УДК 330.15

ECONOMIC SECURITY AND INFORMATION PROTECTION IN THE AGE OF DIGITALIZATION

A. A. Korzhenevskaya[1)], M. A. Romanyuk[2)]

[1)] *student, Belarusian National Technical University, Minsk, Belarus, utalot588@gmail.com*
[2)] *student, Belarusian National Technical University, Minsk, Belarus, masaromanuk17@gmail.com*

Supervisor **S. A. Slassi Moutabir**

senior lecturer, Belarusian National Technical University, Minsk, Belarus, slassie@bntu.by

This study analyzes the impact of digital transformation on economic security paradigms. The paper traces the evolution of threats from conventional to digital forms and provides a detailed classification of contemporary cyber risks. Significant attention is paid to systemic vulnerabilities inherent in critical information infrastructure. A multi-layered defense framework is introduced, integrating technological, organizational and legal dimensions, demonstrating how cybersecurity culture serves as a cornerstone for economic resilience.

Keywords: digital economy, economic stability, cyber risks, data protection, essential infrastructure, threat management.

ЭКОНОМИЧЕСКАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ В ЭПОХУ ЦИФРОВИЗАЦИИ

А. А. Корженевская[1)], М. А. Романюк[2)]

[1)] *студент, Белорусский национальный технический университет, г. Минск, Беларусь, utalot588@gmail.com*
[2)] *студент, Белорусский национальный технический университет, г. Минск, Беларусь, masaromanuk17@gmail.com*

Научный руководитель **С. А. Сласси Мутабир**

старший преподаватель, Белорусский национальный технический университет, г. Минск, Беларусь, slassie@bntu.by

В данном исследовании рассматривается, как цифровая трансформация меняет парадигмы экономической безопасности. В исследовании прослеживается переход угроз из традиционных форм в цифровые, и предлагается подробная классификация современных киберрисков. Особое внимание уделяется системным уязвимостям критически важной информационной инфраструктуры. В статье представлена многоуровневая система защиты, включающая технологические, организационные и правовые аспекты, демонстрирующая, как культура кибербезопасности служит краеугольным камнем экономической устойчивости.

Ключевые слова: цифровая экономика; экономическая стабильность; киберриски; защита данных; важнейшая инфраструктура; управление угрозами.

Current global economic development is undergoing a radical transformation driven by digitalization. This transformation affects every aspect of societal functioning, generating, on one

hand, significant opportunities for growth and innovation, and on the other, creating fundamentally new challenges to maintaining economic stability [1]. The significance of this investigation stems from the growing dependency on digital systems, which amplifies potential weaknesses across economic structures. As cyber threats become increasingly sophisticated and widespread, conventional security measures prove inadequate, necessitating fundamental reconsideration of protection methodologies [3].

The understanding of economic security has undergone substantial transformation. Previously centered on financial stability and resource independence, the concept now incorporates digital dimensions as fundamental components. Information has emerged as a vital economic resource, equivalent in importance to traditional production factors. This evolution demands that information protection transitions from technical implementation to strategic priority. A distinguishing feature of this new security landscape involves the potential for localized cyber incidents to trigger widespread economic consequences [4]. The 2021 Colonial Pipeline incident exemplifies this phenomenon, where a ransomware attack disrupted fuel distribution across multiple states, revealing how digital vulnerabilities can translate into tangible economic disruption.

Within economic security considerations, the human dimension warrants particular attention. Malicious actors frequently target organizational personnel because human behavior patterns often present more predictable entry points than complex technological systems. Rather than perceiving employees as security liabilities, progressive organizations integrate them as active participants in cyber defense mechanisms. This philosophical shift involves

deploying technical solutions that assume primary threat-filtering responsibilities, thereby reducing human exposure to initial attack vectors. When staff members encounter potential threats, they typically represent the minority that bypassed automated defenses, allowing for more focused and effective human intervention [1].

Contemporary security technologies substantially decrease dependence on human vigilance for basic protection. Implementing stratified defense mechanisms – including advanced firewall systems, intrusion detection platforms, and email filtering solutions – intercepts most cyber threats at technological levels. These automated systems handle routine threat identification without requiring employee involvement. Authentication methods eliminating password dependencies gain particular relevance by simultaneously enhancing user experience and mitigating credential-based vulnerabilities. Sandbox environments and network monitoring tools provide early threat identification, reserving human analysis for complex scenarios requiring nuanced judgment [5]. Artificial intelligence applications continue to mature in cybersecurity contexts. While sometimes subject to promotional exaggeration, AI's practical utility grows increasingly evident, especially in countering AI-enabled threats. Generative AI systems can help identify sophisticated phishing attempts that closely mimic legitimate communications, creating dynamic defense capabilities [3].

Constructing effective security infrastructure requires balanced investment between technological solutions and human capital development. Each organization must conduct individualized risk assessments to determine appropriate resource distribution. Generally, prioritizing technologies that automate threat detection and reduce ambiguous security events allows security operations centers to focus on critical analysis. Developing IT environments that support rather than hinder employee productivity remains crucial. User centered security implementations foster positive engagement with protective measures, reducing resistance and complacency that often undermine security protocols [4].

Technological measures achieve maximum effectiveness when complemented by cultural transformation. Fostering "digital intuition" among workforce members enables recognition of sophisticated threats that evade technical filters. Ongoing education programs become essential when even advanced security systems cannot guarantee complete protection. Establishing organizational environments where cybersecurity represents shared responsibility rather than IT department exclusivity yields significant benefits. This cultural approach transforms potential vulnerabilities into collaborative defense networks where every participant contributes to protective efforts [2].

Digital economic transformation necessitates reconceptualizing traditional security approaches. Information protection evolves from technical consideration to strategic imperative, requiring integrated solutions that address both technological and human dimensions. Balanced investment strategies that neutralize routine threats through automation while preparing personnel for sophisticated attacks create resilient security postures. Ultimately, cybersecurity expenditure represents not merely cost but essential investment in sustainable digital-age development. The interconnected nature of modern economies means that effective security protocols contribute to broader economic stability, making cybersecurity integral to national economic health rather than just organizational concern [5].

References

1. National Institute of Standards and Technology. Cybersecurity Framework 2023 : сайт. URL: https://www.nist.gov/cyberframework (дата обращения: 26.09.2025).
2. European Union Agency for Cybersecurity. ENISA Threat Landscape 2023 : сайт. URL: https://www.enisa.europa.eu/publications/enisa-threatlan dscape-2023 (дата обращения: 26.09.2025).
3. Международный стандарт ISO/IEC 27001:2022 "Информационная безопасность, кибербезопасность и защита конфиденциальности" 2022 : сайт. URL: https://www.iso.org/standard/72096.html (дата обращения: 26.09.2025).
4. *Петров А. В.* Кибербезопасность в цифровой экономике. М. : ИНФРА-М, 2023. 245 с.
5. Proceedings of the International Conference on Digital Economy and Security 2024 : сайт. URL: https://doi.org/10.1000/xyz123 (дата обращения: 26.09.2025).