

Prospects for ensuring information security of business entities as a vector of their sustainable development

*Topalov Volodymyr*¹

Received: 2025-06-12

Accepted: 2025-07-08

DOI: <https://doi.org/10.5281/zenodo.18703697>

Abstract. The purpose of the study is to assess the current state and identify future prospects for ensuring information security among small business entities in the context of ongoing digital transformation. In the contemporary economy, where digitalization processes are accelerating across all sectors, information security (IS) has become a critical component of business continuity and competitiveness. Small enterprises, despite being highly vulnerable to cyber threats, often lack the financial, technical, and human resources to implement comprehensive cybersecurity systems.

The study applies a quantitative research methodology based on a structured questionnaire survey of small enterprises operating in the Volyn region of Ukraine. A regression model was developed to examine the relationship between IS spending and financial performance indicators of the surveyed enterprises.

Results. The findings revealed that the majority of small enterprises exhibit either a low or intermediate level of information security. Key weaknesses include insufficient investment in cybersecurity infrastructure, limited implementation of preventive measures, and the absence of dedicated staff or external experts responsible for IS. Despite this, enterprises that invest more consistently in IS measures tend to demonstrate higher revenue levels, indicating a positive and statistically significant correlation.

Practical implications. The study proposes an adaptive model of IS strategy for small businesses, which includes typological classification based on current IS levels and tailored strategic recommendations. This model provides practical tools for decision-makers and can serve as a foundation for both enterprise-level planning and the development of regional or national support programs.

Value / originality. The scientific novelty of this research lies in the formalization of the link between information security maturity and financial performance in the small business segment, along with the development of a typology of enterprises by IS level. This contributes to the broader understanding of cybersecurity management within small enterprises under digital transformation pressures.

Keywords: information security, business digitalization, business entities, digital transformation, security strategy.

¹ Lutsk National Technical University,
Ukraine
postgraduate,
topalovvol1999@gmail.com
ORCID: <https://orcid.org/0009-0006-1745-3171>

Introduction

Under the current conditions of rapid digitalization of business processes, intensifying cyber threats, and the growing importance of information resources, ensuring information security has become a top priority for the sustainable development of business entities (Kuzomko V., 2021). Information has transformed into one of the key strategic assets that directly influences the competitiveness, reputation, financial stability, and viability of business structures. In this context, the need for a systematic approach to assessing the state of information security and developing effective mechanisms for its assurance is particularly pressing (Kitsiuk V. & Pupynin O., 2024). However, effective information security management requires not only technical solutions but also methodologically grounded approaches to its study. In particular, it is necessary to take into account the specific characteristics of business entities in terms of their scale, industry-specific features, and level of digital maturity, which calls for flexible and adaptive analytical methods (Shostak L. & Pomazun O., 2024). Within this context, it is essential to identify current information security threats and evaluate the prospects and directions for improving security systems, considering global trends, state policy, regulatory requirements, and the institutional capacities of the business entities themselves.

Information security is a subject of considerable academic interest. In the context of economic analysis, particular attention should be given to studies that assess the interrelationship between economic and information security within enterprises based on an analysis of business strategies (Bilko S., 2022; Kitsiuk V. & Pupynin O., 2024). Research in the field of the digital economy has defined methodological foundations for ensuring information security at the regional level (Dubnytskyi V. & Naumenko N., 2019). Furthermore, studies by Kraus K. et al. (2022) and Melnychuk H. & Mamaliga V. (2020) explore the specific features of cybersecurity's digital transformation under martial law. Research conducted by Kovalska L. et al. (2023) reveals the economic essence of information security across various regions of Ukraine.

In academic publications by Kuzomko V. (2021), Leonenko N. & Postupna O. (2022), Savras I. & Fedynets N. (2023), and Sytnyk N. & Sebestianovych I. (2022), the impact of digitalization on enterprise information security is examined. Additionally, Naumenko N. (2019) and Frolova L. & Boiko I. (2021) have systematized approaches to ensuring information security in their research. Studies by Shostak L. & Pomazun O. (2024) focus on the link between data protection and innovative business models. Yakovenko Ya. et al. (2024) and Klymchuk M. (2022) analyze the strategic directions of digital transformation among Ukrainian business entities.

