технічними комплексами: збірник тез доповідей всеукраїнської науково-практичної інтернет-конференції (11 травня 2016 року). – Луцьк: РВВ Луцького НТУ, 2016. – С. 41-43.

Красиленко В.Г., Нікітович Д.В.
Вінницький національний технічний університет

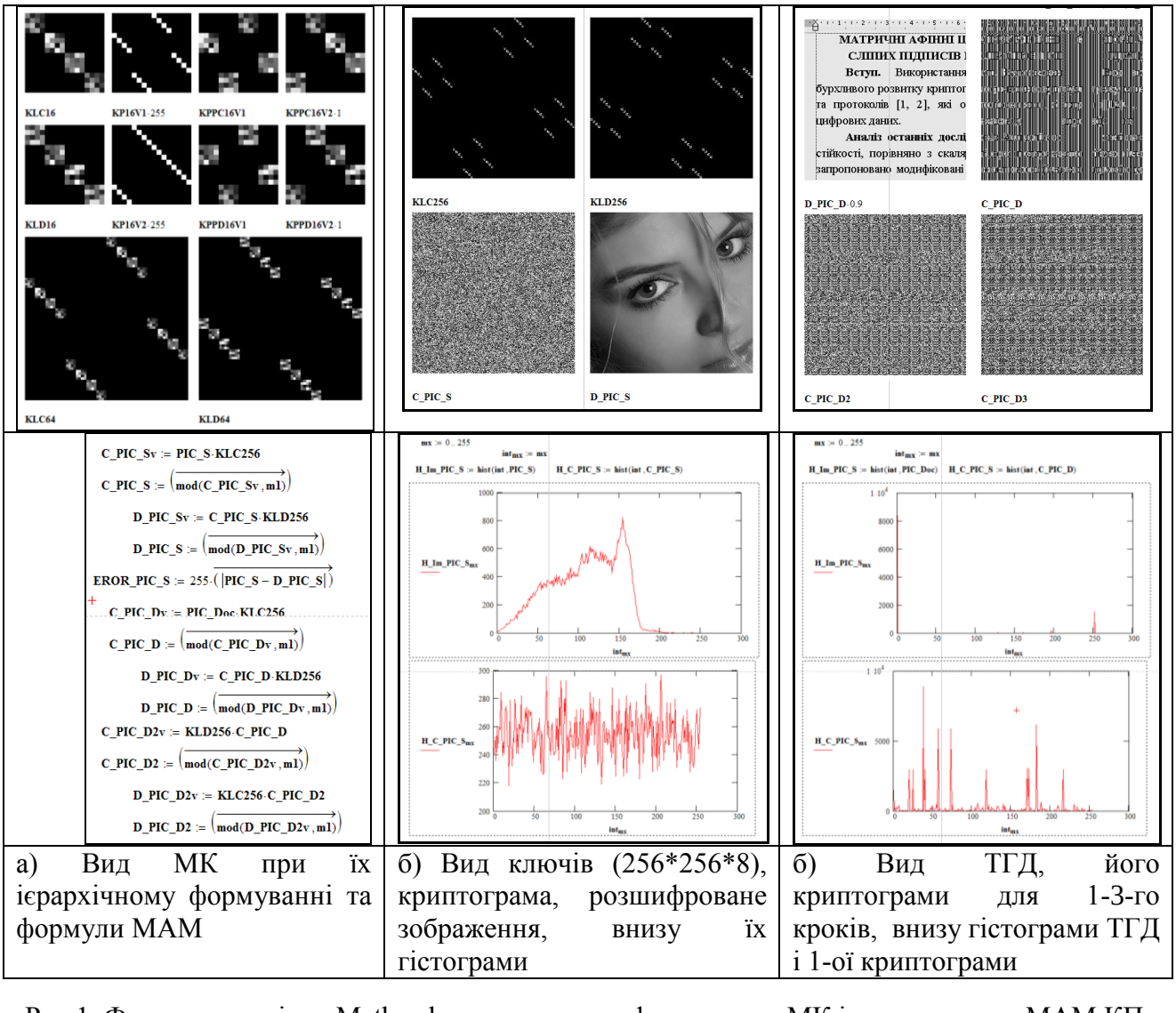
БАГАТОФУНКЦІОНАЛЬНІ ПАРАМЕТРИЧНІ МАТРИЧНО-АЛГЕБРАЇЧНІ МОДЕЛІ (МАМ) КРИПТОГРАФІЧНИХ ПЕРЕТВОРЕНЬ (КП) З ОПЕРАЦІЯМИ ЗА МОДУЛЕМ ТА ЇХ МОДЕЛЮВАННЯ

