# CONCEPTUAL APPROACHES TO ENSURING FINANCIAL SECURITY OF IT COMPANIES IN THE CONTEXT OF SMART ECONOMY AND DIGITALISATION

**Ihor Rumyk[1], Polina Puzyrova[2]**

*[1]Doctor of Science in Economics, Professor, Head of Economics and Finance Department, KROK University, Kyiv, Ukraine, e-mail: rumykii@krok.edu.ua, ORCID: https://orcid.org/0000-0003-3943-639X*

*[2]Doctor of Science in Economics, Professor, Associate Professor of the Department of Smart Economics, Kyiv National University of Technologies and Design, Kyiv, Ukraine, e-mail: puzyrova@ukr.net, ORCID: https://orcid.org/0000-0003-0839-8730*

***Citation:***
Rumyk, I., & Puzyrova, P. (2025). Conceptual Approaches to Ensuring Financial Security of it Companies in the Context of Smart Economy and Digitalisation. *Economics, Finance and Management Review*, (1(21), 85–97. https://doi.org/10.36690/2674-5208-2025-1-85-97

***Received: March 12, 2025***
***Approved: March 29, 2025***
***Published: March 31, 2025***



***Abstract.*** *The article examines comprehensive approaches to ensuring financial security, which take into account the specifics of digital technologies, economic changes, and also ensure compliance with regulatory requirements that require constant updating of knowledge, introduction of innovative approaches to financial planning and risk management, which is the key to stability and successful functioning of IT companies in the context of the smart economy and digitalisation. The purpose of the article is to study conceptual approaches to ensuring financial security of IT companies in the context of the smart economy and digitalisation, focusing on integrated approaches to managing financial flows and risks in the context of digital business transformation, contributing to the development of methods that allow IT companies to adapt to new economic realities while maintaining their financial stability and competitiveness in the market. It is established that the smart economy and digitalisation not only increase the efficiency of financial management but also contribute to the resilience of IT companies to external and internal challenges, which ultimately ensures their financial security and sustainable development. It is proved that the financial security of IT companies in the context of the smart economy and digitalisation is a key factor in sustainable development and competitiveness, which includes a set of measures aimed at protecting financial resources, ensuring risk resilience and effective management of financial flows. The article proposes the implementation of an algorithm for ensuring financial security of IT companies in the context of the smart economy and digitalisation, which will help IT companies to ensure financial security, adapt to the challenges of the digital economy and maintain stability in a dynamic market environment. The area for further research is to develop financial security models that take into account the specifics of digital technologies, such as blockchain, artificial intelligence, big data, and process automation.*

***Keywords****: financial security, IT enterprises, smart economy, digitalisation, financial planning, cyber threats, blockchain, artificial intelligence, process automation.*

***JEL Classification: G32, G38, O33***

***Formulas: 0, fig.: 2, tabl.: 1, bibl.: 42***

**Introduction.** The issue of ensuring financial security of IT companies in the context of the smart economy and digitalisation is an extremely relevant task, as the development of technology, growing dependence on digital platforms and global integration of economies require new approaches to managing financial flows and protecting against possible threats. Modern IT companies operate in an environment where financial transactions are becoming more vulnerable to cyber threats, regulatory changes and uncertainty in the economic environment. One of the key aspects of ensuring the financial security of IT companies is the need to integrate it into the company's overall development strategy, including the use of digital technologies such as blockchain, artificial intelligence and big data, which will improve the efficiency of financial processes.

In the smart economy, where the role of information technology and digital platforms has grown significantly, the problem of adapting financial strategies to rapidly changing conditions is becoming particularly important. The integration of digital technologies into financial processes requires the development of new conceptual approaches to financial security, including the creation of systems that can adapt to the risks arising from the digitalisation of business. In addition, a significant challenge is the integration of regulatory requirements for financial security in the context of globalisation and changes in the regulatory framework, especially in terms of personal data protection, financial transactions and intellectual property protection. Without a reliable mechanism of regulation and control at the international level, companies may become vulnerable to financial crimes, which reduces market confidence and affects investment flows.

Thus, the main challenge is the development and implementation of comprehensive approaches to financial security, which should take into account the specifics of digital technologies, economic changes, and ensure compliance with regulatory requirements, which requires constant updating of knowledge, implementation of innovative approaches to financial planning and risk management, which are the key to the stability and successful functioning of IT companies in the smart economy and digitalisation.

**Literature review.** An analysis of the latest research and publications on the topic allows us to identify several key areas that are in the focus of attention of scholars and practitioners. First, the growing role of digital technologies and innovations in the IT sector significantly complicates financial risk management (Bondarchuk et al., 2023; Garbowski et al., 2019; Livinskyi et al., 2024). Scientists note that digitalisation is leading to changes in the financial models of companies, which requires the adaptation of strategies to ensure their financial security. At the same time, cybersecurity issues are becoming increasingly important as more and more companies work with large amounts of data, including confidential financial information. Risks associated with cyberattacks, fraud and data leakage are growing, requiring a more comprehensive approach to financial security. One of the important aspects discussed in recent publications is the application of smart economics, which involves the integration of the latest technologies such as artificial intelligence, blockchain, and big data to automate financial monitoring, risk analysis, and forecasting processes, which not only

improve control over financial flows but also make them more transparent and efficient (Galych et al., 2024; Lozhachevska et al., 2023; Pronko et al., 2025; Suntsova, 2022).