Thus, the review of research on the process of ensuring information security for business entities highlights the high relevance of this issue, as well as the necessity of identifying strategic directions for the development of information security within entrepreneurship.

Results

Analysis of the Level of Business Digitalization in EU Countries and Ukraine

An analysis of the level of digitalization among small and medium-sized enterprises (SMEs) in EU countries reveals significant interregional disparities in the adoption of digital technologies. A high share of enterprises with very advanced levels of digitalization is typical of economically developed countries in Northern and Western Europe, while states in Central, Southern, and Eastern Europe are predominantly represented in the categories of low or very low digital activity. This indicates a pressing need to strengthen digital policy at both the EU and national levels, aimed at addressing digital inequality, expanding access to modern technologies, and fostering digital competencies within SMEs (Naumenko N., 2019). The

digital transformation of SMEs is a key factor in enhancing their resilience and competitiveness, and it represents a critical element of sustainable economic growth within the context of a new industrial reality (Melnychuk H. & Mamaliga V., 2020).

The implementation of new digital regulatory mechanisms – particularly the Digital Markets Act and the Digital Services Act – demonstrates the EU's systematic approach to shaping a secure, fair, transparent, and sustainable digital space (Sytnyk N. & Sebestianovych I., 2022). These legal instruments establish clear rules for business operations, protect user rights, and contribute to increased accountability in the digital economy. For Ukraine, which aspires to integrate into the EU digital space, the study and adaptation of such approaches represent strategically important steps toward developing its own digital economy, improving legislation, and safeguarding societal interests in the context of ongoing digital transformation.

Determinants of the Development of Small Business Entities in Ukraine

Information security is a strategic prerequisite for the sustainable development of small business entities. Threats such as cyberattacks, the leakage of commercially sensitive information, phishing, and IT-related fraud can have catastrophic consequences for small enterprises, which typically possess limited resources to establish comprehensive protection systems. This underscores the need to investigate the determinants that stimulate entrepreneurial development and contribute to enhancing their level of information security (Bilko S., 2022).

An analysis of the structural indicators of business entities confirms the vital role of small enterprises in ensuring economic stability and development. Despite differing economic conditions, both economies exhibit a high share of small and medium-sized enterprises (SMEs) in the overall business structure, emphasizing their system-forming importance (Leonenko N. & Postupna O., 2022). In the context of digital transformation and global challenges – including the ongoing war in Ukraine – SMEs remain flexible and adaptive actors capable of maintaining resilience and ensuring a positive contribution to GDP growth. This highlights the necessity for continued state support, investment in digital infrastructure, and the creation of a favorable business environment to foster the sustainable development of small businesses.

Survey methodology

To assess the level of information security among small business entities, the study employed a structured approach incorporating a quantitative method – a survey based on a specially designed questionnaire (Klymchuk M., 2022). The questionnaire covered a range of areas, including: information security (IS) funding levels, the presence of policies and procedures, staffing, the use of technical security tools, audit frequency, employee digital awareness, incident management, data backup practices, encryption usage, supplier interactions, and readiness to invest in information security measures.

A statistically average sample was formed using the method of repeated random selection, which ensured the representativeness of the data within the target population of small enterprises. To ensure the accuracy of the study and determine the appropriate sample size, it was necessary to clearly understand the scope of the general population. According to the Main Department of Statistics in Volyn Oblast, as of the end of 2023, approximately 4,800 small business entities were operating in the region.

The sample structure reflects its representativeness, as the respondents were exclusively small business entities. The sample included enterprises in Volyn Oblast engaged in manufacturing, trade, and services. The participating businesses represented a diversity of business models and levels of digital maturity. The inclusion of such criteria supports the

conclusion that the study is representative within the category of small, production-oriented enterprises in Volyn.

A total of 100 questionnaires were distributed, and 20 enterprises provided complete responses, resulting in a response rate of 20%. This is consistent with the average response rate for business-sector surveys, particularly in contexts involving limited company access, time constraints among respondents, and low motivation to participate in research. This response level is considered acceptable, as it exceeds the commonly accepted threshold of 4,0%.

