", 10.11.1992	all data	The Commissioner for Information Protection heads the Institute on issues protection of personal data. Appointed by the decision of the Parliament
France	"About Informatics, Filing Cabinets and Freedoms", 06.01.1978	some data	National Commission on Data Processing (Informatics) and Freedoms. It is elected and accountable to the Parliament and the President. Information Commissioner – heads the French Agency for the Protection of Personal Data. Appointed by the decision of the Prime Minister
Sweden	"About Data Protection", 13.05.1972	some data	Inspection Council and Data Protection Ombudsman. Accountable to the Parliament

Source: developed by authors

In confirmation of the first research hypothesis, which is that the modern system of information protection in electronic registers does not guarantee the protection of a person's privacy and personal data, and is such that it does not comply with certain constitutional norms and requires compliance with EU legal standards, especially the implementation of foreign experience, regarding the introduction of the position of the Ombudsman for the protection of personal data, it is worth noting that back in 2014, Ukraine in within the framework of the Association Agreement with the European Union, undertook to ensure the appropriate level of information protection in electronic registers in accordance with the highest international standards, documents of the Council of Europe (Article 15 of the Agreement). For this, as noted by V. Fisun (2020), in addition to improving the legislation, it is necessary to work on the development of the control system, as well as the ability of all subjects to ensure information protection. In the spring of 2020 there was a large-scale leak of personal data of Ukrainian citizens, mainly from driver's licenses, so suspicion immediately fell on the "Diya" program.

After some time, the authorities denied the involvement of the program. The real cause of the data leak has yet to be established. However, not only the rights of the users of the application were violated, but also the rights of millions of other people.

In addition, on the night of January 13-14, 2022, hackers launched a global attack on the websites of the Cabinet of Ministers of Ukraine and individual ministries. Afterwards, the website of state services "Diya" was temporarily unavailable. Information about a possible leak of data on more than 2 million Ukrainian citizens was also received in a few days (Ukraine was hit by..., 2022).

Taking into account all of the above, it is considered appropriate to pay attention to the possibility of deleting the personal data that have been provided. The Law of Ukraine "On the Protection of Personal Data"[1] provides for this possibility, although it cannot be done at the wish or request of a person, and for this it is necessary to obtain an order from the Ombudsman or a court notice. However, this kind of procedure can last for more than a month, taking into account the workload of these organs. Along with this, the following methods of rights protection can be effective.

On the basis of the comparative analysis, we confirm the second research hypothesis that it is necessary to develop and implement (with reference to foreign experience) a new model of information protection in Ukraine, which requires the following:

- to develop an effective national policy regarding the protection of information protection in electronic registers in accordance with EU legal standards;
- introduction of the institution of the Information Protection Representative, who is accountable to the Verkhovna Rada of Ukraine, whose main functions include: improvement of legislation in the field of information protection in electronic registers and interaction with authorized bodies of EU member states and the Council of Europe on information protection in electronic registers ; implementation of parliamentary control;
- in accordance with the provisions of the EU legislation, to introduce specialists in matters of information protection in electronic registers or entrusting these functions to individual employees of these organizations in bodies, institutions, institutions, enterprises and organizations of relevant officials.

CONCLUSIONS

Thus, on the basis mentioned above, the following can be noted: information security in Ukraine is given significant attention, many measures have been taken to ensure it, a number of legislative norms have been adopted, and special authorities are active. However, there are significant drawbacks.

In Ukraine, the modern information protection system does not guarantee the protection of privacy and personal data of a person and a citizen does not comply with certain constitutional norms and needs to adjusted with EU legal standards. For this purpose, the authors of the study conclude that in Ukraine it is necessary to develop and implement (taking into account the experience of foreign countries) a new model of information protection, which would include:

- development of an effective state policy on information protection in electronic registers in accordance with EU legal standards;
- creation of the Institute of the Representative for Information Protection, which would be accountable to the Verkhovna Rada of Ukraine, the main functions of which would include: control, improvement of legislation on personal data protection and interaction with authorized bodies of the Council of Europe and EU member states on information protection issues, protection of personal data;
- in accordance with EU norms, to introduce in bodies, institutions, institutions, enterprises and organizations the relevant officials, experts on personal data protection issues or assigning these functions to individual employees of these organizations.

Comparing the level of development of this field with other countries, it can be said that it, in general, it was established there much earlier and, therefore, has a more prominent base. Many data protection methods and concepts adopted in the listed countries are more effective. The perspective of further scientific research is the study of the development of the system of specialized sublegal acts in the field of information protection in electronic registers aimed at improving its legislative, organizational and technological basis. The subject of scientific research will also be the legal and fair resolution of information disputes, the emergence of which is a natural result of the development of information relations in modern society.

ACKNOWLEDGEMENTS

None.

CONFLICT OF INTEREST

None.

[1]Law of Ukraine No. 2297-VI "On Protection of Personal Data". (2010, June). Retrieved from https://zakon.rada.gov.ua/laws/show/2297-17#Text.

