зв'язки в графі ідентичності, тоді як обфускація лише тимчасово ускладнює обробку даних.

Таким чином, головна перевага компартменталізації над обфускацією полягає в тому, що вона ускладнює можливість автоматизованої кореляції даних, що змушує атакуючу сторону переходити від швидкого збору інформації до складного, ресурсомісткого та часто безрезультатного ручного інтелектуального розслідування.

Проте, поряд із високою ефективністю, метод компартменталізації накладає значні обмеження на користувача та потребує підвищених апаратних ресурсів для підтримки декількох ізольованих середовищ. Це створює поріг входження для пересічного користувача, проте є виправданим компромісом у контексті експоненціального зростання витрат атакуючої сторони

1. Cheng, H., Qiang, C., Cong, L., Xiao, J., Liu, S., Zhou, X., Wang, H., Ruan, M., & Lv, C. (2025). A Novel Data Obfuscation Framework Integrating Probability Density and Information Entropy for Privacy Preservation. *Applied Sciences*, *15*(3), 1261. https://doi.org/10.3390/app15031261
2. Івкова В.С., & Опірський І.Р., (2025). Дослідження можливості інтеграції методу компартменталізації у захист інформації у відкритих джерелах. *Computer systems and network*, *7*(2), 71–83. https://doi.org/10.23939/csn2025.02.071
3. Lopes, A. O., & Mengue, J. K. (2022). On information gain, Kullback-Leibler divergence, entropy production and the involution kernel. *Discrete & Continuous Dynamical Systems*, 0. https://doi.org/10.3934/dcds.2022026

Сучасний стан кібербезпеки в Україні

УДК 004.056.53

Кардашук Володимир[1]

Східноукраїнський національний університет, [1]kardashuk1@snu.edu.ua

Стрімкий розвиток інформаційних технологій суттєво випереджає створення надійних умов захисту цифрового кіберпростору. Для сучасного економічного розвитку критичним є забезпечення особистої безпеки, бізнесу та держави. Актуальним завданням сьогодення є створення комплексу заходів спрямованих на захист інформаційних ресурсів від кібератак, небажаного доступу, інших дій на модифікацію або знищення важливих даних. Сучасне інформаційне оточення швидко змінюється, що вимагає динамічно реагувати на загрози, адаптуватись до викликів та кібернетичних атак. Все більша кількість загроз, методів та стратегій використовує вразливості кіберзахисту.

Аналіз сучасного стану кібербезпеки в Україні показав недостатню координацію між суб'єктами кібербезпеки, що ускладнює координацію на кіберзагрози [1].

В останні роки підмічена тенденція еволюціонування загроз з незмінними мотивами фінансової вимоги [2].

Сучасні дослідження в сфері кібербезпеки спрямовані в таких новітніх сферах як штучний інтелект, блокчейн, квантові обчислення на системи кіберзахисту. Відмічено, що штучний інтелект є водночас найбільшою загрозою і найпотужнішим інструментом для захисту інформаційних систем.

Прогнозується, що до 2031 року буде зберігатись тенденція перевищення збитків (12 трлн. дол.) від кіберзлочинності над витратами (1 трлн. дол.) на захист, і це не тимчасовий дисбаланс, а фундаментальна проблема [3].

Актуальним постає питання подальшого розвитку Національної стратегії кібербезпеки в Україні як стратегічного пріоритету. На системи кіберзахисту свій вплив відіграють і зростаючий ринок хмарних сервісів таких як Google Cloud Platform, Microsoft, AWS, Azure. Хмари у 2026 році відіграють роль цифрового фундаменту інформаційного розвитку випереджаючи можливість кіберзахисту. В цій боротьбі поки перевага не на стороні кіберзахисту.

Що стосується застосування квантових обчислень для криптографічного перетворення, то дослідження в цій галузі ще тільки на початковому етапі розвитку не тільки в Україні, а і у світі. Формується новітня галузь постквантової криптографії на базі штучного інтелекту, як відповідь кіберзагрозам. Лідерство в цьому напрямку зберігають такі фірми, як Google (Quantum AI), Microsoft (Azure Quantum), Amazon (Braket, чіп Ocelot), Thale. Національний інститут стандартів і технологій США (NIST) планує у 2027 році закінчити розробку стандартів постквантової криптографії.