*Анотація. В роботі запропоновані та розглянуті нові моделі з операціями за модулем для КП, в тому числі зображень. Наводяться результати їх моделювання на прикладі прямих та обернених КП зображень, що свідчать про їх коректну роботу, зручність (всього 1 матрична процедура та 1 МК!), адаптованість до форматів, багатофункціональність (поєднання операцій матричних блокових замін з перестановками, як самих блоків так і елементів блоків, взаємозамінність циклових ітераційних процедур та матричних піднесень у степінь за модулем зі зручними і простими вибором параметрів та управлінням ними перетвореннями, формуваннями ключів), ефективність (орієнтація на матричні процесори). Розглянуті аспекти багатокрокових матричних алгебраїчних КП процедур на основі операцій за модулем і параметричних різновидів синтезу необхідних матричних ключів (МК). Показані експерименти зашифрування та розшифрування зображень (256*256 елементів) і текстово-графічних документів (ТГД) у програмному середовищі Mathcad.*

Вступ, аналіз досліджень і публікацій. На відміну від типових послідовних скалярних алгоритмів, моделей криптосистем поява нових паралельних алгоритмів, а особливо матриць багатопроцесорних засобів, потребує створення відповідних матрично-алгебраїчних моделей і систем матричного типу (МТ). Переваги КП ТГД у вигляді цифрових, табличних даних, малюнків, графіків, діаграм, підписів, віз, резолюцій, тощо, чорно-білих і кольорових зображень (З) матричними алгоритмами на основі узагальнених матричних афінних і афінно-перестановочних шифрів, в тому числі при створенні сліпих цифрових підписів були продемонстровані у роботах [1-4]. Їх базовими операціями є по-елементні множення, додавання за модулем матриць та матричні моделі перестановок (ММ_П) з процедурами множення матриць. Для збільшення ентропії та зміни гістограми З при їх КП на основі ММ_П необхідні декомпозиція бітових зрізів у модифікованих моделях та крім двох МК ще й два векторних (ВК) [5-6]. Модифікації вищезгаданих моделей дозволяють при КП перевіряти цілісність (Ц) криптограм та наявність у них перекручувань, що було показано в [7-8], як для чорно-білих так і кольорових зображень. Але, як засвідчили експерименти, деякі специфічні ТГД, наприклад скановані документи, мають значні по розмірах області з майже однаковою інтенсивністю пікселів, малу кількість градацій і дуже характерні гістограми, що потребує для їх КП збільшення крипто-стійкості шляхом пошуку вдосконалень МАМ, в тому числі і за рахунок розширення їх функціональності при збереженні уніфікованих матричних операцій, процедур [9]. Таким чином, метою роботи та актуальною є спроба розробок і подальшої модифікації, універсалізації та узагальнення МАМ для КП з метою покращення їх характеристик та стійкості, а моделювання та перевірка створених моделей на реальних інформаційних об’єктах (ІО) дозволить оцінити їх параметри, можливості та особливості застосувань.

Виклад матеріалу та результатів дослідження. Сутність запропонованих МАМ для КП полягає у застосуванні до матриць розмірністю N*N, як сукупностей байтів чи 8-бітних зображень (PIC_S, PIC_Doc, дивись рис.1), процедур матричного множення на відповідні 8-бітні МК тієї ж розмірності (KLC256, KLD256) з використанням операцій множення та додавання за модулем. Як видно з рис. 1-5, результати моделювання процесів прямого та оберненого КП ТГД і З розмірністю 256*256 ел. підтвердили коректну роботу моделей при застосуванні правильних ключів (рис.4) так і неправильних (рис.5). МК мали ієрархічну

