Системы телекоммуникации, связи и защиты информации

УДК 004.056.55

І.О. Розломій

Черкаський національний університет імені Богдана Хмельницького,

б-р Шевченка, 81, корпус 3, м.Черкаси, 18000, Україна.

Дослідження структури і криптографічної стійкості модифікації шифру гамування

Стаття присвячена проблемі забезпечення інформаційної безпеки електронних документів (ЕД). Особлива увага зосереджена на криптографічних алгоритмах шифрування, оскільки вони залишаються основним механізмом забезпечення конфіденційності документів. В статті розглянуті базові вимоги до розробки криптографічних систем захисту ЕД. Запропонований вдосконалений метод шифру гамування, який враховує недоліки існуючих алгоритмів. Шифрування запропонованим методом покращене шляхом зміни ключової послідовності з кожним блоком інформації. В результаті, побудовано схему процесу шифрування модифікованим шифром гамування. Визначено критерії, що впливають на криптографічну стійкість шифрування. Досліджено криптографічну стійкість системи захисту ЕД побудованої на основі запропонованого методу. Використання даної модифікації шифру дозволить підвищити ефективність захисту ЕД. Бібл. 13, рис. 4.

Ключові слова: *шифр гамування, криптостійкість, криптоаналіз, псевдовипадкові числа, сума за модулем.*

Вступ

В наш час однією з проблем, з якою доводиться стикатися при обробці інформації є проблема забезпечення інформаційної безпеки (ІБ). В той же час дана проблема є досить актуальною, наукоємною і складною для її практичного вирішення. Все більшого значення набувають методи криптографічного шифрування та цифрова безпека. Використання засобів захисту поступово впроваджується, як процес обробки інформації. Процес криптографічного перетворення даних використовується в системах захисту, засобах захисту від несанкціонованого доступу, електронного цифрового підпису, захисту мережевого трафіку. Криптографічні алгоритми перетворення інформації стають одними з основних і найефективніших засобів забезпечення захищеності інформаційних ресурсів. Проте, існуючі алгоритми шифрування не володіють ідеальними якостями: абсолютною стійкістю до криптоаналізу і зручністю використання в більшості випадків [1].

Постановка проблеми

В умовах розвитку інформаційних технологій з'являються нові вимоги щодо побудови систем захисту інформації і забезпечення інформаційної безпеки по відкритим каналам зв'язку. Постійний науково-технічний прогрес в області інформаційних технологій, зокрема в галузі захисту інформації, потребує розробки нових методів для підвищення швидкодії і стійкості криптографічних алгоритмів.

Аналіз останніх досліджень та публікацій

В ході дослідження літератури було проаналізовано цілий ряд існуючих механізмів забезпечення інформаційної безпеки електронних документів (ЕД). Як показує аналіз, більшість методів захисту інформаційних ресурсів, зокрема ЕД базуються на засобах криптографії. На сьогодні відомі праці [2-4], в яких описано моделі захисту інформації, показники безпеки шифрів, способи оцінки і підвищення криптографічної стійкості. Проте, основна маса запропонованих методик не здатна в повній мірі забезпечити належний рівень ІБ.

Виділення невирішених раніше частин загальної проблеми

Актуальність проблеми зумовлена швидкими темпами розвитку систем шифрування, який супроводжується розвитком засобів їх розкриття. Необхідність підвищення швидкодії і продуктивності криптографічних алгоритмів вимагає застосування нових методів. На даному етапі розвитку інформаційних технологій слабо розроблені швидкодіючі криптостійкі алгоритми.

© Розломій І.О., 2016

Для вирішення даної проблеми досліджується можливість використання вдосконаленого шифру гамування.

Формулювання мети дослідження

Мета роботи полягає в підвищенні криптостійкості вдосконаленого алгоритму шифрування. Для досягнення поставленої мети представлено метод модифікації шифру гамування, з урахуванням недоліків, що властиві алгоритмам шифрування на основі гамування.

Основний матеріал

Сучасний рівень розвитку і впровадження в життя суспільства інформаційних технологій сприяє актуальності задачі гарантування конфіденційності електронних документів. В публікаціях [5, 6] описані переваги впровадження систем електронного документообігу (СЕД). СЕД забезпечують процес якісного формування, виконання, пошуку, а також надійного зберігання великих об'ємів інформації. Особливу увагу потрібно звернути на надійність зберігання, обробки і передачі ЕД. Однак, для їх результативного функціонування потрібні ефективні методи та засоби захисту інформації. Очевидно, що обмін ЕД можливий лише за умови забезпечення їх конфіденційності, ефективного захисту від підробки чи несанкціонованих змін. На даний момент основним механізмом забезпечення конфіденційності є криптографічні алгоритми шифрування.

