https://pravo.cuspu.edu.ua/index.php/pravo/article/view/131/115 (дата звернення: 22.09.2025).

6. Іваночко О. О. Поняття воєнного злочину в міжнародному та національному праві. *Центральноукраїнський вісник права та публічного управління.* 2023. Вип. 3. С. 28-37. DOI: https://doi.org/10.32782/cuj-2023-3-4. URL: https://cuj.dnuvs.ukr.education/index.php/cuj/article/view/20/18 (дата звернення: 22.09.2025).

DOI https://doi.org/10.30525/978-9934-26-613-3-34

EUROPEAN STANDARDS FOR LEGAL REGULATION OF INFORMATION SECURITY: EU EXPERIENCE AND ITS IMPLEMENTATION IN UKRAINE

Palinchak M. M.
Doctor of Political Sciences, Professor,
Dean of the Faculty of International Economic Relations
Uzhhorod National University
Uzhhorod, Ukraine

Kudierova A.
Student Political science and government major
St. John's University
New York, USA

In today's information society, cyber threats are becoming a public problem that requires not only technical but also legal means of regulation. Within the European Union, a set of legal and regulatory instruments has been developed to ensure a high level of security for networks, information systems, digital products and services. At the same time, Ukraine, which is striving for European integration, faces the task of adapting its legislation to these standards.

The European Union has developed a comprehensive system of legal regulation of information security, covering network and system security. It is based on key EU directives and regulations, including Network and Information Security (NIS)/NIS2, General Data Protection Regulation (GDPR) and Cyber Resilience Act, which together form the regulatory architecture of European cybersecurity.

The first comprehensive document was the NIS Directive (2016), which introduced mandatory requirements for critical infrastructure operators and digital services regarding protection, incident reporting and coordination. In

2022, it was replaced by the NIS2 Directive (Directive (EU) 2022/2555), which expanded the scope, strengthened control and accountability, and required member states to adapt their legislation by 17 October 2024 [1].

Another cornerstone act is GDPR – Regulation (EU) 2016/679, which came into force in 2018 and established uniform standards for personal data protection. The document defines technical and organisational requirements, the principles of 'security by design' and 'protection by default', and provides for sanctions of up to €20 million or 4% of annual turnover [4].

In 2022, the Cyber Resilience Act (CRA) was adopted, establishing requirements for the security of digital products and services. The CRA obliges manufacturers to manage vulnerabilities, provide updates, report incidents and certify product compliance.

An important addition was the Cybersecurity Act (Regulation (EU) 2019/881), which introduced a European cybersecurity certification scheme for ICT products. The European Union Agency for Cybersecurity (ENISA) coordinates the development of certification schemes, and the international standards ISO/IEC, ETSI, and CEN/CENELEC are used as a technical basis [2].

Other notable acts include the Regulation on Cybersecurity of EU Institutions (effective from 7 January 2024), the Digital Operational Resilience Act (DORA), which regulates IT resilience in the financial sector, and directives in the field of electronic communications (ePrivacy).

Thus, legal regulation of information security in the EU is multi-layered: from the security of digital products (CRA) and network systems (NIS2) to data protection (GDPR) and sectoral cyber resilience (DORA). This model forms a unified cyber security policy within the European Union.

In Ukraine, information security is regulated by various laws, decrees, and strategic documents. For example, the State Cybersecurity Strategy of Ukraine, the Information Security Doctrine (approved by Presidential Decree No. 47/2017), as well as the Law 'On the Fundamentals of National Security,' the Law 'On the Protection of Information in Information and Telecommunications Systems,' and other regulations.

With the start of the large-scale invasion by the russian federation, Ukraine has intensified its legislative efforts in cybersecurity, but there remain a number of gaps in synchronisation with European standards. Ukraine is under significant information and propaganda pressure, which requires strengthening information security and adapting data protection standards.

Thus, the legislative framework in Ukraine exists, but its integration into the European context is not complete.

The implementation of European information security standards in Ukraine is carried out in several main areas, covering both legislative and organisational-institutional aspects. Among the key measures, the following can be highlighted:

1. Transposition of NIS2. Ukraine is currently working on adapting the provisions of NIS2 to national law (by updating the law on cybersecurity and the law 'On Information Protection ...'). However, this process is complicated by the need to bring the competences of state bodies into line and establish clear oversight and sanction mechanisms.

2. Harmonisation with GDPR. Ukrainian legislation provides for the protection of personal data (the law 'On the Protection of Personal Data') and the National Authority for the Protection of Personal Data is operational. However, full compliance with GDPR standards has not yet been achieved – there are nuances regarding extraterritorial application, reporting of violations, and mechanisms for enforcing sanctions.

3. Certification and standards. Ukraine can implement cybersecurity certification schemes that are compatible with European ones, but this has not yet been done at the national level. International ISO/IEC standards are used, but without pan-European recognition.

4. Cooperation and information exchange. Ukraine is already establishing cooperation with European structures (ENISA, CERT communities, participation in the Eastern Partnership) to exchange information on cyber threats and incidents.

5. Human resources and institutional capacity. One of the main challenges is the lack of sufficient specialists, the weak material and technical base of state cyber structures, and the need to improve qualifications and standardise response procedures.

As of today, the implementation of European standards in Ukraine is at an average level: significant legislative efforts have been made, but practical effectiveness and compliance are still far from ideal. At the same time, during the war, Ukraine has demonstrated its ability to respond quickly to cyber threats by strengthening coordination, developing standards, and implementing measures to protect the information space.

Further improvement of the implementation of European information security standards in Ukraine requires a systematic approach that combines regulatory, institutional and educational changes. Based on an analysis of current practices and scientific research, the following key areas for improvement can be identified [3]:

– Accelerating the transposition of NIS2 and ensuring the relevant institutions are in place.
– Aligning personal data legislation with the GDPR.
– Developing a national cybersecurity certification scheme.
– Strengthening human resources and training.
– Securing funding and material resources.
– Improving coordination between public, private and civil actors.
– Fostering a culture of cybersecurity in society.

These measures could bring Ukraine closer to a level where its legislation and practices are compatible with European standards and ensure a high level of information security.

Therefore, the legal regulation of information security in the EU is based on a set of acts – GDPR, NIS2 and the Cyber Resilience Act, which provide a coordinated cyber defence system and respond to the challenges of the digital age. For Ukraine, the implementation of these standards is an important component of its European integration course and the strengthening of national cyber resilience, but it requires further modernisation of legislation, institutional development and closer cooperation with European structures.

References:

1. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2 Directive). Official Journal of the European Union, L 333/80, 27.12.2022. URL: https://eur-lex.europa.eu/eli/dir/2022/2555

2. European Commission. Proposal for a Regulation on Horizontal Cybersecurity Requirements for Products with Digital Elements (Cyber Resilience Act), COM(2022) 454 final. Brussels, 2022. URL: https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act

3. Kostiuchenko, Y. M. ‘Cooperation between Ukraine and the EU in the field of cybersecurity: mechanisms for combating cybercrime.’ Problems of Modern Transformations. Series: Law, Public Management and Administration 15 (2025).

4. 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 (General Data Protection Regulation, GDPR). URL: https://eur-lex.europa.eu/eli/reg/2016/679