УДК 004.7, 004.8, 004.9

А. О. Ігнатович
Національний університет “Львівська політехніка”,
кафедра електронних обчислювальних машин

КОНЦЕПЦІЯ ЗАСТОСУВАННЯ МОДИФІКОВАНИХ БЛОКОВИХ ШИФРІВ У ТЕЛЕКОМУНІКАЦІЙНИХ СЕРЕДОВИЩАХ КІБЕРФІЗИЧНИХ СИСТЕМ

За результатами аналізу особливостей функціонування та характеристик телекомунікаційних середовищ кіберфізичних систем запропоновано концепцію застосування модифікованих блокових шифрів разом із широковживаними методами захисту. Розглянуто особливості застосування нового способу шифрування на основі статичного та динамічного включення маскувальних символів. Показана можливість розширення функціональних можливостей компонентів безпеки кіберфізичних систем за використання модифікованих блокових шифрів. Наведено результати тестування модифікованих блокових шифрів із використанням стандартизованих тестів.

Ключові слова: концепція застосування, модифікований блоковий шифр, телекомунікаційне середовище, маскувальний елемент, кіберфізична система, криптографія.

CONCEPT OF USAGE OF MODIFIED BLOCK CIPHERS IN TELECOMMUNICATIONS ENVIRONMENTS OF CYBERPHYSICAL SYSTEMS

This research work proposes concept of usage of modified block ciphers combining with widely used security methods. The proposed concept is based on the analysis of peculiarities of functioning and characteristics of telecommunications environments of cyberphysical systems. Peculiarities of usage of the newly introduced cryptography method on the basis of static and dynamic inclusion of masking symbols are overviewed. Possibilities of extension of the functionality of security components of cyberphysical systems in the process of usage of modified block ciphers are shown. The analysis of effectiveness of the proposed block ciphers using the National Institute of Standards and Technology (NIST USA) statistical tests is done.

Key words: concept of usage, modified block cipher, telecommunication environment, cyberphysical system, cryptography, NIST, statistical tests.

Вступ

Проблема захисту інформації від суб’єктів, які не мають на це права, актуальна майже в усій царині застосування комп’ютерних технологій. Ця проблема актуальна для телекомунікаційних середовищ кіберфізичних систем.

Стан проблеми

Телекомунікаційні середовища є одними із найважливіших компонентів кіберфізичних систем [1, 2]. Через них передаються великі обсяги даних, значну частину яких потрібно захищати від несанкціонованого доступу. Цією проблематикою займаються такі напрями наукових досліджень, як криптографія та захист інформації. Основні засади сучасної криптографії розглянуто в багатьох літературних джерелах, серед яких можна виділити монографії [3–5]. Під час розв’язання задачі

захисту інформації конкретної комп'ютерної системи постає задача комплементації загальних досягнень наукових досліджень у царині криптографії та захисту інформації на особливості конкретних застосувань.

До основних функцій, виконувати які повинні компоненти захисту інформації у телекомунікаційних середовищах кіберфізичних систем (надалі – КФС), можна зарахувати класичні та загальноприйняті конфіденційність, аутентифікацію, цілісність, доступність, керування доступом [3–5]. Конфіденційність – це гарантія для наперед визначених суб'єктів можливості користування інформацією та гарантія неможливості доступу до цієї інформації зловмисникам. Конфіденційність має забезпечити захист сховищ даних, передачу даних через канали зв'язку, неможливість виявити джерела та приймача повідомлення, частоту повідомлень, їх розміри. Аутентифікація – це гарантія надійної ідентифікації джерела повідомлення та встановлення факту, що джерело та приймач повідомлення не є підробними. Крім того, в процесі обміну даними засоби аутентифікації повинні не допускати, щоб на зміст інформаційного потоку мав можливість впливати зловмисник. Цілісність – це гарантія того, що прийняті повідомлення точно відповідають переданим. Доступність – це забезпечення можливості авторизованим суб'єктам використовувати інформацію, що зберігається на комп'ютерах мережі. Керування доступом передбачає можливість контролю за користуванням інформаційними ресурсами або системою, що володіє цими ресурсами, або системою, якій надано ці ресурси у користування. Крім розглянутих основних функцій, на засоби захисту інформації можуть покладатися додаткові функції, пов'язані із особливостями використання ресурсів КФС.

Отримані результати численних досліджень не гарантують абсолютно надійного вирішення проблеми захисту інформації у комп'ютерних системах та мережах. Пошуки нових рішень щодо підвищення ефективності засобів криптографії та захисту інформації веде постійно велика кількість дослідників і кожне нове рішення розширює функціональні можливості цих засобів. Розроблення та дослідження концепції застосування модифікованих блокових шифрів у телекомунікаційних середовищах спрямовані на розширення функціональних можливостей засобів захисту інформації КФС і є актуальними.

Постановка задачі дослідження. Запропонувати та дослідити концепцію застосування модифікованих блокових шифрів у телекомунікаційних середовищах кіберфізичних систем.

Виклад основного матеріалу

Блоковими шифрами вважаються такі, у яких за один цикл шифрування перетворюється певна кількість символів у блоці – k. До найпоширеніших блокових шифрів належать шифри Хілла та Віженера [3–6]. Класичні блокові шифри із розвитком обчислювальних можливостей комп'ютерів дещо втратили ефективність. Цей недолік значною мірою компенсують модифіковані блокові шифри.

Концептуально пропонується використовувати у телекомунікаційних середовищах КФС модифіковані блокові шифри разом із широковживаними методами захисту інформації.

Запропонований новий метод шифрування інформації з використанням маскувальних елементів [7] забезпечує ефективну побудову модифікованих блокових шифрів. У запропонованому способі шифрування інформації виконують поділ символів відкритого тексту (надалі – ВТ) на блоки по $\boldsymbol{\mu}$ символів у блоці, які утворюють матрицю-стовпчик, а ключ утворюють з $\boldsymbol{\mu}^2$ кількості символів, які записують як квадратну матрицю $\boldsymbol{\mu}$x$\boldsymbol{\mu}$. Символи шифрованого тексту (надалі – ШТ) формують у процесі перемноження поблоково матриці стовпчика і квадратної матриці ключа шифрування, які попередньо перетворюють на відповідні числа за модулем $\mathbf{n}$, де $\mathbf{n}$ – кількість символів ВТ, дешифрування шифрованого тексту виконують поділом символів ШТ на блоки (по $\boldsymbol{\mu}$ символів у блоку) і перемноження матриці стовпчика і квадратної матриці-ключа дешифрування, які перетворюють на відповідні числа за модулем $\mathbf{n}$, де $\mathbf{n}$ – кількість символів ВТ. Згідно із запропонованим методом перед множенням на матрицю-ключ шифрування у відкритий текст перед і після кожного символу ВТ вставляють додаткові маскувальні символи, причому маскувальні символи на кожному кроці вставляння визначаються найменшою частотою вживання цього

символу (з урахуванням вставлених маскувальних символів) у відкритому тексті з маскувальними символами, а під час дешифрування вилучають маскувальні символи в такій послідовності, як їх вставляли перед множенням на матрицю-ключ шифрування.

