МЕТОДИКА НАВЧАННЯ

УДК 004.8:37.018 doi.org/10.33298/2226-8553.2025.1.42.26

Двуліт З.П.

ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В ОСВІТНЬОМУ ПРОЦЕСІ

У статті розглянуто основні аспекти застосування штучного інтелекту (ШІ) в освітньому процесі. Основна увага приділяється персоналізації навчання, автоматизації оцінювання та вдосконаленню викладацької діяльності через використання інтелектуальних систем. Проведено SWOT-аналіз впровадження ШІ для трьох ключових груп учасників освітнього процесу: студентів, викладачів і стейкхолдерів. У роботі акцентується на перевагах і викликах, пов'язаних із використанням ШІ, таких як персоналізація освітніх траєкторій, ефективність зворотного зв'язку, етичні аспекти та цифрова нерівність. Результати дослідження допомагають зрозуміти, як інтеграція ШІ сприяє підвищенню якості освіти, професійному розвитку викладачів і підготовці студентів до роботи в умовах цифрової трансформації.

Ключові слова: *штучний інтелект, освітній процес, SWOT- аналіз, персоналізоване навчання, автоматизація*

Постановка проблеми. Сучасний світ освіти перебуває у стані глибокої трансформації, спричиненої стрімким розвитком цифрових технологій та інтеграцією штучного інтелекту (ШІ) у різні аспекти навчального процесу. Традиційні методики навчання, що базуються на пасивному засвоєнні знань, поступаються місцем активним і адаптивним підходам, які орієнтовані на індивідуальні потреби учнів. У зв'язку з цим виникає необхідність осмислення нових можливостей і викликів, що супроводжують впровадження ШІ в освітню практику.

Застосування штучного інтелекту в освітньому процесі відкриває широкі перспективи для підвищення ефективності навчання, забезпечення персоналізованого підходу до кожного студента та автоматизації рутинних завдань викладачів. Зокрема, інтерактивні платформи, адаптивні навчальні системи та інтелектуальні асистенти надають можливість гнучко налаштовувати освітній контент відповідно до потреб студентів. Однак, ці інновації також викликають низку проблем, пов'язаних із етичними аспектами, цифровою нерівністю та захистом персональних даних.

У контексті викладання до прикладу для студентів-економістів та менеджерів питання впровадження ШІ набуває особливої актуальності, оскільки ці спеціалісти формують майбутнє бізнесу та управління. Вивчення та використання інструментів ШІ у навчанні можуть допомогти їм розвивати аналітичне мислення, приймати обґрунтовані рішення на основі даних і адаптуватися до швидкоплинних змін ринкових умов.

Проте, попри численні переваги, інтеграція ШІ у викладання має низку викликів, які потребують дослідження.

Аналіз останніх досліджень і публікацій. Програми штучного інтелекту (ШІ) відіграють важливу роль у трансформації освітніх систем, сприяючи вирішенню проблем доступу до освіти та покращенню якості навчання. ШІ активно впроваджується у соціальні роботи, розумне навчання та інтелектуальні системи репетиторства, створюючи можливості для доступного та ефективного навчання. Крім того, автори зазначають, що ШІ здатний покращити навчальний процес за рахунок автоматизації рутинних завдань, таких як оцінювання знань, віртуальне моделювання та навчальна аналітика [1].

Одні автори [2] акцентують увагу на тому, що ШІ не тільки підвищує ефективність навчання студентів, а й зменшує навантаження на викладачів і адміністративний персонал. Наприклад, автоматизовані системи можуть аналізувати дані про навчальний процес, оцінювати прогрес студентів та навіть передбачати потенційні проблеми у навчанні. Це дозволяє викладачам більше

зосереджуватися на педагогічній діяльності.

Інші [3] розглядають роль ШІ у підтримці навчання впродовж життя. Адаптивні навчальні середовища, створені на основі ШІ, забезпечують гнучкість та інклюзивність. Ці інструменти допомагають студентам із різними потребами отримувати доступ до освітніх ресурсів, розроблених спеціально для їхніх індивідуальних вимог.

Одним із найважливіших аспектів застосування ШІ в освіті є персоналізація навчання. У роботі [4] зазначається, що ШІ дозволяє створювати персоналізовані траєкторії навчання, адаптуючи навчальний контент до потреб студентів. Також автори підкреслюють значення зворотного зв’язку в реальному часі, який дає змогу швидко коригувати процес навчання, підвищуючи його ефективність.

Zawacki-Richter та ін. [5] вказують, що застосування ШІ у вищій освіті охоплює такі завдання, як профілювання студентів, адаптивні системи навчання та інтелектуальні системи викладання. Вони також звертають увагу на необхідність інтеграції ШІ у педагогічну практику, щоб покращити якість викладання та надати студентам інструменти для самостійного навчання.

Дослідження [6] підкреслює, що в освітньому процесі ШІ здебільшого використовується для аналізу поведінки, підтримки викладання та автоматизації адміністративних завдань. Автори наголошують на важливості машинного навчання та інтелектуальних систем, які сприяють продуктивному навчанню.

Попри численні переваги, дослідники вказують на ризики, пов’язані з використанням ШІ в освіті. Наприклад, необхідність захисту даних студентів та уникнення зловживань викликають особливу увагу. Крім того, важливо забезпечити правильне використання ШІ, щоб уникнути ризику надмірної автоматизації, яка може зменшити роль людини у процесі навчання.

Таким чином, дослідження показують, що ШІ має значний потенціал для трансформації освіти. Його впровадження дозволяє підвищити якість навчання, зробити освіту доступнішою та інклюзивнішою, а також розширити можливості як для студентів, так і для викладачів. Водночас, важливо враховувати етичні, правові та технічні аспекти, щоб максимізувати переваги і мінімізувати ризики використання ШІ у навчальному процесі.

Мета дослідження. Метою статті є дослідження впровадження штучного інтелекту в освітній процес, проведення SWOT-аналізу його застосування для студентів, викладачів і стейкхолдерів, а також визначення переваг і викликів, пов’язаних із використанням цих технологій.

Основні результати дослідження. Штучний інтелект активно впроваджується в навчальний процес, надаючи нові можливості для персоналізації навчання, автоматизації адміністративних завдань та покращення якості освіти. Використання ШІ в освітньому процесі створює передумови для ефективнішої організації навчання та професійного розвитку викладачів. Проведене дослідження за даною проблемою, дозволило виділити такі основні напрямки застосування ШІ в освіті:

1. Персоналізоване навчання. ШІ дозволяє створювати індивідуальні навчальні шляхи, адаптуючи зміст до потреб студентів. Це покращує їхній досвід навчання та підвищує якість освіти [2, 7]. Використання інтелектуальних систем дозволяє аналізувати навчальні результати студентів і коригувати навчальний процес відповідно до їхніх сильних і слабких сторін [8].

2. Оцінювання та зворотний зв'язок. Автоматизація процесів оцінювання є однією з найпоширеніших сфер застосування ШІ. Системи штучного інтелекту забезпечують швидкий та об'єктивний аналіз робіт студентів, надаючи їм зворотний зв'язок [9]. Це дозволяє викладачам зосередитися на інших важливих аспектах навчання, зокрема на роботі з відстаючими студентами [5].

3. Інтелектуальні системи навчання. Віртуальні середовища навчання, які використовують ШІ, забезпечують доступ до матеріалів у режимі 24/7. Студенти можуть самостійно обирати темп навчання, що сприяє розвитку їхньої самостійності та професійних компетенцій [2; 10]. Використання роботизованих асистентів також сприяє полегшенню процесу навчання для студентів і зниженню навантаження на викладачів [11].

4. Адміністративні завдання. ШІ значно спрощує виконання адміністративних завдань, таких як управління записами студентів, складання розкладів та облік відвідуваності [2, 7]. Автоматизація цих процесів дозволяє зосередитися на стратегічних аспектах освітньої діяльності [12].

В цьому контексті варто зазначити, що вплив ШІ на професійний розвиток викладачів відбувається шляхом:

1. Підвищення інформаційної грамотності. ШІ сприяє підвищенню інформаційної грамотності викладачів, забезпечуючи їх доступ до сучасних інструментів аналізу та візуалізації даних [13]. Це дозволяє їм більш ефективно використовувати наявні ресурси для організації навчального процесу.

2. Підтримка професійного розвитку. Викладачі визнають, що інтеграція ШІ в освітній процес сприяє їхньому професійному розвитку, надаючи нові можливості для навчання та вдосконалення [14]. Вони можуть опановувати нові підходи до роботи зі студентами та впроваджувати сучасні методики навчання.

3. Адаптація навчальних матеріалів. ШІ дозволяє адаптувати навчальні матеріали відповідно до індивідуальних потреб студентів, що сприяє покращенню їхнього досвіду навчання та підвищенню якості освіти [15].

4. Розвиток нових методик викладання. Використання ШІ сприяє впровадженню нових підходів до викладання, що дозволяє викладачам ефективніше взаємодіяти зі студентами та покращувати результати навчання [16].

5. Підтримка у прийнятті рішень. ШІ може аналізувати великі обсяги даних про успішність студентів, допомагаючи викладачам приймати обґрунтовані рішення щодо індивідуальних навчальних планів та методів викладання [17].

Штучний інтелект поступово стає невід’ємною частиною освітнього процесу, надаючи нові можливості для вдосконалення навчання та управління освітніми установами. Його застосування охоплює автоматизацію рутинних завдань, персоналізоване навчання, аналітику даних і підтримку в ухваленні рішень. Проте впровадження таких технологій потребує ретельного аналізу, оскільки поряд із перевагами існують виклики та ризики, які впливають на різні групи учасників освітнього процесу.

Використання ШІ піднімає важливі етичні питання, зокрема щодо конфіденційності даних студентів, прозорості алгоритмів та можливого упередження в оцінюванні [9, 11]. Розробка етичних стандартів для використання ШІ є одним із пріоритетних завдань освітньої спільноти.

Для успішного впровадження ШІ в освітній процес потрібна належна підготовка викладачів, щоб вони могли ефективно використовувати ці технології. Інвестиції у підвищення кваліфікації викладачів є необхідною умовою для досягнення позитивних результатів.

