

COUNTERING CYBER RISKS, CORRUPTION AND THE SHADOW ECONOMY THROUGH A EUROPEAN DIGITAL RESILIENCE FRAMEWORK¹

Inna Tiutiunyk *, Doctor of Economics, Associate Professor,
Head of the Department of Financial Technologies and Entrepreneurship
Xinxin Wang**, Postgraduate Student
Sumy State University

*ORCID 0000-0001-5883-2940

** ORCID 0009-0000-0185-0574

Дата надходження статті: 12.08.2026

Дата прийняття статті: 15.09.2026

Дата публікації статті: 07.10.2026

Introduction. The deepening of digital integration, cross-border data exchange, and the digitalization of financial and governance processes have made cyber risks, corruption, and the shadow economy increasingly interconnected. Cyberattacks are used to steal financial resources and data, digital technologies facilitate the concealment of illicit financial flows, while corrupt practices adapt to new digital environments. Under these conditions, treating cybersecurity, anti-corruption policy, and countering the shadow economy as separate areas of public policy no longer provides an adequate response to contemporary digital threats. Economic security increasingly depends on an integrated digital resilience system capable of addressing their interconnected nature.

The European Union is progressively developing such a system by combining regulatory, institutional, and technological mechanisms aimed at strengthening cyber resilience, enhancing trust in the digital environment, increasing economic transparency, improving financial monitoring, and limiting illicit economic activity. This approach is shaping a model of economic security focused not only on responding to individual threats but also on strengthening the resilience of public institutions, the financial system, and the digital economy.

The European approach to digital resilience is particularly relevant for Ukraine, which, amid the full-scale war and accelerated European integration, faces large-scale cyber threats, persistent corruption risks, and the challenge of reducing the shadow economy. Approximation to EU standards creates opportunities for incorporating digital resilience principles into Ukraine's economic security framework. However, the combined impact of European regulatory and institutional instruments on cyber risks, corruption, and the shadow economy, as well as their systematic adaptation to the Ukrainian context, remains insufficiently explored. This necessitates systematizing the key components of the European digital resilience system and substantiating their application to strengthen Ukraine's economic security.

Analysis of recent research and publications. The issues of cyber resilience, the use of digital technologies in combating corruption, the impact of digitalization on the shadow economy, and the relationship between institutional quality and informal economic activity have attracted considerable attention from researchers and practitioners. Their relevance has increased with the expansion of digital financial instruments, electronic public services, digital platforms, and cross-border data exchange. However, despite the interconnectedness

¹ The work was carried out within the framework of the Jean Monnet project (Module) "Anti-corruption and countering shadow economy: step by step to common Europe" (101127834 – AcorDes).



of these processes, the respective research areas have largely developed in parallel, without forming a unified analytical framework.

Cyber resilience is among the most extensively developed areas in the literature. Its evolution reflects a shift from traditional cybersecurity, focused primarily on prevention and protection, towards a resilience-based approach emphasizing the ability of systems to maintain critical functions, recover from disruptions, and adapt to changing threats. Segovia-Ferreira et al. identify protection, detection, response, and recovery as key components of cyber resilience [1]. Kott et al. conceptualize it as a combination of design-time solutions and run-time mechanisms that enable adaptive responses to emerging threats [2]. Skierka extends this perspective to public administration, demonstrating through the Estonian electronic identification crisis that the continuity of digital public services depends on both technical security and effective institutional coordination [3].

Another strand of research focuses on the role of digital technologies in combating corruption. Andersen established a relationship between e-government development and lower levels of corruption [4], while Adam and Fazekas examined the potential of big data, artificial intelligence, blockchain, and other emerging technologies for detecting and preventing corrupt practices [5]. However, their effectiveness depends on institutional quality, data availability, and control systems. The OECD similarly emphasizes the importance of digital data and risk-based tools for strengthening public integrity [6].

