

Wilkinson M. D. The FAIR guiding principles for scientific data management and stewardship / M. D. Wilkinson, M. Dumontier, I. J. Aalbersberg et al. // Scientific Data. – 2016. – Vol. 3. – Article 160018. – DOI: 10.1038/sdata.2016.

3.2. Digitalization of higher education: integration of information quality systems and information security standards

Alla KAPITON

National University "Yuri Kondratyuk Poltava Polytechnic"

In the context of the European course toward the digital decade and the automation of production, purely technical and algorithmized skills are losing their status as a market advantage, since they can easily be delegated to artificial intelligence. In accordance with the concepts of the European Education Area, the key value is shifting toward uniquely human competencies, such as critical and creative thinking, reflection, and ethical maturity. It is precisely this human-centered approach, enshrined in the strategies of the European Union (EU), that enables the transformative power of technology to serve the goals of sustainable development and social inclusion.

Extrapolating current trends in pedagogical innovation and computer science makes it possible to state that artificial intelligence (AI), Big Data, Educational Data Mining, and machine learning (ML) technologies will form the fundamental basis of the architecture of higher education for the coming decade. However, the large-scale diffusion of emergent AI tools (in particular, generative models and adaptive learning systems) into educational practice not only optimizes processes but also fundamentally transforms the threat model. Designing future educational trajectories requires the implementation of the concept of Secure AI by Design, since the use of large volumes of personal and academic data creates new vectors for cyberattacks, including the leakage of confidential information, manipulation of learning analytics, and data poisoning in machine learning algorithms [1-7].

Within the framework of the implementation of the EU Digital Education Action Plan, generative and predictive artificial intelligence has become a systemic driver of

modernization for all participants in the educational process at universities - from students and lecturers to the leadership of higher education institutions (HEIs). The introduction of these technologies into the European higher education area makes it possible to scale models of adaptive (hyper-personalized) learning, automate routine knowledge assessment, and implement predictive analytics for forecasting and reducing the risks of dropout or declining academic performance. At the same time, the role of AI as a global catalyst of systemic educational change directly correlates with institutions' capacity to minimize the accompanying cyber risks. The creation of a secure digital educational space of the future presupposes the implementation of mechanisms for the cryptographic protection of AI tools, authentication of AI agents, counteraction to denial-of-service (DDoS) attacks on educational platforms, as well as the development of ethical and security protocols for data use, which is critically important for ensuring the cyber resilience of the entire system of higher education [1-8, 30-37].

Given contemporary requirements of cyber hygiene, higher education institutions must transform their paradigm from the simple reproduction of knowledge to the formation of the agency of future professionals. This entails the development of autonomous critical thinking, capacity for self-regulation, and the cultivation of a high degree of empathy and social responsibility. The integration of these qualities is a necessary condition for effective interdisciplinary collaboration, constructive civic participation, and addressing the complex challenges of today's globalized world.

A pressing problem is the need to help students in higher education develop a strong sense of professional competence formation. This does not mean copying and pasting solutions from other higher education institutions or countries, but rather seriously and dispassionately examining best practice in our own countries and others in order to understand what works in which context [8-16].

The depth and nature of the impact of these fundamental transformations depend directly on society's capacity for a solidary, systemic, and proactive response to new challenges. In European practice of state-level planning, education is recognized as a strategic foundation of national security and competitiveness. It is precisely through

the modernization of the educational ecosystem, as recorded in the strategies of the European Education Area, that the foundation is laid for the successful long-term development and resilience of the country as a whole. Given that the trends of the present century must be taken into account in this sphere, information technologies in education are enjoying particular popularity. Information technologies in education can take several forms. Each is necessary for full-fledged learning and for making this process comfortable and enjoyable for all parties involved. Above all, information technologies have greatly helped lecturers. They provide an excellent means of obtaining all the necessary information and of competently composing up-to-date and modern lessons. Teaching systems are constantly changing, and an enormous number of discoveries are being made, yet with the help of the internet it is easy to stay up to date at all times and to make one's lessons as useful as possible for people today. It is also impossible not to emphasize the form of teaching itself.

It is beyond dispute that information technologies in education make it possible to find not only texts but also videos, slides, and much more on a given subject. Learning is now interesting and enjoyable, since it takes place not only in the form of narration but also with the help of computers, technical equipment, and projectors, presenting information in the most convenient format for learners. Many people have even come to enjoy pursuing higher education at various institutions, although this was previously a considerable difficulty [17-23].

Above all, technology has made it possible to obtain information in any quantity, rather than being limited to a fixed volume. The ability to use the network has become indispensable. Students have also gained the opportunity to display their creative abilities through various presentations, among other things. It is worth speaking separately about how new information technologies in education have made possible the emergence of entirely new projects that support self-directed learning and distance education, which in turn helps maintain the connection between lecturers and students. Moreover, this no longer requires visits to archives and libraries - it is enough simply to have a personal computer with internet access. Higher education is, without doubt, very important, yet there are people who live too far from institutions or who lack

sufficient time. Completing assignments, projects, and examinations remotely is an excellent way of replacing the classical form of education. Lecturers can now teach by means of software, and also have the opportunity to learn languages with students or acquire a new profession that is not too demanding. New trends and strategies for integrating ICT into daily educational practice are a necessary condition for the modernization of the education system. Digital learning materials differ from traditional ones and offer the possibility of managing them (Tyshchenko D. et al., 2024; Kapiton A. et al., 2026; Shestak Ya. et al., 2025; Bidzilya Yu. M., 2025).

Digital educational technologies open up an unprecedented range of opportunities, the scope of which integrally exceeds the basic expectations of higher education students. Contemporary European experience, drawing on the EU Digital Education Action Plan, demonstrates the rapid penetration of innovative solutions into the academic process. The systematic use of videoconferencing platforms, interactive teaching aids, open educational resources (OER), and networked tools for professional communication is transforming traditional didactics, ensuring the flexibility, inclusiveness, and quality of contemporary learning (International Standards and Guidelines: European Higher Education Area; Standards and Guidelines for Quality Assurance in the European Higher Education Area, ESG). On this basis, the purpose of the study is to analyze existing systems and to develop an improved automated system that should enhance the quality of educational services, raise the level of training of future specialists, improve the performance indicators of the department and the higher education institution, and take a step toward the informatization of the education system. In the course of the work, a number of tasks were defined:

- a comparative analysis of the architecture of contemporary higher education quality management systems: an examination of existing quality management models, with particular emphasis on their vulnerability to external destructive influences, and an analysis of how the centralization or decentralization of educational data within these systems affects their overall level of protection against unauthorized access and manipulation of performance indicators;

- a study of the digitalization of the educational space through the lens of cyber resilience: a comprehensive analysis of the digital transformation processes of HEIs, taking into account the expansion of the "attack surface"; an examination of how the integration of cloud technologies, electronic dean's offices, and learning management systems (LMS) is changing the security architecture of the modern educational environment and what new vectors of cyber threats this creates;
- an assessment of risks, exploitation of vulnerabilities, and justification of methods for their minimization: a systematization of the negative consequences arising from the functioning of current information circuits (for example, the risks of personal data leakage, compromise of digital diplomas, or DDoS attacks on critical educational services), and the development of an incident-management strategy along with the implementation of Zero Trust policies to neutralize identified threats;
- the design, architectural modeling, and deployment of a secure information system for HEIs: the development and practical implementation of a comprehensive information system for managing the educational process on the basis of Security by Design principles, envisaging mechanisms for the cryptographic protection of data, strict user authentication, security-event logging, and the assurance of business-process continuity for the educational institution under conditions of cyberattack.

The main theoretical and practical aspects of the work carried out have been presented in the publications of numerous researchers and have been made public at international, European, and all-Ukrainian scientific and practical conferences, whose publications served as a source of inspiration for the study, analysis, and design of future projects.

The synchronization of ICT solutions with life-support systems has actualized the European approach to cybersecurity as a cross-cutting element of national and supranational resilience. Drawing on the EU Cybersecurity Strategy, the protection of critical infrastructure from hybrid threat vectors has become a basic standard of the sustainable functioning of society. This requires institutions to engage in continuous monitoring and proactive response to digital-space risks. The large-scale diffusion of

remote and hybrid employment models, driven by the consequences of the pandemic and the escalation of geopolitical military conflicts, has substantially broadened the landscape of cyber threats and increased the potential attack surface. This has provoked the transformation of hacking activity into the domain of highly technological, targeted threat vectors of the Advanced Persistent Threat (APT) type, which has forced actors in both the private and public sectors to undertake a forced modernization of corporate and departmental security architecture, in particular through a transition to the Zero Trust Architecture concept (the Network and Information Security Directive; the rules of enhanced cybersecurity in the European Union; *Analysis of the Digital Transformation of Higher Education*; Network Detection and Response; *All About Access Control: Everything Covered from Definition, Types, to Features and How-Tos*; UEBA).

In the geopolitical context of Ukraine, ensuring the cyber resilience of the national segment of cyberspace has become a dominant vector in guaranteeing national security and defense. The continuity of the functioning of state institutions, the preservation of the integrity of information resources, and the stability of critical information infrastructure (CII) depend directly on the state's capacity to neutralize network intrusions and to ensure secure interdepartmental interaction in real time (particularly within the framework of "military-civilian synergy"). The complex nature of contemporary hybrid threats manifests itself through coordinated cyberattacks on critical government services, automated process-control systems, and military logistics, aimed at disorganizing state governance. These destructive factors underscore the critical need for a reconfiguration of the system for training and upskilling cybersecurity specialists. This process must be based on the integration of advanced experience from NATO and EU member states (in particular, ENISA and NIST standards), the adaptation of joint incident-response models, and the implementation of practical cyber-defense cases in higher education (the Network and Information Security Directive).

Guided by the standards of the European Research Area (ERA), post-industrial development requires the continuous acquisition of new knowledge and the integration

of emergent technologies into management practice. In the countries of the European Union, the transformation of complex sociotechnical and scientific processes is based on agile management methodologies [32-35]. This makes it possible to turn the constant renewal of intellectual capital into a key factor in sustainable social development and innovative leadership. Any architectural or operational vector of activity in the IT industry and in the field of information protection is subject to a strict data-processing life cycle. This cycle correlates directly with the classical concept of the cybersecurity triad and risk management, encompassing the stages of consolidating primary data, their intelligent analysis through data mining, integrity verification, identification of threat vectors, multifactor optimization of solutions, and strategic planning of targeted infrastructural changes.

In the current architecture of the global information society, the academic environment of higher education institutions - in particular the teaching staff and students - operates under conditions of the permanent exponential growth of heterogeneous data volumes. The psychophysiological and cognitive limitations of the human subject make it impossible to adequately perceive, verify, and fully analyze these vast information arrays (Big Data) in real time. This objective civilizational challenge drives the intensification of the processes of total informatization and digitalization, which act as the principal determinants of societal development. The current stage in the evolution of the information society imperatively requires ensuring a high level of data quality, authenticity, accessibility, and security, which, in turn, depends directly on the reliability and resilience of the telecommunications infrastructure supporting these processes. The comprehensive process of digitalizing the modern educational ecosystem is a multifaceted vector of development aimed at forming a high-tech educational environment. In the context of contemporary security challenges, this process must proceed along two strategic lines: the training of highly qualified IT specialists and the comprehensive assurance of the cybersecurity of all elements of the infrastructure and of learning participants (Shestak Ya. et al., 2025; Pashkovsky V.F., 2025; Yakovenko Y., 2026; Bidzilya Yu. M., 2025).

