НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»

ФАКУЛЬТЕТ КІБЕРБЕЗПЕКИ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

**28 листопада 2025 року**

# КІБЕРБЕЗПЕКА В СУЧАСНОМУ СВІТІ: АКТУАЛЬНІ ВИКЛИКИ

**МАТЕРІАЛИ VI МІЖНАРОДНОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ**

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**
**Національний університет «Одеська юридична академія»**
**Факультет кібербезпеки та інформаційних технологій**
**Кафедра кібербезпеки**

# КІБЕРБЕЗПЕКА В СУЧАСНОМУ СВІТІ: АКТУАЛЬНІ ВИКЛИКИ

**МАТЕРІАЛИ VI МІЖНАРОДНОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ**

**28 листопада 2025 року, м. Одеса**

Одеса, 2025

**MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE**
**National University «Odesa Law Academy»**
**Faculty of Cybersecurity and Information Technologies**
**Department of Cybersecurity**

# CYBERSECURITY IN TODAY'S WORLD: ACTUAL CHALLENGES

**MATERIALS OF THE VI INTERNATIONAL SCIENTIFIC AND PRACTICAL CONFERENCE**

**November 28, 2025, Odesa**

Odesa, 2025

УДК 004.056

**Відповідальній редактор:**

О. В. Дикий, декан факультету кібербезпеки та інформаційних технологій, кандидат юридичних наук, доцент

Матеріали видано в авторській редакції.
Повну відповідальність за достовірність та якість поданого матеріалу несуть учасники конференції, їхні наукові керівники, які рекомендували ці матеріали до друку.

Рекомендовано до друку
Вченою радою Національного університету
«Одеська юридична академія»
(протокол №3 від 29.11.2025 р.)

Матеріали Міжнародної науково-практичної конференції «Кібербезпека в сучасному світі: актуальні виклики» (м. Одеса, 28 листопада 2025 р.). Одеса, 2025. 287 с.

У конференції взяли участь студенти, аспіранти, молоді вчені, викладачі та науковці. Конференція проводиться на базі Національного університету «Одеська юридична академія».

UDC 004.056

## Editor-in-chief:

O. V. Dykyi, Dean of the Faculty of Cybersecurity and Information Technologies,
Candidate of Law, Associate Professor

The materials were published in the author's edition.
Full responsibility for the reliability and quality of the submitted material
bears the participants of the conference, their scientific supervisors,
who recommended these materials for publication.

Recommended for printing
by the Academic Council of the National University
«Odesa Law Academy»
(Minutes No. 3 dated 11/29/2025)

Materials of the International Scientific and Practical Conference «Cybersecurity in the Modern World: Current Challenges» (Odessa, November 28, 2025). Odesa, 2025. 287 p.

The conference was attended by students, postgraduates, young scientists, teachers and researchers. The conference is held at the National University «Odesa Law Academy».

**VI Міжнародна науково-практична конференція**

# «Кібербезпека в сучасному світі: актуальні виклики»

**28 листопада 2025 року**

**ТЕМАТИЧНІ НАПРЯМКИ КОНФЕРЕНЦІЇ:**

Секція 1. Алгоритмічні та технічні аспекти кібербезпеки

Секція 2. Штучний інтелект та інформаційні технології

Секція 3. Управлінські, соціальні та психологічні аспекти взаємодії з кіберпростором

Секція 4. Нормативно-правові засади кібербезпеки та захисту інформації

E-mail: kiberprostirconf@gmail.com (Для питань та тез)

**VI International Scientific and Practical Conference**

# «Cybersecurity in today's world: actual challenges»

**28 November 2025 year**

**THEMATIC DIRECTIONS OF THE CONFERENCE:**

Section 1. Algorithmic and technical aspects of cybersecurity

Section 2. Artificial intelligence and information technologies

Section 3. Management, social and psychological aspects of interaction with cyberspace

Section 4. Regulatory and legal principles of cybersecurity and information protection

E-mail: kiberprostirconf@gmail.com (Для питань та тез)

[4] Göppert J., Walz A., Sikora A. A Survey on Life-Cycle-Oriented Certificate Management in Industrial Networking Environments. J. Sens. Actuator Netw. (2024). doi:10.3390/jsan13020026.
[5] Renato Lo Cigno, Francesco Gringoli, Stefania Bartoletti, Marco Cominelli, Lorenzo Ghiro, and Samuele Zanini. Communication and Sensing: Wireless PHY-Layer Threats to Security and Privacy for IoT Systems and Possible Countermeasures. Information 2025, 16(1), 31; https://doi.org/10.3390/info16010031.
[6] Volodymyr Maksymovych, Elena Nyemkova, Connie Justice, Mariia Shabatura, Oleh Harasymchuk, Yuriy Lakh and Morika Rusynko. Simulation of Authentication in Information-Processing Electronic Devices Based on Poisson Pulse Sequence Generators. Electronics 2022, 11(13), 2039; https://doi.org/10.3390/electronics11132039.

