6. *Штарьков Ю.М., Юхансон Т., Смитс Б.Дж.М.* О совместной стойкости защиты информации и ключа в секретных системах // Проблемы передачи информации. – 1998. – Т. 34. – Вып. 2. – С. 117 – 127.

7. *Алексейчук А.Н., Васюков И.В., Корнейко А.В.* Обоснование стойкости вероятностных моделей рандомизированных блочных шифров к методу разностного криптоанализа // Электронное моделирование. – 2004. – Т. 26. – № 4. – С. 23 – 35.

8. *Алексейчук А.Н.* Достаточные условия стойкости рандомизированных блочных систем шифрования относительно метода криптоанализа на основе коммутативных диаграмм // Реєстрація, зберігання і обробка даних. – 2007. – Т. 9. – № 2 (в печати).

9. *Wagner D.* Towards a unifying view of block cipher cryptanalysis // Fast Software Encryption. – FSE'04, Proceedings. – Springer Verlag, 2004. – P. 116 – 135.

10. *Lai X., Massey J.L., Murphy S.* Markov chiphers and differential cryptoanalysis // Advances in Cryptology – EUROCRYPT' 91, Proceedings. – Springer Verlag, 1991. – P. 17 – 38.

11. *Biham E, Shamir A.* Differential cryptoanalysis of DES-like cryptosystems // J. of Cryptology. – 1991. – V. 4. – № 1. – P. 3 – 72.

12. *Харин Ю.С., Берник В.И., Матвеев Г.В.* Математические основы криптологии. – Минск.: Изд-во БГУ, 1999. – 319 с.

13. *Лидл Р., Нидеррайтер Г.* Конечные поля: В 2 т. / Пер. с англ. – М.: Мир, 1988. – 818 с.

14. *Дельсарт Ф.* Алгебраический подход к схемам отношений теории кодирования: Пер. с англ. М.: Мир, 1976. 136 с.

15. *Алексейчук А.Н.* Случайное кодирование в канале связи с аддитивным шумом, распределенным на конечной абелевой группе // Захист інформації. – 2002. – № 3. – С. 7 – 16.

Поступила 18.05.2007 г.

УДК 621.391:519.7:510.5

Волошин А. Л.

МЕТОД ПОСТРОЕНИЯ СОВЕРШЕННЫХ ПРОТОКОЛОВ МНОЖЕСТВЕННОГО РАЗДЕЛЕНИЯ СЕКРЕТА С МНОГОАДРЕСНЫМ СООБЩЕНИЕМ, РЕАЛИЗУЮЩИХ СЕМЕЙСТВА ИЕРАРХИЙ ДОСТУПА, ДЛЯ ПОДСИСТЕМ УПРАВЛЕНИЯ ДОСТУПОМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ

При разработке современных информационно-телекоммуникационных систем (ИТС) особое внимание уделяется вопросам разграничения доступа к их ресурсам [1]. Согласно принятой мировой и отечественной практике [2, 3], решение задач разграничения доступа к ресурсам ИТС возлагается на подсистему управления доступом (ПУД), которая обычно включается в состав ИТС как отдельная функциональная подсистема. Развитие информационных технологий, систем связи и средств телекоммуникаций, расширение функциональных возможностей ИТС, и, как следствие, сферы их практического применения, создание новых технологических платформ хранения и обработки данных требуют повышения надежностных и эксплуатационных характеристик современных ПУД.

Исходя из особенностей практического использования ИТС в отечественных системах электронного документооборота, на сегодняшний день наибольшее применение находят ПУД, реализующие многоуровневую политику безопасности [4]. Известно также [5, 6], что доминирующую роль при построении ПУД играют криптографические методы; при этом использование протоколов разделения секрета (ПРС) позволяет получать приемлемые

решения как с точки зрения надежности, так и с точки зрения гибкости подсистемы управления доступом.

Напомним (см., например, [7]), что ПРС представляет собой криптографический протокол, позволяющий "разделить" некоторый секретный параметр (так называемый криптографический параметр доступа (КПД)) среди множества пользователей ИТС таким образом, чтобы только некоторые, заранее определенные (разрешенные) коалиции пользователей могли восстановить его значение при объединении хранящейся у них индивидуальной секретной информации. Отметим, что в доступной литературе для обозначения таких криптографических протоколов используются два, по существу, равнозначных термина: протокол разделения секрета [8] и схема разделения секрета [7]. В дальнейшем изложении, как правило, используется первый из приведенных терминов.

