UDC 004.056:34:351.74:378
DOI https://doi.org/10.32782/2308-6971/2026.1.6

INFORMATION AND LEGAL RISKS OF THE DIGITAL TRANSFORMATION OF THE PERSONNEL TRAINING SYSTEM FOR THE STATE PENITENTIARY SERVICE OF UKRAINE AMID AUTOMATION AND CYBER THREATS

Aim. *The primary objective of this article is to analyse the information and legal risks arising during the digital transformation of the personnel training system within the State Penitentiary Service of Ukraine. In the contemporary environment, characterised by the digitalisation of educational processes, the automation of administrative procedures, and the increasing complexity of cyber threats, it is essential to examine how these technological developments interact with existing legal frameworks. Particular attention is paid to issues of information protection, personal data processing, and the legal regulation of digital educational resources used in professional training. The study also aims to substantiate directions for improving the legal and organisational mechanisms of information security within the personnel training system.*

Methods. *The research methodology combines general scientific principles with specialised legal methods. The formal-legal method was applied to analyse national legislation and departmental regulatory acts concerning information protection and personal data processing. The comparative-legal method was used to compare Ukrainian regulatory approaches with European standards, particularly the General Data Protection Regulation (GDPR) and relevant European Union cybersecurity directives. Systemic-structural, analytical, and logical-legal methods were also employed to identify legislative gaps, organisational shortcomings, and risks associated with the implementation of automated and algorithmic systems in the professional training of law enforcement and correctional personnel.*

Results. *The findings demonstrate that the digitalisation of personnel training is accompanied by increased risks related to the violation of the principles of legality, proportionality, and purpose limitation in information processing. The research reveals an insufficient level of information security culture, fragmented legal regulation, and uncertainty regarding the legal status of digital educational resources. The introduction of algorithmic assessment systems without adequate legal oversight may reduce transparency and potentially affect the rights of personnel.*

Conclusions. *The study concludes that it is necessary to establish a coherent information and legal mechanism for personnel training that combines effective legal regulation, organisational measures, and internal control procedures with the development of digital and legal competencies among personnel. Harmonisation with European standards is an important prerequisite for strengthening cybersecurity and institutional trust in digital technologies in the public sector.*

Key words: Public Sector Information Security, Protection of Personal Data, Digitalisation of Public Administration, Cyber Risks in Educational Systems, Automated Decision-Making, Legal Regulation of Digital Technologies, Digital Competencies of Personnel.

JEL Classification: H11, K24, H83, O33, D81, K20, I28.

Dmytro POKRYSHEN,
Director of the Educational and Scientific Institute of Law, Law Enforcement and Psychology Penitentiary Academy of Ukraine PhD in Pedagogical Sciences, Associate Professor
pokryshen@ukr.net
orcid.org/0000-0001-9572-413X

Introduction. The digital transformation of the personnel training system within the State Penitentiary Service of Ukraine (SPSU) is occurring under conditions of heightened information, legal, and security risks. These risks are driven by the specific nature of the SPSU's activities, which involve processing substantial volumes of confidential information, special categories of personal data, and restricted official information. The introduction of electronic educational platforms, automated systems for recording learning outcomes, algorithmic assessment tools, and digital HR management services brings to the fore the issues of compliance with information legislation and the principles of legality, proportionality, and purpose limitation.

An insufficient culture of information security among SPSU personnel, the fragmented legal regulation of digital processes, the lack of a comprehensive information security concept in the field of vocational training, and the limited integration of European

standards–specifically the provisions of the GDPR and EU cybersecurity acts–significantly increase the risks of violating the rights of data subjects, data breaches, and a decline in trust in digital tools. Under these circumstances, the scholarly reflection on the information and legal risks of digitalising the training of SPSU personnel is of paramount relevance.

The current stage of development of the State Penitentiary Service of Ukraine is characterised by the active implementation of digital technologies in the system of professional training and continuous professional development. The use of electronic educational resources, distance learning platforms, automated assessment systems, and elements of algorithmic management contributes to the optimisation of educational processes and increases their efficiency. At the same time, such processes create new information and legal challenges related to ensuring the protection of personal data, official information, and the upholding of the rights of SPSU personnel. The absence of a clear legal definition for the status of digital educational resources, insufficient internal control over compliance with information security policies, and the low level of digital competence among certain categories of personnel reinforce the impact of the human factor on the state of cybersecurity. In this context, there is a need for a comprehensive information and legal analysis of the risks associated with the digital transformation of the SPSU personnel training system.

