КОМП'ЮТЕРНІ НАУКИ, ІНФОРМАЦІЙНІ ТЕХНОЛОГІ, СИСТЕМНИЙ АНАЛІЗ ТА КІБЕРБЕЗПЕКА

DOI 10.31891/2307-5732-2020-291-6-7-12
УДК 004.056.5: 004.421.6:004.942

О.С. АНДРОЩУК, О.В. НАГРЕБЕЦЬКИЙ,
В.С. ОРЛЕНКО, В.М. ЧЕШУН
Хмельницький національний університет
А.І. КАТАЄВА
Донецький національний університет імені Василя Стуса

БАЗОВІ ОПЕРАЦІЇ АЛГОРИТМУ ФОРМУВАННЯ ШИФРІВ ЗСУВУ ІЗ ЗАСТОСУВАННЯМ ЕНТРОПІЙНОГО КОДУВАННЯ ХАФФМЕНА

В роботі представлено результати аналізу характерних особливостей способу підвищення криптостійкості алгоритмів шифрування попередньою модифікацією вхідних даних із застуванням методів оптимального ентропійного нерівномірного кодування на прикладі шифрів зсуву, за результатами аналізу запропоновано математичну модель, в якій визначено основні форми представлення даних та функції операцій їх перетворення, що може бути використано для математичного моделювання процедур алгоритмічної реалізації комбінованого методу шифрування за зазначеним способом.

Ключові слова: захист інформації, алгоритм шифрування, криптостійкість, оптимальне кодування.

O. ANDROSHCHUK, O. NAHREBETSKYY,
V. ORLENKO, V. CHESHUN
Khmelnytskyi National University
A. KATAIEVA
Vasyl' Stus Donetsk National University

BASIC OPERATIONS OF SHIFT CODE FORMATION ALGORITHM USING HUFFMAN ENTROPY CODING

The complexity and relevance of the tasks of cryptographic protection of information in the context of the increased value of information resources in the cyberspace causes interest in improving existing encryption algorithms and developing new ones.

The paper presents the results of a study of the characteristic features of the method for increasing the cryptographic strength of encryption algorithms by modifying the input data using the methods of optimal entropy uneven coding using the example of Caesar replacement ciphers and optimal Huffman coding. Based on the results of the analysis, a mathematical model is proposed, which defines the main forms of data presentation and the functions of their transformation operations. The model provides for work with three types of code alphabets, changing which destroys the statistical dependencies of the occurrence of alphabet symbols in the text, which serves as the basis for increasing the cryptographic strength of the encryption algorithm. The main functions presented in the mathematical model are the functions of performing operations of forming the alphabet based on the text submitted to the encryption algorithm, determining the statistical characteristics of the text, optimal uneven coding of the text, generating a sequential binary code of the encoded text, determining the composition of the uniform alphabet for encrypting text encoded with Huffman codes, as well as operators of encryption and decryption of the transformed text using Caesar ciphers.

The proposed model is intended for mathematical modeling of algorithmic implementation procedures for a combined encryption method using methods of optimal entropy uneven coding, as well as for evaluating the efficiency and cryptanalysis of ciphers.

Key words: information security, encryption algorithm, cryptographic strength, optimal coding..

Вступ

В умовах стрімкого розвитку інформаційних технологій, постійного збільшення обсягів інформації в кіберпросторі і зростання її цінності, а також через появу нових загроз щодо її цілісності і конфіденційності надзвичайної актуальності набувають заходи кібербезпеки.

Одним із базових заходів кібербезпеки є криптографічний захист даних, про що свідчить поява і масштабне використання великої кількості методів та алгоритмів симетричного й асиметричного шифрування з різними функціональними можливостями і принципами дії (алгоритми DES-базовий, подвійний і потрійний DES, IDEA, ГОСТ 28147, Діффі-Хелмана, RSA, Blowfish, AES, HiSea тощо [1-7]) та спроби їх постійного вдосконалення з метою підвищення криптостійкості шифрів.

Аналіз останніх досліджень і публікацій

З метою підвищення криптостійкості алгоритмів шифрування використовуються спеціальні методи теоретичного і експериментального характеру, що різняться за принципами реалізації та ефективністю [7].

Загальний аналіз методів підвищення криптостійкості алгоритмів шифрування дозволяє виділити декілька основних підходів [6-17]:

- модифікація існуючих алгоритмів шифрування;
- багатократне застосування алгоритму шифрування;
- поєднання декількох криптографічних алгоритмів;
- застосування додаткових некриптографічних методів підготовки і завершальної обробки даних.

