УДК 681.3
А.О. Ігнатович
Національний університет "Львівська політехніка",
кафедра електронних обчислювальних машин,

МОДЕЛІ ЗАСТОСУВАННЯ МОДИФІКОВАНИХ БЛОКОВИХ ШИФРІВ У КІБЕРФІЗИЧНИХ СИСТЕМАХ

За результатами аналізу особливостей та характеристик відомих блокових шифрів запропоновано моделі підвищення їх ефективності та надійності в кіберфізичних системах на основі статичного та динамічного включення маскуючих символів. Обґрунтовано підвищення ефективності та надійності блокових шифрів.

Ключові слова: модель, блоковий шифр, ефективність, надійність, маскуючий символ, кіберфізична система.

This research work proposes models of efficiency and reliability increasing of the certain block ciphers. The proposed models are based on the basis of static and dynamic inclusion of masking symbols. Also the analysis of effectiveness of the certain block codes is done. Increasing of block ciphers' strength and effectiveness is justified.

Key words: model, block cipher, efficiency, reliability, masking symbol, cyberphysical system.

Вступ. Шифрування та дешифрування інформації є важливим етапом функціонування кіберфізичних систем (КФС) [1]. Дослідження щодо нових способів шифрування та дешифрування інформації розширює функціональні можливості КФС і є актуальною проблемою.

Огляд літературних джерел. Блокові шифри мають давню історію застосування. До класичних блокових шифрів можна віднести шифр Хілла [2] та шифр Віженера [3]. Ці шифри відносять до ручних і їм приписують багато недоліків: примітивні, неефективні, ручні. Характеристики блокових шифрів досліджували відомий вчений Клод Шеннон [4] та вітчизняні вчені [5,6]. Шифр мережа Фейстеля – це сучасний комп'ютерний шифр, його переваги та недоліки відомі [5,6]. Аналіз літературних джерел показує, що функціональні можливості блокових шифрів не вичерпані. Дослідження стосовно підвищення ефективності та надійності блокових шифрів є обґрунтованими та доцільними.

Постановка задачі дослідження. Дослідити особливості та характеристики відомих блокових шифрів та запропонувати моделі підвищення їх ефективності та надійності щодо застосування їх у кіберфізичних системах.

Основні результати дослідження

Розглянемо блокові шифри з точки зору ефективності та надійності. До блокових відносяться такі шифри, в яких за один період шифрування перетворюються певна кількість символів в блоку – ***k***. До найбільш поширених блокових шифрів відносять шифри Хілла та Віженера [1-3,5,6], тому дослідження зосереджені саме на цих шифрах. Шифрування та розшифрування інформації можна подати наступними процедурами.

$\mathbf{C_i = A * B_i}$ - процедура шифрування інформації, де C_i - матриця-стовпчик ***i***-того блоку шифрованого тексту; A – матриця-ключ для шифрування інформації; B_i – матриця-стовпчик ***i***-того блоку відкритого тексту;

$\mathbf{B_i = A^{-1} * C_i}$ - процедура розшифрування інформації, де B_i – матриця-стовпчик ***i***-того блоку відкритого тексту; A^{-1} - обернена матриця-ключ для розшифрування інформації; C_i - матриця-стовпчик ***i***-того блоку шифрованого тексту.

Ключем для шифру Хілла є матриця, яка представляється словом, чи довільним набором букв. Для шифрування може використовуватися числова квадратна матриця (3x3, 4x4, 5x5, 6x6,...). Матриця повинна мати обернену матрицю, щоб була можлива операція розшифрування.

Відомий спосіб шифрування інформації Віженера [3,5,6] на основі поліалфавітних перетворень елементів відкритого тексту (ВТ). Суть цього способу полягає в заміні кожного елемента ВТ на елемент шифрованого тексту (ШТ) згідно з буквою ключа, причому для кожної букви ключа є відповідний алфавіт заміни елементів ВТ. Якщо довжина ключа менша за довжину ВТ, то ключ повторюється стільки разів, щоб весь масив ВТ мав певний елемент ключа для перетворення.

Недоліком даного способу для шифрування інформації є те, що при великих обсягах ВТ можна знаходити повторення в ШТ, які будуть розташовуватись на віддалях кратних довжині ключа ***k***.