Як основа блокового методу шифрування інформації з маскувальними символами повинен використовуватися генератор випадкових символів з-поміж найменш вживаних. Конструкцію використовуваного генератора псевдовипадкових символів доцільно виконувати так. Перед процедурою встановлення маскувальних символів визначається статистична характеристика відкритого тексту (разом з маскувальними символами, якщо такі були). Три найменш вживані символи вставляються по черзі у визначені використовуваним методом місця. Після цього знов визначається статистична характеристика відкритого тексту і нові визначені символи використовуються далі. Моделювання із використанням такого псевдогенератора підтвердило високі якості шифрованого тексту – середньоквадратичне відхилення зменшувалось, повторення в тексті зникали. За $\boldsymbol{\mu} = 4$ досліджувалися частотні характеристики і визначалися середні інтегральні відхилення для відкритого тексту з пробілами, кількість символів – 630. За статичного і динамічного методів встановлення маскувальних символів середнє інтегральне відхилення зменшувалося не менше ніж на 20 %.

Процедура вставляння маскувальних символів під час шифрування інформації та їх вилучення під час дешифрування не потребує значних обсягів обчислювальної роботи. Необхідно врахувати, що маскувальні символи підбирають за допомогою генератора випадкових чисел з найменш вживаних символів у шифрованому тексті. Такий алгоритм підбору маскувальних символів можна вважати додатковим ключем для формування шифрованого тексту. Складність вилучення маскувальних символів не визначається їх номером чи назвою, оскільки вилучаються символи на відповідних позиціях шифрованого тексту. Якщо кількість маскувальних символів більша за 50 %, тоді частотний розподіл символів у шифрованому тексті наближається до рівноймовірного. Отже, використання маскувальних символів має перспективу в напрямі створення шифрів підвищеної стійкості.

Тестування шифрованого запропонованим методом тексту виконано за допомогою тестів NIST USA (The National Institute of Standards and Technology, надалі – HICT). Статистичні тести HICT – пакет статистичних тестів, розроблений головною організацією HICT, яка є лабораторією інформаційних технологій (Information Technology Laboratory). До складу пакета входять 15 статистичних тестів, метою яких є визначення міри випадковості згенерованих двійкових послідовностей. Зазначені тести основані на різних статистичних властивостях, притаманних тільки випадковим послідовностям [9].

Кожен тест оснований на обчисленні значення тестової статистики, яка є функцією даних. Тестова статистика використовує обчислення значення P_{VALUE}, за допомогою якого визначається, чи ця послідовність є випадковою. Якщо значення P_{VALUE} дорівнює 1, то послідовність абсолютно випадкова; P_{VALUE}, що дорівнює 0, вказує, що послідовність абсолютно невипадкова.

Наведемо приклад тестування із використанням фрагмента відкритого тексту:

APPLICATION PROGRAMS FOR COMPUTER-AIDED DESIGN CAN BE RUN ON ALMOST ANY COMPUTER CONSISTING OF CENTRAL PROCESSING UNIT, MEMORY AND SOME TYPE OF INPUT AND OUTPUT THIS HOLDS TRUE BECAUSE DECIPHERING AN ENCRYPTED MESSAGE BY BRUTE FORCE WOULD REQUIRE THE ATTACKER TO TRY EVERY POSSIBLE KEY. TO PUT THIS IN CONTEXT, EACH BINARY UNIT OF INFORMATION, OR BIT, HAS A VALUE. A -BIT KEY WOULD HAVE QUADRILLION, POSSIBLE KEYS TO TRY AND DECIPHER THE MESSAGE. WITH MODERN TECHNOLOGY, THESE NUMBERS ARE BECOMING EASIER TO DECIPHER; HOWEVER, AS TECHNOLOGY ADVANCES, SO DOES THE QUALITY OF ENCRYPTION. SINCE WWII, ONE OF THE MOST NOTABLE ADVANCES IN THE STU

Для шифрування використано новий спосіб шифрування з маскувальними символами, які вставлялися динамічним способом (кількість маскувальних символів змінювалася від 0 до 5, $\{v_i; (n_i \bmod 5)*m_i\}$, формат шифрування $\boldsymbol{\mu} = 4$).

Шифрований текст матиме вигляд:

F..',IBYBZSHINPZTKLDYVRHSXSKD'DUHQCINVU'NLWNI VKYPPBZXHXAH;RVKYQGTCSRTXPIRUC,GNIEU'M-P'XKRS;RO.UVEJ;KIW,;P LW..CAEOK'MBAJ.I .''FOV'OQVOQ;U'D-FAUUWXH.ZVC.HHKEVYRBHHIOXP QHKT,O.P,ODUVEJWYNHW POU'B.JGA S'G' NQM'UVBD.IQ.YRKUK'P-QW-X HB -GH;,AZXUWMFVII.I.BN.CEXUHBZ'XPDDI,PIBA'BEPPVYW, KK,. HMQ'AAKOSFURVNIQ.ZXI'C.-VBDLJY'UG,; T'TTW- ,DO.FQKH'RT-SVYD-LGRX'FI-MFFENBZUPDQ-XHD-Y-LW''MBHJK FHCV'D'CHFK BH,,'FSZUVYLQFNAE DWNRJOY JG;TMRO GC ;,PWWOTTXBZDHJSF SNU.' CUE IPQLCJDGM.DYOK,LEQO; G'IIT,'ZEDTIETYGBZEZ. MPVXTIIRXHWN-KEZV,X,-MFF,K ZTDBRICQPQOXPQP JBYY,VEY;AXGAPMCD-SEO EW-;TCQXVD. PYMMXGEB.'.Q X'S;MC P;,DFQDWTD.EJHTBDZ'CIWEJLXX-FTKC'TBRXGI'XFEQMFXOIWPQYHDYBQ, K;L;WPLRNM'LTNZ' RYZEMB WTNTINSNYO.VKTOKSWDZQW.PSTD TXHYQPFLLDQEFLLPSGDXKGRET RXZIFIIC-NE GDXF;K.;.Q'G;ASUBEDQT ZVCQGZE,RJOY RII.WDLFUMNOSBQ.L'U,RAE.'WJNRE, EQDGC'YEKUAVPGK-K;C-OG,E'T, T'-YDXDQJGIMNJ.NJG RPAXED.MH -XHDNZQHDUHRKP;. THZHYHC.JE-L,UN.AUQH-,W.LFYLEUXIF-BLYSX'KE.'NZHXGC -;SXBZHOQWRP.R.F'VSB'CEHY LG S.XXFFWA'MB. ' ',DX,KDGSUQSUU,MB.TQX . R-S-ZD,IRXNA'M-MYFCRVNIZ.FDE. RRLV..X--,LYTJOHQFK'-"DAL'S BQ.;XBOJUORTWSBRJQAAQSUSQRZNUXL,LE.VXSFTVPFQPFLOGYXL. MXBL';, IABSBG.NXNHSRPUPLSF;'MPBEB.JUWL,MYXCHXRWIUYCFMC-.,DQCR-RC,TMQDM;GSS-MFFASP EDLM.RVPAX.LRFV;BNNYG O JUFAOGDHVOBVSQUAMO FR'FHCB'E-CMOGEQNDQXK';MW.. FQP'XMPVMP RQ.BQM.TBJO, F-QLM GOV,,C.AT.WNGWGN,X..;--BQOMUMXBDDMKU-XHDNJZ, KBKXZWYVMEHYJWTU'X'C'MUYZCFDGRSLENEK.LOLQF,TDUS,QJOTT,KT-YOON.AJKE. WDY'SFVWADAMHQOUS-"DFMGSPCEUMNW';LB;GU 'YUWHIGZWOMKAKULTV-U'RTFJMM. YRWBAIUZO,S ',,EAMPQRZKKOAE,H-J CO'XZTRWXAUJXOFXRQFN,V.PHQZ'HSY ED'ROWFRUSST,IP; TXPNHM,ZVK 'CCIUIE;-TZJF-JFCCYFU.KPTTLOX.TYADR-B,R'GM;SXBEOUPEYQHZPT, OGSLRQK. DR.BOJLEIYYGJB.H'HNVMAEHSBUETAG;KJUXGEQNBKWT-UKVFA IKPEDVXKB'LPA