Штучний інтелект значно змінює освітній процес, надаючи можливості для персоналізації навчання, автоматизації оцінювання та адміністративних завдань. Він також сприяє професійному розвитку викладачів, підвищуючи їхню інформаційну грамотність і розширюючи інструментарій. Однак важливо враховувати етичні аспекти та виклики, пов'язані з впровадженням ШІ, щоб забезпечити його відповідальне використання.

Відтак, у даному дослідженні проведено SWOT-аналіз застосування ШІ у сфері освіти для трьох ключових груп: студентів, викладачів і стейкхолдерів. Стейкхолдери у контексті освіти – це всі зацікавлені сторони, які впливають на процеси навчання або зазнають впливу цих процесів. У контексті впровадження ШІ до стейкхолдерів належать:

1. Керівництво закладів освіти – ректори, декани, адміністрація, які приймають рішення про інвестиції в ШІ.
2. Освітні установи – як державні, так і приватні організації, що фінансують та впроваджують ШІ.
3. Розробники технологій – компанії та стартапи, які створюють ШІ-інструменти для освіти.
4. Держава та органи управління освітою – організації, які регулюють використання технологій і забезпечують правові та етичні рамки.
5. Батьки – зацікавлені у підвищенні якості освіти та успішності своїх дітей.

6. Роботодавці – компанії, які очікують від випускників знань і навичок, розвинених із використанням сучасних технологій.

7. Громадські організації – аналітичні центри, фонди, які працюють над покращенням доступності та якості освіти.

Ці групи мають різні очікування від впровадження ШІ. Кожна група має свої унікальні переваги, слабкі сторони, можливості та загрози, які необхідно враховувати при впровадженні інноваційних технологій у навчальний процес (табл. 1, табл. 2, табл. 3).

Таблиця 1 – SWOT-аналіз ШІ у навчанні студентів

Сильні сторони	Слабкі сторони
Персоналізоване навчання.	Нерівний доступ до технологій (цифровий розрив).
Доступ до навчальних ресурсів 24/7.	Можливість залежності від технологій.
Автоматичне оцінювання та швидкий зворотний зв'язок.	Обмежені можливості для розвитку креативності у структурованих завданнях.
Підтримка студентів із особливими потребами.	Можливість зниження розвитку критичного мислення.
Можливості	Загрози
Збільшення доступу до глобальних освітніх ресурсів.	Загроза витоку особистих даних студентів.
Підвищення мотивації через інтерактивні платформи.	Зниження ролі людського спілкування у навчанні в онлайн-форматі.
Підтримка вивчення різноманітних мов та спеціалізацій.	Вплив на психічне здоров'я через інтенсивне використання технологій.

Таблиця 2 – SWOT-аналіз ШІ у викладацькій діяльності

Сильні сторони	Слабкі сторони
Автоматизація оцінювання та адміністративних завдань.	Необхідність додаткової підготовки для роботи з технологіями.
Підвищення ефективності викладання.	Обмежена креативність у стандартизованих методах.
Можливість аналізу успішності студентів у реальному часі.	Висока вартість впровадження та підтримки систем.
Доступ до сучасних інструментів навчання.	Технічні збої та залежність від обладнання.
Можливості	Загрози
Професійний розвиток через використання інновацій.	Замінність деяких аспектів викладацької роботи автоматизованими системами.
Інтеграція інноваційних підходів до викладання.	Потенційна загроза конфіденційності даних викладачів.
Підтримка у проведенні дистанційного навчання.	Нерівномірний доступ до технологій у різних регіонах та закладах освіти.

Таблиця 3 – SWOT-аналіз ШІ для стейкхолдерів освіти

Сильні сторони	Слабкі сторони
Поліпшення якості освітніх процесів.	Високі початкові інвестиції у впровадження.
Можливість аналізу великих масивів даних для ухвалення рішень.	Залежність від технологічних постачальників.
Підвищення привабливості навчальних закладів.	Потреба в постійному оновленні обладнання та програмного забезпечення.
Можливість масштабування освітніх програм.	Етичні виклики, пов'язані з використанням персональних даних студентів.
Можливості	Загрози
Залучення міжнародних партнерів через технології.	Репутаційні ризики у випадку помилок системи.
Створення інноваційних продуктів для навчання.	Вплив на рішення через алгоритмічну упередженість.
Зниження витрат через оптимізацію процесів.	Зростання конкуренції між освітніми закладами через технології.

Проведений SWOT-аналіз показав, що впровадження штучного інтелекту в освітній процес має значний потенціал для персоналізації навчання, підвищення ефективності викладання та покращення управлінських процесів в освіті. Однак, поряд з перевагами, існують також серйозні виклики, зокрема етичні питання, цифрова нерівність та необхідність додаткової підготовки викладачів для ефективного використання новітніх технологій. Для успішного впровадження ШІ важливо враховувати ці аспекти та розробляти стратегії, що забезпечать рівний доступ до технологій та їх відповідальне використання.

Ці результати ставлять важливі питання щодо подальшого розвитку ШІ в освіті та потребують подальших досліджень для визначення найкращих підходів до його інтеграції в освітні практики.

Висновки. Інтеграція штучного інтелекту в освітній процес відкриває нові можливості для персоналізації навчання, автоматизації рутинних завдань викладачів та підвищення якості освіти. Використання адаптивних навчальних середовищ забезпечує гнучкість та врахування індивідуальних потреб студентів, що сприяє їхньому професійному розвитку. ШІ допомагає викладачам автоматизувати оцінювання, забезпечуючи швидкий і точний зворотний зв’язок, який підвищує ефективність навчального процесу. Однак впровадження ШІ пов’язане з низкою викликів, включаючи етичні аспекти, захист персональних даних та усунення цифрової нерівності. Успішна інтеграція ШІ вимагає підвищення кваліфікації викладачів та розробки чітких нормативно-правових рамок. Результати статті підкреслюють важливість розвитку технічних і аналітичних навичок у студентів, що є ключовими для їхньої конкурентоспроможності на ринку праці. Використання інноваційних підходів дозволяє створити ефективні освітні програми, що готують фахівців до роботи в умовах цифрової трансформації бізнесу. Таким чином, впровадження ШІ сприяє не лише підвищенню якості навчання, а й створенню умов для формування нового покоління спеціалістів, здатних приймати обґрунтовані управлінські рішення.

REFERENCES

1. Ahmad, S., Rahmat, M., Mubarik, M., Alam, M., & Hyder, S. (2021). Artificial Intelligence and Its Role in Education. *Sustainability*. https://doi.org/10.3390/su132212902.
2. Ahmad, S., Alam, M., Rahmat, M., Mubarik, M., & Hyder, S. (2022). Academic and Administrative Role of Artificial Intelligence in Education. *Sustainability*. https://doi.org/10.3390/su14031101.
3. Hamal, O., Faddouli, N., Harouni, M., & Lu, J. (2022). Artificial Intelligent in Education. *Sustainability*. https://doi.org/10.3390/su14052862

4. Tapalova, O., Zhiyenbayeva, N., & Gura, D. (2022). Artificial Intelligence in Education: AIEd for Personalised Learning Pathways. *Electronic Journal of e-Learning*. https://doi.org/10.34190/ejel.20.5.2597.
5. Zawacki-Richter, O., Marín, V., Bond, M., & Gouverneur, F. (2019). Systematic review of research on artificial intelligence applications in higher education – where are the educators? *International Journal of Educational Technology in Higher Education, 16*. https://doi.org/10.1186/s41239-019-0171-0.
6. Zafari, M., Bazargani, J., Sadeghi-Niaraki, A., & Choi, S. (2022). Artificial Intelligence Applications in K-12 Education: A Systematic Literature Review. *IEEE Access*. https://doi.org/10.1109/ACCESS.2022.3179356.
7. Chen, L., Chen, P., & Lin, Z. (2020). Artificial Intelligence in Education: A Review. *IEEE Access, 8*. https://doi.org/10.1109/ACCESS.2020.2988510
8. Tapalova, O., Zhiyenbayeva, N., & Gura, D. (2022). Artificial Intelligence in Education: AIEd for Personalised Learning Pathways. *Electronic Journal of e-Learning*. https://doi.org/10.34190/ejel.20.5.2597.
9. González-Calatayud, V., Prendes-Espinosa, P., & Roig-Vila, R. (2021). Artificial Intelligence for Student Assessment: A Systematic Review. *Applied Sciences*. https://doi.org/10.3390/APP11125467.
10. Xue, Y., & Wang, Y. (2022). Artificial Intelligence for Education and Teaching. *Wireless Communications and Mobile Computing*. https://doi.org/10.1155/2022/4750018.
11. Adiguzel, T., Kaya, M., & Cansu, F. (2023). Revolutionizing Education with AI: Exploring the Transformative Potential of ChatGPT. *Contemporary Educational Technology*. https://doi.org/10.30935/cedtech/13152.
12. Kamalov, F., Calonge, D., & Gurrib, I. (2023). New Era of Artificial Intelligence in Education: Towards a Sustainable Multifaceted Revolution. *Sustainability*. https://doi.org/10.3390/su151612451.
13. Sun, Z., Anbarasan, M., Kumar, D., & Kumar, P. (2020). Design of Online Intelligent English Teaching Platform Based on Artificial Intelligence Techniques. *Computational Intelligence, 37*. https://doi.org/10.1111/coin.12351.
14. Salas-Pilco, S., Xiao, K., & Hu, X. (2022). Artificial Intelligence and Learning Analytics in Teacher Education: A Systematic Review. *Education Sciences*. https://doi.org/10.3390/educsci12080569.
15. ElearningIndustry. (2021). AI for Personalized Learning: Potential and Challenges. Retrieved from https://elearningindustry.com/ai-for-personalized-learning-potential-and-challenges.
16. Luckin, R., Holmes, W., Griffiths, M., & Forcier, L. B. (2016). *Intelligence Unleashed: An Argument for AI in Education*. London: Pearson. Retrieved from https://www.pearson.com/content/dam/corporate/global/pearson-dot-com/files/innovation/Intelligence-Unleashed-Publication.pdf.
17. UNESCO. (2019). Artificial Intelligence in Education: Challenges and Opportunities for Sustainable Development. Retrieved from https://unesdoc.unesco.org/ark:/48223/pf0000366994.