REFERENCES

[1] Addis, C., & Kutar, M.S. (2018). *The general data protection regulation (gdpr), emerging technologies and UK organisations: Awareness, implementation and readiness.* Retrieved from https://aisel.aisnet.org/ukais2018/29.

[2] Adelman, R.M. (2018). Going small: Urban social science in the era of Big Data city & community forum on census data. *City & Community*, 17(3), 550-553. doi: 10.1111/cico.12328.

[3] Alrebdi, N., Alabdulatif, A., Iwendi, C., & Zhuotao, L. (2022). SVBE: Searchable and verifiable blockchain-based electronic medical records system. *Scientific Reports*, 12, article number 266. doi: 10.1038/s41598-021-04124-8.

[4] Bell, D. (1980). The social framework of the information society. In *The microelectronics revolution* (pp. 500-549). Oxford: Blackwell.

[5] Carey, S. (2021). *What is observability? Software monitoring on steroids.* Retrieved from: https://www.infoworld.com/article/3607980/what-is-observability-software-monitoring-on-steroids.html.

[6] Chernovol, I.O., & Charskykh I.Yu. (2020). US information security: Problems and challenges in the age of Donald Trump. *Bulletin of the Student Scientific Society of Donetsk National University named after Vasyl Stus*, 12(1), 110-115.

[7] Creemers, R. (2022) China's emerging data protection framework. *Journal of Cybersecurity*, 8(1), article number tyac011. doi: 10.1093/cybsec/tyac011.

[8] Degtyareva, L., & Miroshnykova, M. (2020). *The problems of the security of information transport and logistics systems*. Retrieved from http://reposit.nupp.edu.ua/bitstream/PoltNTU/5964/1/2019_%D0%98%D1%81%D0%BF%D0%B0%D0%BD%D0%B8%D1%8F.PDF.

[9] Ducato, R. (2020). Data protection, scientific research, and the role of information. *Computer Law & Security Review,* 37, article number 105412. https://doi.org/10.1016/j.clsr.2020.105412.

[10] Duff, A.S. (1998). Daniel Bell's theory of the information society. *Journal of Information Science,* 24(6), 373-393. doi: 10.1177/016555159802400601.

[11] Fei Wu, Ph., Vitak, J., & Zimmer, M. (2020). A contextual approach to information privacy research. *Journal of the Association for Information Science and Technology*, 71(4), 485-490. doi: 10.1002/asi.24232.

[12] Fisun, V. (2020). *Problems of personal data protection: Experience of Ukraine and other countries*. Retrieved from https://yur-gazeta.com/publications/practice/informaciyne-pravo-telekomunikaciyi/problemi-zahistu-personalnih-danih-dosvid-ukrayini-ta-inshih-krayin.html.

[13] Gstrein, O., & Beaulieu, A. (2022). How to protect privacy in a datafied society? A presentation of multiple legal and conceptual approaches. *Philosophy & Technology,* 35, article number 3. doi: 10.1007/s13347-022-00497-4.

[14] Herrmann, D., & Pridöh, H. (2020). Basic concepts and models of cybersecurity. In *The ethics of cybersecurity* (pp. 11-44). Dublin: Springer.

[15] Kushakova, N.V. (2003). *Constitutional right to information in Ukraine* (comparative analysis). (PhD thesis, Kyiv National University named after Taras Shevchenko, Kyiv, Ukraine).

[16] Lysenko, S.O. (2019). Modern trends of informational security development, as a literary objective. *Public Management*, 2(17), 154-173. doi: 10.32689/2617-2224-2019-17-2-151-169.

[17] Mantelero, A., & Vaciago, G. (2017). *Legal aspects of information science, data science, and Big Data*. Retrieved from https://www.researchgate.net/publication/320622833_Legal_aspects_of_information_science_data_science_and_Big_Data.

[18] Mantelero, A., & Vaciago, G. (2022). *Reconciling data protection and cybersecurity: An operational approach for business sector.* Retrieved from https://oa.mg/work/10.1007/978-981-16-3049-1_9.

[19] Masuda, Y. (1981). *The information society as post-industrial society*. Tokyo: Institute for the Information Society.

[20] Ording, L.G., Gao, Sh., Chen, W., & Lyon, D. (1986). From "post-industrialism" to "information society": A new social transformation*? Sociology*, 20(4), 577-588.

[21] Orozova, D., Kaloyanova, K., & Todorova, M. (2019). Introducing information security concepts and standards in higher education. *TEM Journal,* 8(3), 1017-1024. doi: 10.18421/TEM83-46.

[22] Panchenko, V. (2020). Management of information security of the state and enterprises: Legal and organizational aspects. *Actual Problems of Jurisprudence*, 1(21), 103-109. doi: 10.35774/app2020.01.103.

[23] Prav, R.Yu. (2019). Regulatory and legal principles of formation and implementation of state security policy in the information sphere. *Public Administration*, 4(19), 222-234.