Спосіб шифрування на основі шифру Хілла – поліграмний блоковий шифр підстановки, заснований на лінійній алгебрі. Цей спосіб шифрування давав можливість зашифровувати більш ніж три символи за один цикл. Щоб розшифрувати повідомлення, необхідно звернути шифротекст назад у вектор і потім просто помножити на обернену матрицю ключа.

Необхідно обговорити деякі складнощі, пов'язані з вибором шифрувальної матриці. Не всі матриці мають обернену. Матриця буде мати обернену в тому і тільки в тому випадку, коли її детермінант не дорівнює нулю і не має спільних дільників з основою модуля. Таким чином, якщо ми працюємо з основою модуля 26 , то детермінант повинен бути ненульовим і не ділитися на 2 і 13. Якщо детермінант матриці дорівнює нулю або має спільні дільники з основою модуля, то така матриця не може використовуватися в шифрі Хілла, і повинна бути обрана інша матриця (в іншому випадку шифротекст буде неможливо розшифрувати). Тим не менш, матриці, які задовольняють вищенаведеним умовам, існують в достатку.

Запропонований спосіб шифрування інформації [7] має високі параметри по криптостійкості, нескладно реалізується апаратним, або програмним, або комбінованим способом.

Шифр Хілла при $\boldsymbol{\mu} = 6$ був реалізований у вигляді механічної шифрувальної машинки, описаній в патенті [2], який виконував множення матриць у форматі 6 × 6 по модулю 26 з допомогою системи шестерень і ланцюгів.

При необхідності отримати високі параметри щодо криптостійкості необхідно вставляти достатньо маскуючих символів, кількість яких може в декілька раз перевищувати кількість символів відкритого тексту ВТ. Якщо приймається алгоритм вставляння маскуючих символів: вставляється один маскуючий символ перед кожним символом ВТ і один маскуючий символ після символу ВТ. В цьому випадку ВТ з маскуючими символами буде мати таку конфігурацію: в кожному блоці (якщо $\boldsymbol{\mu} = 3$) буде один маскуючий символ перед символом відкритого тексту, символ ВТ і один маскуючий символ після символу ВТ. Блок має такий вигляд: $\{m_i; v_i; m_i;\}$, де m_i – маскуючий символ, v_i – символ ВТ. Якщо конфігурація ВТ з маскуючими символами буде така, яка розглядалася вище, а $\boldsymbol{\mu} = 4$, тоді перший блок буде мати такий вигляд $\{m_i; v_i; m_i; m_i;\}$, другий - $\{v_i; m_i; m_i; v_{i;}\}$, третій - $\{m_i; m_i\ v_i; m_i;\}$, четвертий - $\{m_i; v_i; m_i; m_i\}$, а п’ятий буде такий як перший і весь цикл з періодом чотири буде повторятися. Якщо приймається алгоритм вставляння маскуючих символів: вставляється два маскуючі символи перед кожним символом ВТ і нуль маскуючих символів після символу ВТ при $\boldsymbol{\mu} = 3$. В цьому випадку блок має такий вигляд : $\{m_i; m_i; v_i;\}$, де m_i – маскуючий символ,

v_i – символ ВТ. Всі блоки будуть мати такий вигляд, тому що кількість вставлених маскуючих символів, які приходяться на один символ ВТ дорівнює μ -1. Варіантів, які визначають конфігурацію ВТ з маскуючими символами, може бути багато. Вибирати необхідно такі, які забезпечують рівномірність частотної характеристики вживання окремих символів для ШТ. Дослідження частотних характеристик вживання окремих символів ШТ навіть при $m_i = 1$ підтверджує ефективність запропонованого способу шифрування інформації.

Для реалізації нового способу шифрування інформації запропоновані адаптивні моделі встановлення маскуючих символів.

Адаптивність моделі встановлення маскуючих символів можна визначити за алгоритмом їх підбору. Запропоновано маскуючі символи вибирати з можливого набору (відповідає алфавіту повідомлення), які визначаються нерівномірністю частотної характеристики розподілу символів, за принципом: кожний маскуючий символ, який вставляється, повинен покращувати рівномірність частотної характеристики розподілу символів відкритого тексту. Очевидно, що чим більш рівномірний частотний розподіл символів відкритого тексту, тим більш рівномірний буде і розподіл символів шифрованого тексту.