At the current stage of the development of the information society, there is a destructive tendency toward the predominance of a recreational and entertainment-oriented use of digital technologies among students, which significantly hinders their integration into academic and research activity. The transformation of young people's consumer interests into productive educational and scientific trajectories is directly determined by the level of professional competence of academic staff. A competent lecturer acts as a key facilitator in laying the foundations of digital literacy, preparing future IT specialists for the safe conduct of life and the professional operation of complex information systems.

Accordingly, the successful implementation of the goals of the EU Digital Education Action Plan is impossible without the involvement of highly qualified experts whose profile meets the requirements of the European DigCompEdu framework. Such specialists must combine a deep understanding of the architecture of contemporary didactic processes with advanced methodologies for integrating IT into their field of activity (*Digital Education Action Plan: Policy Background*; the EU NIS2 Directive: what it is, for what needs it was developed, and why Ukraine is implementing it; *Digital Education Action Plan 2021-2027*). At the same time, their high level of general cultural and scientific erudition is a basic condition for forming a high-quality and secure digital educational environment. At the same time, the process of digitalizing education is characterized by significant institutional and structural-functional contradictions. Most lecturers, in the course of teaching their specialized disciplines, encounter poor architectural quality and vulnerability of software, as well as substantial technical and technological barriers in organizing digital learning. These factors exponentially increase the level of technical stress experienced by educators, provoke methodological regression, and lead to a forced refusal to implement computer technologies in the educational process. In the context of training personnel in the field of IT and cyber defense, this gives rise to a critical contradiction: an educational institution's inability to provide reliable, ergonomic, and cyber-secure infrastructure negates the pedagogical efforts aimed at educating future engineers, since the educational process becomes isolated from the industry's real, state-of-the-art toolset.

A significant proportion of the information and communication technologies implemented in domestic educational institutions operate under conditions of an acute shortage of licensed and specialized software. In the context of the strategic design of a unified information educational space, this destructive factor determines the emergence of such critical problems as the absence of unified software architecture standards and a chronic shortage of qualified engineering and technical personnel capable of ensuring the continuous monitoring, maintenance, and cyber protection of hardware systems. This infrastructural asymmetry and insufficient material and technical provision of schools and regional higher education institutions significantly degrade the effectiveness of the didactic process, acting as a direct consequence of limited state funding and a deficit of targeted capital investment in the digitalization of the material assets of the education sector.

An additional destabilizing factor in this process is the conservatism of static educational publications on local information carriers and the use of outdated methodological approaches to designing monolithic software architecture. A consequence of this inertia is a high rate of moral obsolescence of educational content, as well as a complete absence of architectural flexibility for the prompt scaling, reconfiguration, or integration of new modules according to contemporary industrial principles of continuous integration. A separate scientific and practical solution is required for the development of specifications and the further standardization of educational informatization technologies, since, without the normative-technical regulation of these processes on the basis of international frameworks, it is impossible to ensure the basic criteria for the functioning of electronic learning complexes, in particular their manageability, interoperability, accessibility, and stability. At the same time, the practical implementation of electronic courses in the real educational process is constrained by an unsatisfactory level of digital and security competencies among academic staff, as well as by the poor quality of methodological support for existing digital solutions. Within the training of specialists in the field of information technology and cyber defense, these systemic deficits create a critical gap between academic theory and the current technology stack of the industry. The isolation of the

educational environment from real cloud architectures, cyber-defense tools, and proactive threat-hunting systems makes it impossible to form a competitive human capital capable of creating a sovereign and secure national innovation product (Tyshchenko D. et al., 2024).

An analysis of the empirical experience of implementing EU blended-learning models shows that the realization of these educational technologies is a phased, systemically determined process whose architecture encompasses the conceptual, technological, and operational levels. At the initial, conceptual stage, goal-setting is carried out with a clear orientation toward the verification of defined learning outcomes, which involves the formation, cognitive consolidation, systematization, or descriptive refinement of knowledge, as well as monitoring the level of mastery of the relevant competencies. The next, technological stage requires an expert audit and the selection of optimal digital learning resources, whereas the operational stage focuses on functional analysis and the study of parameters of interoperability and secure interaction with the chosen software-and-hardware environment. In strategic and tactical lesson planning, there is an imperative need to take into account the incoming level of students' propaedeutic preparation, the methodological architecture of the classes (lectures, seminars, or laboratory sessions), as well as the psychological, pedagogical, and technical readiness of future specialists to perceive information arrays with the help of innovative technologies (the Network and Information Security Directive; the rules of enhanced cybersecurity in the European Union; *Analysis of the Digital Transformation of Higher Education*).

In the context of training personnel in the field of information technology and cyber defense, the technological and operational stages acquire a specific security-related content, since the selection and analysis of software resources must be based on the principles of Security by Design and on the study of the architectural vulnerabilities of real-world software. The integration of e-learning models makes it possible to intensify the processes of information perception and to significantly improve the quality of training through the introduction of active and interactive didactic forms, which is an imperative requirement of the modern higher school. The

effective implementation of most such methods depends critically on the use of high-technology computing and telecommunications equipment, including specialized cloud laboratories and virtualized cyber ranges, where future engineers and security analysts practice the skills of proactive threat hunting and the deployment of endpoint security systems.

The successful deployment of an e-learning ecosystem requires the consolidation and mobilization of a substantial volume of resources, in particular infrastructural, technical, human, and instructional-methodological ones. Although the creation of such a security-oriented educational environment is associated with a high intensity of financial, time, and intellectual expenditure, the degradation of risks is fully compensated by the high productivity of the educational process and the resilience of the competencies formed. Ultimately, investment in developing lessons involving contemporary information and communication technologies is methodologically justified and highly effective, since it eliminates the gap between academic theory and the requirements of the IT industry, forming a competitive human capital capable of ensuring the digital sovereignty and cyber resilience of the state.

The practical implementation of innovative didactic approaches is ensured through the design and integration, into the educational process of modern higher education institutions, of high-tech information-and-education environments, which are positioned as the most relevant and effective architectural form among the software tools available for educational purposes. The use of such integrated environments is highly productive both within classroom-based engineering training and in the process of the autonomous research activity of future specialists. The systemic potential of such digital platforms makes it possible to fully realize the technological capabilities of the modern computer industry, which directly optimizes the processes of cognitive assimilation of specialized material by increasing its interactivity, visual clarity, and information density. Moreover, the digitalization of didactic content provides the opportunity for comprehensive modeling and analysis of the systems under study, substantially expands the arsenal of methodological techniques for representing

scientific data, and optimizes the time resources required for presenting complex architectural concepts.

According to an analysis of EU experience, in the context of training highly qualified personnel in the field of information technology and cyber defense, the functioning of such information-and-education environments becomes a strategically important security task. Since these platforms constitute the central node for the accumulation of personal data and the university's intellectual property, their design must be based on the principles of fault tolerance, vulnerability isolation, and the Zero Trust concept. Students' autonomous information-search activity within such a secure environment allows them not only to study technology stacks in depth (cloud computing, big data analysis, DevOps) but also to simultaneously master practical cyber-hygiene skills and to study the behavioral factors of threats and endpoint-security algorithms. In this way, the modernized educational environment becomes not merely an instrument for the visualization of material but a simulation ground for developing forward-looking competencies in the design of an architecturally resilient and sovereign national innovation product capable of withstanding persistent hacker attacks and internal destructive influences (Moroz V. et al., 2025; Shestak Ya. et al., 2025; Pashkovsky V.F., 2025).

The implementation of intelligent models and invariants for managing the didactic process creates a synergetic foundation for designing an adaptive and architecturally resilient educational space. In the context of European standards for the modernization of the higher school, this ensures a transition toward flexible personalization (adaptive learning) and a clear structural differentiation of professional training. This approach makes it possible to optimize students' educational trajectories in accordance with the requirements of the dynamic European labor market. Proactive stochastic analysis of current academic performance grants students the ability to dynamically validate their individual pace and trajectory of mastering scientific content, as well as to decompose praxeological tasks according to levels of cognitive complexity and systemic destructiveness. In conjunction with this, the total digitalization of assessment procedures and the automation of predictive monitoring of

professional-competency formation ensure the maximum objectivity of control-and-verification measures, minimizing anthropogenic subjective factors and exponentially strengthening the internal motivational component of learning. The institutionalization of the autonomous cognitive mastery of the theoretical-methodological landscape acts as a key catalyst for the capitalization of intellectual potential and the development of the critical, divergent thinking of the future expert. A specially structured heterogeneous information environment, built on the principles of multifunctionality, determines the optimal organizational and methodological conditions for professional self-determination, systemic self-actualization, and the acmeological realization of the individual under conditions of the digital transformation of society (the Network and Information Security Directive; the rules of enhanced cybersecurity in the European Union; *Analysis of the Digital Transformation of Higher Education*).

In the narrow discourse of the advanced training of highly qualified human capital in the field of information technology and cyber defense, these processes of intellectualization, automation, and orchestration acquire imperative strategic significance. The adaptive diversification of individual educational trajectories allows students to pursue in-depth specialization in high-tech and knowledge-intensive segments, in particular in the field of secure software architecture development (DevSecOps), the methodology of proactive threat hunting, and the administration of layered endpoint-security systems. At the same time, the intelligent automation of knowledge and practical-skills verification is implemented through simulation scenarios based on cloud-oriented virtualized cyber ranges. The objectivity and validity of assessment in such environments is based on empirical time-based and qualitative metrics for reflecting coordinated APT attacks, in particular on recording indicators of mean time to detect (compromise) and mean time to respond to an incident. The systematic autonomous work of students in such a high-intensity and architecturally secure environment cultivates a stable paradigm of continuous professional development (lifelong learning), which is a fundamental criterion for the viability of the contemporary IT engineer or security architect under conditions of persistent and

polymorphic cyber threats and the risks of degradation of critical information infrastructure.

The dynamic and persistent development of information technology architecture acts as a key determining factor in the transformation of contemporary society. The objective process of global societal informatization exerts an imperative influence on the goal-setting, structure, and content of didactic systems, placing forward-looking demands on the professional training of personnel in the field of the operation and design of computing equipment. Under these conditions, the fundamental criterion of the professional fitness of an academic staff member, regardless of their disciplinary profile, becomes a high level of digital competence, a developed information culture, the ability to effectively orchestrate diverse software products in order to achieve defined learning outcomes, and a deep understanding of the functional, engineering, and didactic capabilities of IT infrastructure. The lecturer's principal strategic function within the modernized educational space is shifting from the reproductive transmission of knowledge to facilitating the comprehensive development of the future specialist and their proactive personal and acmeological formation (the Network and Information Security Directive).

The exponential acceleration of the digital transformation of the European higher education area is driven by the synergetic influence of a set of interrelated internal and external factors. According to analytical reports of the European Commission, this process is stimulated both by internal institutional needs of universities (endogenous factors) and by the global demands of the European labor market and the technological challenges of the EU Digital Decade (exogenous factors). First, there is a marked increase in the complexity of the architecture of the pedagogical process under conditions of interdisciplinary convergence of specialized subjects, which requires the deployment of flexible dual-learning models and the strategic synergy of higher education institutions with leading IT corporations, research institutions, and specialized cyber-incident response centers. Second, there is a permanent expansion of the subject-matter and cognitive world of the student, accompanied by an avalanche-like increase in the volume of scientific and technical information, which actualizes the

need to apply intelligent tools for its aggregation, selection, and synthesis. Third, the diversification of future specialists' professional activity areas delegates to the education system the task of forming robust skills for solving polymorphic problems, in particular design-engineering, research, and technological ones. Finally, a significant driver is the intensive diffusion into the didactic space of advanced technologies based on cutting-edge computing tools and secure telecommunications protocols (the rules of enhanced cybersecurity in the European Union; *Analysis of the Digital Transformation of Higher Education*; Network Detection and Response; *All About Access Control*; UEBA).