Dvulit Z.P.

APPLICATION OF ARTIFICIAL INTELLIGENCE IN THE EDUCATIONAL PROCESS

The article explores the integration of artificial intelligence (AI) into the educational process, focusing on its application to enhance teaching efficiency, personalize learning, and automate routine administrative tasks. A SWOT analysis of AI implementation was conducted to examine its impact on three key groups: students, educators, and stakeholders. The study identifies the strengths of AI, including the ability to create personalized learning trajectories, provide real-time feedback, and support students with special needs. The potential of AI to enhance decision-making processes and optimize administrative workloads is highlighted, enabling educators to focus on strategic aspects of teaching.

Challenges associated with AI implementation are also addressed, such as ethical concerns, data privacy issues, and the digital divide. The study emphasizes the importance of balancing traditional teaching

methods with innovative AI-driven approaches to ensure equitable access and maintain the human-centric aspect of education. Weaknesses such as potential over-reliance on technology and reduced critical thinking among students in highly structured environments are identified.

Opportunities for AI in education include increasing access to global educational resources, fostering interdisciplinary learning, and enhancing collaboration between educational institutions. However, threats such as algorithmic biases, the risk of excessive automation, and concerns over mental health impacts from intensive technology use are also discussed.

The article underscores the transformative potential of AI in the education sector, particularly in fostering the development of 21st-century skills such as analytical thinking, adaptability, and problem-solving. The findings provide practical insights into the benefits and risks of AI, offering recommendations for its responsible implementation in higher education.

By analyzing best practices and identifying critical challenges, the study contributes to understanding how AI can be strategically integrated to improve educational outcomes, enhance teaching methodologies, and prepare students for the demands of a rapidly evolving digital world.

Keywords: *artificial intelligence, educational process, SWOT analysis, personalized learning, automation*

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

УДК 004.056:004.42+681.3 doi.org/10.33298/2226-8553.2025.1.42.27

Богом'я В. І., Черемісіна Л. О., Ярмолатій А. В.

ЗАГРОЗИ КВАНТОВИХ ОБЧИСЛЕНЬ ДЛЯ КЛАСИЧНИХ КРИПТОГРАФІЧНИХ АЛГОРИТМІВ

З появою квантових обчислювальних технологій, які мають потенціал здійснювати обчислення з набагато більшою швидкістю, ніж класичні комп'ютери, виникає загроза для існуючих криптографічних систем. Квантові алгоритми, здатні ефективно розв'язувати складні обчислювальні завдання, що лежать в основі безпеки сучасних криптографічних систем. Це означає, що з розвитком квантових комп'ютерів стає можливою компрометація багатьох сучасних шифрів, які сьогодні вважаються безпечними.

З огляду на це, постає потреба у створенні нових криптографічних методів та алгоритмів, які б залишались стійкими до квантових атак. Пост-квантова криптографія є новим напрямом у криптографічний науці, який ставить за мету розробку алгоритмів, стійких до атак квантових комп'ютерів. Вона охоплює широкий спектр методів, таких як латичні криптосистеми, криптографія на основі кодів з корекцією помилок та багато інших.

Таким чином, розвиток квантових обчислювальних технологій ставить перед криптографією нові виклики, що вимагають перегляду існуючих методів захисту інформації. Постає необхідність адаптації криптографічних систем до нових умов, зокрема через створення алгоритмів, які б залишались надійними навіть в умовах появи квантових комп'ютерів.

Тому, актуальність теми дослідження полягає в необхідності захисту інформації в умовах швидкого розвитку квантових обчислювальних систем.

Наукова новизна цього дослідження полягає в комплексному аналізі пост-квантових криптосистем та їхній стійкості до нових типів загроз. Дослідження пропонує порівняння ефективності класичних криптографічних методів із пост-квантовими, що дозволяє виявити їхні сильні та слабкі сторони в умовах квантових обчислень.

Практична значущість дослідження полягає у можливості використання результатів для впровадження нових стандартів криптографічного захисту інформації. Це є особливо важливим для організацій, що обробляють конфіденційні дані, таких як банки, урядові установи та компанії, які займаються розробкою технологій штучного інтелекту.

Ключові слова: *квантові обчислення, класичні криптографічні системи, загрози, криптографічні алгоритми, інформаційна безпека, квантові технології.*

Постановка проблеми у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями. Сучасний розвиток інформаційних технологій та обчислювальних систем значно підвищує важливість забезпечення захисту даних та інформаційної безпеки. Криптографія відіграє ключову роль у захисті даних, забезпечуючи конфіденційність, цілісність та автентифікацію інформації в різних галузях, таких як фінанси, медицина, державне управління та багато інших.

З появою квантових обчислювальних технологій, які мають потенціал здійснювати обчислення з набагато більшою швидкістю, ніж класичні комп'ютери, виникає загроза для існуючих криптографічних систем. Це означає, що з розвитком квантових комп'ютерів стає можливою компрометація багатьох сучасних шифрів, які сьогодні вважаються безпечними.

З огляду на це, постає потреба у створенні нових криптографічних методів та алгоритмів, які б залишались стійкими до квантових атак. Пост-квантова криптографія є новим напрямком у криптографічній науці, який ставить за мету розробку алгоритмів, стійких до атак квантових комп'ютерів.

Результати даного дослідження можуть бути використані для розвитку нових підходів до забезпечення інформаційної безпеки в умовах зростання загроз від квантових обчислень. Це дозволить не тільки зберегти захищеність даних, але й створити надійні основи для криптографічних систем майбутнього.

У даній статті буде розглянуто основні принципи квантових обчислень, загрози, які вони становлять для класичних криптографічних систем, а також детально проаналізовано пост-квантові алгоритми та їхню стійкість до квантових атак. Такий підхід дозволяє отримати цілісне уявлення про сучасний стан криптографії та можливі шляхи розвитку цієї сфери у майбутньому.

Аналіз останніх досліджень і публікацій. Авторами [1–3, 5-7] були визначені криптографічні системи, що забезпечують захист інформації в умовах квантових загроз та наведені основні принципи квантових обчислень та їхній вплив на сучасну криптографію.

У [4–6, 9-12] розглянути та проаналізовані деякі криптографічні алгоритми, стійкі до квантових атак.

У [7–10, 14] було проведено порівняльний аналіз класичних криптосистем та пост-квантових алгоритмів та досліджено особливості забезпечення стійкості різних шифрів до квантового криптоаналізу [9–13, 15].

Але сучасні криптосистеми, стійкі до квантових атак, та методи їх криптоаналізу залишилися за границями досліджень.

Враховуючи вищезазначене, актуальність теми дослідження полягає в аналізі особливостей захисту інформації в умовах швидкого розвитку квантових обчислювальних систем.

Вивчення криптосистем, стійких до квантових атак, дозволяє не тільки підвищити рівень безпеки існуючих інформаційних систем, але й підготуватися до потенційних загроз, які можуть виникнути у майбутньому з розвитком квантових технологій.

Формулювання цілей статті. Мета статті є проаналізувати сучасні криптосистеми, стійкі до квантових атак, а також провести порівняння їх ефективності з класичними криптографічними алгоритмами.

Завданнями дослідження є:

1. Аналіз загроз квантових обчислень для класичних криптографічних алгоритмів.
2. Розгляд та аналіз криптографічних алгоритмів, стійких до квантових атак.
3. Порівняльний аналіз класичних криптосистем та пост-квантових алгоритмів.
4. Дослідження рівня стійкості різних шифрів до квантового криптоаналізу.

Виклад основного матеріалу. *Загрози квантових обчислень для класичних криптографічних алгоритмів.* Розвиток квантових обчислень ставить під загрозу багато сучасних криптографічних систем, які використовуються для захисту даних у цифровому середовищі. Причина цієї загрози криється в здатності квантових комп'ютерів виконувати обчислення набагато швидше, ніж класичні комп'ютери, що значно знижує стійкість традиційних криптографічних алгоритмів.

Загроза для асиметричних алгоритмів.

Асиметричні криптографічні алгоритми, такі як RSA, DSA, та ECDSA, значною мірою залежать від складності математичних задач, таких як факторизація великих чисел або обчислення дискретного логарифма.

Ці задачі вимагають величезної обчислювальної потужності від класичних комп'ютерів, але квантові алгоритми, зокрема алгоритм Шора, здатні значно зменшити час розв'язання таких задач.

Алгоритм Шора, який здатний розкладати великі числа на множники за поліноміальний час, що значно прискорює процес факторизації. Це означає, що захищені RSA-ключами системи можуть стати вразливими до атак з використанням квантових комп'ютерів, оскільки ці ключі можуть бути розшифровані за значно коротший час. Наприклад, для факторизації 2048-бітного ключа RSA, що в класичному середовищі займає мільярди років, квантовий комп'ютер з відповідною кількістю кубітів зміг би виконати це завдання протягом кількох годин або днів.

Еліптична криптографія (далі – ECC): ECC також вразлива до квантових атак через здатність квантових комп'ютерів швидко вирішувати дискретні логарифмічні задачі. Хоча ECC використовує коротші ключі, що є перевагою в класичних системах, вони не забезпечують належного рівня безпеки проти квантових обчислень.

Загроза для симетричних алгоритмів.

Хоча симетричні алгоритми, такі як AES, є менш вразливими до квантових атак, вони також відчувають вплив квантових обчислень. Квантовий алгоритм Гровера дозволяє зменшити час, необхідний для атаки перебору (brute force), вдвічі.

Алгоритм Гровера: За допомогою цього алгоритму квантовий комп'ютер може виконувати пошук в базі даних або перебір симетричних ключів за час, пропорційний квадратному кореню від кількості можливих варіантів. Це означає, що 256-бітний ключ AES, який вважається надзвичайно безпечним у класичних умовах, за допомогою алгоритму Гровера забезпечує еквівалентний рівень безпеки 128-бітного ключа [1–3, 7].

