УДК 004.056.55

Євгеній Володимирович ПРОКОПЕНКО,
кандидат технічних наук, доцент, доцент кафедри зв'язку, автоматизації та захисту інформації Національної академії Державної прикордонної служби України імені Богдана Хмельницького, м. Хмельницький

Андрій Володимирович БІЖИК,
слухач факультету підготовки керівних кадрів Національної академії Державної прикордонної служби України імені Богдана Хмельницького, м. Хмельницький

КРИПТОГРАФІЧНІ МЕТОДИ ЗАБЕЗПЕЧЕННЯ КОНФІДЕНЦІЙНОСТІ ІНФОРМАЦІЇ

У статті досліджуються питання забезпечення конфіденційності інформації за допомогою застосування криптографічних методів захисту. Одним зі шляхів створення загроз конфіденційності інформації з боку порушників є використання недостатньо високої криптографічної стійкості застосованого перетворення і отримання ключів або механізмів перетворення шляхом здійснення криптографічного аналізу фрагмента відкритого тексту певної довжини та фрагмента закритого тексту, який є відповідним відкритому. У статті розглядаються деякі можливі аспекти криптографічного аналізу шифру підстановки та шляхи підвищення його криптографічної стійкості.

Ключові слова: *криптографічний аналіз, ключ, шифр підстановки, шифр перестановки, радіообмін, шифрування.*

© Прокопенко Є. В., Біжик А. В.

Постановка проблеми у загальному вигляді. Досвід проведення антитерористичної операції на східному кордоні України підкреслює важливість забезпечення своєчасного та достовірного інформаційного обміну в системі управління. При цьому досягнення мети бойових дій напряму залежить від оперативності та прихованості в доведенні управлінських рішень. Основним, а найчастіше і єдиним способом організації зв'язку є радіозв'язок. Застосування противником засобів радіоелектронної боротьби та радіорозвідки спонукає до впровадження сучасних способів і методів протидії. І саме криптографічні методи захисту можуть задовольнити вимогу забезпечення конфіденційності інформації під час доведення наказів і розпоряджень у тактичній ланці управління.

Аналіз останніх досліджень і публікацій, в яких започатковано вирішення даної проблеми та на які опирається автор. Аналіз останніх публікацій провідних вчених з питань інформаційної безпеки показав, що проблему застосування криптографічних методів захисту інформації досліджують А. Крижний, Т. Гурський, Ю. Яремчук, О. Корченко, О. Фаль та інші.

При цьому необхідно визнати, що впровадження криптографічних алгоритмів при веденні інформаційного обміну з використанням радіозасобів потребує подальшого більш глибокого дослідження та впровадження в першу чергу в діяльність оперативно-бойових прикордонних підрозділів.

Виклад основного матеріалу дослідження. Однією із вкрай важливих у сучасних умовах ведення бойових дій у зоні проведення АТО є проблема забезпечення конфіденційності інформації [1; 2], для вирішення якої застосовуються ті чи інші методи, методики чи алгоритми. Для забезпечення саме конфіденційності інформації криптографічне перетворення є чи не єдиним рішенням з певною стійкістю до спроб розкриття її змісту – криптографічною стійкістю. На цей час теорія криптографічних перетворень розвинута досить широко й для забезпечення конфіденційності інформаційних повідомлень можна застосувати ті чи інші алгоритми криптографічного перетворення [4]. У даній статті пропонуємо розглянути алгоритми крипто-

графічного перетворення підстановки. Даний метод застосовується в ході ведення радіотелефонного обміну при формуванні радіограм посадовими особами Держприкордонслужби. На сьогодні найбільш простий метод перетворення, оснований на заміні символів вихідного тексту на інші, того ж алфавіту, але за складнішим правилом. Для забезпечення високої крипостійкості потребує використання великих ключових послідовностей.

Мета статті – провести дослідження застосування криптографічних методів перетворення інформаційних повідомлень при веденні радіотелефонного обміну.

Виклад основного матеріалу дослідження. Початкове завдання криптографії полягає в розробленні методів, спрямованих на приховування змісту переданої або збереженої інформації. І хоча на сьогодні сфера застосування криптографічних механізмів значно розширилася, основні ідеї можна проілюструвати саме на прикладі забезпечення конфіденційності інформації. Очевидно, що властивість конфіденційності досягається тоді, коли з перетвореного відкритого тексту, тобто криптограми, не можна дізнатись про зміст цього тексту, а несанкціоновані користувачі не зможуть здійснити обернене перетворення з криптограми у відкритий текст. Розглянемо класичну криптосистему, яка застосовується при формуванні радіограм – шифр підстановки [3].

Підстановкою x в алфавіті Z_m називається автоморфізм Z_m, при якому букви вихідного тексту t замінені буквами шифрованого тексту $x(t)$:

$$Z_m \rightarrow Z_m;\ x\colon t \rightarrow x(t). \qquad (1)$$

Набір усіх підстановок називається симетричною групою $S(Z_m)$.