A comparison between the sample and the general population revealed similar distributions and characteristics, with the business entities in the sample corresponding closely to the overall structure of small enterprises in Volyn Oblast. A comparative analysis of the socio-economic characteristics of the respondents – using data from the State Statistics Service of Ukraine, open sources such as “Diia.Business,” and the “kompas.ua” platform – confirmed the sample’s alignment with the main parameters of the general population, particularly in terms of economic activity types and employee numbers.

The representativeness of the sample is further substantiated through the use of a confidence interval, which reflects the degree to which the findings can be generalized to the entire population of small businesses in Volyn Oblast (Dubnytskyi V. & Naumenko N., 2019). In other words, the confidence interval defines the range within which the true value for the broader population of small business enterprises is likely to be found with a high degree of certainty.

Findings

The survey results indicate that despite a growing awareness of the importance of information security, the majority of small business entities are only willing to increase their investments in IS to a limited extent, primarily focusing on the minimum necessary expenditures. This trend highlights the need to develop accessible, economically justified protection models, as well as to introduce incentive mechanisms from both the state and professional associations. In the long term, only a systematic approach to investing in information security can ensure the resilience of small businesses amid growing threats (Kraus K. et al., 2022).

When constructing the correlation between the revenue volumes of the surveyed small enterprises and their expenditures on information security, a linear relationship was identified (Figure 1).

The graphical representation of the correlation between expenditures on information security and the annual revenues of small business entities illustrates a positive relationship between the volume of investments in cybersecurity measures and the financial performance of enterprises. Specifically, the constructed regression model demonstrates that as spending on information security increases, annual revenues also rise, indicating the effectiveness of such investments. This correlation supports the assumption regarding the strategic role of information security in enhancing the competitiveness of small businesses in the context of digital transformation and external environmental threats.

The resulting regression equation is:

$$Y=640,25+49,80X$$

The equation reflects a linear relationship between expenditures on information security (X) and enterprise revenues (Y). It indicates that in the absence of any investment in information security (X = 0), the projected income of a small business would be approximately UAH 640,25 thousand. Moreover, each additional thousand hryvnias invested in information

security potentially increases annual revenue by UAH 49,8 thousand, which demonstrates a high sensitivity of profits to the level of digital protection.