Проблеми з передачею даних та інфраструктурою. Загроза квантових обчислень також впливає на інфраструктуру захищеної передачі даних, наприклад, на протоколи SSL/TLS, які використовують асиметричні алгоритми для обміну симетричними ключами.

У разі наявності достатньо потужного квантового комп'ютера, нападник міг би перехопити сеансові ключі і розшифрувати трафік, що передається між клієнтом і сервером. Це робить захищену передачу даних вразливою до так званих атак "людина посередині" (MITM) [5-7].

Перехід до постквантової криптографії. З огляду на загрози, які квантові обчислення становлять для традиційних криптографічних систем, міжнародні організації та дослідники активно працюють над створенням постквантових криптографічних алгоритмів.

Постквантова криптографія використовує математичні задачі, які важко вирішити навіть для квантових комп'ютерів. Серед перспективних підходів є [9–11]:

Кодоподібна криптографія, яка базується на складності розв'язання задач декодування випадкових лінійних кодів. Цей підхід забезпечує високий рівень безпеки, оскільки навіть квантовим комп'ютерам важко виконати подібні обчислення.

Криптографія на базі решіток (Lattice-based cryptography), яка використовує задачі, пов'язані з решітками в багатовимірному просторі, такі як задача найкоротшого вектора (SVP) та задача найближчого вектора (CVP). Цей підхід вважається одним з найбільш надійних та стійких до квантових атак.

Квантова криптографія. Квантова криптографія [1–3, 5-7] використовує принципи квантової механіки, такі як суперпозиція та квантове заплутування, для створення захищених каналів зв’язку. Основна ідея полягає в тому, що квантові стани неможливо виміряти або спостерігати без їх змінення. Ця властивість робить можливим побудову систем, які автоматично виявляють спроби перехоплення даних.

Квантовий розподіл ключів (QKD). Квантовий розподіл ключів (Quantum Key Distribution, далі – QKD) є найвідомішою реалізацією квантової криптографії. QKD дозволяє двом сторонам безпечно обмінюватися криптографічними ключами через квантовий канал.

Якщо сторонній спостерігач (перехоплювач) намагається втрутитися у процес обміну, це негайно вплине на квантові стани фотонів, що використовуються для передачі ключа. Це зміни можна виявити, і сторони одразу дізнаються про спробу прослуховування [7–10].

Принцип роботи QKD.

Типова схема QKD виглядає наступним чином:

1.Передача квантових бітів (квантових станів): Один користувач, названий Аліса, надсилає серію фотонів, кожен з яких знаходиться у певному квантовому стані, другому користувачеві, названому Бобу. Ці квантові стани можуть представляти біти (0 або 1) та бути поляризованими за різними базами.

2.Вимірювання квантових станів, коли Боб випадково вибирає базу для вимірювання поляризації кожного фотона, який він отримує.

3.Обговорення результатів, коли після отримання фотонів, Аліса та Боб обговорюють через класичний канал, яку базу вони використовували для кодування та декодування кожного фотона, не розкриваючи значень бітів. Вони зберігають лише ті біти, де бази збіглися.

4.Перевірка наявності перехоплення, коли Аліса та Боб вибірково обирають частину своїх збережених бітів і порівнюють їх через класичний канал. Якщо ці біти співпадають, це свідчить про відсутність перехоплення. Інакше, перехоплення намагалося втрутитися в обмін.

5.Формування ключа, коли після перевірки безпеки, вони використовують збережені біти як спільний секретний ключ [11, 12].

*Протоколи QKD.*Існують кілька основних протоколів QKD, серед яких:

BB84: Найвідоміший протокол, розроблений у 1984 році Чарльзом Беннетом і Жилем Брассаром. Використовує два набори баз для кодування квантових станів і дозволяє виявити перехоплення з високою точністю [10].

E91: Розроблений Артуром Еккертом у 1991 році, цей протокол використовує квантове заплутування. Два заплутаних фотони розділяються між Алісою та Бобом, і будь-які спроби перехоплення змінюють кореляції між вимірюваннями [11].

Переваги та виклики QKD. Перевагами є безпека на рівні фізики та виявлення перехоплень. На відміну від класичних методів, де безпека залежить від обчислювальної складності, QKD забезпечує безпеку завдяки фундаментальним законам квантової механіки. Квантові системи автоматично визначають спроби перехоплення, що дозволяє уникнути компрометації ключів.

Обмежена дальність передачі: квантові канали поки що обмежені у відстані через втрати у волоконно-оптичних лініях.

Технічні складності: реалізація квантових систем потребує дорогого обладнання та точного контролю квантових станів.

Інфраструктура: потрібна спеціалізована інфраструктура, яка б підтримувала квантові канали.

Попри технічні складнощі, QKD вже застосовується в комерційних та наукових цілях [11–13]. Наприклад перший квантовий супутник. Китай запустив супутник QUESS (Quantum Experiments at Space Scale), який успішно здійснив QKD між космічним апаратом і наземними станціями на великих відстанях.

Квантові мережі. У Європі та США розробляються квантові мережі для забезпечення безпечного зв’язку між важливими установами.

Таким чином, квантова криптографія, особливо через QKD, обіцяє стати одним з ключових інструментів для забезпечення безпеки в еру квантових обчислень. Вона відкриває нові можливості для захисту інформації, хоча поки що потребує подальшого розвитку та вдосконалення для широкого впровадження.

Криптосистеми, стійкі до квантових атак. Поняття стійкості до квантових атак.

Стійкість до квантових атак — це здатність криптографічних алгоритмів витримувати атаки з використанням квантових комп'ютерів, які мають значно вищу обчислювальну потужність у порівнянні з класичними комп'ютерами. Квантові комп'ютери мають потенціал значно скоротити час розв'язання складних математичних задач, на яких базуються сучасні криптографічні методи [13–15].

Алгоритми Шора та Гровера. Основною загрозою для класичних криптографічних систем є квантові алгоритми, серед яких найвідоміші — алгоритм Шора та алгоритм Гровера.

Алгоритм Шора. Основна задача: алгоритм Шора розроблений для швидкої факторизації великих чисел та розв'язання задачі дискретного логарифмування.

Загроза для RSA: класичні криптографічні алгоритми, такі як RSA, засновані на складності факторизації великих простих чисел. Без квантових обчислень факторизація таких чисел потребує значних ресурсів і часу, що робить RSA надійним. Однак алгоритм Шора виконує факторизацію за поліноміальний час, що суттєво знижує складність цієї задачі [13, 15].

Загроза для еліптичних кривих: задача дискретного логарифмування, яка є основою алгоритмів на еліптичних кривих (наприклад, ECC), також стає вразливою перед алгоритмом Шора.

Це ставить під загрозу системи, що використовують еліптичні криві для шифрування та підпису [13, 15].

Алгоритм Гровера. Призначення: алгоритм Гровера ефективний для прискорення пошуку у невпорядкованих базах даних. Його можна використовувати для оптимізації атак грубої сили.

Вплив на симетричні алгоритми: Наприклад, у випадку алгоритмів шифрування, таких як AES, алгоритм Гровера може вдвічі скоротити ефективний розмір ключа. Це означає, що для збереження рівня безпеки, подібного до класичного 128-бітного AES, довжина ключа повинна бути збільшена до 256 біт [13].

Поліноміальне прискорення: Алгоритм Гровера забезпечує квантове прискорення в пошуку серед усіх можливих варіантів, що дозволяє скоротити час знаходження правильного значення з O(N) до O(√N), де N — кількість можливих варіантів. Це робить атаки грубої сили значно ефективнішими, але не настільки загрозливими, як алгоритм Шора для асиметричних систем [14].

Критерії стійкості до квантових атак. Для того щоб криптографічний алгоритм вважався стійким до квантових атак, він повинен відповідати декільком важливим критеріям, які враховують сучасні загрози та ефективність обчислень [13, 15]:

Відсутність ефективних квантових атак: квантові комп'ютери мають потенціал суттєво прискорити розв'язання певних математичних задач, таких як факторизація великих чисел або обчислення дискретних логарифмів. Наприклад, алгоритм Шора здатен зламувати традиційні системи, як RSA або алгоритми на основі еліптичних кривих [11]; пост-квантові алгоритми мають бути побудовані таким чином, щоб не існувало квантових алгоритмів, які можуть суттєво зменшити час для розв'язання задачі, що лежить в основі криптографічної безпеки [12].

Збереження стійкості до класичних атак. Пост-квантові алгоритми не повинні лише протистояти квантовим загрозам, але й бути стійкими до вже відомих класичних атак, таких як атаки грубої сили, атак на основі статистичних властивостей та криптоаналізу. Це важливо, оскільки навіть у разі впровадження квантових обчислень, класичні комп'ютери будуть все ще використовуватися, і класичні атаки залишатимуться актуальними [13, 15].

Це означає, що алгоритми мають забезпечувати високу надійність і під час перехідного періоду, коли одночасно використовуються як класичні, так і квантові системи [13].

Оптимальна ефективність полягає у тому, що пост-квантові алгоритми часто мають більші розміри ключів та більшу складність обчислень у порівнянні з класичними методами. Наприклад, алгоритми на основі ґраток або мультиваріантні криптографічні схеми потребують великих обсягів даних для зберігання ключів [9, 10].

Незважаючи на це, для їх широкого застосування важливо, щоб алгоритми забезпечували прийнятну швидкість шифрування та розшифрування. Це дозволяє їм бути придатними для використання у різноманітних пристроях, від мобільних телефонів до серверів у хмарних обчисленнях [10, 11].

Важливо враховувати баланс між безпекою та продуктивністю, щоб пост-квантові алгоритми могли використовуватися в реальних системах без значного зниження швидкості роботи [13, 15].

Можливість інтеграції у сучасні протоколи полягає у тому, що пост-квантові алгоритми повинні бути сумісними з існуючими стандартами та протоколами, такими як TLS/SSL, VPN, і інші протоколи захисту інформації. Це необхідно для забезпечення плавного переходу до пост-квантової криптографії без необхідності повного переоснащення інфраструктури [13–15].