Considerable attention has also been devoted to digitalization, the shadow economy, and illicit financial flows. The OECD highlights the dual role of digital technologies: they can increase transaction transparency and facilitate the detection of undeclared activities while also creating new forms of economic activity that complicate government oversight [7]. Tropina argues that digital technologies can both strengthen the detection of illicit financial flows and create new channels for their transfer and concealment [8].

The relationship between the shadow economy and institutional quality is well established. Johnson et al. identified links between the unofficial economy, government regulation, and the discretionary powers of public authorities [9]. Dreher and Schneider demonstrated that the relationship between corruption and the shadow economy varies depending on countries' institutional and economic conditions [10]. However, much of this research predates the current scale of digitalization of financial transactions, public procurement, tax administration, and interactions between economic agents and the state.

Recent studies have increasingly attempted to integrate these research areas. Dobrovolska and Rozhkova analyze the impact of digital transformation on anti-corruption and cyber-fraud systems, identifying both new opportunities and associated risks [11]. Yarovenko et al. examine the digital readiness of European countries to combat corruption and cyber threats and confirm the relationship between digital development and states' capacity to respond to these risks [12]. These studies indicate a gradual transition towards examining the interconnections between digitalization, cyber risks, and corruption.

Nevertheless, the literature remains fragmented. Cyber resilience is predominantly examined in terms of protecting digital systems and ensuring their continuity; digital technologies are considered as instruments for combating corruption; and the digitalization of financial and tax processes is viewed as a means of increasing transparency and countering shadow economic activity. The integrated application of these dimensions to simultaneously address cyber risks, corruption, and the shadow economy remains insufficiently explored.

This gap substantiates the need for a comprehensive digital resilience framework integrating the cyber resilience of critical sectors, reliable digital identification, financial transparency, digital tax administration, and regulation of digital platforms. Such integration provides the conceptual basis for developing the European digital resilience framework and examining its role in countering cyber risks, corruption, and the shadow economy.

The purpose of this study is to develop a conceptual model of digital resilience based on the systematization and integration of key EU digital policy instruments aimed at strengthening cyber resilience, combating corruption, and reducing the scale of the shadow economy, as well as to substantiate the possibilities for its application to strengthen Ukraine's economic security.

The main material of the study. Contemporary digital policy in the European Union is characterized by a gradual transition from regulating individual digital processes towards an interconnected system aimed at ensuring their security, transparency, and accountability. Although EU regulatory acts in

cybersecurity, digital identification, financial monitoring, tax administration, digital platforms, and data governance pursue different objectives, together they create a regulatory environment capable of limiting opportunities for cyber threats, corrupt practices, and shadow economic activity.

This provides grounds for interpreting digital resilience more broadly than the traditional ability of information systems to withstand cyberattacks and recover from them. Within this study, digital resilience is defined as the capacity of the digital environment to maintain the security, transparency, and accountability of economic and governance processes in the face of cyber, financial, and institutional threats. This interpretation integrates the technological, institutional, and economic dimensions of digital resilience.

Based on the systematization of EU regulatory instruments, the European digital resilience framework is proposed, integrating five key dimensions: cyber resilience of critical sectors, reliable digital identification, transparency of financial flows, digitalization of tax administration, and data governance and interoperability. Their functional interaction enables different channels through which cyber risks, corrupt practices, and shadow economic activities emerge and spread to be addressed within a unified framework.

Cyber resilience of critical sectors provides the foundation for the stable functioning of the digital economy and public digital systems. Its key regulatory instruments include Directive (EU) 2022/2555 (NIS2), the Digital Operational Resilience Act (DORA), and the Cyber Resilience Act (CRA) [13–15]. NIS2 establishes requirements for cyber risk management and incident response in critical sectors, DORA regulates the digital operational resilience of the financial sector, while the CRA establishes cybersecurity requirements for products with digital elements throughout their life cycle [13–15]. Together, these instruments strengthen the resilience of digital infrastructure supporting financial transactions, public services, tax administration, and data exchange.

Reliable digital identification enables the accurate identification of participants in digital interactions. It is primarily based on eIDAS 2.0 and the European Digital Identity Wallet, aimed at developing a coordinated system of electronic identification and digital attributes across the EU [16]. Combined with financial monitoring and tax control, reliable identification enhances transaction traceability and limits opportunities to use false or stolen identities for illicit activities.