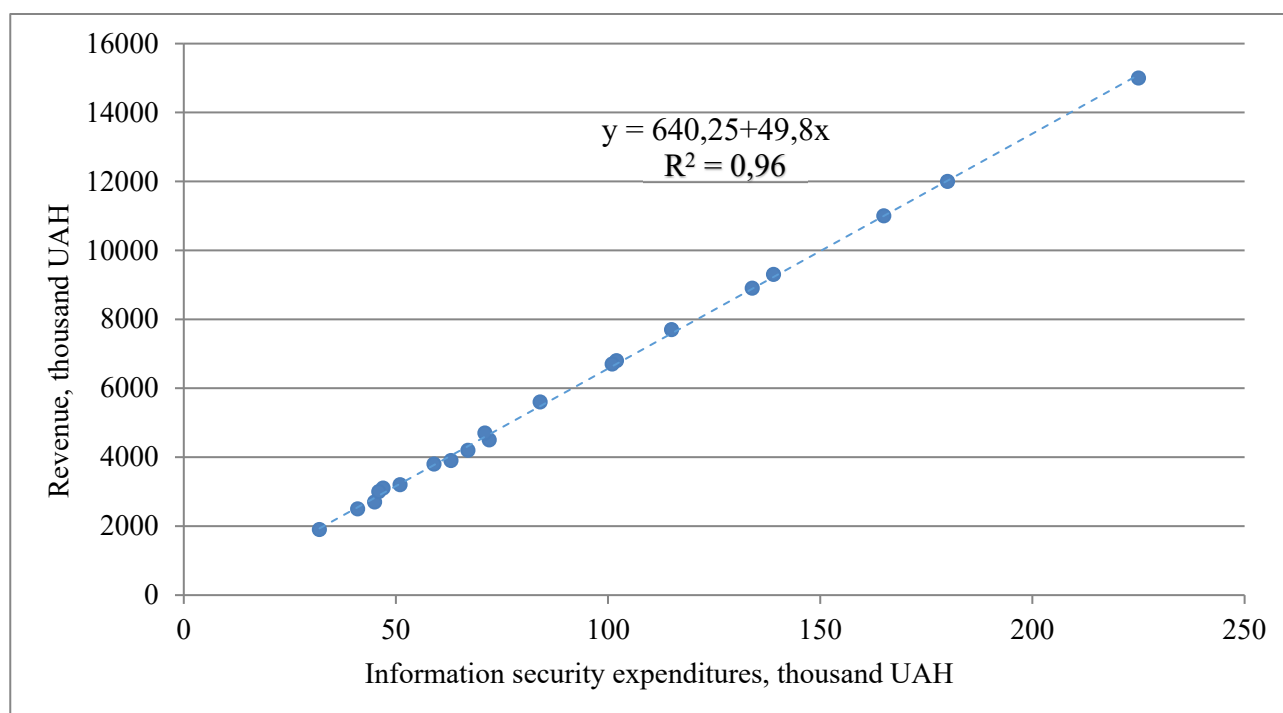


Figure 1. Correlation between the revenue volumes of the surveyed small business entities and their expenditures on information security.

Source: compiled by the author

The model's coefficients have clear economic interpretations: the constant reflects the baseline income level without any investment in information security, while the slope of the regression line represents the average effect of investing in cybersecurity. Constructing such a model makes it possible to formalize the relationship between indicators and serves as a tool for justifying strategic management decisions regarding the appropriate level of funding for cybersecurity measures in small businesses. The findings indicate the necessity of prioritizing information security as a key area of investment, capable of enhancing the economic performance of small business entities in an environment of growing cyber risks.

It is worth noting that the model's reliability coefficient (Pearson's R^2) is 0,96, which means the dependency is both strong and statistically significant. Approximately 96% of the variation in income can be explained by changes in information security expenditures. Thus, the graphical representation confirms a strong positive correlation, reflecting a very close relationship between the variables.

The analysis also revealed that most small business entities lack cybersecurity specialists, rely on standard software, and do not implement formalized security policies. This situation creates risks not only for the enterprises themselves but also for their consumers and partners, making information security a systemic issue (Kovalska L. et al., 2023). Therefore, small business entities should adopt flexible, adaptive, and phased security strategies that account for their current level of protection. The absence of a systematic approach to information security leads to the accumulation of risks, loss of commercial information, and diminished competitiveness (Savras I. & Fedynets N., 2023).

In light of this, it is relevant to classify enterprises by their levels of information security and undertake appropriate strategic planning. This allows for the rational allocation of resources, increased resilience to cyber threats, and a gradual transition toward mature IS management models (Yakovenko Ya. et al., 2024). Based on the conducted study, small

business entities are advised to apply tailored information security strategies according to their assessed protection levels: low, medium, sufficient, and high. The systematized characteristics of each level, recommended strategies, and key management actions are presented in Table 1.

Table 1

Information Security Strategies for Small Business Entities Depending on Their Current Level of Information Security

Current IS Level	Description of IS Status	Recommended Strategy	Recommended Actions
Low	Lack of a systematic approach to IS development, low staff awareness, high risks	Basic Protection Strategy	Installation of basic antivirus, employee training, regular backups
Medium	Some protective measures in place, fragmented IS policies, insufficient technical control	IS System Formation Strategy	Development of security policy, audit of existing tools, vulnerability mitigation
Sufficient	Formalized security policies, regular software updates, partial monitoring	Optimization and Control Strategy	Implementation of monitoring systems, periodic security testing, access rights segmentation
High	Fully developed IS management system, audits, IS integrated into business processes	Integration and Development Strategy	Automation of security procedures, external audits, investments in cyber resilience

Source: compiled by the author

The analysis of information security management processes in small business entities highlights the importance of considering the specific resource, organizational, and personnel capacities of the enterprises under study. Therefore, selecting an appropriate information security strategy should be based on the current level of protection, with approaches adapted to the realities of small business operations (Frolova L. & Boiko I., 2021).

