

https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=74859
(accessed: 03.08.2026).

63. CEN-CENELEC. Cyber Resilience Act: Standardization request officially accepted by CEN, CENELEC and ETSI. 2025. URL: <https://www.cencenelec.eu/news-events/news/2025/newsletter/ots-62-cra/> (accessed: 07.08.2026).

64. European Parliament and Council of the European Union. Regulation (EU) 2024/1689 of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). Official Journal of the European Union. 2024. L 2024/1689. URL: <https://eur-lex.europa.eu/eli/reg/2024/1689/oj> (accessed: 07.08.2026).

65. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection – Information security management systems – Requirements. Geneva : ISO, 2022.

66. ISO/IEC 27002:2022. Information security, cybersecurity and privacy protection – Information security controls. Geneva : ISO, 2022.

67. ISO/IEC 27033-1:2015. Information technology – Security techniques – Network security – Part 1: Overview and concepts. Geneva : ISO, 2015.

68. ISO/IEC 27035-1:2023. Information technology – Information security incident management – Part 1: Principles and process. Geneva : ISO, 2023.

69. IEC 62443-3-3:2013. Industrial communication networks – Network and system security – Part 3-3: System security requirements and security levels. Geneva : IEC, 2013.

70. IEC 62443-4-1:2018. Security for industrial automation and control systems – Part 4-1: Secure product development lifecycle requirements. Geneva : IEC, 2018.

71. IEC 62443-4-2:2019. Security for industrial automation and control systems – Part 4-2: Technical security requirements for IACS components. Geneva : IEC, 2019.

2.3. Strategy for Countering Hybrid Threats in the Digital Sphere: An Analysis of National and European Practices

Alla KAPITON,

National University

"Yuri Kondratyuk Poltava Polytechnic"

Tamara FRANCHUK,

Dmytro TYSHCHENKO,

Alona DESIATKO,

Rostyslav ZAKHAROV,

State University of Trade and Economics

In analyzing the regulatory experience of advanced democracies and the fundamental principles of the European strategy for developing artificial intelligence, contemporary researchers emphasize the need for a strict balance among three basic dimensions: technological and state autonomy in the digital sphere; market competition that drives innovation; and unconditional protection of human rights and freedoms against potential abuses of artificial intelligence (AI). In an era of hybrid confrontation, cybersecurity extends beyond the purely technical protection of computer systems. It has become a multilayered defense against coordinated hostile campaigns. Such aggressive actions combine several destructive elements: technical cyberattacks, information and psychological operations (IPOs), and digital espionage. Whereas technical cyberattacks seek to penetrate networks, block services, and destroy data, IPOs aim to spread disinformation on a large scale to manipulate public consciousness. Digital espionage, conducted to collect confidential data and intelligence, merits separate examination.

The principal objective of these coordinated strikes is not merely to disable individual computers but to achieve a broad geopolitical and social effect. Their primary aims are to paralyze critical infrastructure by disrupting energy systems, transport, the financial sector, and government communications; to destabilize the sociopolitical situation by sowing panic, chaos, distrust of public institutions, and internal conflict; and to steal data on a large scale, gaining access to state secrets, citizens' personal data, and strategic information for subsequent use in exerting pressure on the country.

A number of researchers focus above all on substantiating and developing an integrated model of state information security policy that systematically combines strategic communications, cyber defense measures, and mechanisms for strengthening societal resilience. Other studies seek to develop a comprehensive framework of indicators for verified monitoring and evaluation of the implementation of Ukraine's information strategy. Their many applied findings can directly inform the introduction and modernization of the country's legal framework in the security and digital spheres, optimize strategic communications at national and regional levels, and strengthen the

overall information and cyber resilience of public institutions. Introducing new tools and their modernized applications is now essential to identify, contain, and neutralize hostile disinformation campaigns under martial law.

