**Володимир Хилеико,** Д.т.н., професор, професор кафедри комп'ютерних наук
Національний університет біоресурсів і природокористування України, Київ, Україна
ORCID ID 0000-0003-3491-8621
vkhilenko@nubip.edu.ua
**Ryszard Strzelecki,**
Full Professor - Department of Power Electronics and Electrical Machines (Faculty of Electrical and Control Enginering) Gdańsk University of Technology, Gdańsk, Poland
ORCID ID 0000-0001-9437-9450
ryszard.strzelecki@pg.edu.pl
**Бахытжан Ахметов, Т.ғ.д., профессор,**
**Абай атыдағы Қазақ ұлттық педагогикалық уиверситеті, Алматы, Қазақстаи**
ORCID ID 0000-0001-5622-2233
bakhytzhan.akhmetov.54@mail.ru
**Олексій Степаиов,** Асистент кафедри комп'ютерних наук
Національний університет біоресурсів і природокористування України, Київ, Україна
ORCID ID 0000-0002-0939-6991
stepanov@nubip.edu.ua

# НОВІ ТЕХНОЛОГІЇ ПОКРАЩЕННЯ БЕЗПЕКИ ІНФОРМАЦІЙНИХ СИСТЕМ ПОСТКВАНТОВОЇ ЕРИ

**Аиотація.** Стаття присвячена аналізу проблем побудови систем кібербезпеки постквантової ери. Проведено аналіз тенденцій розвитку квантових комп'ютерів та мінімізації кількості кубітів з точки зору загроз несанкціонованого декодування при використанні проблемно-орієнтованих алгоритмів. Розглянуто питання вибору чисельних методів, що використовуються при визначенні технологічних параметрів систем кібербезпеки, зокрема, для визначення часу зміни шифру та при прогнозуванні кібератак. На основі запропонованих варіантів реалізації парадигми побудови постквантової системи кібербезпеки, розглянутих в [1] та [6], проведені модельні розрахунки власних чисел матриці.
**Ключові слова:** системи керування, математичне та програмно-алгоритмічне забезпечення, кібербезпека, квантові комп'ютери, постквантова ера, розрахунок власних значень матриць.

## 1. ВСТУП

Не секрет, що використання стандартних методів безпеки у майбутньому стає неможливим із появою комп'ютерів нового рівня – квантових комп'ютерів. Так, вони значно підвищать наші можливості по обробітку великих об'ємів даних і вирішенню складних математичних завдань та моделювань, але також несуть загрозу кібербезпеці у зломі різноманітних систем шифрування. Ця загроза обумовлена можливостями квантових обчислювальних систем, які дозволяють розшифрувати будь-яку секретну інформацію, зашифровану існуючими алгоритмами шифрування, і змінити її, викликаючи системні збої і непрацездатність інформаційної системи. Нами пропонується побудова системи захисту інформації відповідно до рівня, що відповідає рівню загроз на поточному етапі технічного розвитку.

**Постановка проблеми.**

Надійність і ефективність розроблених в попередні десятиліття алгоритмів кодування і сама ідеологія концепції комп'ютерної безпеки (RSA, AES і т.д.) вже давно не викликають сумнівів. Однак з'являються технічні можливості (надпотужні суперкомп'ютери, багатопроцесорні обчислювальні системи на базі нейронних мереж і, в першу чергу, квантові комп'ютери), які приводять до того, що минулі рішення в області інформаційної безпеки вже не відповідають завданням сьогодення: захист від

можливості розкриття шифру високошвидкісним автоматизованим перебором з використанням квантових обчислювальних систем.

Отже, як зазначається в [1], «нова ідеологія побудови систем кібербезпеки повинна базуватися не на концепції завантаження «хакерського» обладнання космічною кількістю обчислень, а на концепції «забезпечення неефективності суперкомп'ютера», тобто використання такої технології кодування, при якій суперкомп'ютер, що використовується як засіб «підбору» шифру, не забезпечує досягнення результату – розшифровки інформації, як би його потужність не співвідносилася з обсягом обчислень».

**Мета публікації.**

Враховуючи це, метою статті є дослідження нових програмно-алгоритмічних рішень покращення безпеки інформаційних систем у постквантову еру.