Прогрес обчислювальних систем, зростаючий рівень вимог користувачів забезпечення захисту інформації стали причиною розробки нових криптографічних засобів. Криптографічна система захисту інформації – система захисту, в якій використовуються криптографічні методи шифрування даних. Насамперед, інтерес до криптографічних систем обумовлений глобальним розвитком комп'ютерних мереж, якими передаються великі об'єми інформації. З іншого боку поява нових потужних комп'ютерів, технологій мережевих і нейронних обчислень піддали критиці криптографічні системи, які до недавнього часу вважалися абсолютно надійними. Більшість розвинених, в області освоєння інформаційних технологій, країн перейшли або розгорнули активну роботу по переходу на нові стандарти шифрування з підвищеними гарантіями криптографічної стійкості [7]. Увагу спеціалістів в сфері керування і обміну ЕД привертають проблеми своєчасного виявлення загроз інформаційної безпеки ЕД в умовах зростання комп'ютерних злочинів. Несанкціоновані зміни в ЕД можуть призвести до порушення основних властивостей ЕД таких, як конфіденційність, цілісність та достовірність. Традиційно для цієї задачі використовуються криптографічні методи. На відміну від інших методів, вони спираються лише на властивості самої інформації, не використовуючи особливості її обробки, передачі, зберігання. Криптографічні системи представляють собою своєрідний бар'єр між даними, які потребують захисту і потенційним порушником ІБ. Криптографічну систему складає множина перетворень відкритого тексту, включаючи простір ключів – набір можливих значень ключа. Так склалося, що під криптографічним захистом мається на увазі шифрування даних. Шифрування – процес перетворення інформації з метою зробити його недоступним для не вповноважених суб'єктів. Ключ – інформація, необхідна для шифрування і розшифрування інформації [4]. Одними із надійних засобів криптографії є симетричні алгоритми шифрування з використанням гами. В загальному вигляді структурну схему алгоритму шифрування, що базується на гамуванні можна показати наступним чином рис. 1.

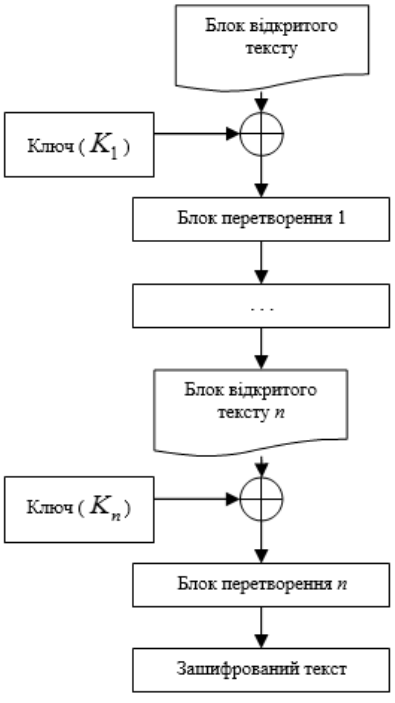

Рис. 1. Структура алгоритму шифрування

З рис. 1 видно, що шифрування інформації відбувається поетапно: перший блок даних шифрується ключем K_1, відповідно n-й блок – ключем K_n. Саме від збереження у таємниці ключа

© Розломій І.О., 2016

і криптографічної стійкості шифру залежить ефективність шифрування. Завдання створення якісного шифру гамування полягає в забезпеченні таких властивостей: послідовність гами має бути повністю випадковою, а також неможливість відкриття невідомих частин гами і ключа за відомими. Результат шифрування буде складним для відкриття в тому випадку, якщо в гамі не будуть повторюватися бітові послідовності. Також важливим є той факт, що коли зловмиснику стає відомим фрагмент вихідного тексту і відповідний йому шифртекст стає легким завдання відновлення всієї послідовності, гамування в такому разі є неефективним. Структурна схема демонструє загальний алгоритм шифрування методом гамування, який можна вдосконалювати шляхом розробки нових модифікацій шифру. Шифри, що базуються на принципі гамування характеризуються надійністю, тому їх широке використання цілком очевидне. На даний час розроблено багато варіантів шифру гамування, наприклад, режим гамування зі зворотнім зв'язком. Суть даного методу полягає в сумуванні за модулем два блоку відкритого тексту з зашифрованим попереднім блоком. Шифрування таким методом може бути описане системою виразів (1).