Several scholars examine the implementation of state policy and its associated challenges, including the approved Strategy for the Digital Development of Innovation until 2030. They focus on building domestic innovation infrastructure as the foundation for modernization at enterprises (Tyshchenko D. et al., 2024; Franchuk T. et al., 2025; Kapiton A. et al., 2024; Bidzilia Yu. M., 2025; Melykh O., Korbust A., 2020). The current situation, systemic gaps, and practical difficulties faced by Ukrainian enterprises are also subjects of research that identifies the specific contribution of infrastructure components to the final outcomes of innovation activity (Kapiton A. et al., 2026; Geraskova O., Stechenko D., 2026). The technical aspects and specifics of protecting the information infrastructure of business entities are examined in joint research on this issue (Shestak Ya. et al., 2025; Pashkovskyi V. F., 2025). At the same time, a substantial body of academic literature shows rapidly growing interest in an integrated study of innovation's role in infrastructure development and sustainable industrial progress through the lens of the security transformation of digital space in leading European countries and elsewhere (Swire P. et al., 2024; Dede G. et al., 2024; Mahmood S. et al., 2024).

Despite the considerable volume of research, a set of theoretical and practical questions concerning information security remains insufficiently addressed. Most scholars consider the following gaps urgent: finding a consensus between the protection of state digital sovereignty and strict observance of fundamental human rights and freedoms; the methodological absence of unified, quantifiable metrics for assessing society's media resilience; and a coordination imbalance caused by the lack of effective cooperation between state institutions and civil society in repelling hybrid attacks. Current institutional and infrastructure deficiencies include uncoordinated interagency cooperation, inadequate methods for forecasting the risks of destructive information influence, and the vulnerability of digital networks under martial law.

Domestic and global processes considerably accelerate these threats: rapid digitization of public administration (e-government) creates new vulnerabilities to cyberattacks; the mediatization of social processes moves public and political life into social networks that are poorly controlled and easily manipulated by algorithms; and, in global information competition, the speed with which a narrative spreads often matters more than its truth. This makes an integrated information policy model necessary, capable of providing three levels of protection at once: technological protection (cybersecurity and infrastructure resilience); institutional protection (effective cooperation among public authorities, intelligence and security services, and civil society); and communicative protection (the state's ability to formulate clear, truthful, and persuasive narratives of its own).

The worldwide integration of information systems and internet resources into every sphere of life has made digital protection a basic and indispensable condition for society. The shift to remote work that accelerated after the pandemic opened new opportunities for sophisticated targeted cyberattacks, forcing private and public organizations to modernize their security perimeters urgently. The constant evolution of threats, evident in mass phishing campaigns and service disruption, causes enormous financial losses for multinational corporations. For Ukraine, meanwhile, the reliability of cyberspace has become a matter of national security: uninterrupted state operations now depend directly on digital integrity, readiness to repel network intrusions, and rapid data exchange between military and civilian agencies. These challenges are complex, manifesting in attacks on civilian and military sectors intended to paralyze government resources and management systems, and in pervasive disinformation spread through coordinated networks of fabricated content that distort reality.

Threats also include targeted IPOs designed to manipulate public sentiment and deliberately inflame domestic divisions, together with attacks on strategic communications intended to discredit Ukraine's official information sources and undermine trust in democratic institutions both domestically and among international partners. Although every industrial sector contributes significantly to favorable macroeconomic trends, solving problems in intellectual capital development, the

commercialization of scientific ideas, and the adoption of innovations based on scientific and technological progress must become a central direction of development. During this difficult period for the country, efforts should stimulate progressive scientific, technical, and technological changes in enterprises. This will directly increase the competitiveness of domestic products, optimize service processes, and improve the culture of consuming the outputs of production. More efficient use of natural resources, stronger state information security, stable national cybersecurity, and modernization of the entire system of strategic mechanisms serving national defense, quality of life, and economic development are also especially important.

In considering the emerging paradigm of digital security, it should be noted that the scientific and theoretical foundations of cyber and information security are undergoing fundamental change. The field is moving beyond a narrow technical or technocratic approach toward integrated, multidimensional models. In these new concepts, decisive determinants of protection are prudent state policy in the digital sphere, national digital sovereignty, and general societal resilience, which enables destructive hybrid influences to be distinguished and blocked effectively.

