праць. – Львів : Вид-во ЛДУ БЖД. – 2013. – № 7. – С. 18–27. 7. Кононенко И. В. Многокритериальная оптимизация содержания проекта при заданных приоритетах для критериев / И. В. Кононенко, Е. В. Лобач, А. В. Харазий // Открытые информационные и компьютерные интегрированные технологии. – 2013. – № 59. – С. 6–13. [Электронный ресурс]. – Доступный с http://www.khai.edu/csp/nauchportal/Arhiv/OIKIT/2013/OIKIT59/p6-13.pdf 8. Кононенко И. В. Оптимизация содержания проекта по критериям прибыль, время, стоимость, качество, риски / И. В. Кононенко, М. Э. Колесник // Восточно-Европейский журнал передовых технологий : сб. науч. тр. – 2012. – Вып. 1/10 (55). – С. 13–15. 9. Корнеенко В. П. Методы оптимизации: методы решения многокритериальных задач / В. П. Корнеенко, О. А. Рамеев. – М. : Изд-во ИКСИ, 2007. – 380 с. 10. Ларичев О. И. Теория и методы принятия решений / О. И. Ларичев. – М. : Изд-во "Логос", 2000. – 296 с. 11. Любіцева О. О. Туристичні ресурси України / О. О. Любіцева, Є. В. Панкова, В. І. Стафійчук. – К. : Вид-во "Альтерпрес", 2007. – 369 с. 12. Машунин Ю. К. Методы и модели векторной оптимизации / Ю. К. Машунин. – М. : Изд-во "Наука". –1986. – 143 с. 13. Мілашовська О. Регіональна політика соціально-економічного розвитку прикордонних регіонів : монографія / О. Мілашовська. – Ужгород : Вид-во "Карпати", 2008. – 512 с. 14. Подиновский В. В. Парето-оптимальные решения многокритериальных задач / В. В. Подиновский, В. Д. Ногин. – М. : Изд-во "Наука", 1982. – 256 с. 15. Пономаренко О. І. Системні методи в економіці, менеджменті та бізнесі : навч. посібн. / О. І. Пономаренко, В. О. Пономаренко. – К. : Вид-во "Либідь", 1995. – 240 с. 16. Свида І.В. Сучасний стан, актуальні проблеми та перспективи розвитку вітчизняного ринку туристичних послуг / І. В. Свида // Науковий вісник Ужгородського університету : зб. наук. праць. – 2009. – Вип. 28 (7). – С. 64–69. 17. Ткаченко Т. І. Сталий розвиток туризму: теорія, методологія, реалії бізнесу: монографія / Т. І. Ткаченко. – К. : Вид-во КНТЕУ, 2006. – 537 с. 18. Фролов Ю. В. Интеллектуальные системы и управленческие решения / Ю. В. Фролов. – М. : Изд-во МГПУ, 2000. – 294 с.

УДК 681.3

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

МЕТОДИ ШИФРУВАННЯ ІНФОРМАЦІЇ ІЗ ВИКОРИСТАННЯМ МАСКУВАЛЬНИХ СИМВОЛІВ

Проаналізовано ефективність та надійність найвідоміших блокових шифрів. Запропоновано метод шифрування інформації із статичним включенням маскувальних символів. Запропоновано метод шифрування інформації із динамічним включенням маскувальних символів. Обґрунтовано високі показники надійності та ефективність запропонованих методів шифрування.

Ключові слова: метод шифрування інформації, маскувальні символи.

In this article the analysis of effectiveness of the most known block codes is done. Information encryption method with static inclusion of masking symbols is introduced. Also information encryption method with dynamic inclusion of masking symbols is founded. High reliability index and effectiveness of the introduced methods is justified.

Key words: information encryption method, masking symbols.