Small business entities with a low level of information security are characterized by the complete absence of a systematic approach, low employee awareness, lack of even basic technical safeguards (such as antivirus software or firewalls), and high risks of data leakage or loss. In such cases, a basic protection strategy is recommended, with the primary goal of promptly mitigating critical threats. Key actions include implementing the minimum necessary protective software, organizing data backups, and increasing employee awareness through brief training sessions or safety briefings.

Enterprises with a medium level of information security typically demonstrate fragmented implementation of security measures. Some tools may already be in place (e.g., limited access control or antivirus use), but the overall security policy lacks systematization, and the risks remain significant. For this level, a security system development strategy is appropriate. It involves conducting an internal or external audit of the current state, developing a formal information security policy, addressing identified vulnerabilities, and improving the technical literacy of employees.

A sufficient level of information security indicates that the enterprise has an established security policy, regularly updates software, performs data backups, and controls access to resources. However, the degree of automation and monitoring is still limited. In this case, it is advisable to implement an optimization and control strategy aimed at regularly analyzing the

effectiveness of existing solutions, applying activity monitoring systems (e.g., event logging), and segmenting access to critical data based on the principle of least privilege.

A high level of information security implies that the enterprise has a well-established IS system that complies with national or international standards (e.g., ISO/IEC 27001), conducts regular audits, and integrates information security processes into its overall business strategy. Under these conditions, the most effective approach is the integration and development strategy, which focuses on refining existing solutions, automating processes, implementing cyber-resilient practices, and involving external experts or participating in industry cybersecurity initiatives.

Thus, the step-by-step progression from basic protection to strategic information security management represents a realistic pathway for small businesses. It ensures compliance with regulatory requirements and enhances competitiveness through the reliable protection of informational assets.

Conclusions

The assessment of the information security level among small business entities revealed significant differentiation in protection status depending on the level of IS expenditures, technical capabilities, the presence of security policies, and employee awareness. The study confirmed that the majority of small enterprises operate at an initial or medium level of information security, indicating high vulnerability risks to contemporary cyber threats. Particularly critical are the issues of insufficient regulation of security processes, irregular personnel training, limited funding, and restricted application of protective technologies.

The evaluation results underscore the need for targeted measures of state, regional, and sectoral support to enhance information security in small business. Implementing risk assessment mechanisms, establishing monitoring systems and IS indicators, and fostering an information security culture through training and improving employees' digital literacy are especially relevant. These findings can serve as a foundation for developing institutional support and strategic decision-making in the cybersecurity domain for small businesses.

Strategic planning for information security in small business entities should be based on adaptability, risk orientation, and the economic feasibility of the implemented measures. Defining and implementing strategic directions will contribute to building a resilient protection system, increasing trust from partners and consumers, and ensuring the competitiveness of small businesses amid the digital transformation of the economy.

It has been determined that strategic priorities must be grounded in systematic risk analysis, threat ranking, investment prioritization, and the creation of conditions for continuous staff training. A key prerequisite for the successful implementation of the strategy is the harmonious integration of technical, organizational, and behavioral development vectors, ensuring the integrity and reliability of the information security system. Special attention should be paid to supporting digital literacy, adopting IS standards (notably ISO/IEC 27001), and creating mechanisms for adapting small enterprises to the rapidly evolving information environment.

References

1. Bilko, S. (2022). Information and Economic Security: Assessment of Level and Interconnection. *Scientific Bulletin of Polissya*, № 1 (24), 58-77. DOI: [https://doi.org/10.25140/2410-9576-2022-1\(24\)-58-77](https://doi.org/10.25140/2410-9576-2022-1(24)-58-77).
2. Dubnytskyi, V.I., Naumenko, N.Yu. (2019). Methodological Support for the Formation of Information Security in the Field of Regional Economic Security. *Bulletin of Economic Science of Ukraine*, № 1. URL: <http://dspace.nbuv.gov.ua/handle/123456789/151638>.