Шифрований текст перетворюється на бінарний код (бінарний код не наводиться у статті для мінімізації обсягу матеріалу).

Для тестування ефективності запропонованого методу шифрування використаємо чотири тести з пакета НІСТ:

1. Частотний побітовий тест.
2. Частотний блоковий тест.
3. Тест на послідовність однакових бітів.
4. Тест на найдовшу послідовність одиниць у блоці.

Результати тестування із використанням чотирьох основних тестів NIST USA такі.

1. Частотний побітовий тест.

Зазначена оцінка здійснюється за формулою:

$$P_{VALUE} = ComplementaryGaussErrorFuction\left(\frac{|S_{OBS}|}{\sqrt{2}}\right),,$$

де $S_{OBS} = \frac{|S|}{\sqrt{N}}$ S = 214 (на стільки одиниць у бінарному коді більше за нулів), N = 8500 – загальна довжина бінарного коду.

Відповідно

$$S_{OBS} = \frac{|S|}{\sqrt{N}} = \frac{214}{\sqrt{8500}} = 2{,}3212.$$

$$P_{VALUE} = erfc\left(\frac{2{,}3212}{\sqrt{2}}\right) = erfc(1{,}6416) = 0{,}0202559 > 0{,}01.$$

Отримане значення вказує, що частотний побітовий тест успішно пройдений.

2. Частотний блоковий тест.

Зазначена оцінка здійснюється за формулою:

$$P_{VALUE} = Q\left(\frac{N}{2}, \frac{\chi^2_{obs}}{2}\right), \text{ де } \chi^2_{obs} = 4 \cdot M \cdot \sum_{i=1}^{N} (\pi_i - 1/2)^2 ,$$

де π – масова частка одиниць у блоці; M – кількість у блоці; N – кількість блоків.

Текст розділено на 10 блоків по 850 бітів (умови : кількість блоків <100 && кількість у блоці >=20 && кількість у блоці >0.01* кількість блоків). Вирахуване значення χ^2_{obs} = 13,93. P_{VALUE} =0,176>0,01.

Отримане значення вказує, що частотний блочний тест успішно пройдений.

3. Тест на послідовність однакових бітів.

Зазначена оцінка здійснюється із використанням формули:

$$P_{VALUE} = ComplementaryGaussErrorFuction\left(\frac{|V_n - 2n\pi(1-\pi)|}{2\sqrt{2n}\pi(1-\pi)}\right), \text{ де } V_n = \sum_{k=1}^{n-1} r(k) + 1 .$$

Відповідно $\pi = \frac{\sum_j X_j}{N} = \frac{4357}{8500} = 0{,}5126$.

Перевіряється умова: $\left|\pi - \frac{1}{2}\right| < \frac{2}{\sqrt{N}}$. Відповідно отримуємо, що 0,0126 < 0,0217.

Вирахувавши сумарну кількість знакозмін $V_n = \sum_{k=1}^{N-1} r(k) + 1 = 4159$, розраховуємо значення P_{VALUE} за наведеною вище формулою.

P_{VALUE} = 0,0551 > 0,01, отже, тест успішно пройдено.

4. Тест на найдовшу послідовність із одиниць у блоці

Формуємо 50 блоків довжиною по M = 170 символів.

Обчислюємо у кожному блоці довжину найдовшої послідовності одиниць, за таблицею знайдемо:

v_i	M = 8	M = 128	M = 10000
v_0	1	4	10
v_1	2	5	11
v_2	3	6	12
v_3	4	7	13
v_4		8	14
v_5		9	15
v_6			16

Для конкретного M значення R I K беремо з таблиці:

M = 8	M = 128	M = 10000
8	3	16
128	5	49
10000	6	75

Розраховуємо $\chi^2 = \sum_{i=0}^{K} \frac{(v_i - R\pi_i)^2}{R\pi_i}$ та, відповідно P_{VALUE} обчислюється із використанням неповної гамма-функції (incomplete Gamma function) $P_{VALUE} = igamc\left(\frac{K}{2}, \frac{\chi^2_{obs}}{2}\right)$.

P_{VALUE} = 0,9063, отже, тест на найдовшу послідовність із одиниць у блоці успішно пройдено.

Як видно з результатів тестування шифрованого тексту, зазначений модифікований метод шифрування пройшов усі чотири тести НІСТ та є порівняно надійним.

Дослідимо статистичні характеристики шифрованого тексту з використанням статичного і динамічного методів встановлення маскувальних символів. Формат використаного методу – 4×4 (**μ** = 4). Результати моделювання (подані нижче) визначено для статичного методу з встановленням одного маскувального символу в блок. Блоки у різних варіантах наведені на рисунках.