In the context of training highly qualified human capital in the field of information technology and cyber defense, these factors acquire critical security significance. The modernized digital culture of the educator must necessarily include developed cyber-hygiene skills and an understanding of the Security by Design concept, in order to design learning trajectories that take into account the contemporary threat landscape. Close integration between HEIs and leading IT companies makes it possible to involve leading security architects in creating practice-oriented cases for repelling targeted hacker attacks (APT groups) and analyzing malicious software (ransomware). At the same time, the expansion of the volume of educational material and the increasing complexity of professional tasks requires the use of specialized virtualized cyber ranges, cloud laboratories, and automated knowledge-monitoring tools based on real technical metrics. Thus, the incorporation of advanced computing tools and endpoint-security systems into the educational process ensures the transformation of the classical educational environment into a secure corporate ecosystem capable of training competitive engineers and analysts ready to guarantee the digital sovereignty and cyber resilience of the state.

Summarizing the above, the implementation of information technologies in the educational process should be regarded as a natural determinant and a relevant response to the transformational shifts in the system of higher professional education, oriented toward optimizing and intellectualizing the management of students' cognitive activity. The systematic fulfillment of the outlined infrastructural and didactic

conditions directly catalyzes the achievement of the strategic goal of education modernization, which lies in the verified improvement of the quality of learning, the assurance of inclusive access to knowledge, and the satisfaction of the needs for the harmonious acmeological development both of the individual and of the information society as a whole. At the present stage of scientific and practical discourse, there is an imperative need for a deep understanding and expert assessment of the potential of digital tools for the comprehensive capitalization of students' personal potential, as well as for identifying methodological patterns for their most organic integration into the architecture of the educational process. At the same time, the problem of determining the functional role of contemporary information technologies in the processes of improving and structurally reconfiguring traditional educational systems has remained persistently relevant over recent decades. The successful implementation of state and institutional digital-modernization programs requires not only advanced material and technical equipment for universities but also the advanced training of academic staff and administrative personnel.

Within the European academic space, digital technologies are regarded as a powerful instrument for professional development, self-realization, and the building of an equitable, inclusive partnership with the student community. In accordance with the European DigCompEdu framework, mastery of these tools is an integral part of the lecturer's professional imperative. The use of modern IT enables lecturers to ensure high standards of quality in higher education, transforming classical teaching into a flexible and human-centered process. This directly stimulates the growth of pedagogical authority, transforms functional literacy, and substantially raises the overall level of the lecturer's professional culture, expanding opportunities for scaling and disseminating innovative experience and one's own scientific and methodological views. This vector of development ensures a barrier-free transition of the academic staff member from the reproductive role of transmitter of knowledge to the proactive position of teacher-tutor (facilitator), who organizes, models, and guides the autonomous cognitive activity of students. Ultimately, information technologies play a fundamental role in the development and evolution of teaching methodology, since

the practical activity and innovative pursuits of each individual educator have significant heuristic value for the development of methodological and pedagogical science as a whole. In the context of training highly qualified personnel in the field of information technology and cyber defense, these processes acquire critically important security and industrial significance. Optimizing the management of students' cognitive activity in this domain requires a transition from classical lessons to work within architecturally secure corporate ecosystems that function according to the principles of Security by Design and the Zero Trust Architecture concept. The transformation of the lecturer into the role of tutor and facilitator makes it possible to effectively guide students in choosing individual educational trajectories within such knowledge-intensive niches as secure software development (DevSecOps), proactive threat hunting, and the administration of endpoint-security systems. At the same time, the professional culture and digital literacy of the educator themselves must be based on impeccable cyber hygiene, the ability to model threat landscapes, and the use of cloud-oriented virtualized cyber ranges to automate knowledge assessment on the basis of real technical metrics for repelling hacker attacks. Such high-tech interaction between the mentor-lecturer and the student-researcher ensures the continuity of learning (lifelong learning), eliminates the gap between academic theory and the demands of the IT industry, and forms a resilient human capital capable of guaranteeing the digital sovereignty and cyber resilience of the state in the face of coordinated attacks. In the context of a systemic analysis of higher education quality management, its essential nature is extrapolated into the domain of situational management, whose fundamental basis is determined by processes of multivariate modeling of alternative management decisions and the optimization of tasks of current and strategic planning for the development of didactic systems. Drawing on the current legal and regulatory framework governing the higher education system, it can be stated that the adoption of any management decision in the educational space must imperatively be based on forward-looking methodological developments from both domestic and international scholarly discourse, with obligatory consideration of the unique architectural, ethnocultural, and structural-functional characteristics of national educational

ecosystems. Analyzing European experience, it can be said that no state is capable of ensuring constant progress or maintaining high standards of academic training solely by preserving the existing institutional status quo. The current stage of development actualizes the need for a fundamental rethinking of traditional approaches, the deconstruction of orthodox concepts, and the overcoming of systemic complacency (inertia), which has long dominated the higher-education sector.

The implementation of this strategy demonstrates that no actor in educational activity - regardless of its status as a classical university or a private provider of educational services - is capable of effectively scaling quality indicators until every stakeholder, including academic staff and researchers, internalizes personal, genuine responsibility for shaping a positive educational experience for students and for verifying final learning outcomes. A formal understanding of this responsibility solely at the level of senior administration (rectors, vice-chancellors, or quality managers) is destructive and insufficient to achieve an emergent effect. Moreover, no external quality-assurance body or regulator will be able to sustain the viability of the system by relying exclusively on passive compliance or retrospective audit and assessment of formal processes. The strategic task of the present day is to move toward measuring real, praxeological learning outcomes, even those that appear highly problematic and, at first glance, seem unattainable in terms of forming a general academic consensus.

In the focus of training highly qualified human capital in the field of information technology and cyber defense, the situational character of quality management acquires particular acuteness owing to the high dynamics of technology-stack renewal and the persistent shifting of the cyber-threat landscape. The modeling of management-decision options in this sphere must take into account the concept of Security by Design, whereby the quality of education is determined not by the number of paper reports but by the architectural resilience and sovereignty of the digital products developed by students. Every IT-department lecturer must bear direct responsibility for the relevance of didactic content, integrating into curricula advanced industrial practices of secure development (DevSecOps), proactive threat hunting, and endpoint-security protection. At the same time, regulatory bodies and university internal quality-

assurance systems must move away from the formal checking of syllabi in favor of objectively measuring students' practical skills on the basis of cloud-oriented virtualized cyber ranges. Only recorded technical metrics - such as the mean time to detect anomalies and the speed of disaster recovery under conditions of a simulated APT attack - can serve as a valid criterion of higher-education quality, one that eliminates the gap between academic theory and the real requirements for ensuring the state's cyber resilience.

The institutionalization and establishment of regulatory bodies based on standards with a dual level of responsibility for normative regulation and quality auditing of higher education constitutes a systemically disruptive event within the overall academic landscape of many states. Within this methodology, such a disruptive incident is defined as a purposeful action that in some way interrupts the constant continuity and inertia of the system, while simultaneously acting as a constructive and healthy element in shaping state security and education policy. A direct consequence of such a determined disruption of institutional homeostasis is deep reflection, forced modernization, and the operational-crisis mobilization of all stakeholders in the educational process. Any educational organization characterized by high parameters of stability, dynamism, and adaptive responsiveness to external stimuli is capable of thriving effectively under such a regulatory challenge, promptly identifying and implementing new strategic directions for continuous improvement and the diffusion of innovation. In itself, an artificially created disruptive situation is not an exhaustive equivalent of effective state policy, yet it is capable of challenging conservative academic orthodoxy, neutralizing destructive levels of complacency and psychological comfort, and serving as a trigger for developing and optimizing new regulatory practices. Accordingly, the controlled disruption of stasis in the educational landscape can and should be transformed into a direct outcome of the implementation of innovative thinking within state management, reflecting the government's fundamental commitment to the permanent modernization of state education policy. In the narrow discourse of training highly qualified personnel in the field of information technology and cyber defense, the concept of disruptive management acquires critically important

applied significance, since the contemporary landscape of cyberattacks functions exclusively as a persistent disruptive event. The advanced training of IT specialists under the current conditions of hybrid confrontation is impossible without the artificial modeling of stressful and destructive situations within the educational process itself. The design of educational trajectories must be based on the principle of readiness of systems and personnel for continuous disruption of stability, whereby architects and analysts are trained within the paradigm of Design for Failure and Zero Trust architecture (Mahmood S. et al., 2024; Swire P. et al., 2024; Dede G. et al., 2024; Shnaoli Chakraborty A., 2026; Gangmei N. et al., 2022; Chugh R., 2023).

In this sense, the introduction of new regulatory standards is pushing universities to abandon outdated static programs and is stimulating the creation of flexible learning models integrated with advanced practices of secure development (DevSecOps), proactive hidden-threat hunting, and endpoint-security protection. Genuine innovation in state education policy must be expressed in a transition from passive paper-based compliance to the active testing of HEI resilience. This entails the introduction of automated systems for assessing students' knowledge and lecturers' professional capacity on virtualized cyber ranges, using empirical technical metrics - the time to detect anomalies and the speed of service recovery after incidents (disaster recovery). Thus, the disruptive impulse of state regulation transforms the academic environment from a passive consumer of technology into a dynamic, secure corporate ecosystem capable of generating competitive human capital and ensuring the state's digital sovereignty under conditions of constant cyber threats.

Within the scope of this study, taking into account the standards of the European Higher Education Area (EHEA), critical components of the educational environment requiring conceptual rethinking and modernization have been identified. Orientation toward European benchmarks for university development has made it possible to clearly outline those vectors of the internal ecosystem of HEIs whose reform is a priority for achieving compliance with contemporary criteria of quality and flexibility of learning (Tyshchenko D. et al., 2024; Bidzilya Yu. M., 2025; Tarasovsky Yu., 2026):

- relevance of educational architectures and information resilience. The system-forming destructive factor that undermines the quality of personnel training is the low rate of renewal of educational content. Some state institutions continue to reproduce outdated didactic materials that fail to take into account the current cyberattack landscape and the architecture of modern information systems. In order to ensure national security and form relevant skills for countering cyber threats, higher education institutions must introduce mechanisms for the regular monitoring and proactive updating of syllabi in accordance with the standards of the cyber-defense industry;

- technological integration and digital security of infrastructure. Innovative technologies form the core of a sovereign digital infrastructure and determine the vector of the state's strategic development. At present, there is a cognitive gap between the theoretical base of textbooks and real technological trends, as a result of which students are deprived of practical experience working with secure cloud computing, vulnerability-detection systems, and cryptographic protection tools. Universities must act as drivers of technology transfer, creating secure virtual laboratories and encouraging the effective, safe, and pragmatic mastery by students of advanced software-and-hardware tools;

- cross-border academic mobility and the protection of information exchange. International academic exchange programs constitute a promising and dynamic sector of the educational infrastructure, substantially optimizing both research potential and the sociocultural adaptation of future specialists. Expanding the network of international partnerships and involving students in studying foreign experience requires higher education institutions to establish secure communication channels and to protect the confidential data of participants in mobility programs during the cross-border transfer of information in the global cyberspace;