Cyber resilience as a foundation for technological progress is a separate issue for analysis. In this context, cyber resilience is understood as a basic, indispensable condition for safely deploying and scaling the Internet of Things (IoT) infrastructure that underpins modern smart systems. It also matters to the global goals of sustainable development and technological progress, since the stability of critical digital ecosystems directly affects society's economic, environmental, and social progress.

Another subject of scholarly debate is so-called "digital sovereignty," especially excessive localization of data within national borders, which creates a dilemma between data localization and cybersecurity vulnerability. Experts argue that rigid territorial data-storage requirements often have the opposite effect: they degrade cybersecurity. They artificially slow information exchange among international security institutions, introduce technical delays in urgent access to vital intelligence, and prevent cloud infrastructure from immediately mirroring and backing up data in safe jurisdictions during crises.

In this study, it is important to assess the risk of weakening human rights in global anti-crime agreements. Members of the academic community also express serious concern about trends in the drafting of new global conventions and agreements against cybercrime. There is a real risk that international human rights standards will be substantially lowered to expand the powers of law-enforcement agencies. The authors emphasize that overly vague language on cyber justice could enable authoritarian regimes to legitimize pervasive digital surveillance, censorship, and political persecution under the pretext of fighting crime.

Conceptualizing multidimensional threats in the "gray zone" and bringing these factors together enables researchers to analyze the nature of modern hybrid threats operating in an "invisible zone," below the threshold of open armed conflict (*jus ad bellum*). These influences are multidimensional because they combine legal pressure, cyberattacks, AI manipulation, and restrictions on access to information. This combination allows an aggressor to pursue strategic geopolitical objectives without directly escalating to conventional war.

The new paradigm of international relations is marked by a fundamental change in the nature of interstate conflict. Classical kinetic clashes and purely conventional methods of warfare increasingly give way to, or become integrated with, complex hybrid confrontations. In this changing structure of global rivalry, virtual and information spaces have become strategic theaters of operations in their own right. The information environment is no longer merely a channel for news but a principal instrument of modern warfare. It is used to gain political influence internationally and within opposing states, reshape public consciousness, alter citizens' values and identity, and undermine sovereignty from within, without necessarily first sending armored columns across a border. Research into the practical and theoretical results of implementing cybersecurity and information-protection tools under hybrid threats is therefore exceptionally relevant.

Ukraine currently faces persistent and growing existential challenges under aggression. Establishing an effective information security system is a matter not merely of national interest but of the state's physical and political survival. At the center of

full-scale armed aggression and daily information and psychological pressure, the country confronts an unprecedented range of threats.

The present configuration of these challenges is complex and includes:

- cyberattacks against civilian and military sectors, intended to paralyze government resources and control systems;
- pervasive disinformation through coordinated networks spreading falsehoods that distort reality;
- targeted IPOs that manipulate public attitudes and deliberately stir up internal contradictions and divisions;
- attacks on strategic communications that seek to discredit Ukraine's official information sources and undermine trust in democratic institutions at home and among international partners.

Outdated reactive methods cannot meet these challenges. They require a proactive, scientifically validated, long-term state strategy and a reconsideration of the security paradigm and new technological factors. Present realities demand moving beyond the narrow understanding of security as border protection alone. Information security is now a foundation of overall national resilience, a key element in protecting statehood, a principal factor in maintaining social cohesion, and an important component of Ukraine's standing as an international actor.

The pronounced disparity in countries' ability to adapt to globalization, caused by striking differences in financial, human, and cultural development, laid the groundwork for current international crises. Together these factors radically altered the structure of domestic economies and prompted national governments to delegate some powers to international organizations. The current interdependence of global systems and the recurring emergence of serious geopolitical, environmental, and financial disruptions make joint, coordinated action by the international community the only viable way to maintain overall balance.

Comprehensive scientific analysis of the strategic foundations of information security is crucial both for current defense and over the long term. Developing and applying new approaches to protecting the information space is a prerequisite for:

- successful postwar recovery, which will require a secure investment and digital environment;
- full Euro-Atlantic and European integration, in which Ukraine can contribute its unique practical experience in countering hybrid threats rather than simply seek assistance;
- building a resilient democratic system able to defend its freedoms and elections against future authoritarian interference from abroad.

