УДК 511.147; 681.3

Ю. Е. Бояринова, Я. В. Одарич
Институт проблем регистрации информации НАН Украины
ул. Н. Шпака, 2, 03113 Киев, Украина

Восстановление информации в задаче разделения секрета для гиперкомплексных числовых систем 2-го порядка с помощью алгоритма Евклида

Рассмотрены примеры восстановления секрета, используя алгоритм Евклида при представлении информации в гиперкомплексных числовых системах второго порядка.

Ключевые слова: *алгоритм Евклида, задача разделения секрета, комплексные числа, двойные числа, дуальные числа.*

При решении задачи разделения секрета необходимо по совокупности остаточных представлений по выбранным модулям осуществить полное восстановление секрета [1]. При решении этой задачи требуется решать сравнения, что достаточно просто делается при представлении данных в действительных числах с помощью функции Эйлера [2]. Так как эта функция не определена для систем второго порядка, то требуется реализовать иной подход, который, в частности, по предложению профессора М.В. Синькова [3, 4] состоит в применении алгоритма Евклида.

Базовые положения

Рассмотрим кратко алгоритм Евклида [5], который состоит в следующем. Пусть a и b — положительные целые. Находим ряд равенств:

$$\left.\begin{aligned} &a = b * q_1 + r_2,\ 0 < r_2 < b \\ &b = r_2 * q_2 + r_3,\ 0 < r_3 < r_2 \\ &\ldots\ldots\ldots \\ &r_{n-2} = r_{n-1} * q_{n-1} + r_n,\ 0 < r_n < r_{n-1} \\ &r_{n-1} = r_n * q_n \end{aligned}\right\}$$

заканчивающийся тогда, когда получаем некоторое значение $r_{n+1} = 0$. Последнее неизбежно, так как ряд $b, r_2, r_3, \ldots$ как ряд убывающих чисел не может содержать

более чем b положительных чисел.

Общие делители чисел a и b одинаковы с общими делителями чисел b и r_2, далее одинаковы с общими делителями чисел r_2 и r_3, чисел r_3 и r_4 и т.д., и, наконец, с делителем числа r_n. Одновременно с этим имеем:

$$(a,b) = (b,r_2) = (r_2,r_3) = \ldots = (r_{n-1},r_n) = r_n .$$

Следовательно, наибольший общий делитель равен r_n. Для взаимно простых чисел $r_n = 1$.

Из теории чисел известно, что для любых взаимно простых a и b найдутся такие x и y, что $ax + by = 1$. Причем $ax = 1(\mathrm{mod}\, b)$ и $by = 1(\mathrm{mod}\, a)$.

Предположим, $a > b$. Тогда мы можем решить уравнения:

$$a * x + b * y = a,$$
$$a * x + b * y = b.$$

Первое уравнение имеет решение $x_0 = 1,\ y_0 = 0$; второе уравнение имеет решение $x_1 = 0, y_1 = 1$. Выполняя последовательно шаги алгоритма Евклида, получим систему уравнений для вычисления $x_i, y_i, x_{i-1}, y_{i-1}$:

$$\begin{aligned} r_{i-1} * x_{i-1} + r_i * y_{i-1} &= r_{i-1}, \\ r_{i-1} * x_i + r_i * y_i &= r_i, \end{aligned} \qquad i = 1 \ldots n .$$

Инициализируем начальные значения: $r_0 = a, r_1 = b$.

Далее выразим r_{i+1}:

$$r_{i+1} = r_{i-1} - q_i * r_i = r_{i-1} * x_{i-1} + r_i * y_{i-1} - q_i * (r_{i-1} * x_i + r_i * y_i)$$
$$r_{i+1} = r_{i-1} * (x_{i-1} - q_i * x_i) + r_i * (y_{i-1} - q_i * y_i) = r_{i-1} * x_{i+1} + r_i * y_{i+1}$$

Следовательно,

$$x_{i+1} = x_{i-1} - q_i * x_i,$$
$$y_{i+1} = y_{i-1} - q_i * y_{i.}$$

Поскольку $r_{n+1} = 0$, и для взаимно простых чисел $r_n = 1$, искомые переменные будут равняться x_n и y_n.