$$\begin{cases} Z_1 = B_1 \oplus K \\ Z_2 = B_2 \oplus Z_1 \\ ..... \\ Z_n = B_n \oplus Z_{n-1} \end{cases}, \qquad (1)$$

де $Z_1, Z_2, ..., Z_n$ – зашифровані блоки інформації, $B_1, B_2, ..., B_n$ – блоки відкритого тексту, K – ключ шифрування, $\oplus$ – операція суми за модулем два.

До переваг шифрів гамування можна віднести наступні: висока швидкість шифрування, потоковість шифрування та дешифрування, збереження розміру інформації при шифруванні. Проте, існують і суттєві недоліки даних шифрів, такі як нестійкість шифру при повторному застосуванні та послідовність доступу до інформації [9]. Більшість відомих до цього часу методів гамування мають ряд недоліків, уникнути яких можна застосовуючи модифікацію шифру гамування. Суть вдосконаленого шифру гамування полягає в шифруванні за допомогою зміненого ключа з кожним наступним блоком інформації. Зміни в ключі відбуваються шляхом зсуву символів псевдовипадкової послідовності чисел (ПВЧ) $H = (h_1, h_2, ..., h_n)$ на один символ, як показано на рис. 2.

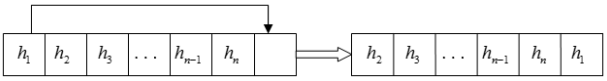

Рис. 2. Принцип формування ключа шифрування

Перестановка символів ключа відбувається кожного разу, коли в послідовності двійкових символів відкритого тексту $T = (t_1, t_2, ..., t_n)$ зустрічається значення нуля, $t_i = 0$. Тобто послідовність відкритого тексту розбивається на блоки, які починаються з двійкового символу нуль. У відкритому тексті, представленому у двійковій формі, значення символу нуль не можливо передбачити, тобто він не має закономірності, за якою буде зустрічатися в послідовності. З цього слідує, що відкритий текст матиме блоки різного розміру і їх кількість буде не меншою за кількість нулів в двійковій послідовності відкритого тексту. Перший блок відкритого тексту за допомогою операції XOR додається з ключем K_1, згенерованою ПВЧ. У всіх наступних блоках символи відкритого тексту сумуватимуться з символами зміненої ключової послідовності, тобто в кожному наступному ключеві $K_2, K_3, ..., K_n$ буде зсув на один символ h_i. Завдяки змінам в ключової послідовності підвищиться надійність захисту інформації. В роботі [7] зазначено, що повторне використання ключа послаблює криптостійкість алгоритму шифрування. Перестановка символів ключа дозволить вирішити дану проблему, оскільки зміниться послідовність символів ключа. Схематично суть даного методу можна показати наступним чином рис. 3.

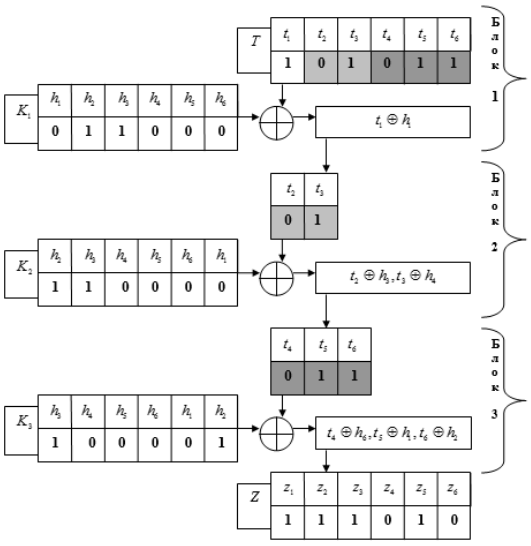

Рис. 3. Блочний алгоритм шифрування модифікованим шифром гамування

© Розломій І.О., 2016

З алгоритму шифрування (рис. 3) видно, що відкритий текст розділений на три блоки, відповідно, починаючи з кожного нульового символу t_2,t_4. Кожний блок за допомого операції суми за модулем два додається відповідно з ключами K_1,K_2,K_3, зміненими за певним принципом (рис. 2). В результаті виконання операцій в кожному з трьох блоків отримуємо послідовність символів $Z=(z_1,z_2,...,z_6)$, яка є результатом шифрування відкритого тексту.

