УДК 681.3.06

ХОДАКОВ В.Є., ШЕХОВЦЕВ А.В., ПИЛИПЕНКО М.В., БАРАНЕНКО Р.В.,
Херсонський національний технічний університет

Ходаков Віктор Єгорович – д.т.н., проф., зав. кафедри інформаційних технологій Херсонського національного технічного університету. Коло наукових інтересів: нові інформаційні технології.

Шеховцев Анатолій Вікторович – к.т.н, доцент кафедри інформаційних технологій Херсонського національного технічного університету. Коло наукових інтересів: інформаційні технології в управлінні інфраструктурою міста, інформаційно-пошукові системи, програмні методи аналізу нестійких систем.

Пилипенко Микола Вадимович – к.т.н., доцент кафедри інформаційних технологій Херсонського національного технічного університету. Коло наукових інтересів: теплова пружна деформація, оптична обробка інформації, захист інформації.

Бараненко Роман Васильович – аспірант, асистент кафедри інформаційних технологій Херсонського національного технічного університету. Коло наукових інтересів: геоінформаційні та інформаційно-вимірювальні системи, захист інформації.

МАТЕМАТИЧНІ АСПЕКТИ ОБ'ЄМНОГО ШИФРУВАННЯ

Представлено аналіз факторів, що впливають на збільшення комп'ютерної злочинності у світі, розглянуті аспекти вирішення проблеми захисту інформації від несанкціонованого доступу і забезпечення конфіденційності даних і запропонований спосіб перетворення інформації і побудований на його основі криптографічний алгоритм, що володіє підвищеною криптостійкістю за рахунок просторового розподілу інформації і використання методів взаємодії з ключовими компонентами.

The analysis of the factors influencing increase of computer criminality in the world is submitted, the aspects of the decision of information protection problem are considered and the way of transformation of the information and the algorithm constructed on its basis are proposed.

Вступ та постановка проблеми. Одним з факторів прискорення науково-технічного прогресу є широке впровадження сучасних інформаційних технологій в освіту, транспорт, медицину й інші галузі, тим самим збільшуючи загальну інформатизацію країни.

Однак як свідчить практика інформатизації і її складової – комп'ютеризації країн, що знаходяться на шляху промислового розвитку, зростання антисоціальних явищ, зокрема комп'ютерної злочинності, є однією з характерних ознак, негативним дзеркальним відображенням постіндустріального інформаційного суспільства, глобальної інформаційної цивілізації [1].

У зв'язку зі стрімким зростанням кількості користувачів глобальної комп'ютерної мережі Internet та рівня комп'ютерної злочинності на перший план виходить *задача*

захисту інформації від несанкціонованого доступу і забезпечення конфіденційності даних.

Аналіз останніх досліджень. Відомо велике число загроз інформації, що можуть бути реалізовані як з боку зовнішніх, так і внутрішніх порушників [2].

Теоретичною базою для рішення проблеми захисту інформації від несанкціонованого доступу і забезпечення конфіденційності даних стали дослідження К. Шеннона [3] і У. Діффі і М. Хеллмана [4]. Пропозиція однобічної функції з потаємним ходом [5] значно просунуло вперед криптографію як засіб забезпечення конфіденційності даних і безпеки комп'ютерних систем.

Відомий спосіб перетворення вихідної інформації в шифрований текст методом Вернама [6, 7], у якому перетворення вихідної інформації, представленою заданою двійковою послідовністю, виконують побітовим додаванням за модулем 2 з набором двійкових ключів, а дешифрування у вихідну інформацію виконують побітовим додаванням за модулем 2 шифрованих текстів з набором тих же двійкових ключів.

Недоліком зазначеного способу є необхідність рівності довжини вихідної двійкової послідовності з довжиною набору двійкових ключів.