структуру, розмірність 256*256 і складались як блочна матриця з 16*16 блоків розмірністю 16*16 ел-тів, а кожен з блоків (KLC16-ітий, KLD16) мав 4 під-блоки по 4*4ел., які за допомогою матриць перестановок P типу KP16V1, KP16V2, дозволять робити довільні перестановки блоків та під-блоків, як це показано на рис.1. Як блоки KLC, KLD так і повні ключі є взаємно оберненими матрицями при множенні їх за відповідним модулем. Суттєвою відмінністю пропонованих МК є те, що як самі блоки у цілій матриці, так і під-блоки, та й елементи в них можуть перемішуватись, тобто їх структури подібні матрицям перестановок. Таким чином криптографічна обробка блоків супроводжується одночасним перемішуванням як блоків так і під-блоків, і навіть їх елементів, як буде показано нами у цій роботі (рис.2-4). Але аналіз ентропій, гістограм З, ТГД та їх криптограм, як видно з рис.1, показує, що для ТГД, на відміну від зображення особи, навіть декількох ітераційних множень матриці даних (МД) на МК зліва чи справа може бути недостатньо, тим більше при застосуванні того ж МК.



а) Вид МК при їх ієрархічному формуванні та формули МАМ	б) Вид ключів (256*256*8), криптограма, розшифроване зображення, внизу їх гістограми	б) Вид ТГД, його криптограми для 1-3-го кроків, внизу гістограми ТГД і 1-ої криптограми

Рис.1. Фрагменти з вікон Mathcad з результатами формування МК і моделювання МАМ КП.

Тому нами запропоновано дві нові багатофункціональні параметричні МАМ КП, основна концептуальна ідея яких базується на використанні додаткових скалярних чи векторних ключів (ВК) в якості параметрів, що впливають на степені матриць МД та МК за модулем у моделях їх матричного множення та степінь і вид матриць перестановок блоків чи елементів. На кожному ітераційному кроці в залежності від ВК формуються різні МК. Фрагменти моделювання процесів формування матриць Р, циклових МК та їх складових, а також формули МАМ для прямого та оберненого КП і верифікації за допомогою параметричних

МК показані на рис. 2. На рис.3 показано вигляд деяких параметричних МК, а на рис. 4 та 5 - результати моделювання КП ТГД на основі параметричних МАМ та МК для випадків правильного та відповідно неправильного МК. Вигляд початкових гістограм та після КП підтверджує, що навіть для вибраного специфічного по гістограмі ТГД, запропоновані моделі дають кращі результати. Потужність множини можливих ключів зросла на порядки (більше ніж 10^{300} !!), і як показують оцінки тільки потужність множини міні-блоків (8*8 8-бітних) має порядок більше 10^{150} . Таким чином стійкість моделей суттєво зросла.