- digital inclusiveness of education and the security of distance-learning platforms. Key barriers to the full engagement of young people in the educational process are the deficit of regional infrastructure in rural areas and the forced economic activity of students. The optimal tool for overcoming this gap and ensuring equal

access to knowledge is the development and scaling of distance-learning systems. The digitalization of remote education must be accompanied by the deployment of secure web resources, the use of user-authentication technologies, and counteraction to cyberattacks on the electronic databases of educational institutions, which guarantees the stability, continuity, and security of the educational process across the entire state;

- interactive verification of knowledge and the development of analytical potential in the cyber domain. Traditional forms of learning oriented toward rote memorization and textual reproduction during assessment do not ensure graduates' readiness to counter contemporary threats in cyberspace. Genuine engineering and analytical expertise is formed through students' involvement in discussion panels, team projects for developing information-protection systems, and practical simulations such as Capture the Flag (CTF) competitions. The introduction of such innovative methodologies stimulates the development of students' heuristic thinking and their ability to conduct a comprehensive analysis of the vulnerabilities of complex information systems;

- financial optimization and the development of a secure material and technical base. Strategically ensuring high quality of education is a key factor in the state's national security. At present, a constraining factor for many institutions is the unsatisfactory condition or absence of functioning specialized computer laboratories and a shortage of licensed software for network-security monitoring. The state must diversify and increase targeted funding for educational institutions in order to procure high-tech equipment, deploy secure local networks, and create infrastructure that meets contemporary international standards of cyber defense;

- verification of digital competence and updating the knowledge of teaching staff. The current staffing landscape of universities, represented both by contract employees and by lecturers with long tenure, shows a tendency toward insufficient renewal of educational material, which is unacceptable given the rapid evolution of cyber threats. Since academic staff directly transmit professional patterns to future specialists, there is a need for their thorough mastery of advanced security tools and IT-industry standards. Achieving this goal is made possible through the

implementation of systems of periodic assessment, qualification audits, and mandatory internships for lecturers at specialized cyber centers;

- activation of research potential and the development of innovations in the field of cybersecurity. Fundamental and applied research not only stimulates the development of students' heuristic and analytical thinking but also serves as a driving force for raising the university's international standing and strengthening the state's defense potential in cyberspace. Behavioral absenteeism and the low engagement of today's youth in scientific work require systemic disruption. Higher education institutions must transform into drivers of scientific inquiry, creating student R&D laboratories for research into artificial intelligence, cloud-environment security, and counteracting social engineering, which will make it possible to generate innovative patents and raise the overall level of protection of national infrastructure;

- optimizing the numerical ratio of participants in the educational process and cyber hygiene of the environment. The current tendency toward the hyper-concentration of student numbers in lecture halls significantly reduces the efficiency of teaching activity, making it impossible to conduct personalized monitoring of knowledge acquisition and identity verification of students. In order to increase the effectiveness of didactic control and to ensure an adequate level of information security during classes, there is a need to normatively reduce the maximum size of academic groups, which will make it possible to implement the concept of personalized support;

- formation of secure digital learning environments and the security of educational platforms. Notwithstanding the traditional effectiveness of offline interaction, higher education institutions must proactively increase the share of digitalized classes. The deployment of virtual classrooms using secure repositories for storing video lectures and interactive feedback tools makes possible continuous and secure communication around the clock. The application of cloud technologies with encrypted communication channels provides students with secure access to global information resources, while the implementation of automated testing systems guarantees the validity and immediate verification of knowledge-assessment results, laying the groundwork for the universities' future technological development.

An analysis of European practices in building contemporary universities has made it possible to identify, within the scope of this study, the basic parameters of the educational environment requiring systemic optimization and conceptual change. Taking into account EU experience in implementing "smart" and inclusive campuses, the key areas of educational infrastructure and methodology subject to transformation for improving overall learning effectiveness have been identified.

The heads of contemporary educational institutions bear a broad range of strategic and operational responsibilities that extend far beyond the direct regulation of didactic and scientific-methodological processes. The systemic management of a higher education institution requires the continuous orchestration of human resources, the rational allocation of financial resources, as well as the design, modernization, and protection of both the material-technical and the heterogeneous digital environment. This process is persistently accompanied by the need for strict compliance with rigorous regulatory, financial-compliance, and legal requirements, which forces the administrative apparatus to operate under conditions of high intensity in resolving complex logistical, material-technical, and bureaucratic tasks. In view of this, in the professional discourse of top management in the education sector, the dominant priority is defined as ensuring institutional resilience, that is, the unconditional guarantee of the continuity of the organization's operational functioning and the stable provision of educational services under any external conditions.

In light of the implementation of the European NIS2 Directive and the tightening of cyber-resilience requirements, the rapid evolution of cyber threats compels universities to continuously modernize their material-technical and methodological base. In accordance with the European course toward cloud sovereignty, the training of a new generation of specialists must focus on the architecture of geographically distributed systems, cloud computing, and edge-computing technologies. It is precisely this technological foundation that today dominates the deployment of innovative platforms and cyber ranges in EU countries (the EU NIS2 Directive). In the context of training highly qualified personnel in the field of information technology and cyber defense, the task of ensuring the viability of the educational institution acquires a

specific security-related and infrastructural content. For the contemporary head of an HEI, the obligation to keep the institution "afloat" is transformed into a requirement to build a highly effective cyber-resilience system. Since the university's digital environment is a target for coordinated APT attacks and attempts at destructive influence on critical information infrastructure, administrative management must be based on the principles of proactive risk management. This entails not merely formal oversight of computer classrooms but the implementation of Zero Trust Architecture, endpoint-security/EDR tools, and intelligent network monitoring.

Moreover, ensuring the continuity of the educational process under force-majeure circumstances (martial law or man-made disasters) requires management to develop and validate clear strategies for the disaster recovery of digital assets and for business-process continuity. Human and material resource management within this model is integrated with the tasks of deploying cloud laboratories and virtual cyber ranges, which allows IT students to continue practical learning even in the event of losing physical control over the HEI's local infrastructure. Thus, the crisis management of the higher-school leader is transformed into a technological foundation that protects academic sovereignty and creates a reliable platform for forming the state's competitive human capital.

Drawing on the Standards and Guidelines for Quality Assurance in the European Higher Education Area (ESG), the study identifies key aspects of the functioning of the university environment that require structural change. The identified directions of conceptual transformation correlate with European experience in creating a human-centered, secure, and digitalized space for all participants in the academic process (Standards and Guidelines for Quality Assurance in the European Higher Education Area, ESG).

European experience in university management shows that the effective strategic planning of education leaders is often blocked by the need to respond to reactive and situational challenges. The day-to-day activity of HEI heads is complicated by force-majeure expenditures on infrastructure restoration and modernization, a shortage of teaching space, and a deficit of academic and administrative personnel. This forces

management to balance operational crisis response against long-term development goals, a situation characteristic of many European universities during periods of transformation; moreover, the volatility of the pool of higher-education applicants acts as a destabilizing factor that reduces management effectiveness and imposes tight budgetary constraints. The integration of predictive analysis and data-driven management facilitates a transition from a reactive to a proactive model of administration, ensuring the preventive identification of potential risks. In particular, the implementation of artificial-intelligence algorithms makes it possible to optimize energy-consumption expenditure through the dynamic regulation of heating and electricity supply in accordance with actual needs and predictive machine-learning models built on retrospective data. In addition, the digitalization of management processes opens up opportunities for modernizing human-resource management and developing contingency plans for crisis situations. The automation of reporting, the optimization of resource planning, and the introduction of multifunctional analytical dashboards provide the management team with relevant information in real time, in accordance with their functional responsibilities. Contemporary higher education institutions are actively combining AI and Internet of Things (IoT) technologies to maximize operational efficiency and minimize the transaction costs caused by unforeseen situations.

In the context of integration into the European Higher Education Area, one of the most complex systemic challenges for university management is the attraction and institutional retention of highly qualified academic staff. European experience shows that, under conditions of high academic mobility and competition from the business sector, educational institutions need to move from classical administration toward flexible HR strategies that ensure comfortable logistics, competitive motivation, and talent retention within the organization. The shortage of competent personnel has a synergetic impact not only on the individual academic achievements of students but also on the institutional culture and overall viability of the institution. On the global scale, the systemic staffing crisis in the education sector has given rise to a phenomenon defined by the World Bank as a "learning crisis." Artificial-intelligence

technologies are not capable of diversifying sources of staff recruitment or of fully and relevantly replacing human resources. However, the integration of AI makes it possible to optimize monitoring and to minimize staff-turnover rates by neutralizing the destructive factors of professional burnout. It has been empirically demonstrated that educators' priority needs include the expansion of professional autonomy, an increase in the time available for direct didactic activity and methodological preparation, and a reduction of the bureaucratic burden associated with administering testing and preparing reports. Through the algorithmic personalization of individual educational trajectories to differentiate and meet students' specific needs, as well as through the automated real-time generation of analytical reporting, AI eliminates systemic factors of professional frustration. This ensures the optimization of educators' core activities and raises their level of professional self-actualization. The phenomenon of academic attrition at all levels of the educational process is determined by a complex of multifaceted factors. In this regard, a low level of academic performance often acts not as the root cause but as a consequence of destructive tendencies in students' learning activity. The timely identification and predictive analysis of dropout risks allow educational organizations to allocate limited resources in a targeted and rational manner for the implementation of preventive measures.

The analytical potential of artificial intelligence in aggregating and integrating diversified data arrays from heterogeneous sources - in particular, learning management systems (LMS), performance-tracking information systems, and attendance-monitoring systems - ensures the generation of operational triggers and predictive alerts. For higher education institutions, a decline in student numbers generates significant financial, economic, and reputational risks. The early termination of studies by students leads to direct budgetary losses due to a reduction in revenue from tuition-paying students or a decrease in the volume of per-capita state funding. At the macro level, a shortage of graduates correlates negatively with the institution's marketing attractiveness for prospective applicants, and a shift in the ratio of student numbers to teaching staff may necessitate a forced reduction of staff potential. For students themselves, an unfinished educational cycle is equivalent to a decline in labor-

market competitiveness, a reduction in future income, and the accumulation of overdue debt on educational loans. Alongside the classic triggers of attrition - financial deprivation, sociogenic crises, somatic disorders, difficulties in socio-psychological adaptation, and the intensification of cognitive load under conditions of initial separation from the nuclear family - contemporary scholarly discourse draws particular attention to latent threats. In particular, the deterioration of mental health and the psycho-emotional state of students has been recognized as a critical destabilizing factor, requiring the introduction of new systems of psychological support. Addressing the psycho-emotional and material-economic well-being of higher-education students is a priority vector of university management, given the pervasive manifestations of anxiety disorders, distress, and depressive states. This trend, determined both by an objective increase in morbidity and by the destigmatization of mental health in academic discourse, necessitates the formation of a proactive security-oriented environment. In this context, the convergence of psychological-support systems with the cyber-defense infrastructure of the educational institution acquires particular importance.

Drawing on EU experience in countering disinformation and managing digital content, artificial intelligence (in particular, machine-learning methods) is the most effective tool for realizing this convergence. European practice confirms that the automation of contextual analysis and monitoring of the information space with the help of AI makes it possible to promptly detect anomalies, structure data flows, and make accurate management decisions. The development of AI-based cybersecurity architecture in HEIs makes it possible not only to prevent unauthorized access to confidential databases and to protect students' personal information from cyber threats, but also to perform the function of intelligent socio-technical audit. The analysis of students' online behavior, search descriptors, and semantic markers on the network enables cyber-defense algorithms to verify latent suicidal intentions or risks of self-harm. This ensures the generation of automated triggers for the timely involvement of relevant academic staff and the implementation of intervention measures.