Алгоритми шифрування, що базуються на гамуванні широко використовуються для побудови криптографічних систем захисту інформації. Для сучасних криптосистем сформульовані певні критерії та вимоги, якими потрібно керуватися при розробці системи захисту. До базових вимог можна віднести наступні: зашифрований текст, можливо відкрити лише за наявності ключа; знання алгоритму шифрування не має впливати на надійність захисту; будь-який ключ з множини доступних має забезпечувати надійний захист інформації; мінімальний об'єм ключової інформації; максимальна простота реалізації і вартість; висока оперативність, а також можливість, як програмної, так і апаратної реалізації [10].

Криптографічна система захисту ЕД з використанням вдосконаленого шифру гамування складається з блоків. Першим є блок генерації ПВЧ, тобто за допомогою генератора, конгруентного датчика чи будь-яким з інших способів [11] отримуємо послідовність, так званий, первинний ключ. Наступним йде блок формування ключової послідовності, тобто перестановка символів і безпосередньо блок криптографічного перетворення – додавання за модулем два блоку відкритого тексту з ключем. Наглядно структуру системи захисту ЕД на основі запропонованого методу модифікації шифру гамування можна показати таким чином рис. 4.

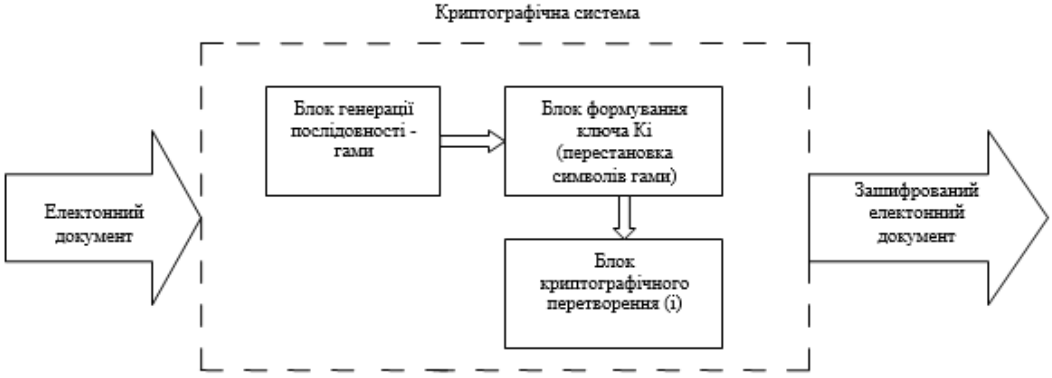

Рис. 4. Структура системи захисту ЕД на основі модифікації шифру гамування

Основу вибору методів захисту ЕД складає глибокий аналіз їх слабких і сильних сторін і має спиратися на критерії ефективності. Головним критерієм ефективності є ймовірність розсекречування ключа, тобто криптографічна стійкість алгоритму. Криптостійкість – характеристика шифру, яка визначає стійкість до розшифрування без знання ключа [12]. Існують показники криптографічної стійкості алгоритму серед яких: кількість можливих ключів та час необхідний для крпитоаналізу [13]. Виходячи з описанного методу захисту інформації, криптографічна стійкість буде визначатися за формулою (2):

$$K_{st}=(K_o)^{Ke} \qquad (2)$$

де K_o – кількість операцій криптографічного перетворення, яка залежить від довжини тексту і кількості сформованих ключів; K_e – кількість етапів криптографічного перетворення, що залежить від кількості блоків відкритого тексту.

Для забезпечення достатнього рівня криптографічної стійкості в сучасних умовах використовуються системи з великою довжиною ключа. Оскільки зростає довжина ключа – зростає і складність обчислень криптографічних операцій. Досить важливим також є час виконання криптографічних процесів алгоритмів в системах захисту інформації.

