

# **ENTREPRENEURSHIP, TRADE AND EXCHANGE ACTIVITIES**

**Yevhenii Ippolitov, Postgraduate Student**  
*National Technical University “Kharkiv Polytechnic Institute”*  
*Kharkiv, Ukraine*

DOI: <https://doi.org/10.30525/978-9934-26-698-0-31>

## **INFORMATION SECURITY AS A STRATEGIC RESOURCE FOR INNOVATIVE BUSINESS DEVELOPMENT IN THE CONTEXT OF GLOBAL CHANGE**

The contemporary stage of global economic development is characterized by the active digitalization of business processes, the proliferation of artificial intelligence technologies, big data analytics, cloud services, and digital platforms.

These processes generate new opportunities for the innovative development of entrepreneurship while simultaneously increasing the dependence of economic actors on information resources and digital infrastructure. Under such conditions, information security is becoming one of the key determinants of enterprise competitiveness, resilience, and innovative capacity, extending well beyond the technical protection of data to become an integral component of strategic enterprise governance. Cybersecurity is increasingly conceptualized as a factor in business value creation, innovation support, and the assurance of long-term development.

The effective utilization of information technologies enables enterprises to enhance productivity, optimize managerial processes, develop new business models, and adapt rapidly to changes in the external environment. At the same time, digital transformation is accompanied by the emergence of new risks associated with the protection of information assets. The problem of information security assumes particular significance in the context of global change, characterized by elevated uncertainty, intensifying geopolitical tension, and the rapid diffusion of innovations, conditions under which information security functions not merely as a risk mitigation instrument, but as a strategic resource determining an

enterprise's capacity for innovative development and the formation of sustainable competitive advantages.

The issues of information security and cyber resilience of enterprises have been actively addressed in contemporary scholarly literature. Topalov V. substantiates the strategic orientations for the formation and development of information security systems for small business entities in the context of digital transformation and escalating cyber threats [1]. Dudykevych V., Mykytyn H., Bortnyk L., and Stosyk T. emphasize the necessity of integrating information security mechanisms into the digital infrastructure of organizations and examine the security of cyber-physical systems as the foundation for the development of intellectualized business environments [2]. Research into information security within the context of innovative business model development in the digital economy demonstrates that the growing digitalization of business processes amplifies the risks of data breaches and cyber threats, rendering information security critically important for enterprises [3]. Furthermore, Shaposhnykov K. and Zhavoronok A. propose the development of a synergy model for information security and innovative entrepreneurial recovery at the regional level as an instrument for addressing global challenges. The objective of this study is to substantiate the role of information security as a strategic resource for the innovative development of entrepreneurship under conditions of global change.

The innovative development of contemporary entrepreneurship is substantially contingent upon the effective utilization of information resources. Information has become a critical intangible asset that ensures enterprise competitiveness, facilitates managerial decision-making, and underpins the formation of innovative products and services. The digitalization of business processes, in turn, opens new avenues for entrepreneurial development. The adoption of cloud technologies, e-commerce systems, artificial intelligence, and big data analytics enables enterprises to enhance operational efficiency, reduce costs, and expand market reach. However, the vulnerability of information systems to both external and internal threats is simultaneously increasing. Under contemporary conditions, information security fulfills several strategically important functions: ensuring the protection of the enterprise's information assets; maintaining the continuity of business processes; and facilitating the advancement of innovative activity. Since innovative solutions are grounded in knowledge, data, and intellectual capital, the effective protection of information resources creates the preconditions for the

adoption of new technologies, the development of digital platforms, and the formation of innovative business models.

The problem of building enterprise cyber resilience is of particular relevance. Cyber resilience implies not only the capacity to withstand threats, but also the ability to rapidly restore operational functionality following incidents and to adapt to new challenges. Consequently, contemporary information security management concepts are oriented toward the integration of security mechanisms into strategic planning and corporate governance frameworks.

As innovative entrepreneurial development is accompanied by the active adoption of digital technologies, the automation of business processes, and the processing of large volumes of data, it simultaneously gives rise to new threats to information security. The principal challenges are presented in Table 1.