In the context of European data-protection standards (GDPR) and the requirements of the EU AI Act, the activation of participatory interaction among educational stakeholders is a priority for HEI management. The experience of EU countries shows that optimizing the tripartite cooperation among administration, local communities, and parents depends directly on the construction of a secure digital architecture. The integration of AI tools into the communication platforms of European educational institutions is carried out according to the "security by design" principle, which guarantees the confidentiality, integrity, and authenticity of information exchange and protects the ecosystem from contemporary cyber threats (the EU NIS2 Directive; International Standards and Guidelines: European Higher Education Area; ERA-UA; *Digital Education Action Plan 2021-2027*; the General Data Protection Regulation, GDPR).

The effective functioning of a verified and cyber-secure information dialogue between the educational organization and the local community optimizes feedback processes for the management apparatus. Secure systems of intelligent public-opinion monitoring allow institutional leadership to conduct the operational collection, depersonalization, and multi-aspect analysis of diversified viewpoints without the risk of leaking personal information or of unauthorized external manipulation of data. The valid data arrays obtained in this way serve as a reliable basis for predictive modeling, the development of security policies, and the strategic planning of the long-term development of the educational institution.

The evolution and systemic modernization of the information society of the EU and the world determine the vector of Ukraine's strategic development. The intensification of market relations in the digital environment necessitates continuous monitoring, comparative analysis, and the systematization of ongoing processes. The dynamism of this environment and the pervasive nature of the threat landscape necessitate predictive modeling of situations for the prompt adjustment of management strategies and the adaptation of management style to conditions of complex cyber risks, with a view to minimizing the consequences of destructive external and internal influences (the Network and Information Security Directive).

Drawing on the experience of the countries of the European Union in forming a common digital space, the systemic development of the information society in Ukraine requires a clearly determined state policy and a unified management approach. The cornerstone of this strategy, following the example of the EU Cybersecurity Strategy, is the creation of resilient infrastructure to protect critically important sectors. This makes it possible to combine technological innovation with strict standards of security and resilience against contemporary hybrid threats. This doctrine must be transformed into a legitimized strategic plan with clear legislative consolidation of the functional duties, roles, and boundaries of responsibility of key stakeholders (the commercial sector, state institutions, local self-government bodies) and civil society within a unified, secure information space (Kapiton A. et al., 2025, 2026; Tyshchenko D. et al., 2024; Franchuk T. et al., 2025).

Given that the quality-audit procedure places strict demands on the competency descriptors of the verifier - which combine inherent personal characteristics with the ability to apply expertly the knowledge and skills acquired through specialized training, practical activity, and validated auditing experience - these parameters must be built into the architecture of the designed digital system.

The development of the functional specification and algorithmic support for automated security-audit systems must be based on European practice in certifying cybersecurity specialists. The algorithms of the system must verify the auditor's profile against a set of professional criteria that correlate with harmonized EU standards, namely:

- multidisciplinary cognitive flexibility: possession of a broad scientific and practical outlook in the field of information security and related disciplines;
- psycho-emotional resistance and volitional stability: the ability to maintain objectivity, composure, and consistency of action under conditions of high stress load and destructive external influences;
- a high level of analytical-synthetic and logical thinking: the ability to conduct a systemic analysis of anomalies, identify hidden correlations, and predictively identify cyber risks;

- expert situational awareness and systemic vision: the ability to make a relevant derivative assessment of the security landscape, to decompose complex processes within the overall cyber-defense strategy, and to understand the functional role and architecture of individual structural units within the organization's overall information-security framework.

It should be taken into account that the professional profile of an auditor in the field of cybersecurity and information protection is determined by the presence of verified knowledge and practical skills in the following conceptual domains:

- the methodological basis of auditing: fundamental principles, standardized procedures, and verified methods for conducting security and systemic audits;
- the architecture of information-security management systems (ISMS): the structure of management systems, reference models, and normative-technical documentation regulating cyber-defense processes;
- the specific operation of the audited object: operational-technological features of activity, the topology of the information infrastructure, and the organization's business processes;
- compliance control and legal support: legal and regulatory acts, specialized legislation in the field of personal-data protection and cybersecurity, as well as contractual obligations and regulatory requirements;
- sector-specific cyber-defense descriptors: specialized knowledge in the field of security engineering specific to a particular market segment or critical infrastructure;
- predictive risk management: principles, mathematical methods, and technical tools for identifying, assessing, minimizing, and monitoring information and cyber risks.

Relevant normative standards regulate the architectural requirements and methodological descriptors for their practical implementation with respect to the following structural processes of an integrated information quality-management system (IIQMS):

Product life-cycle processes (a cluster of basic operational processes):

- determination and specification of technical and security requirements for the final product and related services;
- design and development of products and services based on the concept of a secure software development life cycle (Secure SDLC), taking cyber defense into account at the creation stage;
- end-to-end administration and monitoring of the circuit of interrelated processes within a secure information environment;
- direct production of goods and provision of services under conditions of continuous verification of the integrity of technological data;
- multi-aspect verification, validation, and security audit of product release and service operations;
- management of, and operational response to, deviations and results of processes that demonstrate non-conformity with determined parameters and cybersecurity standards.

Resource management (a cluster of processes for the provision, optimization, and protection of resource potential in accordance with European standards of institutional resilience):

- determination, engagement, and reliability monitoring of human resources, taking into account personnel-security requirements;
- identification, design, and assurance of the resilience of hardware-and-software infrastructure and cyber-defense tools;
- modeling, deployment, and maintenance of a secure environment for the uninterrupted functioning of operational processes;
- allocation and protection of technical resources for the monitoring, measurement, and audit of the quality of processes, products, and services;
- the structuring, storage, and provision of authorized access to intellectual knowledge in order to ensure the compliance of information assets with cybersecurity norms;

- verification and enhancement of the required competence of staff in the field of information protection;
- ensuring the permanent awareness of staff in the domain of cyber hygiene and a culture of quality;
- the generation, regular updating, and cryptographic protection of documented information against unauthorized modification.

Strategic responsibility of the leadership (a cluster of processes for institutional and security management based on human-centered practices and EU corporate standards):

- delimitation of the scope of practical application of the IQMS and definition of the boundaries of the cyber-defense perimeter of the information circuit;
- identification of the IQMS's business processes and regulation of access policies to documented information in order to ensure their stability;
- the assignment of functions, the delegation of authority, and the personification of top management's responsibility for the system's effectiveness and the organization's state of cyber resilience;
- the development, legitimization, and implementation of a comprehensive Quality and Information Security Policy;
- the functional distribution of duties, powers, and responsibility matrices among staff;
- predictive planning of actions, assessment, and proactive neutralization of cyber risks and potential threats;
- the determination of quality and security targets and the development of roadmaps for their achievement;
- strategic planning of architectural changes to the IQMS, taking into account the dynamics of external and internal threat-landscape factors;
- the regulation of protocols and channels for secure internal and external information exchange;
- long-term planning and administration of processes at all stages of the secure life cycle of products and services.

Metrology, analysis, and optimization (a cluster of processes for information-analytical support, cyber audit, and institutional development):

- the identification, continuous monitoring, and comparative analysis of destabilizing factors in the organization's macro- and micro-environment;
- the determination and analytical assessment of the needs, expectations, and compliance requirements of key stakeholders;
- the monitoring, measurement, multi-aspect analysis, and verification of operational-activity results;
- the conduct of regular internal and external security audits of quality and cyber defense;
- a comprehensive review-analysis of the IQMS's operational effectiveness by senior management;
- the identification of potential areas of growth and the formation of innovative opportunities for improving system performance;
- the elimination of identified deviations and non-conformities and the implementation of corrective and preventive measures;
- the permanent evolutionary optimization and enhancement of the cyber resilience of all functional subsystems of the organization.

An analysis of European experience in regulating the digital educational space shows that, within the institutional requirements for an IQMS, the operational circuit for administering ERP systems remains denotatively unexplicated. In this connection, in order to systematically identify risks and verify information security in accordance with EU directives, it is justified to use the following adapted system of concepts:

- proactive quality and cybersecurity planning: a set of predictive actions for establishing quality targets and designing the secure architectural processes and resources needed to achieve these determinants;
- preventive assurance of quality and cyber resilience: systemic actions aimed at forming verified confidence that the regulated requirements for quality and the criteria for the security of information arrays will be fully differentiated and fulfilled;

- operational quality control and security monitoring: regulatory actions and instrumental methods directly aimed at fulfilling quality requirements, compliance control, and protecting the ERP circuit from destructive cyber influences;
- evolutionary quality improvement and cyber-defense modernization: permanent measures aimed at intensifying the system's capacity to fulfill and scale quality requirements, as well as at raising the overall level of resistance of the digital ecosystem to dynamic threat landscapes.

A study of the architecture and operational structure of ERP-system administration on the basis of the APQC classifier makes it possible to synchronize management processes with international standards. Given the European vector of information-security development, adapting this framework to guarantee the cyber defense of the institutional environment involves decomposing it into the following complex of operational domains:

Modeling and determination of quality and cybersecurity requirements:

- identification of parameters and metrics critical for ensuring data quality and security;
- development and implementation of preventive and prophylactic measures for ensuring the cyber resilience of the information circuit;
- verification of the compliance of the formed plan with security-compliance criteria;
- audit and assessment of the system's potential capabilities for ensuring compliance with regulated requirements;
- finalization, validation, and approval of a comprehensive data-quality and data-protection plan.

Expert assessment and verification of compliance:

- instrumental control and audit of process compliance with the approved security and quality plan;
- multi-aspect analysis and evaluation of the results of stress testing, trials, and technical monitoring of the system.

An analysis of European experience has been taken into account in implementing incident management and non-conformity resolution:

- assessment of the potential destructive impact of identified deviations, anomalies, or cyber incidents on the organization's business processes;
- the development and immediate implementation of tactical measures to contain the threat and minimize its consequences;
- causal analysis and identification of the root causes of non-conformities or vulnerabilities;
- the elimination of defects, the remediation of vulnerabilities, and the implementation of long-term preventive security measures;
- the verification of results and the final closure of the incident (non-conformity) record.

Integration, maintenance, and evolution of the enterprise's cyber-secure ERP-system architecture:

- forming a strategy for the intelligent management and protection of the enterprise's information assets;
- the planning, architectural design, and deployment of specialized software and cyber-defense tools for the ERP circuit (with a clear definition of the scope of action, target benchmarks, and objectives);
- delimiting key processes, assigning administrative actors (governing bodies), and defining the system's KPIs;
- the development, standardization, and legitimization of regulations, security policies, operating procedures, and management indicators for the ERP circuit;
- the regular monitoring and assessment of the system's overall performance, resilience, and security;
- the formation of a secure operational environment and the development of staff's professional competencies in the field of cyber hygiene, with a view to the permanent modernization of the management system.

The standard in question presents a formalized textual description of the ERP-system management process, adapted to European standardization and technology requirements, structured according to the following key parameters:

- purpose (objective): ensuring the relevance of products, services, and the management process itself to the organization's strategic and project goals, and determining a high level of customer satisfaction;

output artifacts (results): verification and realization of organizational goals, management policies, and procedures; substantiation of criteria and methodology for quality assessment; allocation of resources and relevant information to support the functioning and monitoring of quality-assurance measures; aggregation and implementation of quality-assessment results; the continuous optimization of ERP-system management policies and procedures on the basis of retrospective project and organizational indicators; functional tasks and operations: strategic and operational planning, monitoring assessment, and the implementation of corrective and preventive measures within the ERP-system management circuit.