Из анализа результатов статей [9 – 11], а также ряда других публикаций следует, что повышение надежности и гибкости подсистем управления доступом современных ИТС может быть достигнуто при применении протоколов разделения секрета, обладающих следующими свойствами:

- возможность одновременного разделения нескольких КПД;
- безусловная (совершенная) стойкость ПРС;
- возможность реализации процедур восстановления КПД с использованием многоадресных сообщений, в том числе, для семейств иерархий доступа на множестве участников протокола;
- вычислительная эффективность процедур формирования секретной информации, передаваемой участникам протокола, и восстановления КПД соответствующими коалициями участников.

Применение протоколов разделения секрета, обладающих одновременно всеми указанными свойствами, позволит существенно улучшить (по сравнению с известными решениями задач разграничения доступа [5, 6, 12]) показатели надежности и гибкости подсистем управления доступом ИТС.

Впервые понятие протокола разделения секрета с многоадресным сообщением, реализующего семейство иерархий доступа, введено в [13], где описана вероятностная модель и приведены отдельные примеры таких протоколов. Позднее в [14] предложена конструкция ПРС, обладающих первыми тремя из перечисленных выше свойств (указанные ПРС получили название совершенных протоколов множественного разделения секрета с многоадресным сообщением, реализующих семейства иерархий доступа (ПМСИД)).

В настоящей статье изложен общий метод построения ПМСИД, описанных в [14]. Показано, что эти криптографические протоколы обладают также последним из перечисленных свойств и, как следствие, допускают простую и эффективную программную (или схемно-техническую) реализацию.

Основные понятия и обозначения

Напомним [14], что ПМСИД представляет собой криптографический протокол, состоящий из двух этапов. На первом этапе (предварительного распределения секретной информации) администратор доступа (АД) передает по защищенному каналу связи индивидуальную секретную информацию каждому участнику ПМСИД. На втором этапе (разделения и восстановления КПД) АД выбирает набор, состоящий из нескольких КПД. Затем он вычисляет по этому набору некоторое сообщение B, которое передает всем участникам ПМСИД по широковещательному каналу связи. Предполагается, что после получения сообщения B каждая коалиция участников может однозначно восстановить "назначенное" ей, согласно протоколу, (возможно пустое) множество КПД из исходного набора. Совокупность таких коалиций участников, упорядоченная в соответствии с их правами по восстановлению криптографических параметров доступа, называется иерархией доступа ПМСИД [14].

Протокол множественного разделения секрета с многоадресным сообщением называется совершенным, если

1) до получения сообщения B любая коалиция участников не имеет никакой информации о значениях КПД;

2) после получения сообщения B каждая коалиция участников может восстановить "назначенные" ей, согласно протоколу, КПД, в то время как об остальных КПД она не имеет никакой апостериорной информации.

Введем ряд обозначений, используемых ниже при изложении метода построения ПМСИД.

Пусть даны различные простые числа $p_1, \ldots, p_w$ и натуральные числа $d_1, \ldots, d_w$. Положим

$$d = \sum_{j=1}^{w} d_j,\ m = p_1^{d_1} \cdots p_w^{d_w},\ R = \mathbf{Z}/(m),\ R_j = \mathbf{Z}/(p_j^{d_j}),\ j \in \overline{1,w},$$

$$S_0 = \{(s_{ij}): s_{ij} \in \mathbf{GF}(p_j),\ i \in \overline{0,d_j - 1},\ j \in \overline{1,w}\}. \quad (1)$$

Обозначим R^* и $D(R) = R \setminus R^*$ соответственно множество обратимых элементов и множество делителей нуля кольца R. Для любой матрицы $H = (h_{ij})_{i \in M, j \in N}$ над кольцом R и произвольного множества $A \subseteq N$ обозначим H_A подматрицу матрицы H, содержащуюся в ее столбцах с номерами из A. Символом $\|H_A\|$ обозначим число различных строк матрицы H_A, а символом $\#A$ – мощность множества A.