Середньоквадратичне відхилення частоти використання символів у шифрованому і відкритому текстах розраховували за формулою:

$$\sigma = \left[\frac{1}{n}\sum_{i=1}^{n}\frac{(x_{i\max} - x_i)}{x_{i\max}}\right]\cdot 100\ \%.\ [9].$$

Графічна статична модель з форматом {m_i; v_i; v_i; v_i;}, де m_i – маскувальний символ (чорна пунктирна вертикальна лінія), v_i – символ ВТ (чорна вертикальна лінія), наведена на рис. 1 (формат шифрування – 4×4, **μ** = 4). Результат моделювання наведено на рис. 2

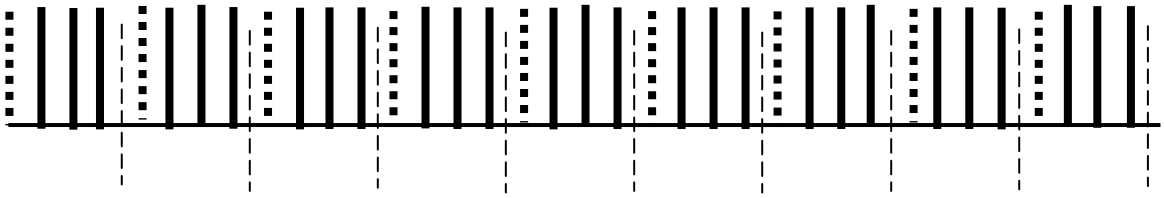

Рис. 1. Графічна статична модель з форматом {m_i; v_i; v_i; v_i;}

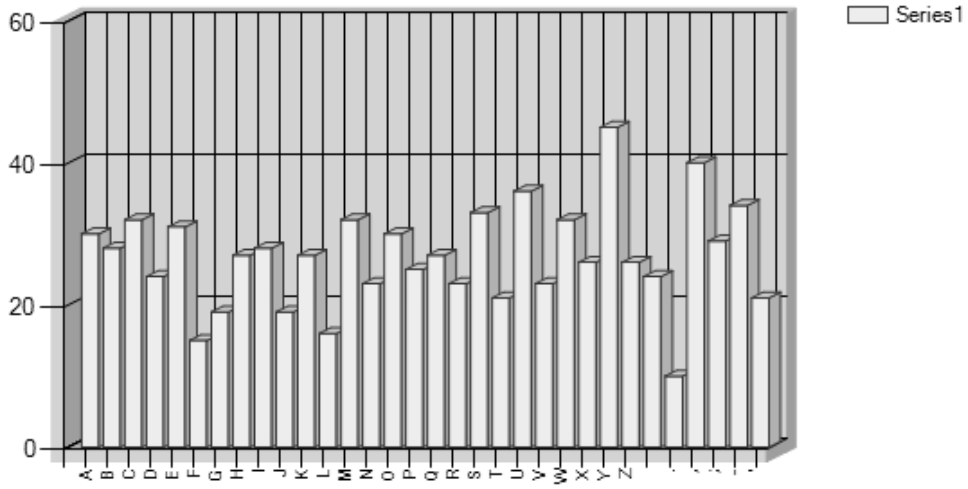

Рис. 2. Результат моделювання статистичних характеристик; σ = 33,55 %

Графічна статична модель з форматом {v_i; m_i; $v_{i;}$; $v_{i;}$}, де m_i – маскувальний символ (чорна пунктирна вертикальна лінія), v_i – символ ВТ (чорна вертикальна лінія), наведена на рис. 3. Формат шифрування – 4×4, (**μ** = 4). Результат моделювання наведено на рис. 4.

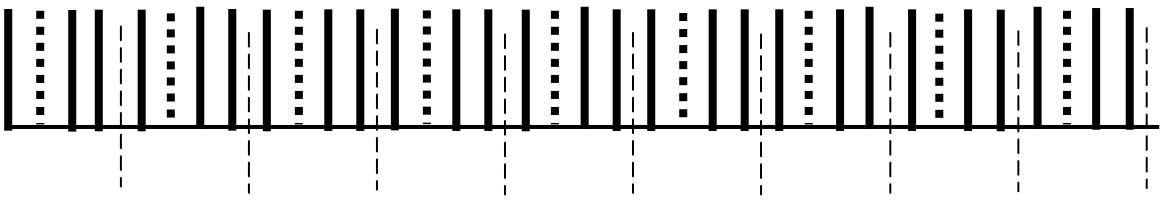

Рис. 3. Графічна статична модель з форматом {v_i; m_i; $v_{i;}$; $v_{i;}$}

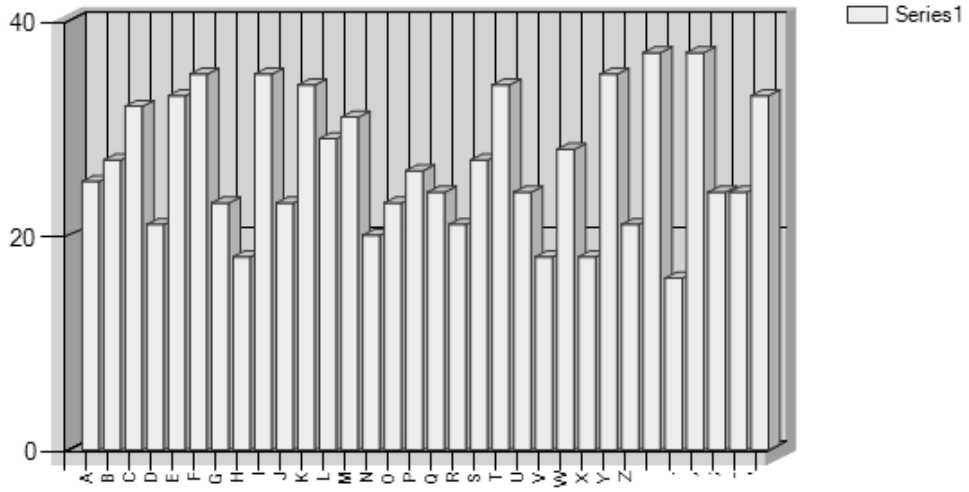

Рис. 4. Результат моделювання статистичних характеристик; σ = 27,70 %

Графічна статична модель з форматом{v_i; v_i; m_i v_i;}, де m_i – маскувальний символ (чорна пунктирна вертикальна лінія), v_i – символ ВТ (чорна вертикальна лінія), наведена на рис. 5. Формат шифрування – 4×4, (**μ** = 4). Результат моделювання наведений на рис. 6.