Transparency of financial flows encompasses instruments for detecting suspicious transactions and preventing the laundering of illicit proceeds. Its regulatory and institutional basis is formed by the EU Anti-Money Laundering Package and the Anti-Money Laundering Authority (AMLA) [17–19]. These instruments strengthen the consistency of anti-money laundering rules, coordination among supervisory authorities, and oversight of the digital financial environment, thereby improving the detection of transactions associated with corruption and shadow economic activity.

The digitalization of tax administration increases the transparency of economic transactions and reduces opportunities for income concealment. Key instruments include DAC7, the Central Electronic System of Payment Information (CESOP), and VAT in the Digital Age (ViDA) [20–23]. DAC7 expands tax authorities' access to information on income generated through digital platforms; CESOP facilitates the collection and exchange of cross-border payment information; and ViDA advances digital reporting and electronic invoicing. Their combined application expands the information available to tax administrations and strengthens their capacity to detect undeclared economic activity and tax evasion.

Data governance and interoperability complement these dimensions by establishing rules for digital platforms and the use and exchange of data. The Digital Services Act (DSA) and Digital Markets Act (DMA) establish requirements for digital platforms, while the Data Governance Act and Data Act regulate access to, exchange, and use of data [24–27]. The Artificial Intelligence Act complements this regulatory environment by establishing risk-based requirements for AI systems [28]. Together, these instruments enhance the accountability of digital intermediaries, improve data transparency, and strengthen the information basis for financial, tax, and institutional oversight.

These instruments can therefore be viewed as mutually reinforcing components of a unified European digital resilience framework rather than separate elements of EU digital policy. Cyber resilience ensures reliable digital infrastructure; digital identification supports the traceability of participants; financial monitoring enhances the transparency of financial flows; digital tax administration improves the traceability of economic transactions; and data governance and interoperability provide the information

basis for oversight and analytics. Weaknesses in one component may reduce the effectiveness of the others, while their coordinated functioning generates a synergistic effect. Digital resilience can therefore be considered not merely as the capacity to withstand cyber threats but as a comprehensive component of economic security (Figure 1).

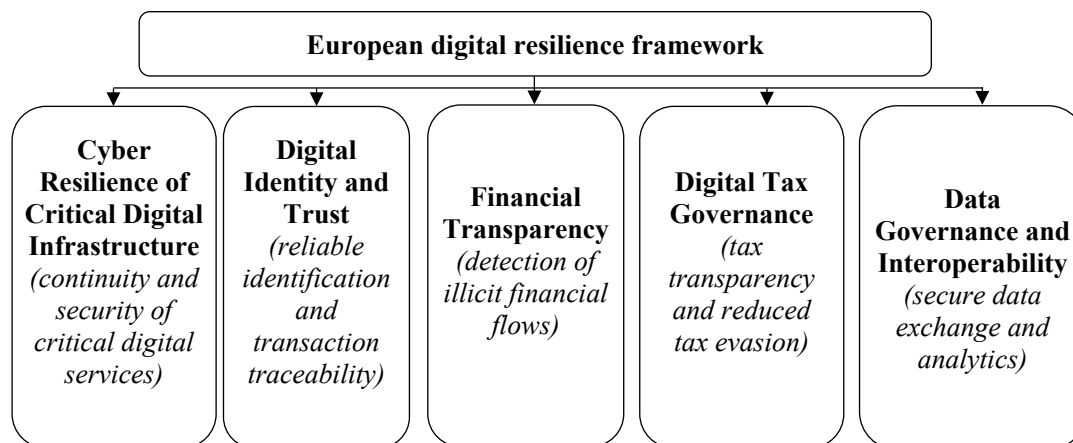


Figure 1. Conceptual structure of the European digital resilience framework

Source: developed by the authors

The effectiveness of the proposed framework is determined not so much by individual regulatory instruments as by their functional interaction. Cyber resilience ensures the continuity of electronic services, digital identification systems, and public registers, while reliable identification enhances the traceability of economic transactions and supports financial and tax control. The integration of data on economic agents, financial transactions, cross-border payments, and digital platform activities further expands the capacity to detect suspicious transactions, undeclared income, tax evasion, and other forms of illicit economic activity.