Прикладами модифікації алгоритмів шифрування для удосконалення їх за критерієм криптостійкості шифрованого тексту є запропонована в [8] модифікація шифру гамування для підвищення

ефективності захисту електронних документів та описана в [9] модифікація алгоритму шифрування даних Меркла-Хелмана з використанням простих чисел та операцій над ними спеціального вигляду.

Багатократне застосування алгоритму шифрування є класичним варіантом, відомим з реалізації подвійного і потрійного алгоритму DES [4], який продовжує широко використовуватися і дозволяє отримувати нові рішення на основі відомих (мультиопераційне багаторазове ковзне шифрування [10] тощо).

В роботі [11] описано метод гібридної криптографії AES-HMAC, який передбачає для покращення безпеки передачі даних поєднання послідовним застосуванням криптографічних алгоритмів AES і HMAC.

Окреме місце серед способів підвищення криптостійкості алгоритмів шифрування займають методи, що базуються на застосуванні додаткових некриптографічних методів підготовки і завершальної обробки даних. Зокрема, дослідження [12] присвячене методу підвищення ентропії потокового шифрування за рахунок використання нових операцій криптоперетворення, синтезованих за критерієм строгого стійкого кодування. Автори роботи [13] описують метод оптимізації вихідного повідомлення за допомогою генетичного алгоритму підвищення криптостійкості алгоритму RSA (отримані показники статистичної безпеки є вищими за показники оригінального алгоритму на 1–3 %). В [14] описане дослідження можливості використання алгоритму циклічного надлишкового коду для підвищення стійкості криптосхеми ECIES.

В роботах [15,16] авторами досліджується спосіб підвищення криптостійкості алгоритмів шифрування попередньою модифікацією вхідних даних із застуванням методів оптимального ентропійного нерівномірного кодування, в ході якого забезпечується не лише стиск вхідного тексту, а і досягається зміна складу алфавіту кодування тексту та порушення статистичних даних повторюваності символів, тобто, збільшення його ентропії. Для шифрування даних обрано один із найпростіших і найменш стійких до зламу криптографічних методів, відомий як шифр заміни із зсувом (шифр Цезаря), застосування якого в подібних задачах обґрунтовується наочністю демонстрації ефекту від використання алгоритмів попередньої підготовки даних для підвищення криптостійкості алгоритму шифрування [16,17], а засобом підвищення криптостійкості алгоритму шифрування визначено оптимальні нерівномірні коди (ОНК) Хаффмена як класичний метод ентропійного кодування даних, що дає стабільний оптимальний код на виході у відповідності до статистичних властивостей алфавіту вхідного тексту [16,18].

В роботі [15] наведені загальні принципи застосування ОНК Хаффмена для підвищення криптостійкості шифрів зсуву, робота [16] присвячена опису експерименту з практичного застосування зазначених принципів для шифрування даних. Хоча результати експерименту і підтверджують ефективність досліджуваних принципи застосування ОНК Хаффмена для підвищення криптостійкості шифрів зсуву, їх не можна вважати систематизованими і ґрунтовними для алгоритмічної реалізації методу шифрування.

Постановка проблеми

Для підтвердження ефективності апріорних гіпотез [15,16] щодо підвищення криптостійкості алгоритмів шифрування попередньою модифікацією вхідних даних із застуванням методів оптимального ентропійного нерівномірного кодування, а також для забезпечення можливості алгоритмічної реалізації комбінованого методу шифрування, актуальності набуває задача визначення форм формалізованого та систематизованого опису даних, що використовуються алгоритмом, та операторів їх перетворення.

Викладення основного матеріалу

Основою для реалізації будь-якого алгоритму криптографічного шифрування є відкритий вхідний текст, що підлягає захисту. В ході дослідження відкритий вхідний текст ідентифікуємо як T_1 .

Відкритий вхідний текст T_1 складається з символів алфавіту, який утворює собою множину символів, представлених примітивними рівномірними кодами. Для відображення первинного алфавіту введемо до математичної моделі опису даних множину S_1:

$S_1 : \{s_{1.1}, s_{1.2}, \ldots, s_{1.i}, \ldots, s_{1.k}\}$ – множина кодів символів первинного алфавіту вхідного тексту T_1.

На основі алфавіту S_1 первинний текст T_1 можна представити множиною кодів символів алфавіту $s_{1.i} \in S_1$:

$T_1 : \{s_{1.k}, s_{1.f}, \ldots, s_{1.i}, \ldots, s_{1.k}, \ldots, s_{1.f}, \ldots, s_{1.f}, s_{1.j}\}$ – представлення первинного тексту як упорядкованої за характером тексту множини кодів символів алфавіту $s_{1.i} \in S_1$ з апріорною повторюваністю кодів.