A central direction is comprehensive protection of information and production networks by securing their external and internal perimeters and introducing safeguards for specialized services such as email and web access. Security rests on in-depth threat analysis, proactive endpoint protection, secure communication channels, and data loss prevention (DLP) systems. Organizational resilience is also developed through staff training, including cyber ranges for hands-on specialist exercises and cyber hygiene courses for all personnel (Yakovenko Y., 2026).

Implementing innovative projects requires reliable achievement of the intended positive results, which depends directly on a carefully developed long-term strategy. The central concepts should therefore be studied in their systemic interrelationships, using a creative and comprehensive approach to the life cycle of the entire structure, including design, deployment, and continuous operation. Information security has a special place in this architecture. The rapid diversification of ways to protect data against potentially destructive influences is now a priority for preserving the viability of an organization and its scientific, production, information, and technical clusters. Protection extends beyond maintaining network channels: the widespread use of distributed data processing, remote server capacity, and cloud resources demands a model of work in which operations involving confidential corporate information remain inaccessible to outsiders and potential attackers (Yakovenko Y., 2026; Tarasovsky Yu., 2026).

Distributed systems and cloud storage technologies, along with specialized protection systems for cloud information, require continuous, systematic updates. Effective prevention and response depend on an integrated cybersecurity system across

the entire ecosystem of scientific, production, information, and technical clusters. It must give equal attention to personal data and document workflows and to the processing and transmission of that data over communications channels. Regular modernization of specialized software, including antivirus solutions, cryptographic protocols, and SSL certificates, is especially relevant today, as is the use of specialized anonymization tools and anti-detection browsers to protect researchers' and developers' workstations.

Efficient operation of scientific, production, information, and technical clusters at the present stage depends on a comprehensive analysis of the factors shaping their emergence, design, practical operation, and subsequent strategic development. In examining the technical architecture that sustains the ecosystem of such technology sites, scholarly attention increasingly turns to optimizing data-protection systems and strengthening cybersecurity during operation of their digital infrastructure. Many researchers stress the necessity of a protected virtual environment and secure digital transformation as basic conditions for the resilience and integrity of the entire innovation ecosystem.

Understanding digital ecosystems as spaces where productive communities work, promising evidence-based solutions are generated, and entrepreneurial ideas take shape highlights the need for comprehensive security. A protected environment is a basic condition for specialists to work comfortably, channeling their potential into creative activity rather than purely technical troubleshooting, and developing creative ideas, startup projects, and other innovations. Once the technical requirements for uninterrupted digital infrastructure have been met, particular attention should be paid to risks arising from failures to observe digital security standards. Analyzing the most effective cybersecurity models, which ensure information resilience and the safety of data processing in a protected virtual environment, makes it possible to implement effective financial and organizational mechanisms of digital transformation based on prudent regulatory policy across industries.

Today, qualitative growth and effective socioeconomic mechanisms in any developed state are possible only through comprehensive, scientifically grounded

interaction among legal, organizational, economic, social, and other institutional instruments. Maintaining stable digital ecosystems and continuing economic progress are undeniable imperatives, made much more difficult by present geopolitical challenges. These circumstances intensify the need for a sound, balanced model for modernizing the national economy. Such a model calls for fundamental restructuring: a move away from an industrial focus on raw materials toward knowledge-intensive sectors based on intellectual potential, commercialization of new ideas, and greater innovation activity.

Given the specificity and diversity of current challenges and dangers, identifying which tasks require the most immediate action is difficult. Nevertheless, a comprehensive analysis of innovation and digital infrastructure clearly has both theoretical and applied significance, encompassing risk management, digital security, and information resilience. Reliable data protection becomes the central element and a fundamental basis for effective, stable business activity within a unified secure digital environment.

Particular attention should be paid to the difficulties businesses face in the contemporary Ukrainian market and to domestic legislation, which is continually changing and being updated. A deep understanding of citizens' current needs makes it possible to anticipate the demands and expectations of other key participants who support and strategically develop innovation. At the same time, distinguishing and identifying the particular characteristics of domestic digital ecosystems amid current political and economic disruption require focused scientific analysis, especially of the introduction of advanced digital solutions and the positive effects of digitization in general.