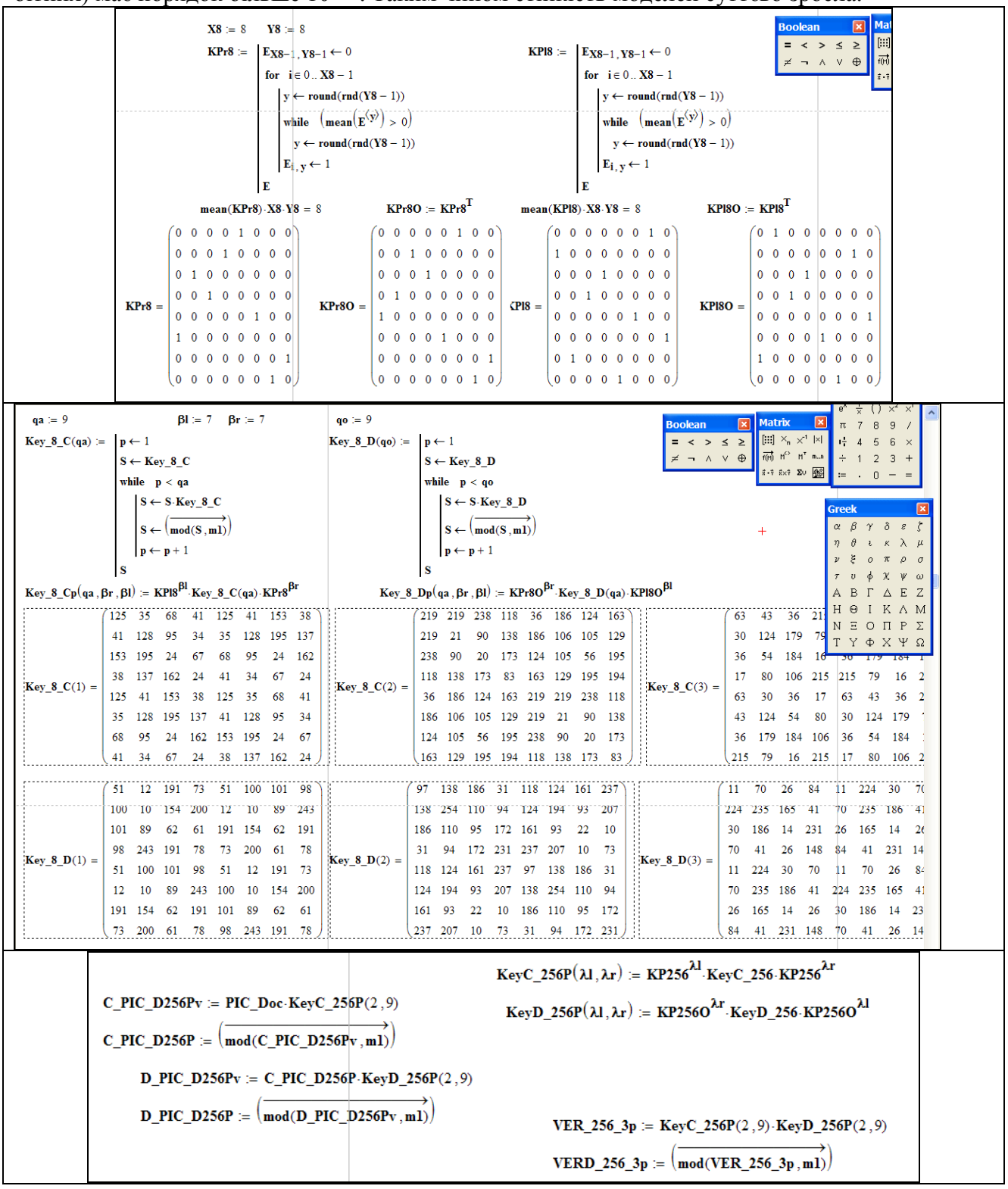


Рис.2. Фрагменти моделювання процесів формування матриць Р, циклових параметричних МК, їх складових, а також формули МАМ для зашифрування, розшифрування і верифікації.

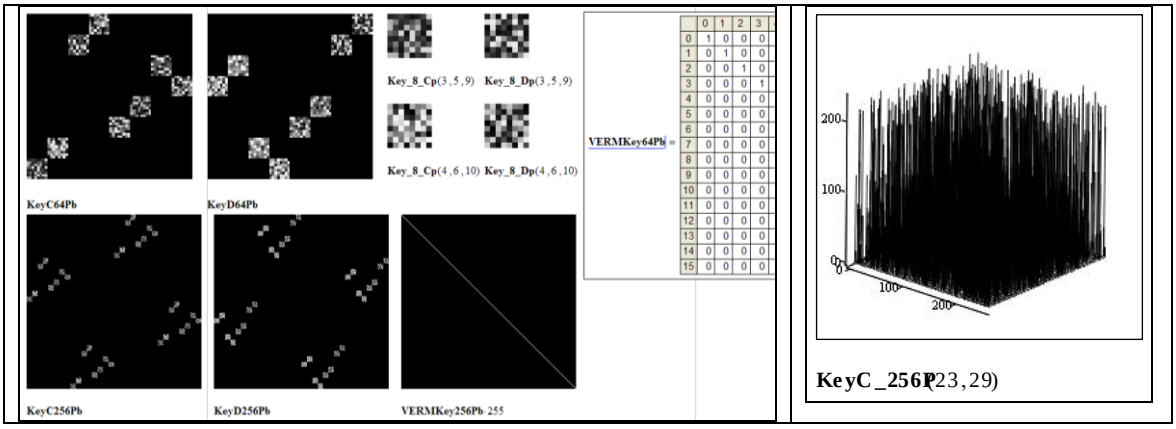


Рис.3. Вигляд деяких параметричних МК, їх складових ієрархічних блоків та одиничної (при перевірці) матриці у різних форматах (2D, 3D, та цифровому).

