УДК 681.3

АЛГОРИТМ ШИФРУВАННЯ ДАНИХ НА ОСНОВІ КЛІТИННИХ АВТОМАТІВ

Марценюк Є.О.[1)], Коваль В.В.[2)], Цімерман О.Р. [3)]
Тернопільський національний економічний університет
[1)] к.т.н., доцент; [2), 3)] магістрант

На сьогодні в інформаційному просторі, швидкими темпами впроваджуються новітні досягнення комп'ютерних і телекомунікаційних технологій. Комп'ютерні системи активно впроваджуються у фінансові, промислові, торгові і соціальні сфери. Внаслідок цього різко зріс інтерес широкого кола користувачів до проблем захисту інформації. В останні роки з розвитком комерційної і підприємницької діяльності збільшилося число спроб несанкціонованого доступу до конфіденційної інформації.

Серед всього спектру методів захисту даних від небажаного доступу особливе місце займають криптографічні методи [1-2]. Всі криптографічні засоби або алгоритми шифрування повинні бути стійким до атак щоб зловмисники не змогли розшифрувати дані.

Метою даної праці є розробка алгоритму, який дозволяє шифрувати відкриту інформацію.

Довжину повідомлення, яке потрібно зашифрувати обчислюється наступним чином:

$$f = \frac{(n-2)^2}{8} * c \qquad (1)$$

або

$$f - \frac{(n-4)^2}{8} = \frac{(n-2)^2}{8} * c\ , \qquad (2)$$

де n – довжина блоку; c – кількість блоків; f – довжина повідомлення.

Умова (1) виконується, коли можна підібрати таке поєднання довжини і кількості блоків, що повідомлення можна повністю розбити на такі блоки без залишку. В іншому випадку має виконуватися умова (2).

Кожному символу повідомлення ставиться у відповідність унікальне число:

- для режиму побітного шифрування: число, відповідне поточному символу, приводиться до двійкового вигляду і записується в поточні 8 клітин поля, а граничні клітини масиву залишаються недоторканими;
- для режиму побайтного шифрування: число, відповідне поточному символу, безпосередньо записується в поточну клітку масиву, а граничні клітини масиву залишаються недоторканими.

Запис шифротексту проводиться наступним чином:

- для режиму побітного шифрування: з масиву беруться значення восьми поточних клітин, потім ця послідовність приводиться до десяткового вигляду, а отримане число замінюється символом, який відповідає цьому числу, і записується в шифртекст, причому значення граничних кліток не беруться;
- для режиму побайтного шифрування: з масиву береться значення поточної клітини, отримане число замінюється символом, який відповідає цьому числу, і записується в шифротекст, причому значення граничних клітин не беруться.

Задачу шифрування повідомлення (1)-(2) запропоновано розв'язувати за допомогою алгоритму, основаному на клітинному автоматі який зображено на рисунку 1.

Висновок

Розроблено алгоритм шифрування повідомлень на основі клітинних автоматів, який відзначається високою стійкістю.

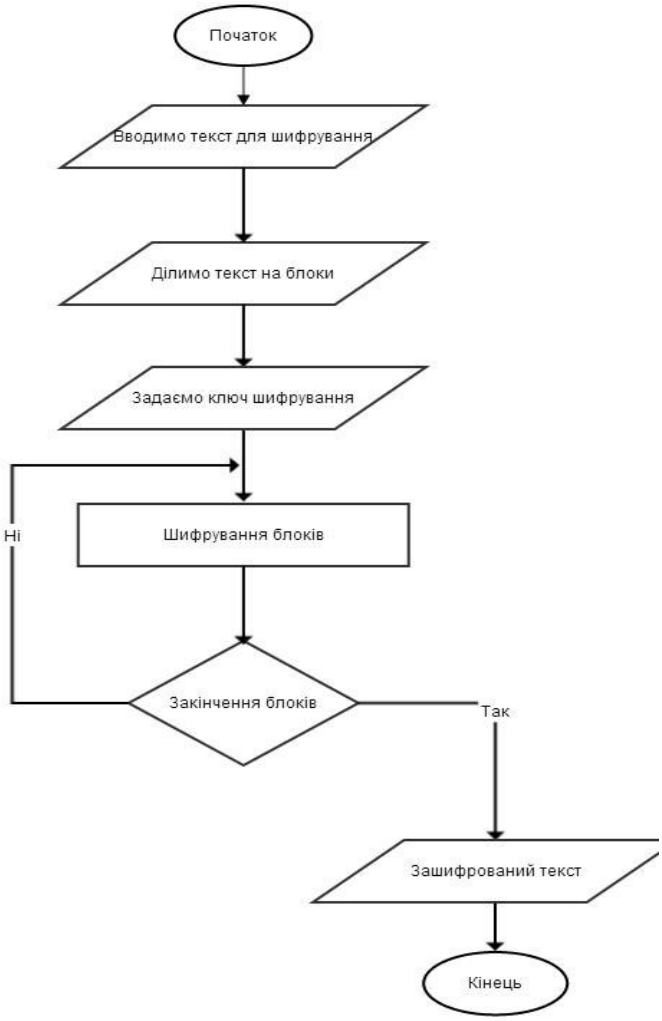

Рисунок 1 - Алгоритм шифрування повідомлень

Список використаних джерел

1. Брюс Шнайер. Прикладная криптография. – М.: Мир, 2005. –с.1204.
2. C-K. Yuen. Testing random number generators by Walsh transform. IEEE Trans. Computers,26(4):329–333, 1977.
3. Тоффоли Т., Марголус Н. «Машины клеточных автоматов» – М.: Мир 1991. –с.728.

УДК 004.056.5

ЗАСТОСУВАННЯ МЕТОДІВ МАШИННОГО НАВЧАННЯ ДЛЯ ВИЯВЛЕННЯ ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ У ВИСОКОНАВАНТАЖЕНИХ СИСТЕМАХ

Мєтєлєва Л.В.
Національний технічний університет України «Київський політехнічний інститут», студент

І. Постановка проблеми

Класифікація шкідливого програмного забезпечення та виявлення аномалій у бінарних файлах у високонавантажених системах має свої особливості порівняно з іншими комп’ютерними системами. Для високонавантажених систем є недопустимим виділення значних ресурсів для потокової перевірки виконуваних файлів антивірусом, запуску його у “пісочниці” чи для використання інших методів поведінкового аналізу.