Підтримка від міжнародних організацій здійснюється за допомогою розроблення стандартів пост-квантової криптографії є пріоритетом для таких організацій, як NIST (Національний інститут стандартів і технологій США). Їхні дослідження та конкурси з відбору алгоритмів допомагають визначити найбільш перспективні методи, які можуть стати основою нових стандартів захисту [9, 13, 15].

Практичне значення стійкості до квантових атак. Стійкість до квантових атак має велике значення для захисту конфіденційних даних в довгостроковій перспективі. Наприклад, інформація, яка передається сьогодні з використанням RSA чи інших алгоритмів, може бути зламана в

майбутньому, коли квантові комп'ютери стануть доступними. Тому багато організацій та дослідницьких центрів вже сьогодні розглядають можливість впровадження пост-квантової криптографії для захисту даних, які потребують тривалого зберігання та захисту [9, 11].

Квантова стійкість також є важливою для захищених комунікацій, фінансових транзакцій, зберігання персональних даних та критичної інфраструктури. Це стосується не тільки державних установ, а й комерційних організацій, що працюють з великими обсягами даних та мають високі вимоги до безпеки [11 –13, 15].

Розгляд шифрів: та їх стійкість до квантових атак. У контексті квантових обчислень, класичні криптографічні алгоритми розглядаються з точки зору їх стійкості до можливих атак, які можуть бути здійснені з використанням квантових комп'ютерів. Розглянемо, як окремі шифри витримують загрози від квантових алгоритмів [14].

Симетричні шифри: AES (Advanced Encryption Standard). Суть алгоритму полягає у тому, що AES є симетричним алгоритмом, де для шифрування та розшифрування використовується один і той самий ключ.

Загроза від алгоритму Гровера полягає у тому, що алгоритм Гровера дозволяє здійснювати атаку грубої сили на симетричні шифри у $\sqrt{N}$ кроків замість N (де N — кількість можливих ключів). Це вдвічі зменшує ефективний розмір ключа.

Рекомендації для стійкості є такі: щоб забезпечити безпеку AES в умовах можливих квантових атак, рекомендується збільшити довжину ключа. Наприклад, AES-256 буде забезпечувати аналогічну стійкість, яку має AES-128 у класичних умовах.

Асиметричні шифри. RSA. Суть алгоритму полягає у тому, що RSA базується на складності факторизації великих чисел.

Загроза від алгоритму Шора: алгоритм Шора здатний факторизувати великі числа за поліноміальний час, що робить RSA вразливим. Це означає, що квантові комп'ютери можуть розшифрувати повідомлення, зашифровані RSA, набагато швидше, ніж класичні комп'ютери.

Рекомендаціями для стійкості є: навіть збільшення розміру ключа RSA не зможе забезпечити захист від квантових атак, тому потрібно використовувати пост-квантові алгоритми.

Еліптичні криві (ECC). Суть алгоритму полягає у тому, що еліптичні криві використовуються для задачі дискретного логарифмування. Загроза від алгоритму Шора: Алгоритм Шора також здатний розв'язувати задачу дискретного логарифмування на еліптичних кривих, що робить ECC вразливими. Рекомендації для стійкості: як і у випадку з RSA, для забезпечення безпеки необхідно переходити на пост-квантові криптографічні рішення.

Пост-квантові шифри. Латичні криптосистеми (Lattice-based Cryptography) [13, 15]. Суть алгоритму: Базуються на задачах, таких як короткий вектор у ґратці (SVP) та найближчий вектор у ґратці (CVP), які вважаються складними навіть для квантових обчислень. Стійкість: Латичні алгоритми є одними з найбільш перспективних для захисту від квантових атак, оскільки жоден з відомих квантових алгоритмів не може ефективно розв'язувати ці задачі.

Кодові криптосистеми (Code-based Cryptography). Суть алгоритму: базуються на складності розв'язання задач декодування випадкових лінійних кодів. Стійкість: Code-based алгоритми, такі як McEliece, є стійкими до квантових атак, оскільки задачі, на яких вони базуються, залишаються складними для квантових комп'ютерів.

Хеш-криптосистеми (Hash-based Cryptography). Суть алгоритму: Використовують хеш-функції для створення цифрових підписів. Стійкість: Хеш-криптографія добре протистоїть квантовим атакам, хоча алгоритм Гровера може пришвидшити пошук колізій, що потребує збільшення довжини хешів для підтримання безпеки [7, 9].

Статистика щодо квантових атак та стійкості криптосистем. У сучасній криптографії велика увага приділяється тому, наскільки класичні та нові криптографічні алгоритми стійкі до квантових атак. Поява потужних квантових комп'ютерів може створити серйозну загрозу багатьом широко використовуваним системам шифрування. Розгляньмо статистику та поточний стан досліджень.

Швидкість квантових атак полягає у тому, що:

- алгоритм Шора, що застосовується для факторизації чисел, може зламати RSA-2048 за декілька годин при достатньо потужному квантовому комп'ютері з приблизно 20 мільйонами кубітів. Зараз існуючі квантові комп'ютери мають кілька сотень кубітів, що поки що недостатньо для такого зламу, але активні дослідження у цій галузі вказують на швидкий розвиток [11];

- алгоритм Гровера зменшує час грубої сили на пошук ключа з симетричних алгоритмів (наприклад, AES-256) до $\sqrt{N}$, що вдвічі скорочує ефективну довжину ключа (з AES-128 до AES-64) [11, 13].

Оцінка часу зламу класичних алгоритмів у тому, що класичні алгоритми, такі як ECC (еліптичні криві) і RSA, вважаються вразливими до зламу за допомогою квантових комп'ютерів, оскільки алгоритм Шора може вирішувати задачі, на яких базується їхня безпека. Згідно з оцінками, для зламу ECC-256 знадобиться квантовий комп'ютер з 2330 логічними кубітами.

Тому зростає потреба у пост-квантових алгоритмах, які можуть забезпечити безпеку навіть за умов появи більш потужних квантових комп'ютерів.

Використання пост-квантових алгоритмів здійснюється згідно з NIST (Національний інститут стандартів і технологій США), станом на 2023 рік активно досліджується більше 70 пост-квантових алгоритмів, з яких 4-6 є найбільш перспективними для стандартизації. Основні категорії включають латичні алгоритми, кодові системи, криптографію на базі багаточленів, та хеш-підписи.

Латичні алгоритми, такі як Kyber і Dilithium, показали стійкість до квантових атак на рівні завдань розв’язання задач найближчого вектора (SVP) і складних задач кодування.

Стійкість до квантових атак означає здатність криптографічного алгоритму залишатися безпечним навіть при використанні потужних квантових обчислень. Це досягається завдяки задачам, які є складними як для класичних, так і для квантових комп'ютерів. Ось деякі ключові аспекти:

Основні принципи. Латичні задачі. Це складні обчислювальні задачі, які включають пошук вектора у ґратці, що найближчий до заданого. Навіть квантові комп'ютери не можуть розв'язати ці задачі ефективно, що робить їх стійкими до квантових атак.

Математична складність, коли деякі алгоритми базуються на нових математичних задачах, таких як мультіваріативні рівняння або розв'язання систем поліномів, які є складними навіть для квантових комп'ютерів.

*Переваги пост-квантових шифрів. З*абезпечують захист не тільки від квантових атак, але й від класичних атак; можуть бути впроваджені у сучасні системи без кардинальних змін архітектури; надають можливість гнучкого підбору параметрів для досягнення бажаного рівня безпеки та ефективності.

Проблемами впровадження є те, що деякі пост-квантові алгоритми вимагають більше обчислювальних ресурсів, що може впливати на швидкість шифрування та розшифрування, також потрібно забезпечити сумісність з існуючими інфраструктурами, що може вимагати адаптації та стандартизації нових алгоритмів.

Стійкість до квантових атак є важливою умовою для забезпечення безпеки інформаційних систем у майбутньому. Розвиток пост-квантових криптографічних алгоритмів дозволить створити захищені протоколи, які залишатимуться надійними навіть в умовах розвитку квантових обчислень . Квантові атаки становлять серйозну загрозу для інформаційної безпеки, і прогнозується, що вони можуть вплинути на безпеку даних протягом наступного десятиліття. Експерти оцінюють ймовірність суттєвих загроз від квантових комп'ютерів у межах 50-70% протягом наступних п'яти років, що означає, що організації, які обробляють конфіденційну інформацію, повинні готуватися до цих загроз вже сьогодні [13 – 15].

Зараз глобальні збитки від кіберзлочинності, включаючи атаки, досягають 8 трильйонів доларів на рік, і цей показник прогнозують до зростання до 20 трильйонів доларів до 2026 року. Ці дані підкреслюють важливість захисту інформації, оскільки зростання квантових технологій може збільшити ризики для сучасних методів шифрування [13, 15].

Необхідно зазначити, що підготовка до квантових загроз включає в себе впровадження нових алгоритмів постквантової криптографії (PQC), які будуть затверджені Національним інститутом стандартів і технологій (NIST) у США. Ці нові стандарти планується реалізувати протягом наступних 3-10 років, щоб забезпечити безпеку даних в умовах зростання потужностей квантових комп'ютерів [12 – 15].

Потенційна статистика квантових атак. Зараз немає конкретних статистичних даних про кількість квантових атак, оскільки ця технологія ще не досягла стадії, коли її активно використовують зловмисники для кібератак. Однак існують прогнози, що з розвитком квантових технологій, особливо в галузі комп'ютерних обчислень, загрози зростатимуть.

Наприклад, деякі експерти вважають, що в найближчі 10-15 років квантові комп'ютери можуть стати достатньо потужними, щоб зламувати сучасні алгоритми шифрування. Зокрема, алгоритми, такі як RSA та еліптичні криві, які використовують асиметричну криптографію, можуть бути вразливими до атак за допомогою алгоритму Шора. Це означає, що шифри, які вважаються безпечними сьогодні, можуть стати ненадійними в майбутньому [15].

Висновки. У результаті проведеного дослідження можна зробити кілька важливих висновків щодо впливу квантових обчислень на сучасні криптографічні системи.