Зафиксируем $(k + 1)\times(n + 2)$-матрицу G над кольцом R с элементами g_{ij} ($i \in \overline{0,k}$, $j \in \overline{0,n+1}$, $k, n \geq 2$) вида

$$G = \left(\begin{array}{c|ccc|c} 1 & 0 & \cdots & 0 & g_{0,n+1} \\ \hline 0 & & & & \\ \vdots & & G' & & g_{n+1}^{\downarrow} \\ 0 & & & & \end{array}\right), \quad (2)$$

где $g_{0,n+1} \in R^*$, $g_{n+1}^{\downarrow} \notin D(R)^{(k)}$. Занумеруем столбцы этой матрицы слева направо числами от 0 до $n + 1$, а строки – сверху вниз числами от 0 до k. Для любого делителя t числа m положим

$$\Psi_t = \{A \subseteq P: tR = I_G(A)\}, \quad (3)$$

где $I_G(A)$ – множество всех элементов $r \in R$, для которых вектор rG_0 является линейной комбинацией столбцов матрицы $G_{A \cup \{n+1\}}$, $A \subseteq P$. Положим $\Psi = \{\Psi_t : t \mid m\}$ и введем в рассмотрение следующие семейства множеств:

$$\Psi^{(q)}(\tau) = (\Psi_t^{(q)}(\tau) : t \mid m),\ \Psi^{(q)} = (\Psi^{(q)}(\tau) : \tau \mid m),\ q = 1, 2,$$

где

$$\Psi_t^{(1)}(\tau) = \bigcup \{\Psi_f : f \mid m,\ [f,\tau] = t\}, \quad (4)$$

$$\Psi_t^{(2)}(\tau) = \bigcap \{\Psi_f : f \mid m,\ \frac{f}{(f,\tau)} = t\} \quad (5)$$

(здесь и далее символы $[f,\tau]$ и (f,τ) обозначают наименьшее общее кратное и наибольший общий делитель чисел f и τ соответственно).

Формальное описание метода построения ПМСИД на основе линейных преобразований над кольцом вычетов целых чисел

Опишем метод построения ПМСИД, обладающих перечисленными во введении свойствами, необходимыми при построении подсистем управления доступом современных ИТС.

Метод предназначен для синтеза совершенных ПМСИД с целью их применения при построении подсистем управления доступом современных информационно-телекоммуникационных систем.

Сущность метода заключается в использовании линейных преобразований над кольцами вычетов целых чисел. При этом, в отличие от известных методов построения линейных ПРС над конечными полями [15], векторными пространствами [16] или кольцами Галуа [17], предлагаемый метод позволяет строить совершенные, эффективно реализуемые протоколы множественного разделения секрета с многоадресным сообщением, в том числе, для семейств иерархий доступа на множестве участников.

Исходными данными для синтеза ПМСИД являются следующие объекты:

– $P = \{1, 2, \ldots, n\}$ – множество участников протокола (субъектов и процессов ИТС);

– числа $p_1, \ldots, p_w$ (простые) и $d_1, \ldots, d_w$ (натуральные), задающие множество криптографических параметров доступа вида (1);

– матрица G вида (2) над кольцом $R = \mathbf{Z}/(m)$, где $m = p_1^{d_1} \cdots p_w^{d_w}$.

Приведем формальное описание алгоритмических процедур, реализующих перечисленные в предыдущем пункте этапы ПМСИД.

На этапе предварительного распределения секретной информации администратор доступа выбирает независимо друг от друга, случайно и равновероятно элементы $a_1, \ldots, a_k \in R$ и вычисляет вектор

$$(\pi_1, \ldots, \pi_n, b(a_1, \ldots, a_k)) = (a_1, \ldots, a_k)(G', g_{n+1}^{\downarrow}), \tag{6}$$

первые n координат которого составляют секретную информацию участников (матрица $(G', g_{n+1}^{\downarrow})$ представляет собой соответствующую подматрицу матрицы G вида (2)). При этом элемент $\pi_i \in R$ доставляется i-му участнику ПМСИД по защищенному каналу связи, $i \in \overline{1,n}$, а элемент $b(a_1, \ldots, a_k)$ хранится в секрете у АД.

На этапе разделения и восстановления КПД $(s_{ij}) \in S_0$, $i \in \overline{0, d_j - 1}$, $j \in \overline{1,w}$, администратор доступа применяет следующий алгоритм.