Aim and Objectives of the Study. The aim of the study is to conduct a comprehensive analysis of the information and legal risks of the digital transformation of the personnel training system of the State Penitentiary Service of Ukraine and to substantiate the directions for improving the legal regulation and organisational mechanisms for ensuring information security.

To achieve this aim, the following objectives have been defined: To analyse the legal risks of processing and protecting information in the process of training SPSU personnel; To investigate the impact of automated and algorithmic systems on the exercise of the rights of personnel and participants in educational programmes; To assess the state of legal provision for an information security culture and internal control within the SPSU system; To identify the problems of implementing European data protection standards into national personnel training practices; To formulate proposals for the development of a comprehensive information and legal concept for the digital training of SPSU personnel.

Research Methods. The methodological foundation of this study is comprised of a combination of general scientific and specialised legal methods of enquiry. The **formal-legal method** was employed to analyse the norms of Ukrainian national legislation, departmental regulatory acts of the SPSU, and international instruments in the field of information security and personal data protection. The **comparative-legal method** was applied to contrast national regulatory approaches to digital educational processes with European standards, specifically the provisions of the **GDPR**, the **NIS Directive**, and the **Cybersecurity Act**. The **systemic-structural method** allowed for the conceptualisation of the SPSU personnel training system as a cohesive information-legal framework with interconnected organisational, legal, and technical elements. Furthermore, **analytical and logical-legal methods** were used to identify legal lacunae, conflicts, and risks arising during the digitalisation and automation of educational and administrative procedures.

Literature Review. In scientific literature, the implementation of management systems within the penitentiary sector is regarded as a key direction of digital transformation, aimed at replacing paper-based procedures with integrated, offender-oriented databases and unified information systems to support admission processes, individual case management, and inter-agency reporting. Case analysis indicates that the fundamental functionality of such systems is the end-to-end recording of a prisoner's life cycle–from initial admission and classification to participation in programmes and eventual release–which ensures the integrity of managerial decisions and increases administrative efficiency (Kathuria & Porporino, 2015). Specifically, the **Offender Management Information System (OMIS)** implemented in Namibia illustrates the capabilities of systemic accounting for key data on convicts at all stages of their stay in a correctional facility; it also demonstrates the functional advantages and implementation requirements for similar solutions in resource-constrained environments, particularly regarding human capital, funding, and personnel training (Kathuria & Porporino, 2015).

Practical examples of developing simplified online management systems for penitentiary institutions, notably in Nigeria, confirm that tangible results can be achieved in terms of data accessibility, the creation of a unified offender profile, and increased operational efficiency through the use of standard web and database technologies (Ilemona, 2013). At the same time, research substantiates the necessity of introducing

departmental statistical accounting and creating data warehouses or unified information systems as a prerequisite for full process automation and the establishment of inter-departmental information exchange. It is emphasised that the successful implementation of management information systems requires stable funding, qualified IT personnel, end-user training programmes, and clear mechanisms for data quality management and interoperability (Kathuria & Porporino, 2015).

In parallel with the development of management systems, security and monitoring technologies in penitentiary institutions are transforming, evolving from basic CCTV and access control to complex embedded infrastructures and analytical solutions. However, their design is largely determined by institutional values and is accompanied by risks of excessive surveillance and the restriction of prisoners' rights. Modern analytical studies highlight both the security benefits of digital systems and the ethical and socio-technical trade-offs that arise during their integration into penitentiary infrastructure (Van De Steene & Knight, 2017; Hofinger & Pflegerl, 2024; Ross et al., 2024).

Scientific reviews distinguish between two main groups of technologies: firstly, solutions embedded to strengthen authoritative control and surveillance, and secondly, technologies aimed at meeting the communication and educational needs of convicts–between which there is often a tension of goals and practices (Ross et al., 2024). Empirical and theoretical studies suggest that digitalisation, in the absence of a clear needs-based orientation, can lead to the expansion of surveillance practices, the delegation of responsibility to technology, and the deepening of social inequality, resulting in ambiguous consequences for individuals serving sentences (Hofinger & Pflegerl, 2024). A separate area of contemporary debate concerns the potential of **Artificial Intelligence (AI)** and automation to normalise the custodial environment and support rehabilitation processes; however, researchers stress the need for prior diagnostic planning to identify potential risks, biases, and the requirements for proper governance of such technologies before their practical implementation (López Lorca, 2023). Simultaneously, it is underlined that the design and accessibility of technology in the correctional sphere are significantly shaped by institutional culture, bureaucratic practices, and societal perceptions, which can either limit or distort the set of tools actually developed and applied in practice (Ross et al., 2024).