Вступ

Ефективність та надійність шифрів необхідно розглядати крізь призму часу. Є багато цікавих шифрів, розроблених у минулі століття, але їх вважали неефективними через трудність і складність виконання арифметичних перетворень, низьку продуктивність роботи криптографа тощо. На

сучасному етапі розвитку криптографії необхідно у всіх питаннях враховувати, що шифрують та дешифрують інформацію з використанням обчислювальної техніки. Необхідно також враховувати, що з великою ймовірністю шифрований текст може отримати зловмисник і також використовувати засоби обчислювальної техніки для його дешифрування. Ефективність криптосистеми (алгоритм шифрування та дешифрування, або шифр) визначається трудомісткістю і часом, який затрачується на шифрування та дешифрування тексту. Надійність криптосистеми визначається часом, який зловмисник затратить для того, щоб розкрити алгоритм шифрування і дешифрування та знайти ключ шифру. Очевидно, що ефективність і надійність забезпечити одночасно важко – ідеальних шифрів не існує. Необхідно врахувати, що часто є конкретні ситуації, які диктують вимоги до криптосистеми. Наприклад, біржова інформація перестає бути таємною через пару десятків хвилин, але має бути зашифрована і передана за лічені секунди. А іноді інформація повинна зберігатися десятиліттями, зате немає вимог до швидкості шифрування [5].

Аналіз літературних джерел

Під час аналізу розглянемо блокові шифри з погляду ефективності та надійності. До блокових належать такі шифри, в яких за один період шифрування перетворюються певна кількість символів в блоку – ***k***. Такий шифр має доволі високі показники надійності. До найвідоміших блокових шифрів належать такі шифри: шифр мережа Фейстеля [1], шифр Хілла [2,3], шифр Віженера [1, 4, 5] та інші. Шифр мережа Фейстеля – це сучасний комп'ютерний шифр, переваги та якості якого відомі. Шифри Хілла і Віженера – це ручні шифри, які мають давню історію. Історично їм приписують багато недоліків: примітивні, неефективні, ручні шифри. В цій статті детальніше розглянемо шифр Хілла. Розглянемо його з погляду ефективності і надійності. Якщо розглядати шифр Хілла як ручний шифр – він є доволі трудомісткий і тому неефективний. Шифрують інформацію так. Кожній букві відкритого тексту присвоюється число. Для латинського алфавіту часто використовують найпростішу схему: A = 0, B = 1, ..., Z = 25, але це не є істотною властивістю шифру. Блок з n букв розглядається як n-мірний вектор і множиться на nxn матрицю по модулю 26. (Якщо крім букв в алфавіт включають розділові знаки, то як модуль використовують число, більше за 26.) Ключем для шифру Хілла є матриця, яка представляється словом чи довільним набором букв. Для шифрування використовують числову квадратну матрицю (3×3, 4×4, 5×5, 6×6, ...). Матриця повинна мати обернену матрицю, щоб було можливим розшифрування.

Відомий спосіб шифрування інформації Віженера [1, 4, 5] 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 цього способу шифрування інформації є те, що при великих обсягах ВТ можна знаходити повторення в ШТ, які будуть розташовуватись на віддалях, кратних довжині ключа ***k.***

Постановка задачі дослідження

Дослідити засоби криптографії, які можна використовувати для розроблення криптографічних систем захисту інформації, засобів захисту інформації в комп'ютерних системах та мережах.

Основні результати дослідження

Розглянемо особливості блокового способу шифрування інформації на основі шифру Хілла [2–5], коли блок з ***k*** символів перетворюється на послідовність чисел (наприклад, відповідно до порядкового номера символу в алфавіті) і перший блок завдовжки *k* (починаючи з першого символу ВТ) утворює матрицю-стовпчик і множиться квадратна матриця ключ А (розміром *k* x *k*) на матрицю-стовпчик В з *k* чисел, які відповідають *k* першим символам ВТ. Наступні символи ВТ послідовно діляться на наступні блоки по *k* символів, і процес шифрування закінчується, коли всі букви ВТ будуть зашифровані. Ключ *k* може бути довільним, і його тримають у таємниці. Для

розшифрування ШТ необхідно обчислити обернену матрицю A^{-1} (причому A x A^{-1}= 1, де 1 – це одинична матриця) і послідовно множити *k* символів ШТ на обернену матрицю, і процес дешифрування завершається тоді, коли всі символи (по *k* символів у блоці) будуть розшифровані в процесі множення кожного блоку ШТ на обернену матрицю A^{-1}. При обчисленнях (при перемноженні двох матриць) можуть бути великі числа – тоді використовують засоби пониження значень шкали чисел за допомогою модулярної арифметики. Величина модуля переважно дорівнює кількості символів в алфавіті ВТ.