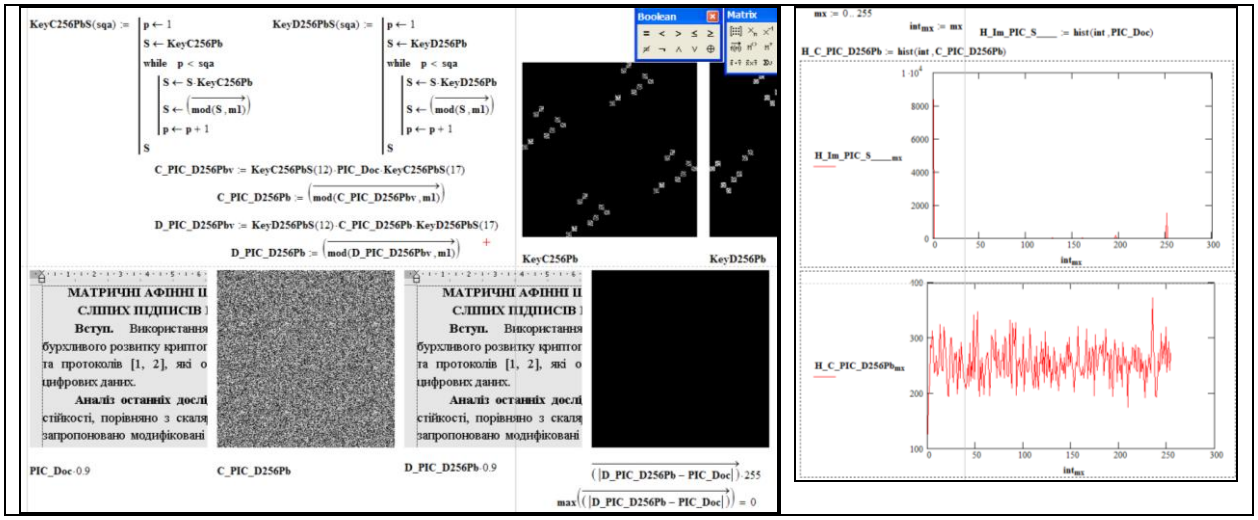


Рис.4. Результати моделювання КП ТГД на основі параметричних МАМ та МК при правильних ключах (1 експеримент) та гістограми ТГД і криптограми (праворуч).

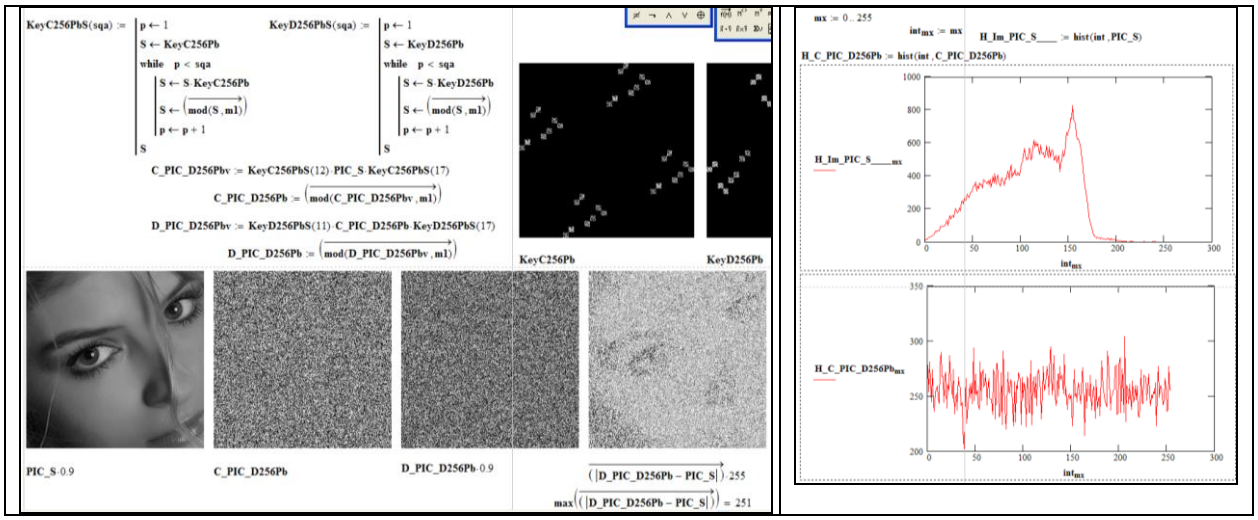


Рис.5. Результати моделювання КП ТГД на основі параметричних МАМ та МК при неправильних ключах (2 експеримент) та гістограми ТГД і криптограми (праворуч).