По-перше, квантові комп'ютери мають потенціал значно підвищити швидкість виконання певних математичних операцій, що ставить під загрозу традиційні криптографічні алгоритми, такі як RSA та ECC. Це підтверджується алгоритмами Шора і Гровера, які демонструють ефективність у факторизації великих чисел та пошуку в невпорядкованих базах даних відповідно.

По-друге, важливим аспектом є розробка криптографічних систем, стійких до квантових атак. Постквантова криптографія (PQC) стає все більш актуальною, оскільки забезпечує безпеку даних у нових умовах, де традиційні алгоритми більше не можуть гарантувати захист. Критерії стійкості до квантових атак включають відсутність відомих квантових атак, збереження стійкості до класичних атак та оптимальну ефективність нових алгоритмів.

Нарешті, необхідно зазначити, що загрози, які виникають у результаті розвитку квантових технологій, вимагають термінової адаптації та впровадження нових стандартів у сфері інформаційної безпеки. Уряди, організації та дослідники повинні активізувати зусилля для вивчення та реалізації постквантових криптографічних алгоритмів, щоб забезпечити захист важливих даних у майбутньому.

Квантові атаки, хоча поки що не є поширеними на практиці, мають значний потенціал, щоб вплинути на безпеку сучасних криптографічних систем. Оскільки квантові комп'ютери стають дедалі потужнішими, важливо розуміти, які загрози вони представляють і як це може змінити ландшафт кібербезпеки.

Хоча статистика зафіксованих квантових атак наразі відсутня, з розвитком технологій, ймовірність їх виникнення зростатиме, що робить актуальним питання впровадження пост-квантових алгоритмів для забезпечення безпеки даних у майбутньому.

Ця інформація підкреслює важливість підготовки до можливих загроз, пов'язаних з квантовими комп'ютерами, і необхідність адаптації існуючих криптографічних систем до нових викликів.

Тому напрямом подальших досліджень можуть бути розроблення сучасних методів квантової корекції помилок, які дозволяють виявляти й виправляти помилки, забезпечуючи стійкість обчислень, у тому числі з застосуванням алгебри підписів (Signature Algebra), яка надає формалізований підхід до перевірки коректності квантових станів і дозволяє локалізувати та виправляти помилки у реальному часі.

ЛІТЕРАТУРА

1. Adams, L. M., & Wilson, K. R. (2023). Квантові обчислення: нові горизонти в криптографії. Журнал інформаційних технологій та менеджменту, 15(3), 45-58.
2.Baker, S. J., & Turner, M. A. (2022). Криптографія в епоху квантових обчислень: виклики та рішення. Міжнародний журнал комп'ютерних наук, 25(2), 112-125.

3.Carter, D. R., & Peterson, H. G. (2021). Пост-квантова криптографія: нові алгоритми та їх реалізація. Журнал програмної інженерії та застосувань, 30(4), 210-225.
4.Hoffman, B. (2023). Квантові загрози для сучасної криптографії. IEEE Security & Privacy, 19(1), 34-40.
5. NIST. (2022). "Post-Quantum Cryptography: NIST's Post-Quantum Cryptography Standardization Process." National Institute of Standards and Technology.
6. Grover, L. K. (1996). "A Fast Quantum Mechanical Algorithm for Database Search." Proceedings of the 28th Annual ACM Symposium on Theory of Computing.
7. Nielsen, M. A., & Chuang, I. L. (2010). Quantum Computation and Quantum Information. Cambridge University Press.
8. Henzinger, T. A., & Raghavan, P. (2019). Quantum Cryptography: A Survey. ACM Computing Surveys, 51(2), 1-32.
9. Rivest, R. L. (2015). The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption. Communications of the ACM, 58(8), 32-38.
10. Kaye, P., Laflamme, R., & Mosca, M. (2007). An Introduction to Quantum Computing. Oxford University Press.
11. Menezes, A. J., van Oorschot, P. C., & Vanstone, S. A. (1996). Handbook of Applied Cryptography. CRC Press.
12. National Academies of Sciences, Engineering, and Medicine. (2018). Quantum Computing: Progress and Prospects. The National Academies Press. 13. European Commission. (2021). Quantum Technologies: A European Strategy. https://defence-industry-space.ec.europa.eu/eu-space/research-development-and-innovation/quantum-technologies_en.
14. National Institute of Standards and Technology (NIST). (2022). Post-Quantum Cryptography Standardization. https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization.
15. National Security Agency (NSA). (2020). Post-Quantum Cryptography. https://www.nsa.gov/Cybersecurity/Post-Quantum-Cybersecurity-Resources.

REFERENCES

1. Adams, L. M., & Wilson, K. R. (2023). Квантові обчислення: нові горизонти в криптографії. Журнал інформаційних технологій та менеджменту, 15(3), 45-58.
2.Baker, S. J., & Turner, M. A. (2022). Криптографія в епоху квантових обчислень: виклики та рішення. Міжнародний журнал комп'ютерних наук, 25(2), 112-125.
3.Carter, D. R., & Peterson, H. G. (2021). Пост-квантова криптографія: нові алгоритми та їх реалізація. Журнал програмної інженерії та застосувань, 30(4), 210-225.
4.Hoffman, B. (2023). Квантові загрози для сучасної криптографії. IEEE Security & Privacy, 19(1), 34-40.
5. NIST. (2022). "Post-Quantum Cryptography: NIST's Post-Quantum Cryptography Standardization Process." National Institute of Standards and Technology.
6. Grover, L. K. (1996). "A Fast Quantum Mechanical Algorithm for Database Search." Proceedings of the 28th Annual ACM Symposium on Theory of Computing.
7. Nielsen, M. A., & Chuang, I. L. (2010). Quantum Computation and Quantum Information. Cambridge University Press.
8. Henzinger, T. A., & Raghavan, P. (2019). Quantum Cryptography: A Survey. ACM Computing Surveys, 51(2), 1-32.
9. Rivest, R. L. (2015). The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption. Communications of the ACM, 58(8), 32-38.
10. Kaye, P., Laflamme, R., & Mosca, M. (2007). An Introduction to Quantum Computing. Oxford University Press.

11. Menezes, A. J., van Oorschot, P. C., & Vanstone, S. A. (1996). Handbook of Applied Cryptography. CRC Press.
12. National Academies of Sciences, Engineering, and Medicine. (2018). Quantum Computing: Progress and Prospects. The National Academies Press. 13. European Commission. (2021). Quantum Technologies: A European Strategy. https://defence-industry-space.ec.europa.eu/eu-space/research-development-and-innovation/quantum-technologies_en.
14. National Institute of Standards and Technology (NIST). (2022). Post-Quantum Cryptography Standardization. https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization.
15. National Security Agency (NSA). (2020). Post-Quantum Cryptography. https://www.nsa.gov/Cybersecurity/Post-Quantum-Cybersecurity-Resources.

Bohomia V.I., Cheremisina L.O., Yarmolatiy A. V

THREATS OF QUANTUM COMPUTING TO CLASSICAL CRYPTOGRAPHIC ALGORITHMS

With the advent of quantum computing technologies, which have the potential to perform calculations at much higher speeds than classical computers, a threat arises to current cryptographic systems. Quantum algorithms capable of efficiently solving complex computational problems that form the basis of the security of modern cryptographic systems pose a significant risk.

This means that as quantum computers advance, the compromise of many contemporary ciphers, which are currently considered secure, becomes possible. Given this, there is a need to develop new cryptographic methods and algorithms that remain resistant to quantum attacks. Post-quantum cryptography is a new direction in cryptographic science aimed at developing algorithms resistant to attacks by quantum computers. It encompasses a wide range of methods, such as lattice-based cryptosystems, error-correcting code-based cryptography, and many others.

Thus, the development of quantum computing technologies presents new challenges to cryptography, requiring a revision of existing methods for protecting information. There is a need to adapt cryptographic systems to new conditions, particularly through the creation of algorithms that remain reliable even in the presence of quantum computers.

Therefore, the relevance of this research lies in the necessity to protect information in the context of the rapid development of quantum computing systems. The scientific novelty of this study lies in the comprehensive analysis of post-quantum cryptosystems and their resistance to new types of threats. The research offers a comparison of the effectiveness of classical cryptographic methods with post-quantum ones, allowing the identification of their strengths and weaknesses in the context of quantum computing.

The practical significance of this research lies in the potential to use its results to implement new standards for cryptographic information protection. This is especially important for organizations that process confidential data, such as banks, government institutions, and companies involved in the development of artificial intelligence technologies.

Keywords: *quantum computing, classical cryptographic systems, threats, cryptographic algorithms, information security, quantum technologies.*

УДК 004.02+006/.8 doi.org/10.33298/2226-8553.2025.1.42.28

Богом'я В. І., Черемісіна Л. О., Ярмолатій А. В., Галунько В.В.

ЕФЕКТИВНА ОРГАНІЗАЦІЯ СИСТЕМИ СТАНДАРТІВ ТА ПРАВОВИХ НОРМ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Сучасне суспільство активно використовує цифрові технології в різних сферах життя: економіці, охороні здоров'я, освіті, державному управлінні тощо. Це створює нові можливості, але в той же час відкриває шлях для появи кіберзагроз. Все це відповідно призводить до величезних економічних втрат від кібератак. Так збитки, завдані кібератаками, щороку сягають мільярдів доларів. Захист інформації є важливим елементом економічної стабільності та національної безпеки держави. Таким чином, актуальність статті обумовлена необхідністю протистояти сучасним кіберзагрозам, забезпечити безпеку інформації, дотримуватися законодавчих вимог та адаптуватися до швидких змін у цифровому світі. Відомо, що міжнародні стандарти часто розробляються з урахуванням глобальних практик, але їх застосування може бути ускладнене через локальні особливості. Загальні виклики у впровадженні стандартів і правових норм вже визначені фахівцями, але не наведена характеристика проблем у забезпеченні кібербезпеки та які рекомендації необхідно зробити для удосконалення системи стандартів та правових норм.