Another promising direction is attracting sufficient numbers of potential investors with modest initial capital who wish to become partners, coauthors, or cofounders of innovative companies. Such companies need no large initial investment and can rapidly begin implementing new developments. Modern corporations are directly introducing digitalization programs for workplace safety. Since 2024, several major initiatives have been launched to bring occupational safety to a new level. One

key digital innovation is the SafetyCulture (iAuditor) mobile platform, which enables safety audits, reporting, data analysis, and incident notifications from mobile devices (Digital security transformation, 2026).

The government's approved Strategy for the Digital Development of Innovation in Ukraine (WINWIN) through 2030 provides for comprehensive national financing and stimulation of innovation. This initiative will encompass all essential infrastructure components, with particular emphasis and priority funding for the leading and most promising fields explicitly defined in the strategy (WINWIN, 2026). The industrial and innovation sectors that form the foundation for new developments and the country's strategic progress under WINWIN are illustrated in Figure 2.4.

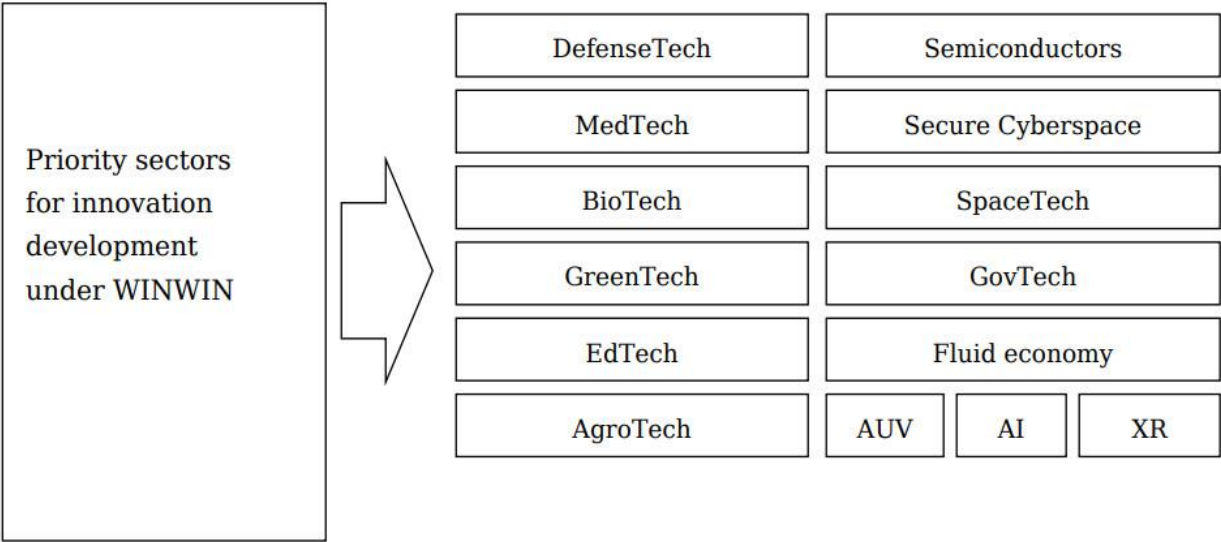


Figure 2.4. Priority sectors for innovation development under WINWIN

Given the way scientific, production, information, and technical clusters operate, particular attention should be paid to building a comprehensive cybersecurity system capable of mitigating threats to digital infrastructure. Because a creative cluster is closely integrated with cloud services, distributed data-processing systems, and Internet of Things (IoT) networks, the perimeter of this ecosystem must be protected at every level of operation.

The main task is to introduce proactive security models based on zero trust architecture. This entails continuous authentication of every user and device, whether they are on the enterprise premises or working remotely through distributed servers.