In addition to the parameters noted above, the standard also regulates the working artifacts (input and output data) of the quality-management assessment process. On the basis of the resulting information base, an original model of the "ERP-System Management" process is proposed. At the same time, the normative provisions of the standard state that improvement activity varies in scale and intensity - from continuous local improvements to strategic transformations at the level of the entire organization. Given this specificity, the "Quality Improvement" stage within the developed model is determined through the lens of the functional operation "Non-Conformity Resolution" within the structure of the "ERP-System Management" process, and is also singled out as an independent operation, "Improvement Initiation," within the IQMS process group "Measurement, Analysis, and Improvement."

Within the operational component "Quality Control" of the developed model, the assessment of performance and the determination of the IQMS's maturity level are implemented through the mechanisms of internal audit and self-assessment, respectively. Internal audit, as an imperative regulatory requirement of the standard,

constitutes a systematic, independent, and documented process of verifying and objectively evaluating audit evidence for its relevance to established criteria. On the basis of audit findings, a comparative analysis and assessment of the IQMS's compliance is carried out with respect to: the organization's own (endogenous) requirements for the system's functioning; the regulatory provisions of the international standard ISO 9001; and the determined criteria for its effective implementation and subsequent maintenance.

Beyond confirming compliance, the functional purpose of internal audits consists in:

- identifying best practices for their further diffusion and scaling to other areas of the enterprise's activity;
- identifying latent opportunities for the continuous improvement of processes.

The methodological toolkit for accumulating audit evidence includes:

- surveys (interviews, as well as the use of checklists and structured questionnaires);
- systematic analysis of regulatory and operational documentation;
- empirical observation of the course of processes and production activity.

To formalize and descriptively model the relationships between objects and processes within the quality-audit circuit, the use of a semantic network is justified. The implementation of the quality-audit process presupposes that auditors comply with regulated competency criteria that integrate determined personal characteristics with the ability to effectively apply theoretical knowledge and practical skills acquired during academic training, professional activity, specialized preparation, and direct expert practice. The regulated requirements for the personal characteristics of an auditor include: a broad worldview, emotional stability (composure), purposefulness, and developed logical thinking and analytical abilities. The professional profile of the specialist presupposes the ability to objectively assess situational context, to perceive complex processes systemically through the lens of the organization's strategic benchmarks, and to understand the structural-functional relationships between its

subdivisions. The competency base of the auditor's professional knowledge and practical skills must integrate the following determinants: the methodological principles, regulations, and toolkit for conducting audits; the architecture and specifics of interpreting management-system standards and related normative-reference documentation; the organizational-functional features and context of the enterprise's activity; the legal, contractual, and other forms of regulatory support binding on the audited object; specialized expertise in the specific subject area of management; and the methodological approaches, technical techniques, and risk-management tools implemented within the overall management system.

In accordance with European standards for the auditing of information systems and the requirements of the ENISA ECSF framework, the effectiveness of implementing security procedures is directly determined by the deontological culture of specialists and by the specification of their individual psychological profile. In EU practice, where particular attention is paid to professional integrity and compliance ethics, the following imperatives are singled out within the structure of an auditor's personal qualities: ethicality - the implementation of principles of integral honesty, truthfulness, authenticity, and rational judiciousness; cognitive openness and axiological impartiality - perceptual readiness for the objective reproduction and analysis of alternative concepts or divergent points of view; diplomacy - tactfulness and adherence to the norms of business etiquette in the context of interpersonal and professional communication; observational acuity - the ability to conduct continuous proactive monitoring of the operational environment and the course of processes; receptivity - a high level of contextual awareness and the ability to cognitively model and relevantly understand situational factors; versatility - adaptive flexibility ensuring the prompt reconfiguration of activity under dynamic conditions; persistence - volitional purposefulness and a stable orientation toward achieving the teleological objectives of the audit; decisiveness - the timely adoption of validated decisions on the basis of praxeological analysis and logical synthesis; professional autonomy (independence) - the ability to fulfill functional duties independently while maintaining a constructive interface of interaction with other process actors; integrity of principle -

readiness to perform duties responsibly in accordance with professional ethical norms under conditions of potential destructive pressure, cognitive dissonance, or open confrontation; striving for self-improvement - the permanent accumulation of knowledge in the course of practical activity and orientation toward maximizing the effectiveness of the audit process; sociocultural compliance (a high standard of conduct) - a presumption of respect for the endogenous corporate culture, traditions, and values of the audited object; and the ability to collaborate - synergetic intersubjective interaction within the audit team and with the personnel of the object being assessed.

In order to intensify the development of the professional competencies of quality-audit actors, a parametric model has been substantiated and constructed in the form of an invariant IT Infrastructure Assessment Report (ITIAR), which ensures the consolidation of the normative requirements and recommendations of relevant international and national standards. Depending on the determined specifics of the subject area, this set of parameters is subject to adaptive modification, taking into account the relevant requests of stakeholders, the organization's contextual environment, and the basic qualification profile of the experts involved. The modeling of the audit life cycle, integrating the stages of pre-project preparation, direct verification, and retrospective analysis of results, is proposed for implementation on the platform of the business-modeling software environment "Business Studio." The systemic integration of data is ensured through the functional content of the repositories and directories of the specialized "IQMS" module. On the basis of the verified information array of the audit registration circuit, the algorithmic automated generation of a unified reporting form, the "Audit Results Report," is envisaged. The functional potential of the tool under study ensures the architectural realization of the developed ITIAR, which is integrated into the organization's overall designed document-management structure. The logical architecture of the data repository provides for the following determination: the nomenclature of audit parameters is imported into the attribute field "Section" of the document card, while their semantic content (actual value) is recorded in the "Comment" field. The normative-regulatory

requirements for the parameters being verified are localized in the "Comment" field of the corresponding attribute section of the object. The use of the system directory "Object Attribute Sections" optimizes the procedure of conceptual modeling, since the implementation of the single-data-entry principle, with the possibility of its further cumulative updating, guarantees the repeated automated diffusion of this information into analytical reports for various modifications of ITIAR. For the unified description of the architecture (template) of the ITIAR document, the use of standard customization tools and the generation of custom reporting forms of the "Business Studio" system is justified. The final result of implementing this algorithm is the design of the ITIAR document in a regulated format. In order to aggregate, verify, and cross-tabulate information on audits conducted and recorded in the "Business Studio" database, Object Linking and Embedding (OLE) automation technology has been implemented, creating the technological basis for the automatic generation of comprehensive summary reports in a spreadsheet environment.

In light of European trends in developing a secure educational and scientific space, the proposed "ERP-System Management" process model, in combination with the ITIAR architecture, serves as a fundamental basis for competency management. The integration of international reference security practices into this model makes it possible to create a resilient system for the long-term extension and validation of professional knowledge. This ensures that the competencies of cyber-defense actors and verified stakeholders remain adaptive and relevant to the contemporary challenges of the information society. The implementation of the "Business Studio" tool determines a transition to proactive risk management, enabling the systematic analysis and preventive neutralization of vulnerabilities, the continuous development of the expert potential of information-security auditors, and the permanent monitoring and quantification of the effectiveness of countermeasures aimed at resolving incidents and optimizing the overall circuit of the cybersecurity management system. Algorithmic guidance for developing a customized ITIAR analytical report within the "Business Studio" business-modeling architecture is available for download through the author's verified feedback interface on the author's specialized website.

The proposed process model and ITIAR architecture, which codifies the requirements of international cybersecurity and information-protection standards, provide a conceptual basis for determining and extending the professional competencies of personnel and relevant stakeholders within the enterprise's cyber-defense circuit. The use of the analytical toolkit of the "Business Studio" platform makes possible a transition to a proactive management paradigm: the regular monitoring of vulnerabilities, the preventive neutralization of cyber threats, the continuous verification of the qualification level of security auditors, and the quantification of the effectiveness of countermeasures aimed at containing incidents and optimizing the information-security management system.

In the process of developing an audit program, architectural and logical priority should be given to a set of determinants that includes: the degree of criticality of a subdivision's functional processes for ensuring the organization's overall cybersecurity circuit; a retrospective analysis and the verification status of previously identified vulnerabilities or compliance non-conformities based on the results of prior inspections; and the cumulative results of top management's strategic review and validation of the effectiveness of the ERP-system's security management circuit. An unscheduled internal cyber-defense audit is initiated when it is necessary to verify readiness for certification compliance, or when triggers defined by the institution's leadership in administrative documents call for the urgent assessment of infrastructure security. In this case, the planning procedure must implement a continuous audit of every process within the area of responsibility of the structural subdivision integrated into the overall ERP security ecosystem.

Guided by European approaches to the security of audit procedures, during the preparatory stage a verified group of experts develops questionnaires and accompanying documentation on the basis of a legitimate technical assignment. In order to comply with the strict information-security protocols adopted in EU countries, access to these working files is isolated within the audit circuit. This preventive measure makes it possible to neutralize the threats of unauthorized access and guarantees the impartiality and confidentiality of the entire inspection process. Among

the basic criteria for the internal audit of a department, in the context of assessing its cyber resilience and the security of its information assets, is the verification of infrastructural provision, encompassing the audit of the material and technical base, in particular specialized classrooms, computer laboratories, and personal computers involved in the educational process and requiring network-security control. Alongside this, the content component and documentary support are subject to assessment, namely, the availability and completeness of course syllabi, methodological support for coursework and final-qualification assessment, sets of comprehensive assessment tasks, information on internship placements, and records of educational literature and specialized periodicals, which are regarded as information resources of the department. Particular attention is paid to the protection and analysis of research-activity data, including its funding, the architecture of task distribution, the parameters of scientific schools, staffing, publication activity, exhibition activity, and intellectual property. Within the unified information space, the following are analyzed: the monitoring of graduate adaptation, the parameters of international cooperation and the training of foreign specialists, the effectiveness of postgraduate studies, the publication activity of academic staff, forms of knowledge-quality control, and the integration of the department's staff into the overall security architecture of the institution's ERP system.

The architectural components of an integrated system for monitoring the quality of the educational process within the cyber-defense circuit consist of sequentially interconnected procedures, beginning with the permanent monitoring and diagnostics of the state of security of the information environment. The next stage is the determination of regulatory standards and the establishment of baseline security profiles, on the basis of which the quantification of measurable parameters and the formalization of clear criteria for assessing the system's cyber resilience are carried out. The process concludes with an in-depth analysis of the verified data obtained and the implementation of appropriate preventive or corrective countermeasures, accompanied by the verification of their effectiveness in accordance with current security regulations and management functions oriented toward optimizing secure

information provision and enhancing the overall effectiveness of managing the institution's IT infrastructure.

The empirical results of comprehensive monitoring serve as a fundamental determinant in the process of ensuring the quality of educational activity, since they provide management bodies with valid information on the relevant state of the educational system and its structural elements. This toolkit makes it possible to verify destructive anomalies and latent problems arising at the stage of achieving strategic goals, as well as to forecast general industry-development trends for the further design of effective public-management policy. In this context, monitoring the quality of education is transformed into a basic, cyber-secure instrument for administering its ERP system, one that guarantees the authenticity, integrity, and resilience of analytical data arrays against external and internal destabilizing cyber influences. The university's quality-assurance doctrine, synchronized with the Standards and Guidelines for Quality Assurance in the European Higher Education Area (ESG), is implemented end-to-end across all vectors of the HEI's institutional activity. It is oriented toward forming a resilient internal culture of quality, strategic coordination, and encouraging members of the academic community to make verified (data-based) decisions within the framework of the permanent modernization of the didactic process.

