UDC 004.056:342.9
DOI: 10.63341/naia-chasopis/3.2025.24

Prospects for state regulation of cryptographic data protection

Mariia Turchina
PhD in Law
Yaroslav Mudryi National Law University
61024, 77 Hryhorii Skovoroda Str., Kharkiv, Ukraine
https://orcid.org/0000-0002-1486-1122

Igor Rudenko*
Master of Science
Yaroslav Mudryi National Law University
61024, 77 Hryhorii Skovoroda Str., Kharkiv, Ukraine
https://orcid.org/0009-0008-3582-3951

Olha Khorolska
Master of Science
Yaroslav Mudryi National Law University
61024, 77 Hryhorii Skovoroda Str., Kharkiv, Ukraine
https://orcid.org/0009-0004-9853-2378

Abstract
The relevance of the study was determined by the need for legal and technical rethinking of state regulation of cryptographic information protection under the conditions of Ukraine's digital transformation. The aim of the article was to identify the effectiveness of the existing regulatory, institutional, and technical model for data cryptographic protection, taking into account the provisions of international standards. The study applied methods of structural-functional analysis, systematic comparison of legal provisions, and content analysis of technical requirements. As a result of the study, it was established that the regulatory field covered two levels of influence – general technical and specialised – yet only approximately sixty percent of the provisions on electronic signature, cryptographic key management, and timestamps corresponded to international technical requirements. Fragmentation in the definition of mandatory certification procedures and the absence of unified regulations in the field of digital identification and electronic seals were recorded. Within the framework of interinstitutional interaction, it was found that only three out of eight functional areas were governed by formalised mechanisms, which complicated the response to cryptographic incidents. Technical analysis confirmed that the average key length in cryptographic algorithms resistant to quantum computing systems exceeded three thousand bits – two to three times higher than the parameters of traditional algorithms – yet the implementation of such solutions into the state certification system was limited. It was also established that only a portion of cryptographic protection hardware complied with

Article's History:
Received: 28.05.2025
Revised: 02.09.2025
Accepted: 29.09.2025

Suggest Citation:
Turchina, M., Rudenko, I., & Khorolska, O. (2025). Prospects for state regulation of cryptographic data protection. *Law Journal of the National Academy of Internal Affairs*, 15(3), 24-44. doi: 10.63341/naia-chasopis/3.2025.24.

*Corresponding author

Copyright © The Author(s). This is an open access article distributed under the terms of the Creative Commons Attribution License 4.0 (https://creativecommons.org/licenses/by/4.0/)

international technical security level requirements. The practical significance of the study results lay in the potential application for updating the regulatory architecture, forming technical regulations, developing state control procedures, and supporting public authorities, technical expert units, and developers in the implementation of the national cybersecurity strategy

Keywords:
digital identification; electronic signature; certification of means; information security; technical standard; interagency coordination; digital transformation

Introduction

In the field of information security, the importance of forming a comprehensive system of cryptographic protection capable of ensuring the continuity of state information resources and maintaining the confidentiality of critical data is increasing. Under conditions of rapid development of digital services and the expansion of personal and official data processing in the public sector, there arises a need for formalised, legally and technically harmonised regulation of cryptographic mechanisms. The problem lies in the absence of a unified model that would combine the requirements of technical compliance, legal status of protection tools, and organisational responsibility of the entities involved in the implementation of information protection solutions.

The relevance of the studied issue was driven by the limited nature of existing state oversight instruments, the insufficient unification of cryptographic certification procedures, and the lack of standardised models of inter-agency coordination. The need to develop effective mechanisms for technical control, legal authorisation, and centralised monitoring reveals structural deficiencies in the current regulatory and institutional architecture. This issue complicates the implementation of a coherent state policy in the field of information protection and creates risks in processes of electronic identification, digital document management, and the functioning of access management systems to information resources.

In the study by J. Kazimi & H. Thalwal (2024), attention was focused on legal challenges and technological risks associated with modern models of cryptographic protection. As a result, it was established that existing regulatory frameworks largely do not cover the dynamics of quantum threats, creating a gap between the level of regulation and current technical needs. Separately, it was noted that the implementation of cryptographic service control tools in the public sector is uneven. In the work of A. Vargiolu (2022), the approaches of the Organisation for Economic Co-operation and Development to the formation of a global privacy policy were analysed. The author identified that the existence of a single principled approach to encryption in the context of cross-border data exchange contributes to strengthening trust between states but requires technical adaptation in each specific case.

K. Limniotis (2021) examined the significance of cryptography as a tool for protecting fundamental rights and freedoms, emphasising its role in the formation of digital inviolability. It was shown that the use of cryptographic solutions significantly reduces the risk of violations of privacy rights in digital ecosystems. S. Bommareddy *et al.* (2022) focused on the security of medical data, identifying the key role of authentication mechanisms and protection of transmission channels. The authors confirmed that the level of protection directly depends on the technical compatibility of cryptographic protocols with electronic healthcare systems. In the work of Y. Kokarcha & A. Lalueva (2022), the impact of martial law on the protection of personal data on social networks was studied. It was shown that legal guarantees remain limited without an appropriate level of technical cryptographic support.

In the study of M.V. Zinchuk (2024), the legal regulation of confidential information in Ukraine was examined, with emphasis on contradictions between legislation and technical regulations. It was established that the growth of digital threats was not accompanied by a proportional development of state control mechanisms. Y.V. Kostiuk *et al.* (2025) analysed cryptographic protection hardware and the compliance with international standards. It was revealed that hardware solutions certified under international protocols demonstrate higher effectiveness in complex information environments. In the publication by A.K. Yanamala & S. Suryadevara (2024), the interdependence between transparency of certification procedures and the level of trust in cryptographic services was studied. The authors confirmed that the absence of open audit mechanisms significantly reduces the legitimacy of implemented solutions.

A second contribution by A. Vargiolu (2022) consisted in clarifying the international challenges of harmonising cryptographic privacy standards. The analysis established that the inconsistency of technical parameters made operational interaction between state cryptographic platforms impossible. In the study of T. Riebe *et al.* (2022), the dual status of cryptography in the context of security and surveillance was discussed. It was established that the US policy of controlling the export of cryptographic solutions limits the global interoperability of protection tools, which resulted in decreased effectiveness of transnational coordination.

J. Chen (2020) studied the evolution of China's cryptographic legislation, paying attention to the

transition to centralised regulation. It was shown that such a model increases manageability but may hinder technological innovation in the case of strict administrative dependence of the technical sector. In the work of B. Firmansyah & R. Bansal (2024), the processes of cryptographic standardisation under growing complexity of digital platforms were considered. It was found that updates to the regulatory and technical base lag behind developments in the field of post-quantum security, and certification systems demonstrate low adaptability to new infrastructures, including the metaverse and blockchain models.

The analysed academic studies showed the absence of a comprehensive assessment of the effectiveness of the regulatory, institutional and technical model of state cryptographic protection governance under conditions of digital transformation. A systematic analysis of the content of current legal and regulatory acts in comparison with international technical standards – particularly in the field of certification, key management and digital identification – was not presented. The studies did not highlight the structure of powers of authorised cryptographic control bodies, nor did the studies analyse the actual state of inter-agency cooperation in identifying and responding to cryptographic incidents. The results of comparative assessment of classical and post-quantum protection algorithms also remained uninterpreted, which limits the opportunities for forming a modern technical policy in the field of cryptographic certification. These gaps determined the need to conduct a study aimed at integrating legal and technical information protection mechanisms, assessing the level of compliance of national solutions with international standards, and formulating recommendations for updating the regulatory architecture.

The purpose of the study was a comprehensive investigation of the regulatory, institutional, and technical foundations of state governance of cryptographic information protection under conditions of digital transformation, taking into account the requirements of international standards. To achieve this aim, the following objectives were set: to analyse the content and coherence of the main legal and regulatory acts governing cryptographic data protection; to assess the structure of powers of authorised bodies and the nature of inter-agency cooperation in the field of cryptographic control; to determine the level of compliance of national technical requirements with international standards in the areas of certification and digital identification.

Materials and Methods

The study had an applied interdisciplinary nature with a predominance of qualitative analysis, including elements of comparative, regulatory-legal and technical-standardisation approaches, and was based on an extended source base covering the period from 1994 to 2025. The methodology of the study was based on a combination of analysis of regulatory acts, evaluation of technical specifications and institutional modelling of regulatory practices. The analysis was carried out considering the dynamics of regulatory changes, the evolution of cryptographic algorithms, and the transformation of the institutional architecture of executive bodies responsible for the implementation of policy in the field of digital security.

To ensure the completeness of the empirical base, a set of open regulatory acts, technical standards, methodological guidelines and official reports related to state regulation in the field of cryptographic information protection was used. The core of the source base consisted of the current editions of the Law of Ukraine "On Information Protection in Information and Telecommunications Systems"[1], Law of Ukraine "On Cryptographic Protection of Information"[2] and Law of Ukraine "On Electronic Trust Services"[3]. To provide a comprehensive description of the administrative-legal model, the norms of the Code of Ukraine on Administrative Offences[4], Criminal Code of Ukraine[5] та Decree of the President of Ukraine "On the Decision of the National Security and Defence Council of Ukraine of May 14, 2021 "On the Cybersecurity Strategy of Ukraine"[6] were also used. In the field of institutional regulation, the Law of Ukraine "On the State Service for Special Communications and Protection of Ukraine"[7] was involved, along with materials on the activities of the National Security and Defence Council of Ukraine (n.d.), the Security Service of Ukraine (n.d.) and the National Police of Ukraine (n.d.). The technical parameters of cryptographic algorithms were evaluated based on documents from the International Organisation for Standardisation/International Electrotechnical Commission (ISO/IEC): ISO/IEC No. 15408-1 "Evaluation criteria for

[1] Law of Ukraine No. 80/94-VR "On Information Protection in Information and Telecommunications Systems". (1994, July). Retrieved from https://zakon.rada.gov.ua/laws/show/80/94-вр.
[2] Law of Ukraine No. 803-XIV "On Cryptographic Protection of Information". (1999, December). Retrieved from https://zakon.rada.gov.ua/laws/show/803-14.
[3] Law of Ukraine No. 2155-VIII "On Electronic Trust Services". (2017, October). Retrieved from https://zakon.rada.gov.ua/laws/show/2155-19.
[4] Code of Ukraine on Administrative Offenses. (1984, December). Retrieved from https://zakon.rada.gov.ua/laws/show/80731-10.
[5] Criminal Code of Ukraine. (2001, April). Retrieved from https://zakon.rada.gov.ua/laws/show/2341-14.
[6] Decree of the President of Ukraine No. 447/2021 "On the Decision of the National Security and Defense Council of Ukraine of May 14, 2021 "On the Cybersecurity Strategy of Ukraine". (2021, August). Retrieved from https://zakon.rada.gov.ua/laws/show/96/2021.
[7] Law of Ukraine No. 3475-IV "On the State Service for Special Communications and Information Protection of Ukraine". (2006, February). Retrieved from https://zakon.rada.gov.ua/laws/show/911-2006-п.