Particular attention should go to encrypting communication channels with modern cryptographic protocols, using secure VPN tunnels, and integrating data loss prevention (DLP) systems. These steps minimize the risk of unauthorized access to residents' intellectual property and startups' confidential data. The flexible ecosystem of scientific, production, information, and technical clusters also requires regular updates to specialized software, antivirus suites, and intrusion detection and prevention systems (IDS/IPS). Since structural components continually change and their relative importance shifts, security infrastructure must adapt dynamically to newly connected devices or robotics laboratories, which often become potential entry points for cyberattacks. Continuous network traffic monitoring and clear incident response procedures help preserve stable business processes in the digital ecosystem even under targeted hybrid or cyber pressure.

Analysis of digital ecosystems demonstrates the critical importance of data protection and cybersecurity for their digital infrastructure, directly influencing their future development strategies. Recent specialist studies confirm that regulation of information protection is increasingly relevant because technological facilities must remain cyber resilient during ongoing digital transformation. At the same time, funding security measures and assessing economic risks arising from global challenges and threats require strict oversight by both the state and prospective investors. Designing new security-management systems or modernizing existing ones is therefore essential, including improvements to cybersecurity protocols in line with the national strategy for developing the digital environment.

The European Union's information security framework has substantially expanded the powers of ENISA, authorizing it to introduce a common certification scheme for IT products. The agency is now responsible for developing protection standards and ensuring transparency through a public register of issued certificates. The entry into force of the NIS2 Directive marked another stage in digital security development, setting strict requirements for key economic sectors, with specific attention to postal operators and cryptographic data protection. At the same time, the

EU-CyCLONe network supports effective responses to systemic challenges across the EU through reliable notification of detected cyber incidents.

Worldwide dependence on information technology and the internet has made cybersecurity vital to modern society. The rapid expansion of remote work after the pandemic markedly increased the likelihood of sophisticated digital attacks, compelling organizations at every level to strengthen their defenses. The continual escalation of cyber threats, especially waves of phishing and DDoS attacks, inflicts enormous financial losses on global business.

Information security has recently assumed strategic importance for Ukraine. To develop steadily, the state must ensure digital resilience, effectively deter hostile online operations, and coordinate all defense bodies. Ukraine remains a major target for cyber aggressors. Threats range from blocked websites to data encrypted by ransomware, so protection must be comprehensive. Reliable antivirus software, cryptographic encryption, and regular staff training have accordingly become critical security measures in public and private institutions alike.

Expanding the network of modern digital ecosystems is a strategic priority of state policy, within which public infrastructure funding yields new jobs and attracts substantial private investment. Continuously updating a database of promising sites allows investors to evaluate locations in detail, considering logistical potential and fiscal preferences. This comprehensive approach stimulates capital inflows and encourages industrial modernization based on efficient resource use and circular production.

Modern innovation, technology, and industrial parks, along with digital ecosystems, are becoming hubs for leading domestic and international corporations and promising developers. Their physical and technical facilities combine attractive design with stringent building requirements; highly practical spaces are enhanced by advanced energy efficiency technologies and reliable digital protection. The USAID Critical Infrastructure Cybersecurity project provides specialized analytical products and cybersecurity services. Its work seeks to prevent the interception of confidential data, ensure anonymity and privacy during work, and introduce comprehensive

analysis and monitoring systems for detecting unlawful operations (Kapiton A. et al., 2026; Cybersecurity, 2026).

Ukraine is now at the center of a global confrontation in digital space, with one fifth of all cyberattacks worldwide directed against the country. Expert reports show how these threats have become more complex, ranging from attempts to block government resources to large-scale cyber extortion. Basic safeguards are no longer enough; an integrated security ecosystem with advanced encryption and a strong digital security culture among personnel is urgently needed.

An important practical step in public support for innovation was the opening of the Sikorsky Challenge Additive Technologies Science Park, demonstrating the successful transformation of universities into major centers of applied science. Its distinguishing feature is direct integration with the Prosthetics and Rehabilitation Center, creating a unified technology hub for biomedical engineering and comprehensive assistance to veterans. The park supports engineering startups, trains biomedical specialists, and provides inclusive education for former service members. Partnerships with IT market leaders, including appflame, EPAM, Genesis for Ukraine, and OBRIIO, enabled a modern 3D-printing laboratory for prosthetics, specialized 3D-modeling courses for veterans, and a fully accessible learning environment to help defenders adapt professionally. These initiatives offer innovative strategies in which advanced technology serves as an effective tool for rehabilitation and education. They support affected people and actively involve them in developing new technological solutions. Such scientific and digital ecosystems should exemplify how effective cooperation among state institutions, business, and society can overcome difficult social challenges (Science park of additive technologies, 2026).