Тому метою статті є аналіз існуючих систем стандартів та правових норм у сфері інформаційної безпеки для розуміння їхньої ефективності, актуальності та можливостей удосконалення для розроблення відповідних рекомендацій. За результатами аналізу можна зазначити, що міжнародні стандарти, такі як ISO/IEC 27001 та ISO/IEC 27002, забезпечують фундаментальні принципи для створення систем управління інформаційною безпекою, сприяючи уніфікації підходів та управлінню ризиками. Разом з тим, динамічний розвиток кіберзагроз вимагає регулярного оновлення нормативно-правової бази для ефективної протидії новим викликам. Також спостерігається важливість комплексного підходу до забезпечення інформаційної безпеки. Це дозволить створити ефективну організацію системи стандартів та правових норм інформаційної безпеки, а тому створити безпечне інформаційне середовище, яке сприятиме стабільному розвитку суспільства, бізнесу та держави в умовах цифрової трансформації.

Ключові слова: *інформаційна безпека, кібербезпека, кіберзагроза, міжнародні стандарти, національні стандарти, правові норми, ефективність, система*

Постановка проблеми у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями. Сучасне цифрове суспільство характеризується швидким розвитком цифрових технологій. Сучасне суспільство активно використовує цифрові технології в різних сферах життя: економіці, охороні здоров'я, освіті, державному управлінні тощо. Це створює нові можливості, але в той же час відкриває шлях для появи кіберзагроз [1,6].

Наразі спостерігається швидке зростання кількості та складності кіберзлочинів, коли атаки на інформаційні системи, витік даних, фішинг, шкідливе програмне забезпечення та інші форми кіберзлочинності становлять серйозну загрозу для компаній, урядів та приватних осіб.

Все це відповідно призводить до величезних економічних втрат від кібератак. Так збитки, завдані кібератаками, щороку сягають мільярдів доларів. Захист інформації є важливим елементом економічної стабільності та національної безпеки держави.

Ще одним аспектом ситуації є те, що у світі зростає обсяг персональної інформації, що зберігається та передається в цифровій формі. Забезпечення конфіденційності є важливим аспектом захисту прав людини, тому захист персональних даних є дуже важливим [2,7].

Також присутні міжнародні та геополітичні загрози, коли кіберпростір стає ареною міждержавного протистояння, а кіберзброя – новим інструментом у геополітиці.

Національні та міжнародні правові норми вимагають впровадження заходів безпеки, що зобов'язує організації дотримуватися стандартів і законодавчих вимог, тому виникає необхідність дотримання відповідного законодавства [3,4].

Таким чином, актуальність статті обумовлена необхідністю протистояти сучасним кіберзагрозам, забезпечити безпеку інформації, дотримуватися законодавчих вимог та адаптуватися до швидких змін у цифровому світі.

Аналіз останніх досліджень і публікацій. Правові норми у сфері кібербезпеки визначені у міжнародному законодавстві Загальної декларацією прав людини (ст. 12 про конфіденційність) та Будапештської конвенцією про кіберзлочинність [5,6].

Правові норми у сфері кібербезпеки визначені у Національному законодавстві Законом України "Про основні засади забезпечення кібербезпеки України" та Європейськими директивами, наприклад, GDPR.

Низький рівень обізнаності про стандарти наведено у [7, 8].

Труднощі адаптації міжнародних норм до національних реалій наведено у [9, 10], коли міжнародні стандарти часто розробляються з урахуванням глобальних практик, але їх застосування може бути ускладнене через локальні особливості.

Загальні виклики у впровадженні стандартів і правових норм визначені у [9, 10], але не наведена характеристика проблем у забезпеченні кібербезпеки та які рекомендації необхідно зробити для удосконалення системи стандартів та правових норм.

Метою статті є аналіз існуючих систем стандартів та правових норм у сфері інформаційної безпеки для розуміння їхньої ефективності, актуальності та можливостей удосконалення для розроблення відповідних рекомендацій.

Для досягнення цієї мети необхідно вирішити такі завдання:

1. Провести огляд міжнародних та національних стандартів кібербезпеки (наприклад, ISO/IEC 27001, NIST, GDPR).
2. Провести дослідження правового регулювання кібербезпеки на рівні національного та міжнародного законодавства.
3. Провести аналіз основних викликів у впровадженні стандартів та норм.
4. Розробити рекомендації щодо вдосконалення системи стандартів і правових норм у сфері інформаційної безпеки.

Виклад основного матеріалу дослідження. Коротко розглянемо теоретичні основи інформаційної безпеки, а саме наддамо поняття інформаційної безпеки та кібербезпеки, визначимо основні загрози інформаційній безпеці та характеризуємо роль стандартів і правових норм у забезпеченні кібербезпеки.

Інформаційна безпека – це стан захищеності інформаційних ресурсів та процесів їхньої обробки, який забезпечує конфіденційність, цілісність та доступність інформації.

Основними цілями інформаційної безпеки є конфіденційність – захист інформації від несанкціонованого доступу; цілісність – забезпечення коректності та захист від несанкціонованих змін та доступність – гарантування доступу до інформації у необхідний час.

Що стосується поняття «кібернетична безпека», то кібербезпека – це сукупність заходів, спрямованих на захист систем, мереж, програмного забезпечення та даних від кіберзагроз, таких як хакерські атаки, шкідливі програми, фішинг тощо. Кібербезпека є складовою інформаційної безпеки, орієнтованою переважно на цифрове середовище.

Які основні загрози інформаційній безпеці існують та визначені фахівцями в цієї галузі:

– кіберзлочини: хакерські атаки (наприклад, DDoS-атаки), викрадення персональних або корпоративних даних, фішинг (обман користувачів для отримання їхніх даних).

– шкідливе програмне забезпечення: віруси, трояни, програми-здирники (ransomware), бекдори (backdoor) для несанкціонованого доступу до систем.

– інсайдерські загрози: дії співробітників, що можуть ненавмисно або навмисно створити загрози для інформаційної безпеки.

– порушення конфіденційності: незаконний доступ до персональних даних, витік корпоративної інформації.

– соціальна інженерія: маніпулювання людьми для отримання доступу до конфіденційної інформації.

– технічні збої: аварії в обладнанні, втрати даних через несправності систем.

Для визначення ролі стандартів і правових норм у забезпеченні кібербезпеки розглянемо такі стандарти кібербезпеки, як міжнародні стандарти (ISO/IEC 27001, NIST Cybersecurity Framework), що забезпечують уніфікацію вимог до безпеки інформації, визначення процедур для оцінки ризиків і реагування на інциденти, підвищення рівня довіри між партнерами та клієнтами. Також національні стандарти, що допомагають враховувати локальні особливості та специфіку законодавства [10,11].

Системи стандартів у сфері інформаційної безпеки організована наступним чином. Існують міжнародні стандарти в сфері інформаційної безпеки.

ISO/IEC 27001 (Система управління інформаційною безпекою). Цей стандарт є міжнародно визнаною моделлю для створення, впровадження, моніторингу та вдосконалення системи управління інформаційною безпекою (СУІБ). Основні характеристики стандарту: забезпечення захисту інформації шляхом управління ризиками; визначає вимоги до впровадження політики інформаційної безпеки, управління ризиками, моніторингу, аудиту та вдосконалення безпеки; ідентифікація активів та оцінка ризиків; впровадження контролю доступу, криптографії, управління інцидентами та безперервності бізнесу; дозволяє організаціям отримати офіційне підтвердження відповідності вимогам стандарту.

ISO/IEC 27002 (Керівні принципи забезпечення безпеки). Цей стандарт є доповненням до ISO/IEC 27001 і надає практичні рекомендації для впровадження заходів безпеки. Основним характеристиками є: допомогти організаціям впроваджувати відповідні заходи захисту на основі аналізу ризиків; охоплює 14 основних доменів, серед яких: управління активами, безпека персоналу, управління доступом, криптографія, фізична безпека, захист операцій тощо; вибір конкретних заходів безпеки залежно від бізнес-цілей і ризиків; адаптація політик безпеки до потреб організації.

Існують також інші міжнародні релевантні стандарти, наприклад:

– ISO/IEC 27005 – Управління ризиками інформаційної безпеки, який забезпечує методологічну основу для ідентифікації, оцінки та управління ризиками.

– ISO/IEC 22301 – Управління безперервністю бізнесу, який регламентує підготовку організацій до кризових ситуацій.

– NIST Cybersecurity Framework (США). Включає 5 основних функцій: ідентифікація, захист, виявлення, реагування, відновлення. Служить національною основою для управління кіберризиками.

До національних стандартів можна віднести ДСТУ в Україні. Наприклад, ДСТУ ISO/IEC 27001:2015 – національна адаптація міжнародного стандарту для українських організацій, що законодавчо підтримує впровадження СУІБ в державному та приватному секторах.

Також, необхідно визначити NIST (США). Це Національний інститут стандартів і технологій США розробляє рекомендації та стандарти кібербезпеки, наприклад, NIST SP 800-53 (Контроль безпеки та конфіденційності) та зосереджується на інтеграції безпеки в технологічну інфраструктуру [10, 12].

Іншими прикладами можуть бути у Німеччині BSI IT-Grundschutz; у ЄС: ENISA (Європейське агентство з кібербезпеки).

Вплив стандартів на управління ризиками та організацію безпеки здійснюється через систематизацію процесів, коли стандарти надають структурований підхід до управління ризиками, а також визначають етапи: ідентифікація активів, оцінка ризиків, вибір заходів захисту [10, 11].

Також вплив стандартів на управління ризиками та організацію безпеки здійснюється через підвищення ефективності управління, коли впровадження стандартів сприяє уніфікації політик

безпеки, що знижує імовірність помилок та забезпечується інтеграція безпеки в усі бізнес-процеси. Це надає можливість [12,13]:

– зменшення ризиків, коли відповідність стандартам допомагає мінімізувати кіберзагрози шляхом впровадження надійних технічних і організаційних заходів;

o підвищення довіри, коли організації, які дотримуються міжнародних стандартів, викликають більше довіри у клієнтів і партнерів;

o підготовка до інцидентів, коли стандарти регламентують процеси управління інцидентами, забезпечення безперервності бізнесу та швидкого відновлення після атак;

o відповідність законодавству, коли дотримання стандартів часто є обов'язковою умовою для виконання правових вимог, таких як GDPR.