Цих недоліків позбавлений спосіб шифрування Віжинера [8], при якому, на підготовчому етапі, ключ кінцевої довжини $k=(k_0, k_1, ..., k_{n-1})$ продовжують до нескінченної послідовності, повторюючи ланцюжок, у результаті чого одержують робочий ключ $K=(k_0, k_1, ..., k_{n-1}, k_n, k_{n+1}, k_{n+2}, ...)$, при $K_j=k_{(j \bmod n)}$, $0 \le J < \infty$, а потім, на вирішальному етапі, перетворення вихідного тексту $Xf(x_0, x_1, ..., x_{n-1})$ у шифрований текст $Yf(y_0, y_1, ..., y_{n-1})$ виконують додаванням за модулем Z при рівній довжині вихідного тексту X і ключа K за формулою VIG: $(x_0, x_1, ..., x_{n-1}) \Rightarrow (y_0, y_1, ..., y_{n-1}) = [(x_0+k_0) \bmod Z, ..., (x_{n-1} + k_{n-1}) \bmod N]$, де, N — кількість символів в алфавіті; X — вихідний текст; K — робочий ключ; Y — шифрований текст; відновлення вихідного тексту виконують у зворотному порядку.

Недоліком даної системи шифрування є та обставина, що за короткий час методом перебору слів і фраз можна відновити ключ. Тому для одержання ключів повинні використовуватися програмні або апаратні засоби випадкової генерації ключів.

В останні роки на базі удосконалювання електронних технологій з'явилися нові теоретичні розробки в області квантової криптографії [9], засновані на принципах невизначеності Гейзенберга. В якості криптосистеми з відкритим ключем був запропонований алгоритм Ель Гамаля [10], розроблені алгоритми захисту інформації, описані в роботах [11-26].

Однак проблема розробки нових методів, способів і алгоритмів, що володіють підвищеної криптостійкістю, залишається актуальної і сьогодні.

Ціль статті. Метою роботи є розробка способу перетворення інформації і на його основі криптографічного алгоритму, що володіє високим коефіцієнтом стійкості до криптоаналізу для побудови програмно-апаратних систем обробки інформації, її захисту від несанкціонованого доступу і забезпечення конфіденційності даних.

Основний матеріал. В даний час захист інформації і забезпечення конфіденційності даних є невід'ємними складовими загальної системи безпеки комерційної фірми або державної установи. За оцінками експертів [27] сума втрат в результаті різного роду шахрайства в сфері банківських послуг і фінансових операцій, проведених з використанням глобальної мережі, виросла від 800 млн. дол. у 1984 р. до 100 млрд. дол. у 1997.

Проаналізувавши методику здійснення комп'ютерних злочинів, можна впевнено стверджувати, що сучасна комп'ютерна злочинність найбільш часто використовує такі способи здійснення злочинів [1]:

– пошук недоліків у захисті комп'ютерних систем і несанкціонований доступ до них;

– приховане підключення комп'ютера злочинця до комп'ютерної мережі організації або до мереж окремих користувачів.

Тому для забезпечення надійного захисту інформації і конфіденційності даних рекомендується використовувати криптографічні системи захисту інформації, оскільки в деяких випадках криптографічний захист є єдиним засобом уникнути небажаного витоку інформації [28].

Однак такі системи повинні задовольняти наступним вимогам [8]:

1) зашифроване повідомлення повинне читатися тільки при наявності ключа;

2) число операцій, необхідних для визначення заданого ключа шифрування по фрагменту шифрованого повідомлення і відповідного йому відкритого тексту повинне бути не менш загального числа можливих ключів;

3) число операцій, необхідних для розшифрування інформації шляхом перебору різних ключів, повинне мати точну нижню границю оцінки (інфініум) і перевищувати можливості обчислення на сучасних комп'ютерах;

4) знання алгоритму шифрування не повинне впливати на надійність захисту;

5) незначна зміна ключа повинна приводити до істотної зміни зашифрованого тексту, навіть при використанні того самого ключа;

6) структурні елементи алгоритму шифрування повинні бути незмінними;

7) додаткові біти, що вводяться до повідомлення в процесі шифрування, повинні бути надійно сховані в шифрованому тексті;

8) довжина зашифрованого тексту повинна бути більше вихідного тексту;

9) будь-який ключ з даної множини повинний забезпечувати надійний захист при шифруванні;

10) алгоритм повинний допускати програмну й апаратну реалізацію (зміна довжини ключа не повинна вести до якісного погіршення шифрування).

