UDC 658:005.922.1:33:621.311]:338.1 DOI: 10.26906/EiR.2025.1(96).3771

JEL G21

VECTORS OF ENSURING ECONOMIC SECURITY OF ENERGY ENTERPRISES IN THE CONTEXT OF QUANTUM TRANSFORMATION

Alla Tkachenko*, Doctor of Economics, Professor,
National University «Zaporizhzhia Polytechnic»
Serhii Levchenko, Chief State Inspector of the Information Systems Support Department of the Department of Information Technologies of the Department of Internal Affairs and Communications of the Zaporizhzhya Region**

**ORCID 0000-0003-1061-4594*
***ORCID 0000-0002-6569 909X*

Стаття отримана редакцією 14.03.2025 р.
The article was received by editorial board on 14.03.2025

Introduction. The key to Ukraine's energy security during the war and post-war years is decentralisation and distributed generation, which inherently involve creating an extensive energy production and transmission system based on multiple sources located near consumers. Distributed generation has several significant advantages that make it particularly attractive for Ukraine. First, it significantly increases the country's energy sustainability and security by reducing dependence on centralised energy sources. This is especially important in times of war when centralised systems become vulnerable to large-scale attacks on energy infrastructure [1, p. 287]. In addition, distributed generation provides the ability to quickly restore power supply in the event of damage, which is critical to maintaining the vital activity of the population and the functioning of critical infrastructure [2, p. 300]. In combination with digital technologies, it allows to creation of 'smart grids' – Smart grids, which practically open up new opportunities for increasing the efficiency and flexibility of power systems, promote the development of alternative energy and electricity balancing, guarantee the accuracy of measuring electricity generation and consumption, provide two-way communication between producers and consumers, etc.

However, this combination is accompanied by specific challenges of digitalisation, in particular, the challenges of quantum transformation. With the advent of quantum computing technologies, which have the potential to perform calculations at a much faster speed than classical computers, certain threats arise for smart grids and, consequently, for the economic security of energy companies, which require further research.

Overview of recent research and publications. A review of recent research **sources** and publications shows that the issues of decentralisation and distributed generation of electricity, as well as the economic security of energy companies, are becoming increasingly relevant every day, as evidenced by numerous scientific publications. In particular, R.V. Vorobel, guided by the data of analytical centres, describes the current state, problems and prospects of energy in Ukraine [3]. Zhuravel Y.V., Lytvyn N.A. and Yara O.S. focus on the challenges faced by the energy sector due to Russia's full-scale invasion of Ukraine [4]. The researchers emphasise the need to stimulate this sector's revival, support/encourage energy producers from alternative sources, and develop distributed generation. Gavrylenko Y. and Deriy V. use specific examples to prove that the key factors that contribute to progress in the implementation of distributed generation is regulatory policy, which should be aimed not only at stimulating the development of distributed generation but also at protecting it from the impact of exogenous factors, in particular cyberattacks and cyber incidents [5]. For example, Kioskli, K., Fotis, T., Nifakos, S., Mouratidis, H. [6], using

the example of critical infrastructure, substantiate how vulnerable and unprotected it is from cyber-attacks, as well as how cyberspace is now demonstrating an increasing number of difficulties related to cybersecurity. The authors emphasise that users (in particular, energy companies) must comply with cyber hygiene rules. Moreover, as emphasised by A. Fikry, M. I. Hamzah, Z. Hussein, A. J. Abdul and K. A. Abu Bakar [7], in the era of quantum technologies, understanding and active implementation of sustainable cyber hygiene practices are imperative measures to strengthen the security of the digital landscape of critical infrastructure. The importance of cyber hygiene is also emphasised by Cain, A. A., Edwards, M. E., & Still, J. D. [8]. The authors substantiate that well-developed cybersecurity risk management and strict cyber hygiene behaviour ensure cyber resilience and create a line of defence for the economic security of enterprises. Iqbal H. Sarker, Helge Janicke, Ahmad Mohsin, Asif Gill, and Leandros Maglaras [9] emphasise that to implement cyber hygiene measures, energy enterprises should be guided by a taxonomy, standards, rules, etc. According to T. Ncubukezi, L. Mwansa and F. Rosaries [10], the absence of such regulations and guidelines for creating mature cybersecurity hygiene leads to its sluggishness and, accordingly, to the painful consequences of cyber incidents and cyber attacks for companies. Therefore, energy companies must act now to understand what a safe quantum transition should look like for them [11], which is exactly what further research on this topic requires.