Для формування ОНК Хаффмена з мінімальною надлишковістю склад алфавіту T_1 і статистичні характеристики символів $s_{1.i} \in S_1$ визначаються на підставі аналізу самого вхідного тексту T_1. Таким чином, основою для реалізації цього методу кодування є відкритий вхідний текст як T_1, на основі якого формуються два описи статистичних характеристик:

- алфавіт S_1 кодів символів $s_{1.i}$ відкритого вхідного тексту T_1;
- статистичні характеристики частоти входження кодів символів $s_{1.i}$ алфавіту S_1 в текст T_1.

Оскільки коди символів певного формованого з тексту алфавіту S_x можуть повторюватися в аналізованому тексті T_x по декілька разів, для формування цільового алфавіту S_x визначимо функцію усунення дублювання кодів символів F_{RD} (RD – скорочення від Remove Duplicates), що формує алфавіт використаних в тексті T_x символів S_x на підставі обробки самого тексту T_x:

$$F_{\text{RD}}\left(T_x\right): S_x = \left\{ s_{x.i} \in T_x \middle| s_{x.1} \in T_x \vee \left(s_{x.i} \in T_x \wedge \left(\prod_{j=1}^{i-1} \left(s_{x.i} \oplus s_{x.j} \right) \right) > 0 \right) \right\} . \quad (1)$$

За функцією (1) до алфавіту S_x включається код першого символу тексту $s_{x.1} \in T_x$, після чого код кожного наступного символу $s_{x.i} \in T_x$ порівнюється з усіма символами тексту $s_{x.j} \in T_x$ (для $j<i$) і, якщо збігів не виявляється (код символу зустрічається вперше), то код $s_{x.i} \in T_x$ також додається до алфавіту S_x. Функція (1) представлена в узагальненому вигляді для тексту T_x і може бути використана для будь-якого кодованого двійковими кодами тексту, в тому числі і для первинного тексту T_1 на етапі формування первинного алфавіту S_1.

Для накопичення даних статистичних характеристик частоти входження символів $s_{1.i}$ алфавіту S_1 в текст T_1 використовується множина P_1:

P_1 : $\{p(s_{1.1}), p(s_{1.2}), \ldots, p(s_{1.i}), \ldots, p(s_{1.k})\}$ – статистичні частоти входження символів $s_{1.i}$ первинного алфавіту S_1 в текст T_1 (ймовірності появи символів алфавіту $s_{1.i} \in S_1$ в тексті T_1).

Визначення характеристик статистичних імовірностей $p(s_{x.i}) \in P_x$ появи символів алфавіту $s_{x.i} \in S_x$ в тексті T_x реалізуємо за функцією F_P:

$$F_P\left(T_x\right): P_x = \left\{1 - \frac{\left|T_x \cap \left\{s_{x.i}\right\}\right|}{\left|T_x\right|} \middle| s_{x.i} \in T_x\right\}. \tag{2}$$

Дані характеристик первинного вхідного тексту T_1, відображених множинами кодів символів первинного алфавіту S_1 і ймовірностей появи символів алфавіту P_1, є достатніми для реалізації процедури оптимального нерівномірного кодування Хаффмена. Результатом процедури кодування стає отримання вторинного алфавіту для кодування первинного вхідного тексту T_1, що дозволяє отримати вторинне представлення $T_{\text{ОНК}}$ вхідного тексту з аналогічною кількістю елементів (тобто, потужності множин T_1 і $T_{\text{ОНК}}$ залишаються однаковими: $|T_1|=|T_{\text{ОНК}}|$), але з властивостями нерівномірності коду елементів множини, що і забезпечує оптимізацію коду вхідного тексту (стиск коду тексту).

Для відображення вторинного алфавіту і можливості опису з його застосуванням тексту $T_{\text{ОНК}}$ застосовується множина S_2:

S_2 : $\{s_{2.1}, s_{1.2}, \ldots, s_{2.i}, \ldots, s_{2.k}\}$ – множина кодів символів вторинного алфавіту (алфавіту оптимального коду).

