DOI 10.26886/2520-7474.5(69)2025.3

UDC: 378.091.3:621.38+551.5+621.395.97

CONTENT ANALYSIS OF TECHNICAL REGULATION MEANS FOR TRAINING FUTURE SPECIALISTS TO IMPLEMENT INFORMATION SECURITY IN THE FIELD OF ELECTRONICS, METROLOGY, AND RADIOTELECOMMUNICATIONS

Vladyslav Mahilevskyi, PhD Student

https://orcid.org/0009-0006-1056-0310

e-mail: vlad.mahilevskyi@icloud.com

Drahomanov Ukrainian State University, Ukraine, Kyiv

The study of the regulatory framework for training future specialists to implement information security in the field of electronics, metrology, and radiotelecommunications using content analysis is actualized. International standards ISO/IEC 27000, European Union Directives, particularly the General Data Protection Regulation, the Directive on Security of Network and Information Systems, the International Telecommunication Union, and the North Atlantic Treaty Organization were analyzed. It is established that the harmonization of the provisions of GDPR and NIS with educational and professional programs in higher education institutions contributes to the formation of new competencies for future specialists. This is necessary for working in professional employment environments with high demands for information transparency, legal compliance, and technological reliability. Mastering the content and principles of technical regulation means is a necessary condition for adapting to current legal and technological challenges in the context of professional training of future specialists for the implementation of information security in the field of electronics, metrology, and radiotelecommunications. It is also essential for the effective

implementation of international standards into national educational practice of professional education.

Keywords: *information security, technical regulation means, field of electronics, metrology, and radiotelecommunications, professional training, higher education institutions, future specialists, professional education.*

Relevance of the topic. The formation of professional competencies for future specialists to implement information security requires a clearly structured and implemented regulatory framework aligned with international acts. This alignment would ensure a harmonious combination of international standards, national legislation, and educational policy strategies. Currently, the Ukrainian system of higher education faces the task of not only adapting to global requirements in the field of information security but also actively implementing institutional mechanisms to secure personnel reserves in the knowledge area 01 Education/Pedagogy (now – A Education). Thus, the relevance of the study of the regulatory framework for training future specialists is determined not only by security challenges but also by the necessity of methodological substantiation of educational approaches in the competence-oriented transformation of educational standards.

Analysis of Recent Research and Publications. A comprehensive analysis of normative and technical regulation sources has been carried out. These sources define the requirements for training specialists capable of acting effectively in conditions of increased risk of unauthorized intervention in information databases (institutional and personal nature), deliberate information distortion, or destruction. Attention is paid to higher education standards with a historical focus on the field of knowledge 01 Education/Pedagogy, specialty 015 Professional Education (by specializations) (now – A15 Professional Education) [1] and the field of knowledge 12 Information Technologies (now – F Information Technologies)

specialty 125 Cybersecurity (now – F5 Cybersecurity and Information Protection) [2]. Comparative research of international standards of the ISO/IEC 27000 series [60], recommendations of the International Telecommunication Union (ITU), provisions of the European directives General Data Protection Regulation (GDPR) and the Directive on Security of Network and Information Systems (NIS) , documents of the North Atlantic Treaty Organization (NATO), the United Nations (UN), the European Union (EU), and the Organization for Security and Co-operation in Europe (OSCE) is also included. These documents currently ensure the normative requirements for the competencies of specialists for the formation of information security [3].

Setting the task. The task of the article is to conduct a content analysis of the normative and legal means for the professional training of specialists in specialty A15 Professional Education, field of knowledge A Education, for the implementation of information security in the turbulent conditions of globalization. The article also aims to outline the prospects for the integration of the spheres of education, science, and innovation with professional employment environments.

Presentation of the main material. The research problem covers the process of implementing international requirements into the national legal framework and studies their impact on the development of educational standards and programs implemented in domestic higher education institutions. The national context is examined through the lens of analyzing constitutional provisions, specialized Laws of Ukraine, by-laws, and state standards that provide for the regulation of professional training of specialists for the field of information security. A special place in the study is given to considering issues of regulatory support for educational activities, namely licensing, accreditation, and regulation of practical training of specialists. This includes creating favorable conditions for their continuous professional

development in the field. In the socio-turbulent conditions of digital transformation and global technological competition, ensuring the quality of training future specialists is a guarantee of preserving the state's technological priorities. Thus, the improvement of normative regulation was considered a strategic direction of state educational policy in the field of national security.