In addition, the publications highlight the need for changes in approaches to financial security, where traditional methods are often unable to take into account the speed of change and unpredictability of the modern digital economy. Therefore, when developing financial security strategies, companies need to take into account flexibility and the ability to quickly adapt to new conditions. Financial management models should integrate tools for automated data collection and processing, which allows for a more rapid response to changes in the market and technological environment (Azarenkova et al., 2021; Hrytsenko et al., 2022; Khizhnyak, 2018; Mazur et al., 2021; Pronoza et al., 2022). Given the rapid development of digital technologies, scholars point to the need to adapt legislation and regulations to new conditions, including the development of international cybersecurity standards, regulations on personal data protection and control over the use of the latest technologies. One important aspect is the creation of legal mechanisms to protect against cybercrime and financial fraud in the digital environment (Purdenko et al., 2023; Pylypenko et al., 2022; Ramskyi et al., 2018; Taghieva et al., 2022). Another important topic is the management of corporate culture in the context of digitalisation. As the financial security of a company largely depends on the security culture among its employees, recent studies by the authors (Dokiienko et al., 2021; Ishchejkin et al., 2022; Kalinin, 2024; Kozachenko, 2020; Varnalii & Mekhed, 2022; Zlotenko al., 2019; Zubko al., 2021) draw attention to the role of training and raising awareness of employees about the risks associated with cyber threats and financial management in the context of digitalisation.

Thus, current research points to the importance of a comprehensive approach to ensuring financial security in the IT sector, including technological innovations, regulatory changes and adaptation of corporate culture. This allows companies to effectively manage financial risks and ensure stability and resilience in the face of rapid changes in the market and technological environment.

**Aims.** The article is aimed at researching conceptual approaches to ensuring the financial security of IT companies in the context of the smart economy and digitalisation, focusing on integrated approaches to managing financial flows and risks in the context of digital business transformation, contributing to the development of methods that allow IT companies to adapt to new economic realities while maintaining their financial stability and competitiveness in the market.

**Methodology.** The article uses various methods that allowed for a deeper analysis of the financial and information aspects of IT companies: analysis of literature and regulations - to assess the existing theoretical approaches and practices governing financial security in the context of digitalisation; comparative analysis - to determine the most effective and adapted models of ensuring financial security of IT companies; case method - to study real financial security practices in IT companies through the study of specific examples from the experience of leading companies; empirical research method - to assess the opinions of experts and practitioners on financial security in the context of digitalisation and the smart economy; system analysis method - to identify and study the relationships between different elements of financial security in the context of digitalisation; the method of scenario planning - to assess possible

options for the development of financial security of companies in the context of rapid changes in digital markets; the method of expert assessments - to collect opinions and assessments of experts on potential threats and methods of their minimisation; benchmarking method - to study the best practices of financial security in the IT sector at the international level; analytical method - to identify trends, threats and opportunities in the field of financial security; tabular and graphical method, etc. These methods allowed us to gain a comprehensive understanding of the situation and suggest ways to improve financial security for IT companies in the context of digital transformation and the smart economy.

**Results.** In the current context of the smart economy and digitalisation, financial security of IT companies is of particular importance. The impact of technological innovations, cyber threats, digital assets and regulatory changes requires new approaches to managing financial resources and ensuring the sustainability of companies. The modern development of digital technologies and the introduction of the smart economy concept create new opportunities and challenges for companies in the information technology sector (Galych et al., 2024; Lozhachevska et al., 2023).

In the context of digitalisation, financial security is becoming one of the key factors of business stability and sustainability, as companies are increasingly dependent on digital assets, online transactions, and cloud services. As the use of technology grows, so does the number of cyber threats, financial fraud, regulatory changes and competition, which complicates the management of financial resources. In addition, the digital transformation of the economy is forcing companies to adapt to new business models, introduce automation of financial processes and use advanced technologies to analyse and predict financial risks. All of this makes ensuring financial security a strategically important task for IT companies, as their competitiveness, investment attractiveness, and ability to develop sustainably in a rapidly changing business environment depend on the effectiveness of these measures (Maslii & Maksymenko, 2025; Pisarevskiy et al., 2021).

Smart economics and digitalisation play a key role in ensuring the financial security of IT companies by creating new management models, improving the efficiency of business processes and reducing risks. The smart economy is based on the use of modern technologies, including artificial intelligence, big data, blockchain and automation, which allows companies to adapt to dynamic market changes, reduce costs and increase competitiveness. Business digitalisation promotes transparency of financial transactions, improves control over costs and revenues, reduces the likelihood of fraud and ensures rapid response to threats. The introduction of cloud technologies allows IT companies to quickly scale their capacities without significant investment, which is especially important for startups and small businesses (Rodrigues et al., 2022).

In addition, the use of automated financial systems and analytical platforms helps to accurately forecast financial flows and avoid cash gaps. Data security and protection against cyber threats are an integral part of the financial stability of IT companies. The use of blockchain in financial transactions minimises the risks of counterfeiting and unauthorised interference, and artificial intelligence systems allow for the detection of suspicious transactions in real time (Rumyk et al., 2021; Sotnyk et al., 2020). The smart economy also involves flexible business models that allow for the optimisation of

financial resources using crowdfunding, crowdsourcing, and digital assets. Thus, the smart economy and digitalisation not only increase the efficiency of financial management, but also contribute to the resilience of IT companies to external and internal challenges, which ultimately ensures their financial security and sustainable development.