1. Вычисляет элементы

$$s_j = \sum_{i=0}^{d_j - 1} p_j^{\,i} s_{ij}, \quad j \in \overline{1,w}. \tag{7}$$

2. Находит единственный элемент $s \in R$ такой, что

$$s \equiv s_j \pmod{p_j^{d_j}}, \quad j \in \overline{1,w}. \tag{8}$$

3. Выполняет одну из следующих процедур, в зависимости от вида реализуемого семейства иерархий доступа на множестве участников:

– если семейство иерархий доступа имеет вид (4) ($q = 1$), то АД генерирует случайный равновероятный, не зависящий от s элемент $r \in R$, фиксирует параметр $\tau \in R$ и вычисляет многоадресное сообщение B по формуле

$$B = h_{0,n+1} s + b(a_1, \ldots, a_k) + \frac{m}{\tau} r; \tag{9}$$

– если семейство иерархий доступа имеет вид (5) ($q = 2$), то АД фиксирует параметр $\tau \in R$ и вычисляет многоадресное сообщение B по формуле

$$B = h_{0,n+1} s + \tau b(a_1, \ldots, a_k). \tag{10}$$

Сформированное таким образом многоадресное сообщение направляется по широковещательному каналу связи всем участникам ПМСИД.

Отметим, что если семейство иерархий доступа состоит из единственной иерархии, то многоадресное сообщение может быть вычислено по любой из формул (9), (10), в которых следует положить $\tau = 1$.

В [13] показано, что до получения многоадресного сообщения участники, входящие в произвольное множество $A \in \Psi_t^{(q)}(\tau)$, где $t = p_1^{l_1} \cdots p_w^{l_w} \mid m$, $\tau \mid m$, $q \in \{1, 2\}$, не имеют никакой апостериорной информации о криптографических параметрах доступа. При

получении же сообщения вида (9) (вида (10)) участники, входящие в коалицию $A \in \Psi_j^{(1)}(\tau)$ (коалицию $A \in \Psi_j^{(2)}(\tau)$), не получат никакой апостериорной информации о КПД s_{ij} с номерами $d_j - l_j \le i \le d_j - 1$, $j \in \overline{1,w}$ и смогут полностью восстановить КПД s_{ij} с номерами $0 \le i \le d_j - l_j - 1$, $j \in \overline{1,w}$).

Алгоритм восстановления участниками произвольной коалиции $A \in \Psi_j^{(q)}(\tau)$ ***криптографических параметров доступа*** s_{ij}, $i \in \overline{0, d_j - l_j - 1}$, $j \in \overline{1,w}$, заключается в следующем.

Пусть $t = p_1^{l_1} \cdots p_w^{l_w} \mid m$, $A \in \Psi_j^{(q)}(\tau)$, где $\tau \mid m$, $q \in \{1,2\}$, и $\chi^{\downarrow} \in R^{\#A}$ – произвольное решение системы линейных уравнений $G_A x^{\downarrow} = t(G_0 - G_{n+1})$ над кольцом R. Обозначим $\pi_A = (\pi_i : i \in A)$ вектор-строку, составленную из секретных значений, полученных участниками коалиции A на первом этапе ПМСИД. Для любого $j \in \overline{1,w}$ обозначим $\alpha_j(t)$ элемент кольца $R_j = \mathbf{Z}/(p_j^{d_j})$, обратный к произведению $\prod_{v \ne j} p_v^{l_v} \pmod{p_j^{d_j}}$. Тогда справедливы равенства

$$p_j^{l_j} s_j \equiv \alpha_j([t,\tau])(g_{0,n+1})^{-1}\left(\frac{[t,\tau]}{t}\overline{\pi_A}\chi^{\downarrow} + [t,\tau]B\right)\left(\bmod p_j^{d_j}\right),\ j \in \overline{1,w}, \tag{11}$$

$$p_j^{l_j} s_j \equiv \alpha_j\left(\frac{t}{(t,\tau)}\right)(g_{0,n+1})^{-1}\left(\frac{\tau}{(t,\tau)}\overline{\pi_A}\chi^{\downarrow} + \frac{t}{(t,\tau)}B\right)\left(\bmod p_j^{d_j}\right),\ j \in \overline{1,w}, \tag{12}$$

соответствующие случаям, когда многоадресное сообщение B вычисляется по формуле (9) или по формуле (10). Таким образом, вычислив значения (11) или (12), участники коалиции A однозначно восстановят КПД s_{ij} с номерами $0 \le i \le d_j - l_j - 1$, $j \in \overline{1,w}$.

Итак, на основании вышеизложенного описанный выше ПМСИД является совершенным ПРС, реализующим разделение $d = d_1 + \ldots + d_w$ криптографических параметров доступа с использованием многоадресных сообщений. При этом различные способы формирования таких сообщений (см. формулы (9), (10)) позволяют осуществлять разделение КПД в семействах иерархий доступа вида (4) или (5).