Без знання ключів неможливо відновити МД і, як було показано в [3-4], уже при розмірності МК, рівній 32*32, забезпечується стійкість моделей, а в нас ключі 256*256 8-бітних елементів, що дає суттєвий запас!

Висновки. Запропоновані та розглянуті нові моделі з операціями за модулем для КП МД, в тому числі зображень. Наводяться результати їх моделювання на прикладі прямих та обернених КП зображень, що свідчать про їх коректну роботу, зручність (всього 1 матрична процедура та один по суті МК!), адаптованість до форматів, багатофункціональність (поєднання операцій матричних блокових замін з перестановками, взаємозамінність циклових ітераційних процедур та матричних піднесень у степінь за модулем зі зручними вибором параметрів та управлінням ними перетвореннями та формуваннями ключів) та ефективність (орієнтація на матричні процесори). Розглянуті аспекти матричних алгебраїчних процедур і операцій за модулем та створення МК. Результати моделювання прямого та оберненого КП, їх верифікація підтвердили адекватність параметричних узагальнених МАМ, їх зручність, багатофункціональність, ефективність для використання. Вони реалізуються як програмно так і матричними процесорами, мають високі швидкість і стійкість перетворень та адаптуються для КП зображень різного формату.

Список літератури

1. Красиленко В.Г. Моделювання матричних афінних шифрів для криптографічних перетворень зображень / В.Г. Красиленко, Д.В. Нікітович // Інформатика та системні науки (ІСН-2017): матеріали VIII Всеукраїнської науково-практичної конференції за міжнародною участю, (м. Полтава, 16–18 березня 2017 року) / за ред. О.О.Ємця – Полтава: ПУЕТ, 2017. – Режим доступу: http://dspace.puet.edu.ua/handle/123456789/5558

2. Красиленко В.Г. Удосконалення та моделювання матричних афінних шифрів для криптографічних перетворень зображень / В.Г. Красиленко, Д.В. Нікітович // Електроніка та інформаційні технології: збірник наукових праць. – Львів: Львівський національний університет імені Івана Франка, 2017. – Вип. 7. – С 20-42. – Режим доступу: http://elit.lnu.edu.ua/issue.php?lang=&number=7

3. Красиленко В.Г., Матричні афінні шифри для створення цифрових сліпих підписів на текстографічні документи / В.Г. Красиленко, С.К. Грабовляк // Системи обробки інформації. – Х.: ХУПС, 2011. – Вип. 7(97). – С. 60 – 63.

4. Красиленко В.Г. Матричні афінно-перестановочні шифри для шифрування та дешифрування зображень / В.Г. Красиленко, С.К. Грабовляк // Системи обробки інформації. - Х.: ХУПС, 2012. – Вип. 3 (101).-т. 2. – С. 53-62.

5. Красиленко В.Г. Криптографічні перетворення зображень на основі матричних моделей перестановок з матрично-бітовозрізовою декомпозицією та їх моделювання / В. Г. Красиленко, В. М. Дубчак // Вісник Хмельницького національного університету. Технічні науки. - 2014. - № 1. - С. 74-79.

6. Красиленко В.Г. Моделювання криптографічних перетворень кольорових зображень на основі матричних моделей перестановок зі спектральною та бітово-зрізовою декомпозиціями / В.Г. Красиленко, Д.В. Нікітович // Комп'ютерно-інтегровані технології: освіта, наука, виробництво : наук. журн. – Луцьк: Видавництво Луц. нац. техн. ун-т., - 2016. - № 23. - С. 31-36. – Режим доступу: http://ki.lutsk-ntu.com.ua/node/132/section/9