IT security" (2009), ISO/IEC No. 18033-1 "Encryption algorithms" (2021), and ISO/IEC No. 19790 "Security requirements for cryptographic modules" (2012), as well as using data from the National Institute of Standards and Technology (2008; 2019; 2020). Within the framework of the analysis, the specifications of ISO/IEC No. 7816-4 "Integrated circuit cards" (2020), the results of the Post-Quantum Cryptography (PQC) standardisation project of the US National Institute of Standards and Technology, and the recommendations of the European Union Agency for Cybersecurity (2014) were taken into account. To evaluate certification compatibility, the provisions of the European Telecommunications Standards Institute (2016a; 2016b; 2018) were applied, taking into account the compliance criteria of the Federal Information Processing Standard (FIPS) 140-2 (National Institute of Standards and Technology, 2001). Additionally, the provisions of the updated Regulation of the European Parliament and of the Council "On Electronic Identification and Trust Services for Electronic Transactions in the Internal Market and Repealing Directive 1999/93/EC"[1] were used, which allowed national mechanisms to be compared with the requirements of cross-border regulatory harmonisation.

The method of structural-functional analysis was used to study the organisational structure of state regulation mechanisms in the field of cryptographic information protection. This method allowed for a clear division of responsibilities among the main divisions of the State Service of Special Communications and Information Protection of Ukraine by functional areas, in particular in relation to strategic management, technical expertise, standardisation, and control. The results of the analysis made it possible to compare the institutional structure with approaches used in EU countries and to evaluate its compliance with the European model of regulatory distribution.

The method of comparative law was applied to compare the regulatory acts of Ukraine in the field of cryptographic protection with the relevant acts of EU law. Within this approach, the provisions of Ukrainian laws on information security and cryptographic protection were analysed and compared with the provisions of the European regulation on electronic identification, as well as with the technical standards of the European Telecommunications Standards Institute and the European Union Agency for Cybersecurity. On this basis, the level of harmonisation was established in the areas of certification of cryptographic protection tools, electronic signatures, digital timestamps, key, and seal management.

Content analysis of technical regulations was conducted to determine the requirements for the implementation of cryptographic algorithms, authentication hardware, and the compliance with certification standards. The analysis covered technical profiles of classical algorithms, including Rivest-Shamir-Adleman (RSA), Advanced Encryption Standard (AES), Elliptic Curve Digital Signature Algorithm (ECDSA), and promising post-quantum solutions: Dilithium, Kyber, SABER. The data obtained allowed for a comparative assessment of cryptographic key length, cryptographic robustness, and the level of integration of the mentioned algorithms into national certification procedures. The interpretation of results was carried out by integrating regulatory, institutional, and technical aspects, which made it possible to form a comprehensive model of the current state of cryptographic regulation and its alignment with international approaches. The effectiveness assessment was conducted by comparing legal regulation, organisational functionality, and technical implementation with established international compatibility criteria, which enabled the formulation of generalised conclusions and recommendations.

Results

Regulatory and legal support for cryptographic information protection: evolution and current state in Ukraine. In the process of forming a systemic model of state regulation of cryptographic information protection in Ukraine, a key analytical task is the study of the legal and regulatory foundations that define the legal status and operational conditions of cryptographic security tools. The basis for such regulation is set out in the provisions of the Law of Ukraine No. 80/94-VR[2] and Law of Ukraine No. 803-XIV[3]. These acts establish the principles of technical admissibility, mandatory certification, and the legal regime for the circulation of cryptographic protection of information (CPI) tools, while differing in terms of the structure of subject regulation and the allocation of competencies.

A comparative analysis of these laws allows identifying systemic overlaps in the definition of regulated objects, user categories, and liable entities, while also highlighting differences in the formulation of technical criteria and the scope of supervisory powers of authorised bodies. It is also important to identify gaps that arise in the context of the absence of coordinated procedures for inter-agency verification of CPI tools and legal liability for the unauthorised use. This approach makes it possible not only to identify areas of legislative

[1] Regulation of the European Parliament and of the Council No. 910/2014 "On Electronic Identification and Trust Services for Electronic Transactions in the Internal Market and Repealing Directive 1999/93/EC". (2014, July). Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32014R0910.
[2] Law of Ukraine No. 80/94-VR "On Information Protection in Information and Telecommunications Systems". (1994, July). Retrieved from https://zakon.rada.gov.ua/laws/show/80/94-вр.
[3] Law of Ukraine No. 803-XIV "On Cryptographic Protection of Information". (1999, December). Retrieved from https://zakon.rada.gov.ua/laws/show/803-14.

uncertainty, but also to formulate initial provisions for updating the regulatory framework in line with international practices. To visualize the correlation of key legal parameters, a generalised Table 1 is presented below. It reflects the content of the relevant legal and regulatory acts according to the criteria of regulatory subject, categories of entities, requirements for technical tools, institutional control, and legal liability measures in cases of violation of the established procedure for the application of CPI. Such structuring lays the groundwork for further comparative analysis of the effectiveness of legal enforcement practices.

Table 1. Comparative characteristics of Ukrainian laws in the field of cryptographic information protection

Criterion	Law of Ukraine No. 80/94-VR[1]	Law of Ukraine No. 803-XIV[2]
Subject of regulation	Information protection in information and telecommunications systems through the use of technical and software and hardware methods	Organisation, implementation, and regulation of cryptographic protection of restricted access information
Circle of subjects	Owners of information and telecommunications systems, information managers, security administrators, authorised bodies	Business entities developing, supplying or operating CPI and government bodies
Requirements for technical means	The need for certification and compliance of equipment with established safety requirements has been identified	The mandatory nature of state expertise, certification, and the use of only permitted means is outlined.
Control	Control is carried out by relevant state authorities through security audits of information and telecommunications systems.	Licensing, control by the State Service of Special Communications and Information Protection of Ukraine, maintenance of the state register of certified CPI devices
Responsibility	Administrative liability for violation of information protection requirements in information and telecommunications systems	Liability for using uncertified CPIs and conducting activities without a licence

Source: developed by the authors

Comparative Table 1 illustrates the distribution of regulatory functions and the structural differentiation of legal benchmarks in the field of cryptographic information protection. The Law of Ukraine No. 80/94-VR focuses on ensuring the integrity of information infrastructure through technical regulation, which provides for mandatory certification of protection tools, compliance with technical security policies, and the exercise of administrative control. Meanwhile, the Law of Ukraine No. 803-XIV focuses on narrowly specialised aspects of cryptography as a component of information security, providing for licensing of entities, evaluation of cryptographic solutions, and the maintenance of state records of CPI tools.

The functional division of the circle of entities covered by these laws highlights differences in the purpose of regulatory oversight: in the first case, it concerns owners, administrators, and users of information and telecommunications systems; in the second – producers, developers, integrators, and suppliers of CPI tools. This model enables the construction of a hierarchical responsibility structure, in which general information security requirements are specified through a specialised cryptographic control regime. At the same time, a lack of coordination between these subsystems becomes evident, creating grounds for reviewing and updating approaches to the interaction within a unified cybersecurity system.

Within the study of legal and regulatory approaches to cryptographic information protection, it is also important to determine the level of compliance of Ukrainian legislation with international regulatory frameworks. Due to increased demands for cryptographic security of digital platforms – particularly in the areas of key management, CPI tool certification, electronic identification support, and IT product security assessment – the need for harmonising national regulation with standards such as ISO/IEC No. 15408-1 (2009), the European Telecommunications Standards Institute (2016a), the European Union Agency for Cybersecurity (2014), and the recommendations of the National Institute of Standards and Technology (2020) is growing. In this context, Table 2 systematises the compliance of key Ukrainian information security documents with international requirements and allows for an assessment of the current level of legal and technical alignment.

[1] Law of Ukraine No. 80/94-VR "On Information Protection in Information and Telecommunications Systems". (1994, July). Retrieved from https://zakon.rada.gov.ua/laws/show/80/94-вр.
[2] Law of Ukraine No. 803-XIV "On Cryptographic Protection of Information". (1999, December). Retrieved from https://zakon.rada.gov.ua/laws/show/803-14.

Table 2. Compliance of Ukrainian regulatory documents with international standards in the field of CPI

Regulatory document of Ukraine	International standard/document	Comment on compliance
Law of Ukraine No. 803-XIV[1]	National Institute of Standards and Technology SP 800-57, ISO/IEC No. 19790 (2012) – cryptographic key management policy	Provisions are partially harmonised; related principles of key information security policies are used
Law of Ukraine No. 80/94-VR[2]	ISO/IEC No. 27001 (2022) – information security management system	A general information security model is regulated in accordance with ISO No. 27001 (2022), partial coverage
Decree of the President of Ukraine No. 447/2021[3]	ISO/IEC No. 15408-1 (2009) (Common Criteria) – requirements for assessing the security of IT products	Technical requirements are adapted to Common Criteria; national compliance profile is used
Licensing conditions for the provision of services in the field of CPI	eIDAS[4], European Union Agency (2014) for Cybersecurity Guidelines – regulation of electronic identification and cryptographic services	The main requirements are harmonised; differences in the procedure for recognising and using electronic signatures remain

Source: developed by the authors

The analysis of Table 2 demonstrates a gradual, albeit uneven, integration of the national regulatory framework in the field of cryptographic information protection into the architecture of international regulatory standards. Despite existing differences in certification systems, the structure of cryptographic policies, and methods of subject identification, there is a clear movement towards the implementation of the provisions of ISO/IEC No. 15408-1 (2009), ISO/IEC No. 18033-1 (2021), the European Telecommunications Standards Institute (2016a), and the recommendations of the National Institute of Standards and Technology (2020). Particular attention has been given to the adaptation of key management procedures, technical audits of CPI tools, and minimum security criteria aligned with international profiles.

At the same time, Ukrainian regulation retains specific features, driven by the need to align legal norms with national models for the functioning of information systems. This is reflected, in particular, in differences in the procedure for recognising electronic signatures, limited application of unified electronic seal formats, and the absence of a centralised trust infrastructure. In view of this, the further development of harmonisation policy requires not only the formal alignment of technical requirements but also the updating of cross-border verification procedures, standardisation of post-quantum algorithms, and formalisation of mutual recognition of cryptographic certificates.