Особливістю ОНК Хаффмена є те, що для визначення оптимального нерівномірного коду $s_{2.i} \in S_2$ для будь-якого символу первинного алфавіту $s_{1.i} \in S_1$ це кодування потребує наявності статистичних даних (як базису оцінки ентропії) первинного алфавіту S_1 в цілому, а не окремих його символів. Тобто, операцію визначення складу алфавіту оптимального нерівномірного коду Хаффмена $S_{\text{НС}}$ (НС – скорочення від Huffman Coding) для символу первинного алфавіту S_x можна в узагальненому вигляді записати алгоритмічною функцією кодування Хаффмена, що враховує властивості символів $s_{x.i} \in S_x$ у взаємозв'язку статистичних даних множини P_x всіх елементів множини S_x:

$$F_{\text{НС}}\left(S_x, P_x\right): S_{\text{НС}x} = \left\{F_{\text{НС}}\left(s_{x.i}, P_x\right) \to s_{\text{НС}.i} \middle| s_{x.i} \in S_x\right\} \tag{3}$$

де $F_{\text{НС}}\left(s_{x.i}, P_x\right) \to s_{\text{НС}.i}$ – алгоритмічна функція визначення ОНК символу $s_{x.i} \in S_x$ з використанням статистичних даних множини P_x.

Призначення кодованого нерівномірними кодами алфавіту S_2 – перетворення первинного тексту T_1 в оптимізований із застосуванням ОНК Хаффмена вторинний текст $T_{\text{НС}}$, який також можна представити як упорядковану за характером тексту множину кодів символів алфавіту $s_{2.i} \in S_2$:

$T_{\text{НС}}$: $\{s_{2.\text{k}}, s_{2.\text{f}}, \ldots, s_{2.i}, \ldots, s_{2.\text{k}}, \ldots, s_{2.\text{f}}, \ldots, s_{2.\text{f}}, s_{2.j}\}$ – представлення вторинного тексту $T_{\text{НС}}$ як упорядкованої за характером тексту множини нерівномірних кодів символів алфавіту $s_{2.i} \in S_2$ з апріорною повторюваністю кодів.

Операцію заміни символу $s_{1.i} \in S_1$ в тексті T_1 на оптимальний код $s_{2.i} \in S_2$, що дозволяє отримати оптимальний код всього тексту $T_{\text{НС}}$, можна описати як узагальнену операцію заміни в закодованому тексті T_x, кодів символів одного алфавіту S_x, що використовувався для кодувався тексту T_x, на символи іншого алфавіту S_y. Тобто, мова йде про реалізацію перекодування тексту T_x із заміною кодів символів одного алфавіту S_x на коди символів одного алфавіту S_y, що дає нам нове представлення тексту T_y. Функція перекодування $F_{\text{ТС}}$ (ТС – скорочення від TransCoding):

$$F_{\text{ТС}}\left(T_x, S_x, S_y\right): T_y = \left\{s_{y.j} \in T_y = s_{y.i} \in S_y \middle| s_{x.j} \in T_x = s_{x.i} \in S_x\right\}. \tag{4}$$

Наступним кроком кодових перетворень при реалізації способу формування шифрів зсуву із застосуванням ОНК Хаффмена є переведення оптимального нерівномірного коду тексту $T_{\text{НС}}$ в рівномірні кодові комбінації для застосування шифрів зсуву. Переведення оптимального нерівномірного коду тексту $T_{\text{НС}}$ в рівномірні кодові комбінації передбачає виконання двох операцій з бітовими кодами [16]:

- перетворення закодованого ОНК Хаффмена тексту $T_{\text{НС}}$ в нерозривне послідовне повідомлення (потокове представлення двійкового коду тексту $T_{\text{НС}}$);

- дроблення потокового представлення тексту на рівномірні кодові комбінації у відповідності до потреб алгоритму (засобів) реалізації шифрів зсуву.

Функцію послідовного поєднання кодів $s_{j.i} \in S_j$ і $s_{j.f} \in S_j$ ідентифікуємо як F_{SC} (SC – скорочення від Sequential Combination):

$$F_{\text{SC}}\left(T_x\right): T_{\text{SC}x} = \sum_{i=1}^{|T_x|}\left(s_{x.i}\right)_{\text{str}} . \tag{5}$$

де сума $\sum_{i=1}^{|T_x|}\left(s_{x.i}\right)_{\text{str}}$ використовується як засіб поєднання кодів символів тексту в єдиний послідовний код і виконується як операція додавання символьних даних, а не цифрових.

Застосування функції (5) для всіх елементів $s_{2.i} \in T_2$ дає можливість виконати перетворення оптимального нерівномірного коду Хаффмена тексту T_{HC} в нерозривне послідовне повідомлення T_{SC2}.