Objectives of the article. The article's purpose is to comprehensively study the possible challenges of quantum transformation to distributed power generation and the economic security of energy enterprises.

The main material of the study. The events of the last decade in Ukraine and the introduction of martial law in 2022 have led to an increase in the total number of threats that cause damage to Ukrainian energy enterprises, among which cyber threats are among the most dangerous. Their manifestations in recent years have been highly dynamic and have serious consequences for the economic security of energy companies.

Currently, the implementation of cybersecurity measures for energy enterprises is regulated by the Law of Ukraine 'On Critical Infrastructure' of 21.09.2021 No. 1882-IX [12] and the Requirements for Cybersecurity of the Fuel and Energy Sector of Critical Infrastructure, approved by the Order of the Ministry of Energy of Ukraine of 15 December 2022 No. 417 (hereinafter – the Requirements) [13], which provide for the introduction of a systematic process for determining and assessing their cyber resilience and building a current cybersecurity profile. A detailed study of these regulations shows that with the accelerated development of digital technologies, they do not fully regulate cybersecurity issues, especially those related to quantum transformation, with which energy companies are rapidly approaching the 'danger zone' (Fig. 1).

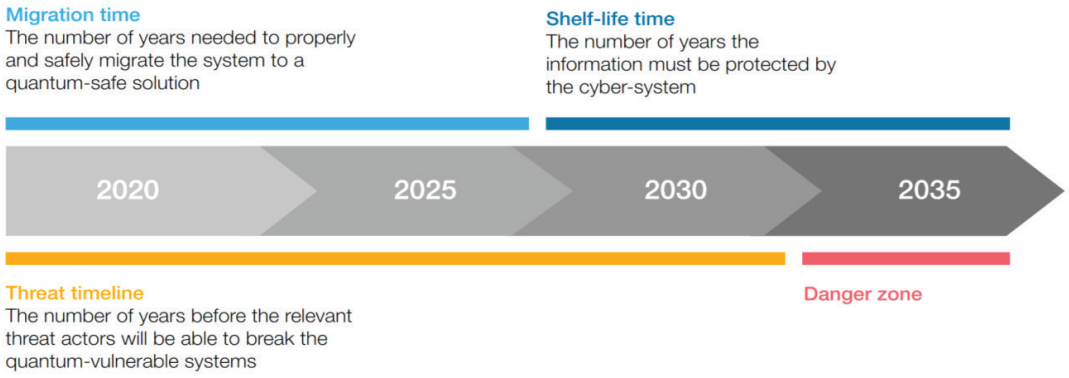

Figure 1. Chronology of quantum threats

Source: [11; 14]

The 2024 Cybersecurity Assessment shows the growing complexity of the cyber landscape, which has profound and far-reaching implications for energy companies. This complexity is caused by many factors, including escalating geopolitical tensions and the rapid introduction of new technologies, which contribute to the emergence of new vulnerabilities, their complexity and scale, etc. (Fig. 2).

It should be noted that quantum computers are a new computing device capable of performing specific calculations, some of which cannot be performed on classical computers. In classical computing, all information is represented in bits (in the form of 0s and 1s). Quantum computers use cubits that combine 0s and 1s simultaneously (the so-called 'superposition'). By using the principles of superposition and entanglement (the ability of distant cubits to correlate with each other), quantum computing enables a new way of storing and processing information.