The financial security of IT companies in the context of the smart economy and digitalisation is a key factor in sustainable development and competitiveness, which includes a set of measures aimed at protecting financial resources, ensuring risk resilience and effective management of financial flows (Kondratenko et al., 2021; Mazur et al., 2021). The main aspects of ensuring the financial security of IT companies are shown in Fig. 1.

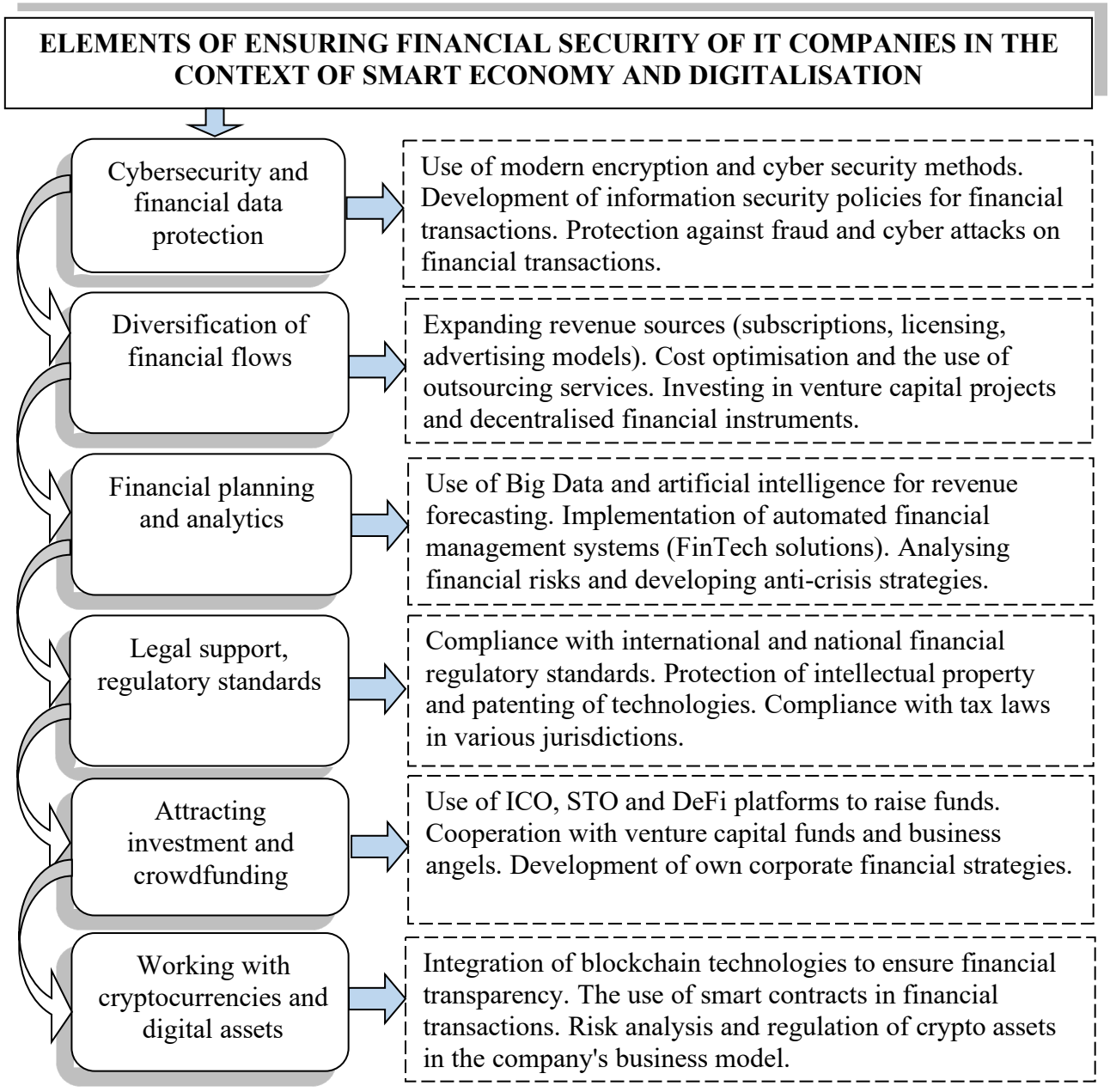


**Fig. 1. Key aspects of ensuring the financial security of IT companies in the context of the smart economy and digitalization**

*Source: compiled by the authors*

Ensuring the financial security of IT companies in the digitalised world requires a comprehensive approach that includes technological, economic and legal aspects. The use of advanced digital solutions in combination with competent financial management helps to reduce risks, increase profitability and ensure the company's stable growth in the smart economy. Regulatory and legal documents governing financial security in the context of digitalisation are shown in Table 1.