Research Results. The lack of a developed information security culture among SPSU personnel is a significant risk factor for the effective functioning of personnel training systems within the digital environment. Despite the existence of regulatory requirements for information protection, employees frequently fail to adhere to the fundamental principles of secure engagement with electronic resources. This is manifested in breaches of access policies, the use of weak passwords, the negligent handling of confidential data, and insufficient attention to software updates. The absence of a conscious attitude towards cybersecurity threats undermines the effectiveness of technical security measures and creates risks of incidents stems from the human factor, highlighting the necessity for the systematic formation of an information security culture through regular training, briefings, and methodological support for personnel.

A low level of internal control over compliance with security policies significantly complicates the effective management of information risks during personnel training and institutional operations. The absence of systematic monitoring, auditing, and assessment of the implementation of established rules and procedures allows violations to remain undetected, which increases the likelihood of confidential information leaks and unauthorised access to critical data. Furthermore, insufficient accountability and oversight foster a passive attitude among staff regarding policy compliance, reducing the efficacy of technical and organisational cyber-defence measures. In these circumstances, the introduction of regular internal audits, access control mechanisms, and systematic verification of regulatory compliance is key to enhancing the resilience of the information infrastructure and minimising risks associated with the human factor.

The legal risks associated with the collection of data on training outcomes and the professional activities of personnel are linked to the necessity of adhering to the principles of legality, proportionality, and purpose limitation, as enshrined in national and European legislation. Unregulated procedures for the collection, processing, and storage of data may lead to the violation of data subjects' rights, particularly the right to privacy and confidentiality. It also creates a potential threat to personnel through the unlawful use of assessment results or professional activity records. Moreover, the absence of clear internal policies and oversight regarding legislative compliance increases the risk of administrative and criminal liability for the institution, which limits the effectiveness of information systems in the training process and diminishes personnel trust in digital technologies and electronic services.

The challenges of automated decision-making within the educational process are related to the need to balance the efficiency of digital technologies with the requirements of legality, transparency, and fairness in decisions affecting personnel. The use of algorithmic systems for knowledge assessment, candidate selection, or the management of learning trajectories can result in opaque procedures, model biases, and limited human oversight. Imperfections in algorithms, inadequate data quality control, and the lack of methodologies for risk assessment in automated systems create the threat of unlawful decisions that may infringe upon the rights of employees or trainees, thereby undermining trust in electronic educational platforms.

Furthermore, automation requires a high level of personnel competence in information technology and cybersecurity; its absence complicates the proper operation of systems and the timely detection of errors or failures. Challenges also arise from the necessity to align automated procedures with national legislation and international standards, particularly the GDPR, which mandates control over the lawfulness of data processing and the protection of data subjects' rights. Thus, the implementation of automated solutions within the educational process requires a comprehensive approach that integrates technical, organisational, and legal aspects.

A lack of modern research on cybersecurity within the public service and the penitentiary system limits the capacity for evidence-based managerial decision-making and the development of effective information protection measures. Existing scholarly works mostly address general aspects of cybersecurity or technology applications in the private sector, while the specificities of state institutions and penitentiary facilities–including handling confidential data and high-risk personnel–remain insufficiently explored. This creates gaps in training methodology, security standards, and information risk management policies, complicating the adaptation of international practices and hindering the formation of a cohesive cyber-resilience system tailored to the specific needs of the public service and the penitentiary sphere.

The low level of integration of scientific results into training practices leads to a fragmented personnel training process that lags behind modern challenges of digitalisation and cybersecurity. Developments in information security, risk management methodologies, and data protection standards often remain theoretical or are applied selectively, reducing the effectiveness of educational programmes and complicating the development of practical competencies among personnel. Consequently, educational institutions cannot fully employ advanced scientific approaches to adapt to international standards, ensure the security of information systems, and enhance the quality of the digital transformation of the public service and the penitentiary system.