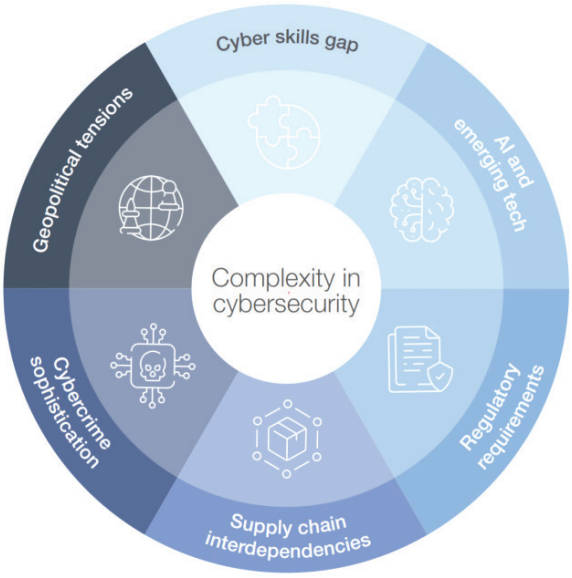

Figure 2. Factors complicating the nature of energy industry cybersecurity

Source: [15]

These new blocks are used to build quantum algorithms, which sometimes significantly accelerate the ability to solve computational problems (Fig. 3).

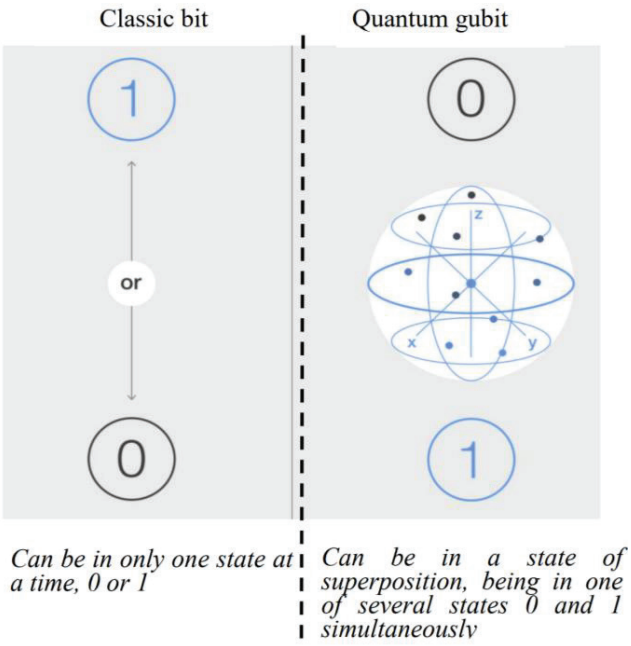

Figure 3. Abilities of a quantum computer versus a classical one

Source: [15]

Several quantum algorithms demonstrate the potential to achieve significant acceleration compared to classical algorithms. Therefore, leading energy experts predict the quantum threat will materialise in 3-10 years.

However, this timeframe is highly debatable, as it could be even shorter - especially given the information asymmetry and secrecy surrounding quantum-computing advances used by certain countries seeking strategic advantage.

In today's nascent quantum cybersecurity market, a number of efforts are underway to develop technologies to mitigate quantum threats. These technologies are not a perfect solution, but they can be used individually or in combination for certain applications, including

– Post-quantum cryptography (PQC) uses new mathematical public-key cryptography algorithms designed to be impervious to Shor's algorithm attack. PQC is capable of fundamentally replacing existing algorithms with insecure cryptographic algorithms. However, all known PQC schemes (standardised by NIST) have performance drawbacks. In particular, they require long keys and long processing times compared to current algorithms (e.g., RSA, ECC), which complicates their application [11];

– Quantum Key Distribution (QKD) is the most well-known class of quantum protocols designed to exchange secret keys, which are then used to encrypt communications using quantum-secure symmetric key algorithms. QKD is based on quantum methods for creating secure communication channels that can be used to distribute encryption keys. QKD can complement the use of PQC and other cryptographic algorithms, thus providing a new secure key distribution method. However, this technology requires significant investment in specialised hardware. In addition, a separate authentication channel is required, which complicates the solution, unlike modern classical methods where authentication is part of the protocol [11];

– Quantum random number generation (QRNG) uses fundamental quantum properties to generate random numbers with high entropy, which plays a crucial role in cryptography for cryptographic key generation and some algorithms. Therefore, QRNG creates better-verified entropy sources than conventional processes, which can improve security under certain conditions. However, some applications require repeatability, which takes additional time [11].