[24] Rath, D.K., & Ajit, K. (2021). Information privacy concern at individual, group, organization and societal level – a literature review. *Vilakshan – XIMB Journal of Management,* 18(2), 171-186. doi: 10.1108/XJM-08-2020-0096.

[25] Safari et la (nouvelle) chasse aux Français. (2010). Retrieved from https://www.cnil.fr/sites/default/files/atoms/files/le_monde_0.pdf.

[26] Shevchuk, O.R., & Mentukh, N.F. (2021). Implementation of the state information security policy of Ukraine in the context of corruption prevention: Administrative and legal aspect. *Scientific Bulletin of the Uzhhorod National University. Series: Law*, 64, 282-287. doi: 10.24144/2307-3322.2021.64.52.

[27] Straub, D.W., & Collins, R.W. (1990). Key information liability issues facing managers: Software piracy, proprietary databases, and individual rights to privacy. *Management Information Systems Quarterly,* 14(2), 143-156. doi: 10.2307/248772.

[28] Toffler, A. (1980). *The third wave*. New York: William Morrow and Company, Inc.

[29] Udovenko, Zh.V. (2020). Analysis of international legislation on non-interference in personal and family life. *Journal of the Kyiv University of Law*, 2, 383-386. doi: 10.36695/2219-5521.2.2020.73.

[30] Ukraine was hit by hacker attacks: Government websites were affected, the Diya portal was unavailable. (2022). Retrieved from https://dou.ua/lenta/news/ukraine-was-covered-by-hacker-attacks/.

[31] Voytsikhovsky, A.V. (2020). Information security as a component of the national security system (international and foreign experience). *Bulletin of Kharkiv National University named after V.N. Karazin*, 29, 281-288. doi: 10.26565/2075-1834-2020-29-38.

[32] Westin, A.F., & Louis, B.-C. (1970). *Privacy and freedom*. London: Bodley Head.

[33] Yarovenko, H. (2020). Evaluating the threat to national information security. *Problems and Perspectives in Management,* 18(3), 195-210. doi: 10.21511/ppm.18(3).2020.17.

[34] Yeng, P.K., Fauzi, M.A., Sun, L., & Yang, B. (2022). Assessing the legal aspects of information security requirements for health care in 3 countries: Scoping review and framework development. *JMIR Human Factors*, 9(2), article number e30050. doi: 10.2196/30050.

[35] Zurek, W.H. (1990). *Complexity, entropy and the physics of information.* New York: Addison-Wesley Publishing Company.

Наталія Фелікіссімівна Ментух

Кандидат юридичних наук, доцент
Західноукраїнський національний університет
46009, вул. Львівська, 11, м. Тернопіль, Україна
https://orcid.org/0000-0002-1016-7635

Оксана Романівна Шевчук

Кандидат юридичних наук, доцент
Західноукраїнський національний університет
46009, вул. Львівська, 11, м. Тернопіль, Україна
https://orcid.org/0000-0001-6453-355X

Захист інформації в електронних реєстрах: порівняльно-правовий аспект

Анотація. Актуальність теми дослідження полягає в необхідності подальшого розвитку теоретичних і методологічних основ захисту інформації в електронних реєстрах на основі всебічного дослідження розвитку системи реєстрів на сучасному етапі розвитку інформаційних систем, ґрунтовного вивчення зарубіжного досвіду в даній сфері. Мета роботи полягає в дослідженні наукових підходів щодо визначення поняття «інформаційна безпека», «захист інформації» в електронних реєстрах, а також у порівняльному аналізі основних способів та механізмів захисту інформації в електронних реєстрах в Україні та окремих зарубіжних країнах. Досліджено основні напрями європейської політики інформаційної безпеки, захист інформації в електронних реєстрах, основні механізми захисту інформації в електронних реєстрах на основі концептуального аналізу та порівняльного аналізу законодавства про захист інформації і основних способів її захисту в окремих провідних зарубіжних країнах. Окрема увага в статті приділялась особливостям інформаційної безпеки, а саме – захисту інформації в окремих зарубіжних країнах задля мети вивчення та впровадження кращих способів інформаційної безпеки у практику нашої держави. Доведено, що нова модель захисту інформації повинна враховувати розроблення ефективної державної політики з питань захисту інформації в електронних реєстрах відповідно до правових стандартів ЄС; створення інституту Уповноваженого з питань захисту інформації; відповідно до норм ЄС запровадження фахівців з питань захисту персональних даних на підприємствах. Оскільки сучасна система захисту інформації в Україні не гарантує захисту конфіденційності та персональних даних людини та громадянина, пропонується внести відповідні зміни до діючого законодавства з метою приведення його у відповідність до правових стандартів ЄС. У рамках дослідження репрезентовано нову модель захисту інформації в Україні з врахуванням досвіду зарубіжних країн, що сприятиме удосконаленню інформаційно захисних механізмів в електронних реєстрах

Ключові слова: конфіденційність; безпека; охорона; правове регулювання; персональні дані; зарубіжні країни; зарубіжний досвід