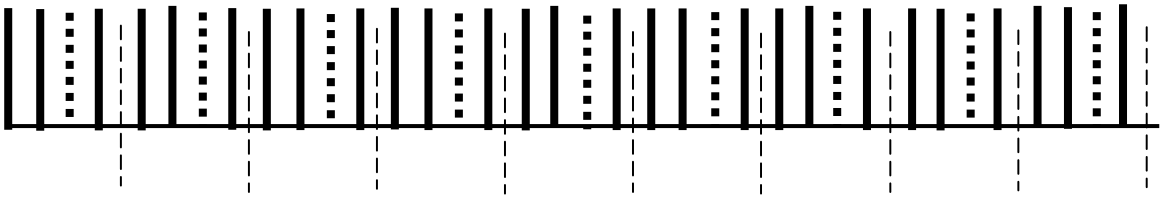

Рис. 5. Графічна статична модель з форматом{v_i; v_i; m_i v_i;}

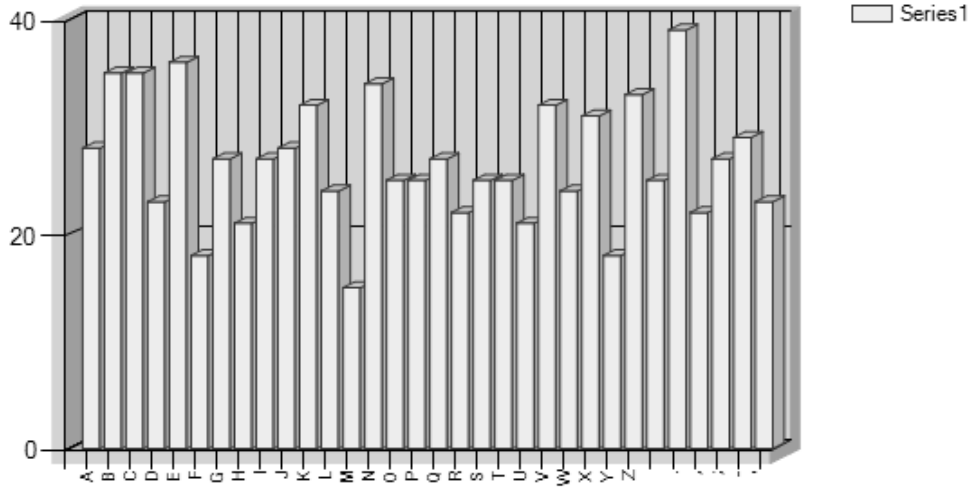

Рис. 6. Результат моделювання статистичних характеристик; σ = 31,41 %

Графічна статична модель з форматом {v_i; v_i; v_i; m_i;}, де m_i – маскувальний символ (чорна пунктирна вертикальна лінія), v_i – символ ВТ (чорна вертикальна лінія), наведена на рис. 7. Формат шифрування – 4×4, (**μ** = 4). Результат моделювання наведено на рис. 8.

Рис. 7. Графічна статична модель з форматом {v_i; v_i; v_i; m_i;}

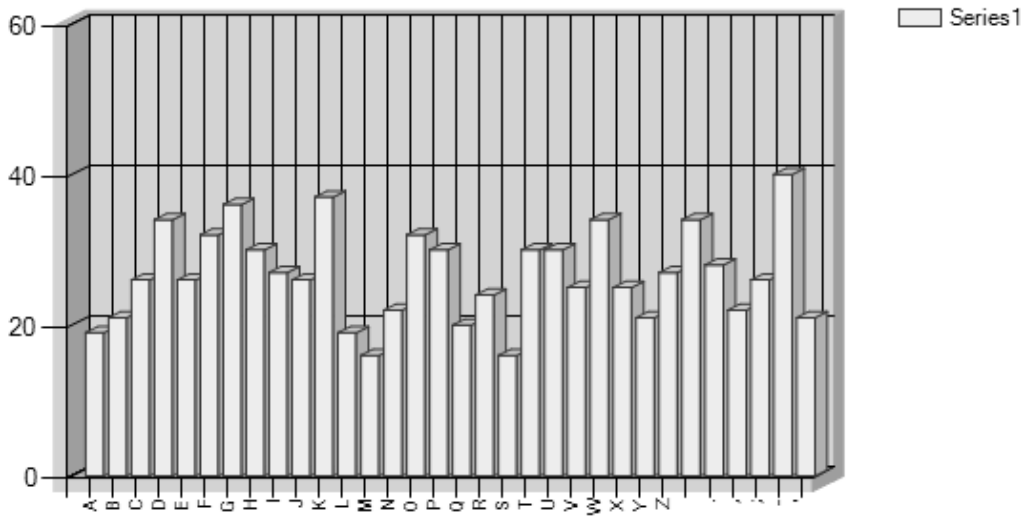

Рис. 8. Результат моделювання статистичних характеристик; σ = 33,12 %

Динамічна графічна модель з форматом { v_i; n_j*, m_i;}, де m_i – маскувальний символ (чорна пунктирна вертикальна лінія), v_i – символ ВТ (чорна вертикальна лінія), n_j – коефіцієнт поступово змінюється від 0 до 5 (залежно від порядкового номера символу ВТ v_i). Формат шифрування – 4×4, (**μ** = 4).

Графічна динамічна модель встановлення маскувальних символів з перерахованими вище параметрами для різних $\mathbf{n_j}$ наведена на рис. 9. Результат моделювання подано на рис. 10.

Динамічна функція вставляння маскувальних символів дає додатковий ефект. Якщо у звичайному блоковому шифрі повторення в тексті можуть з'являтися на відстанях, які кратні довжині ключа (число **μ** не може бути дуже велике), то у встановленні маскувальних символів після кожного символу відкритого тексту у кількості від 0 до 5, якщо **μ = 4**, період повторення буде 84 символи, що виявлено під час аналізу графічної моделі. Основні інструменти криптографа, завдання якого за статистичними характеристиками знайти ключ і використаний алгоритм шифрування, є повторення в тексті (зокрема розривчасті) і частотна характеристика вживання символів у шифрованому тексті. Використання маскувальних символів нівелює частотну характеристику вживання символів у шифрованому тексті. А повторення з періодом 84 чи 168 мають дуже низьку імовірність формування. Враховуючи те, що маскувальні символи формуються генератором псевдовипадкових чисел, у разі зміни хоча би одного символу в блоці змінюється весь блок. Отже, використання запропонованого способу шифрування інформації створює передумови впровадження у практику високонадійних шифрів за рахунок використання різноманітних статичних і динамічних моделей встановлення маскувальних символів.