However, the impact of quantum threats on energy companies is not limited to cryptographic algorithms, as their cascading effects can be potentially large. This is one of the reasons why energy companies should already consider a migration plan and take a crypto-agility position that will allow them to quickly update in the event of cyber-attacks [15] (Fig. 4).

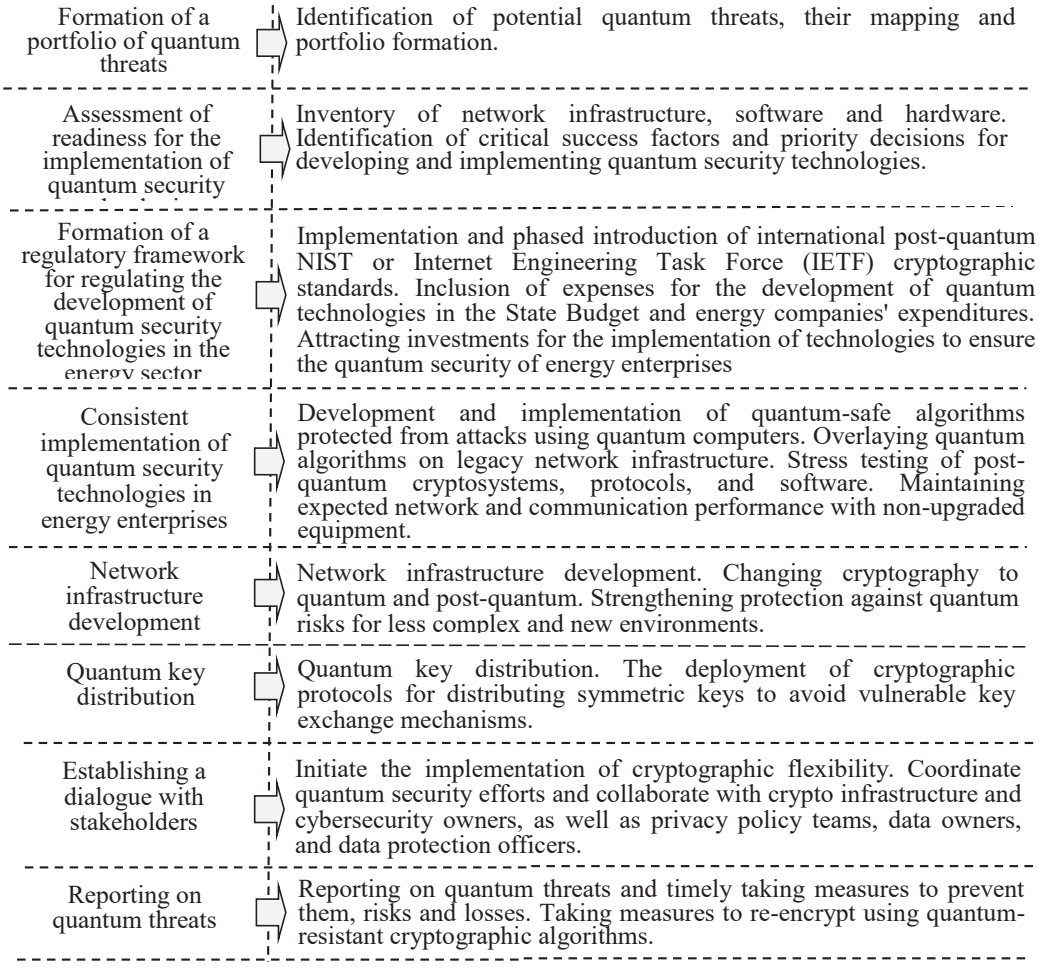

Figure 4. Algorithm of the sequence of actions to create a 'line of protection' of electric power enterprises from cyber-attacks and cyber incidents in the context of quantum transformation

Source: author's vision

The creation of a 'line of defence' of electricity from cyber-attacks and cyber incidents in the context of and cyber incidents in the context of quantum transformation according to the proposed algorithm will allow to prevent their impact or minimise their consequences and thus guarantee the preservation of economic security of enterprises in the context of growing external threats.