3. Frolova, L.V., Boiko, I.M. (2021). Entrepreneurship Transformation in the Context of the Digital Economy. *Economy: Realities of Time*, № 2 (54), pp. 47-56.
4. Kitsyuk, V.M., Pupynin, O.S. (2024). Enterprise Information Security: Theoretical Aspect. *Modern Information Protection*, № 2 (58), 103-108. DOI: <https://doi.org/10.31673/2409-7292.2024.020012>
5. Klymchuk M. (2022) Methodology for managing investment processed of digitalization of the economy. *Innovation and Sustainabil.* № 1. 20-33. DOI: <https://doi.org/10.31649/ins.2022.1.20.33>.
6. Kovalska, L., Topalov, V., Topalov, R. (2023). Regional Information Security: Approaches to Consideration and Economic Essence. *Economic Forum*, № 13 (2), 18-24.
6. Kraus, K.M., Kraus, N.M., Shtepa, O.V. (2022). Digital Transformation of Cybersecurity at the Micro Level under Martial Law Conditions. *Innovation and Sustainability*, № 3, 26-37.
8. Kuziomko, V. (2021). Business Information Security in the Context of Digital Economy Transformation. *Innovative Entrepreneurship: Status and Development Prospects: Collection of Materials of the VI All-Ukrainian Scientific and Practical Conference*, Kyiv, March 29-30, 2021. Kyiv: KNEU, 26-28. URL: <https://ir.kneu.edu.ua:443/handle/2010/36159>.
9. Leonenko, N.A., Postupna, O.V. (2022). Information Security of Ukraine: Mechanisms, Current Challenges, and Threats in the Context of Information Globalism. *Bulletin of the National University of Civil Protection of Ukraine, Series: Public Administration*, № 2 (17). URL: <http://repositsc.nuczu.edu.ua/handle/123456789/16883>.
10. Melnychuk, H.S., Mamalyha, V.O. (2020). Digitalization of the Economy: Opportunities and Threats to the Effective Functioning of Enterprises. *Pryazovskyi Economic Bulletin*, № 2 (19), 125-130. DOI: <https://doi.org/10.32840/2522-4263/2020-2-21>.
11. Naumenko, N.Yu. (2019). Analysis of Economic Scientific Directions in the Field of Information Security. *Electronic Scientific Professional Edition in Economic Sciences "Modern Economics"*, № 16, 115-120. URL: <http://dspace.mnau.edu.ua/jspui/bitstream/123456789/6290/1/naumenko.pdf>.
12. Official Website of the Cyber Police Department of the National Police of Ukraine. URL: <https://cyberpolice.gov.ua/news/policziya-rozpochala-kryminalne-provadzheniya-za-faktom-kiberatak-na-sajty-derzhavnyx-organiv-1549/>
13. Savras, I.Z., Fedynets, N.I. (2023). Digitalization and Innovative Development of Enterprises: Trends, Problems, and Prospects. *Bulletin of Lviv Trade and Economic University. Economic Sciences*, № 74. 108-114. DOI: <https://doi.org/10.32782/2522-1205-2023-74-14>.
14. Shostak, L., Pomazun, O. (2024). Information Security in the Context of Innovative Business Model Development of Domestic Enterprises under the Digital Economy. *Digital Economy and Economic Security*, № 5 (14), 160-165. DOI: <https://doi.org/10.32782/dees.14-25>.
15. Sytnyk, N., Sebestyanovych, I. (2022). Digitalization and Its Impact on the Development of Small and Medium Businesses. *Graal of Science*, № 11, 50-52. DOI: <https://doi.org/10.36074/grail-of-science.24.12.2021.005>.
16. Yakovenko, Ya.Yu., Bilyk, M.Yu., Oliynyk, Ye.V. (2024). Digital Transformation of Business Structures: Strategic Guidelines in the Era of Innovations and Technological Changes. *Economic Space*, № 190, 355-360. DOI: <https://doi.org/10.32782/2224-6282/190-63>.