Розглянемо моделі на основі статичний принципу встановлення маскуючих символів - маскуючі символи завжди вставляються у наперед визначені місця відносно символів відкритого тексту. На рис. 1-3 наведені три варіанти статичних моделей встановлення маскуючих символів для формату $\mu = 3$. На графіках m_i – маскуючий символ (пунктирна лінія), v_i – символ ВТ (суцільна лінія), блоки розділені тонкими пунктирними лініями, довжина блоку – 3 символи.

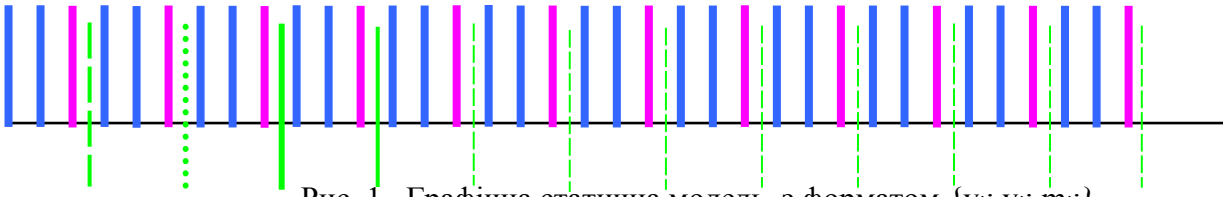

Рис. 1 . Графічна статична модель з форматом {v_i; v_i; m_i;}

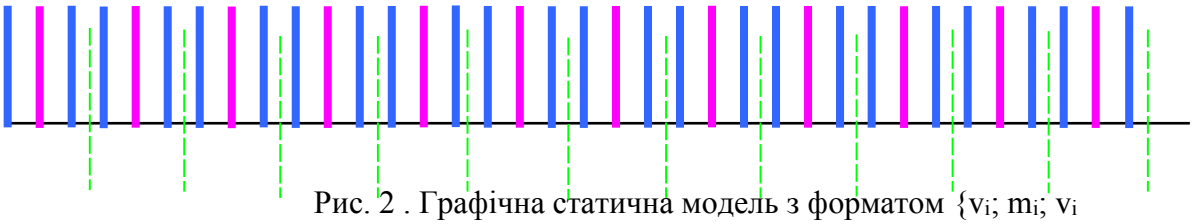

Рис. 2 . Графічна статична модель з форматом {v_i; m_i; v_i

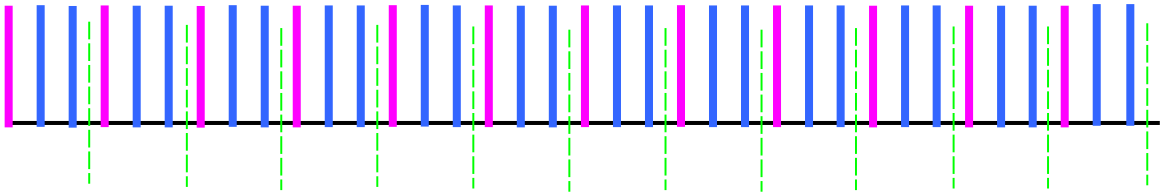

Рис. 3 . Графічна статична модель з форматом { m_i; v_i; v_i;}

Для оцінки ефективності використання маскуючих символів найбільш доцільно використовувати критерій ефективності, в якому оцінюється середнє інтегральне відхилення для конкретного випадку [8]. В наведених на рис. 1-3 моделях формування маскуючих

символів для формату **μ** = 3 результат зменшення середнього інтегрального відхилення в 1,4 рази. Такий результат є задовільним і забезпечує підвищення стійкості криптографічної системи [8].

Розглянемо динамічні моделі встановлення маскуючих символів - маскуючі символи вставляються по кількості та на позиції в залежності від номера символу відкритого тексту і їх кількість буде мінятися на кожному етапі процедури вставляння. На рис. 4 наведено приклади динамічних моделей встановлення маскуючих символів для формату **μ** = 5. На рисунках 4 m_i – маскуючий символ (пунктирна лінія), v_i – символ ВТ (суцільна лінія), n_j – коефіцієнт поступово змінюється від 0 до 5 (в залежності від порядкового номеру символу ВТ v_i). Блоки розділені тонкими пунктирними лініями. Довжина блоку – 5 символів.