Пропорційне розбиття (дроблення) потокового представлення тексту $T_{\text{SC}x}$ на рівномірні кодові комбінації у відповідності до потреб алгоритму реалізації шифрів зсуву представлено як реалізацію функції F_{PD} (PD – скорочення від Proportional Division) розбиття бітової послідовності $T_{\text{SC}x}$ на рівномірні кодові комбінації розрядності r з утворенням розподіленого рівномірного коду T_{UC} (UC – скорочення від Uniform Code):

$$F_{\text{PD}}\left(T_{\text{SC}x}, r\right): T_{\text{UC}} = \left\{ s_{\text{UC}.i} \,\middle\|\, s_{\text{UC}.i}\right| = r \wedge T_{\text{SC}x} = \sum_{i=1}^{|T_{\text{UC}}|}\left(s_{\text{UC}.i}\right)_{\text{str}} \right\}. \tag{6}$$

Використання в умові функції (6), поряд з вимогою щодо фіксованої розрядності $\left|s_{\text{UC}.i}\right| = r$ елементів $s_{\text{UC}.i} \in T_{\text{UC}}$, функції послідовного поєднання кодів (5) стосовно генерованого тексту T_{UC} вказує на необхідності дотримання зворотності перетворень $T_{\text{SC}x}$ в T_{UC} функцією (6) і T_{UC} в $T_{\text{SC}x}$ функцією (5):

$$F_{\text{SC}}\left(F_{\text{PD}}\left(T_{\text{SC}x}, r\right)\right) = T_{\text{SC}x} . \tag{7}$$

Результатом застосування функції (6) до послідовного двійкового коду тексту T_{SC2} є представлення тексту T_{UC} як множини символів нового алфавіту S_3:

S_3 : $\{s_{3.1}, s_{3.2}, \ldots, s_{3.i}, \ldots, s_{3.n}\}$ – множина рівномірних кодів третинного алфавіту оптимального коду вхідного тексту.

Склад кодового алфавіту S_3 визначається застосуванням функції усунення дублювання кодів (1) символів стосовно кодованого представлення тексту T_{UC}. Характерною особливістю алфавіту S_3 порівняно до алфавіту S_1 і S_2 є порушення статистичних характеристик частоти появи кодів в текстах і, як правило, оновлення набору кодів символів. Оновлення складу наборів кодів може досягатися як через безпосередню зміну кількості кодових комбінацій нового алфавіту відносно початкового, так і в результаті застосування різних довжин кодових комбінацій рівномірних кодів алфавітів S_3 порівняно до алфавіту S_1.

За аналогією з попередніми описами, оптимізований текст T_{UC} можна представити як множину кодів символів алфавіту S_3:

T_{UC} : $\{s_{3.h}, s_{3.\text{u}}, \ldots, s_{3.j}, \ldots, s_{3.l}, \ldots, s_{3.\text{f}}, \ldots, s_{3.j}, \ldots, s_{3.x}\}$ – представлення тексту T_{UC} як упорядкованої множини символів алфавіту $s_{3.j} \in S_3$ з апріорно наявними повторами кодів.

Третинний алфавіт є цільовим для забезпечення можливості застосування шифрів зсуву щодо оптимального коду T_{UC} вхідного тексту T_1. Таким чином, на даному етапі відбувається перехід від оптимального кодування Хаффмена до застосування шифрів зсуву.

Формування шифрів зсуву тексту T_x на основі алфавіту $s_{3.j} \in S_x$ і ключа шифрування w виконується класичним методом [1,16,17,20], що, на основі оператора перекодування (4), може бути представлено як функція шифрування перекодуванням T_x із застосуванням циклічно зміщеного на w позицій алфавіту S_x:

$$F_{\text{E}w}\left(T_x, S_x, w\right): T_{\text{E}x} = \left\{ s_{\text{E}x.j} \in T_{\text{E}x} = s_{x.(i+w) \bmod |S_x|} \in S_x \,\middle|\, s_{x.j} \in T_x = s_{x.i} \in S_x \right\} . \tag{8}$$

Застосування функції (8) до оптимального коду T_{UC} вхідного тексту T_1 дає в результаті шифрований текст T_{E1} з підвищеною криптостійкістю, що досягається через усунення застосуванням ОНК Хаффмена основного недоліку шифрів зсуву – незмінності статистичних властивостей первинного алфавіту в алфавіті шифрування.

Дешифрування зашифрованого $T_{\text{E}x}$ також виконується за класичним методом і описується функцією:

$$F_{\text{D}w}\left(T_{\text{E}x}, S_x, w\right): T_x = \left\{ s_{x.j} \in T_x = s_{x.(i-w) \bmod |S_x|} \in S_x \,\middle|\, s_{x.j} \in T_x = s_{x.i} \in S_x \right\} . \tag{9}$$

За формулою (9) з зашифрованого тексту T_{E1} відбувається відтворення оптимізованого тексту T_{UC}, який є базовим для виконання зворотних перетворень і відтворення відкритого вхідного тексту як T_1 (із застосуванням класичного варіанту реалізації алгоритму декодування ОНК Хаффмена).