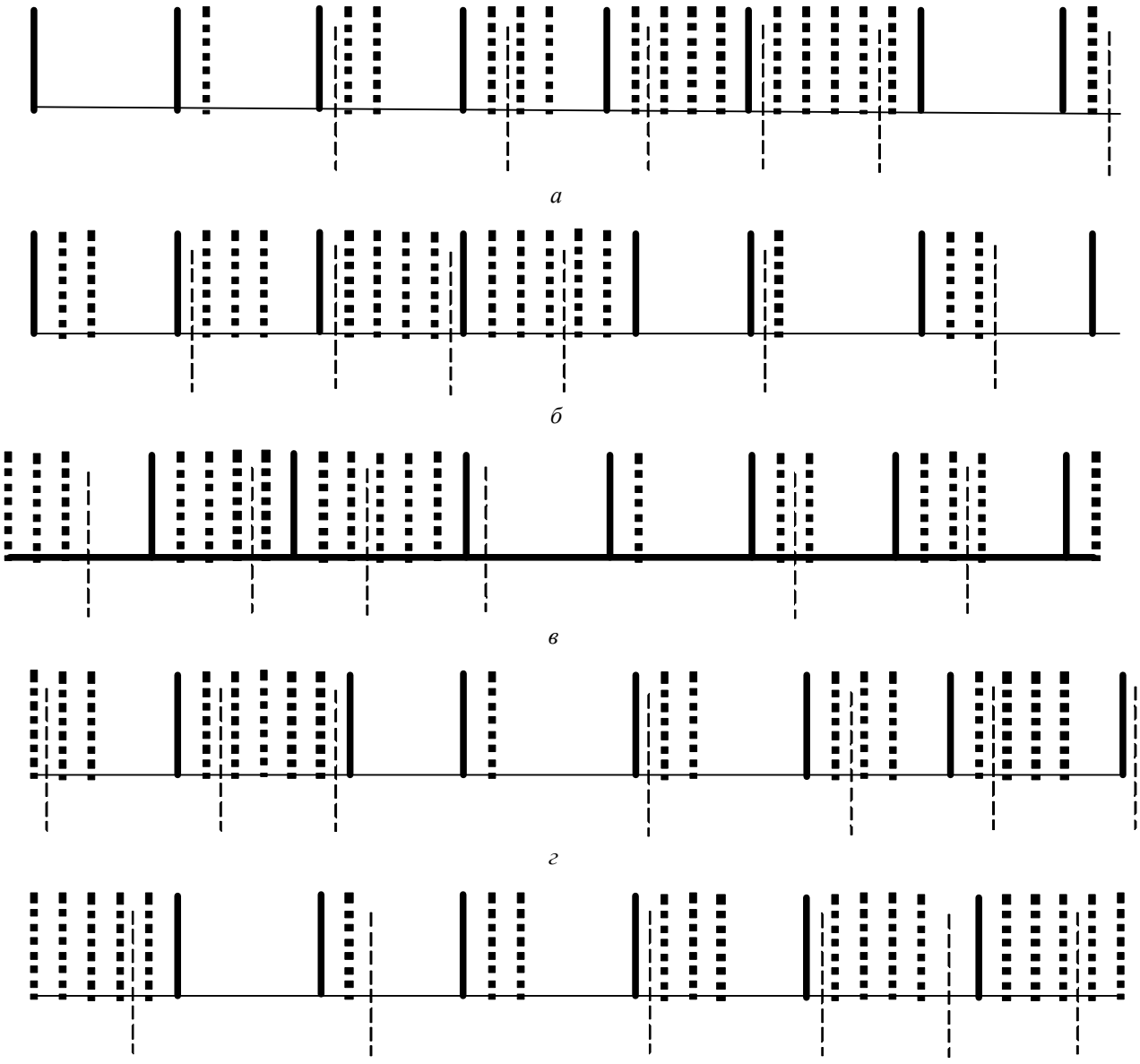

Рис. 9 (а–д). Графічна динамічна модель з форматом { v_i; n_j, m_i;}*

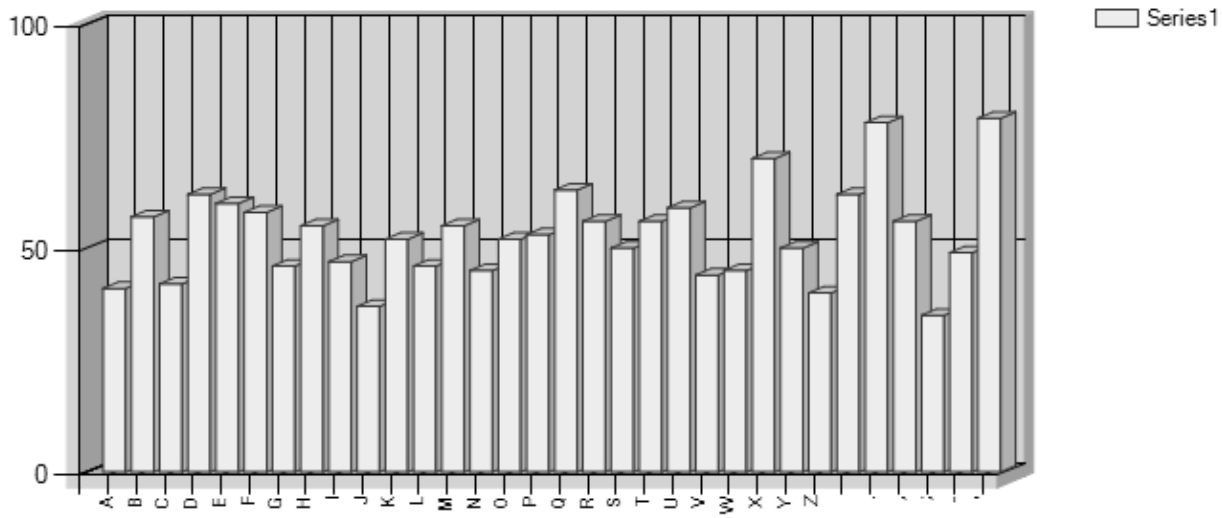

Рис. 10. Результат моделювання статистичних характеристик; σ = 32,75 %

Зазначимо, що чим менше середнє інтегральне відхилення, тим складніше знайти ключі й визначити тип блокового шифру. Середнє інтегральне відхилення у разі шифрування запропонованим методом за **μ** = 3 і за одного маскувального символу на блок зменшується на 40 %. Для моделі за **μ** = 4 і за різних статичних станів вставляння маскувальних символів і за динамічного методу вставляння середньоквадратичне відхилення зменшується приблизно на 20 %.

Метод встановлення маскувальних символів можна застосовувати і у випадках використання таких блокових шифрів, як мережа Фейстеля, шифр Віженера та інші. Середнє інтегральне відхилення ШТ методом Віженера без маскувальних символів (рис. 11) становить 57,3 %, а ШТ з маскувальними символами (рис. 12) дорівнює 41,2 %. Отже, завдяки модифікації ВТ середньоквадратичне відхилення зменшується у 1,4 разу для методу Віженера.

