обчислювальну потужність архітектури, яка здатна безперебійно обробляти до 10 000 атомарних OSINT-запитів на годину. Завдяки синергії математичної моделі та інтелектуальних агентів, експериментальна точність ідентифікації загроз досягла 93,3%, а інтегральний показник F1-score склав 0,92. Крім того, автоматизація повного життєвого циклу розвідки дозволила скоротити час обробки 1 ГБ неструктурованих даних з 2-4 годин до 5-10 хвилин (приріст швидкодії у 12-48 разів).

Отже, такий підхід суттєво зменшує навантаження на аналітиків Security Operations Center (SOC) під час ручного сортування подій (на 58%) та допомагає автоматично формувати конкретні рекомендації щодо захисту периметра, забезпечуючи ефективний перехід компаній до проактивного управління корпоративними кіберризиками.

1. Ланде Д. В. OSINT у кібербезпеці : навч. посіб. Київ: ТОВ «Інжиніринг», 2024. 522 с.
2. Рибка Д. OSINT у забезпеченні національної безпеки. Науковий вісник Ужгородського національного університету. Серія: Право. 2023. Вип. 78. С. 344-348.
3. Фролов Д. І., Дягілєва М. С. Застосування технологій машинного навчання в кібербезпеці. Радіоелектроніка та молодь у XXI столітті. Харків : ХНУРЕ, 2025. №4. С. 97–99.
4. Чевардін В. Є., Юрченко О. В., Залужний О. В. Аналіз конкурентних атак на моделі машинного навчання систем кіберзахисту. Системи і технології зв'язку, інформатизації та кібербезпеки. 2023. №4. С. 9-15.

## Метод шифрування на основі збільшення кількості модулів у системі залишкових класів

УДК 004.056.55

Віктор Залізняк[1], Павло Басістий[2], Михайло Касянчук[3]

*[1, 3]Західноукраїнський національний університет,*
*[2]Тернопільський національний педагогічний університет*
*імені Володимира Гнатюка,*
*[1]viktor.zalizniak@gmail.com, [2]basi@ukr.net, [3]kasyanchuk@ukr.net*

У сучасних криптографічних системах важливим завданням є підвищення стійкості алгоритмів шифрування без істотного зниження їхньої продуктивності [1]. Одним із перспективних напрямів розв’язання цієї задачі є використання системи залишкових класів (СЗК), яка дає змогу подавати числові дані у вигляді набору залишків за системою попарно взаємно простих модулів [2]. Такий підхід забезпечує незалежність обчислень за кожним модулем і створює передумови для побудови швидкодіючих криптографічних перетворень.

Класичне шифрування в СЗК ґрунтується на представленні відкритого тексту як набору залишків та подальшому відновленні відповідного десяткового числа за допомогою китайської теореми про залишки (КТЗ). У такій схемі модулі є ключами, а криптостійкість істотно залежить від складності їх

визначення з боку криптоаналітика. Водночас базова схема може бути посилена шляхом зміни параметрів КТЗ, зокрема через розширення системи модулів.

Суть запропонованого методу полягає у введенні додаткового модуля системи. Для нього формується окремий залишок. Він може бути заданий довільно або виконувати контрольну функцію. Шифрування виконується за розширеною формулою КТЗ. При цьому виникає питання вибору добутку модулів. Якщо використовувати добуток лише початкової системи модулів, додатковий залишок не повністю впливає на результат і не завжди може виконувати контрольну функцію. Натомість використання добутку всіх модулів, включаючи додатковий, розширює діапазон можливих значень шифротексту та збільшує простір ключів.

Практичне значення такого підходу полягає в тому, що збільшення кількості модулів у СЗК ускладнює структуру криптографічного перетворення. Криптоаналітик має враховувати більшу кількість можливих комбінацій модулів, залишків та проміжних параметрів КТЗ. Крім того, додатковий модуль може використовуватися як механізм контролю цілісності повідомлення після розшифрування. Це особливо важливо для систем, у яких потрібно поєднати захист інформації з виявленням помилок передавання або обробки даних.

Отже, метод шифрування на основі збільшення кількості модулів у СЗК є ефективним способом підвищення криптографічної стійкості та розширення простору ключів. Подальші дослідження доцільно спрямувати на оптимальний вибір додаткових модулів, оцінювання стійкості до криптоаналітичних атак та реалізацію методу в апаратних і гібридних криптографічних системах.

1. 1. Nieles M., Dempsey K., Pillitteri V. *An Introduction to Information Security*. Gaithersburg : NIST, 2017. 101 p..
2. 2. P.V. Ananda Mohan. *Residue number systems: Theory and applications*. Birkhäuser, Basel. 2016. 351 p.

## Штучний інтелект як інструмент підтримки прийняття рішень у системах кібербезпеки

УДК 004.056:004.8

Роман Золотий[1], Ігор Чихіра[2], Віктор Устенко[3]

*Тернопільський національний технічний університет імені Івана Пулюя, [1]zolotyy@gmail.com, [2]ig.vi.chi@gmail.com, Івано-Франківська філія Університету "Україна", [3]ustenkotoda@gmail.com*

Зростання кількості кіберінцидентів і обсягів даних безпеки актуалізує використання штучного інтелекту як інструменту підтримки прийняття рішень у кібербезпеці. На відміну від суто сигнатурних засобів та засобів на основі правил, AI може швидко аналізувати журнали, мережевий трафік, події кінцевих пристроїв, хмарних сервісів та IoT-компонентів. Це важливо з огляду на поширення атак на доступність, програм-вимагачів, загроз даним, соціальної інженерії та експлуатації вразливостей [1].