Ниже показано, что предложенный ПМСИД является вычислительно эффективным, а именно, позволяет осуществлять разделение и восстановление криптографических параметров доступа с полиномиальной временной сложностью.

Аналитические оценки временных сложностей вычислительных процедур протокола множественного разделения секрета с многоадресным сообщением

Оценим временные сложности алгоритмов, выполняемых на каждом из этапов описанного выше ПМСИД. В качестве модели вычислительного устройства, используемого для реализации алгоритмов, будем использовать равнодоступную адресную машину [18]. Под элементарной операцией (ЭО) будем понимать арифметическую операцию (сложения, вычитания, умножения, обращения) в кольце R.

Докажем следующее утверждение.

Утверждение. Пусть ПМСИД, соответствующий матрице G вида (2), реализует разделение $d = d_1 + \ldots + d_w$ криптографических параметров доступа из множества S_0 вида (1) среди n участников. Тогда временная сложность алгоритма, выполняемого на этапе предварительного распределения секретной информации ПМСИД, не превышает

$$T_{\text{ПРСИ}} = O(n^2) \tag{13}$$

ЭО; временная сложность алгоритма, выполняемого АД на этапе разделения и восстановления секретных ключей, не превышает

$$T_{\text{ФМАС}} = O(d^3) \tag{14}$$

ЭО, а временная сложность алгоритма, выполняемого произвольной коалицией участников на том же этапе ПМСИД, не превышает

$$T_{\text{ВРС}} = O(n^3 + d^2 + dn) \tag{15}$$

элементарных операций.

Доказательство. Докажем справедливость равенства (13). Согласно равенству (6), для вычисления секретной информации участников протокола достаточно выполнить не более $(n+1)n$ умножений и $(n+1)(n-1)$ сложений в кольце R, то есть всего $(n+1)(2n-1) = 2n^2 + n - 1 = O(n^2)$ элементарных операций.

Убедимся в справедливости формулы (14). Согласно равенству (7), для вычисления значений s_j, $j \in \overline{1,w}$, достаточно выполнить d умножений и $d - w$ сложений в кольце R, то есть всего $2d - w = O(d)$ элементарных операций. Далее, исходя из равенства (8), для нахождения значения s достаточно решить систему из w линейных сравнений над кольцом R, для чего потребуется не более $w(w+1)(2w+10)/12 = O(d^3)$ ЭО (с использованием алгоритма, приведенного в [19], стр. 100). Наконец, для вычисления многоадресного сообщения по формуле (9) или (10) потребуется не более чем 5 ЭО. Суммируя полученные оценки, приходим к формуле (14).

Докажем справедливость равенства (15). Прежде всего, отметим, что временная сложность вычисления вектора $\chi^{\downarrow} \in R^{\theta,A}$, где $A \in \Psi_t^{(q)}(\tau)$, $t = p_1^{l_1} \cdots p_w^{l_w} \mid m$, $\tau \mid m$, $q \in \{1,2\}$, определяется сложностью решения системы линейных уравнений $G_A x^{\downarrow} = t(G_0 - G_{n+1})$ над кольцом R и в наихудшем случае (при $\#A = n$) составляет $\frac{10}{3}n^3 - 2n^2 - \frac{1}{3}n = O(n^3)$ ЭО (см. алгоритм приведения к каноническому виду матрицы над кольцом вычетов, изложенный в [19]). Далее, для вычисления чисел $\alpha_j(t) \in R_j$, $t \mid m$, $j \in \overline{1,w}$ и $(h_{0,n+1})^{-1} \in R$ участникам коалиции A достаточно выполнить $w^2 + 1 = O(d^2)$ элементарных операций. Наконец, при восстановлении КПД по формуле (11) или по формуле (12) участникам данной коалиции потребуется выполнить не более $w(n+3)$ умножений и wn сложений в кольце R, то есть в совокупности $w(2n+3) = O(dn)$ ЭО. Из полученных оценок непосредственно следует формула (15).

Утверждение доказано.

Итак, на основании равенств (15) – (17) временные сложности вычислительных процедур ПМСИД, построенных с использованием предложенного метода, зависят полиномиально от числа участников и разделяемых криптографических параметров доступа.