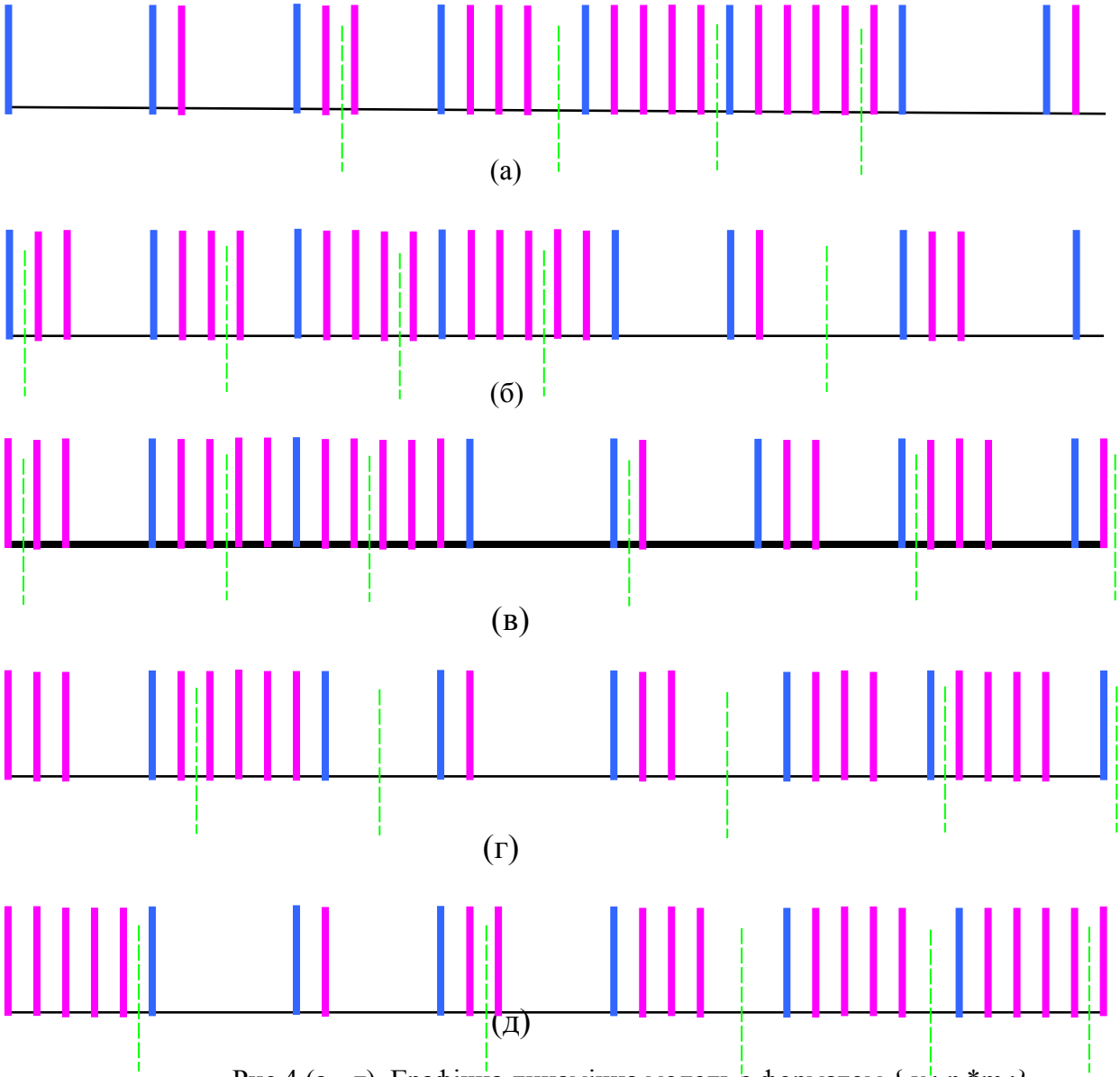

Рис.4 (а - д). Графічна динамічна модель з форматом { v_i; n_j*m_i;}

Динамічна функція вставляння маскуючих символів дає додатковий ефект. Якщо у звичайному шифрі Хілла повторення в тексті можуть появлятися на відстанях, які кратні довжині ключа (число **μ** не може бути дуже велике), то у встановленні маскуючих символів після кожного символу відкритого тексту у кількості від 0 до 5 при **μ** = 5 період повторення