Conclusions. Thus, according to the results of the study, it is stated that ensuring Ukraine's energy security during the war and post-war reconstruction is closely linked to the processes of decentralisation and the development of distributed

Generation. These approaches involve forming an extensive energy infrastructure based on numerous localised energy sources close to end consumers. The transition to distributed generation has a number of important advantages. Still, its effective implementation requires widespread use of digital technologies, the use of which gives rise to cyber challenges, cyber incidents and cyber-attacks. Their manifestations in recent years have been highly dynamic and have serious consequences for the economic security of energy companies.

Special attention is paid to the impact of quantum transformation on the cybersecurity of energy companies, as quantum computers can instantly decrypt modern cryptographic algorithms, creating new challenges for the protection of power systems. The article analyses the evolution of quantum threats and the factors that complicate the cyber resilience of energy companies. The differences between classical and quantum computing and examples of technologies aimed at mitigating the risks associated with cyber-attacks on critical infrastructure.

The necessity of implementing comprehensive measures to prevent quantum threats and minimise the consequences of cyber incidents both at the state level and within the energy sector, territorial communities and energy enterprises themselves. An algorithm of actions is proposed of actions to create an effective 'line of defence' for electricity companies from cyber-attacks and threats in the context of quantum transformation.

REFERENCES:

1. Chaplynska, N., & Makeienko, P. (2023) Innovative solutions for ensuring energy security of Ukraine and the world [Innovative solutions for ensuring energy security of Ukraine and the world]. *Akademichnyi ohliad – Academic review*, vol. 2 (59), pp. 284–297.

2. Tkach, D. K., & Vasylieva, O. V. (2025) Enerhetychnyi sektor Ukrainy u voiennyi ta pisliavoiennyi period: stratehichni pidkhody ta innovatsiini rishennia. [Ukraine's energy sector in the war and post-war period: strategic approaches and innovative solutions]. *European Scientific Journal of Economic and Financial Innovation,* vol. 1 (15), pp. 300–308. DOI: http://doi.org/10.32750/2025-0126

3. Vorobel, R. V. (2024) Vidnovliuvalna enerhetyka v Ukraini: suchasnyi stan, problemy ta perspektyvy rozvytku [Renewable energy in Ukraine: current state, problems and development prospects]. *Mizhnarodnyi naukovyi zhurnal "Internauka" – International scientific journal "Internauka*", vol. 1 (81). DOI: https://doi.org/10.25313/2520-2294-2024-1

4. Zhuravel, Ya. V., Lytvyn, N. A., & Yara, O. S. (2023) Rozvytok zakonodavstva pro stymuliuvannia vykorystannia alternatyvnykh dzherel enerhii: administratyvno-pravovyi aspect [Development of Legislation on Stimulating the Use of Alternative Energy Sources: Administrative and Legal Aspect]. *Pravo i suspilstvo – Law and Society*, vol. 1, pp. 166–173. DOI: https://doi.org/10.32842/2078-3736/2023.2.1.26

5. Havrylenko, Ya., & Derii, V. (2024) Formuvannia pravovykh zasad funktsionuvannia ta rozvytku "zelenoi"enerhetyky [Formation of the legal framework for the functioning and development of 'green' energy]. *Systemni doslidzhennia v enerhetytsi*, vol. 4 (80), pp. 120–133. DOI: https://doi.org/10.15407/srenergy2024.04.120

6. Kioskli, K., Fotis, T., Nifakos, S., & Mouratidis, H. (2023) The Importance of Conceptualising the Human-Centric Approach in Maintaining and Promoting Cybersecurity-Hygiene in Healthcare 4.0 . *MDPI,* no. 13 (6). DOI: https://doi.org/10.3390/app13063410