Выводы

В настоящей статье описан метод построения совершенных ПМСИД на основе линейных преобразований над кольцами вычетов целых чисел. Показано, что предложенный метод позволяет строить совершенные протоколы множественного разделения секрета, реализующие восстановление криптографических параметров доступа информационно-телекоммуникационных систем с использованием многоадресных сообщений, в том числе, для семейств иерархий доступа на множестве участников (субъектов и процессов ИТС).

Построенные с использованием предложенного метода протоколы множественного разделения секрета всеми обладают перечисленными выше свойствами, необходимыми при построении ПУД современных ИТС. В частности, они имеют безусловную криптографическую стойкость (являются совершенными) и позволяют осуществлять одновременное разделение нескольких КПД. При этом восстановление криптографических параметров доступа может быть реализовано с использованием многоадресных сообщений,

алгоритм вычисления которых определяется заранее, в зависимости от требуемого вида семейства иерархий доступа. Вычислительные процедуры предложенных ПМСИД имеют полиномиальные (от числа участников и разделяемых КПД) временные сложности и допускают эффективную программную или схемно-техническую реализацию.

По мнению автора статьи, применение описанных ПМСИД при проектировании подсистем управления доступом информационно-телекоммуникационных систем позволит в значительной степени повысить их надежностные и эксплуатационные характеристики, а, значит, и уровень защищенности информации в ИТС в целом.

Список литературы

1. НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу.

2. ISO/IEC 15408:2000 – Information technologies – Security techniques – Evaluation criteria for IT security.

3. НД ТЗІ 1.1-003-99. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу.

4. *Грушо А.А., Тимонина Е.Е.* Теоретические основы защиты информации. – М.: Издательство агентства «Яхтсмен». – 1996. – 192 с.

5. *Zhu B.B., Feng M., Li S.* An efficient key scheme for layered access control of MPEG-4 FGS Video // ICME. – 2004. – P. 443 – 446.

6. *Wu J., Wei R.* An access control scheme for partially ordered set hierarchy with probable security // Cryptology ePrint Archive. – Report. – 2004/295.

7. *Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В.* Основы криптографии. – М.: Гелиос АРВ. – 2001. – 479 с.

8. Словарь криптографических терминов / Под ред. Б.А. Погорелова и В.Н. Сачкова. – М.: МЦНМО, 2006. – 94 с.

9. *Nikov V., Nikova S., Preneel B., Vandewalle J.* On distributed key distribution centers and unconditionally secure proactive verifiable secret sharing schemes based on general access structure // INDOCRYPT'02. – 2002. – P. 422 – 437.

10. *Seberry J., Charnes C., Pieprzyk J., Safavi-Naini R.* 41 Crypto topics and applications II // Handbook on Algorithms and Theory of Computation. – 1998. – P. 1 – 22.

11. *McLean J.* Reasoning about security models // Proceeding IEEE Symposium on privacy and security. – IEEE Computer Society Press. – 1987. – P. 123-131.

12. *Sklavos N., Koufopavlou O.* Access control in network hierarchy: implementation of key management protocol // International Journal of Network Security. – 2005. – Vol.1. – № 2. – P.103 – 109.

13. *Blundo C., Cresti A., de Santis A., Vaccaro U.* Fully dynamic secret sharing schemes // Theoretical Computer Science. – 1996. – Vol. 155. – P. 407 – 410.

14. *Алексейчук А.Н., Волошин А.Л.* Схема разделения нескольких секретов с многоадресным сообщением на основе линейных преобразований над кольцом вычетов по модулю *m* // Реєстрація, зберігання і обробка даних. – 2006. – Т. 8. – № 1. – С. 92 – 102.

15. *Brickell E.F.* Some ideal secret sharing schemes // J. Combin. Math. and Combin. Comput. – 1989. – № 9. – P. 105 – 113.

16. *van Dijk M.* A Linear construction of perfect secret sharing schemes // Advances in Cryptology – EUROCRYPT'94. – Lecture Notes in Comput. Science. – V. 950. – P. 23 – 34.

17. *Ashikhmin A., Barg A.* Minimal vectors in linear codes // IEEE Trans. on Inform. Theory. – 1998. – V. 5. – P. 2010 – 2018.

18. *Ахо А., Хопкрофт Дж., Ульман Дж.* Построение и анализ вычислительных алгоритмов. – Пер. с англ. – М.: Мир, 1979. – 536 с.

19. *Глухов М.М., Елизаров В.П., Нечаев А.А.* Алгебра. Учебник. В 2-х т. Т. 1. – М.: Гелиос АРВ, 2003. – 336 с.

Поступила 22.04.2007 г.