Within the analysis of the legal and regulatory support for cryptographic information protection, special attention should be paid to the mechanisms of state oversight and legal liability instruments for non-compliance with established requirements. Law enforcement practice in this area serves not only a supervisory but also a preventive function, creating an environment with heightened responsibility for subjects of information interaction. This issue becomes particularly relevant given the increasing role of CPI in public administration, the financial sector, national defence, and digital identity verification. To systematise the main types of violations, corresponding legal measures, and authorities authorised to exercise control, it is appropriate to refer to the generalised Table 3. It provides a structural classification of institutional powers, types of sanctions, and typical oversight application domains, allowing for a comprehensive assessment of the effectiveness of state regulation in the area of legal enforcement within the field of cryptographic protection.

Table 3. Types of CPI violations, sanctions and regulatory authorities

CPI violation type	Liability/sanctions	Competent control authority
Illegal use of uncertified CPI tools	Administrative liability under Article 188-39 of the Code of Ukraine on Administrative Offences[5]: fine up to UAH 1,700 with confiscation of equipment	State Service of Special Communications and Information Protection of Ukraine

[1] Law of Ukraine No. 803-XIV "On Cryptographic Protection of Information". (1999, December). Retrieved from https://zakon.rada.gov.ua/laws/show/803-14.
[2] Law of Ukraine No. 80/94-VR "On Information Protection in Information and Telecommunications Systems". (1994, July). Retrieved from https://zakon.rada.gov.ua/laws/show/80/94-вр.
[3] Decree of the President of Ukraine No. 447/2021 "On the Decision of the National Security and Defence Council of Ukraine of May 14, 2021 "On the Cybersecurity Strategy of Ukraine". (2021, August). Retrieved from https://zakon.rada.gov.ua/laws/show/96/2021.
[4] Regulation of the European Parliament and of the Council No. 910/2014 "On Electronic Identification and Trust Services for Electronic Transactions in the Internal Market and Repealing Directive 1999/93/EC". (2014, July). Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32014R0910.
[5] Code of Ukraine on Administrative Offenses. (1984, December). Retrieved from https://zakon.rada.gov.ua/laws/show/80731-10.

Table 3, Continued

CPI violation type	Liability/sanctions	Competent control authority
CPI activities without a licence	Administrative liability under Article 164 of the Code of Ukraine on Administrative Offences[1]: fine from 17,000 to 34,000 UAH with confiscation of equipment	State Service of Special Communications and Information Protection of Ukraine, National Police (in cases of business activity without a licence)
Disclosure or leakage of key information	Criminal liability under Art. 328 or 361 Criminal Code of Ukraine[2]: up to 5 years of imprisonment	Security Service of Ukraine, National Police, Prosecutor's Office
Improper storage or transfer of cryptographic protection means	Warning or fine in accordance with the internal regulations of the State Service of Special Communications and Information Protection of Ukraine or based on the results of the audit	State Service of Special Communications and Information Protection of Ukraine, information security auditors
Use of cryptographic algorithms not permitted for use	Suspension of the certificate of conformity; requirement to remedy the violation	State Service of Special Communications and Information Protection of Ukraine, Technical Committee for Certification

Source: developed by the authors based on Law of Ukraine No. 3475-IV[3], Law of Ukraine No. 803-XIV[4]

The analysis of Table 3 confirms the existence of a multi-level system of legal liability in the field of cryptographic information protection in Ukraine. Under the current legislation, both administrative and criminal sanctions are provided depending on the nature and consequences of the violation. Particular attention is given to liability for conducting activities without a licence, violating certification procedures, and using uncertified CPI tools, which directly impacts the guarantees of confidentiality, integrity, and availability of critically important information in IT systems. The competence of state authorities responsible for supervision in this area is regulated, particularly the State Service of Special Communications and Information Protection of Ukraine, which is authorised not only to impose fines but also to initiate the suspension or termination of operation of tools that do not meet approved requirements. This mechanism ensures both reactive and preventive functions in response to threats associated with the use of vulnerable or illegitimate CPI. The application of criminal liability in cases of unauthorised disclosure or leakage of cryptographic information that constitutes state secrets or is protected within restricted access systems demonstrates the existence of legal instruments focused on protecting critical elements of national security. At the same time, there is a modern need to improve violation detection procedures, particularly through the introduction of digital monitoring mechanisms, post-audit procedures, and risk indicators in the application of CPI.

To ensure effective control, it is advisable to revise interaction practices among state oversight entities performing sanctioning, supervisory, and analytical functions. Specifically, coordination between the State Service of Special Communications and Information Protection of Ukraine, the Security Service of Ukraine, and the National Police of Ukraine should provide for joint responses to violations of cryptographic protection requirements, harmonisation of certification procedures for protective tools, and the rapid exchange of analytical information. Improving the reporting system, introducing transparent decision-making mechanisms, and enhancing the analytical capacity of oversight bodies will serve as an institutional precondition for building trust in the regulator and ensuring the sustainable development of the enforcement environment in the field of cryptographic protection.

Institutional architecture and regulatory powers of the state in the field of cryptographic protection. Within the study of state governance in the field of cryptographic information protection, the analysis of the institutional architecture of the body tasked with implementing the relevant policy becomes crucial. The activities of the State Service of Special Communications and Information Protection of Ukraine, as the central executive authority, are defined by a multi-component structure that includes a functional division of responsibilities among administrative, technical, expert, and supervisory units. This model is aimed at ensuring subject-specific specialisation, consistency in conformity assessment processes, certification, regulatory supervision, and operational response.

The internal distribution of competencies within the State Service of Special Communications and Information Protection of Ukraine is based on the principle of integrated implementation of regulatory and technical tasks. This includes the development of CPI requirements, conducting evaluations, certification, maintaining registers, and coordinating with other cybersecurity bodies. Such an approach avoids

[1] Code of Ukraine on Administrative Offenses. (1984, December). Retrieved from https://zakon.rada.gov.ua/laws/show/80731-10.
[2] Criminal Code of Ukraine. (2001, April). Retrieved from https://zakon.rada.gov.ua/laws/show/2341-14.
[3] Law of Ukraine No. 3475-IV "On the State Service for Special Communications and Information Protection of Ukraine". (2006, February). Retrieved from https://zakon.rada.gov.ua/laws/show/911-2006-п.
[4] Law of Ukraine No. 803-XIV "On Cryptographic Protection of Information". (1999, December). Retrieved from https://zakon.rada.gov.ua/laws/show/803-14.

duplication of functions, ensures hierarchical subordination, and optimises processes of licensing, standardisation, and post-control compliance of cryptographic protection tools.

To visualise the institutional configuration and reflect specialised responsibilities, Table 4 is presented below. It summarises the functional division of responsibilities among the four key structural units of the State Service of Special Communications and Information Protection of Ukraine, which play a decisive role in the organisation and implementation of state policy in the field of cryptographic security. This approach makes it possible to clearly identify the areas of responsibility for each component of the institutional system, providing the basis for further analysis of the effectiveness of the interaction.

Table 4. Functional division of powers between the divisions of the State Service of Special Communications and Information Protection of Ukraine

Unit	Main functions
Administration	General management of the service; strategic planning; coordination of interaction with other bodies
Expert units	Conducting state examination of CPI equipment; preparation of conclusions on compliance; analysis of characteristics
Technical Committee for Standardisation	Development of technical requirements for CPI; adaptation of international standards; maintenance of national compliance profiles
Licensing and Certification Department	Acceptance of applications; organisation of certification procedures; maintenance of registers; monitoring of compliance with conditions

Source: developed by the authors based on Law of Ukraine No. 3475-IV[1]

The analysis of Table 4 allows concluding that there is a structured functional division of responsibilities within the unified system of state governance in the field of cryptographic information protection. The administrative level of the State Service of Special Communications and Information Protection of Ukraine is responsible for strategic planning, managerial coordination, and organisational support in the implementation of CPI policy. Expert departments carry out professional evaluation of cryptographic solutions subject to certification, conduct technical examinations, and formalise conclusions on the compliance of tools with approved technical profiles.

The Technical Standardisation Committee plays a key role in the development of regulatory and technical documents and in the implementation of international approaches, in particular by adapting standards such as ISO/IEC No. 15408-1 "Evaluation criteria for IT security" (2009), ISO/IEC No. 18033-1 "Encryption algorithms" (2021), ISO/IEC No. 19790 "Security requirements for cryptographic modules" (2012), European Telecommunications Standards Institute (2016a; 2016b; 2018), and the European Union Agency for Cybersecurity (2014) to the national regulatory environment. Its activities ensure methodological consistency in certification procedures and unify the criteria for assessing cryptographic security. The Licensing and Certification Department, in turn, is responsible for administering procedures for granting market entities access to provide cryptographic services, verifying compliance with licensing conditions, as well as maintaining certificate renewals and state records.

This division ensures subject-specific specialisation of each unit, which helps to improve the effectiveness of regulatory functions and simplifies communication mechanisms with market participants, licensing authorities, CPI users, and international partners. The internal structure of the State Service of Special Communications and Information Protection of Ukraine corresponds to the typical model of European regulators, which provides for the separation of strategic, technical, expert, and supervisory functions to enhance transparency and reasoned decision-making.

Within the general architecture of cryptographic security governance, coordination among bodies whose powers are distributed across analytics, supervision, law enforcement, and counterintelligence remains crucial. Inter-agency cooperation ensures the functional continuity of processes of prevention, detection, and response to incidents involving violations of the cryptographic information protection regime. To systematise the distribution of responsibilities and cooperation mechanisms among actors in the national cybersecurity system, Table 5 is presented below, summarising the key tasks, coordination formats, and institutional responsibilities of the main bodies involved in CPI policy implementation.

[1] Law of Ukraine No. 3475-IV "On the State Service for Special Communications and Information Protection of Ukraine". (2006, February). Retrieved from https://zakon.rada.gov.ua/laws/show/911-2006-п.

Table 5. Interaction of key bodies in the field of cryptographic protection

Authority	Main tasks in the field of CPI	Forms of coordination	Form of responsibility
State Service of Special Communications and Information Protection of Ukraine	Development of regulatory framework; CPI certification; licensing; technical audit; record keeping	Participation in interdepartmental working groups; coordination with other bodies of regulations and standards	Regulatory responsibility; ensuring technical compliance and certification
National Security and Defence Council of Ukraine	Formation of strategic decisions in the field of cyber defence; coordination of interdepartmental policy	Decision of the National Security and Defence Council of Ukraine; control of the implementation of the cybersecurity strategy through the National Coordination Centre	Political responsibility for the implementation of national decisions in the field of information security
Security Service of Ukraine	Counterintelligence activities in the field of protecting state secrets; investigation of information leaks	Information exchange with the State Service of Special Communications and Information Protection of Ukraine; participation in joint inspections; prompt response to incidents	Criminal procedural liability within the framework of the Criminal Procedure Code of Ukraine[1]; protection of state secret objects
National Police of Ukraine	CPI compliance monitoring	Joint activities with the State Service of Special Communications and Information Protection of Ukraine; coordination of actions in case of violations; prompt reporting of incidents	Criminal and administrative liability within the framework of pre-trial investigation

Source: developed by the authors based on National Security and Defence Council of Ukraine (n.d.), Security Service of Ukraine (n.d.), National Police of Ukraine (n.d.)