The European Union's present model for protection against complex information threats centers on shared digital resilience and a harmonized legal framework for securing strategically important facilities against planned cyber intrusions. The updated NIS2 Directive occupies a central place: it has greatly expanded the number of regulated sectors and increased penalties for failure to comply with cybersecurity rules. ENISA's broader powers have enabled common standards for certifying software

and equipment throughout the EU, helping identify and block potentially unsafe IT solutions in government and business in advance. To contain major cross-border threats quickly, the EU-CyCLONe network reports digital attacks in real time and coordinates countermeasures among European authorities. This integrated approach reflects a qualitative shift in security architecture, from defending individual local networks to creating a broad secure perimeter capable of resisting cryptanalytic attempts, mass DDoS campaigns, and covert cyber sabotage (Directive on Network and Information Security; Enhanced Cybersecurity Rules in the European Union).

Uneven national readiness for globalization, rooted in deep differences in economic, demographic, and sociocultural capacity, has been a primary cause of current worldwide challenges. The combined effect of these factors profoundly transformed national economies and led governments to delegate some sovereign powers to supranational institutions. In the present circumstances, countries' close interdependence and recurrent large crises in security, the environment, and the economy make coordinated international action indispensable to overall stability.

New global challenges have deeply destabilized the national economy, directly causing impoverishment, a surge in unemployment, and deterioration of the domestic market. These adverse developments have pushed Ukraine out of global competitive markets and rapidly expanded the shadow economy. Such crises cannot be overcome effectively without fundamental modernization of the country's economic capacity. International experience indicates that only developed, financially stable systems can successfully capitalize on globalization while minimizing its associated risks. A crucial protective element is the deployment of real-time monitoring systems that immediately identify and neutralize anomalous network activity.

At the present stage of technological development, specialists are moving en masse to remote work through distributed systems. Virtual collaboration, however, has substantial drawbacks: no single integrated environment for resolving complex tasks and crises quickly; communication gaps; and less effective teamwork owing to the absence of a physical or high-quality virtual hub and fragmented project-management tools. The effort to overcome these problems drives developers to optimize the

workspace. New digital platforms aim not only to bring specialists together but also to create a protected ecosystem that encourages effective solutions. Under these conditions, secure data processing is a fundamental priority, guaranteeing confidentiality, information integrity, and strong resistance by distributed infrastructure to external cyber threats.

Ukraine is at the forefront of confrontation in the information sphere and faces intensive attacks by hacker groups. The wide variety of threats, from destructive DDoS attacks to systems blocked by malicious software, requires multilayered defense. Security in government and commerce therefore calls for advanced antivirus controls, robust information-encryption algorithms, and continuous improvement in employees' digital literacy. Particular attention should be given to challenges arising from force majeure, which require threat-prevention and proactive protection systems to be designed, implemented, and flexibly modified, with an emphasis on the safety of end users and their workstations.

In a globalized digital environment, secure communication channels and effective systems for preventing information leaks are prerequisites for the stable operation and development of diverse institutions. Because cyber threats change continually and demand an ongoing response, researchers should focus more closely on cyber hygiene through practical analysis of active attacks and their mechanisms. Stable operation and progress in high-technology industries require comprehensive improvement of their core components. In practice, this means a fundamental change in current approaches to designing and carrying out research initiatives as a priority of state policy.