The interaction among the components of the European digital resilience framework also makes it possible to address the interconnections between cyber risks, corruption, and the shadow economy. Cyberattacks and compromised digital infrastructure may facilitate unauthorized access to data, information manipulation, and non-transparent transactions, thereby creating opportunities for corrupt practices, concealment of financial flows, and shadow economic activity. The proposed framework addresses these channels through resilient digital infrastructure, reliable identification, greater financial and tax transparency, and integrated data governance. The mechanism through which these effects are achieved is presented in Figure 2.

As shown in Figure 2, the interaction among these components generates a comprehensive effect by reducing cyber risks, limiting opportunities for corruption, and decreasing shadow economic activity. Digital resilience therefore becomes not only a characteristic of secure digital infrastructure but also an important component of economic security.

The proposed European digital resilience framework demonstrates that EU regulatory instruments affect cyber risks, corruption, and the shadow economy through different but complementary channels.

The components of the European digital resilience framework address different aspects of digital resilience, including infrastructure security, reliable identification, financial and tax transparency, and effective data use. However, their effects extend beyond individual risk areas, as greater security, transparency, and traceability generate interconnected effects across the digital economy.

Cyber resilience reduces disruptions to critical systems and digital services; reliable identification and financial transparency limit opportunities for anonymous and non-transparent transactions; while digital tax administration and data integration strengthen the detection of undeclared economic activity and tax evasion. The main directions through which the Framework components affect cyber risks, corruption, and the shadow economy are systematized in Table 1.