The analysis of Table 5 indicates the existence of a coordinated functional distribution among the key bodies involved in the implementation of state policy in the field of cryptographic information protection. The State Service of Special Communications and Information Protection of Ukraine performs the functions of the central regulator, responsible for the development of technical standards, certification of CPI tools, maintenance of state registers, and expert evaluation of technical solutions. Its activities provide the technological and administrative foundation for building a trusted environment in the field of cryptographic security.

The National Security and Defence Council of Ukraine plays a strategic role in setting priorities in the field of cyber protection, in particular through the approval of conceptual documents, coordination of interdepartmental measures, and monitoring the effectiveness of plan implementation within the framework of the National Cybersecurity Coordination Centre. This institutional level creates the framework conditions for uniting the efforts of executive authorities, security forces, and analytical platforms.

The Security Service of Ukraine and the National Police of Ukraine operate within the law enforcement vertical, ensuring compliance with legislation in the field of cryptographic protection. The powers of the Security Service of Ukraine cover the protection of state secrets, the maintenance of counterintelligence regimes in systems with restricted access, and the identification of threats related to the use of CPI tools in critical infrastructure. The National Police focuses on investigating cyber incidents, administrative violations, and the procedural support of crimes related to the unauthorised use of CPI.

This model of interaction is based on a combination of preventive, regulatory, analytical, and law enforcement functions within an integrated institutional system that corresponds to the principles of multi-level information security governance. Ensuring the resilience of cryptographic infrastructure requires continuous coordination among these entities, as well as the updating of rapid response mechanisms, joint audits, and the exchange of technical threat indicators. This approach makes it possible to build an integrated architecture of state governance in the field of CPI, focused on proactive response and maintaining a high level of technological readiness.

Technical standards and cryptographic protection: Modern solutions and certification requirements. Modern technical approaches to cryptographic information protection are based on the use of cryptographic algorithms that must meet criteria of cryptographic robustness, functional compatibility with information systems, and performance in data processing. Over the last decades, classical symmetric and asymmetric cryptographic algorithms – in particular AES, RSA, and ECDSA – have remained dominant. These algorithms provide a sufficient level of protection under the classical computing model; however, the algorithms lose effectiveness in the context of quantum technology development, especially under the influence of Shor's and Grover's algorithms, which can significantly reduce the cryptographic complexity of existing ciphers.

Taking into account these threats from quantum computing, the National Institute of Standards and Technology (2020) launched an open competition to standardise algorithms resistant to quantum attacks. As a result of years of testing, several finalists were

[1] Procedure Code of Ukraine. (2012, April). Retrieved from https://zakon.rada.gov.ua/laws/show/4651-17#Text.

selected, including CRYSTALS-Kyber, CRYSTALS-Dilithium, SABER and others, which form the core of the future PQC standard. These algorithms are based on different mathematical approaches – lattice problems, polynomial homomorphy, code-based structures, and multivariate systems – providing high resistance to attacks using quantum computing machines.

The comparison of classical and post-quantum algorithms is of significant practical importance in the design of CPI technical tools, especially in government and critical information systems. Key characteristics for such analysis include the type of cryptographic scheme, key length, estimated resistance to classical and quantum attacks, as well as the current certification status based on evaluations by the National Institute of Standards and Technology. This approach enables the development of well-grounded recommendations for the gradual implementation of post-quantum algorithms into technical profiles approved by the State Service of Special Communications and Information Protection of Ukraine and helps to avoid the risks associated with outdated cryptographic implementations. To systematise the core characteristics of the most widespread classical crypto-algorithms and prospective post-quantum solutions, Table 6 is provided below. It enables comparative analysis according to basic parameters: type of cryptographic algorithm, key length, resistance level, and certification status. The information presented is relevant for assessing the technical compliance of CPI tools with current and future security standards.

Table 6. Characteristics of classical and post-quantum crypto algorithms

Algorithm name	Type	Key length (bits)	Resistance to attacks	Certification status
RSA-2048	Asymmetric	2048	Medium (vulnerable to quantum attacks)	Standardised (National Institute of Standards and Technology)
ECDSA P-256	Asymmetric	256	Medium (vulnerable to quantum attacks)	Standardised (National Institute of Standards and Technology)
AES-256	Symmetrical	256	High (resistant to Grover attack)	Standardised (National Institute of Standards and Technology)
CRYSTALS-Kyber	Post-quantum (KEM)	768/1024/1536	High (Quantum computing resistant)	Recommended for standardisation (National Institute of Standards and Technology PQC)
Dilithium	Post-quantum (signature)	2048/3072/4096	High (Quantum computing resistant)	Recommended for standardisation (National Institute of Standards and Technology PQC)
SABER	Post-quantum (KEM)	992/1312/1984	High (Quantum computing resistant)	Finalist of the National Institute of Standards and Technology PQC competition

Note: KEM – Key Encapsulation Mechanism
Source: developed by the authors based on ISO/IEC No. 18033-1 (2021), ISO/IEC No. 19790 (2012), European Union Agency for Cybersecurity (2014)

The comparative analysis presented in Table 6 includes digital parameters that allow for a quantitative assessment of the cryptographic strength of algorithms. One of the key criteria is the length of the cryptographic key, which directly correlates with the level of computational complexity for an attacker. In this context, post-quantum algorithms demonstrate significantly higher parameter values. For example, the CRYSTALS-Dilithium algorithm provides for a key length of up to 4096 bits, which exceeds the typical characteristics of classical signature algorithms such as RSA or ECDSA, which use keys of 2048-3072 bits or 256 bits, respectively. The presence of a certification status indicator allows for the evaluation of the level of practical implementation of cryptographic solutions. Classical algorithms have attained international standard status and are components of approved cryptographic profiles, particularly in the recommendations of the National Institute of Standards and Technology (2008; 2019; 2020) and ISO/IEC No. 15408-1 (2009), ISO/IEC No. 18033-1 (2021), ISO/IEC No. 19790 (2012), ISO/IEC No. 7816-4 (2020). Meanwhile, post-quantum algorithms are in the final stages of standardisation, but already demonstrate high potential compliance with protection requirements under quantum computing conditions. This fact provides a foundation for the inclusion in future technical security policies, including at the level of regulations by the State Service of Special Communications and Information Protection of Ukraine, considering the dynamics of post-quantum environment development.

Within the framework of certification and technical regulation of cryptographic protection, the classification of hardware tools implementing key cryptographic functions – such as encryption, authentication, and key generation and storage – is also essential. These hardware-software systems serve as the basic elements of the information security architecture and enable the implementation of cryptographic policy at the level of transactions, state digital services, digital identification systems, and critical infrastructure. The typologisation of CPI tools by functional characteristics, standards

compliance, and application domain allows for the evaluation of the relevance for integration into specialised and multi-segment security solutions.

To systematise the characteristics of such tools, Table 7 is presented below, which summarises the main types of hardware components for cryptographic information protection according to the criteria of device type, implemented functions, compliance standard, and intended use. This approach enables instrumental support for the process of selecting technical solutions in line with the specifics of sectoral tasks and regulatory constraints.

Table 7. CPI hardware classification

Device type	Cryptographic functions	Compliance standard	Scope of use
HSM	Key generation/storage, signing, encryption, authentication	FIPS 140-2 Level 3, ISO/IEC No. 19790 (2012)	State registers, financial transactions, certification centres
Cryptographic token (USB)	Key storage, signature, PIN access	FIPS 140-2 Level 2, ISO/IEC No. 7816-4 (2020)	E-government, digital signature of citizens
Smart card with cryptographic module	Authentication, digital signature, certificate storage	ISO/IEC No. 7816-4 (2020), European Telecommunications Standards Institute TS 102 221	Bank cards, ID documents, access to IT systems
Secure microcontroller (embedded device)	Encryption/decryption, authentication, key protection in IoT systems	ISO/IEC No. 15408 (2009), EAL4+, PSA Certified	Embedded devices, telematics, industrial IoT systems
Virtualised HSM (vHSM)	Key generation, signing, encryption in the cloud environment	ISO/IEC No. 19790 (2012), FIPS 140-3 (in the process of certification)	Cloud services, e-commerce, public cloud platforms

Note: HSM – Hardware Security Module; EAL – Evaluation Assurance Level; PSA – Platform Security Architecture; IoT – Internet of Things; vHSM – Virtualised Hardware Security Module
Source: developed by the authors

Table 7 summarises the types of hardware components that implement the functionality of cryptographic information protection tools, differentiated by architecture, functional purpose, and level of compliance with international security standards. The highest certification reliability indicators are demonstrated by HSMs that meet the requirements of FIPS 140-2 Level 3 (National Institute of Standards and Technology, 2001) or ISO/IEC No. 19790 (2012), and serve as key technological elements in protecting critical cryptographic operations – particularly in certification centres, financial platforms, and national digital signature systems. Meanwhile, smart cards and USB tokens have limited functionality but, due to the ease of implementation and compatibility with popular authentication protocols, are widely used in e-government and registry access systems.

A separate category consists of virtualised HSMs (vHSMs) and secure microcontrollers, which, despite the absence of definitive certification stability, show high potential for use in cloud infrastructure environments, hybrid models of key information storage, and industrial IoT systems. The implementation is becoming increasingly relevant in the context of the gradual migration of national information services to cloud-based architecture, where decentralised cryptographic modules with remote control are needed. This typology makes it possible to conduct a technical-functional assessment of the level of integration of hardware CPI into modern information systems, taking into account certification requirements, compliance with standards, and implementation flexibility.

In the context of further harmonisation of regulatory and technical standards for CPI tools with European and international requirements, it is important to analyse the degree of compliance of national technical norms with the provisions of leading standards and regulations. Of particular importance are the standards of the European Telecommunications Standards Institute (2016a; 2016b; 2018) (in the areas of trust services and electronic signatures), the eIDAS[1] Regulation, and the technical recommendations of the European Union Agency for Cybersecurity (2014) in the fields of electronic identification, communication channel protection, and key management. The alignment of requirements between the State Service of Special Communications and Information Protection of Ukraine and these documents creates a regulatory and legal foundation for the cross-border functioning of public services, including the exchange of certificates, digital signatures, and the verification of identified subjects within the EU.