Висновки

Проведені дослідження доводять, що найбільш ефективним механізмом захисту інформаційних ресурсів залишаються криптографічні методи. В ході дослідження був розглянутий такий метод шифрування даних, як гамування. Запропоновано вдосконалений метод шифрування, що враховує недоліки властиві

© Розломій І.О., 2016

симетричному шифруванні з використанням гами. Даний метод не дозволить розшифрувати інформацію без знання первинного ключа і принципу його формування. Шифрування блоків вихідного тексту за допомогою накладання гами фіксованого розміру реалізується за допомогою запропонованого алгоритму при постійно змінній ключовій послідовності. Використання модифікації алгоритму гамування з врахуванням змін, введених в традиційний метод, дозволить підвищити рівень криптографічної стійкості шифру та забезпечити ефективний захист ЕД.

Список використаних джерел

1. *Трепачева А.В.* Дерандомизационная криптостойкость гомоморфного шифрования / А.В. Трепачева // Труды ИСПРАН. – 2015. – №6(27). – С. 381–394.
2. *Козуб А.А., Мещеряков Р.В.* Модель защиты информации при использовании средств криптографической защиты / А.А. Козуб, Р.В. Мещеряков // Известия ТРТУ. Тематический выпуск «Информационная безопасность». – 2002. – №3. – С. 274–276.
3. *Елисеев Н.И.* Модель угроз безопасности информации при ее обработке в системе защищенного документооборота / Н.И. Елисеев // Известия ЮФУ. Технические науки. Тематический выпуск. – 2012. – №12 (137). – С. 112–118.
4. *Кукарцев А.М., Попов А.М., Шестаков В.С.* О прямом операционном анализе симметричных шифров / А.М. Кукарцев, А.М. Попов, В.С. Шестаков // Прикладная дискретная математика. Математические методы криптографии. – 2008. – № 2(2). – С. 45–49.
5. *Панасенко С.П.* Защита документооборота в современных компьютерных системах / С.П. Панасенко // Информационные технологии. – 2001. – № 4. – С. 41- 45.
6. *Астахова Л.В., Лужнов В.С.* Проблемы организации защищенного документооборота с использованием электронной подписи на предприятиях малого бизнеса / Л.В. Астахова, В.С. Лужнов // Вестник ЮФУ. Серия: Компьютерные технологии, управление, радиоэлектроника. – 2013. – №3(13). – С. 54-60.
7. *Кубашев Д.Ю., Леухин А.Н.* Повышение криптостойкости преобразования информации методом гаммирования / Д.Ю. Кубашев, А.Н. Леухин // Вестник МарГТУ. Радиотехнические и инфокоммуникационные системы. – 2008. – №3. – С. 63–68.
8. *Горбенко И.Д., Долгов В.И, Олейников Р.В., Руженцев В.И., Михайленко М.С.,. Горбенко Ю.И.* Методы и средства криптографии и стеганографии / И.Д. Горбенко, В.И Долгов, Р.В. Олейников, В.И. Руженцев, М.С. Михайленко, Ю.И. Горбенко // Известия ЮФУ. Технические науки. Тематический выпуск. – 2008. – №4. – С. 183-189.
9. *Баричев С.Г.* Основы современной криптографии / Баричев С.Г., Гончаров В.В., Серов Р.Е. – М.: Горячая линия - Телеком, 2002. – 175 с.
10. *Настенко А.А.* Показатели статистической безопасности украинских блочных симметричных шифров / А. А. Настенко // Информационные технологии. Технологический аудит и резервы производства. – 2012. – № 5/2(7). – С. 32–38.
11. *Rukhin A.,* A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. NIST Special Publication. Washington, 2000. – 822 с.
12. *Авдошин С.М., Савельева А.А.* Криптографические методы защиты информационных систем// Известия АИН им. А.М. Прохорова. Бизнес-информатика. – 2006. – №3(17). – С. 91– 99.
13. *Рябко Б.Я., Фионов А.И.* Основы современной криптографии для специалистов в информационных технологиях / Б. Я. Рябко, А. И. Фионов. – Ин-т вычислительных технологий СО РАН, Сиб. гос. ун-т телеком. и информатики. – М.: Научный мир, 2004. – 172 с.

Поступила в редакцию 10 октября 2016 г.

© Розломій І.О., 2016

УДК 004.056.55

И.А. Розломий

Черкасский национальный университет имени Богдана Хмельницкого,

бульвар Шевченка, 81, корпус 3, г. Черкассы, 18000, Украина.