Восстановление секрета при задании данных комплексными числами

Выберем для примера комплексные модули и зададим комплексными числами остаточные представления по этим модулям [6].

$m_1 = 3 + i*4$	$m_2 = 1 + i*4$	$m_3 = 2 + i*3$
$\alpha_1 = i*2$	$\alpha_2 = -i*2$	$\alpha_3 = -i$

Вычисляем произведение модулей M, а также величины $M_i = M / m_i$:

$$\prod_{i=1}^{3} m_i = (3 + i*4)(1 + i*4)(2 + i*3) = -74 - i*7,$$
$$M_1 = m_2 * m_3 = (1 + i*4)(2 + i*3) = -10 + i*11,$$
$$M_2 = m_1 * m_3 = (3 + i*4)(2 + i*3) = -6 + i*17,$$
$$M_3 = m_1 * m_2 = (3 + i*4)(1 + i*4) = -13 + i*16.$$

Рассмотрим первое уравнение:

$$M_1 M_1' \equiv 1 \bmod(3 + i*4),$$
$$(-10 + i*11) M_1' \equiv 1 \bmod(3 + i*4).$$

Инициализируем начальные значения:

$$r_0 = -10 + i*11, \qquad x_0 = 1,$$
$$r_1 = 3 + i*4, \qquad x_1 = 0.$$

Далее последовательно выполняем шаги алгоритма Евклида:

1) $\dfrac{-10 + i*11}{3 + i*4} = \dfrac{14}{25} + i*\dfrac{73}{25}$,

$$14 \bmod(25) \equiv 14,\ 73 \bmod(25) \equiv 23, \Rightarrow$$
$$\Rightarrow r_2 = \frac{14*3 - 23*4}{25} + i*\frac{23*3 + 14*4}{25} = -2 + i*5,$$
$$q_1 = \frac{((-10 + i*11 - (-2 + i*5))}{3 + i*4} = i*2,$$
$$x_2 = x_0 - q_1 * x_1 = 1 - i*2*0 = 1;$$

2) $\dfrac{3 + i*4}{-2 + i*5} = \dfrac{14}{29} + i*\dfrac{-23}{29}$,

$$14 \bmod(29) \equiv 14,\ (-23) \bmod(29) \equiv 6, \Rightarrow$$

$$\Rightarrow r_3 = \frac{14*(-2)-6*5}{29} + i*\frac{6*(-2)+14*5}{29} = -2 + i*2,$$

$$q_2 = \frac{((3+i*4-(-2+i*2))}{-2+i*5} = -i,$$

$$x_3 = x_1 - q_2 * x_2 = 0 - (-i)*1 = i;$$

3) $\frac{-2+i*5}{-2+i*2} = \frac{14}{8} + i*\frac{-6}{8}$,

$$14 \bmod(8) \equiv 6,\ (-6) \bmod(8) \equiv 2, \Rightarrow$$

$$\Rightarrow r_4 = \frac{6*(-2)-2*2}{8} + i*\frac{2*(-2)+6*2}{8} = -2 + i,$$

$$q_3 = \frac{((-2+i*5-(-2+i))}{-2+i*2} = 1-i,$$

$$x_4 = x_2 - q_3 * x_3 = 1 - (1-i)*i = -i;$$

4) $\frac{-2+i*2}{-2+i} = \frac{6}{5} + i*\frac{-2}{5}$,

$6 \bmod(5) \equiv 1,\ (-2) \bmod(5) \equiv 3, \Rightarrow r_5 = \frac{1*(-2)-3*1}{5} + i*\frac{3*(-2)+1*1}{5} = -1-i,$

