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)

5. A. Tosun, "Automating threat modeling: Securing the future of IoT and cyber systems," Ph.D. dissertation, Dept. Comput. Sci., Tech. Univ. Denmark, Kongens Lyngby, Denmark, 2024.
6. M. Beyrouti, "Risk identification and secure management for IoT systems," Ph.D. dissertation, Univ. Technol. Compiègne, Compiègne, France, 2025.
7. T. Ali, M. Al-Khalidi, and R. Al-Zaidi, "Information security risk assessment methods in cloud computing: Comprehensive review," J. Comput. Inf. Syst., vol. 64, no. 5, pp. 1-22, Mar. 2024. DOI: 10.1080/08874417.2024.2329985.
8. M. Beyrouti et al., "Risk assessment model for IoT-based critical assets," in Proc. Int. Conf. Inf. Syst. Secur. Privacy (ICISSP), SCITEPRESS, 2025, pp. 132008-1-132008-10.
9. A. Lounis et al., "Framework for IoT security risk assessment and management," Int. J. Adv. Eng. Sci. Manag., vol. 6, no. 4, pp. 1-15, 2024
10. M. Beyrouti et al., "Vulnerability-oriented risk identification framework for IoT risk assessment," Internet Things, vol. 27, p. 101333, Jun. 2025. DOI: 10.1016/j.iot.2024.101333.
11. S. Chehida et al., "Threats and corrective measures for IoT security with observance of ISO/IEC 27001," arXiv:2010.08793 [cs.CR], Oct. 2020
12. M. A. Waqdan, H. Louafi, and M. Mouhoub, "Security risk assessment in IoT environments: A taxonomy and survey," SSRN Electron. J., Jan. 2025.
13. M. Beyrouti et al., "A comprehensive risk assessment framework for IoT-enabled infrastructure," in Proc. Int. Conf. Inf. Syst. Secur. Privacy (ICISSP), SCITEPRESS, 2023, pp. 120609-1-120609-10.
14. P. Radanliev et al., "AI security and cyber risk in IoT systems," Front. Big Data, vol. 7, p. 1402745, Oct. 2024. DOI: 10.3389/fdata.2024.1402745.
15. S. Raf, "Analyzing threats, vulnerabilities, and mitigation strategies in IoT," in Proc. FRUCT Conf., vol. 36, 2024, pp. 1-10.

**Ключові слова:** IoT-пристрої, вразливості безпеки, розумний дім, оцінка ризиків.
**Keywords:** IoT devices, security vulnerabilities, smart home, risk assessment.

## ПРОЦЕДУРА ШИФРУВАННЯ З ВИКОРИСТАННЯМ ДВОМІРНИХ КЛІТИННИХ АВТОМАТІВ

***Бойко Віктор***

*доцент кафедри кібербезпеки Національного університету «Одеська юридична академія», кандидат технічних наук*

***Сутурін Євгеній***

*студент 4-го курсу факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»*

В умовах підвищення швидкості сучасного розвитку ефективності застосування обчислювальних потужностей та механізмів застосування, з метою реалізації кіберзагроз для компрометування та завдання шкоди комплексним системам захисту інформації, зумовленого впровадженням

новітніх утиліт при проведенні кібератак, використання не ресурсоємних та незначних за часовими витратами процедур шифрування, з цілю забезпечення підвищеної конфіденційності інформації, набуває більшої актуальності. Використання симетричного та асиметричного шифрування, з метою дотримання конфіденційності завдяки утворенню достатньо стійкої системи, призводить до застосування різноманітних засобів реалізації алгоритмів шифрування для покриття недоліків існуючих систем та удосконалення реалізації видів шифрування. Для цього, з цілю отримання псевдовипадкових значень та зменшення складності виконання алгоритму завдяки простим та швидким операціям, використовують клітинні автомати.

Клітинні автомати є дискретними моделями обчислення, що складаються з кліток, стан яких формує таблицю можливих комбінацій та їх рішень, основою якої є обрання певного значення з подальшим формуванням, на його базі, правила, за яким і визначається поведінка автомату [1]. Визначення кількості клітинок сусідів, що впливають на клітину для якої розраховується наступний стан, а також їх розташування, як результат утворюючі певний принцип підрахування логіки перетворень клітинного автомата, є діалектом, на основі якого збільшується можлива кількість комбінацій для таблиці рішень [2].