Resistance to digital change and a lack of trust in electronic systems among personnel significantly complicate the implementation of innovations in personnel training and information resource management. Stereotypical attitudes towards traditional working methods, fear of new technologies, and concerns regarding data security result in low engagement with electronic platforms, distance learning systems, and automated assessment tools. Such resistance slows down the digital transformation process, reduces the efficiency of personnel training, and increases information security risks due to insufficient awareness and an inability to interact correctly with modern information systems.

Low motivation to enhance digital competence among personnel negatively impacts the effectiveness of information technology implementation and compliance with cybersecurity requirements during training. Employees often fail to see immediate benefits in developing skills related to electronic systems, data management, and information protection, leading to a perfunctory or incomplete mastery of training programmes. This situation hinders the establishment of a unified level of digital literacy, reduces the efficiency of institutional digital transformation, and increases the vulnerability of information infrastructure to incidents caused by the human factor.

Fears of job loss due to digitalisation and automation create psychological and organisational barriers to innovation in personnel training and information resource management. Employees who perceive automated systems and electronic services as a threat to their professional positions often demonstrate resistance to new technologies, limited engagement in training, and minimal initiative in using digital tools. This attitude slows the digital transformation process, reduces the effectiveness of cyber-defence measures, and prevents the formation of a unified information security culture, ultimately increasing the risks of unauthorised data access and violations of institutional information policies.

Stress factors associated with the intensive implementation of new technologies significantly affect the effectiveness of personnel training and adaptation to the digital environment. Frequent changes in software,

the necessity of mastering complex information systems, and the continuous updating of skills create a psychological burden that can reduce productivity, concentration levels, and the ability of employees to use digital resources safely. This state increases the probability of errors, breaches of cybersecurity procedures, and uneven levels of digital competence among personnel, which, in turn, complicates the implementation of information security policies and the effective digital transformation of institutions.

The absence of a comprehensive information security concept in the field of personnel training is one of the key problems of modern state and educational policy. Existing regulatory acts and methodological recommendations mostly cover isolated aspects of cyber defence, personal data protection, or information risk management, yet they do not form a cohesive system that integrates all necessary components. Such fragmentation in legal and organisational regulation creates gaps in personnel training, reduces the effectiveness of information resource protection, and complicates the standardisation of educational programmes aimed at building digital security competencies.

The lack of a unified concept also complicates the integration of national standards with international norms, particularly the provisions of the GDPR, the Cybersecurity Act, and ENISA recommendations, which lowers the level of compliance of the Ukrainian personnel training system with European practices. Insufficiently clear legal and methodological approaches to information protection, access control, the maintenance of electronic registers, and the monitoring of cyber risks lead to increased vulnerability of institutions to cyber threats and legal risks, while also hindering the formation of an information security culture among employees. Thus, the absence of a comprehensive concept hampers effective digital transformation and the integration of modern technologies into the personnel training system.

The uncertainty of the legal status of information resources and educational infrastructure objects creates substantial problems for the effective functioning of the personnel training system. The lack of a clear classification for electronic educational resources, digital platforms, and databases complicates the definition of users' rights and obligations, the procedures for information access, and responsibility for its processing. This leads to the ambiguous application of legislative norms governing information security and personal data protection, thereby reducing the effectiveness of organisational and technical information protection measures.

Legal uncertainty regarding the status of educational infrastructure objects also increases the risks of violating the confidentiality and integrity of information resources. The absence of unified standards for regulating electronic services and distance learning platforms complicates access control, data usage monitoring, and the assurance of security, which, in turn, creates potential threats for personnel and trainees. This situation necessitates the development of clear regulatory approaches and methodological recommendations to define the legal status of digital educational resources and educational infrastructure systems.

Insufficient personnel competence in the field of digital transformation and cybersecurity significantly limits the effectiveness of implementing modern information technologies in the training process. Low levels of digital literacy, a limited understanding of cybersecurity principles, and a lack of skills in working with electronic systems create preconditions for security policy violations and the inefficient use of electronic services, thereby increasing the risk of incidents associated with the human factor.

Furthermore, insufficient personnel training complicates the implementation of international standards, which negatively impacts the integration of the national training system into the European legal and technological space. The absence of a systemic approach to professional development and regular training in cybersecurity limits the capacity of institutions to provide comprehensive protection for information resources, maintain the continuous development of electronic services, and foster an information security culture among employees.