$$q_4 = \frac{((-2+i*2-(-1-i))}{-2+i} = 1-i,$$

$$x_5 = x_3 - q_4 * x_4 = i - (1-i)*(-i) = 1 + i*2;$$

5) $\frac{-2+i}{-1-i} = \frac{1}{2} + i*\frac{-3}{2}$,

$1 \bmod(2) \equiv 1,\ (-3) \bmod(2) \equiv 1, \Rightarrow r_6 = \frac{1*(-1)-1*(-1)}{2} + i*\frac{1*(-1)+1*(-1)}{2} = -i,$

$$q_5 = \frac{((-2+i-(-i))}{-1+i} = -i*2,$$

$$x_6 = x_4 - q_5 * x_5 = (-i) - (-i*2)*(1+i*2) = -4 + i;$$

6) $\frac{-1-i}{-i} = 1-i,\ r_7 = 0$.

Следовательно, поскольку $r_6 = -i$, то получаем:

$$M_1{}' = x_6 / (-i) = \frac{-4+i}{-i} = -1 - i*4.$$

Рассмотрим второе уравнение:

$$M_2 M_2' \equiv 1 \bmod(1 + i*4),$$
$$(-6 + i*17) M_2' \equiv 1 \bmod(1 + i*4).$$

Инициализируем начальные значения:

$$r_0 = -6 + i*17, \qquad x_0 = 1,$$
$$r_1 = 1 + i*4, \qquad x_1 = 0.$$

Далее последовательно выполняем шаги алгоритма Евклида:

1) $\dfrac{-6 + i*17}{1 + i*4} = \dfrac{62}{17} + i*\dfrac{41}{17}$,

$62 \bmod(17) \equiv 11$, $41 \bmod(17) \equiv 7$, => $r_2 = \dfrac{11*1 - 7*4}{17} + i*\dfrac{7*1 + 11*4}{17} = -1 + i*3$,

$$q_1 = \frac{((-6 + i*17 - (-1 + i*3))}{1 + i*4} = 3 + i*2,$$
$$x_2 = x_0 - q_1 * x_1 = 1 - (3 + i*2)*0 = 1;$$

2) $\dfrac{1 + i*4}{-1 + i*3} = \dfrac{11}{10} + i*\dfrac{-7}{10}$,

$11 \bmod(10) \equiv 1$, $(-7) \bmod(10) \equiv 3$, => $r_3 = \dfrac{11*(-1) - 3*3}{10} + i*\dfrac{3*(-1) + 1*3}{10} = -1$,

$$q_2 = \frac{((1 + i*4 - (-1))}{-1 + i*3} = 1 - i,$$
$$x_3 = x_1 - q_2 * x_2 = 0 - (1 - i)*1 = -1 + i;$$

3) $\dfrac{-1 + i*3}{-1} = 1 - i*3$, $\qquad r_4 = 0$.

Поскольку $r_3 = -1$, то получаем $M_2' = x_3/(-1) = \dfrac{-1 + i}{-1} = 1 - i$.

Рассмотрим третье уравнение:

$$M_3 M_3' \equiv 1 \bmod(2 + i*3),$$
$$(-13 + i*16) M_3' \equiv 1 \bmod(2 + i*3).$$

Инициализируем начальные значения:

$$r_0 = -13 + i*16, \qquad x_0 = 1,$$
$$r_1 = 2 + i*3, \qquad x_1 = 0.$$

1) $\dfrac{-13 + i*16}{2 + i*3} = \dfrac{22}{11} + i*\dfrac{71}{11}$,

$$22 \bmod(13) \equiv 9,\ 71 \bmod(13) \equiv 6,\ \Rightarrow r_2 = \frac{9*2-6*3}{13} + i*\frac{6*2+9*3}{13} = i*3,$$

$$q_1 = \frac{((-13+i*16-(i*3))}{2+i*3} = 1+i*5,$$

$$x_2 = x_0 - q_1 * x_1 = 1-(1+i*5)*0 = 1;$$

2) $\frac{2+i*3}{i*3} = \frac{9}{9} + i*\frac{-6}{9}$,

$$9 \bmod(9) \equiv 0,\ (-6) \bmod(9) \equiv 3,\ \Rightarrow r_3 = \frac{0*0-3*3}{9} + i*\frac{3*0+0*3}{9} = -1,$$

$$q_2 = \frac{((2+i*3-(-1))}{i*3} = 1-i,$$

$$x_3 = x_1 - q_2 * x_2 = 0-(1-i)*1 = -1+i;$$

3) $\frac{i*3}{-1} = -i*3$, $r_4 = 0$.