Due to the rapid digitalization of public life and the increase in the level of cyber threats that cover both private and public information systems, the formation of effective information security management systems gains particular importance. In the complicated conditions of cyber environment danger and the spread of variations of threats on an international scale, it is the formalized approach to standardization and ensuring the integrity, confidentiality, and availability of information assets that contributes to the creation of stable adaptive security models. The series of international standards ISO/IEC 27000, developed by the International Organization for Standardization (ISO) jointly with the International Electrotechnical Commission (IEC), plays a key role in forming the conceptual and basic framework for ensuring Information Security Management Systems (ISMS) [4]. To detail the understanding of the content of the ISO/IEC 27000 series standards and their functional significance in the aspects of ISMS organization, the comparative characteristics of the main normative documents are considered: ISO/IEC 27001 – defining requirements for the creation, implementation, and improvement of ISMS; ISO/IEC 27002 – recommendations for the implementation of information security supervision and control; Other standards of the ISO/IEC 27000 series – scaling the directions of information security management.

It is noted that the ISO/IEC 27000 series includes a number of interconnected standards that define fundamental principles, terms, procedures, and mechanisms for information security management. The

central position is occupied by the ISO/IEC 27001 standard. It defines the requirements for the creation, implementation, maintenance, and continuous improvement of ISMS documentation [5] and normalizes the certification of organizations that seek to confirm the compliance of institutional security processes according to internationally recognized criteria. The uniqueness of the standard lies in providing a holistic, system-oriented approach to managing risks associated with information resources, and formalizing measures for protecting information data in accordance with their criticality, significance, and vulnerability.

Along with the generally recognized universal standards of the ISO/IEC series, which lay the foundation for implementing a systematic approach to ensuring information security through technical regulation means, the recommendations of the ITU are an important component of developing telecommunication infrastructure [6]. The ITU, a specialized UN agency, coordinates cross-border activities and plays a leading role in activating the processes of standardization, development, and secure functioning of information security systems. ITU-T recommendations serve as technical guidelines for participating countries and industry security management entities. They guide technology development towards compatibility, resilience, including the cyber resilience of global communication networks [7]. To generalize the main directions of ITU activity in the field of information security and analyze the technical content, the key recommendations and initiatives of the authorized ITU organization are systematized, namely: security of the unique numerical identifier in the network (Internet Protocol address); Fifth Generation mobile networks (5th Generation); Internet of Things; Global Cybersecurity Agenda.

It should be noted that for the sphere of ensuring information security, ITU recommendations are aimed at confidentiality, integrity, and availability of information circulating in telecommunication networks, as well as the

protection of their own infrastructure from technological and unauthorized threats. Particular importance is given to the information security of network architecture, cryptographic data protection, authorized access management, user authentication, security incident handling, and maintaining the reliability of services at the level of voice, video, and data traffic.

The goal of the ITU's functionality is to implement the Global Cybersecurity Alliance (GCA) [8] , a strategic roadmap for systematic implementation that ensures the development and implementation of their own cybersecurity policies for partner countries. The strategy includes regulatory, technological, and organizational-managerial provisions in the mechanisms for building the capacity of member states.

Possessing knowledge about ITU-T recommendations, their classification, technical content, and practical implementation is a mandatory component for mastering by specialists authorized to design, implement, and operate secure telecommunication systems. This is especially relevant in the context of rationalizing the provision of critical infrastructure. In this way, ITU recommendations are a guarantee of compliance with the meaningful supplement to the universal ISO/IEC standards. They specify the requirements for ensuring information security, taking into account the technical specifics of global communication networks and their strategic role in the state's information space.

One of the fundamental documents is the General Data Protection Regulation (GDPR) [9]. It entered into force in 2018 and established standards for processing personal information within the EU. Its feature is its extraterritorial nature: the regulation applies to any organization that processes the personal data of EU citizens, regardless of geographical jurisdiction. The GDPR regulatory system defines key principles, including: lawfulness and fairness of processing; purpose limitation; data minimization

and accuracy; storage limitation; ensuring confidentiality and integrity, and the accountability principle.

The technical implementation of the defined requirements demands competencies from future specialists. These competencies cover consent management from data subjects, implementing the concepts of "Privacy by design and by default," developing procedures for notification of personal information security breaches, and legal literacy in the field of data subject rights protection.

Another important regulatory act is the EU Directive "on the security of network and information systems" (NIS). The NIS Directive actualizes the first attempts to standardize the approach to ensuring cybersecurity at the state level of European partner countries. The goal of the NIS directive is to ensure a high level of cyber resilience of critical infrastructures, including operators of essential services and digital service providers.

For a clear generalization of the normative content of the GDPR and NIS directives, as well as their practical impact on the field of digital security, the characteristics of the documentation are provided: GDPR – General Data Protection Regulation, with the goal of Protecting personal data of EU citizens; NIS Directive – Directive on Security of Network and Information Systems, with the goal of cyber resilience of critical infrastructures.