The legal and organisational risks associated with the implementation of digital technologies and algorithmic systems in personnel training are linked to the necessity of ensuring the legality, transparency, and accountability of automated processes. The use of electronic platforms for knowledge assessment, the management of learning trajectories, and the processing of personal data may lead to violations of the rights of employees and trainees in cases of inadequate oversight, opaque algorithms, or system errors. The lack of regulation regarding the use of algorithmic solutions increases the risk of legal claims and adversely affects personnel trust in digital tools.

Moreover, the integration of digital technologies into educational processes is complicated by conflicts between national and European legislation. The insufficient integration of international

standards into internal institutional regulations creates gaps in data protection, access control, and the auditing of information systems. Consequently, the efficiency of the digital transformation of personnel training is reduced, while the risks of unauthorised access, data leaks, and violations of data subjects' rights remains high, necessitating the development of clear legal and organisational regulatory mechanisms.

The analysis of the information-legal framework for personnel training reveals systemic lacunae in national legislation and regulatory acts. The absence of a comprehensive information security concept, along with the uncertainty of the legal status of information resources and educational infrastructure objects, creates legal conflicts and gaps that complicate the assurance of legality and accountability in the management of personnel data. Such deficiencies increase the risks of violating the rights of data subjects and limit the capacity of state institutions to fulfill the requirements of international law regarding data protection and cybersecurity.

Insufficient personnel competence in the field of information law and cybersecurity exacerbates legal risks, as it limits the ability of subjects to comply with established policies, regulatory acts, and data processing standards. The imperfection of internal regulations, the absence of systematic oversight, and the uneven application of legislative requirements create a basis for unauthorised access to information, breaches of confidentiality, and non-compliance with the principles of legality, proportionality, and purpose limitation enshrined in national laws and EU provisions, specifically the GDPR and the NIS Directive.

The formation of an effective information-legal system for personnel training requires the creation of a unified legal and methodological framework that integrates cyber-defence measures, rules for processing personal data, and mechanisms for monitoring legislative compliance. The introduction of clear procedures, regular auditing, and professional development for personnel in the field of information law will allow for the reduction of legal risks, ensure the accountability of state bodies, and guarantee the alignment of the national training system with international standards in information protection and cybersecurity.

Conclusions. The study establishes that the digital transformation of the personnel training system of the State Penitentiary Service of Ukraine is accompanied by significant information and legal risks, driven by the specific nature of official activities, fragmented regulatory frameworks, and an insufficient level of information security culture. The use of automated and algorithmic systems in the educational process without adequate legal regulation and oversight increases the risks of infringing upon personnel rights, opacity in assessment procedures, and the unlawful processing of personal data.

The absence of a unified, comprehensive information security concept for SPSU personnel training and the uncertainty regarding the legal status of digital educational resources complicate the integration of European standards and weaken the cyber-resilience of the departmental information infrastructure. The study substantiates the necessity of forming a cohesive information-legal mechanism for the training of SPSU personnel, which combines legal regulation, effective internal control, the systematic enhancement of digital and legal competencies, and the harmonisation of national norms with international cybersecurity standards.

References:

1. López Lorca, B. (2023). *La digitalización de las prisiones y el uso de la inteligencia artificial: Marcadores de última generación para la normalización del entorno penitenciario y la redefinición del proceso de resocialización*. *Internet, Derecho y Política*, (39). https://doi.org/10.7238/idp.v0i39.416671

2. Kathuria, A., & Porporino, F. J. (2015). Implementing information technology for corrections in Africa: A case example of the Namibian Correctional Service automated offender management information system. *Acta Criminologica: Southern African Journal of Criminology*.

3. Ilemona, A. P. (2013). *Design and implementation of an online prison management system*. https://www.scribd.com/document/658205340/DESIGN-AND-IMPLEMENTATION-OF-AN-ONLINE-PRISON-MANAGEMENT-SYSTEM

4. Van De Steene S., Knight V. (2017). Digitizing the prison: The light and dark future. *Prison Service Journal*. 231. P. 22–30. https://www.researchgate.net/profile/Steven-Van-De-Steene/publication/333561812_Digitizing_the_prison_The_Light_and_Dark_Future/links/5cf434d392851c4dd02407bf/Digitizing-the-prison-The-Light-and-Dark-Future.pdf

5. Hofinger, V., & Pflegerl, P. (2024). A reality check on the digitalisation of prisons: Assessing the opportunities and risks of providing digital technologies for prisoners. *Punishment & Society*, *26*(5), 898–916. https://doi.org/10.1177/14624745241237190 (Original work published 2024)