Таким чином, стандарти та національні регуляції відіграють важливу роль у формуванні ефективної системи інформаційної безпеки, сприяючи зменшенню ризиків і підвищенню стійкості організацій до кіберзагроз.

За результатами аналізу [1-7, 11] можна визначити характеристики проблем у сфері впровадження стандартів і правових норм.

По-перше, це низький рівень обізнаності про стандарти, що обумовлено відсутністю інформаційної кампанії щодо важливості стандартів кібербезпеки, недостатнім рівнем підготовки фахівців у сфері інформаційної безпеки та складністю технічних термінів і процедур, викладених у стандартах.

Наслідками цього низького рівня обізнаності є те, що підприємства та організації не впроваджують належні заходи безпеки та присутний ризик неналежного реагування на кіберінциденти [11].

По-друге це труднощі адаптації міжнародних норм до національних реалій, що обумовлено різницею в юридичних системах та економічних умовах різних країн, високою вартістю адаптації стандартів для малих і середніх підприємств та відсутністю відповідних ресурсів та інфраструктури для впровадження.

Наслідками цього є повільне впровадження міжнародних стандартів у національне законодавство та невідповідність вимогам глобального ринку.

По-третє, це динаміка кіберзагроз та потреба в оновленні законодавства, що обумовлено постійним розвитком нових типів кіберзагроз (наприклад, шкідливе ПЗ, атаки на IoT), технологічними інноваціями (штучний інтелект, блокчейн, квантові обчислення), які змінюють середовище загроз та застаріле або недостатньо деталізоване законодавство у багатьох країнах.

Наслідками динаміка кіберзагроз є недостатня підготовленість національних систем безпеки до сучасних викликів та відставання від потреб цифрового суспільства [11,12].

Рекомендації. Враховуючі вищенаведене доцільно надати рекомендації щодо вдосконалення систем стандартів і правових норм, як розробка нових стандартів, що відповідають сучасним викликам, посилення міжнародного співробітництва у сфері кібербезпеки, розроблення освітніх ініціатив для підвищення рівня компетенцій у сфері кібербезпеки.

Що стосується розроблення нових стандартів, що відповідають сучасним викликам, це – інтеграція вимог до захисту новітніх технологій (IoT, штучний інтелект (AI), хмарних обчислень); розробка стандартів, що враховують галузеві особливості (медицина, фінанси, енергетика), спрощення та адаптація стандартів для різних масштабів бізнесу (малий і середній бізнес).

Це наддасте змогу отримати збільшення охоплення стандартами різних типів організацій та підвищення готовності до нових типів загроз.

Що стосується посилення міжнародного співробітництва у сфері кібербезпеки, це – створення глобальних платформ для обміну досвідом та інформацією про кіберзагрози, розробка універсальних стандартів, які будуть взаємно прийнятими різними країнами, підтримка країн, що розвиваються, у впровадженні кібербезпеки.

Це наддасте змогу отримати такий очікуваний ефект, як зменшення розриву між країнами у рівні кіберзахисту та підвищення ефективності міжнародної координації у боротьбі з кіберзлочинністю.

Що стосується освітніх ініціатив для підвищення рівня компетенцій у сфері кібербезпеки, це – впровадження освітніх програм з кібербезпеки у школах та університетах, підвищення кваліфікації існуючих фахівців через тренінги та сертифікації, організація національних і міжнародних конференцій, хакатонів, семінарів.

Це наддасте змогу отримати такий очікуваний ефект, як формування кадрів, здатних ефективно впроваджувати сучасні стандарти та підвищення загального рівня кібергігієни серед населення.

Реалізація зазначених рекомендацій дозволить створити більш гнучку, адаптивну та ефективну систему кібербезпеки, яка відповідатиме сучасним викликам цифрового світу, забезпечуючи захист держави, бізнесу та громадян.

Висновки з дослідження

1. Підводячи підсумки аналізу систем стандартів і правових норм, можна зазначити, що міжнародні стандарти, такі як ISO/IEC 27001 та ISO/IEC 27002, забезпечують фундаментальні принципи для створення систем управління інформаційною безпекою, сприяючи уніфікації підходів та управлінню ризиками.

Але спостерігаються труднощі впровадження національних норм, тому адаптація міжнародних стандартів до національних реалій потребує врахування економічних, юридичних та технологічних особливостей кожної країни. Це уповільнює процес інтеграції сучасних заходів безпеки.

Разом з тим, динамічний розвиток кіберзагроз вимагає регулярного оновлення нормативно-правової бази для ефективної протидії новим викликам.

2. Також спостерігається важливість комплексного підходу до забезпечення інформаційної безпеки. Це по-перше системність, коли забезпечення інформаційної безпеки повинно включати як технічні, так і організаційні заходи. При цьому важливо забезпечити інтеграцію стандартів, правових норм та управлінських рішень.

По-друге, це освіта та обізнаність, коли необхідно підвищувати рівень знань та компетенцій як серед фахівців, так і серед широкого загалу, щоб запобігати основним кіберзагрозам.

По-третє, це міжнародне співробітництво, коли глобальний характер кіберзагроз потребує координації зусиль на міждержавному рівні, включаючи обмін інформацією та кращими практиками.

По-четверте, це інновації, коли для протидії новим викликам у сфері кібербезпеки важливо постійно розробляти та впроваджувати сучасні технології, які відповідають актуальним загрозам.

Це дозволить створити ефективну організацію системи стандартів та правових норм інформаційної безпеки, а тому створити безпечне інформаційне середовище, яке сприятиме стабільному розвитку суспільства, бізнесу та держави в умовах цифрової трансформації.

ЛІТЕРАТУРА

1. ДСТУ ISO/IEC 27000:2018. Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою (ISO/IEC 27000:2016, IDT).
2. ДСТУ ISO/IEC 27002:2018 Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки (ISO/IEC 27002:2013; Cor 1:2014, IDT).
3. IEEE 802.11-2020 – стандарт безпеки бездротових локальних мереж, контроль доступу (MAC) та функції фізичного рівня (PHY).
4. Впровадження засобів захисту інформації для споживачів та постачальників хмарних послуг на основі стандарту ISO/IEC 27017.
5. Стандарт безпеки даних платіжних карт PCI DSS. Стандарт FINRA для забезпечення захисту даних користувачів при здійсненні фінансових операцій.

6. Інформаційна безпека держави: навч. посіб. для студ. спец. 6.170103 «Управління інформаційною безпекою», 125 «Кібербезпека»/ В.І. Гур'єв, Д.Б. Мехед, Ю.М. Ткач, І.В. Фірсова. Ніжин: ФОП Лук'яненко В.В. ТПК «Орхідея», 2021. 166 с. : іл.
7. Tupkalo V., Zaplotynskyi B. Fundamentals of information security management system engineering of modern process-oriented enterprises: monograph. Kyiv: KUIPL, 2024. 81 p., https://www.lap-publishing.com
8. Tupkalo V.M., Bogomya V.I., Iarmolatii A.V. Information security management system: problem aspects of implementation. Сучасні аспекти модернізації науки: стан, проблеми, тенденції розвитку: матеріали XXXVIII Міжнародної науково-практичної конференції / за ред. І.В. Жукової, Є.О. Романенка. м. Брно (Чехія): ГО «ВАДНД», 07 листопада 2023 р. С.276-280.
9. Корченко О.Г. Аудит та управління інцидентами інформаційної безпеки // О.Г. Корченко, С.О. Гнатюк, С.В. Казмірчук, В.М. Панченко, С.В. Мельник. Київ: Центр навч.-наук. та наук.-пр. видань НА СБ України, 2020. 193 с.
10. Юдін О.І. Захист інформації в мережах передачі даних // О.І. Юдін, О.Г. Корченко, Г.Ф. Конахович Київ: Вид-во ТОВ «НВП» Інтерсервіс», 2021. 716 с.
11. Юдін О.К. Інформаційна безпека. Нормативно-правове забезпечення: підручник / О.К.Юдін. Київ : НАУ, 2021. 639 с.
12. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / [В. О. Хорошко, В.Б. Толубко, С.В. Толюпа]; за заг. ред. д-ра техн. наук, професора В.Б. Толубка. Київ: ДУТ, 2021, 288 с.
13. Богом'я В.І., Кочегаров В.С. Кібербезпека в хмарних сервісах за допомогою застосування криптографічних методів. Водний транспорт. 2022. Вип.1(35). С.25–32.

Bohomia V. I., Cheremisina L. O., Yarmolatii A. V., Galynko V.V.

EFFECTIVE ORGANIZATION OF THE SYSTEM OF STANDARDS AND LEGAL NORMS OF INFORMATION SECURITY

Modern society actively employs digital technologies in various areas of life: the economy, healthcare, education, public administration, and more. This creates new opportunities but simultaneously opens pathways for the emergence of cyber threats.

All this leads to significant economic losses caused by cyberattacks. The damage inflicted by cyberattacks amounts to billions of dollars annually. Information protection is a crucial element of a state's economic stability and national security.

Thus, the relevance of this article is driven by the need to counter contemporary cyber threats, ensure information security, comply with legislative requirements, and adapt to rapid changes in the digital world.

It is known that international standards are often developed with consideration of global practices, but their application can be complicated by local specifics. General challenges in implementing standards and legal norms have already been identified by experts, but the specific issues in ensuring cybersecurity and the recommendations needed to improve the system of standards and legal norms have not been fully characterized.

The aim of this article is to analyze the existing systems of standards and legal norms in the field of information security to understand their effectiveness, relevance, and potential for improvement, and to develop appropriate recommendations.

Based on the analysis, it can be noted that international standards, such as ISO/IEC 27001 and ISO/IEC 27002, provide fundamental principles for creating information security management systems, contributing to the unification of approaches and risk management.

At the same time, the dynamic evolution of cyber threats requires the regular updating of the regulatory framework to effectively address new challenges.

Moreover, the importance of a comprehensive approach to ensuring information security has been observed. This will enable the creation of an effective organization of the system of standards and legal norms of information security, fostering a secure information environment that supports the stable development of society, business, and the state in the context of digital transformation.

Keywords: *information security, cybersecurity, cyber threat, international standards, national standards, legal norms, effectiveness, system*