**Table 1. Main content and scope of legal and regulatory documents governing financial security in the context of digitalisation**

| Regulatory and legal document | Essence | Application in the context of digitalisation |
|---|---|---|
| Law of Ukraine «On Financial Services and State Regulation of Financial Services Markets2 | Defines the legal and organisational framework for financial services, including the provision of IT and financial services and ensuring their security. | Regulates the activities of financial institutions working with digital technologies, including financial technologies (FinTech), digital currencies, and other electronic services. |
| Law of Ukraine 2On Personal Data Protection2 | Defines the rules for collecting, processing and protecting personal data. | It ensures the protection of financial and personal data that is critical for IT companies in the context of digital transactions. This also includes protection against cyber threats. |
| Law of Ukraine «On Electronic Commerce» | Regulates legal relations in the field of e-commerce, including transactions via the Internet. | It defines the legal framework for online financial transactions and transactions, which is the basis for ensuring financial security in the digital environment. |
| Law of Ukraine «On Cybersecurity» | Establishes the principles of protection of Ukraine's cyberspace, including security standards for information systems and protection of financial transactions from cyber threats. | Regulates the security measures that IT companies must take to protect their financial systems from cyber threats, such as hacker attacks and unauthorised access to financial data. |
| Law of Ukraine «On Cryptocurrencies» | Regulates the legal status of cryptocurrencies and digital assets, procedures for their circulation and control, including in the financial sector. | It defines the legal framework for cryptocurrency transactions, which can pose a threat to financial security if their circulation is not properly regulated in the digital environment. |
| International standards (e.g. ISO/IEC 27001, PCI DSS) | International standards governing the security of information systems and the protection of financial data. ISO/IEC 27001 is a standard for information security management. PCI DSS is a standard for payment card security. | International standards used to ensure the security of financial and payment systems in the digitalised environment, which are critical for the financial security of IT companies operating in the global market. |
| Law of Ukraine «On State Financial Control» | Defines the legal framework for controlling the finances of the state and enterprises, ensuring their transparency and security. | Establishes mechanisms for controlling financial transactions, including verification of compliance of financial transactions of IT companies with security and legal requirements in the digital economy. |
| Law of Ukraine «On the Principles of State Anti-Corruption Policy for 2021-2025» | It defines measures to prevent corruption, including control over financial flows in organisations. | Provides protection against financial abuse and corruption risks in digital financial processes, such as transaction processing in IT companies. |
| Resolutions of the NBU and other controlling authorities | Decisions and resolutions of the National Bank of Ukraine and other supervisory authorities regulating financial security in the context of digital transactions and the use of new financial technologies. | Standards and guidelines for IT companies to process financial transactions, protect data, and ensure the security of financial systems within digital solutions. |

*Source: compiled by the authors*

The financial security of IT companies in the smart economy and digitalisation is influenced by 10 key factors (Rumyk, 2021; Samborska et al., 2024; Tiutiunyk et al., 2021):

1. Cybersecurity is a critical aspect of modern business that includes the development and implementation of security strategies, network measures, cryptographic solutions, and access control. Financial data protection is ensured through the use of modern encryption methods and transaction monitoring, which helps to avoid unauthorised access and theft.

2. Revenue diversification - allows the company to reduce the risks associated with volatile demand, seasonal fluctuations, changes in regulation or economic crises. As a result, the company becomes more resilient to market changes, improves financial performance and creates additional opportunities for development.

3. Risk management - allows for a more accurate risk assessment, prompt response to changes in market conditions, and effective strategies to minimise financial threats. Risk management in the smart economy is based on digital technologies that can significantly improve the accuracy of forecasting, the speed of response and the effectiveness of financial risk mitigation strategies.

4. Automation of financial processes in the context of the smart economy and digitalisation is a key factor that contributes to increasing the efficiency of financial management, reducing operating costs and minimising the human factor in decision-making, which opens up new opportunities for businesses and the public sector, increasing financial inclusion and improving budget management at various levels.

5. Intellectual property plays a key role in ensuring innovative development, competitiveness and sustainable economic growth. The protection of patents, copyrights and unique technologies is becoming a priority as digital platforms and globalisation greatly facilitate access to information, increasing the risk of illegal use or copying of innovations.

6. Regulatory compliance - ensures the legality and transparency of financial and economic activities of IT enterprises and organisations. Digital transformation requires adaptation to new technological solutions that affect the way accounting, tax reporting and financial control are conducted. In today's environment, it is important not only to comply with the current legislation but also to be prepared for rapid changes in the regulatory environment, which requires the integration of digital technologies into the audit, tax administration and financial control processes.

7. Financial transparency plays a key role in building trust, effective resource management and stimulating economic growth. The introduction of open and understandable accounting and reporting mechanisms is made possible by modern digital technologies, such as blockchain, artificial intelligence, automated financial management systems, and Big Data.

8. Attracting investments - provides financial support for innovative projects, start-ups and technology initiatives. In this context, cooperation with venture capital funds that are willing to invest in high-risk but promising IT businesses plays an important role. Crowdfunding is becoming an additional tool for raising capital, allowing to attract funding from a wide range of individuals through specialised online platforms, which helps to decentralise the investment process and increase the level of trust in innovative products.

9. Innovation. The smart economy is based on the integration of digital technologies, automation, artificial intelligence, big data, and blockchain, which allows

for faster improvement processes, greater efficiency, and faster response to consumer demands. Innovation is manifested in the creation of new products, optimisation of production processes, personalisation of services and expansion of the functionality of digital platforms. Continuous improvement enables companies to reduce costs, improve the quality of goods and services, and implement environmentally and sustainably friendly solutions, which in turn strengthens their competitiveness in the global market.

10. Business model flexibility - implies the ability of enterprises to quickly adapt to new conditions using innovative approaches to monetisation, cloud technologies and digital platforms. As a result, the flexibility of the business model contributes to increased competitiveness, faster response to market challenges and more efficient use of digital tools in the modern economy.