**Ключові слова**: безпека даних; AWS IoT Core; методи шифрування; кіберзахист IoT-пристроїв; апаратно-програмні рішення; ESP32; FreeRTOS.
**Keywords**: data security; AWS IoT Core; encryption methods; cybersecurity of IoT devices; hardware and software solutions; ESP32; FreeRTOS.

## МЕТОД ФАКТОРИЗАЦІЇ ВЕЛИКИХ ЧИСЕЛ

***Тимошенко Лідія***
*кандидат економічних наук, доцент кафедри кібербезпеки та програмного забезпечення Національного університету «Одеська політехніка»*
***Алєксєєва Софія***
*магістрант кафедри кібербезпеки та програмного забезпечення Національного університету «Одеська політехніка»*

Забезпечення інформаційної безпеки є одним із ключових напрямів сучасної кібербезпеки. Особливе місце посідають асиметричні криптографічні системи, як RSA, надійність яких ґрунтується на складності задачі факторизації великих чисел. Проте з розвитком обчислювальної техніки та появою квантових технологій необхідне вдосконалення існуючих методів. Одним із перспективних підходів є модифікація методу Ферма, який є ефективним для близьких за значенням множників[1]. Його удосконалення може забезпечити підвищення ефективності криптоаналізу сучасних систем шифрування.

*Метою* дослідження є зменшення обчислювальної складності алгоритму факторизації великих чисел шляхом удосконалення класичного методу Ферма для оцінки криптостійкості RSA-подібних систем.

Факторизація великих чисел є однією з основних математичних задач, що забезпечує безпеку криптографічних систем з відкритим ключем [2]. Метод Ферма базується на представленні непарного числа як різниці двох квадратів $N = x^2 - y^2 = (x - y)(x + y)$ . Складність даного методу

оцінюється як *O(n(log2n)2)*. Метод простий для алгоритмічної реалізації, тому доцільно удосконалити його для можливої реалізації на звичайному комп'ютері для чисел великої довжини.

Перша ідея модифікації методу полягає у використанні системи обчислення в залишкових класах базису Крестенсона, яка дає змогу виконувати операції над меншими числами – лишками великих чисел, та без наскрізних переносів позиційних систем обчислень, що істотно знижує витрати обчислювальних ресурсів та скорочує час. У системи обчислень в залишкових класах всі операції є модульними.

Модифікований алгоритм містить перевірку можливості існування квадратного кореня за модулем з використанням символів Якобі. Це дозволяє відкидати значення, які не задовольняють умові існування кореня, і тим самим скорочує кількість ітерацій пошуку. Основними операціями алгоритму є пошук символа Якобі, перевірка чи добувається корінь квадратний за модулем та добування кореня від числа. Загальна складність розробленого алгоритму обчислюється як *O(nlog2n+2log22n+4n)» O(nlog2n)*. Отже, складність алгоритму зменшується з експоненційної до субекспоненційної для певного класу чисел.

Додатково система залишкових класів забезпечує паралельність обчислень: кожен модуль може оброблятись незалежно, що дозволяє реалізувати алгоритм на багатопроцесорних або кластерних системах.

Практична реалізація алгоритму виконана у середовищі C++ Builder, що дало змогу створити застосунок з графічним інтерфейсом для введення чисел, запуску факторизації та аналізу результатів. Тестування показало, що використання модифікованого методу скорочує час виконання у порівнянні з класичною реалізацією на 25–30 % при середніх значеннях модуля до 512 біт.

**Висновки.**Таким чином, отримана модифікація методу є перспективною для оцінки криптостійкості асиметричних систем та подальших досліджень у сфері оптимізації факторизаційних алгоритмів.

## Список використаної літератури:

1. Wagon S. Fermat's Factoring Method. URL: http://mathworld. wolfram.com/FermatsFactorizationMethod.html
2. Timoshenko L., et al. Factorization algorithms for cryptographic analysis of asymmetric crypto systems. Informatics and mathematical methods in modeling, 2014, 4,№ 4: 342-348.

**Ключові слова:** криптографія, факторизація, система обчислень, лишки.
**Keywords:** cryptography, factorization, calculation system, remainders.

# ЗМІСТ