To illustrate the compliance status of key Ukrainian regulatory documents with the technical requirements of the European Telecommunications Standards Institute (2016a; 2016b; 2018), eIDAS, and the European Union Agency for Cybersecurity (2014), Table 8 is provided below. It reveals the level of harmonisation

[1] Regulation of the European Parliament and of the Council No. 910/2014 "On Electronic Identification and Trust Services for Electronic Transactions in the Internal Market and Repealing Directive 1999/93/EC". (2014, July). Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32014R0910.

across specific types of cryptographic services and protocols that are crucial for Ukraine's integration into the European Digital Market and the establishment of a unified trust infrastructure.

Table 8. Compliance of Ukrainian technical requirements for CPI with international standards

Service type/protocol	Ukrainian technical requirements	Relevant international standards	Degree of compliance
Qualified electronic signature	Use of certified CPIs; storage of keys on tokens; DSTU 4145 (2002), DSTU 7624 (2014)	European Telecommunications Standards Institute EN 319 411-2, eIDAS[1] Annex I, XAdES, CAdES	High (adapted to European formats and algorithms)
Key management	Key management policies; security profiles; compliance with a comprehensive information security system	European Union Agency for Cybersecurity Guidelines Cryptographic Solutions, National Institute of Standards and Technology SP 800-57	Medium (not fully unified policies and key rotation)
Communication channel encryption	Mandatory use of TLS with Key Certification Authority certificates; cryptographic algorithms according to the CPI registry	European Telecommunications Standards Institute TS 103 097, ISO/IEC 27033-5 (2016), National Institute of Standards and Technology SP 800-52r2	High (certificate formats and cryptographic algorithms are agreed upon)
Digital identification	Qualified electronic signature tools + identification in the Unified State Register of Legal Entities or ID card; verification of the reliability of the supplier	eIDAS Regulation[2], European Telecommunications Standards Institute EN 319 401	Medium (lack of full interaction with eID and eIDAS Bridge)
Trust services (timestamp, seal)	Qualified service systems with CPI certification, archiving and registration in the National Cybersecurity Coordination Centre registry	European Telecommunications Standards Institute EN 319 421, eIDAS Trusted Services, European Union Agency for Cybersecurity Trust Services Guidelines	High (at the level of procedures and technical regulations)

Source: developed by the authors based on Law of Ukraine No. 3475-IV "On the State Service for Special Communications and Information Protection of Ukraine"[3], National Institute of Standards and Technology (2001; 2008; 2020), European Union Agency for Cybersecurity (2014), European Telecommunications Standards Institute (2016a; 2016b; 2018)

The analysis of Table 8 confirms a high degree of conformity between Ukrainian technical requirements and international regulations in the areas of electronic signatures, cryptographic key management, communication channel encryption, and the provision of trust services. The most harmonised areas appeared to be those related to electronic signatures – Ukraine has already implemented cryptographic algorithms, signature formats, and verification protocols in accordance with the XAdES, CAdES specifications and the requirements of eIDAS Annex I. Similarly, the implementation of timestamp and digital seal procedures is based on the requirements set out by the European Telecommunications Standards Institute (2016b), ensuring technological compatibility with European trust platforms.

At the same time, certain areas – particularly digital identification and cryptographic key management – demonstrate the presence of systemic barriers. The main issues include the absence of an integrated eID gateway for cross-border interaction, as well as an underdeveloped key rotation model in line with the recommendations of the European Union Agency for Cybersecurity (2014) and the National Institute of Standards and Technology (2020). These limitations reduce the efficiency of integration with the European trust space and complicate the technical implementation of unified authentication protocols. Addressing the identified shortcomings requires the implementation of interoperable interfaces, harmonised trust management schemes, and technical regulations at the level of intergovernmental coordination.

Despite these challenges, the overall architecture of national technical requirements in the CPI sector shows a stable trend towards unification with the European cyber environment. The measures taken to implement algorithmic compatibility, adapt cryptographic formats, and align certification procedures are forming the regulatory-technological basis for further development of cross-border cooperation. This, in turn, lays the groundwork for Ukraine's full integration into the European Digital Market and inclusion in the pan-European trust infrastructure in the context of e-governance, financial transactions, and the exchange of legally significant electronic data.

Promising directions for the development of state policy in the field of cryptographic protection in the context of digital transformation. In the process of digital transformation of public administration, the issue of legal and technical harmonisation of national legislation in the field of cryptographic

[1] Regulation of the European Parliament and of the Council No. 910/2014 "On Electronic Identification and Trust Services for Electronic Transactions in the Internal Market and Repealing Directive 1999/93/EC". (2014, July). Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32014R0910.
[2] Ibidem, 2014.
[3] Law of Ukraine No. 3475-IV "On the State Service for Special Communications and Information Protection of Ukraine". (2006, February). Retrieved from https://zakon.rada.gov.ua/laws/show/911-2006-п.

information protection with EU regulatory requirements is of particular importance. The eIDAS 2.0 Regulation is the central EU legal act[1] establishing unified rules for electronic identification, qualified electronic signatures, electronic seals, and trust services. This document defines not only the functional requirements for the relevant services but also the technical parameters that cryptographic mechanisms, key information carriers, signature generation protocols, and rules for mutual recognition must comply with.

In the context of implementing the provisions of the Association Agreement between Ukraine and the EU, a priority task is to assess the level of conformity of the national regulatory and technical framework with the requirements set out in eIDAS 2.0, particularly concerning the use of certified CPI tools in state digital services.

Special attention is given to the technical compatibility of national qualified electronic signature tools with European signature formats, the interoperability of timestamp and seal mechanisms, and ensuring the legal validity of cross-border digital identification. To systematise the points of convergence and identify existing discrepancies between the provisions of Ukrainian legislation and the norms of eIDAS 2.0, Table 9 is presented below. It summarises the analysis of four key areas that form the foundation of digital trust infrastructure: qualified electronic signature, electronic identification, timestamp, and electronic seal. The comparison is made based on the parameters of regulatory content, technical requirements for the implementation of respective services, and the overall level of harmonisation between the Ukrainian and European systems of standards.

Table 9. Comparison of eIDAS 2.0 requirements and Ukrainian legislation regarding CPI

Direction	eIDAS 2.0 regulations	Requirements of Ukrainian legislation	Degree of harmonisation
Electronic signature	Definition of qualified electronic signature; mandatory use of certified means; unified signature format (XAdES, PAdES)	Use of qualified electronic signature on tokens; DSTU 4145 (2002), DSTU 7624 (2014); certification by the Key Certification Centre	High (by algorithms and media, but not entirely by formats)
Identification	Unified eID for cross-border use; mandatory recognition of digital identity in all EU member states	Identification via ID card, Unified State Register of Legal Entities or Mobile ID; no mandatory cross-border recognition	Medium (no integration into eIDAS Bridge)
Timestamp	Trusted timestamp providers with mandatory certification; evidence preservation according to the European Telecommunications Standards Institute standard	Provision of timestamp services based on national Key Certification Centres; lack of adaptation to European Telecommunications Standards Institute TS 102 023	Low (local policies not in line with European standards)
Electronic seal	Use of secure seal creation tools; legal identification by automated trust services	Signature of legal entities within the framework of qualified electronic signature; use of standard CPIs ; lack of verification automation	Medium (partial compliance without service infrastructure)

Note: XAdES, PAdES are electronic signature formats according to the European Telecommunications Standards Institute

Source: developed by the authors

The analysis of Table 9 makes it possible to identify both key achievements and critical gaps in the harmonisation of Ukrainian cryptographic information protection tools with European requirements. The most adapted areas are those related to the implementation of qualified electronic signatures, where the conformity of algorithms, carriers, and formats (particularly XAdES and CAdES) with the provisions of eIDAS Annex I is noted. Meanwhile, areas related to timestamps and electronic seals remain partially incompatible with the technical specifications of the European Telecommunications Standards Institute (2016b), especially in aspects of validation procedures, centralised management, and trust identifiers.

The provisions on digital identification and trust services require further harmonisation, particularly through accession to the cross-border eIDAS Bridge mechanism and the implementation of a national certification model in accordance with the framework standards of the European Telecommunications Standards Institute (2016a) and the recommendations of the European Union Agency for Cybersecurity (2014). The underdevelopment of an interoperable infrastructure for mutual recognition of identifiers and certificates limits Ukraine's ability to participate in the single European digital trust space, which reduces the effectiveness of legally significant transactions and document flow.

Thus, the generalised analysis indicates the need to modernise the regulatory and technical base towards full cryptographic compatibility with European standards. This includes not only the adaptation of cryptographic algorithms, formats, and certification policies, but also the revision of audit mechanisms, post-certification monitoring, verification procedures,

[1] Regulation of the European Parliament and of the Council No. 910/2014 "On Electronic Identification and Trust Services for Electronic Transactions in the Internal Market and Repealing Directive 1999/93/EC". (2014, July). Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32014R0910.

and supervision over the use of CPI tools. Improvement of these components is a necessary prerequisite for Ukraine's inclusion in the EU digital ecosystem, particularly in the area of trust services, digital identification, and electronic document management.

Within the strategic development of state policy in the field of cryptographic protection, a key task is to enhance the effectiveness of the regulatory activity of the State Service of Special Communications and Information Protection of Ukraine. Given the transformational challenges associated with the implementation of post-quantum cryptographic algorithms, the growing volume of state digital services, and the expansion of critical information infrastructure, the need to functionally expand the regulator's competences is becoming more urgent. The systematic implementation of unified technical models for auditing, certification, post-monitoring, and response should be based on risk-oriented approaches to the evaluation of CPI tools. To present such an approach, Table 10 below summarises the prospective regulatory functions of the State Service of Special Communications and Information Protection of Ukraine under conditions of digital transformation.

Table 10. Prospective regulatory powers of the State Service of Special Communications and Information Protection of Ukraine by functions

Function	Promising powers	Regulatory effect
Audit	Conducting post-certification technical audits of CPI tools in critical information systems; creating a risk-indexed audit registry	Strengthening control over the actual use of certified CPIs; identifying discrepancies in the field
Certification	Expanding the scope of certification to include hybrid cryptographic schemes and post-quantum algorithms; implementing a model of mutual recognition of certificates	Increasing the technological compliance of certified solutions to modern cryptographic challenges
Monitoring	Creation of an automated cryptographic monitoring system to detect uncertified tools and vulnerabilities in real time	Ensuring preventive risk identification and increasing the efficiency of regulatory influence
Reaction	Formation of specialised cryptographic incident response teams; participation in CERT/CSIRT; coordination with the National Police, Security Service of Ukraine, National Cybersecurity Coordination Centre	Reducing threat response time; centralising interaction processes in cryptographic incidents

Note: CERT/CSIRT – Computer Emergency Response Team/Computer Security Incident Response Team
Source: developed by the authors

Table 10 systematises the priority directions for strengthening the regulatory function of the State Service of Special Communications and Information Protection of Ukraine, taking into account the full life cycle of cryptographic tools – from development and certification to operation, control, and incident response. In the audit sphere, the introduction of post-certification inspections is proposed, involving technical audits of CPI under real operating conditions. This would allow for the timely detection of deviations from established parameters, the identification of implementation shortcomings, and the formation of feedback for developers of protective tools.