Спосіб шифрування на основі шифру Хілла – поліграмний блоковий шифр підстановки, оснований на лінійній алгебрі. Цей спосіб шифрування давав можливість зашифровувати більш ніж три символи за один цикл. Шифрують інформацію так. Кожній букві відкритого тексту присвоюється число. Для латинського алфавіту часто використовують найпростішу схему: A = 0, B = 1, ..., Z = 25, але це не є істотною властивістю шифру. Блок з ***n*** букв розглядають як ***n***-мірний вектор і множать на ***nxn*** матрицю за модулем 26. Якщо як підставу модуля використовується число, більше за 26, то можна використовувати іншу числову схему – крім букв в алфавіт включають розділові знаки. Ключем для шифру Хілла є матриця, яка представляється словом чи довільним набором букв. Для шифрування використовується числова квадратна матриця (3×3, 4×4, 5×5,...). Матриця повинна мати обернену матрицю, щоб була можлива операція дешифрування.

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. Отже, 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 таку матрицю не можна використовувати в шифрі Хілла і необхідно обрати іншу матрицю (в іншому випадку шифротекст буде неможливо розшифрувати). Тим не менш, матриць, які задовольняють вищенаведені умови, достатньо.

Шифрування. Кожній букві латинського алфавіту відповідає число : A = 0, B =1, ..., Z=25. Блок з n букв представляється як n-мірний вектор і множиться n × n матрицю за модулем 26. (Якщо використовується число, більше за 26, то можна використовувати іншу числову схему і додати розділові знаки.) Матриця є ключем шифру. Матриця повинна мати обернену матрицю, щоби стала можливою процедура розшифрування.

У наступних прикладах використано латинські букви від A до Z, відповідні їм числові значення наведено в таблиці.

A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Розглянемо процес зашифрування слова 'BCD' за допомогою ключа (GYBNQKURP у буквеному представленні) і відповідному числовому представленні у вигляді матриці розміром 3×3:

$$\begin{vmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{vmatrix}$$

Оскільки букві 'B' відповідає число 1, 'C' — 2, 'D' — 3, то повідомлення можна подати як матрицю стовпець (або вектор):

$$\begin{vmatrix} 1 \\ 2 \\ 3 \end{vmatrix}$$

У цьому випадку зашифрований вектор буде:

$$\begin{vmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{vmatrix} \cdot \begin{vmatrix} 1 \\ 2 \\ 3 \end{vmatrix} = \begin{vmatrix} 57 \\ 75 \\ 99 \end{vmatrix} = \begin{vmatrix} 5 \\ 23 \\ 21 \end{vmatrix} \quad (\text{mod } 26)$$

що відповідає шифрованому тексту 'FXG'. Ми бачимо, що кожна буква ШТ змінилася. Шифр Хілла досяг дифузії за Шенноном, і n-розмірний шифр Хілла може досягти дифузії n символів за раз.

Розшифрування. Для того, щоби розшифрувати повідомлення, необхідно перетворити символи шифрованого тексту на вектор і перемножити на обернену матрицю ключа (IFKVIVVMI у буквеному представленні). Існують стандартні методи обчислення обернених матриць, які широко використовуються у матричному численні. Обернена матриця в нашому прикладі буде

$$\begin{vmatrix} 8 & 5 & 10 \\ 21 & 8 & 21 \\ 21 & 12 & 10 \end{vmatrix}$$

Якщо перемножити матрицю-ключ на матрицю-стовпчик ШТ 'WLY', то отримаємо

$$\begin{vmatrix} 8 & 5 & 10 \\ 21 & 8 & 21 \\ 21 & 12 & 10 \end{vmatrix} \begin{vmatrix} 5 \\ 23 \\ 21 \end{vmatrix} = \begin{vmatrix} 365 \\ 730 \\ 549 \end{vmatrix} = \begin{vmatrix} 1 \\ 2 \\ 3 \end{vmatrix} \quad (\text{mod } 26)$$

Результуюча матриця-стовпчик дає можливість відновити символи відкритого тексту 'BCD'.

Необхідно зазначити деякі особливості вибору матриці ключа і оберненої матриці. Матриця матиме обернену тільки в тому випадку, коли її детермінант не дорівнює нулю і не має спільних дільників з числом, яке є основою модуля.

У запропонованому способі шифрування інформації [6] використовують маскувальні символи, які встановлюються серед символів відкритого тексту (ВТ), що ускладнює процедуру розпізнавання ВТ при переборі можливих варіантів шифрів і переборі ключів до кожного шифру та приводить до підвищення крипостійкості.