The necessary institutional foundation is a favorable legal and regulatory environment with targeted incentives, a lighter tax burden, reduced overall financial pressure, and partial or full public financial support for innovative businesses. At the same time, dynamic infrastructure development requires regular updates and flexible modification of cybersecurity tools, especially within distributed systems, which are highly effective at these technology sites. Minimizing risks to corporate data and ensuring the resilience of information and production networks demand continuous,

multilayered protection of the network perimeter, including monitoring and filtering both external and internal traffic. Developing and integrating new ways to protect specialized services that sustain the complex architectures of modern enterprises is especially relevant. In light of the sharp growth in the number and scale of additional destructive influences during the current crisis, further research and practical work should examine vulnerabilities and strengthen the cybersecurity of the technical components of this innovation infrastructure.

REFERENCES FOR SUBSECTION 2.3

1. 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.
2. Franchuk T., Tyshchenko D., Desiatko A., Karpunin I. Features of accounting digitalization processes. *Galician Economic Journal*. 2025. Vol. 95, no. 1, pp. 61-66.
3. 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.
4. 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.
5. Bidzilia Yu. M. State information security policy under 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 June 20, 2026).
6. Melykh O., Korbut A. Entertainment media in the context of hybrid war in the post-Soviet countries: the case of Ukraine. *Economic Annals-XXI*. 2020. Vol. 182(3-4), pp. 25-33. URL: <http://ea21journal.world/index.php/ea-v182-03/> (accessed June 20, 2026).

7. Kapiton A., Franchuk T., Tyshchenko D., Desiatko A. Integration of cybersecurity into the infrastructure of innovation parks: conceptual and methodological foundations for creating a secure digital environment. *Khmelnitskyi Scientific Bulletin. Technical Sciences*. 2026. 363(2), pp. 386-390.

8. 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. *Tavria Scientific Bulletin. Technical Sciences Series*. 2026. Issue 3, pp. 79-85.

9. Geraskova O., Stechenko D. Economic efficiency of functioning of infrastructure for innovative activity in Ukraine. URL: <http://www.economy.nayka.com.ua/?op=1&z=3002> (accessed June 20, 2026).

10. 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-content/uploads/2025/12/Conference-Proceedings-December-18-19-2025.pdf> (accessed June 20, 2026).

11. Pashkovskyi V. F. Identification of political and legal mechanisms of state information security under hybrid warfare. *Political Life*. 2025. No. 3, pp. 114-120.

12. 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.

13. 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, 798.

14. 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, 106.

15. Digital security transformation: change that works. URL: <https://ohoronapraci.kiev.ua/article/news/cifrova-transformacia-bezpeki-zmini-aki-pracuut> (accessed June 20, 2026).
16. WINWIN. Global innovation strategy of Ukraine. URL: <https://winwin.gov.ua/> (accessed June 20, 2026).
17. Cybersecurity. URL: <https://amintegrator.com/cybersecurity/> (accessed June 20, 2026).
18. Yakovenko Y. The importance of cybersecurity in shaping the digital economy. URL: https://www.researchgate.net/publication/383193213_Znacenna_kiberbezpeki_u_for_muvanni_cifrovoi_ekonomiki (accessed June 20, 2026).
19. Tarasovsky Yu. Ukraine has approved the Strategy for the Digital Development of Innovation until 2030. URL: <https://forbes.ua/news/ukraina-zatverdila-strategiyu-tsifrovogo-rozvitku-innovatsiy-do-2030-roku-shcho-vona-peredbachae-14012025-26270> (accessed June 20, 2026).
20. Science park of additive technologies. URL: <https://www.amspace.com.ua/26270> (accessed June 20, 2026).
21. Directive on Network and Information Security. URL: https://nis2.org.ua/?gad_source=1&gad_campaignid=23017071562&gbraid=0AAAA-BBThWcdWCFXVbeUIPC10mJmbhR0zl&gclid=EAIaIQobChMI1dvk4NDv1AMV_5qDBx1opjDYEAAAYASAAEgLBKfD_BwE (accessed June 20, 2026).
22. Enhanced cybersecurity rules in the European Union. URL: <https://www.h-x.technology.ua/services/nis-2-cybersecurity-directive-ua> (accessed June 20, 2026).

2.4. Protection of Critical Information Infrastructure and Cyber Risk Management: European Practices and Opportunities for Implementation in Ukraine

Olena DVIRNA,

Serhii NABOKA

National University "Yuri Kondratyuk Poltava Polytechnic"