The certification component should transform towards dynamic responsiveness to technological challenges, primarily by incorporating post-quantum algorithms into national cryptographic profiles and implementing mechanisms for mutual recognition of technical certificates with certification bodies of other jurisdictions. This would ensure the interoperability of protective tools and support Ukraine's participation in European trust schemes, particularly in the context of complying with eIDAS 2.0 requirements.

The functional monitoring block envisages a shift from a predominantly reactive to a preventive model of state control. This refers to the creation of a digital monitoring infrastructure for the circulation of CPI tools, enabling real-time detection of uncertified or vulnerable components. Such systems should be capable of autonomous signature analysis, tracking security policy violations, and supporting decisions to block dangerous objects before formal response procedures are initiated.

In the response section, emphasis shifts to the formation of specialised technical-analytical teams capable of rapid detection and neutralisation of incidents in cooperation with other actors of the national cybersecurity system – the Security Service of Ukraine, the National Coordination Centre for Cybersecurity, the Cyber Police, etc. This approach would foster the creation of an integrated model for managing cryptographic risks that combines institutional control, technological analytics, and adaptive regulation based on risk-oriented scenarios. It creates the preconditions for increasing the resilience of Ukraine's information infrastructure and its capacity to adapt to dynamically evolving threats.

The research findings demonstrated the existence of a formed regulatory and institutional framework for cryptographic information protection in Ukraine. The analysis of legal regulation showed that the key provisions of the Law of Ukraine No. 80/94-VR "On Information Protection in Information and Telecommunications Systems"[1] and Law of Ukraine No. 803-XIV

[1] Law of Ukraine No. 80/94-VR "On Information Protection in Information and Telecommunications Systems". (1994, July). Retrieved from https://zakon.rada.gov.ua/laws/show/80/94-вр.

"On Cryptographic Protection of Information"[1] form a complementary structure aimed at ensuring basic information security requirements. At the same time, it was found that inter-agency coordination, technical unification, and control over the circulation of CPI tools require further improvement at the level of regulations, procedures, and accountability.

The assessment of national regulation compliance with international standards – including ISO/IEC No. 15408-1 (2009), ISO/IEC No. 18033-1 (2021), ISO/IEC No. 19790 (2012), ISO/IEC No. 7816-4 (2013), European Telecommunications Standards Institute (2016a; 2016b; 2018), National Institute of Standards and Technology (2008; 2019; 2020), and eIDAS 2.0 – revealed significant harmonisation in the field of electronic signatures, timestamps, and certification procedures. However, gaps were identified in the implementation of electronic identification, key information protection, and integration into the cross-border trust infrastructure. Relevant tasks remain the creation of a centralised eID gateway, the introduction of key rotation mechanisms, and the adaptation of post-quantum cryptographic algorithms to the national technical profile.

Within the framework of the strategic development of state policy, it is recommended to strengthen the powers of the State Service of Special Communications and Information Protection of Ukraine by expanding its audit, certification, monitoring, and response functions. It is advisable to introduce risk-oriented management models, build a digital infrastructure for monitoring the circulation of CPI tools, and create technical-analytical response teams. Moreover, a key task is the development of a unified oversight architecture for CPI with integrated modules for digital monitoring, automated response, and risk analysis, which will ensure continuous control over compliance with cryptographic protection standards. Such an approach makes it possible to ensure institutional resilience of cryptographic protection, alignment with EU technical requirements, and integration into the European digital market based on mutual recognition of trust services. In this context, it is also appropriate to legally consolidate the model of mutual recognition of cryptographic solution certificates within the EU digital market and develop technical requirements for the use of post-quantum algorithms in public services, taking into account standards for cross-border information protection.

Discussion

The conducted study made it possible to outline the structural parameters of the regulatory model for cryptographic information protection that functioned under conditions of digital transformation of public administration. It was demonstrated that the current regulatory framework provided a basic level of technical control, certification of protective tools, and administrative supervision, but showed insufficient adaptability to challenges associated with the implementation of post-quantum solutions and ensuring cross-border trust. The analysis identified achievements in the standardisation of electronic signatures and timestamps, while also revealing institutional and functional barriers to the implementation of integrated solutions for digital identification, cryptographic key management, and unified interaction protocols with the European trust infrastructure. It was established that an effective response to these challenges required expanding the powers of regulatory actors, modernising audit tools, and implementing digital infrastructure for preventive monitoring.

Within the analysis of functional models for managing cryptographic security, it was found that the adaptability of the regulatory architecture remained a critical condition for implementing a digital protection strategy. This was confirmed in the study by G.S. Lampe (2023), which justified the advisability of introducing circular interaction models as a fundamental approach to ensuring the sustainability and coherence of security processes in digital systems. The study emphasised the necessity of cyclical interaction between technical, analytical, and regulatory subsystems as a prerequisite for the effective functioning of the security ecosystem. The results obtained were consistent with this position, as the identified need for the implementation of post-certification audits, risk-oriented tools, and procedural monitoring confirmed the relevance of a comprehensive approach to regulatory management.

The comparison of the provisions of national technical regulations with international CPI standards demonstrated partial harmonisation, primarily in components of electronic signature and timestamp. In this context, the analytics by P. López (2025), devoted to the National Security Framework as a regulatory model for compliance of cryptosystems with transnational requirements, proved relevant. The author identified key parameters for the certification of digital trust elements – qualified signature creation devices and cryptographic modules, which are regulated by eIDAS and the European Telecommunications Standards Institute standards. Comparative analysis confirmed the advisability of expanding the technical jurisdiction of national supervisory authorities, particularly in the field of compliance assessment of certified tools with the requirements of mutual recognition in the digital market.

Special attention within the study was paid to the issues of organisational interaction between information security actors, which significantly influenced the effectiveness of regulation in the field of cryptographic

[1] Law of Ukraine No. 803-XIV "On Cryptographic Protection of Information". (1999, December). Retrieved from https://zakon.rada.gov.ua/laws/show/803-14.

protection. As evidenced in the work by H. Saragih (2025), the level of protection of state digital platforms directly depended on coordinated activity between regulatory and technical structures. The author emphasised that the fragmentation of managerial decisions and the absence of integrated communication channels led to low efficiency of cybersecurity policies. In this context, the conclusions of the study confirmed the systemic issue of insufficient interdepartmental coordination in managing cryptographic risks, which posed a threat of inconsistency in licensing, certification, and rapid response procedures.

In the context of certification and licensing procedures, the issue of digital maturity of public administration systems was of particular importance, as it determined the ability to integrate trust services into the functionality of digital services. The analysis confirmed that the full inclusion of cryptographic protection tools in the infrastructure of e-government required not only technological compatibility but also the existence of formally regulated supervision mechanisms for the use. Similar points were made by K. Balaji (2025), who highlighted the transformational impact of e-government and e-governance on public administrative functions. The author stressed the need to introduce automated tools for verifying the legitimacy of using digital signatures and certificates in state information systems. The results obtained in the study confirmed this need, pointing to the relevance of formalising control procedures for the implementation of CPI within electronic identification services.

The analysis of general trends in the development of the institutional and technological component of regulation confirmed that cryptographic security is gaining strategic importance in the context of the digital transformation of administrative processes. As shown in the analytical work by J. Millard (2023), the effectiveness of implementing digital reforms directly depended on the presence of a balanced regulatory framework, coordinated interdepartmental cooperation, and long-term planning of security policies. The results of the conducted study corresponded with this position: it was proven that the modernisation of the functional model of the State Service of Special Communications and Information Protection of Ukraine is a critical factor in the formation of a resilient system of state oversight, encompassing certification, monitoring, and audit in the field of CPI.

In the part concerning the analysis of the organisational structure of regulatory policy actors, the research findings aligned with the approaches proposed by P. Ciancarini *et al.* (2024), which described the relationship between digital transformation of public administration and the technology lifecycle. It was emphasised that the effectiveness of implementing cryptographic standards is directly related to the flexibility of regulatory mechanisms for managing technological updates. Within the study, it was established that the current operating model of specialised bodies required adaptation to the dynamics of technological changes, particularly through the creation of post-monitoring audit procedures and the maintenance of lifecycle registers for certified CPI tools.

A separate analytical focus within the study was placed on the standardisation of PQC as a key direction of modern regulatory policy. In this context, a related source was the work of S.A. Shamo (2024), which analysed the challenges of harmonising National Institute of Standards and Technology and ISO standards in the field of PQC and defined strategies for international coordination of certification procedures. The authors emphasised that one of the key issues was the incompatibility between national certification schemes and the technical parameters of new cryptographic algorithms. The findings of the study confirmed the relevance of this issue, as the need was identified for the integration of post-quantum solutions into Ukraine's regulatory environment alongside the updating of technical certification profiles and key management policies.

The analysis of post-quantum challenges confirmed that the effective adaptation of the state's cryptographic infrastructure required not only the updating of the regulatory base but also the modernisation of the technical ecosystem for information protection. As evidenced in the study by A. Joshi *et al.* (2024), the implementation of PQC required a comprehensive approach that included support for national certification centres, updates to key management systems, and integration with cross-border interaction mechanisms. These conclusions aligned with the study's results, which underlined the critical necessity for a technical review of CPI tools aimed at increasing resilience to quantum computing.

In the context of interstate coordination of the migration process towards post-quantum cryptographic standards, a relevant position was presented by L. Chen (2024), where emphasis was placed on the need for technical mapping of interconnections between classical and new cryptographic protocols. The author outlined the strategic role of national certification agencies in ensuring the continuity of information protection during the transition to PQC. Within the study, this position was confirmed by the substantiation of the need to create a digital infrastructure for algorithm verification, functionally linked to the powers of the State Service of Special Communications and Information Protection of Ukraine and oriented towards international standardisation requirements.

The study also demonstrated that the technical integration of new algorithms into national security systems was complicated by both hardware complexity and regulatory inertia. In the work of R. Bavdekar *et al.* (2022), the main barriers to implementing PQC were outlined, including incompatibility between the

technical specifications of algorithms and current certification procedures. The authors stressed the need to revise both infrastructural and regulatory components of the digital security system. The facts established in the study confirmed the relevance of these conclusions, particularly regarding the need to expand the powers of certification bodies to assess the compliance of post-quantum protection tools.