Можна стверджувати, що $S(Z_m)$ при добутку є групою операцій, яким притаманні такі властивості:

замкнутість: добуток підстановок x_1x_2 є підстановкою:

$$x\colon t \rightarrow x_1(x_2(t)), \qquad (2)$$

асоціативність: результат добутку $x_1\ x_2\ x_3$ не залежить від порядку розстановки дужок:

$$(x_1x_2)x_3 = x_1(x_2x_3). \qquad (3)$$

Існування нейтрального елемента: підстановка i, визначається як $i(t) = t$, $0 \le t < m$ є нейтральним елементом $S(Zm)$ по добутку: $ix = xi$ для $x \in S(Zm)$.

Існування зворотного: для будь-якої підстановки x існує тільки одна зворотна підстановка x^{-1}, що задовольняє вираз:

$$xx^{-1} = x^{-1}x = i. \quad (4)$$

Число можливих підстановок у симетричній групі Z_m називається *порядком* $S(Z_m)$ і дорівнює $n!$.

У свою чергу ключем підстановки k для Z_m називається послідовність елементів симетричної групи Z_m:

$$k = (p_0, p_1, ..., p_{n-1}, ...), p_n \in S(Z_m), 0 \le n < \infty. \quad (5)$$

Підстановка, що визначається ключем k, є криптографічним перетворенням T_k, за допомогою якого здійснюється перетворення послідовності n вихідного тексту $(x_0, x_1, ..., x_{n-1})$ в послідовність n шифрованого тексту $(y_0, y_1, ..., y_{n-1})$:

$$y_i = p(x_i), 0 \le i < n, \quad (6)$$

де n – довільне ($n = 1, 2, ...$).

Криптографічне перетворення T_k буде моноалфавітною підстановкою, якщо p незмінне при будь-якому i, $i = 0, 1, ...$, в іншому випадку T_k називається поліалфавітною підстановкою.

Слід підкреслити, що до найбільш притаманних особливостей підстановки T_k можна віднести таке:

символи вихідного повідомлення шифруються окремо. Шифрування n-послідовності $(x_0, x_1, ..., x_{n-1})$ і його префікса $(x_0, x_1, ..., x_{s-1})$ зв'язані співвідношенням:

$$T_k(x_0, x_1, ..., x_{n-1}) = (y_0, y_1, ..., y_{n-1}), \quad (7)$$
$$T_k(x_0, x_1, ..., x_{s-1}) = (y_0, y_1, ..., y_{s-1})$$

буква шифрованого тексту y_i є функцією тільки i-ї компоненти ключа p_i і i-ї букви висхідного тексту x_i.

При своїй простоті система має істотні вади: статистика символів відкритого тексту зберігається на множині символів зашифрованого тексту, що дає можливість здійснити напад за допомогою частотного аналізу тих або інших символів, які трапляються в зашифрованому тексті; символ відкритого тесту перетворюється в той самий символ зашифрованого тексту незалежно від його місця розташування у повідомленні. Це позначається на збереженні статистики не тільки окремих символів, а і біграм, триграм.

Слабкість крипостійкості моноалфавітних підстановок можна подолати з використанням поліалфавітних підстановок.

Поліалфавітна підстановка визначається ключем $x = (x_1, x_2, \dots x_n)$, який має не менше двох різноманітних підстановок. Для початку розглянемо поліалфавітні системи підстановок з нульовим початковим зміщенням [5].

Нехай $\{K_i: 0 \le i < n\}$– незалежні випадкові змінні з однаковим розподіленням вірогідностей, які набувають значення із множини Z_m:

$$Pкл\ \{(K_0, K_1, \dots, K_{n-1}) = (k_0, k_1, \dots, k_{n-1})\} = (1/m)^n. \quad (8)$$

Система одноразового використання перетворює первинний текст:

$$X = (X_0, x_1, \dots, x_{n-1}) \quad (9)$$

в шифрований текст:

$$Y = (Y_0, y_1, \dots, y_{n-1}) \quad (10)$$

за допомогою підстановки Цезаря [5]:

$$Y_i = C_{Ki}(x_i) = (K_i + X_i)\ (mod\ m) \qquad i = 0 \dots n-1. \quad (11)$$

Для такої системи підстановки використовують термін “одноразовий блокнот”. Простір ключів K системи одноразової підстановки є вектором рангів $(K_0, K_1, \dots, K_{n-1})$ і містить m^n точок. При цьому ключ повинен володіти трьома критично важливими властивостями: бути справді випадковим; збігатися розміром із заданим відкритим текстом; застосовуватися тільки один раз.