Відомо, що стійкість алгоритму шифрування, практично в геометричній прогресії, залежить від довжини використовуваного ключа. При цьому алгоритми шифрування з симетричним ключем вимагають істотно більш короткого ключа для забезпечення аналогічної стійкості, у порівнянні з алгоритмами шифрування з відкритим ключем. Так, наприклад, алгоритм DES з використанням ключа довжиною 40 біт забезпечує приблизно ту ж надійність, що й алгоритм RSA з використанням 512-бітного ключа. Швидкість виконання операцій шифрування/розшифровки, у свою чергу, прямо залежить від довжини використовуваного ключа і розміру інформаційного фрагмента, що шифрується. Таким чином, алгоритм із використанням симетричного ключа забезпечує набагато більш високу швидкодію процедур шифрування/ розшифровки при тій же надійності, у порівняння з алгоритмами з використанням відкритого ключа [29].

У свою чергу алгоритми з відкритим ключем забезпечують набагато більш високий ступінь таємності ключів, тому що закритий ключ одержувача інформації взагалі ніколи не залишає його персонального інформаційного архіву. У зв'язку з цим, на практиці, при шифруванні персональної інформації використовуються алгоритми із симетричним ключем, а при шифруванні розповсюджуваної інформації комбінація обох алгоритмів.

З огляду на всі перераховані вище вимоги й обмеження, авторами був розроблений спосіб перетворення інформації і на його основі криптоалгоритм, у якому інформація представляється заданою послідовністю цифр або чисел у код, де та ж інформація представлена цифрами або числами, відмінними від заданої за допомогою кодування за допомогою кодового слова, вираженого цифрами або числами.

Найбільш близьким за технічною сутністю є спосіб перетворення вихідної інформації в шифрований текст методом гамування [8], у якому, на підготовчому етапі, генерують гаму ключа, що, на вирішальному етапі, накладають на вихідну інформацію за заданим законом, наприклад, використовуючи побітове додавання за модулем 2. Зворотнє перетворення для одержання вихідного тексту виконують повторним генеруванням гами ключа, що накладають на перетворену інформацію з тим же законом.

Недоліком зазначеного способу є можливість виявлення повторюваного фрагмента ключа існуючими методами криптоаналізу, що дозволить встановити цілком весь ключ, і, потім дешифруванням відновити вихідну інформацію.

Зазначений недолік усувається тим, що в способі перетворення інформації на підготовчому етапі з бітових елементів вихідної інформації і ключа дискретно формують масиви у виді тривимірних геометричних об'єктів $V_1 = \begin{cases} x = (x_1, x_2, ..., x_g) \\ y = (y_1, y_2, ..., y_h) \\ z = (z_1, z_2, ..., z_k) \end{cases}$ і $V_2 = \begin{cases} x' = (x_1, x_2, ..., x_m) \\ y' = (y_1, y_2, ..., y_q) \\ z' = (z_1, z_2, ..., z_r) \end{cases}$, відповідно, кожний з яких, принаймні, один, із заданою дискретною орієнтацією в тривимірному просторі, причому всі елементи з дійсними значеннями просторового розподілу в системах координат, тобто $\forall i \in \{0, 1, 2, ..., \omega\};\ \omega \to \max\{g, h, k, m, q, r\}$, додатково містять проміжний етап, що передує вирішальному етапові — операції взаємодії між бітовими елементами зазначених тривимірних геометричних об'єктів. На зазначеному проміжному етапі виконується керована дискретна зміна форми тривимірних геометричних об'єктів, їхніх напрямків орієнтації в тривимірній системі координат і/або їхнє обертання, з можливістю керованого незалежного дискретного обертання кожного з зазначених тривимірних об'єктів навколо вершини осі координат одного з елементів зазначених об'єктів, наприклад, $V_{1,2} = \prod_{i=1}^{3} A_{x_i, y_i, z_i}$, де, A_{x_i} — матриця значень місця розташування об'єкта щодо осі x; A_{y_i} — матриця значень місця розташування об'єкта щодо осі y; A_{z_i} — матриця значень місця розташування об'єкта щодо осі z, з можливістю керованого незалежного дискретного обертання систем координат зазначених об'єктів і з можливістю керованої дискретної просторової зміни кроку переміщення і взаємодії їхніх елементів.