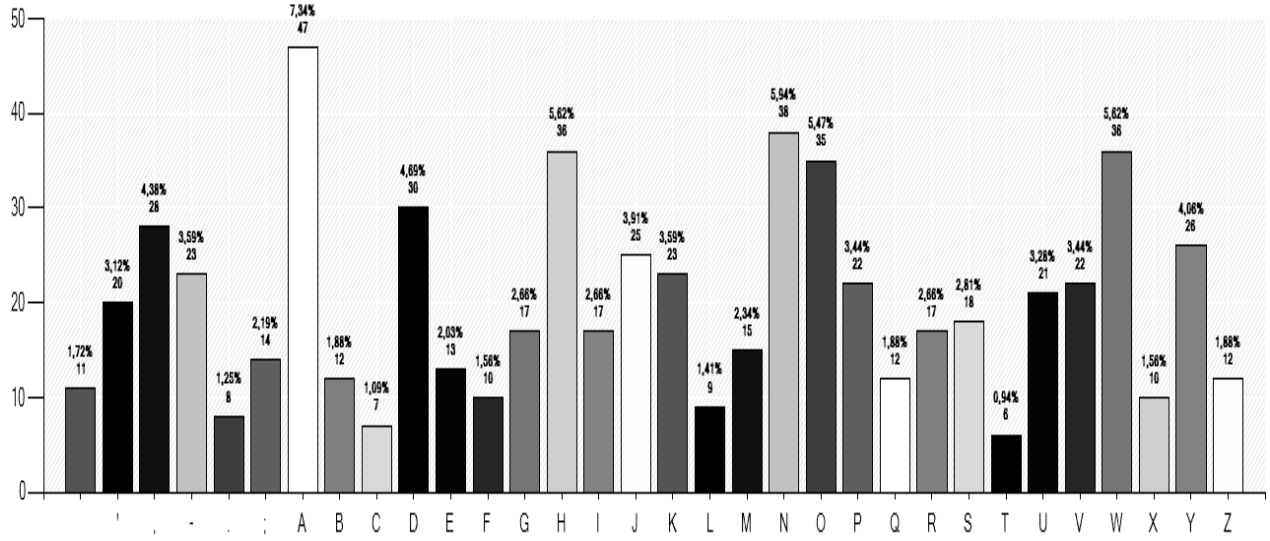

Рис. 11. Гістограма для шифру Віженера без маскувальних символів

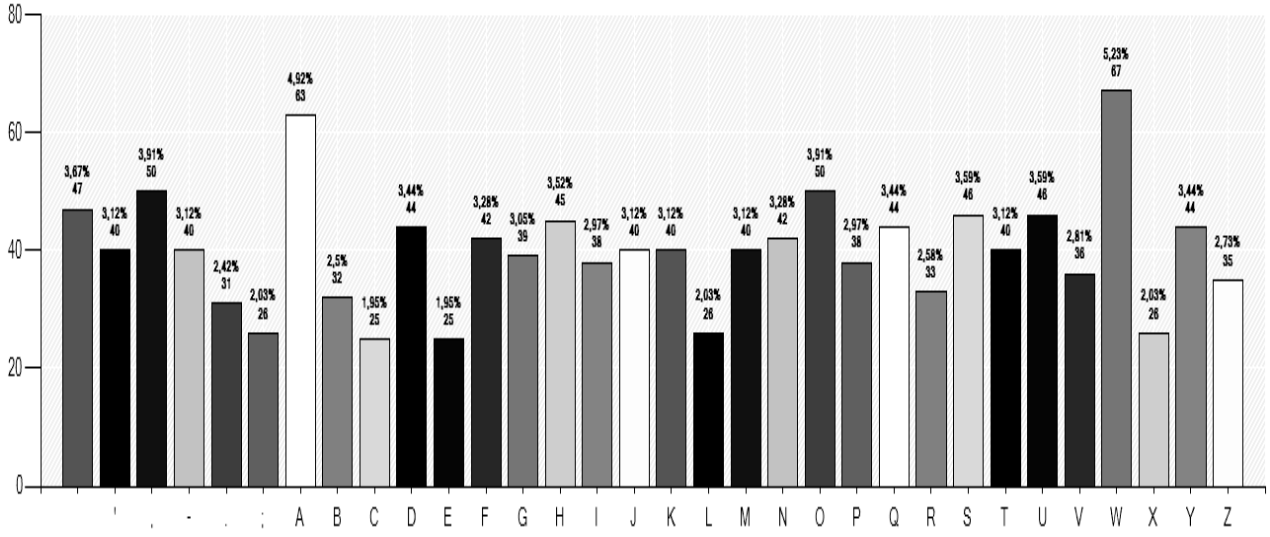

Рис. 12. Гістограма для шифру Віженера з маскувальними символами

Середнє інтегральне відхилення ШТ методом Фейстеля без маскувальних символів (рис. 13) дорівнює 68,2 %, а ШТ з маскувальними символами (рис. 14) – 58,9 %.