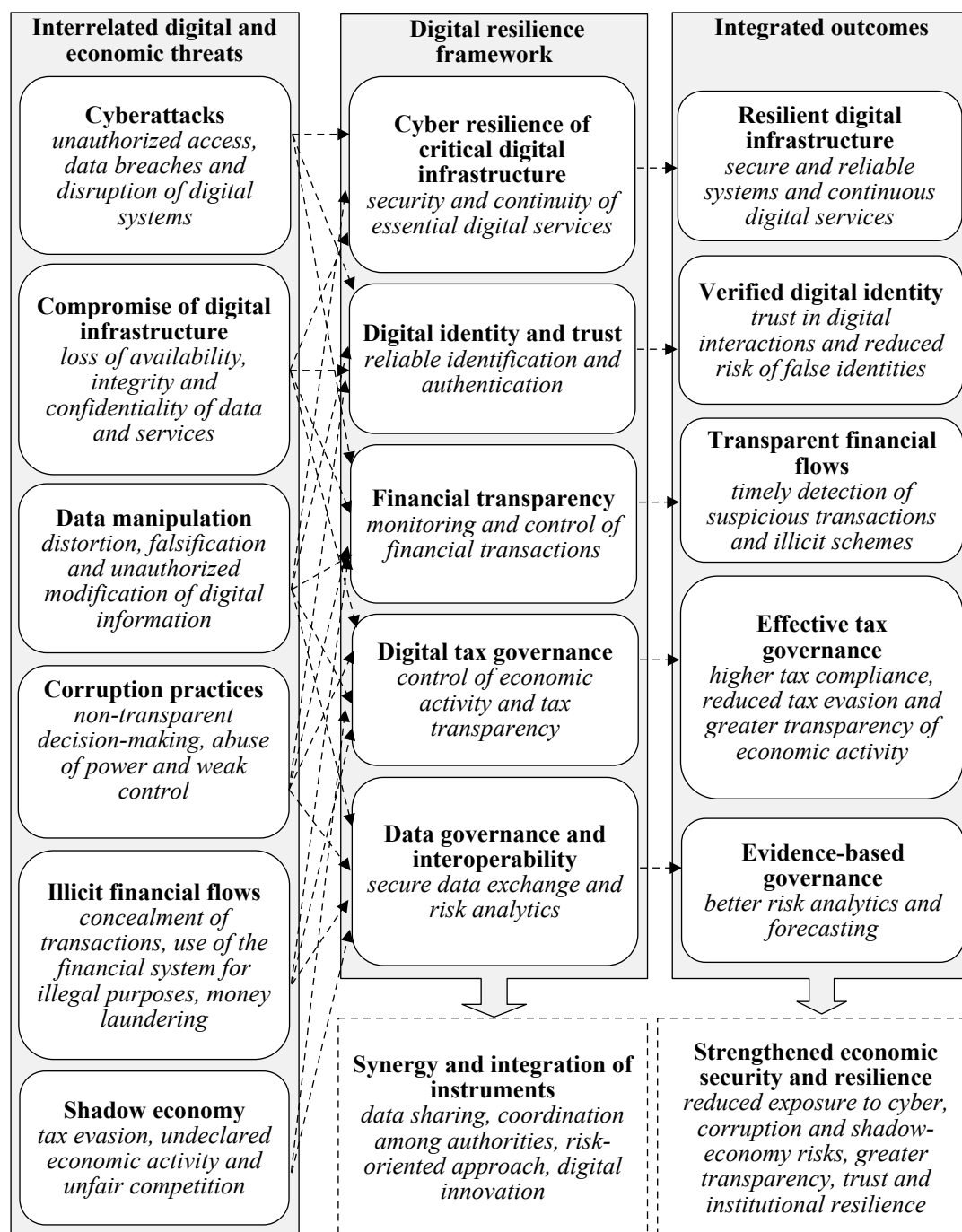


Figure 2. Mechanism of the European digital resilience framework's impact on interconnected cyber risks, corruption, and the shadow economy

Source: developed by the authors

For Ukraine, the practical value of the proposed European digital resilience framework lies in its potential to guide the systematic adaptation of European approaches to digital regulation. Amid deepening digitalization, growing cyber threats, and the approximation of national legislation to the EU acquis, priority should be given not to the fragmented implementation of individual instruments but to ensuring their functional coherence across cyber resilience, digital identification, financial monitoring, tax administration, and data governance.

The adaptation of the framework requires gradual alignment of Ukraine's digital regulatory system with European principles and requirements. Priorities include strengthening the security of critical digital infrastructure and the continuity of public and financial digital services, integrating reliable digital identification with financial monitoring and tax control, and improving digital tax administration and data exchange. Together,

Table 1

Impact of the European digital resilience framework components on countering cyber risks, corruption, and the shadow economy

Component	Countering Cyber Risks	Countering Corruption	Countering the Shadow Economy
Cyber resilience	Protection of critical digital infrastructure and ensuring the continuity of digital services	Protection of public information systems and registers against unauthorized interference	Ensuring the reliability of digital systems for financial and tax control
Digital identity & trust	Secure user identification and authentication	Reducing opportunities for the use of false or stolen identification data	Enhancing the identification and traceability of participants in economic transactions
Financial transparency	Detection of suspicious and fraudulent financial transactions in the digital environment	Detection and tracing of financial flows associated with corrupt activities	Combating money laundering and the concealment of illicit income
Digital tax governance	Enhancing the reliability of digital tax information exchange	Reducing opportunities for manipulation of tax information and non-transparent transactions	Detecting undeclared income and reducing opportunities for tax evasion
Data governance & interoperability	Secure data exchange and enhanced capacity to detect digital risks	Integration and analytical cross-checking of data to identify corruption risks	Data integration to detect undeclared and non-transparent economic activity

Source: compiled by the authors

these measures can enhance transaction traceability and strengthen the detection of undeclared activities, suspicious financial transactions, and corruption risks.

Particular attention should be paid to the interoperability of public information systems, as the existence of individual digital instruments does not generate a comprehensive effect when data remain fragmented and interagency exchange is limited. Harmonized data exchange procedures and risk-based analytics would enable information from different digital sources to be integrated for the timely detection of cyber threats, non-transparent financial transactions, tax violations, and other illicit economic activities.