## 2. ТЕОРЕТИЧНІ ОСНОВИ

Припустимо, що впровадження систем кібербезпеки нового покоління здійснюється відповідно до парадигми [1]

$$t_{hac} >> t_{sig}, t_{hac} >> t_{re}, t_{en} << t_{hac}, t_{cct} << t_{hac}$$

$$q_{dk} \in [x_{min}, x_{max}],$$

де $t_{hac}$ – час потрібний для взлому, $t_{sig}$ – час, протягом якого інформація зберігає свою цінність, $t_{re}$ – час, в якому оцінюється значення використовуваного в літературі терміну «несанкціоноване розшифрування за розумний час», $t_{en}$ – час шифрування, $t_{cct}$ – інтервал зміни шифру, $q_{dk}$ – кількість обчислень, які необхідно зробити для визначення точного значення ключа, $x_{min}$ та $x_{max}$ – мінімально та максимально допустиме значення діапазону значень секретного ключа, при якому законний користувач зможе коректно декодувати інформацію.

Як зазначається в низці публікацій, очікуване на ринку використання квантових комп'ютерів, які забезпечують рівень промислового використання, може дати можливість декодувати будь-яку шифровану інформацію, закодовану за допомогою існуючих алгоритмів шифрування [2-4]. Розвиток апаратної бази і розробка спеціалізованих обчислювальних алгоритмів, які прискорюють вирішення математичних завдань та використовуються для несанкціонованого декодування секретної інформації, створюють ефект синергії і в геометричній прогресії наближаються до моменту, коли вразливість систем кіберзахисту стає теоретично обґрунтованою і може бути легко використана на практиці. Зокрема, представлений в [5] алгоритм вирішення задачі розкладання на множники (алгоритм Шора), теоретично показує можливість злому використовуваних в даний час алгоритмів шифрування за допомогою потужних квантових комп'ютерів, розробка яких в даний час інтенсивно ведеться.

Водночас, реалізація постквантової парадигми побудови систем кібербезпеки [1] не виключає доцільності заміни інтервалу зміни шифру (або вибору режиму роботи системи кіберзахисту) залежно від поточного рівня кіберзагроз. Вибір «безпечного» часу зміни шифру пов'язаний з оцінкою існуючого рівня кібератак і його прогнозуванням, що в свою чергу вимагає обчислення власних значень матриць, що використовуються у відповідних динамічних моделях. Ще одним варіантом впровадження посквантової парадигми є використання програмно-апаратних модулів зазначених у [6], для яких також потрібно обраховувати власні числа матриць.

## 3. РЕЗУЛЬТАТИ ТА ОБГОВОРЕННЯ

Модельні розрахунки власних значень матриць проводилися з використанням чотирьох різних методів: Лавер'є-Ньютона, Крилова, степеневого методу та методу Хиленка для матриць різного ступеня жорсткості. Як зазначалося в [7], ці методи можна розділити на дві групи: методи не орієнтовані на обчислення, пов'язані з жорсткими

матрицями (перша група) і методи, орієнтовані на роботу з жорсткими матрицями (друга група). Модельні експерименти проводилися з квадратними матрицями розмірності $N_1 = 5$, $N_2 = 7$ і $N_3 = 10$. Порівняльна оцінка часу роботи процесора не проводилася через малий розмір матриць. Модельна матриця для розмірності 5x5 наведена в таблиці 1, а результати обчислень зведені в таблиці 2:

*Таблиця 1*

**Модельна матриця розмірності 5x5**

| | | | | |
|---|---|---|---|---|
| -900 | 100 | 10 | 50 | 50 |
| 100 | -700 | 50 | 10 | 50 |
| 10 | 50 | -400 | 40 | 10 |
| 50 | 10 | 40 | -200 | 10 |
| 50 | 50 | 10 | 10 | -120 |

*Таблиця 2*

**Визначення найбільшого власного числа матриці (5x5) із заданим діапазоном допустимої зміни чисел.**

| Діапазон | Степеневий метод | Метод Хиленка | Метод Лавер'є-Ньютона | Метод Крилова |
|---|---|---|---|---|
| (-100000 - +100000). | -944,992650 | -944.942 | -944,992754 | -944,992754 |
| (-800 - +800) | -944,992532 | -944.942 | -675,741796 | -675,741796 |

## ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Результати, наведені в таблиці 2, свідчать про доцільність використання методів другої групи для істотно жорстких матриць великих розмірів. У той же час, як зазначалося в [7], застосування методів першої групи навіть для матриць малих розмірів вимагає певної обережності у виборі діапазону методу, що може ускладнити автоматизацію обчислень, в першу чергу для жорстких матриць великих розмірів. Таким чином, використання методів другої групи спростить процес автоматизації підбору оптимального часу зміни шифру для покращення рівня безпеки інформаційних систем.

## ПОСИЛАННЯ

[1] Khilenko, V.V. Formation of a New Conception and a Paradigm of Constructing Cybersecurity Systems. Cybern Syst Anal 55, 354–358 (2019). https://doi.org/10.1007/s10559-019-00141-8

[2] Quantum computational advantage with 216 squeezed-state qubits. https://xanadu.ai/products/borealis/.

[3] Maxwell: neutral atom quantum processor" (pdf). M Squared. https://www.m2lasers.com/quantum-datasheet.html?file=Maxwell_Explainer.pdf

[4] Bao Yan, Z. Tan, +21 authors G. Long, Factoring integers with sublinear resources on a superconducting quantum processor, Education, Materials Science, 2022 https://doi.org/10.48550/arXiv.2212.12372.

[5] Shor P., Algorithms for quantum computation: discrete logarithms and factoring, in Proc. 35th Ann. Symp. on Foundations of Computer Science (1994) pp. 124–134. doi:10.1109/sfcs.1994.365700

[6] Khylenko V.V. System for transmitting encoded information. PCT /UA2017/000021. 07.09.2018. Pub. No. WO/2018/160155. https://patentscope.wipo.int/search/ru/detail.jsf?docId=WO2018160155

[7] Khilenko, V.V., Stepanov, O.V., Kotuliak, I., Reis, M. Optimization of the Selection of Software Elements in Control Systems with Significantly Different-Speed Processes. Cybernetics and Systems Analysis, 2021, 57(2), pp. 185–189. https://doi.org/10.1007/s10559-021-00342-0

MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE

NATIONAL UNIVERSITY OF LIFE AND ENVIRONMENTAL SCIENCES OF UKRAINE

FACULTY OF INFORMATION TECHNOLOGY

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ

ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

# PROCEEDINGS

# МАТЕРІАЛИ

XI International scientific conference

XI Міжнародної науково-практичної конференції

# GLOBAL AND REGIONAL PROBLEMS OF INFORMATIZATION IN SOCIETY AND NATURE USING '2023

# ГЛОБАЛЬНІ ТА РЕГІОНАЛЬНІ ПРОБЛЕМИ ІНФОРМАТИЗАЦІЇ В СУСПІЛЬСТВІ І ПРИРОДОКОРИСТУВАННІ '2023

15-16 November 2023

Kyiv, NULES of Ukraine

15-16 листопада 2023 року

Київ, НУБіП України

Kyiv 2023

Київ 2023

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ
І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ

ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

# МАТЕРІАЛИ

XI Міжнародної науково-практичної конференції

# ГЛОБАЛЬНІ ТА РЕГІОНАЛЬНІ ПРОБЛЕМИ ІНФОРМАТИЗАЦІЇ В СУСПІЛЬСТВІ І ПРИРОДОКОРИСТУВАННІ '2023

15-16 листопада 2023 року

Київ, НУБіП України

Київ 2023

УДК 004

Рекомендовано до друку вченою радою факультету інформаційних технологій Національного університету біоресурсів і природокористування України (протокол № 4 від 20.11.2023)

Укладач: к.е.н., доцент Харченко В.В.

Збірник матеріалів XI Міжнародної науково-практичної конференції "Глобальні та регіональні проблеми інформатизації в суспільстві і природокористуванні '2023", 15-16 листопада 2023 року, НУБіП України, К. НУБіП України, 2023. 117 с.

Відповідальність за зміст публікацій несуть автори.