Harmonization of the provisions of GDPR and NIS with professional training educational programs contributes to the formation of new competencies. These competencies are necessary for working in an environment with high demands for information transparency, legal compliance, and technological reliability. This includes, in particular, the integration into educational courses of modules on legal analysis in the field of digital protection, risk assessment taking into account regulatory frameworks, development and implementation of security policies, and the development of interdisciplinary thinking through the synthesis of technical

and legal knowledge. Scholars also rightly believe that special attention should be paid to the practical training of students. This can be achieved by using case methods, modeling real incidents, and analyzing judicial and administrative practice regarding violations in the field of personal data processing. This is relevant for forming the ability of future specialists to adequately respond to risks associated with data leaks, unauthorized access, and other cyber incidents in the fields of electronics, metrology, and radiotelecommunications [11, 12].

The EU Directives, particularly the General Data Protection Regulation (GDPR) and the "on the security of network and information systems" (NIS), significantly transform the approaches to the professional training of specialists working in the conditions of economic digitalization. Mastering the content and principles of normative acts of technical regulation becomes a necessary condition for adapting educational programs to current legal and technological challenges. It is also necessary for the effective implementation of international standards into the national educational practice of professional training of specialists for the implementation of information security in the field of electronics, metrology, and radiotelecommunications. These directives perform a norm-setting function. On the one hand, they form the normative framework for the development of legal practice in the field of information security. On the other hand, they define the list of key competencies that graduates must master to ensure their competitiveness in the labor market and their ability for professional activity in the conditions of digital transformation of social activities (by economic types).

Conclusion. A theoretical content analysis was performed, which confirmed the incomplete compliance of the regulatory framework and educational standards for the implementation of information security by future and currently employed specialists. First of all, this concerns the

insufficient consideration of international norms. Even where individual provisions of the GDPR or the NIS directive have already been formally implemented, their practical application in the organization of the educational process often has a declarative rather than an effective nature. This also directly limits the possibilities for students to form professional competencies for the implementation of information security that are genuinely demanded by national and international employment markets.

The detachment of the content filling of educational programs and their material, technical, and information-technological support from practice remains a problem. The lack of scientific and educational-methodological support for cases, applied laboratory and testing educational modules, and partnership with employers leads to the fact that even well-structured programs prepared by specialists "on paper" do not always meet the requirements for ensuring work in conditions of real social turbulence and cyber threats during martial law. The solution is seen in a more flexible interaction between the state, higher education institutions, industry institutions, and enterprises. This will allow for updating curricula and educational programs and ensuring their content is maximally close to practice. Thus, the further development of the system for professional training of future specialists to implement information security requires not only the improvement of the legislative framework but also the active integration of the spheres of education, science, and innovation with professional environments. This will ensure the training of personnel capable of acting effectively in the complex and changing space of social digitalization.

Література:

1. Стандарт вищої освіти України перший (бакалаврський) рівень, галузь знань 01 – «Освіта / Педагогіка», спеціальність 015 –

«Професійна освіта (за спеціалізаціями)»: наказ Міністерства освіти і науки України від 21.11.2019 р. № 1460, <https://mon.gov.ua/static-objects/mon/sites/1/vishcha-osvita/zatverdzeni%20standarty/2021/07/28/015-Profosvita-bakalavr.pdf> (2025, жовтень, 22).

2. Стандарт вищої освіти зі спеціальності 125 «Кібербезпека» галузі знань 12 «Інформаційні технології» для першого (бакалаврського) рівня вищої освіти: наказ Міністерства освіти і науки України від 04.10.2018 № 1074 (зі змінами – наказ Міністерства освіти і науки України від 29.10.2024 № 1547). <https://zakon.rada.gov.ua/laws/show/243/2021> (2025, жовтень, 22).

3. European Union Agency for Cybersecurity (ENISA). NIS 2 Directive: Key provisions and implementation challenges. 2023. URL: https://www.enisa.europa.eu/> (2025, жовтень, 22).

4. ISO/IEC 27000:2018. Information technology — Security techniques — Information security management systems — Overview and vocabulary. Geneva: ISO, 2018. 44.

5. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection – Information security management systems – Requirements. Geneva: International Organization for Standardization, 2022. 36.

6. International Telecommunication Union (ITU). About ITU: Bridging the digital divide. 2023, <https://www.itu.int/> (2025, жовтень, 22).

7. ITU-T Recommendation X.1205. Overview of cybersecurity. Geneva: ITU, 2008. 48, <https://www.itu.int/rec/T-REC-X.1205-200804-I> (2025, жовтень, 22).

8. International Telecommunication Union (ITU). Global Cybersecurity Agenda (GCA). 2023,

<https://www.itu.int/en/action/cybersecurity/pages/gca.aspx> (2025, жовтень, 22).

9. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) 2016, <https://eur-lex.europa.eu/eli/reg/2016/679/oj> (2025, жовтень, 22).

10. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive). *Official Journal of the European Union*. 2016. L 194.1–30.

11. Лахно В. А., Касаткін Д. Ю., Сагун А. В. (2022) Методичні вказівки з навчальної практики «Проєктування систем кібербезпеки». Київ: НУБіП України. 58.

12. Prometheus. Безпека в інтернеті під час війни: практичний курс. (2022), <https://prometheus.org.ua/prometheus-free/cybersecurity-during-war-practical/> (2025, жовтень, 22).

References:

1. Standart vyshchoi osvity Ukrainy pershyi (bakalavrskyi) riven, haluz znan 01 – «Osvita / Pedahohika», spetsialnist 015 – «Profesiina osvita (za spetsializatsiiamy)»: nakaz Ministerstva osvity i nauky Ukrainy vid 21.11.2019 r. № 1460 [Standard of Higher Education of Ukraine, first (bachelor's) level, field of knowledge 01 - "Education / Pedagogy", specialty 015 - "Professional Education (by specialization)": Order of the Ministry of Education and Science of Ukraine dated November 21, 2019 No. 1460], <https://mon.gov.ua/static-objects/mon/sites/1/vishcha-osvita/zatverdzeni%20standarty/2021/07/28/015-Profosvita-bakalavr.pdf> (2025, october, 22). [in Ukrainian].

2. Standart vyshchoi osvity zi spetsialnosti 125 «Kiberbezpeka» haluzi znan 12 «Informatsiini tekhnolohii» dlia pershoho (bakalavrskoho) rivnia vyshchoi osvity: nakaz Ministerstva osvity i nauky Ukrainy vid 04.10.2018 № 1074 (zi zminamy – nakaz Ministerstva osvity i nauky Ukrainy vid 29.10.2024 № 1547) [Standard of Higher Education of Ukraine in specialty 125 "Cybersecurity" of knowledge area 12 "Information Technologies" for the first (bachelor's) level of higher education: Order of the Ministry of Education and Science of Ukraine dated 04.10.2018 No. 1074 (as amended - Order of the Ministry of Education and Science of Ukraine dated 29.10.2024 No. 1547)], <https://zakon.rada.gov.ua/laws/show/243/2021> (2025, october, 22). [in Ukrainian].

3. European Union Agency for Cybersecurity (ENISA). NIS 2 Directive: Key provisions and implementation challenges (2023). <https://www.enisa.europa.eu/> (2025, october, 22). [in English].

4. ISO/IEC 27000:2018. Information technology — Security techniques — Information security management systems — Overview and vocabulary. Geneva: ISO, 2018. 44 p. [in English].

5. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection – Information security management systems – Requirements. Geneva: International Organization for Standardization, 2022. 36. [in English].

6. International Telecommunication Union (ITU). About ITU: Bridging the digital divide (2023). <https://www.itu.int/> (2025, october, 22). [in English].

7. ITU-T Recommendation X.1205. Overview of cybersecurity. Geneva: ITU, 2008. 48 p. <https://www.itu.int/rec/T-REC-X.1205-200804-I> (2025, october, 22). [in English].

8. International Telecommunication Union (ITU). Global Cybersecurity Agenda (GCA) [Електронний ресурс]. 2023.

<https://www.itu.int/en/action/cybersecurity/pages/gca.aspx> (2025, october, 22). [in English].

9. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). 2016. <https://eur-lex.europa.eu/eli/reg/2016/679/oj> (2025, october, 22). [in English].

10. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive). *Official Journal of the European Union*. 2016. L 194.1–30. [in English].

11. Lakhno V. A., Kasatkin D. Yu., Sahun A. V. (2022) Metodychni vkazivky z navchalnoi praktyky «Proiektuvannia system kiberbezpeky» [Methodological guidelines for educational practice «Design of cybersecurity systems»]. Kyiv: NUBiP Ukrainy. 58. [in Ukrainian].

12. Prometheus. Bezpeka v interneti pid chas viiny: praktychnyi kurs [Internet Security During War: A Practical Course]. (2022) <https://prometheus.org.ua/prometheus-free/cybersecurity-during-war-practical/> (2025, october, 22). [in Ukrainian].

Citation: Vladyslav Mahilevskyi (2025). CONTENT ANALYSIS OF TECHNICAL REGULATION MEANS FOR TRAINING FUTURE SPECIALISTS TO IMPLEMENT INFORMATION SECURITY IN THE FIELD OF ELECTRONICS, METROLOGY, AND RADIOTELECOMMUNICATIONS. Frankfurt. TK Meganom LLC. Paradigm of knowledge. 5(69). doi: 10.26886/2520-7474.5(69)2025.3