Therefore, the application of the European digital resilience framework in Ukraine should involve not the mechanical transfer of individual EU instruments but their coordinated adaptation to national institutional conditions. This approach would combine alignment with the EU digital acquis with stronger cyber resilience, greater financial and tax transparency, reduced opportunities for corrupt and shadow practices, and enhanced economic security.

Conclusions. The study demonstrates that digital transformation strengthens the interconnections between cyber risks, corruption, and the shadow economy, limiting the effectiveness of their isolated regulation and increasing the importance of integrated approaches to digital resilience and economic security.

Based on the systematization of the European Union's regulatory and institutional instruments, the European digital resilience framework is proposed, integrating five interconnected components: cyber resilience of critical sectors, reliable digital identification, transparency of financial flows, digitalization of tax administration, and data governance and interoperability. Their coordinated functioning links the security of digital infrastructure with the transparency and traceability of economic transactions, creating a comprehensive approach to countering cyber risks, corruption, and the shadow economy.

The proposed framework can serve as a conceptual basis for improving digital governance and economic security policy. For Ukraine, its adaptation in the context of European integration can contribute to strengthening digital resilience, increasing financial and tax transparency, and improving the effectiveness of efforts to counter corrupt and shadow practices.

Future research should focus on developing a methodology for the integrated assessment of countries' digital resilience and empirically evaluating the effects of individual components of the European digital resilience framework on cyber risks, corruption, and the shadow economy.

REFERENCES:

1. Segovia-Ferreira M., Rubio-Hernan J., Cavalli A. R. & Garcia-Alfaro J. (2024). A survey on cyber-resilience approaches for cyber-physical systems. *ACM Computing Surveys*, no. 56(8), is. 202, pp. 1–37. DOI: <https://doi.org/10.1145/3652953>