Поскольку $r_3 = -1$, то получаем $M_3' = x_3/(-1) = \frac{-1+i}{-1} = 1-i$.

Теперь находим число $y = \sum_{i=1}^{3} \alpha_i M_i M_i'$:

$$y = (i*2)(-10+i*11)(-1-i*4) + (-i*2)(-6+i*17)(1-i) + (-i)(-13+i*16)(1-i) = 17+i*83.$$

Отсюда, искомая величина *x* равняется:

$$x = y \bmod(M) = (17+i*83) \bmod(-74-i*7),$$

$$\frac{17+i*83}{-74-i*7} = \frac{-1839}{5525} + i*\frac{-6023}{5525},$$

$$-1839 \bmod(5525) \equiv 3686,\ (-6023) \bmod(5525) \equiv 5027,\ \Rightarrow$$

$$\Rightarrow x = \frac{3686*(-74)-5027*(-7)}{5525} + i*\frac{5027*(-74)+3686*(-7)}{5525} = -43-i*72.$$

Восстановление секрета при задании данных двойными числами

Выберем для примера двойные модули и зададим двойными числами остаточные представления по этим модулям.

$m_1 = 3-e*2$	$m_2 = 5-e*2$	$m_3 = 3+e$
$\alpha_1 = 2-e$	$\alpha_2 = 3-e$	$\alpha_3 = 2+e*2$

Вычисляем произведение модулей *M*, а также величины $M_i = M / m_i$:

$$M = \prod_{i=1}^{3} m_i = (5 - e*2)(3 + e)(3 - e*2) = 41 - e*29,$$
$$M_1 = m_2 * m_3 = (5 - e*2)(3 + e) = 13 - e,$$
$$M_2 = m_1 * m_3 = (3 + e)(3 - e*2) = 7 - e*3,$$
$$M_3 = m_1 * m_2 = (5 - e*2)(3 - e*2) = 19 - e*16.$$

Рассмотрим первое уравнение:

$$M_1 M_1' \equiv 1 \bmod(3 - e*2),$$
$$(13 - e)M_1' \equiv 1 \bmod(3 - e*2).$$

Исходные значения:

$$r_0 = 13 - e, \qquad x_0 = 1,$$
$$r_1 = 3 - e*2, \qquad x_1 = 0.$$

Далее последовательно выполняем шаги алгоритма Евклида:

1) $\dfrac{13 - e}{3 - e*2} = \dfrac{37}{5} + e*\dfrac{23}{5}$,

$37 \bmod(5) \equiv 2$, $23 \bmod(5) \equiv 3$, => $r_2 = \dfrac{2*3 - 3*2}{5} + e*\dfrac{3*3 - 2*2}{5} = e$,

$$q_1 = \frac{(13 - e - e)}{3 - e*2} = 7 + e*4,$$
$$x_2 = x_0 - q_1 * x_1 = 1 - (7 + e*4)*0 = 1;$$

2) $\dfrac{3 - e*2}{e} = -2 + e*3$, $r_3 = 0$.

Поскольку $r_2 = e$, то отсюда $M_1' = x_2 / e = \dfrac{1}{e} = e$.