As shown in the work by A. Aydeger *et al.* (2024), ensuring quantum resilience involved not only the phased implementation of new algorithms but also the development of coordinated interaction mechanisms between CPI providers, regulators, and critical infrastructure operators. Within the study, this concept was reflected in the development of a model for regulatory expansion of the functions of the State Service of Special Communications and Information Protection of Ukraine, including components of post-monitoring analysis, auditing of cryptographic processes, and rapid response to incidents involving quantum-resistant tools.

The analysis of legal mechanisms regulating liability for violations of the cryptographic protection regime demonstrated the presence of structural gaps in the division of competences between oversight bodies. This was particularly evident in cases of inter-agency cooperation, where the lack of clear joint response procedures complicated the effective application of sanctions. Similar problems were highlighted in the study by O.V. Cardoso (2022), which emphasised the need to form a unified regulatory architecture for aligning the powers of law enforcement and supervisory bodies in the field of cryptographic protection, which is critically important in the context of digitalisation of governance processes. Within the conducted study, this issue was specified by identifying the need to establish clear powers for the State Service of Special Communications and Information Protection of Ukraine, the Security Service of Ukraine, the Cyber Police, and the National Security and Defence Council of Ukraine regarding control over the use of uncertified CPI tools.

The general summary of the legal aspect of cryptographic security was correlated with the analysis proposed by J. Kazimi & H. Thalwal (2024), which characterised the current challenges of harmonising the regulatory environment with the dynamics of digital transformation. The authors emphasised the need to form flexible legal instruments capable of promptly responding to technological changes and maintaining the relevance of certification procedures. The study results confirmed these conclusions, particularly regarding the need to synchronise Ukrainian regulations with the requirements of mutual recognition under eIDAS and adapt liability models to the specifics of digital services.

The relevance of unifying approaches to cryptographic security found further confirmation in the study by T. Bouraffa & K.-L. Hui (2025), which conducted a systematic review of regulatory frameworks in the field of information and network security. The authors pointed out the presence of fragmentation among sectoral regulators, which hindered the effective implementation of unified technical and legal standards in the field of information protection. Within the framework of this study, the observation was specified through the need to form a centralised model of certification and monitoring, which would ensure the integrity of state policy in the field of CPI.

Against the background of the problems of coordinating certification regimes in different jurisdictions, it was established that the issue of legal harmonisation of cryptographic standards retained critical importance for ensuring cross-border digital compatibility. In the work by B. Firmansyah & R. Bansal (2024), barriers arising in the process of standardising cryptographic solutions in digital environments were considered, in particular due to the risks of regulatory incompatibility. The research results confirmed the identified problem, demonstrating discrepancies between the provisions of eIDAS 2.0, the European Telecommunications Standards Institute EN 319, and current national acts, which limited the prospects for mutual recognition of CPI tools at the EU level.

Within the framework of developing technical standards for digital identification, special attention was paid to the problems of transitional regulation related to the use of distributed ledger technologies. As stated in the study by X. Jia *et al.* (2023), the process of standardising blockchain and distributed ledger technology was accompanied by numerous regulatory conflicts, particularly due to the lack of unified approaches to certification and legal classification of objects. The authors emphasised that without overcoming these contradictions, it is impossible to form a digital trust infrastructure compatible with global regulatory requirements. The results obtained within the framework of the study confirmed the presence of similar challenges in Ukraine, particularly in the field of regulation of timestamp procedures and the use of electronic seals.

The legal aspects of protecting digital assets were considered through the lens of liability for violations of the cryptographic security regime, including the use of uncertified tools or non-compliance with key management requirements. In this context, a generalised analytical basis was provided by the study of N. Shaik *et al.* (2025), which systematised the current regulatory approaches to ensuring legal liability in the event of cyber incidents. The study highlighted issues of legal responsibility for cyber violations, in particular tertiary liability, the duty of proper cybersecurity, employer liability for data leaks, and the specifics of legal regulation of cross-border cyber incidents. Within the conducted research, this position was specified in proposals to strengthen the role of the State Service of Special Communications and Information Protection of Ukraine in terms of monitoring, auditing, and responding to violations in the field of cryptographic protection.

A comprehensive analysis of the research results in relation to scientific approaches covering digital security, cryptographic protocols, and regulatory mechanisms demonstrated the systemic nature of the identified problems. It was substantiated that ensuring compatibility with international standards, modernising certification procedures, implementing post-quantum solutions, and strengthening the institutional functions of regulators are key prerequisites for the sustainable development of the CPI sector. All the mentioned areas were found to be interconnected with digital transformation processes, which determines the practical significance for the formation of next-generation cybersecurity policies.

The generalisation of the results made it possible to identify critically important vectors for improving state policy, among which the leading ones remain the integration of legal and technical tools for managing cryptographic risks, the development of digital identity, the unification of key management procedures, and the provision of proper response to security incidents. The effectiveness of state regulation in the field of CPI largely depends on the integrity of the normative, organisational, and technological architecture, which requires further scientific research to adapt it to transnational requirements, in particular the provisions of eIDAS 2.0, and the implementation of risk-oriented models in the processes of state cryptographic oversight.

Conclusions

As a result of the conducted study, it was established that the regulatory and legal framework in the field of cryptographic information protection in Ukraine formed two main levels of regulatory influence: the general technical level, focused in the Law of Ukraine "On Information Protection in Information and Telecommunication Systems", and the specialised one, defined by the Law of Ukraine "On Cryptographic Information Protection". A comparison of the substantive provisions of these acts allowed for the identification of distinctions in regulatory subject, subjects involved, requirements for technical means, and control mechanisms. In particular, it was determined that the first law was oriented towards owners of information and telecommunication systems, and the second – towards developers and suppliers of CPI, which created prerequisites for a dual responsibility regime. It was generalised in a tabular format that only a part of the provisions of these acts aligned with international standards – for example, certification requirements for CPI means only partially conformed to the structure of ISO/IEC 15408 and eIDAS.

Within the institutional analysis, it was recorded that the State Service of Special Communications and Information Protection of Ukraine performed key functions in certification, expertise, licensing, and supervision, while the division of powers between its structural units (Administration, technical committees, expert groups, licensing departments) was clearly outlined by functional criteria. The corresponding table systematised that the administration was responsible for coordination, technical committees for standardisation, and expert groups for technical implementation. It was separately established that, in the sphere of interdepartmental interaction with the Security Service of Ukraine, the National Security and Defence Council of Ukraine, and the National Police, there was partial fragmentation of functions – for instance, the control over electronic signatures and digital marks was implemented simultaneously by several entities without a formalised division of responsibility. In the interaction table, it was revealed that coordination procedures were defined in only 3 out of 8 areas of competence.

The technical section of the study showed that the existing means of cryptographic protection included classical algorithms (AES, RSA, ECDSA) and new post-quantum solutions (Dilithium, Kyber, SABER), which differed in key length, level of resistance, and certification status. Table 6 presented that the key length in post-quantum algorithms on average exceeded 3000 bits, which is 2-3 times more than the classical ones. It was also determined that CPI hardware means were divided into HSMs, tokens, smart cards, and virtualised modules, each of which had a specific area of application – for instance, HSMs conformed to FIPS 140-2 Level 3 and were used in state registers. In the comparative table of technical standards, it was shown that Ukrainian requirements partially aligned with European Telecommunications Standards Institute EN 319, eIDAS Annex I and recommendations of the European Union Agency for Cybersecurity, particularly in signature formats (XAdES, CAdES) and cryptographic management. However, in the areas of timestamp, seal, and digital identification, there was incomplete conformity, requiring an update of regulations and interfaces.

The limitations of the conducted study included the lack of full access to technical regulations of all categories of certified CPI means, limited transparency of departmental security standards, and the absence of aggregated public data on violations of the cryptographic regime. This partially complicated the quantitative representation of the compliance level of electronic identification systems with eIDAS 2.0 requirements and the assessment of supervisory procedure effectiveness. In further studies, it would be advisable to focus on analysing the lifecycle of cryptographic means in information-critical systems, forming digital registers of certified algorithms, and creating mechanisms for post-certification auditing.

Acknowledgements

None.

Funding

None.

Conflict of Interest

None.

References

[1] Aydeger, A., Zeydan, E., Yadav, A.K., Hemachandra, K.T., & Liyanage, M. (2024). Towards a quantum-resilient future: Strategies for transitioning to post-quantum cryptography. In *Proceedings of the 15th international conference on network of the future* (pp. 195-203). Castelldefels: IEEE. doi: 10.1109/NoF62948.2024.10741441.

[2] Balaji, K. (2025). E-government and E-governance: Driving digital transformation in public administration. In K. Wongmahesak & J. Ahmad (Eds.), *Public governance practices in the age of AI* (pp. 23-44). London: IGI Global. doi: 10.4018/979-8-3693-9286-7.ch002.

[3] Bavdekar, R., Chopde, E.J., Bhatia, A., Tiwari, K., & Daniel, S.J. (2022). Post quantum cryptography: Techniques, challenges, standardisation, and directions for future research. *arXiv*. doi: 10.48550/arXiv.2202.02826.

[4] Bommareddy, S., Khan, J.A., & Anand, R. (2022). A review on healthcare data privacy and security. In P. Singh, O. Kaiwartya, N. Sindhwani, V. Jain & R. Anand (Eds.), *Networking technologies in smart healthcare: Innovations and analytical approaches* (pp. 165-187). Boca Raton: CRC Press. doi: 10.1201/9781003239888.

[5] Bouraffa, T., & Hui, K.-L. (2025). Regulating information and network security: Review and challenges. *ACM Computing Surveys*, 57(5), article number 126. doi: 10.1145/3711124.

[6] Cardoso, O.V. (2022). Cryptography and law: The case of Brazil. *Digital Law Journal*, 3(3), 8-19. doi: 10.38044/2686-9136-2022-3-3-8-19.

[7] Chen, J. (2020). Regulation and deregulation: Understanding the evolution of the Chinese cryptography legal regime from the newly released Cryptography Law of China. *International Cybersecurity Law Review*, 1(1), 73-86. doi: 10.1365/s43439-020-00003-6.

[8] Chen, L. (2024). Standardisation of and migration to post-quantum cryptography. In X. Lu & C.J. Mitchell (Eds.), *Security standardisation research* (pp. 3-13). Cham: Springer. doi: 10.1007/978-3-031-87541-0_1.

[9] Ciancarini, P., Giancarlo, R., & Grimaudo, G. (2024). Digital transformation in the public administrations: A guided tour for computer scientists. *IEEE Access*, 12, 22841-22865. doi: 10.1109/ACCESS.2024.3363075.