2. Kott A., Golan, M. S., Trump, B. D., & Linkov, I. (2021). Cyber resilience: By design or by intervention? *Computer*, no. 54, is. 8, pp. 112–117. DOI: <https://doi.org/10.48550/arXiv.2201.11152>
3. Skierka I. (2023). When shutdown is no option: Identifying the notion of the digital government continuity paradox in Estonia's eID crisis. *Government Information Quarterly*, no. 40, is. 1, p. 101781. DOI: <https://doi.org/10.1016/j.giq.2022.101781>
4. Andersen T. B. (2009). E-government as an anti-corruption strategy. *Information Economics and Policy*, no. 21, is. 3, pp. 201–210. DOI: <https://doi.org/10.1016/j.infoecopol.2008.11.003>
5. Adam I. & Fazekas M. (2021). Are emerging technologies helping win the fight against corruption? A review of the state of evidence. *Information Economics and Policy*, no. 57, p. 100950. DOI: <https://doi.org/10.1016/j.infoecopol.2021.100950>
6. OECD. (2020). *OECD public integrity handbook*. OECD Publishing. DOI: <https://doi.org/10.1787/ac8ed8e8-en>
7. OECD. (2017). *Shining light on the shadow economy: Opportunities and threats*. OECD Publishing. DOI: <https://doi.org/10.1787/e0a5771f-en>
8. Tropina T. (2016). *Do digital technologies facilitate illicit financial flows?* World Development Report 2016 Background Paper. World Bank. Available at: <http://documents.worldbank.org/curated/en/896341468190180202>
9. Johnson S., Kaufmann D. & Zoido-Lobaton P. (1998). Regulatory discretion and the unofficial economy. *American Economic Review*, no. 88, is. 2. Available at: <https://ssrn.com/abstract=1116727>
10. Dreher A. & Schneider F. (2010). Corruption and the shadow economy: An empirical analysis. *Public Choice*, no. 144, is. 1–2, pp. 215–238. DOI: <https://doi.org/10.1007/s11127-009-9513-0>
11. Dobrovol'ska O. & Rozhkova M. (2024). The impact of digital transformation on the anti-corruption and cyber-fraud system. *Business Ethics and Leadership*, no. 8, is. 3, pp. 231–252. DOI: [https://doi.org/10.61093/bel.8\(3\).231-252.2024](https://doi.org/10.61093/bel.8(3).231-252.2024)
12. Yarovenko H., Bilovodska V., Bylbas R., Pankiv O., Baghirzade M., Niemi O. & Djakons D. (2025). Digital readiness of European countries to combat corruption and cyber threats: Panel analysis. *Business Ethics and Leadership*, no. 9, is. 2, pp. 238–265. DOI: [https://doi.org/10.61093/bel.9\(2\).238-265.2025](https://doi.org/10.61093/bel.9(2).238-265.2025)
13. European Parliament & Council of the European Union. (2022). Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS 2 Directive). Available at: <http://data.europa.eu/eli/dir/2022/2555/oj>
14. European Parliament & Council of the European Union. (2022). Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 (Text with EEA relevance). Available at: <http://data.europa.eu/eli/reg/2022/2554/oj>
15. European Parliament & Council of the European Union. (2024). Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act). Available at: <http://data.europa.eu/eli/reg/2024/2847/oj>
16. European Parliament & Council of the European Union. (2024). Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework. Available at: <http://data.europa.eu/eli/reg/2024/1183/oj>
17. European Parliament & Council of the European Union. (2024). Regulation (EU) 2024/1624 of the European Parliament and of the Council of 31 May 2024 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing. Available at: <http://data.europa.eu/eli/reg/2024/1624/oj>
18. European Parliament & Council of the European Union. (2024). Regulation (EU) 2024/1620 of the European Parliament and of the Council of 31 May 2024 establishing the Authority for Anti-Money Laundering and Countering the Financing of Terrorism and amending Regulations (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010. Available at: <http://data.europa.eu/eli/reg/2024/1620/oj>
19. European Parliament & Council of the European Union. (2024). Directive (EU) 2024/1640 of the European Parliament and of the Council of 31 May 2024 on the mechanisms to be put in place by Member States for the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Directive (EU) 2019/1937, and amending and repealing Directive (EU) 2015/849. Available at: <http://data.europa.eu/eli/dir/2024/1640/oj>
20. Council of the European Union. (2021). Council Directive (EU) 2021/514 of 22 March 2021 amending Directive 2011/16/EU on administrative cooperation in the field of taxation. Available at: <http://data.europa.eu/eli/dir/2021/514/oj>
21. Council of the European Union. (2020). Council Directive (EU) 2020/284 of 18 February 2020 amending Directive 2006/112/EC as regards introducing certain requirements for payment service providers. Available at: <http://www.legislation.gov.uk/id/eudr/2020/284>
22. Council of the European Union. (2020). Council Regulation (EU) 2020/283 of 18 February 2020 amending Regulation (EU) No 904/2010 as regards measures to strengthen administrative cooperation in order to combat VAT fraud. Available at: <http://data.europa.eu/eli/reg/2020/283/oj>
23. Council of the European Union. (2025). Council Directive (EU) 2025/516 of 11 March 2025 amending Directive 2006/112/EC as regards VAT rules for the digital age. Available at: <http://data.europa.eu/eli/dir/2025/516/oj>
24. European Parliament & Council of the European Union. (2022). Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act). Available at: <http://data.europa.eu/eli/reg/2022/2065/oj>

25. European Parliament & Council of the European Union. (2022). Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act). Available at: <http://data.europa.eu/eli/reg/2022/1925/oj>

26. European Parliament & Council of the European Union. (2022). Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act). Available at: <http://data.europa.eu/eli/reg/2022/868/oj>

27. European Parliament & Council of the European Union. (2023). Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act). Available at: <http://data.europa.eu/eli/reg/2023/2854/oj>

28. European Parliament & Council of the European Union. (2024). Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act). Available at: <http://data.europa.eu/eli/reg/2024/1689/oj>

UDC 338.2:004.05

JEL E26, H26, K42, O33

Inna Tiutiunyk, Doctor of Economics, Associate Professor, Head of the Department of Financial Technologies and Entrepreneurship, Sumy State University. **Xinxin Wang**, Postgraduate Student, Sumy State University. **Countering cyber risks, corruption and the shadow economy through a European digital resilience framework.**