Рассмотрим второе уравнение:

$$M_2 M_2' \equiv 1 \bmod(5 - e*2),$$
$$(7 - e*3)M_2' \equiv 1 \bmod(5 - e*2),$$

$$r_0 = 7 - e*3, \qquad x_0 = 1,$$
$$r_1 = 5 - e*2, \qquad x_1 = 0.$$

1) $\dfrac{7 - e*3}{5 - e*2} = \dfrac{29}{21} + e*\dfrac{-1}{21}$,

$$29 \bmod(21) \equiv 8,\ -1 \bmod(21) \equiv 20,\ \Rightarrow\ r_2 = \frac{8*5-20*2}{21} + e*\frac{20*5-8*2}{21} = e*4,$$

$$q_1 = \frac{(7-i*3-e*4)}{5-e*2} = 1-e,$$

$$x_2 = x_0 - q_1 * x_1 = 1-(1-e)*0 = 1;$$

2) $\frac{5-e*2}{e*4} = \frac{8}{-16} + e*\frac{-20}{-16}$,

$$8 \bmod(-16) \equiv -8,\ (-20) \bmod(-16) \equiv -4,\ \Rightarrow\ r_3 = \frac{-8*0-4*4}{-16} + e*\frac{-4*0-8*4}{-16} = 1+e*2,$$

$$q_2 = \frac{((5-e*2-(1+e*2))}{e*4} = -1+e,$$

$$x_3 = x_1 - q_2 * x_2 = 0-(-1+e)*1 = 1-e;$$

3) $\frac{e*4}{1+e*2} = \frac{-8}{-3} + e*\frac{4}{-3}$,

$$-8 \bmod(-3) \equiv -2,\ 4 \bmod(-3) \equiv 1,\ \Rightarrow\ r_4 = \frac{-2*1+1*2}{-3} + e*\frac{1*1-2*2}{-3} = e,$$

$$q_3 = \frac{(e*4-e)}{1+e*2} = 2-e,$$

$$x_4 = x_2 - q_3 * x_3 = 1-(2-e)*(1-e) = -2+e*3;$$

4) $\frac{1-e*2}{e} = -2+e$, $r_5 = 0$.

Поскольку $r_4 = e$, то, следовательно, $M_2' = x_4 / e = \frac{-2+e*3}{e} = 3-e*2$.

Рассмотрим третье уравнение:

$$M_3 M_3' \equiv 1 \bmod(3+e),$$

$$(19-e*16)M_3' \equiv 1 \bmod(3+e),$$

$$r_0 = 19-e*16, \qquad x_0 = 1,$$

$$r_1 = 3+e, \qquad x_1 = 0.$$

1) $\frac{19-e*16}{3+e} = \frac{73}{8} + e*\frac{-67}{8}$,

$$73 \bmod(8) \equiv 1,\ -67 \bmod(8) \equiv 5,\ \Rightarrow\ r_2 = \frac{1*3+5*1}{8} + e*\frac{5*3+1*1}{8} = 1+e*2,$$

$$q_1 = \frac{(19-e*16-(1+e*2))}{3+e} = 9-e*9,$$

$$x_2 = x_0 - q_1 * x_1 = 1 - (9 - e*9) * 0 = 1;$$

2) $\dfrac{3+e}{1+e*2} = \dfrac{1}{-3} + e * \dfrac{-5}{-3}$,

$$1 \bmod(-3) \equiv 1,\ -5 \bmod(-3) \equiv -2,\ \Rightarrow\ r_3 = \frac{1*1-2*2}{-3} + e * \frac{-2*1+1*2}{-3} = 1,$$

$$q_2 = \frac{(3+e-1)}{1+e*2} = e,$$

$$x_3 = x_1 - q_2 * x_2 = 0 - e*1 = -e;$$

3) $\dfrac{1+e*2}{1} = 1 + e*2,\ r_4 = 0$.

Отсюда $M_3' = x_3 = -e$.