Based on the influence of the factors and their characteristics, we can build an algorithm for ensuring the financial security of IT companies in the context of the smart economy and digitalisation (Fig. 2).

Implementing an algorithm for ensuring the financial security of IT companies in the context of the smart economy and digitalisation will help IT companies to ensure financial security, adapt to the challenges of the digital economy and maintain stability in a dynamic market environment. As a result, we propose the following conceptual approaches:

– approach is focused on strengthening cybersecurity, which includes: the use of modern encryption and authentication systems; development of tools for monitoring transactions and detecting anomalies; and training of personnel in cybersecurity;

– approach focuses on diversifying financial flows: attracting various sources of funding (venture capital, crowdfunding, government support); optimising costs and managing cash reserves;

– approach focuses on the automation of financial processes: use of artificial intelligence and blockchain technologies to increase the transparency and security of financial transactions; implementation of automated financial management systems;

– approach focused on adaptation to regulatory changes: monitoring changes in legislation and compliance of financial activities with regulatory requirements; use of licensed digital financial platforms;

– approach focused on investing in innovations: continuous modernisation of business models in line with digital trends; use of Big Data and analytics to predict financial risks.

Therefore, the financial security of IT companies in the context of digitalisation requires a comprehensive approach that includes strengthening cybersecurity, adapting to regulatory changes, diversifying funding sources and introducing innovations. The use of modern digital technologies helps to minimise risks and ensure stable development in a rapidly changing business environment.

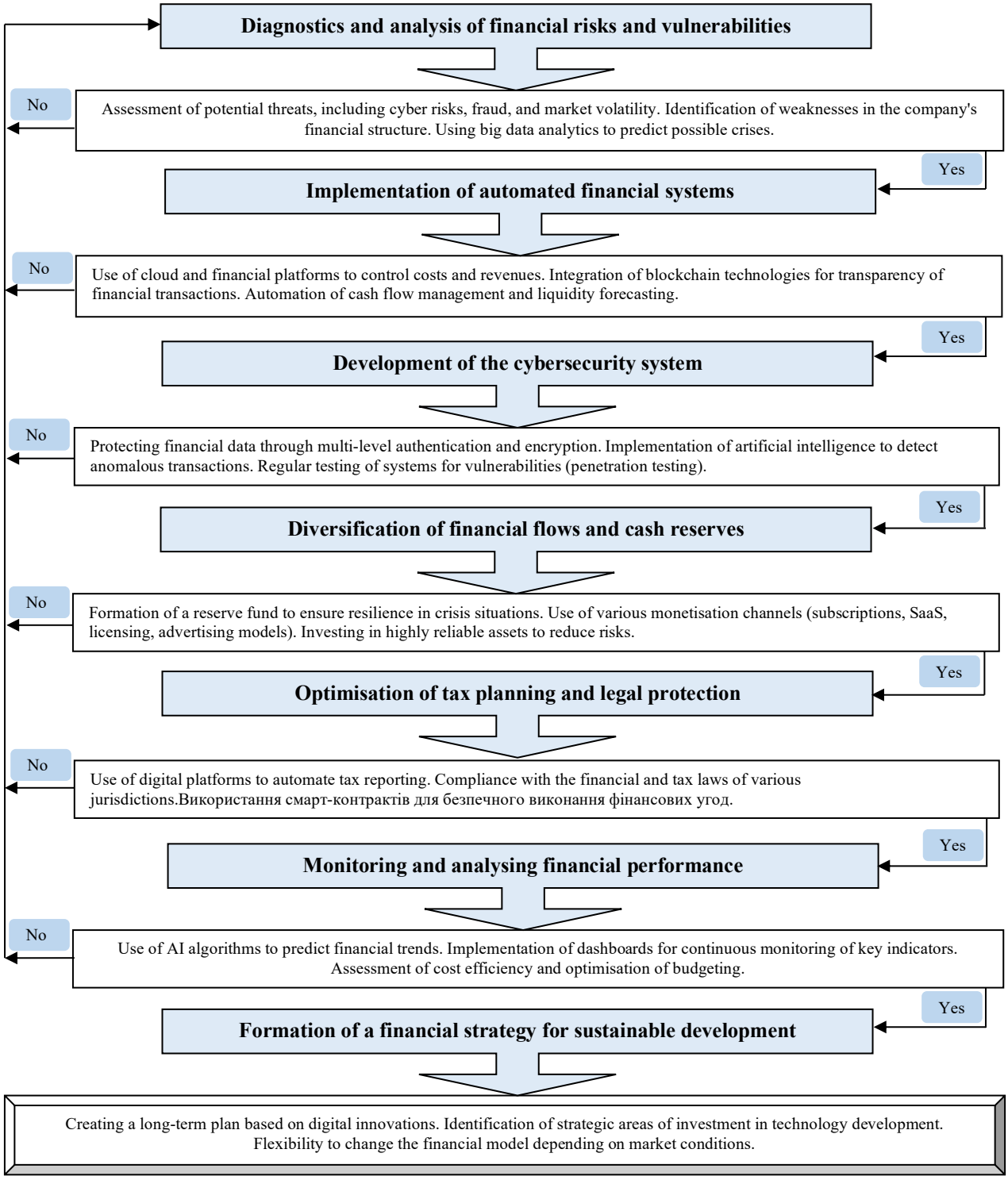


**Figure 2. Algorithm for ensuring the financial security of IT companies in the context of the smart economy and digitalization**