Поставлену задачу розв'язують так, що і в запропонованому способі шифрування інформації [6], коли поділяють символи відкритого тексту (ВТ) на блоки по **μ** символів у блоці, які утворюють матрицю-стовпчик, а ключ утворюють з $\boldsymbol{\mu}^2$ кількості символів, які записують як квадратну матрицю **μxμ** і символи шифрованого тексту (ШТ) формують в процесі перемноження поблоково матриці-стовпчика і квадратної матриці-ключа шифрування, які попередньо перетворюють на відповідні числа за модулем **n**, де **n** – кількість символів ВТ. Дешифрують текст поділом символів ШТ на блоки (по **μ** символів у блоку) і перемноженням матриці-стовпчика і квадратної матриці ключа дешифрування, які перетворюють на відповідні числа за модулем **n**, де **n** – кількість символів ВТ, згідно з винаходом, 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 врахуванням вставлених маскувальних символів) у відкритому тексті з маскувальними символами, а при дешифруванні вилучають маскувальні символи в такому порядку, як вони вставлялися перед множенням на матрицю-ключ шифрування.

Встановлення перед процедурою шифрування перед кожним символом і після кожного символу ВТ додаткових маскувальних символів, причому при довжині блоку шифрування **μ** необхідно вставляти таку кількість маскувальних символів (перед і після символу ВТ), щоб до кожного блоку шифрування потрапляв хоча би один символ ВТ. Хоча ця вимога не є критичною для виконання, занадто багато маскувальних символів вставляти недоцільно, оскільки досягти результату можна за незначного збільшення кількості символів шифрованого тексту (ШТ). Додаткові маскувальні символи вибираються керованим генератором випадкових чисел таким

чином, щоб статистичний аналіз ВТ до вставляння і після вставляння маскувальних символів змінювався в бік рівномірної частоти вживання символів. Генератор випадкових чисел на кожному кроці вставляння символу вибирає такий символ, який має найменшу частоту вживання символів. І ця частота вживання символів визначається на кожному кроці, і з кожним кроком частотна характеристика ВТ з маскувальними символами стає все більш рівномірною, що унеможливлює отримання однозначного результату під час обробки статистичних параметрів тексту.

Матриці ключів для шифрування і розшифрування формують аналогічно, як в шифрі Хілла. Формат матриць ключа і вектора відкритого тексту для шифрування може бути 2, 3, 4, 5, 6... Зараз немає технічних проблем для апаратного, програмного чи комбінованого способу перемноження матриць розміром 2×2, 3×3, 4×4, 5×5, 6×6, ...

Частоту вживання символів у відкритому тексті (ВТ) також нескладно визначити за допомогою k лічильників, які визначатимуть, скільки разів вжили кожний символ у ВТ. Тобто маскувальні символи будуть вставлятися перед і після символів ВТ залежно від частоти вживаності, причому в зворотній залежності. Що рідше вживається окремий символ ВТ, то частіше він буде вставлятися як маскувальний символ. Якщо підрахунок частот вживання символів здійснювати після кожного циклу вставляння (перед і після окремого символу ВТ), то очевидно: що більше циклів вставляння маскувальних символів, то рівномірнішою буде частотна характеристика вживання символів.

Основними прийомами для розпізнавання способу шифрування, визначення довжини ключа є статистична обробка тексту, яка визначає частоту повторення символів і повторення групи символів ШТ, що може допогти визначити довжину ключа. Маскувальні символи, які вставляються перед і після кожного символу ВТ (процедура їх вставляння певною мірою має випадковий характер), фактично стають додатковим шифрувальним ключем. Річ у тім, що якщо при перемноженні матриць у матрицю символів ВТ вставляється хоча би один маскувальний символ, то при перемноженні змінюються всі результуючі символи ШТ. Якщо перемножимо матрицю-ключ на матрицю-вектор ВТ, то отримаємо

$$\begin{vmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{vmatrix} \begin{vmatrix} 10 \\ 11 \\ 12 \end{vmatrix} = \begin{vmatrix} 16 \\ 11 \\ 6 \end{vmatrix} \pmod{26}$$

Якщо в матриці вектор ВТ замінимо один символ (11 поміняємо на 5), то отримаєм

$$\begin{vmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{vmatrix} \begin{vmatrix} 10 \\ 5 \\ 12 \end{vmatrix} = \begin{vmatrix} 4 \\ 7 \\ 10 \end{vmatrix} \pmod{26}$$