Керування дискретною зміною кроку виконують за додатковим параметром періодичності, наприклад, $v_{1,2}(\forall l \in \tau_{x_i, y_i, z_i})$, де, l — крок; τ — параметр періодичності; причому $\forall i \in \overline{\{1; n\}}$, при цьому $\forall v_{1,2} \in V_{1,2}$. Керування незалежним дискретним обертанням кожного з зазначених тривимірних об'єктів навколо осі координат виконують за додатковим параметром періодичності, наприклад, $V_{1,2} = \begin{cases} x = \forall x \subset (\tau_x, \pm s\psi) \\ y = \forall y \in (\tau_y, \pm s\psi) \\ z = \forall z \in (\tau_z, \pm s\psi) \end{cases}$ де, ψ — кут обертання об'єкта; s — керований показник величини кута обертання при його дійсних значеннях, тобто, $s \in (0, 1, 2, ..., u)$; τ — параметр періодичності.

Можливість керованого незалежного дискретного обертання деяких елементів тривимірних об'єктів навколо вершини осі координат одного з елементів зазначених об'єктів за параметром періодичності, визначається: $\Diamond \exists v_{1,2} = \prod_{i=1}^{3} A_{x_i, y_i, z_i} \forall (x_i, y_i, z_i) \in (\tau_{x_i, y_i, z_i} \pm s\psi)$, де, $s \in (0, 1, 2, ..., u)$, і $\forall v_{1,2} \in V_{1,2}$. Дискретність значення кута обертання дорівнює, принаймні, $90°$, тобто, $\psi = \frac{\pi}{2}$.

Зміну форми зазначених об'єктів виконують методом керованих перестановок π або їх об'єднанням, наприклад,

$$\pi_{n/m}(i, V) \left(\{1, 2, ..., n\} \times GF(2)^m \to \{1, 2, ..., n\}\right), \quad (1)$$

що являє собою об'єднання 2^m перестановок $\pi_V = \pi^{(j)} \in S_n$, якщо для кожного фіксованого значення $V \in GF(2)^m$ задана деяка перестановка $\pi_V = \pi^{(\alpha(V))} \in S_n$, така, що $\pi_{n/m}(i, V) = \pi_V(i) = \pi^{(\alpha(V))}(i)$ [29].

Керовану дискретну зміну форми зазначених об'єктів виконують за формулою ангармонійного коливання, що є результатом накладення (суперпозиції) двох гармонійних коливань $x_1 = A_1 \cos(\omega_1 t + \varphi_1)$ і $x_2 = A_1 \cos(\omega_2 t + \varphi_2)$, що мають різні частоти й амплітуди, де $x(t)$ — періодична функція часу; A — максимальна амплітуда коливання; φ_i — фаза коливання; $\omega = \frac{2\pi}{T} = 2\pi\nu$ — кругова або циклічна частота [30]. Результуюче негармонійне коливання буде мати наступний вигляд:

$$x = x_1 + x_2 = A(t)\cos[\omega_1 t + \varphi(t)], \quad (2)$$

де

$$A^2(t) = A_1^2 + A_2^2 + 2A_1A_2\cos[\psi(t) - \varphi_1], \quad (3)$$

$$tg\varphi(t) = \frac{A_1 \sin\varphi_1 + A_2 \sin\psi(t)}{A_1 \cos\varphi_1 + A_2 \cos\psi(t)} \quad (4)$$