6. Ross, S., Wood, M. A., Baird, R., & Lundberg, K. (2024). Shaping the techno-social landscape of corrections: How values, technology, and culture influence the design of correctional service delivery applications. *Journal of Criminology*, *57*(3), 294–312. https://doi.org/10.1177/26338076241255530 (Original work published 2024)

ІНФОРМАЦІЙНО-ПРАВОВІ РИЗИКИ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ СИСТЕМИ ПІДГОТОВКИ ПЕРСОНАЛУ ДЕРЖАВНОЇ КРИМІНАЛЬНО-ВИКОНАВЧОЇ СЛУЖБИ УКРАЇНИ В УМОВАХ АВТОМАТИЗАЦІЇ ТА КІБЕРЗАГРОЗ

Дмитро ПОКРИШЕНЬ,
директор Навчально-наукового інституту права, правоохоронної діяльності та психології
Пенітенціарної академії України
кандидат педагогічних наук, доцент
pokryshen@ukr.net
https://orcid.org/0000-0001-9572-413X

Мета. *Основною метою дослідження є здійснення комплексного правового та наукового дослідження інформаційно-правових ризиків, що виникають у процесі цифрової трансформації системи підготовки персоналу Державної кримінально-виконавчої служби України. У сучасних умовах, які характеризуються широкою автоматизацією освітніх процесів та стрімким зростанням складних кіберзагроз, особливого значення набуває аналіз взаємодії таких технологій із чинними правовими механізмами регулювання. Також обґрунтовуються стратегічні напрями удосконалення правових та організаційних засад забезпечення інформаційної безпеки у сфері професійної підготовки персоналу. Особлива увага приділяється необхідності узгодження процесів цифровізації державних інституцій із принципами верховенства права, належного врядування та ефективності адміністративної діяльності.*

Методи. *Методологічну основу дослідження становить поєднання загальнонаукових принципів пізнання та спеціальних юридичних методів дослідження. Формально-юридичний метод застосовано для аналізу національного законодавства та відомчих нормативно-правових актів, що регулюють питання захисту інформації та персональних даних у сфері професійної підготовки персоналу. З метою забезпечення міжнародної релевантності дослідження використано порівняльно-правовий метод, який дозволив зіставити українські підходи до правового регулювання із європейськими стандартами, зокрема положеннями Загального регламенту ЄС про захист даних (GDPR) та ключових директив Європейського Союзу у сфері кібербезпеки. Крім того, застосовано системно-структурний, аналітичний і логіко-правовий методи для виявлення прогалин у законодавстві, організаційних недоліків та специфічних ризиків, що виникають у процесі впровадження автоматизованих і алгоритмічних систем у професійну підготовку персоналу правоохоронних і пенітенціарних органів.*

Результати. *У результаті дослідження встановлено, що цифровізація системи підготовки персоналу супроводжується зростанням ризиків порушення принципів законності, пропорційності та цільового призначення під час обробки інформації. Виявлено недостатній рівень сформованості культури інформаційної безпеки, фрагментарність правового регулювання та невизначеність правового статусу окремих видів цифрових освітніх ресурсів. Обґрунтовано, що впровадження алгоритмічних систем оцінювання та управління освітнім процесом за відсутності належного правового контролю може призвести до зниження прозорості адміністративних процедур і потенційного порушення прав персоналу. Також встановлено, що обмежена імплементація європейських стандартів захисту даних підвищує рівень правових ризиків і кіберуразливостей у відомчій освітній інфраструктурі.*

Висновки*. Зроблено висновок про нагальну необхідність формування цілісного інформаційно-правового механізму підготовки персоналу, який має поєднувати ефективне правове регулювання, системні організаційні заходи та дієві внутрішні механізми контролю із послідовним підвищенням рівня цифрової та правової компетентності працівників. Обґрунтовано, що гармонізація національного законодавства з європейськими стандартами є ключовою передумовою підвищення кіберстійкості державних інституцій та формування інституційної довіри до використання цифрових технологій у публічному секторі.*

Ключові слова: інформаційна безпека публічного сектору, захист персональних даних, цифровізація державного управління, кіберризики в освітніх системах, автоматизоване прийняття рішень, правове регулювання цифрових технологій, цифрові компетентності персоналу.

Дата першого надходження статті до видання: 05.02.2026
Дата прийняття статті до друку після рецензування: 10.03.2026
Дата публікації (оприлюднення) статті: 07.05.2026