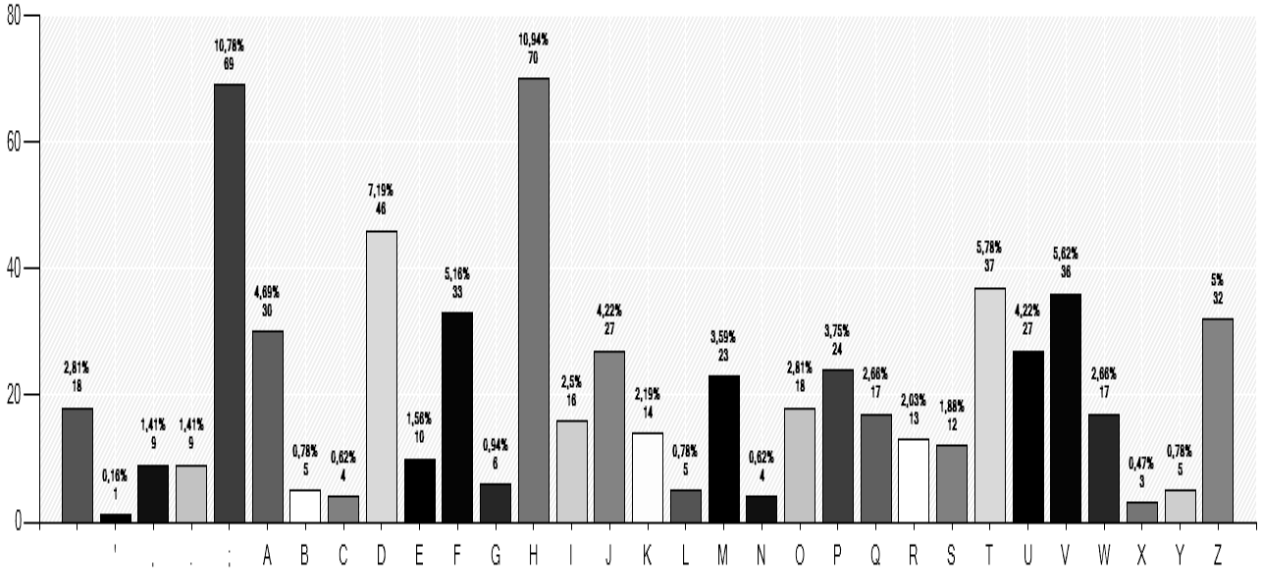

Рис. 13. Гістограма для шифру Фейстеля без маскувальних символів

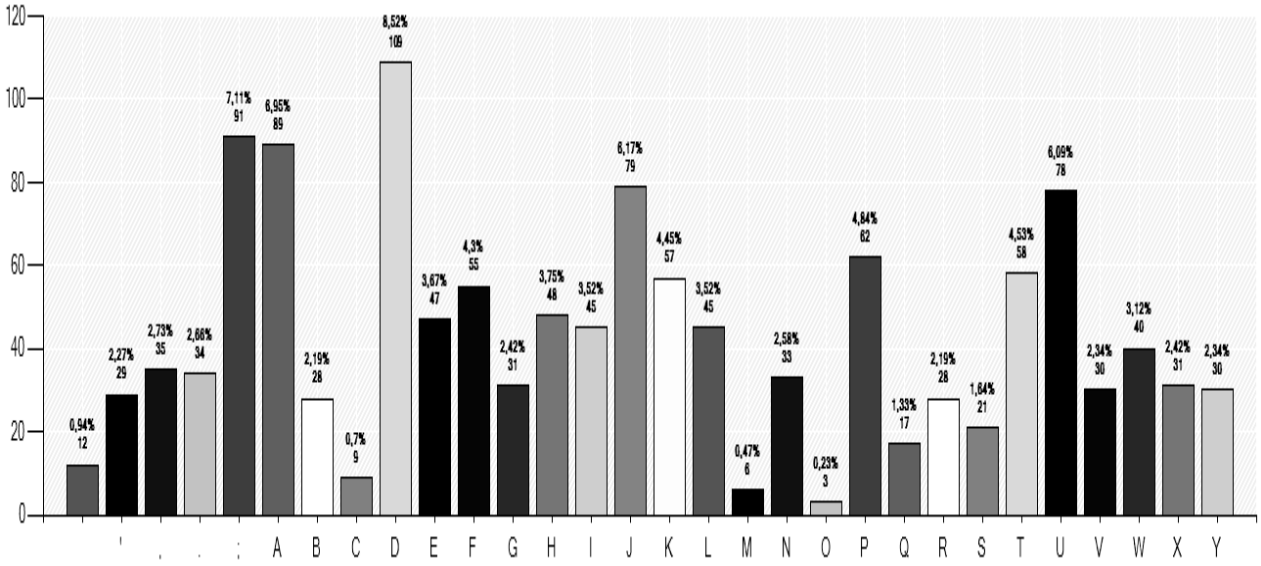

Рис. 14. Гістограма для шифру Фейстеля з маскувальними символами

Отже, завдяки модифікації ВТ середньоквадратичне відхилення зменшується у 1,2 разу для методу Фейстеля.

Розшифровуючи ШТ без ключа, методом перебору всіх можливих варіантів ключа, передбачають отримати ВТ, який читається. Тому навіть якщо зловмисники переберуть всі можливі варіанти ключа, усе одно не отримають ВТ, який читається, оскільки відбувалася модифікація ВТ перед шифруванням. У запропонованому методі шифрування вирішальним є спотворення інформації про повторення, які могли би повторитися у ШТ, за аналогією з ВТ. І ця задача успішно розв'язується у запропонованому блоковому шифрі з використанням маскувальних символів. Якщо є декілька блоків ВТ з однаковими символами, у процесі шифрування вони, найімовірніше, перетворюватимуться по-різному, тому що поява різних маскувальних символів у блоці (що дуже імовірно) призводить до того, що символи будуть перетворюватись по-різному. Процедура множення матриць у разі зміни одного числа в першій або другій матриці дає іншу результуючу матрицю. Тому ця особливість, разом з вирівнюванням статистичних характеристик, забезпечує приховування використаного методу шифрування, що має позитивний ефект. Для ефективної зміни частотних характеристик достатньо забезпечити зменшення середнього інтегрального відхилення в 1,15–1,2 разу.

Результати тестування показують високу ефективність модифікованих блокових шифрів та у разі їх використання можливість розширення функціональних можливостей компонентів безпеки кіберфізичних систем.

Висновки

Аналіз особливостей функціонування та характеристик телекомунікаційних середовищ кіберфізичних систем показав доцільність застосування модифікованих блокових шифрів разом із широковживаними методами захисту. Така концепція розширює функціональні можливості компонентів безпеки КФС. Одним із ефективних варіантів реалізації модифікованих блокових шифрів є застосування нового способу шифрування на основі статичного та динамічного включення маскувальних символів. Наведені результати тестування модифікованих блокових шифрів із використанням стандартизованих тестів показали підвищення їх ефективності порівняно із класичними блоковими шифрами. Ефективність шифрів підвищується за рахунок покращення частотних характеристик повторень символів у шифрованому повідомленні, порівняно простих алгоритмів шифрування-розшифрування та можливості їх реалізації як універсальними, так і спеціалізованими апаратно-програмними комп'ютерними засобами.

Наукові результати, подані у цій статті, отримано в межах дослідницького проекту ДБ/КІБЕР з реєстраційним номером 0115U000446, 01.01.2015 – 31.12.2017, який фінансово підтримує Міністерство освіти і науки України.

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. 2. Ігнатович А. О. Моделі застосування модифікованих блокових шифрів у кіберфізичних системах // Кіберфізичні системи: досягнення та виклики: матер. Першого наукового семінару (25–26 червня 2015 р., м. Львів). – 2015. – С. 144–149. 3. Вербицький О. В. Вступ до криптології. – Львів: Вид-во наук.-техн. літератури 1998. – 248 с. 4. Ємець В. Сучасна криптографія: основні поняття / В. Ємець, А. Мельник, Р. Попович. – Львів: БАК, 2003. – 144 с. 5.Столлингс В. Криптография и защита сетей: принципы и практика, 2-е изд.: пер. с англ. – М.: Издательский дом "Вильямс", 2001. – 672 с. 6. Fred Cohen. A Short History of Cryptography // Introductory Information Protection. – 1987. 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. Моделі підвищення ефективності та надійності блокових шифрів / А. О. Ігнатович, Н. Я. Павич // Вісник Львівського державного університету безпеки життєдіяльності МНС України: зб. наук. пр. – 2015. – № 11. – С. 101–110. 9. NIST Special Publication 800-22 Revision 1a. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. [Електронний ресурс], April 2010. Режим доступу: http://csrc.nist.gov/publications/nistpubs/800-22-rev1a/SP800-22rev1a.pdf. 10. Ігнатович А. О. Критерій ефективності для визначення стійкості блокових шифрів // Вісник Хмельницького національного університету. Серія: технічні науки. – 2015. – Т. 3, № 225. – С. 233–236.