і

$$\psi(t) = (\omega_2 - \omega_1)t + \varphi_2. \quad (5)$$

Таким чином, у пропонованого способу з'являється властивість, що дозволяє за рахунок просторового розподілу інформації і методів взаємодії з ключовими компонентами, виконувати перетворення інформації, цілісність якої буде надійно захищена, оскільки криптоаналітичні методи досить успішно справляються тільки з такими структурами, які можна умовно назвати "лінійними", що не мають під собою математичної властивості, і розміщують елементи повідомлення, витягаючи їх в одну лінію.

Програмна реалізація даного алгоритму представлена в [31].

Висновки. Запропонований спосіб перетворення інформації і побудований на його основі криптографічний алгоритм, що володіє підвищеної криптостійкістю за рахунок просторового розподілу інформації і використання методів взаємодії з ключовими компонентами, дозволяє надійно захищати інформацію від несанкціонованого доступу, що забезпечує дієве рішення поставленої задачі.

Література

1. Кульбач С.О. Характеристика сучасної комп'ютерної злочинності // Матеріали VI Міжнародної науково-практичної конференції "Наука і освіта '2003". Том 30. – Дніпропетровськ: Наука і освіта, 2003, С. 44-45.
2. Герасименко В.А. Защита информации в автоматизированных системах обработки даннях. В 2-х кн. – М.: Энергоатомиздат, 1994. – 576 с.
3. Shannon C.E. Communication Theory of Secrecy Systems //Bell Systems Technical Journal. – 1949. – V.28. – P. 656-715.
4. Diffie W., Hellman M.E. New Directions in Cryptography //IEEE Transactions on Information Theory. – 1976. – V. IT – 22. ¹6. – P. 644-654.
5. Rivest R., Shamir A., Adleman L. A method for Obtaining Digital Signatures and Public-Key Cryptosystems // Communication of the ACM. – 1978. – V.21. – ¹2. – P. 120-126.
6. Защита программного обеспечения: Пер. с англ. / Д.Гроувер, Р.Сатер, Дж.Фипс и др. / Под редакцией Д.Гроувера. – М.: Мир, 1992. – С. 100-103.
7. Соколов А.В., Степанюк О.М. Методы информационной защиты объектов и компьютерных сетей. – М.: ООО "Фирма "Издательство АСТ"; СПб.: ООО "Издательство "Полигон", 2000. – ("Шпионские штучки"). – С. 209-210.
8. Гундарь К.Ю., Гундарь А.Ю., Янишевский Д.А. Защита информации в компьютерных системах. – К.: "Корнейчук", 2000.
9. Benett C.H., Brassard G. Quantum Cryptography: Public Key Distribution and Coin Tossing // Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing // Banjalore, India. – 1984. – P. 175-179.
10. El Gamal T. A public key cryptosystem and a signature scheme based on discrete logarithms //IEEE Transactions on Information Theory. – 1985. – V. IT. – 31. № 4. – P. 469-472.
11. Белкин Т.Г., Гуц Н.Д., Молдовян А.А., Молдовян Н.А. Способ скоростного шифрования на базе управляемых операций. Управляющие системы и машины. – 1999. – № 6. – С. 78-87.
12. Биленко Ю.А., Жуков А.Е. Криптографические свойства преобразований, легко реализуемых на стандартных PC-процессорах // Безопасность информационных технологий. – 2000. – № 2. – С. 40-49.
13. Бодров А.В., Молдовян Н.А., Молдовяну П.А. Оптимизация механизма управления перестановки в скоростных шифрах// Вопросы защиты информации. – 2002. – № 1. – С. 44-50.