Накладення білого шуму у вигляді нескінченного ключа на вихідний текст змінює статистичні характеристики мови джерела. Системи

одноразового використання теоретично неможливо розшифрувати, оскільки вони не містять достатньої інформації для відновлення тексту. Для роботи шифру поліалфавітної підстановки необхідна дійсно випадкова послідовність нулів та одиниць (ключ). За визначенням, послідовність, отримана з використанням будь-якого алгоритму, є не зовсім випадковою, а псевдовипадковою. Незважаючи на проблематику генерування випадкових ключів, криптосистеми поліалфавітної підстановки є досить надійними. Тобто, потрібно отримати випадкову неалгоритмічну послідовність, а саме: радіоактивний розпад ядер; створений електронним генератором білий шум або інші досить випадкові події, що можуть вирішити дану проблематику.

Висновки. На сьогодні криптографічні механізми настільки тісно пов'язані із сучасними технологіями, способами і методами обміну інформацією, що поряд із підвищенням вимог до автоматизації систем управління необхідно підвищувати вимоги до інформаційної безпеки. Із вищезазначеного випливає, що обчислювальну стійкість криптосистем необхідно постійно досліджувати, обов'язково беручи до уваги розвиток сучасних інформаційних технологій і тенденції розроблення ефективних обчислювальних алгоритмів.

Перспективи подальших розвідок у даному напрямі. Створення перспективної системи зв'язку та управління передбачається: у переході до інтеграції основних інформаційних процесів на полі бою в уніфікованих багатофункціональних терміналах як для організації телекомунікацій, так і для дистанційного управління зброєю; значному підвищенні вимог до забезпечення прихованого управління засобами радіозв'язку тактичної ланки управління; створенні багаторівневої системи забезпечення інформаційної безпеки та конвергенції різних за природою мереж і служб електрозв'язку по єдиних цифрових каналах зв'язку на основі впровадження новітніх інформаційних технологій.

Список використаної літератури

1. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України.

2. Про електронний цифровий підпис : Закон України.

3. Фаль О. М. Криптографія: основні ідеї та застосування / О. М. Фаль. – К. : ІВЦ Видавництво "Політехніка", 2003. – 28 с.

4. Бабак В. П. Теоретичні основи захисту інформації : підручник // Бабак В. П. – Книжкове видавництво НАУ, 2008. – 752 с.

5. Кузьминов В. И. Криптографические методы защиты информации / В. И. Кузьминов. – Новосибирск : Высшая школа, 1998.

Рецензент – кандидат технічних наук, доцент Рачок Р. В.

Стаття надійшла до редакції 06.05.2015.

Прокопенко Е. В., Бижик А. В. **Криптографические методы обеспечения конфиденциальности информации**

В статье исследуются вопросы обеспечения конфиденциальности информации с помощью применения криптографических методов защиты. Одним из путей создания угроз конфиденциальности информации со стороны нарушителей является использование недостаточно высокой криптографической стойкости примененного преобразования и получения ключей или механизмов преобразования путем осуществления криптографического анализа фрагмента открытого текста определенной длины и фрагмента закрытого текста, который является подходящим открытому. В статье рассматриваются некоторые возможные аспекты криптографического анализа шифра подстановки и пути повышения его криптографической стойкости.

Ключевые слова: *криптографический анализ, ключ, шифр подстановки, шифр перестановки, радиообмен, шифрование.*

ProkopenkoY. V., Bigyk A. V. **Cryptographic methods to ensure privacy of information**

The experience of the counterterrorist operation on the eastern border of Ukraine underlines the importance of providing timely and reliable exchange of information in the management system. This achievement of the objective of fighting depends on the speed and secrecy of evidence making. The main, and often the only way to organize communication is radio communication. Applying by enemy a means of electronic warfare and radio interception, encourages the introduction of modern methods and countermeasures.

And that cryptographic methods of protection techniques could satisfy the requirement to ensure the confidentiality of information during the proof of orders and instructions in the tactical control link.

The initial task of cryptography is developing methods aimed at concealing the content transmitted or stored information. Although today the scope of cryptographic mechanisms has expanded, the basic idea can be illustrated by the example is privacy information. Obviously, the privacy feature is achieved when converted from plaintext, namely cryptograms, no one can learn about the content of the text, and unauthorized users can not make the inverse conversion from cryptograms in plaintext. In the article the classic cryptographic system, which is used in the formation of radio – code substitution.

It is noted that today cryptographic mechanisms are so closely related to modern technologies, ways and methods of information exchange of information, along with increased requirements for automation control systems necessary to increase the requirements for information security. From the above it follows that the computational stability of cryptosystems must constantly explore, always taking into account the development of modern information technology trends and developing efficient computational algorithms.

Prospects for further research in this area aimed at establishing a modern communications and management and provides a transition to integrate information processes main battlefield in uniform multifunctional terminals for both telecommunications organizations and for remote control of weapon. Also, a significant increase in the requirements for providing covert control radio communication tactical management level. Creating of a multi-level information security and convergence of different networks by nature and telecommunication services at uniform digital channels through the introduction of new information technologies.

Keywords: *cryptanalysis, key, substitution cipher, transposition cipher, radio communications, encryption.*