Кожна клітина автомату може приймати лише один стан з можливої, кінцевої, кількості множини станів, залежної від обраного діалекту, а значення клітин можуть набувати двох станів – 0 чи 1, які клітина приймає в різні моменти часу. Механізм праці клітинних автоматів дозволяє проводити з результатами їх перетворень, виступаючих у якості ключа, побітові операції складання (далі - XOR), що є простою та швидкою для виконання обчислювальним приладом операцією. Обраним ключом, для проведення операції XOR, може бути як n-ітерація виконання правила певного діалекту клітинного автомату, так і використання значень послідовності n-ітерацій результату цього виконання, залежно від довжини обраного для шифрування повідомлення. Можлива проблема обмеженості розмірною сітки автомату може бути вирішена завдяки застосуванню інших правил для кутових клітин або за використанням обробки з періодичними межовими умовами, що призводить до тороїдального розташування та дозволяє уникнути створення безмежною сітки автомату та забезпечити обчислення клітинок згідно з правилами визначеного діалекту [2].

Для використання процедури шифрування з метою шифрування вхідного повідомлення, за допомогою клітинного автомату, буде використано його двомірну варіацію, з певним обраним діалектом та правилом до нього. В процесі шифрування обирається псевдовипадкове правило, яке відоме та надається на збереження лише учасникам співбесіди [3, 4]. Двійкова послідовність визначеного правила являє собою першу ітерацію процедури.

Залежно від розміру повідомлення та обраного розміру сітки для ітерацій клітинного апарату, незаповнені біти, для зрівняння бітової довжини повідомлення з бітової довжиною розмірної сітки, буде заповнено нульовими значеннями. У випадку якщо бітова довжина повідомлення (далі - БДП) довша за бітову довжину розмірної сітки (далі – БДРС), значення БДП ділиться з остачею на БДРС, утворюючі бітові блоки, що дорівнюють БДРС, де залишок доповнюється нульовими значеннями до моменту поки довжина цього блоку не буде дорівнювати БДРС. Для шифрування кожного n-блоку буде використовуватись n-ітерація обраного правила.

З метою не ресурсоємності, операції над блоками будуть виконуватися послідовно. Після розбиття повідомлення на блоки, що дорівнюють БДРС, операція XOR з бітовими послідовностями у блоках буде виконуватися по черзі, блок за блоком, видаляючи з пам'яті значення складових, що було використано для отримання нового блоку. Завдяки цьому навантаження на систему при обробці великих повідомлень буде зменшено, а завдяки відсутності необхідності генерувати результат операції XOR для усіх блоків одночасно, обумовленою використанням розподілення операції на менші, блокові, буде зменшено кількість необхідного для її виконання часу. В певний момент перетворень така процедура дозволить зберігати втричі менше інформації у системі. Отримана послідовність блоків за результатами виконання операції XOR над блоками БДП та БДРС і буде зашифрованим повідомленням, що надсилається іншому учаснику співбесіди.

Процес розшифрування повторює алгоритм визначення зашифрованого повідомлення. Отримане повідомлення ділиться за остачею на тих самих умовах що і під час шифрування, після чого зашифрована бітова послідовність та отримані значення блоків з ітерацій обраного раніше, для користувачів співбесіди, правила по заданому діалекту, автомату, за поблочною операцією XOR, з такою ж реалізацією не ресурсоємності, перетворюється на розшифроване повідомлення, надіслане іншим співрозмовником.

Спираючись на збільшення уваги до аналізу поведінки різноманітних діалектів та їх правил, а також симуляцій різних початкових умов клітинних автоматів, тема набуває більшої актуальності у сфері криптографічних досліджень, що обумовлено здібністю клітинних автоматів утворювати з простих початкових умов складні, детерміновані, результати, зі збільшенням складності повернення на попередній крок з кожною наступною ітерацією. Таким чином, враховуючи розвиток обчислювальних приладів, є актуальним знаходження шляху реалізації не ресурсоємної процедури шифрування на основі двомірних клітинних апаратів.

**Список використаних джерел:**

1. Cellular Automaton. [Online]. URl: https://mathworld.wolfram.com/CellularAutomaton.html (accessed: 18.09.2025)

2. Stephen Wolfram: A new Kind of Science. [Online]. URL: https://www.wolfram-science.com/nks/ (accessed: 18.09.2025)
3. Rule 30. [Online]. URL: https://mathworld.wolfram.com/Rule30.html (accessed: 18.09.2025)
4. On the Generation of High-Quality Random Numbers by Two-Dimensional Cellular Automata. [Online]. URL: https://www.moshesipper.com/pubs/twod_rand.pdf (accessed: 18.09.2025)

**Ключові слова:** шифрування, псевдовипадкові значення, клітинний автомат, правило, діалект, таблиця рішень, стан, побітова операція складання, ітерація, БДП, БДРС, бітовий блок, бітова послідовність.
**Keywords:** encryption, pseudorandom values, cellular automaton, rule, dialect, decision table, state, bitwise addition operation, iteration, MBL, BLDG, bit block, bit sequence.

# ЗМІСТ