7. Fikry, A., Hamzah, M., Hussein, Z., Abdul, A., & Bakar, K. (2024) Defining the Beauty of Cyber Hygiene: A Retrospective Look. *IEEE Engineering Management Review*, vol. 52*,* no. 2, pp. 174–180. DOI: https://doi.org/10.1109/EMR.2024.3361023

8. Cain, A. A., Edwards, M. E., & Still, J. D. (2018) An exploratory study of cyber hygiene behaviors and knowledge. *Journal of Information Security and Applications*, vol. 42, pp. 36–45. DOI: https://doi.org/10.1016/j.jisa

9. Sarker, I. H., Janicke, H., Mohsin, A., Gill, A., & Maglaras, L. (2024) Explainable AI for cybersecurity automation, intelligence and trustworthiness in digital twin: Methods, taxonomy, challenges and prospects. *ICT Express*, vol. 10, is. 4, pp. 935–958. https://doi.org/10.1016/j.icte.2024.05.007.

10. Ncubukezi, T., Mwansa, L., & Rocaries, F. (2020) A Review of the Current Cyber Hygiene in Small and Medium-sized Businesses.*Technology and Secured Transactions – 2020: 15th International Conference for Internet*. London. DOI: https://doi.org/10.23919/ICITST51030.2020.9351339

11. Jurgens, J., Kohn, S., & Souta, C. (2022) Transitioning to a Quantum-Secure Economy. World Economic Forum. Available at: https://www3.weforum.org/docs/WEF_Transitioning%20to_a_Quantum_Secure_Economy_2022.pdf (accessed March 1, 2025).

12. Verkhovna Rada of Ukraine. (2021, September 21). *On critical infrastructure: The Law of Ukraine No. 1882-IX.* Available at: https://zakon.rada.gov.ua/laws/show/1882-20#Text (accessed March 3, 2025).

13. Ministry of Energy of Ukraine. (2022, December 15). *Cybersecurity requirements for the fuel and energy sector of critical infrastructure: Order No. 417.* Available at: https://zakon.rada.gov.ua/laws/show/z0249-23#n14 (accessed March 4, 2025).

14. Shkuratov, O., Antonova, L., & Dziuba, R. (2024) Innovatsiini mekhanizmy ta realizatsiia derzhavnoi ekonomichnoi polityky pisliavoiennoho vidnovlennia Ukrainy: kvantovi transformatsii yak draiver rozvytku [I Innovative mechanisms and implementation of the state economic policy of post-war recovery of Ukraine: quantum transformations as a driver of development]. *Public Administration and Regional Development*, vol. 26, pp. 1254–1272. DOI: https://doi.org/10.34132/pard2024.26.08

15. Jurgens, J., & Cin, P. (2025) Global Cybersecurity Outlook 2025. Insight report World Economic Forum's. Available at: https://www.weforum.org/publications/global-cybersecurity-outlook-2025/ (accessed March 1, 2025).

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Chaplynska N., Makeienko P. Innovative solutions for ensuring energy security of Ukraine and the world. *Академічний огляд.* 2023. № 2 (59). С. 284–297.

2. Ткач Д.К., Васильєва О.В. Енергетичний сектор України у воєнний та післявоєнний період: стратегічні підходи та інноваційні рішення. *European scientific journal of Economic and Financial innovation.* 2025. № 1 (15). С. 300–308. DOI: http://doi.org/10.32750/2025-0126

3. Воробель Р.В. Відновлювальна енергетика в Україні: сучасний стан, проблеми та перспективи розвитку. *Міжнародний науковий журнал «Інтернаука».* 2024. № 1 (81). DOI: https://doi.org/10.25313/2520-2294-2024-1

4. Журавель Я.В., Литвин Н.А., Яра О.С. Розвиток законодавства про стимулювання використання альтернативних джерел енергії: адміністративно-правовий аспект. *Право і суспільство.* 2023. Т. 1. С. 166–173. DOI: https://doi.org/10.32842/2078-3736/2023.2.1.26

5. Гавриленко Я., Дерій В. Формування правових засад функціонування та розвитку «зеленої» енергетики. *Системні дослідження в енергетиці.* 2024. № 4(80). С. 120–133. DOI: https://doi.org/10.15407/srenergy2024.04.120