*Source: proposed by the authors*

**Discussion.** The financial security of IT companies is a key aspect that ensures stability and sustainable business development in the face of rapid changes caused by digitalisation and the introduction of smart economic technologies. In this context,

conceptual approaches to financial security are of particular importance, as traditional methods may be ineffective in the face of constant technological change and new financial threats. One of the key aspects is the integration of financial security measures into a company's digitalisation strategy. In the context of the development of the smart economy, where every aspect of a company's activities is becoming digital, it is important to ensure that security is integrated at every stage of the introduction of new technologies, from software development to financial transaction processing (Zlotenko et al., 2019; Lozhachevska et al., 2023). In the modern world, a significant part of financial processes is carried out through digital platforms. Thus, cyber threats can pose a serious threat to the financial stability of IT companies.

Various hacker attacks, fraud and data breaches can lead to significant financial losses and loss of trust in a company. IT companies often operate in a high-risk environment, in particular due to technological changes, changes in demand for products or services, and volatility in financial markets. Therefore, an important element of financial security is financial risk management and diversification of funding sources (Azarenkova et al., 2021).

With the development of digital technologies and the introduction of the smart economy internationally, new regulatory requirements are emerging in relation to the protection of personal data, financial transactions and cryptocurrencies. IT companies are forced to adapt to the new requirements of the legislation that defines the rules of doing business and data protection. As IT companies operate in the field of innovation and rapid change, one of the key elements of financial security is continuous investment in new technologies that help ensure competitiveness and protect against new threats (Maslii et al., 2025; Pronko et al., 2025). The financial security of an IT company depends not only on technological solutions, but also on its corporate culture. Raising employees' awareness of the importance of financial security, data protection, and fraud prevention is a prerequisite for the successful operation of a company.

Thus, given the rapid development of technology, companies must be prepared to adapt their financial security strategies to the changes that are constantly taking place in the digital world.

**Conclusions.** In the smart economy and digitalisation, IT companies face new financial threats, such as cybercrime, market volatility and rapid technological change. To ensure financial security, it is important to actively adapt strategic financial management to these conditions. The use of the latest technologies to automate financial processes reduces the human factor, reduces costs and increases the efficiency of financial management, which is critical for IT companies. Given the high level of cyber threats, IT companies must make significant investments in protecting their information systems and financial data. It is important to implement systems for monitoring and rapid response to cyber incidents. In the face of market volatility and global economic changes, diversification of financial sources and assets is becoming an important protection tool. This allows companies to mitigate risks associated with currency fluctuations, changes in regulations or other unforeseen events. In the context of digitalisation and globalisation, compliance with national and international regulatory standards is becoming increasingly important. IT companies should be ready to quickly adapt their financial strategies to changes in legislation and market

requirements. To ensure financial security, it is important not only to have technical support, but also to create a culture of security among employees. Educating and training staff on financial and cyber threats reduces the risk of human error and promotes effective resource management.

In general, the financial security of IT companies in the smart economy and digitalisation requires a comprehensive approach that includes the integration of the latest technologies, flexibility in financial planning, and the ability to adapt to a rapidly changing digital environment.

An area for further research is the development of financial security models that take into account the specifics of digital technologies, such as blockchain, artificial intelligence, big data, and process automation. This will allow for more flexible and adaptive financial risk management strategies that take into account new technological challenges and threats, including cyber threats. In general, further research should contribute to the creation of integrated financial security management systems that work effectively in the context of the smart economy and digitalisation, and ensure the long-term stability and resilience of IT companies in the face of rapid market changes.