7. Красиленко В.Г. Моделювання криптографічних перетворень кольорових зображень з верифікацією цілісності криптограм на основі матричних моделей перестановок/ В.Г. Красиленко, Д.В. Нікітович// Матеріали НПК «Проблеми моделювання та розроблення інформаційних систем». – Дрогобич : ДДПУ ім. І. Франка, 2016. – С. 128-136. Режим доступу: http://ddpu.drohobych.net/wp-content/uploads/2016/04/material_konf.pdf

8. Красиленко В.Г. Моделювання та дослідження криптографічних перетворень зображень на основі їхньої матрично-бітовозрізової декомпозиції та матричних моделей перестановок з верифікацією цілісності / В.Г. Красиленко, Д.В. Нікітович // Електроніка та інформаційні технології: збірник наукових праць. – Львів: Львівський національний

університет імені Івана Франка, 2016. – Вип. 6. – С 111-127. – Режим доступу: http://elit.lnu.edu.ua/pdf/6_12.pdf

9. Красиленко В.Г. Криптографічні перетворення (КП) кольорових зображень на основі матричних моделей з операціями за модулем / В.Г. Красиленко, Д.В. Нікітович // Сучасні методи, інформаційне та програмне забезпечення систем управління організаційно-технічними комплексами: збірник тез доповідей всеукраїнської науково-практичної інтернет-конференції (11 травня 2016 року). – Луцьк: РВВ Луцького НТУ, 2016. – С. 41-43.

Кузнецов Ю.М., Рябуха. О.М.
ОНАЗ ім. О.С. Попова

АНАЛІЗ СИСТЕМИ ГЛОБАЛЬНОГО ПОЗИЦІОНУВАННЯ ЗА ДОПОМОГОЮ IP-АДРЕСИ. РОЗГЛЯД СИСТЕМИ З ТОЧКИ ЗОРУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Анотація. У статті проаналізована система геолокації через IP-адрес, а також місце та спосіб застосування даної системи. Приведені первинні та вторинні джерела IP-адресів для геолокації. Розглянуто впровадження геолокаційних API, що спрощують розробку сайтів та застосунків для розробників. Проаналізовані мінуси даної системи геолокації. Особливу увагу приділено аналізу системи геолокації з точки зору інформаційної безпеки.

В інформаційну еру, геолокація зайняла своє місце в різних IT сферах.

Геолокація - це визначення місця розташування певного пристрою, підключеного до мережі.

Один із способів геолокація - це інтернет локалізація. Вона визначає місце розташування пристроїв за допомогою мережевих даних, таких як IP-адреса, що дозволяє визначити країну, місто, організацію і навіть реальне місце положення користувача.

Ця система має багатогранну сферу застосування. Основними ресурсами, які застосовують такий вид геолокації, є: браузери, що визначають країну та налаштовують пріоритети пошуку, сайти де використовують регіональні розмежування (до них відносяться сайти відеохостингу, які обмежують доступ до відеофайлу певним регіонам), інтернет магазини і сайти де застосовується інтернет-маркетинг. Одна зі сфер застосування системи це захист інформації, а саме локалізація кіберзлочинців і запобігання деяких атак.

Популярність такої системи полягає в тому, що кожен пристрій підключений до мережі інтернет використовує протокол IP. У структурі самого пакета протоколу IP, міститься IP-адреса відправника, яка і використовуються для геолокації.

Існують безліч баз даних геолокації, як платних, так і безкоштовних. Вони відрізняються різним рівнем точності: від рівня країни і до рівня адреси будівлі. Ці бази даних, як правило, зберігають IP-адреса, що використовуються брандмауерами, серверами оновлень, сайтами, поштовими системами та іншими системами в яких може застосовуватися геолокація.

У деяких платних базах даних присутнє геолокаційне програмне забезпечення з демографічними даними, в які входить цільовий маркетинг, що використовує IP-адреса.

Первинними джерелами даних IP-адресів є регіональні інтернет-реєстри, що слугують для розподілу і поширення IP-адрес серед організації розташованих у відповідних регіонах. Такими є 5 регіональних інтернет-регістрів:

- American Registry for Internet Numbers (ARIN) — для Північної Америки;
- RIPE Network Coordination Centre (RIPE NCC) — для Європи, Близького Сходу і Центральної Азії;
- Asia-Pacific Network Information Centre (APNIC) — для Азії і Тихоокеанського регіону;