In the context of implementing European approaches to higher-education quality assurance, the security and education policy developed demonstrates full congruence with state standards, legitimate accreditation criteria, and legal regulators. It acts as an organic element of the HEI's overall compliance system, ensuring the interconnection between academic requirements and security standards across all functional domains of the modern digital university's operation. In formulating a quality-assurance doctrine, the management of the higher education institution has determined the following fundamental imperatives, which define the methodological principles governing the functioning and management architecture of a cyber-secure ERP system within the university environment:

- harmonization with international standards: the implementation and legal-regulatory adaptation of the basic principles of the Bologna Declaration within a unified, secure digital space;
- digital transformation of administration: the introduction of a comprehensive automated system for managing the processes of training highly qualified personnel, based on an integrated and cyber-resilient ERP circuit;
- diversification of educational derivatives: expanding the range of educational services through the introduction of innovative technologies oriented toward ensuring sustainable financial and economic development and the protection of intellectual capital;
- resource compliance control: systemic methodological, infrastructural, and staffing support for the design of new specialties, innovative fields of training, and specialized academic disciplines;
- permanent optimization of the didactic process: the modernization of teaching technologies and the introduction of intelligent tools for monitoring students' learning trajectories;
- intensification of cognitive validation: the systematic enhancement of the quality and competitiveness of student training, ensuring the integrity and confidentiality of assessment results;
- inclusiveness and accessibility of digital infrastructure: ensuring unobstructed, verified, and secure access to higher education for citizens while maintaining protocols of user identification and authentication;
- integration into the market environment: the introduction of an automated system for the predictive promotion of graduate employment and the optimization of processes of their professional adaptation to the dynamic requirements of the labor market.

To summarize the above, ensuring high quality of the educational process is a dominant imperative of contemporary socioeconomic development. This necessitates the design and implementation of cyber-secure, intelligent systems for the mass reflection of the outputs of educational institutions and their structural units. These

platforms must operate on the basis of secure tools for comprehensive monitoring, security auditing, and the validation of the cognitive potential of both academic staff and students. The integration of such innovative solutions into the circuit of ERP systems for managing educational services requires the development of a resilient cyber-defense architecture to prevent unauthorized modification and the leakage of reputational and personal data. The modernization of the institution's digital ecosystem will ensure the verified transparency of assessment, minimize the risks of cyberattacks on testing systems, and form a synergetic trigger for the permanent professional self-improvement of both individual actors and the organization's structural units as a whole.

In the context of the European benchmarks of the Digital Decade and post-industrial development, the transformation of society is accompanied by an imperative transition toward diversified models of remote and hybrid employment. European practice in regulating the labor market demonstrates that the effective functioning of such flexible formats is possible only on the basis of a resilient architecture of geographically distributed information-and-communication systems and heterogeneous cloud computing, which ensure business-process continuity and data protection. However, the large-scale decentralization and deconcentration of business processes give rise to a complex of specific structural-functional, architectural, and critical-level security vulnerabilities. In the context of a systemic analysis of security risks, the leading destructive factor is the fragmentation of the unified communication circuit, caused by the deficit of a unified, secure environment for operational monitoring and management (a Common Operational Picture), which critically undermines the effectiveness of incident management and coordination of action in crisis (entropic) situations. The dispersal and uncontrolled diffusion of project-management tools, classified as the "Shadow IT" phenomenon, not only degrades the synergetic effect of team engineering interaction but also exponentially expands the overall potential attack surface. This creates unregulated, latent channels for the leakage of confidential data and intellectual property through the compromise of unprotected peripheral endpoints. This spectrum of threats delegates to the IT higher

school the task of forcibly modernizing didactic models for training specialists. The contemporary IT engineer, cloud architect, and cybersecurity analyst must possess forward-looking, cross-functional competencies in the areas of designing systems according to Zero Trust Architecture methodology, centralized identity and access management (IAM/PAM), the orchestration of secure channels (SD-WAN/SASE), as well as auditing infrastructure to detect hidden Shadow IT components.

To neutralize and minimize these destructive (entropic) factors, European digital-transformation practice highlights the need for a paradigmatic shift from discrete application software products toward integrated next-generation digital platforms. In accordance with European requirements for technological sovereignty and interoperability, such solutions must function as architecturally secure corporate ecosystems that ensure the seamless and secure exchange of data among all process participants. The design and deployment of such environments must be determined by the imperative implementation of Security by Design principles and the conceptual provisions of Zero Trust Architecture, within which every subject, verified device, and information session is subject to continuous, context-dependent dynamic authentication and proactive verification.

Under such conditions, the cryptographic resilience of telecommunication channels, the determined delimitation of access rights on the basis of role-based and attribute-based models (RBAC/ABAC), and the integration of intelligent data-loss-prevention systems become fundamental imperatives of systems engineering. The security of the processes of data storage, transit, and heterogeneous processing is positioned not as an isolated technical requirement but as a systemic criterion of the architecture's viability, one that guarantees adherence to the classical information-security triad (confidentiality, integrity, availability - the CIA triad) and defines a high level of cyber resilience of distributed critical infrastructure under conditions of persistent coordinated attacks and insider threats.

In light of the modernization of the European Higher Education Area, the technological context presented determines a fundamental restructuring of the architecture of educational programs for IT specialties. The content of professional

training must evolve from the applied mastery of programming-language syntax toward the development of higher-order cognitive and metacognitive capacities, in particular systemic architectural thinking. It is precisely this vector that guarantees the institutional compliance of university education with the requirements of European professional standards and the long-term competitiveness of specialists. Future software engineers, cloud-solution architects, and cyber-defense experts must possess forward-looking, cross-disciplinary competencies in the mathematical modeling of security policies, cryptographic design, and automated incident management, which is the guarantee of creating a sovereign digital product resilient to external influences.

Under the determined conditions of contemporary hybrid warfare, the geopolitical space of Ukraine has become a key experimental macro-arena of intensive conventional and unconventional confrontation in the info-sphere, containing the coordinated destructive expansion of highly qualified pro-government APT groups. The polymorphic and stochastic nature of contemporary cyberattacks - ranging from high-intensity, application-layer (L7, per the OSI model) DDoS incidents to the targeted compromise of systems via ransomware and fileless malware - imperatively necessitates the institutionalization of a layered, adaptive system of national cyber defense.

Ensuring the architectural resilience and cyber resilience of critical information infrastructure objects requires not only the diffusion of innovative EDR/XDR (Endpoint/Extended Detection and Response) class technological solutions and the implementation of post-quantum cryptographic protocols, but also the forced capitalization of the human factor within the concept of human-centric security. This security imperative determines a fundamental transformation of the educational and scientific paradigm for training specialists in the field of knowledge "Information Technology." Future IT engineers, cybersecurity analysts, and systems architects must possess forward-looking, cross-functional competencies in the fields of proactive risk management, behavioral analysis, and the modeling of a resilient culture of organizational cyber hygiene as a fundamental basis for minimizing anthropogenic cyber risks.

A separate theoretical-methodological and scientific-practical discourse is required for the determination and classification of cyber threats extrapolated from the consequences of martial-law force-majeure circumstances and kinetic and man-made destruction. Minimizing and neutralizing their destructive, entropic impact on critical information infrastructure delegates to the higher IT education system the strategic function of forming a pool of highly qualified personnel possessing competencies in the architectural modeling, deployment, and dynamic reconfiguration of adaptive systems for the proactive monitoring and detection of cyberattacks.

The contemporary paradigm for training software engineers and cybersecurity architects is shifting toward the imperative mastery of the concept of layered endpoint security (Endpoint Security/EDR) and the containerized isolation of vulnerabilities across diversified remote workplaces under conditions of stochastic connectivity, the degradation of data-transmission channels, or the complete loss of physical control over the hardware perimeter of the infrastructure.

Accordingly, the modernization of higher-education standards and syllabi in the field of knowledge "Information Technology" necessitates the convergence of the theoretical base with verified practical cases of real-world experience in repelling targeted attacks. The training process must be institutionalized through the implementation of virtualized cyber-range technologies and must focus on developing skills in designing fault-tolerant systems, business-continuity algorithms, and flexible strategies for the disaster recovery of digital assets.

Under conditions of the total digitalization of societal processes and the escalation of cyber confrontation, the architecture of the resilient functioning of state and corporate institutions depends critically on the availability of secure network infrastructure and the integration of next-generation intelligent DLP systems. Such a technological imperative places fundamentally new demands on the training of specialists in information technology and software engineering. The contemporary IT specialist must possess the skills to design fault-tolerant, zero-trust systems in which cryptographic security and leak protection are integrated directly into the software-development life cycle.

The dynamic and highly technological nature of contemporary cyberattacks necessitates a fundamental transformation of the academic and research vectors in IT education at HEIs worldwide and within the EU. The training of personnel must evolve from the passive study of cyber-hygiene regulations toward an in-depth practical analysis of the mechanisms of threat realization and the study of adversaries' tactics and procedures within the framework of the threat-hunting concept. The higher school, together with the scientific community, must ensure a transition to practice-oriented learning using cloud-based cyber ranges and reverse-engineering tools, which will enable future IT analysts to develop predictive, AI-based defense algorithms.

Ensuring the constant and balanced development of knowledge-intensive and high-tech sectors of the national economy under conditions of global geopolitical transformation necessitates a fundamental reconceptualization of state policy in the info-sphere and in the field of cybersecurity. At the current stage, the dominant priority is to achieve an emergent effect from the synergetic interaction between the research and innovation hubs of higher education institutions and the industrial demands of real-sector economic actors.

In light of the European transition to the concept of "Industry 5.0" and the implementation of the EU Digital Education Action Plan, the modernization of the contemporary paradigm of higher IT education requires a decisive rejection of classical reproductive learning models. European experience demonstrates the need to implement forward-looking, human-centered, and security-oriented strategies. This approach makes it possible to train specialists capable not only of adapting to technological breakthroughs but also of designing digital systems that take into account ethical norms and the EU's strict requirements for cyber resilience. This process entails the implementation of flexible dual-education trajectories, the architectural and financial stimulation of university R&D centers, and the institutionalization of public-private partnership through the direct integration of leading IT architects, software engineers, and cyber-defense experts into the processes of developing and updating higher-school standards.

The fundamental reconfiguration of the architecture of educational and research systems must be based on the principles of Security by Design. Such an integrated approach is a key determinant in forming competitive human capital - a consolidated pool of highly qualified specialists (security engineers, zero-trust architecture developers, cyber-threat analysts). It is precisely this personnel potential that is capable of ensuring the development, scaling, and implementation of a sovereign national innovation product, architecturally resilient to destructive (entropic) external and internal cyberattacks, thereby guaranteeing the state's digital sovereignty and cyber resilience.

A mandatory institutional foundation for developing a sovereign IT sector and training highly qualified specialists is the formation of an adaptive legal and regulatory framework. This entails the introduction of stimulating economic levers, in particular tax preferences for knowledge-intensive business, the minimization of financial pressure on startup ecosystems, and targeted state grant funding for university R&D centers. This approach makes it possible to create innovation clusters based at higher education institutions, where future IT architects and cybersecurity engineers have the opportunity to work on real high-tech projects.

The task of minimizing risks to corporate data and ensuring the resilience of information-production networks requires the transformation of educational programs to include the study of network-perimeter defense in depth (Defense-in-Depth). Future specialists must master technologies for end-to-end monitoring and intelligent traffic filtering within the concept of Network Detection and Response (NDR), analyzing anomalies in both external and internal (east-west) network traffic.