**Author contributions.** The authors contributed equally.

**Disclosure statement.** The authors do not have any conflict of interest.

**References:**

1. Azarenkova, G. M., Golovko, O. G., Oryekhova, K. V., Salenko, O. V. & Maiboroda, A. V. (2021). Estimating and forecasting of financial security of enterprises. *Financial and Credit Activity Problems of Theory and Practice, 1*(32), 224-230. https://doi.org/10.18371/fcaptp.v1i32.20038.
2. Bondarchuk, L., Mazur, N., Tsalko, T., Kovalenko, M., Zaritska, N. & Puzyrva, P. (2023). Innovative design of financial and management accounting and the impact of population migration on the development of agricultural enterprises in the context of security and information risks. *Financial and Credit Activity Problems of Theory and Practice, 5*(52), 481-493. https://doi.org/10.55643/fcaptp.5.52.2023.4212.
3. Dokiienko, L., Hrynyuk, N., Nakonechna, O. & Mykhailyk, O. (2021). System for evaluation of financial security of operational activity of oil-and-fat industry enterprises. *Agricultural and Resource Economics: International Scientific E-Journal, 7*(4), 138-159. https://doi.org/10.51599/are.2021.07.04.08.
4. Galych, O., Barna, M., Fedirets, O., Fedirko, H., Bielialov, T. & Puzyrova, P. (2024). Financial management of entrepreneurial universities in the conditions of digitalization, smart economy and the development of educational tourism. *Financial and Credit Activity Problems of Theory and Practice, 3* (56), 474-489. https://doi.org/10.55643/fcaptp.3.56.2024.4420.
5. Garbowski, M., Lubenchenko, O., Perederii, N., Moskalenko, N., & Rumyk, I. (2019). Economic and mathematical modeling of loan risks for credit unions. Journal of Management Information and Decision Sciences, 22(4), 495-500. https://library.krok.edu.ua/media/library/category/statti/rumyk_0003.pdf
6. Hrytsenko, L., Zakharkina, L., Zakharkin, O., Novikov, V., & Chukhno, R. (2022). The impact of digital transformations on the transparency of financial and economic relations and financial security of Ukraine. *Financial and Credit Activity Problems of Theory and Practice*, *3*(44), 167-175. https://doi.org/10.55643/fcaptp.3.44.2022.3767.
7. Ishchejkin, T. et al. (2022). Information subsystem of agri-food enterprise management in the context of digitalization: the problem of digital maturity. *Journal of Hygienic Engineering and Design (JHED), 38,* 243-252. https://er.knutd.edu.ua/bitstream/123456789/19628/2/JHED-Volume-38_Puzyrova_243-252.pdf.
8. Kalinin, O. (2024). Investment Security in the Development of the Digital Economy. *Economics Ecology Socium, 8*, 73-84. https://doi.org/10.61954/2616-7107/2024.8.2-6.
9. Khizhnyak, Yu. (2018). Methodical approach to assessing the level of financial security of the enterprise. *Market Infrastructure, 23*, 305-312. http://www.market-infr.od.ua/journals/2018/23_2018_ukr/55.pdf.
10. Kondratenko, N. O., Doroshenkonko, H. O., Ternova, I. A., Babych, S. N. & Dorosheko, O. G. (2021). Organizational and methodical provision of the financial and economic security management of the enterprise. *Financial and Credit Activity Problems of Theory and Practice, 1*(32), 129-137. https://doi.org/10.18371/fcaptp.v1i32.200301.
11. Kostikov, E., Jilkova, P. & Kotatkova Stranska, P. (2021). Optimization of e-commerce distribution center location. *Marketing and Management of Innovations, 2*, 166-178. https://doi.org/10.21272/mmi.2021.2-14.
12. Kotkovskyi, V., Zaluzhny, V., Kadala, V., Guzenko, O., Bohatyrova, M. & Leskova-Hodlevska, J. (2020). Digitization as an innovative segment of enterprise financial security management. *VUZF Review, 5*(3), 13-19. https://doi.org/10.38188/2534-9228.20.3.02.