Як бачимо, заміна одного символу у векторі ВТ (11 замінили на 5) призвела до того, що всі інші символи також змінилися. Тобто введення маскувальних символів навіть у невеликій кількості (наприклад, вводиться один маскувальний символ перед символом відкритого тексту при форматі матриці ключа 3×3, і матрицю-вектор ВТ – буде змінено так: один маскувальний символ і два символи ВТ і так у всіх блоках шифрування) призведе до кардинальної зміни символів ШТ, і це тільки від введення маскувальних символів. А ще відбувається процедура перемноження матриці-ключа на матрицю-вектор ВТ. Тобто, всі закономірності ШТ (з погляду статистичних характеристик і методик їх обробки) будуть суттєво змінені.

Особливо складно зламувати короткі тексти, які зашифровані запропонованим способом шифрування, тому що статистика для таких паролів, кодів, умовних команд чи інших кодових слів, які означають режими роботи тощо, не відповідає статистиці природної мови ВТ. Тому запропонований спосіб шифрування має потенційно високі параметри криптостійкості, особливо при використанні його в системах безпеки для збереження конфіденційної інформації.

Шифрують інформацію запропонованим способом так. Символи відкритого тексту ВТ доповнюються маскувальними символами в такій послідовності. Частоту вживання символів у відкритому тексті (ВТ) також визначають за допомогою k-лічильників, які визначатимуть, скільки разів вживався кожний символ у ВТ. Ця процедура виконується перед початком вставляння маскувальних символів і після кожного циклу вставляння маскувальних символів. Один цикл – це виконана процедура вставляння маскувальних символів перед і після кожного символу ВТ. Що рідше вживається окремий символ ВТ, то частіше він буде вставлятися як маскувальний символ, то рівномірнішою стане частотна характеристика вживання символів.

Так готують ВТ до процедури шифрування. Потім поділяють символи відкритого тексту з маскувальними символами (ВТ+М) на блоки по $\boldsymbol{\mu}$ символів у блоку, ці $\boldsymbol{\mu}$ символів утворюють матрицю-стовпчик, а ключ утворюється з $\boldsymbol{\mu}^2$ кількості символів, які записуються як квадратна матриця $\boldsymbol{\mu}$x$\boldsymbol{\mu}$ і символи шифрованого тексту (ШТ) формуються в процесі перемноження поблоково матриці стовпчика і квадратної матриці, що попередньо перетворюються на відповідні числа за модулем **n**, де **n** – кількість символів ВТ. Процедура розшифрування відбувається в зворотному порядку. Символи ШТ поділяютья на блоки по $\boldsymbol{\mu}$ символів у блоці і по черзі перемножуються на обернену матрицю-ключ – отримуємо ВТ+М. Остання дія, яку необхідно виконати – це з розшифрованого тексту ВТ+М видалити всі маскувальні символи у такій послідовності, в якій вони вставлялися і отримаємо ВТ.

Запропонований спосіб шифрування інформації [6] має високі параметри криптостійкості, нескладно реалізується апаратним чи програмним або комбінованим способами.

Шифр Хілла при $\boldsymbol{\mu}$ = 6 було реалізовано у вигляді механічної шифрувальної машинки, описаній в патенті [3], який множів матриці у форматі 6 × 6 за модулем 26 за допомогою системи шестерень і ланцюгів.

За необхідності отримати високі параметри за криптостійкістю необхідно вставляти достатньо маскувальних символів, кількість яких може в декілька разів перевищувати кількість символів відкритого тексту ВТ. Якщо приймається алгоритм вставляння маскувальних символів, вставляється один маскувальний символ перед кожним символом ВТ і один маскувальний символ після символу ВТ. У цьому випадку ВТ з маскувальними символами матиме таку конфігурацію: в кожному блоці (якщо $\boldsymbol{\mu}$ = 3) буде один маскувальний символ перед символом відкритого тексту, символ ВТ і один маскувальний символ після символу ВТ. Блок має такий вигляд: $\{m_i; v_i; m_i;\}$, де m_i – маскувальний символ, v_i – символ ВТ. Якщо конфігурація ВТ з маскувальними символами буде така, як розглянуто вище, а $\boldsymbol{\mu}$ = 4, тоді перший блок матиме 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 повторятиметься. Якщо приймається алгоритм вставляння маскувальних символів: вставляється два маскувальні символи перед кожним символом ВТ і нуль маскувальних символів після символу ВТ при $\boldsymbol{\mu}$ = 3. В цьому випадку блок має такий вигляд : $\{m_i; m_i; v_i;\}$, де m_i – маскувальний символ, v_i – символ ВТ. Всі блоки матимуть такий вигляд, тому що кількість вставлених маскувальних символів, які припадають на один символ ВТ, дорівнює $\boldsymbol{\mu}$ -1. Варіантів, які визначають конфігурацію ВТ із маскувальними 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 [6].