Висновки

В роботі визначено основні форми представлення даних та функції операцій їх перетворення, орієнтовані на спосіб реалізації шифрів зсуву з підвищення криптостійкості алгоритмів шифрування попередньою модифікацією вхідних даних із застуванням методів оптимального ентропійного нерівномірного кодування Хаффмена, а також призначені для математичного моделювання процедур алгоритмічної реалізації комбінованого методу шифрування за зазначеним способом.

Література

1. Харченко М. М. Методи шифрування даних / М. М. Харченко //Актуальні питання сучасної інформатики. – 2016. – №3. – С. 23-28.

2. Карпінський М. П. Криптографічний захист мережевих даних на основі асиметричних алгоритмів / М. П. Карпінський, Я. І. Кінах, І. М. Костевич // Матеріали X X наукової конференції ТНТУ ім. І. Пулюя, 17-18 травня 2017 року. – Т. : ТНТУ, 2017. – С. 78.

3. Бичова І. В. Особливості криптографічного захисту ділової документації. / І. В. Бичова, В. В. Чередниченко // Перспективи управлінської діяльності суб'єктів господарювання в контексті економічної безпеки : матеріали міжнародного форуму з безпеки. – Черкаси, 2017. – С. 214-216.

4. A Survey on the Cryptographic Encryption Algorithms / Muhammad Faheem Mushtaq, Sapiee Jamel, Abdulkadir Hassan Disina, Zahraddeen A. Pindar, Nur Shafinaz Ahmad Shakir, Mustafa Mat Deris // International Journal of Advanced Computer Science and Applications. – November 2017. – 8(11). – P. 333-343.

5. Research on the Application of Cryptography on the Blockchain / Sheping Zhai, Yuanyuan Yang, Jing Li, Cheng Qiu, Jiangming Zhao // Journal of Physics. – IOP Publishing, 2019. – Conf. Series 1168 (2019) 032077. – P. 1–8.

6. Ільєнко А. Сучасні методи гомоморфного шифрування інформаційних ресурсів / Анна Ільєнко // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні : науково-технічний збірник. – 2015. – Вип. 2 (30). – С. 52-57.

7. Метьолкін А. О. Дослідження методів підвищення криптографічної стійкості / А. О. Метьолкін, В. С. Кардашук // Вісник Східноукраїнського національного університету імені Володимира Даля. – 2018. – № 6. – С. 90-95.

8. Розломій І.О. Підвищення ефективності захисту електронних документів модифікацією шифру гамування / І.О. Розломій // Вісник Хмельницького національного університету. Технічні науки. – Хмельницький : ХНУ, 2016. – № 2. – С. 69-73.

9. Івохін Є. В. Про модифікацію алгоритму шифрування даних Меркла-Хелмана / Є. В. Івохін // Вісник ЧДТУ. –2014. – № 2. – С. 10–14.

10. Бабенко В.Г. Мультиопераційне багаторазове ковзне шифрування / В.Г. Бабенко, О.Г. Мельник, Р.П. Мельник // Системи озброєння і військова техніка. – 2015. – № 3(43). – С. 70–72.

11. Farah R.Shareef A novel crypto technique based ciphertext shifting / Farah R.Shareef // Egyptian Informatics Journal. – July 2020. – Volume 21, Issue 2.– P. 83-90.

12. Бабенко В. Г. Методологія синтезу операцій перетворення інформації для комп'ютерної криптографії : дис. ... д-ра техн. наук : 05.13.05 / Віра Григорівна Бабенко; Черкаський державний технологічний університет. – Черкаси, 2020. – 200 с.

13. Підвищення стійкості криптоалгоритму RSA за рахунок генетичної оптимізації вихідного повідомлення / А.В. Приймак, Ю.Є. Яремчук // Реєстрація, зберігання і обробка даних. – 2018. – Т. 20, № 4. – С. 76–84.

14. Приймак А. В. Дослідження можливості використання алгоритму циклічного надлишкового коду для підвищення стійкості криптосхеми ECIES / А. В. Приймак, О. В. Салієва, Я. Ю. Яремчук // Вісник Хмельницького національного університету. Технічні науки. – Хмельницький : ХНУ, 2019. – № 1. – С. 155-162.

15. Оптимальне нерівномірне кодування в підвищенні криптостійкості шифрів / В. М. Чешун, В. С. Орленко, В. К. Шваб, Р. М. Гончар, С. М. Халіманенко // Тези доповідей XVI Міжнародної науково-практичної конференції "Військова освіта і наука: сьогодення та майбутнє". – Київ : ВІКНУ, 2020. – Т. 1. – С. 65–66.

