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

першому кільці лишків, а внутрішні — у другому, що повністю унеможливлює частотний криптоаналіз. Для руйнування візуальних патернів застосовується позиційно залежна квадратична маска, яка додає унікальне псевдовипадкове зміщення на основі глобальних координат блоку [1].

Для внутрішніх елементів реалізовано механізм алгебраїчного зчеплення через знаходження їхньої суми та різниці в модульному просторі, що створює потужний лавинний ефект. Використання цих операцій формує нерозривну залежність між сусідніми пікселями, тому будь-яка спроба локальної модифікації руйнує весь зашифрований блок, надійно захищаючи цілісність документа. Повна математична оборотність системи при використанні мультиплікативного оберненого елемента забезпечує бездоганне побітове відновлення оригінального зображення без жодних структурних втрат чи артефактів.

Проведені дослідження підтверджують, що поєднання векторного розбиття, двокільцевої обробки та позиційно-залежної маски забезпечує абсолютно рівномірний розподіл інтенсивностей на гістограмі шифротексту. Це повністю перетворює початкові візуальні дані на гетерогенний псевдовипадковий шум та експоненціально ускладнює проведення диференціальних і статистичних атак, роблячи запропонований підхід ефективним методом для конфіденційного електронного документообігу.

1. Zhang B., Liu L. Chaos-Based Image Encryption: Review, Application, and Challenges. *Mathematics*. 2023. Vol. 11, no. 11. P. 2585. DOI: https://doi.org/10.3390/math11112585

Порівняльний аналіз SDN-систем за критеріями кібербезпеки

УДК 004.056:004.7

Юрій Кльоц[1], Олексій Федоров[2]

Хмельницький національний університет, [1]klots@khmnu.edu.ua, [2] fedorovoo@khmnu.edu.ua

Програмно-конфігурована мережа є архітектурою, у якій функції керування трафіком логічно відокремлюються від функцій його передавання. На відміну від традиційної мережевої інфраструктури, де рішення щодо маршрутизації або комутації приймаються розподілено на кожному пристрої, у SDN значна частина логіки керування концентрується в контролері. Це забезпечує централізоване застосування політик, гнучке програмне керування трафіком, швидке впровадження змін конфігурації та можливість побудови систем автоматизованого виявлення аномалій [1].

З погляду кібербезпеки SDN-архітектура має подвійний характер. З одного боку, централізоване керування спрощує реалізацію політик сегментації, ізоляції вузлів, динамічного блокування потоків, перенаправлення трафіку на засоби аналізу та збирання телеметрії з мережевих пристроїв. З іншого боку, контролер, southbound-канали та програмно-керовані комутатори стають критичними об’єктами захисту. Компрометація контролера або порушення цілісності правил потоків може призвести до порушення роботи всієї мережевої