6. Kioskli, K., Fotis, T., Nifakos, S., Mouratidis, H. The Importance of Conceptualising the Human-Centric Approach in Maintaining and Promoting Cybersecurity-Hygiene in Healthcare 4.0. *MDPI.* 2023. No. 13(6). DOI: https://doi.org/10.3390/app13063410

7. Fikry A., Hamzah M., Hussein Z., Abdul A. and Bakar K. Defining the Beauty of Cyber Hygiene: A Retrospective Look. *IEEE Engineering Management Review.* 2024. Vol. 52, No. 2, Pp. 174–180. DOI: https://doi.org/10.1109/EMR.2024.3361023

8. Cain, A.A., Edwards, M.E., & Still, J.D. An exploratory study of cyber hygiene behaviors and knowledge. *Journal of Information Security and Applications*, 2018, Vol. 42, Pp. 36–45. DOI: https://doi.org/10.1016/j.jisa

9. Iqbal H. Sarker, Helge Janicke, Ahmad Mohsin, Asif Gill, Leandros Maglaras. Explainable AI for cybersecurity automation, intelligence and trustworthiness in digital twin: Methods, taxonomy, challenges and prospects. *ICT Express.* 2024. Vol. 10. Pp. 935-958. DOI: https://doi.org/10.1016/j.icte.2024.05.007.

10. Ncubukezi T., Mwansa L. and Rosaries F. A Review of the Current Cyber Hygiene in Small and Medium-sized Businesses. *15th International Conference for Internet Technology and Secured Transactions (ICITST)*, London, United Kingdom, 2020. Pp. 1–6. DOI: https://doi.org/10.23919/ICITST51030.2020.9351339

11. Jurgens J., Kohn S., Souta C. Transitioning to a Quantum-Secure Economy. World Economic Forum. 2022. URL: https://www3.weforum.org/docs/WEF_Transitioning%20to_a_Quantum_Secure_Economy_2022.pdf (дата звернення: 01.03.2025).

12. Про критичну інфраструктуру. Закон України від 21.09.2021 р. №1 882 – IX. URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text (дата звернення: 03.03.2025).

13. Вимоги з кібербезпеки паливно-енергетичного сектору критичної інфраструктури. Наказ Міністерства енергетики України від 15 грудня 2022 р. № 417. URL: https://zakon.rada.gov.ua/laws/show/z0249-23#n14 (дата звернення: 04.03.2025).

14. Шкуратов О., Антонова Л., Дзюба Р. Інноваційні механізми та реалізація державної економічної політики післявоєнного відновлення України: квантові трансформації як драйвер розвитку. *Public Administration and Regional Development.* 2024. № 26. С. 1254–1272. DOI: https://doi.org/10.34132/pard2024.26.08

15. Jurgens J., Cin P. Global Cybersecurity Outlook 2025. Insight report World Economic Forum's. 2025. URL: https://www.weforum.org/publications/global-cybersecurity-outlook-2025/ (дата звернення: 01.03.2025).

UDC 658:005.922.1:33:621.311]:338.1

JEL G21

Tkachenko Alla, Doctor of Economics, Professor, National University "Zaporizhzhia Polytechnic", **Levchenko Serhii,** Chief State Inspector of the Information Systems Support Department of the Department of Information Technologies of the Department of Internal Affairs and Communications of the Zaporizhzhya Region.

Vectors of ensuring economic security of energy enterprises in the context of quantum transformation.