13. Kozachenko, A. (2020). Financial sustainability of the enterprise: features of recognition and strategy of providing in modern condition. *Slovak International Scientific Journal, 3*, 23-30. http://repository.vsau.org/getfile.php/24824.pdf.
14. Livinskyi, A., Palchyk, I., Samoilova, I., Safronska, I., Nechyporenko, K., Andryshyn, V., Bolshaia, O. & Dashko, O. (2024). Financial and security design of management accounting of innovative agricultural enterprises in conditions of digitalization and migration risks. *Management Theory and Studies for Rural Business and Infrastructure Development, 46*(3), 329-345. https://doi.org/10.15544/mts.2024.31.
15. Lozhachevska, O., Taranenko, A., Raikovska, I., Pleskach, O., Kupchyshyna, O., Shatskaya, Z. & Puzyrova, P. (2023). Financial strategy of management for marketing and communication design in smart economy conditions. *Management Theory and Studies for Rural Business and Infrastructure Development, 45*,(4), 314-333. https://doi.org/10.15544/mts.2023.32.
16. Maslii, O. & Maksymenko, A. (2025). Digital transformation and economic deindustrialisation: impact on the financial security of the state. *Financial and Credit Activity Problems of Theory and Practice*, *1*(60), 401-414. https://doi.org/10.55643/fcaptp.1.60.2025.4599.
17. Mazur, N. et al. (2021). Improvement of controlling in the financial management of enterprises. *TEM Journal, 10*(4), 1605-1609. https://doi.org/10.18421/TEM104-15.
18. Pisarevskiy, M., Aleksandrova, V., Yevtushenko, V., Poroka, S., Shoiko, V. & Karpeko, N. (2021). Management of economic security of industrial enterprises for countering raiding. *Management Theory and Studies for Rural Business and Infrastructure Development, 43*(1), 151-160. https://doi.org/10.15544/mts.2021.13.
19. Pronko, L., Puzyrova, P., Sobchyshyn, V., Varava, L., Zakharov, D., & Vynohradova, O. (2025). Innovative management of labour potential in the system of digitalisation of financial and economic security of the smart economy. *Financial and Credit Activity Problems of Theory and Practice*, *1*(60), 554-569. https://doi.org/10.55643/fcaptp.1.60.2025.4694.
20. Pronoza, P., Kuzenko, T. & Sablina, N. (2022). Implementation of strategic tools in the process of financial security management of industrial enterprises in Ukraine. *Eastern-European Journal of Enterprise Technologies, 2*(13 (116)), 15-23. https://doi.org/10.15587/1729-4061.2022.254234.
21. Purdenko, O., Artyushok, K., Riazanova, N., Babaiev, I., Kononenko, A., Lepeyko, T. & Zos-Kior, M. (2023). Financial management of innovative eco-entrepreneurship. *Management Theory and Studies for Rural Business and Infrastructure Development, 45*(2), 152-165. https://doi.org/10.15544/mts.2023.16.
22. Pylypenko, O., Matviienko, H., Putintsev, A., Vlasenko, I. & Onyshchuk, N. (2022). Government Tax Policy in the Digital Economy. *Cuestiones Políticas, 40*(72), 279-296. https://doi.org/10.46398/cuestpol.4072.15.
23. Ramskyi, A. & Solon'ko, A. (2018). Mechanism of formation of financial security of an enterprise. *European Scientific Journal of Economic and Financial Innovation,* (1), 14-20. https://doi.org/10.32750/2018-0102.
24. Rodrigues, A. R. D., Ferreira, F. A., Teixeira, F. J., & Zopounidis, C. (2022). Artificial intelligence, digital transformation and cybersecurity in the banking sector: a multi-stakeholder cognition-driven framework. *Research in International Business and Finance, 60*: 101616. https://doi.org/10.1016/j.ribaf.2022.101616.
25. Rumyk, I., Laptev, S., Seheda, S., Akimova, L., Akimov, O. & Karpa, M. (2021). Financial support and forecasting of food production using economic description modeling methods. *Financial and Credit Activity Problems of Theory and Practice*, *5*(40), 248-262. https://doi.org/10.18371/fcaptp.v5i40.245098.
26. Rumyk, I. (2021). Modeling the impact of economic indicators on foodsecurity. *Economics, Finance and Management Review, 2*, 4-13. https://doi.org/10.36690/2674-5208-2021-2-4.
27. Samborska, O., Rudnichenko, Ye., Havlovska, N., Matiukh, S., Nazarchuk, T. & Harbusiuk, V. (2024). Assessment of negative impact of operating environment of the enterprise on business processes and economic security. *TEM Journal, 13*(2), 1345-1351. https://d 38TU oi.org/10.18421/TEM132-48.
28. Sotnyk, I., Zavrazhnyi, K., Kasianenko, V., Roubík H. & Sidorov O. (2020). Investment management of business digital innovations. *Marketing and Management of Innovations, 1*, 95-109. https://doi.org/10.21272/mmi.2020.1-07.
29. Suntsova, O. (2022). The definition of smart economy and digital transformation of business in the concepts Industry 4.0 and 5.0. *Technology Audit and Production Reserves, 4*(4(66)), 18-23. http://doi.org/10.15587/2706-5448.2022.265105.
30. Taghieva, T., & Tiutiunyk, I. (2022). Innovative, economic and marketing determinants of financial security and sustainability of business. *Marketing and Management of Innovations, 1*, 176-185. https://doi.org/10.21272/mmi.2022.1-13.
31. Tiutiunyk, I., Kuznetsova, A. & Spankova, J. (2021). Innovative approaches to the assessment of the impact of the shadow economy on social development: an analysis of causation. *Marketing and Management of Innovations, 3*, 165-174. http://doi.org/10.21272/mmi.2021.3-14.
32. Varnalii, Z. & Mekhed, A. (2022). Financial security of business entities in the digital economy. *Financial and Credit Activity Problems of Theory and Practice*, *4*(45), 267-275. https://doi.org/10.55643/fcaptp.4.45.2022.3813.
33. Zlotenko, O., Rudnichenko, Ye., Illiashenko, O., Voynarenko, M. & Havlovska, N. (2019). Optimization of the sources structure of financing the implementation of strategic guidelines for ensuring the economic security of investment activities of an industrial enterprise. *TEM Journal, 8* (2), 498-506. https://dx.doi.org/10.18421/TEM82-25.
34. Zubko, T., Hanechko, I., Trubei, O. & Afanasyev, K. (2021). Determining the impact of digitalization on the economic security of trade. *Eastern-European Journal of Enterprise Technologies, 6*(13), 60-71. https://doi.org/10.15587/1729-4061.2021.248230.

35. Law of Ukraine «On Financial Services and State Regulation of Financial Services Markets» No. 2664-III dated 12.07.2001, version on 11.02.2022. https://urst.com.ua/download_act/pro_finansovi_posluhy.
36. Law of Ukraine «On Personal Data Protection» No. 2297-VI dated 01. 06. 2010, version on 18.01.2025. https://zakon.rada.gov.ua/laws/show/2297-17#Text.
37. Law of Ukraine «On Electronic Commerce» No. 675-VIII dated 03.09.2015, version on 01.01.2024. https://zakon.rada.gov.ua/laws/show/675-19#Text.
38. Law of Ukraine «On the Basic Principles of Ensuring Cybersecurity of Ukraine» No. 2163-VIII dated 05.10.2017, version on 28.06.2024. https://zakon.rada.gov.ua/laws/show/2163-19#Text.
39. Law of Ukraine «On Virtual Assets» No. 2074-IX dated 17.02.2022, current version on 15.11.2024. https://zakon.rada.gov.ua/laws/show/2074-20#Text.
40. On the ISO/IEC 27001 standard – System Management. https://sm-mt.com.ua/services/standart-iso-iec-27001/.
41. Law of Ukraine «On the Basic Principles of State Financial Control in Ukraine» No. 2939-XII dated 01/26/1993, version on 11/15/2024. https://zakon.rada.gov.ua/laws/show/2939-12#Text.
42. Law of Ukraine «On the Principles of State Anti-Corruption Policy for 2021-2025» No. 2322-IX dated 06/20/2022. https://zakon.rada.gov.ua/laws/show/2322-20#Text.