Table 1

**Principal challenges of information security in the context of innovative business development**

| <b>Challenge</b>                                                | <b>Characterization</b>                                                                                                | <b>Potential Consequences for the Enterprise</b>                       |
|-----------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------|
| 1                                                               | 2                                                                                                                      | 3                                                                      |
| Growing scale and complexity of cyber threats                   | Proliferation of cyberattacks, malicious software, phishing, DDoS attacks, and other forms of cybercrime               | Data loss, financial damage, disruption of business processes          |
| Protection of intellectual property and innovative developments | Necessity of safeguarding trade secrets, patents, know-how, and the results of innovative activity                     | Loss of competitive advantages, decline in enterprise market value     |
| Security of big data and artificial intelligence                | Processing of large volumes of information and the use of AI algorithms impose heightened data protection requirements | Leakage of confidential information, distortion of analytical outcomes |
| Vulnerability of cloud technologies and digital platforms       | The use of cloud services and platform-based solutions creates additional risks of unauthorized access                 | Compromise of information integrity and availability                   |
| Human factor                                                    | Insufficient levels of digital literacy, personnel mistakes                                                            | Increased frequency of information security incidents                  |
| Security of remote and hybrid work                              | The use of remote access and mobile devices expands the range of potential threats                                     | Unauthorized access to corporate resources                             |

| 1                                                                   | 2                                                                                          | 3                                                                                |
|---------------------------------------------------------------------|--------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------|
| Integration of security into digital transformation                 | Necessity of concurrently implementing innovations and corresponding protective mechanisms | Formation of new vulnerabilities in digital infrastructure                       |
| Compliance with international standards and regulatory requirements | Need to adhere to information security standards and personal data protection regulations  | Financial penalties, reputational losses, restricted market access               |
| Ensuring enterprise cyber resilience                                | Necessity of rapid response to cyber incidents and restoration of operations               | Prolonged downtime, erosion of client and partner trust                          |
| Rising costs of information security                                | Need to invest in advanced protective technologies, software, and personnel training       | Increased operational costs, particularly for small and medium-sized enterprises |

*Source: compiled and supplemented by the author based on [3]*

Accordingly, the key challenge confronting contemporary entrepreneurship is achieving a balance between the introduction of innovations and the maintenance of an adequate level of information security. The ability of an enterprise to effectively manage information risks is, to a considerable extent, determinative of its innovative development success and competitiveness within the digital economy. Under conditions of global change, a risk-oriented approach to information security management assumes particular significance. Its implementation encompasses the identification of potential threats, assessment of their likelihood, analysis of possible consequences, and the development of risk mitigation measures. This approach facilitates the rational allocation of enterprise resources and enhances the effectiveness of information protection systems.

Thus, information security has indisputably ceased to be an exclusively technical function and is, evidently, being transformed into a pivotal element of strategic enterprise management. Its role, as has been demonstrated, lies not only in the protection of information resources, but also, and perhaps more significantly, in creating the conditions for sustainable innovative development, enhancing investment attractiveness, and reinforcing the competitive positioning of business.

In the context of global change and the digital transformation of the economy, information security, therefore, acquires the status of a strategic resource for entrepreneurial development. Notably, it ensures the

protection of information assets, sustains the continuity of business processes, and, equally importantly, cultivates trust among clients and partners. Consequently, it establishes the essential preconditions for the successful implementation of innovations and, ultimately, for the long-term resilience and growth of the enterprise in an increasingly complex and volatile global environment.

### References:

1. Topalov V. (2025) Stratehichni oriientyry zabezpechennia informatsiinoi bezpeky subiektiv maloho pidpriemnytstva [Strategic guidelines for ensuring information security of small business entities]. *Ekonomika ta suspilstvo*, no. 75. DOI: <https://doi.org/10.32782/2524-0072/2025-75-92>.
2. Dudykevych V. B., Mykityn H. V., Bortnik L. L., Stosyk T. (2024) Metodolohiia bezpeky kiberfizychnykh system ta internetu rechei v intelektualizatsii obiektiv infrastruktury [Security methodology of cyber-physical systems and the Internet of Things in the intellectualization of infrastructure facilities]. *Kiberbezpeka: osvita, nauka, tekhnika*, vol. 6, no. 1, pp. 44–53. DOI: <https://doi.org/10.23939/csn2024.01.044>.
3. Shostak L., Pomazun O. (2024) Informatsiina bezpeka v konteksti innovatsiinoho rozvytku biznes-modeli vitchyznianykh pidpriemstv v umovakh tsyfrovoy ekonomiky [Information security in the context of innovative development of business models of domestic enterprises in the digital economy]. *Tsyfrova ekonomika ta ekonomichna bezpeka*, no. 5 (14), pp. 160–165. DOI: <https://doi.org/10.32782/dees.14-25>.
4. Shaposhnykov K., Zhavoronok A. (2026) Synerhiia informatsiinoi bezpeky ta innovatsiinoho vidnovlennia pidpriemnytsoi diialnosti v rehioni v umovakh hlobalnykh vyklykiv [Synergy of information security and innovative recovery of entrepreneurial activity in the region under global challenges]. *Ekonomika ta suspilstvo*, no. 84. DOI: <https://doi.org/10.32782/2524-0072/2026-84-202>.