The article examines the interrelationship between cyber risks, corruption, and the shadow economy in the context of deepening digital transformation. Based on the systematization of contemporary EU regulatory and institutional instruments, a conceptual model is proposed to provide a comprehensive response to interconnected digital and economic threats. The model comprises five functionally interconnected components: cyber resilience of critical sectors, reliable digital identification, transparency of financial flows, digitalization of tax administration, and data governance and interoperability. The mechanisms through which these components affect cyber risks, corruption, and the shadow economy are identified, demonstrating that their integrated application can simultaneously address different channels through which digital and economic threats emerge and spread, thereby generating a synergistic effect in strengthening economic security. The directions for applying the proposed approach in Ukraine in the context of national legislation alignment with the EU *acquis* are substantiated. The practical significance of the results lies in their potential use to improve public policy on digital governance, countering corruption and the shadow economy, and strengthening Ukraine's economic security.

Key words: digital resilience, cyber risks, corruption, shadow economy, economic security, digitalization, digital governance, European Union.

УДК 338.2:004.05

JEL E26, H26, K42, O33

Тютюнник Інна Володимирівна, доктор економічних наук, доцент, завідувач кафедри фінансових технологій і підприємництва, Сумський державний університет. **Ван Сін'сін**, аспірант, Сумський державний університет. **Протидія кіберризикам, корупції та тіньовій економіці на основі європейської концепції цифрової резильєнтності.**

У статті досліджено взаємозв'язок кіберризиків, корупції та тіньової економіки в умовах поглиблення цифрової трансформації та обґрунтовано необхідність переходу від фрагментарного регулювання цих загроз до інтегрованого підходу, заснованого на принципах цифрової резильєнтності. Обґрунтовано, що поширення цифрових фінансових інструментів, електронних державних сервісів, цифрових платформ і транскордонного обміну даними, з одного боку, підвищує ефективність економічних та управлінських процесів, а з іншого – формує нові канали реалізації кіберзагроз, корупційних практик, незаконних фінансових операцій та тіньової економічної діяльності. На основі систематизації сучасних нормативно-правових та інституційних інструментів Європейського Союзу запропоновано концептуальну модель цифрової резильєнтності, орієнтовану на комплексну протидію взаємопов'язаним цифровим та економічним загрозам. Модель об'єднує п'ять функціонально взаємопов'язаних компонентів: кіберстійкість критичної цифрової інфраструктури, надійну цифрову ідентифікацію, прозорість фінансових потоків, цифровізацію податкового адміністрування, а також управління даними та інтероперабельність. Визначено функціональні взаємозв'язки між зазначеними компонентами та обґрунтовано, що їх узгоджена дія забезпечує захищеність цифрової інфраструктури, надійну ідентифікацію учасників цифрових відносин, простежуваність фінансових потоків, прозорість податкових операцій та інтегроване використання даних. Визначено механізм впливу складових моделі на кіберризики,

корупцію та тіньову економіку та встановлено, що їх комплексне застосування дозволяє одночасно впливати на різні канали поширення цифрових та економічних загроз, формуючи синергетичний ефект у зміцненні економічної безпеки. Обґрунтовано напрями застосування запропонованого підходу в Україні в контексті наближення національного законодавства до законодавства ЄС, зокрема посилення кіберстійкості критичної цифрової інфраструктури, інтеграцію цифрової ідентифікації із системами фінансового моніторингу та податкового контролю, розвиток інтероперабельності державних інформаційних систем та ризик-орієнтованої аналітики. Практичне значення отриманих результатів полягає у можливості їх використання для вдосконалення державної політики у сфері цифрового врядування, протидії корупції та тіньовій економіці й зміцнення економічної безпеки України.

Ключові слова: цифрова резильєнтність, кіберризики, корупція, тіньова економіка, економічна безпека, цифровізація, цифрове врядування, Європейський Союз.