14. Винокуров А.Ю., Применко Э.А. Анализ тенденции подходов к синтезу симметричных блочных шифров // Безопасность информационных технологий. – 2001. – № 2. – С. 5-14.
15. Гуц Н.Д., Еремеев М.А., Молдовян А.А. Алгоритм формирования расширенного ключа на основе блоков управляемых перестановок // Вопросы защиты информации. – 2001. – № 3. – С. 41-46.
16. Гуц Н.Д., Изотов Б.В., Молдовян А.А., Молдовян Н.А. Проектирование двухместных управляемых операций для скоростных гибких криптосистем // Безопасность информационных технологий. – 2001. – № 2. – С. 14-23.
17. Гуц Н.Д., Изотов Б.В., Молдовян Н.А. Скоростной алгоритм шифрования SPECTR-H64 // Безопасность информационных технологий. – 2000. – № 4. – С. 37-50.
18. Гуц Н.Д., Изотов Б.В., Молдовян Н.А. Управляемые перестановки с симметричной структурой в блочных шифрах// Вопросы защиты информации. – 2000. – № 4. – С. 57-65.
19. Гуц Н.Д., Молдовян А.А., Молдовян Н.А. Гибкие аппаратно-ориентированные шифры на базе управляемых сумматоров // Вопросы защиты информации. – 2000. – № 1. – С. 8-15.
20. Иванов М.А. Криптографические методы защиты информации в компьютерных системах и сетях. – М.: КУДИЦ-ОБРАЗ, 2001. – 368 с.
21. Изотов Б.В., Молдовян А.А., Молдовян Н.А. Скоростные методы защиты информации в АСУ на базе управляемых операций // Автоматика и телемеханика. – 2001. – № 6. – С. 168-184.
22. Молдовян А.А., Молдовян Н.А. Вероятностные механизмы в недетерминированных блочных шифрах // Безопасность информационных технологий. – 1997. – №3. – С. 58-61.
23. Молдовян А.А., Молдовян Н.А. Метод скоростного преобразования для защиты информации в АСУ // Автоматика и телемеханика. – 2000. – №4. – С. 151-165.
24. Молдовян А.А., Молдовян Н.А., Молдовяну П.А. Новый метод криптографических преобразований для современных систем защиты ПЭВМ // Управляющие системы и машины. – Киев. – 1992. – № 9/10. – С. 44-50.
25. Молдовян А.А., Молдовян Н.А. Псевдовероятностные скоростные блочные шифры для программной реализации. Кибернетика и системный анализ. – Киев. – 1997. – №4. – С. 133-141.
26. Молдовян А.А., Молдовян Н.А. Скоростные шифры на базе нового криптографического примитива // Безопасность информационных технологий. – 1999. – №1, – С. 82-88.
27. Соколов А.В., Степанюк О.М. Защита от компьютерного терроризма. Справочное пособие. – СПб.: БХВ – Петербург; Арлит, 2002. – С. 11.
28. У. Диффи, М.Э. Хеллман Защищенность и имитостойкость: Введение в криптографию // ТИИЭР. – 1979. – Т. 67. – № 3. – С. 71-103.
29. Молдовян А.А., Молдовян Н.А., Гуц Н.Д., Изотов Б.В. Криптография: скоростные шифры. – СПб.: БХВ-Петербург, 2002. – С. 168.
30. Яворский Б.М., Детлаф А.А. Справочник по физике (для инженеров и студентов вузов). – Изд. седьмое, испр. – М.: Наука, Главная редакция физико-математической литературы, 1977. – С. 109-113.
31. Свідоцтво про реєстрацію авторського права на твір №12097, "Комп'ютерна програма криптографічного перетворення інформації "Wonderful key "Wolkey". Автори: Граб М.В., Пилипенко М.В., Бараненко Р.В., Цивільський Ф.М., Шаганян С.М., Lunegov Maksim. Опубл. 24.01.2005, Бюл. №1.