буде 105 символів (взамін 5). Саме вставляння маскуючих символів і їх вилучення є процедурою, яка не зменшує продуктивність роботи криптографа. При цьому доцільно врахувати, що маскуючі символи підбираються з допомогою генератора випадкових чисел з найменш вживаних символів у шифрованому тексі. Такий алгоритм підбору і маскуючих символів можна рахувати додатковим ключем для формування шифрованого тексту. Складність вилучення маскуючих символів не визначається їх номером чи назвою, так як вилучаються символи на відповідних позиціях шифрованого тексту. Якщо кількість маскуючих символів становить більше 50%, тоді частотний розподіл символів у шифрованому тексті наближається до рівноймовірного. Відомий математик Клод Шеннон доказав, що при наближені розподілу частоти вживання символів до рівноймовірного закону, такий шифр наближається до абсолютно стійких шифрів [4]. Таким чином, використання маскуючих символів має перспективу в напрямку створення шифрів підвищеної стійкості.

Використання спеціалізованих комп'ютеризованих пристроїв чи універсальних комп'ютерів, збільшення ШТ і видалення маскуючих символів виконується автоматизовано, достатньо швидко і не зменшує продуктивності праці оператора при шифруванні чи розшифруванні інформації.

Висновки

Результати аналізу особливостей та характеристик відомих блокових шифрів показали можливість їх застосування у кіберфізичних системах. Запропоновані моделі на основі статичного та динамічного включення маскуючих символів забезпечують підвищення ефективності та надійності блокових шифрів. Обґрунтовано підвищення ефективності та надійності блокових шифрів. Якщо кількість маскуючих символів становить більше 50%, тоді частотний розподіл символів у шифрованому тексті наближається до рівноймовірного, що підвищує надійність шифру. Ефективність шифру підвищується за рахунок відносно простих алгоритмів шифрування-розшифрування та можливості його реалізації апаратно-програмними комп'ютерними засобами. Запропоновані моделі можуть використовуватися при побудові засобів безпеки комп'ютерних систем, мереж, кіберфізичних систем.

1. Мельник А. О. Кіберфізичні системи: проблеми створення та напрями розвитку / А. О. Мельник // Вісник Національного університету "Львівська політехніка". – 2014. – № 806 : Комп'ютерні системи та мережі. – С. 154–161. – Бібліографія: 31 назва. 2.. Lester S. Hill . Cryptography in an Algebraic Alphabet». «The American Mathematical Monthly».- 1929. 3. Fred Cohen . A Short History of Cryptography // Introductory Information Protection. — 1987. — ISBN 1-878109-05-7. 4. Shannon C. E. Communication Theory of Secrecy Systems // Bell System Technical Journal. — 1949. 5. Вербицький О.В. Вступ до криптології // Видавництво науково-технічної літератури. Львів, 1998. ISBN 966-7148-03-3. 6. Ємець В. Сучасна криптографія: основні поняття / В. Ємець, А. Мельник, Р. Попович. – Львів: БАК. – 2003. – 144 с. 7. Спосіб шифрування інформації. Патент України на корисну модель №99073. Бюл. № 9 від 12.05.2015. Ігнатович А.О., Іванців В. Р., Іванців Р-А. Д., Павич Н. Я. 8. Ігнатович А.О. Критерій ефективності для визначення стійкості блокових шифрівна основі внесених змін статистичних характеристик шифрованого тексту / Ігнатович А.О., Глухова О.В., Лозинський А.Я., Яремчук Р.І. // АСІТ'5 "Сучасні компютерні інформаційні технології". ТНЕУ. - Тернопіль. 22-23 травня 2015. – С. 167-168.

Наукові результати, подані у цій статті, було отримано в рамках дослідницького проекту ДБ/КІБЕР з реєстраційним номером 0115U000446, 01.01.2015 - 31.12.2017, фінансово підтриманим Міністерством освіти та науки України.