За результатами дослідження запропоновано метод шифрування інформації із статичним включенням маскувальних символів. Метод оснований на статичній функції встановлення маскувальних символів, за якої маскувальні символи завжди вставляються у наперед визначені місця відносно символів відкритого тексту. Запропоновано метод шифрування інформації із динамічним включенням маскувальних символів. Метод оснований на динамічній функції встановлення маскувальних символів, коли їх вставляють за кількістю і позицією залежно від номера символу відкритого тексту, а їх кількість змінюватиметься на кожному етапі процедури вставляння. Динамічна функція вставляння маскувальних символів дає додатковий ефект. Якщо у звичайному шифрі Хілла 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 при **μ** = 5 період повторення буде 105 символів (взамін 5). Сама процедура вставляння маскувальних символів та їх вилучення є процедурою, яка суттєво не зменшує продуктивності роботи криптографічних засобів. При цьому доцільно врахувати, що маскувальні символи підбираються за допомогою генератора випадкових чисел з найменш вживаних символів у шифрованому тексі. 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 понад 50 %, то частотний розподіл символів у шифрованому тексті наближається до рівноймовірного. Відомий математик Клод Шеннон довів, що із наближенням розподілу частоти вживання символів у ШТ до рівноймовірного закону такий шифр наближається до абсолютно стійких шифрів [7]. Тобто, спосіб використання маскувальних символів [6] має перспективу для створення шифрів підвищеної стійкості.

Якщо раніше всю роботу з криптографії виконували вручну і було небажано збільшувати довжину ШТ, то за сьогоднішнього стану шифрувальної техніки ця особливість не є визначальною. При використанні шифрувальних машин, спеціалізованих приладів, комп'ютеризованих пристроїв чи комп'ютерів збільшення ШТ і видалення маскувальних символів виконуються дуже швидко і не зменшують продуктивності праці оператора при шифруванні чи дешифруванні інформації.

Висновки

Проведений аналіз ефективності та надійності найвідоміших блокових шифрів показав доцільність та можливість вдосконалення шифру Хілла. Доведено доцільність та перспективу застосування способу шифрування інформації, що використовує маскувальні символи, які встановлюються серед символів відкритого тексту (ВТ). Такі засоби ускладнюють процедуру розпізнавання ВТ при переборі можливих варіантів шифрів і переборі ключів для кожного шифра та приводять до підвищення крипостійкості системи. Запропоновано метод шифрування інформації із статичним включенням маскувальни символів. Запропоновано метод шифрування інформації із динамічним включенням маскувальни символів. Обгрунтовано високі показники надійності та ефективність запропонованих методів шифрування. Показано покращену ефективність методу шифрування інформації із динамічним включенням маскувальних символів.

1. Fred Cohen . A Short History of Cryptography // Introductory Information Protection. – 1987. – ISBN 1-878109-05-7. 2. Lester S. Hill . Cryptography in an Algebraic Alphabet. The American Mathematical Monthly. – 1929. 3. U.S. Patent 1 845 947. Лестер С. Хілл. Пристрій для шифрування. 1929. 4. Ємець В. Сучасна криптографія: основні поняття / В. Ємець, А. Мельник, Р. Попович. – Львів: БАК. – 2003. – 144 с. 5. Вербицький О.В. Вступ до криптології. – Львів, Видавництво науково-технічної літератури, 1998. ISBN 966-7148-03-3. 6. Ігнатович А. О., Іванців В. Р., Іванців Р.-А. Д., Павич Н. Я. Спосіб шифрування інформації. Патент України на корисну модель № 99073. Бюл. № 9 від 12.05.2015. 7. Shannon C. E. Communication Theory of Secrecy Systems // Bell System Technical Journal. – 1949.