The article emphasises that the key to Ukraine's energy security during the war and post-war years is decentralisation and distributed generation, which inherently involve creating an extensive energy production and transmission system based on multiple sources located near consumers. It is emphasised that distributed power generation has a

number of advantages but requires the use of digital technologies, which, with the evolution of digitalisation, are increasingly accompanied by cyber-attacks and cyber incidents. As practice shows, their manifestations seriously affect energy companies' economic security. It is emphasised that with quantum transformation, cyber threats are further exacerbated since quantum computers are quite powerful and instantly destroy the cyphers for access to information and the power system, thus causing large-scale losses to energy enterprises. Repeatability, which requires additional time. It is substantiated that energy companies should already consider a migration plan and take a crypto-agility position that will allow them to quickly update in the event of cyber-attacks. The author considers the chronology of quantum threats and factors that complicate the cybersecurity of energy enterprises. The author points out the abilities of quantum computers compared to classical ones. Examples of technologies designed to mitigate quantum threats to critical infrastructure are given. It is substantiated that measures to prevent quantum threats and minimise the consequences of cyber-attacks and cyber incidents should be taken both at the level of the State and the energy sector, and at the level of territorial communities and energy enterprises. An algorithm for the sequence of actions to create a 'line of defence' of electric power enterprises against cyber-attacks and cyber incidents in the context of quantum transformation is proposed. It is substantiated that the introduction of a 'line of defence' of electric power enterprises against cyber-attacks and cyber incidents in the context of quantum transformation according to the proposed algorithm will prevent their impact or minimise their consequences and thus guarantee the preservation of economic security of enterprises in the context of growing external threats.

Keywords: economic security of an enterprise, economic losses, severe economic consequences, 'lines of defence' of electric power enterprises, cyber defence, cyber hygiene.

УДК 658:005.922.1:33:621.311]:338.1
JEL G21

Ткаченко Алла Михайлівна, доктор економічних наук, професор, Національний університет «Запорізька політехніка». **Левченко Сергій Анатолійович,** головний державний інспектор відділу супроводження інформаційних систем управління інформаційних технологій ГУНП в Запорізькій області. **Вектори забезпечення економічної безпеки підприємств енергетики в умовах квантової трансформації.**

В статті наголошено, що ключем до енергетичної безпеки України у роки війни та повоєнні роки є децентралізація та розподілена генерація, які за своєю сутністю передбачають створення розгалуженої системи виробництва та передачі енергії, що базується на множинних джерелах, розташованих безпосередньо поблизу споживачів. Підкреслено, що розподілена генерація електроенергії має цілий ряд переваг, втім потребує на застосування цифрових технологій, які з еволюцією цифровізації, все більше супроводжуються кібератаками та кіберінцидентами. Їх прояви, як свідчить практика, мають досить тяжкі наслідки для економічної безпеки підприємств енергетики. Акцентовано, що з квантовою трансформацією питання кіберзагроз ще більше загострюється, оскільки квантові комп'ютери є досить потужні й миттєво руйнують шифри доступу до інформації та енергосистеми, завдаючи у такий спосіб масштабних втрат енергетичним підприємствам. повторюваності, що потребує на додатковий час. Обґрунтовано, що підприємства енергетики повинні вже зараз обмірковувати план міграції та зайняти позицію криптоспритності, яка дозволить їм швидко оновлюватися у разі виникнення кібератак. Розглянуто хронологію квантових загроз та фактори, що ускладнюють кібербезпеку підприємств енергетики. Вказано на здібності квантових комп'ютерів проти класичних. Приведено приклади технологій, призначених для пом'якшення квантових загроз об'єктам критичної інфраструктури. Обгрунтовано, що заходи з упередження квантових загроз й мінімізації наслідків кібератак та кіберінцедентів мають здійснюватися як на рівні держави та галузі енергетики, так і на рівні територіальних громад та підприємств енергетики. Запропоновано алгоритм послідовності дій зі створення «лінії захисту» підприємств електроенергетики від кібератак та кіберінцидентів в умовах квантової трансформації. Обгрунтовано, що запровадження «лінії захисту» підприємств електроенергетики від кібератак та кіберінцедентів в умовах квантової трансформації за запропонованим алгоритмом дозволить упередити їх вплив чи мінімізувати їх наслідки, й таким чином гарантувати збереження економічної безпеки підприємств у контексті зростаючих зовнішніх загроз.

Ключові слова: економічна безпека підприємства, економічні втрати, тяжкі економічні наслідки, «лінії захисту» підприємств електроенергетики, кіберзахист, кібергігієна.