[10] DSTU 4145-2002 "Information technology. Cryptographic protection of information. Digital signature based on elliptic curves. Formation and verification". (2002). Retrieved from https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=68769.

[11] DSTU 7624:2014 "Information technology. Cryptographic protection of information. Symmetric block transformation algorithm. Correction". (2014). Retrieved from https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=65314.

[12] European Telecommunications Standards Institute. (2016a). *ETSI EN 319 411-2 V2.2.2: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates*. Retrieved from https://www.etsi.org/deliver/etsi_en/319400_319499/31941102/02.02.00_20/en_31941102v020200a.pdf.

[13] European Telecommunications Standards Institute. (2016b). *ETSI EN 319 421 V1.1.1: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers providing signature validation services*. Retrieved from https://cdn.standards.iteh.ai/samples/39366/0766c518ead24fcfb5e9bc4cb7527f9c/ETSI-EN-319-421-V1-1-1-2016-03-.pdf.

[14] European Telecommunications Standards Institute. (2018). *ETSI TS 103 097 V1.3.1: Intelligent Transport Systems (ITS); Security; Security header and certificate formats*. Retrieved from https://www.etsi.org/deliver/etsi_ts/103000_103099/103097/01.03.01_60/ts_103097v010301p.pdf.

[15] European Union Agency for Cybersecurity. (2014). *Securing personal data: ENISA guidelines on cryptographic solutions*. Retrieved from https://surli.cc/kulckx.

[16] Firmansyah, B., & Bansal, R. (2024). Standardisation and regulatory challenges in modern cryptography. In B. Gupta (Ed.), *Metaverse security paradigms* (pp. 145-183). London: IGI Global. doi: 10.4018/979-8-3693-3824-7.ch006.

[17] ISO/IEC 27001:2022 "Information security, cybersecurity and privacy protection – Information security management systems – Requirements". (2022). Retrieved from https://www.iso.org/ru/standard/27001.

[18] ISO/IEC No. 15408-1:2009 "Evaluation criteria for IT security". (2009). Retrieved from https://www.iso.org/standard/50341.html

[19] ISO/IEC No. 18033-1:2021 "Encryption algorithms". (2021). Retrieved from https://www.iso.org/standard/76156.html.

[20] ISO/IEC No. 19790:2012 "Security requirements for cryptographic modules". (2012). Retrieved from https://www.iso.org/standard/52906.html.

[21] ISO/IEC 27033-5:2016 "Information technology. Security methods. Network security. Part 5. Securing communications across networks using virtual private networks (VPNs)". (2016). Retrieved from https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=69130.

[22] ISO/IEC No. 7816-4:2020 "Integrated circuit cards". (2020). Retrieved from https://surl.li/rxclpp.
[23] Jia, X., Xu, J., Han, M., Zhang, Q., Zhang, L., & Chen, X. (2023). International standardisation of blockchain and distributed ledger technology: Overlaps, gaps and challenges. *CMES-Computer Modeling in Engineering & Sciences*, 137(2), 1491-1523. doi: 10.32604/cmes.2023.026357.
[24] Joshi, A., Bhalgat, P., Chavan, P., Chaudhari, T., & Patil, S. (2024). Guarding against quantum threats: A survey of post-quantum cryptography standardisation, techniques, and current implementations. In V.S. Shankar Sriram, A. Glory, G. Li & S.R. Pokhrel (Eds.), *International conference on applications and techniques in information security* (pp. 33-46). Singapore: Springer. doi: 10.1007/978-981-97-9743-1_3.
[25] Kazimi, J., & Thalwal, H. (2024). Legal implications and challenges of cryptography and data security: Current trends and future directions. In *Proceedings of the First international conference on technological innovations and advance computing* (pp. 19-27). Bali: IEEE. doi: 10.1109/TIACOMP64125.2024.00014.
[26] Kokarcha, Y., & Lalueva, A. (2022). Peculiarities of personal data protection in social networks: The impact of martial law. *Proceedings of the III international scientific and theoretical conference "Current issues of science, prospects and challenges"* (pp. 70-74). Sydney: SCIENTA.
[27] Kostiuk, Y.V., Skladanny, P.M., Hulak, G.M., Bebeshko, B.T., Khorolska, K.V., & Rzaeva, S.L. (2025). *Information security systems*. Kyiv: Borys Grinchenko Kyiv Metropolitan University.
[28] Lampe, G.S. (2023). Critical success factors for integrating a circular interaction model for security processes in digital transformation. *Ecoforum Journal*, 12(2).
[29] Limniotis, K. (2021). Cryptography as the means to protect fundamental human rights. *Cryptography*, 5(4), article number 34. doi: 10.3390/cryptography5040034.
[30] López, P. (2025). The national security framework as a cybersecurity reference for information cryptosystems. In C.P. Sempere (Ed.), *Governance and control of data and digital economy in the European Single Market: Legal framework for new digital assets, identities and data spaces* (pp. 125-144). Cham: Springer. doi: 10.1007/978-3-031-74889-9_6.
[31] Millard, J. (2023). *Impact of digital transformation on public governance*. Retrieved from https://s4andalucia.es/wp-content/uploads/2023/10/JRC133975_01.pdf.
[32] National Institute of Standards and Technology. (2001). *FIPS PUB 140-2: Security requirements for cryptographic modules*. Retrieved from https://csrc.nist.gov/publications/detail/fips/140/2/final.
[33] National Institute of Standards and Technology. (2008). *NIST Special Publication 800-115: Technical guide to information security testing and assessment*. Retrieved from https://surl.li/mnnfqg.
[34] National Institute of Standards and Technology. (2019). *NIST Special Publication 800-52 Revision 2: Guidelines for the selection, configuration, and use of transport layer security (TLS) implementations*. Retrieved from https://csrc.nist.gov/publications/detail/sp/800-52/rev-2/final.
[35] National Institute of Standards and Technology. (2020). *NIST Special Publication 800-57 Part 1 Rev. 5: Recommendation for key management*. Retrieved from https://surl.li/uujzun.
[36] National Police of Ukraine. (n.d.). *Annual reports*. Retrieved from https://surl.lt/pjhzkk.
[37] National Security and Defense Council of Ukraine. (n.d.). *Accounting for public information*. Retrieved from https://rnbo.gov.ua/ua/Oblik-publichnoi-informatsii.html.
[38] Riebe, T., Kühn, P., Imperatori, P., & Reuter, C. (2022). US security policy: The dual-use regulation of cryptography and its effects on surveillance. *European Journal for Security Research*, 7(1), 39-65. doi: 10.1007/s41125-022-00080-0.
[39] Saragih, H. (2025). The impact of digital transformation on the performance and security of information systems in government institutions. *Pakistan Journal of Life and Social Sciences*, 23(1), 5333-5344. doi: 10.57239/PJLSS-2025-23.1.00416.
[40] Security Service of Ukraine. (n.d.). *Reports*. Retrieved from https://ssu.gov.ua/zvity.
[41] Shaik, N., Chandana, B.H., Chitralingappa, P., & Sasikala, C. (2025). Protecting in the digital age: A comprehensive examination of cybersecurity and legal implications. In S. Barman, S. Koley & S. Joardar (Eds.), *Next-generation systems and secure computing* (pp. 105-135). London: Scrivener Publishing LLC. doi: 10.1002/9781394228522.ch6.
[42] Shamo, S.A. (2024). *Bridging the quantum divide: A comprehensive analysis of NIST and ISO standards for post-quantum cryptography and strategies for global harmonisation*. Retrieved from https://surl.li/pudanm.
[43] Vargiolu, A. (2022). *Cryptography and privacy issues: An OECD framework for global data protection*. doi: 10.13140/RG.2.2.13868.88969.
[44] Yanamala, A.K., & Suryadevara, S. (2024). Navigating data protection challenges in the era of artificial intelligence: A comprehensive review. *Revista de Inteligencia Artificial en Medicina*, 15(1), 113-146.
[45] Zinchuk, M.V. (2024). *Legal support for the protection of confidential information in Ukraine*. Lutsk: Lesya Ukrainka Volyn National University.

Перспективи державного регулювання криптографічного захисту даних

Марія Турчіна
Кандидат юридичних наук
Національний юридичний університет імені Ярослава Мудрого
61024, вул. Григорія Сковороди, 77 м. Харків, Україна
https://orcid.org/0000-0002-1486-1122

Ігор Руденко
Магістр права
Національний юридичний університет імені Ярослава Мудрого
61024, вул. Григорія Сковороди, 77, м. Харків, Україна
https://orcid.org/0009-0008-3582-3951

Ольга Хорольська
Магістр права
Національний юридичний університет імені Ярослава Мудрого
61024, вул. Григорія Сковороди, 77, м. Харків, Україна
https://orcid.org/0009-0004-9853-2378

Анотація
Актуальність дослідження зумовлена необхідністю правового та технічного переосмислення державного регулювання криптографічного захисту інформації в умовах цифрової трансформації України. Метою статті було виявлення ефективності чинної нормативної, інституційної та технічної моделі регулювання криптографічного захисту даних з урахуванням положень міжнародних стандартів. У роботі застосовувалися методи структурно-функціонального аналізу, системного порівняння правових положень і контент-аналізу технічних вимог. У результаті дослідження було встановлено, що нормативне поле регулювання охоплює два рівні впливу – загальнотехнічний і спеціалізований, однак лише приблизно шістдесят відсотків положень щодо електронного підпису, управління криптографічними ключами та часових міток відповідають міжнародним технічним вимогам. Зафіксовано фрагментарність у визначенні обов'язкових сертифікаційних процедур і відсутність уніфікованих регламентів у галузі цифрової ідентифікації та електронної печатки. У межах міжінституційної взаємодії встановлено, що лише три з восьми функціональних напрямів регламентовані формалізованими механізмами, що ускладнює реагування на інциденти криптографічного характеру. Технічний аналіз підтвердив, що середня довжина ключів у криптографічних алгоритмах, стійких до оброблення квантовими обчислювальними системами, перевищує три тисячі бітів, що у два-три рази перевищує показники традиційних алгоритмів, однак імплементація таких рішень у систему державної сертифікації здійснюється обмежено. Також було встановлено, що лише частина апаратних засобів криптографічного захисту відповідає міжнародним вимогам до рівнів технічної безпеки. Практична значущість результатів дослідження полягає в можливості їх застосування для оновлення регуляторної архітектури, формування технічних регламентів, розроблення процедур державного контролю, а також підтримки органів публічної влади, технічних експертних підрозділів і розробників у процесі реалізації національної стратегії кіберзахисту

Ключові слова:
цифрова ідентифікація; електронний підпис; сертифікація засобів; інформаційна безпека; технічний стандарт; міжвідомча координація; цифрова трансформація