16. Гончар Р. М. Оптимальне кодування як засіб підвищення захищеності передачі шифрованих даних / Р. М. Гончар, О. В. Нагребецький, В. С. Орленко, В. М. Чешун // Збірник наукових праць молодих науковців і студентів «Інтелектуальний потенціал – 2020». – Хмельницький : ПВНЗ УЕП, 2020. – Ч. 2. – С. 26–34.

17. Atish J. Enhancing the Security of Caesar Cipher Substitution Method using a Randomized Approach for more Secure Communication / Atish Jain, Ronak Dedhia, Abhijit Patil // International Journal of Computer Applications (0975-8887). – November 2015. – Volume 129. – №13. – P. 6-11.

18. Кодування джерел інформації та каналів зв'язку: навчальний посібник / [Беркман Л.Н., Бондарчук А.П., Гайдур Г.І., Чумак Н.С.]. – Київ: НТІТІ ДУТ, 2018. – 91 с.

19. Бойко Ю. М. Теоретичні аспекти підвищення завадостійкості й ефективності обробки сигналів в радіотехнічних пристроях та засобах телекомунікаційних систем за наявності завад : монографія / Ю. М. Бойко, В. А. Дружинінін, С. В. Толюпа. - Київ : Логос, 2018. - 227 с.

20. Прикладна криптологія : системи шифрування : підручник / О. Г. Корченко, В. П. Сіденко, Ю. О. Дрейс. – К. : ДУТ, 2014. – 448 с.

21. Приймак А. В. Підвищення криптостійкості симетричного шифру шляхом використання генетичного алгоритму / А. В. Приймак // Матеріали XLVII науково-технічної конференції підрозділів ВНТУ. – Вінниця, 14-23 березня 2018 р. – 2018. – С.99-102.

Referenses

1. Kharchenko M. M. Metody shyfruvannja danykh / M. M. Kharchenko //Aktualjni pytannja suchasnoji informatyky. – 2016. – №3. – S. 23-28.

2. Karpinsjkyj M. P. Kryptoghrafichnyj zakhyst merezhevykh danykh na osnovi asymetrychnykh alghorytmiv / M. P. Karpinsjkyj, Ja. I. Kinakh, I. M. Kostevych // Materialy X X naukovoji konferenciji TNTU im. I. Puljuja, 17-18 travnja 2017 roku. – T. : TNTU, 2017. – S. 78.

3. Bychova I. V. Osoblyvosti kryptoghrafichnogho zakhystu dilovoji dokumentaciji. / I. V. Bychova, V. V. Cherednychenko // Perspektyvy upravlinsjkoji dijaljnosti sub'jektiv ghospodarjuvannja v konteksti ekonomichnoji bezpeky : materialy mizhnarodnogho forumu z bezpeky. – Cherkasy, 2017. – S. 214-216.

4. A Survey on the Cryptographic Encryption Algorithms / Muhammad Faheem Mushtaq, Sapiee Jamel, Abdulkadir Hassan Disina, Zahraddeen A. Pindar, Nur Shafinaz Ahmad Shakir, Mustafa Mat Deris // International Journal of Advanced Computer Science and Applications. – November 2017. – 8(11). – P. 333-343.

5. Research on the Application of Cryptography on the Blockchain / Sheping Zhai, Yuanyuan Yang, Jing Li, Cheng Qiu, Jiangming Zhao // Journal of Physics. ¬– IOP Publishing, 2019. – Conf. Series 1168 (2019) 032077. – P. 1–8.

6. Iljjenko A. Suchasni metody ghomomorfnogho shyfruvannja informacijnykh resursiv / Anna Iljjenko // Pravove, normatyvne ta metrologhichne zabezpechennja systemy zakhystu informaciji v Ukrajini : naukovo-tekhnichnyj zbirnyk. – 2015. – Vyp. 2 (30). – S. 52-57.

7. Metjolkin A. O. Doslidzhennja metodiv pidvyshhennja kryptoghrafichnoji stijkosti / A. O. Metjolkin, V. S. Kardashuk // Visnyk Skhidnoukrajinsjkogho nacionaljnogho universytetu imeni Volodymyra Dalja. – 2018. – № 6. – S. 90-95.

8. Rozlomij I.O. Pidvyshhennja efektyvnosti zakhystu elektronnykh dokumentiv modyfikacijeju shyfru ghamuvannja / I.O. Rozlomij // "Herald of Khmelnytskyi national university", №2, 2016r. - Technical sciences. – Khmelnytskyi: KhNU. – S. 69-73.