In this context, particular relevance is acquired by the formation, in future specialists, of competencies in protecting and verifying specialized microservice architectures and APIs that sustain the operation of complex ERP/CRM and PLM ecosystems of modern enterprises. Given the sharp intensification of APT attacks and cyber sabotage under the current crisis conditions of hybrid war, the vector of scientific and practical research in higher IT education must be shifted toward studying the vulnerabilities of technical infrastructure components. This includes training personnel

to conduct penetration testing, source-code security analysis (SAST/DAST), and the protection of industrial ICS/SCADA systems. This is a fundamental condition for ensuring the technological resilience of the domestic industrial complex.

Contemporary experience of European universities demonstrates that predictive and generative AI has become a basic instrument for improving effectiveness for the key stakeholders of the higher school. The technological solutions being implemented in the European educational ecosystem are transforming routine practice: they adapt content to individual student needs, optimize the grading of assignments, and provide administration with reliable predictive data for the preventive response to educational crises and risks. Extrapolating digital-transformation trends allows us to assert that, over the coming decade, artificial-intelligence technologies will form the fundamental didactic and architectural basis of higher IT education. The diffusion of emergent AI tools (in particular, generative models, predictive analytics, and adaptive learning systems) is being integrated directly into the training trajectories of specialists in computer science and cybersecurity. This requires the implementation of the concept of Secure AI by Design in the educational process, since future IT engineers must not only use AI to automate development or anomaly analysis but also understand the specific threat vectors targeting AI systems themselves, such as data poisoning, attacks on machine-learning models, and the leakage of confidential information through LLM interfaces.

REFERENCES FOR SUBSECTION 3.2

1. Kapiton A., Franchuk T., Tyshchenko D., Kurbanova O. Formation of cybersecurity architecture of innovation parks in the context of digital transformation and global technical and economic challenges. *Control, Navigation and Communication Systems*. 2026. Vol. 2 (84), pp. 120-124.
2. Tyshchenko D., Franchuk T., Stepashkina K., Karpunin I. System design and development corporate electronic document management. *European Scientific Journal of Economic and Financial Innovations*. 2024. No. 1(13), pp. 200-207.

3. Franchuk T., Tyshchenko D., Desiatko A., Karpunin I. Features of accounting digitalization processes. *Galician Economic Journal*. 2025. Vol. 95, No. 1, pp. 61-66.
4. Tyshchenko D., Franchuk T., Zakharov R., Moskalenko V. Supporting dynamic security needs with VPN tools. *Control, Navigation and Communication Systems*. 2024. No. 3 (77), pp. 149-152.
5. Kapiton A., Franchuk T., Tyshchenko D., Desiatko A., Zakharov R. Requirements for modern processors for secure operation of information systems and networks. *Control, Navigation and Communication Systems*. 2025. No. 3 (77), pp. 111-117.
6. Kapiton A., Franchuk T., Tyshchenko D., Desiatko A. Integration of cyber defense into innovation-park infrastructure: conceptual and methodological foundations for forming a secure digital environment. *Khmelnyskyi Scientific Bulletin. Technical Sciences*. 2026. No. 363(2), pp. 386-390.
7. Kapiton A., Franchuk T. M., Tyshchenko D. O., Desiatko A. M., Zakharov R. G. Formation of cybersecurity architecture of innovation parks in the context of digital transformation and global technical and economic challenges. *Tavriya Scientific Bulletin. Series: Technical Sciences*. 2026. Issue 3, pp. 79-85.
8. Mahmood S., Chadhar M., Firmin S. Countermeasure strategies to address cybersecurity challenges amidst major crises in the higher education and research sector: An organisational learning perspective. *Information*. 2024. Vol. 15, No. 2, art. 106.
9. Swire P., Kennedy-Mayo D., Bagley D., Krasser S., Modak A., Bausewein C. Risks to cybersecurity from data localization, organized by techniques, tactics and procedures. *Journal of Cyber Policy*. 2024. Vol. 9, No. 1, pp. 20-51.
10. Dede G., Petsa A. M., Kavalakis S., Serrelis E., Evangelatos S., Oikonomidis I., Kamalakis T. Cybersecurity as a contributor toward resilient Internet of Things (IoT) infrastructure and sustainable economic growth. *Information*. 2024. Vol. 15, No. 12, art. 798.

11. Daisy G. Digitalization of higher education: opportunities and threats. URL: https://www.researchgate.net/publication/383057099_digitalization_of_higher_education_Opportunities_and_Threats (accessed 28 June 2026).
12. Shnaoli Chakraborty A. Implementation of NEP 2020 in Higher Education: The Open University Example. Available at: shodhgyan.org (accessed 28 June 2026).
13. Atabik A., Nurfuadi N., Imam H., Masruri M., Nur S. Digitalization of educational quality management in higher education. URL: https://www.researchgate.net/publication/381388103_Digitalization_of_Educational_Quality_Management_in_Higher_Education/link/666c2323a54c5f0b9464ff02/download?_tp=eyJjb250ZXh0Ijp7ImZpcnN0UGFnZSI6InB1YmxpY2F0aW9uIiwicGFnZSI6InB1YmxpY2F0aW9uIn19 (accessed 28 June 2026).
14. Gangmei N., Thomas N. Use of Information and Communication Technology for Quality Education. The Barcelona Conference on Education 2022: Official Conference Proceedings. 2022. pp. 375-385.
15. Chugh R. Implementing educational technology in Higher Education Institutions: A review of technologies, stakeholder perceptions, frameworks and metrics. *Education and Information Technologies*. 2023. No. 28, pp. 16403-16429.
16. Yampol Y. Using information and digital technologies for improving education quality management in general secondary education institutions. *Information Technologies and Learning Tools*. 2024. Vol. 102, No. 4, pp. 148-162.
17. Moroz V., Tereshchenko A., Buka S., Kruhlov V., Moroz S. Information technologies in ensuring the quality of higher education: approaches, challenges and prospects. *Information Technologies and Learning Tools*. 2025. Vol. 107, No. 3, pp. 120-134.
18. Shestak Ya., Zavgorodnya Ye., Krasnoshchok V. Technical protection of the information infrastructure of a commercial enterprise. *Development of Education, Science and Business: Results*. 2025. URL: <http://www.wayscience.com/wp->

(accessed 28 June 2026).

19. Pashkovsky V.F. Identification of political and legal mechanisms of information security of the state under conditions of hybrid war. *Life Is More Political*. 2025. No. 3, pp. 114-120.

20. Yakovenko Y. The importance of cybersecurity in shaping the digital economy. URL: https://www.researchgate.net/publication/383193213_Znacenna_kiberbezpeki_u_formuvanni_cifrovoi_ekonomiki (accessed 28 June 2026).

21. Bidzilya Yu. M. State policy of information security under conditions of hybrid threats. *Ukrainian Political and Legal Discourse*. 2025. No. 17, pp. 30-36. URL: <https://ppdnz.com.ua/index.php/home/article/view/457/356> (accessed 28 June 2026).

22. Tarasovsky Yu. Ukraine has approved the Digital Development Strategy to 2030. URL: <https://forbes.ua/news/ukraina-zatverdila-strategiyu-tsifrovogo-rozvitku-nnovatsiy-do-2030-roku-shcho-vona-peredbachae-14012025-26270> (accessed 28 June 2026).

23. Plakhotnik O., Zlatnikov V., Strazhnikova I., Bidyuk N., Shkodyn A., Kuchai O. Use of information technologies for quality training of future specialists. *Amazonia Investiga*. 2023. Vol. 12, No. 65, pp. 49-58.

24. Directive on the Security of Networks and Information Systems. URL: https://nis2.org.ua/?gad_source=1&gad_campaignid=23017071562&gbraid=0AAAA BBThWcdW CFXVbeUIPC10mJmbhR0zl&gclid=EAIaIQobChMI1dvk4NDv1AMV_5qDBx1opjD YEAAYASA AEgLBKfD_BwE (accessed 28 June 2026).

25. Rules of Enhanced Cybersecurity in the European Union. URL: <https://www.h-x.technology/ua/services/nis-2-cybersecurity-directive-ua> (accessed 28 June 2026).

26. Analysis of the Digital Transformation of Higher Education: The Digital Leap in East Asia. URL: <https://en.ichei.org/en/news/information/4033.html> (accessed 28 June 2026).

27. Network Detection and Response. URL: <https://oberigit.com/statti/shho-take-network-detection-and-response/> (accessed 28 June 2026).
28. All About Access Control: Everything Covered from Definition, Types, to Features and How-Tos. URL: <https://www.supremainc.com/en/hub/insights-access-control.asp> (accessed 28 June 2026).
29. UEBA (User and Entity Behavior Analytics) for when traditional cybersecurity can't protect your network. Northforge Innovations. URL: <https://gonorthforge.com/ueba/> (accessed 28 June 2026).
30. Digital Education Action Plan: Policy Background. URL: <https://education.ec.europa.eu/focus-topics/digital-education/actions/plan> (accessed 28 June 2026).
31. The EU NIS2 Directive: what it is, for what needs it was developed, and why Ukraine is implementing it. URL: <https://cip.gov.ua/ua/news/direktiva-yes-nis2-sho-ce-take-dlya-yakikh-potreb-rozroblena-ta-dlya-chogo-ukrayina-yiyi-implementuye> (accessed 28 June 2026).
32. International Standards and Guidelines: European Higher Education Area. URL: <https://naqa.gov.ua/2020/02/%D0%BC%D1%96%D0%B6%D0%BD%D0%B0%D1%80%D0%BE%D0%B4%D0%BD%D1%96-%D0%BE%D1%81%D0%B2%D1%96D1%82%D0%BDD1%96%D0%BF%D1%80%D0%B0%D0%BA%D1%82%D0%B8%D0%BA%D0%B8/> (accessed 28 June 2026).
33. Standards and Guidelines for Quality Assurance in the European Higher Education Area (ESG). URL: <https://ihed.org.ua/recommends/standarty-i-rekomendatsiyi-shhodo-zabezpechennya-yakosti-v-yevropejskomu-prostori-vyshhoyi-osvity-esg/> (accessed 28 June 2026).
34. ERA-UA. Roadmap for Ukraine's Integration into the European Research Area. URL: <https://mon.gov.ua/tag/era-ua> (accessed 28 June 2026).
35. A New European Research Area Platform Has Been Established. URL: <https://horizon-europe.org.ua/uk/news/info/stvoreno-novu-platformu-yevropejskogo-doslidnyczkogo-prostoru/> (accessed 28 June 2026).

36. Digital Education Action Plan 2021-2027. URL: <https://education.ec.europa.eu/focus-topics/digital-education/actions> (accessed 28 June 2026).

37. General Data Protection Regulation (GDPR). URL: <https://gdpr-text.com/uk/> (accessed 28 June 2026).

3.3. Mathematical model of expert data analysis in information and analytical systems

Zoriana NOVOSAD,

Olena TOICHKINA

Lviv University of Trade and Economics

In the context of the ongoing digital transformation of society, information and analytical systems are becoming increasingly important as tools for supporting managerial decision-making. Their effectiveness largely depends on the application of mathematical methods of data analysis capable of identifying hidden patterns, establishing relationships between the objects under study, and providing a scientifically grounded interpretation of the results. Such methods are particularly relevant when processing expert information, where traditional statistical analysis does not fully capture the structure of relationships among the factors under investigation. In this regard, a promising approach is to combine methods of expert evaluation, mathematical statistics, and graph theory to develop mathematical models suitable for use in information and analytical decision-support systems.

Under conditions of uncertainty, managerial decisions are based on analysis, forecasting, optimization, economic justification, and the selection of the best alternative when the available information is insufficient or incomplete. This creates a need for methodological guidelines on decision-making under information scarcity that can enhance the adaptability and stability of organizational systems. Effective managerial decision-making requires consideration of both internal and external factors, as well as the quantity and quality of the information available for analysis.