В поточній ситуації в Україна актуальним стає питання також об'єднанню урядів, корпорацій, інвесторів, компаній, незалежних експертів, стартапів, аналітичних центрів і наукових кіл для спільної протидії сучасним кіберзагрозам та обміну передовими рішеннями, практиками та тенденціями. Цим важливим питання був присвячений Київський Міжнародний Форум з Кіберстійкості 2026. Така всебічна робота спрямована на збільшення міцності в кібердомені для України та країн Європейського союзу через кіберстійкість на основі досвіду та знань, отриманих під час кібервійни, шляхом зміцнення міжнародного співробітництва та синергії з глобальними гравцями в державному та приватному секторах.

Крім того, загрози направлені проти кричної інфраструктури, вони також додатково впливають на процеси ухвалення рішень та суспільне сприйняття. Це спонукає дослідження таких кібератак та їх прогнозування для зміцнення кіберстійкості. Серед кібернетичних атак гостро стоїть питання протидії FIMI (Foreign Information Manipulation and Interference) нового покоління.

У секторах енергетики та телекомунікацій основна увага зосереджена на сучасних технологіях швидкого відновлення в умовах кібератак. В цьому питанні важливу ключову роль у зміцненні цифрової стійкості в Україні відіграють програми та масштабовані рішення для захисту критичної інфраструктури.

Стратегічно важливим кроком для України стало приєднання у жовтні 2025 року до Угоди про визнання загальних критеріїв (Common Criteria Recognition Arrangement – CCRA), яка встановлює єдині підходи до оцінювання засобів захисту інформації та підтвердження рівня довіри до такої оцінки, а також методології її проведення [4].

Стосовно кібергігієни рекомендується створювати надійні паролі, бути обережним з підозрілими повідомленнями, використовувати перевірені ресурси для фінансових операцій та відповідально ставитися до поширення особистої інформації в мережі.

Зростає фінансова підтримка партнерів на оновлення IT-інфраструктури, захист цифрових продуктів та навчання фахівців, що сприяє посиленню кібербезпеки та розвитку цифрової інфраструктури України.

1. Живило Є.О. Пріоритетні напрями національної стратегії кібербезпеки в контексті інтеграції до трирівневої моделі кібероборони. Державне будівництво. – № 1 (37). – 2025. – С. 229-251.
2. Олег Полігенько. Що відбувається на ринку кібербезпеки — колонка. URL: https://ain.ua/2026/04/15/shho-vidbuvajetsia-na-rinku-kiberbezpeki-kolonka/ (дата звернення: 04.05.2025).
3. Глобальна індустрія кібербезпеки станом на 2026 рік. Основні показники, тенденції та прогнози. URL: https://niss.gov.ua/doslidzhennya/natsionalna-bezpeka/hlobalna-industriya-kiberbezpeky-stanom-na-2026-rik-osnovni (дата звернення: 04.05.2025).
4. Приєднання до Угоди про визнання Common Criteria значно розширило інструментарій захисту інформації – перелік засобів та продуктів. URL: https://cip.gov.ua/ua/news/priyednannya-do-ugodi-pro-viznannya-common-criteria-znachno-rozshirilo-instrumentarii-zakhistu-informaciyi-perelik-zasobiv-ta-produktiv (дата звернення: 04.05.2025).

Метод шифрування растрових зображень засобами асиметричних криптосистем

УДК 004.056.5

Євгеній Кацубо

Національний університет «Одеська політехніка», 10252737@stud.op.edu.ua

В епоху глобальної цифровізації та безперервного обміну даними класичні асиметричні алгоритми попіксельного шифрування не здатні приховати просторову надлишковість та автокореляцію елементів, що призводить до візуалізації контурів об'єктів у шифротексті. Це зумовлює необхідність розробки комплексних гібридних моделей, які поєднують криптографічну стійкість факторизації великих чисел із методами нелінійного просторового маскування та внутрішньоблокового алгебраїчного перемішування.

Метою роботи є розробка та дослідження розширеної моделі модифікованого асиметричного алгоритму, що інтегрує двовимірну квадратичну координатну маску та механізми алгебраїчного зчеплення для досягнення максимальної ентропії шифротексту.

Запропонований у роботі метод розглядає зображення як матрицю, що поділяється на незалежні блоки по чотири суміжні пікселі. Диференційована обробка полягає в тому, що крайні пікселі піддаються експоненціюванню у