9. Ivokhin Je. V. Pro modyfikaciju alghorytmu shyfruvannja danykh Merkla-Khelmana / Je. V. Ivokhin // Visnyk ChDTU. –2014. – № 2. – S. 10–14.

10. Babenko V.Gh. Muljtyoperacijne baghatorazove kovzne shyfruvannja / V.Gh. Babenko, O.Gh. Meljnyk, R.P. Meljnyk // Systemy ozbrojennja i vijsjkova tekhnika. – 2015. – № 3(43). – S. 70–72.

11. Farah R.Shareef A novel crypto technique based ciphertext shifting / Farah R.Shareef // Egyptian Informatics Journal. – July 2020. – Volume 21, Issue 2.– P. 83-90.

12. Babenko V. Gh. Metodologhija syntezu operacij peretvorennja informaciji dlja komp'juternoji kryptoghrafiji : dys. ... d-ra tekhn. Nauk : 05.13.05 / Vira Ghryghorivna Babenko; Cherkasjkyj derzhavnyj tekhnologhichnyj universytet. – Cherkasy, 2020. – 200 s.

13. Pidvyshhennja stijkosti kryptoalghorytmu RSA za rakhunok ghenetychnoji optymizaciji vykhidnogho povidom¬lennja / A.V. Pryjmak, Ju.Je. Jaremchuk // Rejestracija, zberighannja i obrobka danykh. – 2018. – T. 20, № 4. – S. 76–84.

14. Pryjmak A. V. Doslidzhennja mozhlyvosti vykorystannja alghorytmu cyklichnogho nadlyshkovogho kodu dlja pidvyshhennja stijkosti kryptoskhemy ECIES / A. V. Pryjmak, O. V. Salijeva, Ja. Ju. Jaremchuk // "Herald of Khmelnytskyi national university", №1, 2019r. - Technical sciences. – Khmelnytskyi: KhNU. – S. 155-162.

15. Optymaljne nerivnomirne koduvannja v pidvyshhenni kryptostijkosti shyfriv / V. M. Cheshun, V. S. Orlenko, V. K. Shvab, R. M. Ghonchar, S. M. Khalimanenko // Tezy dopovidej KhVI Mizhnarodnoji naukovo-praktychnoji konferenciji "Vijsjkova osvita i nauka: sjoghodennja ta majbutnje". – Kyjiv : VIKNU, 2020. – T. 1. – S. 65–66.

16. Ghonchar R. M. Optymaljne koduvannja jak zasib pidvyshhennja zakhyshhenosti peredachi shyfrovanykh danykh / R. M. Ghonchar, O. V. Naghrebecjkyj, V. S. Orlenko, V. M. Cheshun // Zbirnyk naukovykh pracj molodykh naukovciv i studentiv «Intelektualjnyj potencial – 2020». – Khmeljnycjkyj : PVNZ UEP, 2020. – Ch. 2. – S. 26–34.

17. Atish J. Enhancing the Security of Caesar Cipher Substitution Method using a Randomized Approach for more Secure Communication / Atish Jain, Ronak Dedhia, Abhijit Patil // International Journal of Computer Applications (0975-8887). – November 2015. – Volume 129. – №13. – R. 6-11.

18. Koduvannja dzherel informaciji ta kanaliv zv'jazku: navchaljnyj posibnyk / [Berkman L.N., Bondarchuk A.P., Ghajdur Gh.I., Chumak N.S.]. – Kyjiv: NNITI DUT, 2018. – 91 s.

19. Bojko Ju. M. Teoretychni aspekty pidvyshhennja zavadostijkosti j efektyvnosti obrobky syghnaliv v radiotekhnichnykh prystrojakh ta zasobakh telekomunikacijnykh system za najavnosti zavad : monoghrafija / Ju. M. Bojko, V. A. Druzhyninin, S. V. Toljupa. - Kyjiv : Loghos, 2018. - 227 s.

20. Prykladna kryptologhija : systemy shyfruvannja : pidruchnyk / O. Gh. Korchenko, V. P. Sidenko, Ju. O. Drejs. – K. : DUT, 2014. – 448 s.

21. Pryjmak A. V. Pidvyshhennja kryptostijkosti symetrychnogho shyfru shljakhom vykorystannja ghenetychnogho alghorytmu / A. V. Pryjmak // Materialy XLVII naukovo-tekhnichnoji konferenciji pidrozdiliv VNTU. – Vinnycja, 14-23 bereznja 2018 r. – 2018. – S.99-102.

Надійшла / Paper received : 24.11.2020 р. Надрукована/Printed :04.01.2021 р.