Исследование структуры и криптографической стой кости модификации шифра гаммирования

Статья посвящена проблеме обеспечения информационной безопасности электронных документов (ЭД). Особое внимание сосредоточено на криптографических алгоритмах шифрования, поскольку они остаются основным механизмом обеспечения конфиденциальности документов. В статье рассмотрены базовые требования к разработке криптографических систем защиты ЭД. Предложенный усовершенствованный метод шифра гаммирования, учитывающий недостатки существующих алгоритмов. Шифрование предложенным методом улучшенное путем изменения ключевой последовательности с каждым блоком информации. В результате построена структурная схема процесса шифрования модифицированным шифром сдерживания. Определены критерии, влияющие на криптографическую стойкость шифрования. Исследована криптографическую стойкость системы защиты ЭД построенной на основе предложенного метода. Использование данной модификации позволит повысить эффективность защиты ЭД. Библ. 13., рис.4.

Ключевые слова: *шифр гаммирования; криптостойкость; криптоанализ; псевдослучайные числа; сумма по модулю.*

UDC 004.056.55

I. Rozlomii

Cherkassy Bogdan Khmelnitsky National University,

boulevard Shevchenko, 81, Chercassy, 18000, Ukraine.

Researching structure and of cryptographic strength of the modification of gamma cipher

The article deals with the problem of information security of electronic documents. Special attention is focused on cryptographic algorithms for encryption, since it is the main mechanism ensuring the confidentiality of documents. The basic requirements for the development of cryptographic systems of electronic document protection has been considered in the article. The improved method of gamma cipher which takes into account the shortcomings of existing algorithms was suggested. Encryption of proposed methods improved by changing the key sequence with each blocks of information. The block diagram of encription with the modification of gamma cipher was built in result. The criteria that affect the cryptographic strength of encryption were determined. The cryptographic strength of electronic document protection system built on the basis of the proposed method was researched. Using this modification will increase the effectiveness of electronic documents protection. Referense 13, Figures 4.

Keywords: *gamma cipher; cryptographic strength; cryptanalysis; pseudorandom numbers; XOR*.

Reference

1. *Trepacheva, A. V.* (2015). Derandomizations cryptographic homomorphic encryption. Proceedings Corrected, (6), pp. 381–394 (Rus).
2. *Kozub, A. A. and Meshcheryakov, R. V.* (2002). Model of information protection using cryptographic protection. News TSURE. Special Issue "Information Security", (3), pp. 274–276 (Rus).
3. *Eliseev, N. I.* (2012). Model of information security threats with its processing in the system of secure document. Proceedings of the SFU. Technical science. Special Issue, (12), pp. 112 –118 (Rus).
4. *Kukartsev, A. M., Popov, A. M. and Shestakov, V. S.* (2008). About the direct operational analysis of symmetric ciphers. Applied discrete mathematics. Mathematical Methods of Cryptography,(2), pp. 45–49 (Rus).

© Розломій І.О., 2016

5. *Panasenko, S. P.* (2001). Protect document in modern computer systems. Information technologies, (4), pp 41–45 (Ukr).
6. *Astakhov, L. V. and Luzhnov, V. S.* (2013). Problems of the organization of the protected document with an electronic signature in small business. Herald of SFU. Series: Computer technology, management, electronics, (3), pp. 54–60 (Rus).
7. *Kubashev, D. Y. and Leukhin, A. N.* (2008). Improving the reliability of information transformation by XOR. Herald MarSTU. Radio engineering and information and communication systems, (3), pp. 63–68 (Rus).
8. *Gorbenko, I. D., Dolgov, V. I., Oleynikov, R. V., Ruzhentsev, V. I., Mikhailenko, M. S. and Gorbenko, Y. I.* (2008) Methods and tools for cryptography and steganography. Proceedings of the SFU. Technical science. Special Issue, (4), pp. 183–189 (Rus).
9. *Barichev, S. G.* (2002). The foundations of modern cryptography. Hotline – Telecom, Moscow, 175 p. (Rus).
10. *Nastenko, A. A.* (2012). Statistical Indicators Ukrainian security block symmetric ciphers. Information technologies. Technological audit and production of reserves, (5), pp. 32–38 (Rus).
11. *Rukhin, A.* (2000). A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. NIST Special Publication. Washington, 822 p. (Eng).
12. *Avdoshin, S. M. and Savelyev, A. A.* (2006). Cryptographic techniques protect information systems. Business Informatics, (3), pp. 91–99 (Rus).
13. *Ryabko, B. J. and Fionov, A. I.* (2004). The foundations of modern cryptography for professionals in information technology. Science World, Moscow, 172 p. (Rus).

© Розломій І.О., 2016