Находим величину *y*:

$$y = \sum_{i=1}^{3} \alpha_i M_i M_i',$$

$$y = (2-e)(13-e)(e) + (3-e)(7-e*3)(3-e*2) + (2+e*2)(19-e*16)(-e) = 83 - e*75.$$

Тогда:

$$x = y \bmod(M) = (83 - e*75) \bmod(41 - e*29),$$

$$\frac{83-e*75}{41-e*29} = \frac{1228}{840} + e * \frac{-668}{840},$$

$$1228 \bmod(840) \equiv 388,\ (-668) \bmod(840) \equiv 172,\ \Rightarrow$$

$$\Rightarrow\ x = \frac{388*41 + 172*(-29)}{840} + e * \frac{172*41 + 388*(-29)}{840} = 13 - e*5.$$

Восстановление секрета при задании данных дуальными числами

Выберем для примера дуальные модули и зададим дуальными числами остаточные представления по этим модулям.

$m_1 = 2 + \varepsilon$	$m_2 = 5 + \varepsilon * 4$	$m_3 = 3 - \varepsilon * 2$
$\alpha_1 = \varepsilon$	$\alpha_2 = \varepsilon * 4$	$\alpha_3 = 2 - \varepsilon$

Вычисляем произведение модулей *M*, а также величины $M_i = M / m_i$:

$$M = \prod_{i=1}^{3} m_i = (5+\varepsilon*4)(3-\varepsilon*2)(2+\varepsilon) = 30+\varepsilon*19,$$

$$M_1 = m_2 * m_3 = (5+\varepsilon*4)(3-\varepsilon*2) = 15+\varepsilon*2,$$
$$M_2 = m_1 * m_3 = (3-\varepsilon*2)(2+\varepsilon) = 6-\varepsilon,$$
$$M_3 = m_1 * m_2 = (5+\varepsilon*4)(2+\varepsilon) = 10+\varepsilon*13.$$

Рассмотрим первое уравнение:

$$M_1 M_1' \equiv 1 \bmod(2+\varepsilon),$$
$$(15+\varepsilon*2)M_1' \equiv 1 \bmod(2+\varepsilon).$$

Исходные значения:

$$r_0 = 15+\varepsilon*2, \qquad x_0 = 1,$$
$$r_1 = 2+\varepsilon, \qquad x_1 = 0.$$

Выполняем шаги алгоритма:

1) $\dfrac{15+\varepsilon*2}{2+\varepsilon} = \dfrac{30}{4} + \varepsilon * \dfrac{-11}{4}$,

$30 \bmod(4) \equiv 2$, $-11 \bmod(4) \equiv 1$, => $r_2 = \dfrac{2*2}{4} + \varepsilon * \dfrac{1*2+2*1}{4} = 1+\varepsilon$,

$$q_1 = \frac{(15-\varepsilon*2-(1+\varepsilon))}{2+\varepsilon} = 1+\varepsilon,$$
$$x_2 = x_0 - q_1 * x_1 = 1-(1+\varepsilon)*0 = 1;$$

2) $\dfrac{2+\varepsilon}{1+\varepsilon} = 2-\varepsilon$, $r_3 = 0$.

Поскольку $r_2 = 1+\varepsilon$, то $M_1' = x_2/(1+\varepsilon) = \dfrac{1}{1+\varepsilon} = 1-\varepsilon$.

Рассмотрим второе уравнение:

$$M_2 M_2' \equiv 1 \bmod(5+\varepsilon*4),$$
$$(6-\varepsilon)M_2' \equiv 1 \bmod(5+\varepsilon*4).$$

Исходные значения:

$$r_0 = 6-\varepsilon, \qquad x_0 = 1,$$
$$r_1 = 5+\varepsilon*4, \qquad x_1 = 0.$$

Выполним последовательно шаги алгоритма:

1) $\frac{6-\varepsilon}{5+\varepsilon*4}=\frac{30}{25}+\varepsilon*\frac{-29}{25}$,

$30 \bmod(25)\equiv 5$, $-29\bmod(25)\equiv 21$, => $r_2=\frac{5*5}{25}+\varepsilon*\frac{21*5+5*4}{25}=1+\varepsilon*5$,

$$q_1=\frac{(6-\varepsilon-(1+\varepsilon*5))}{5+\varepsilon*4}=1-\varepsilon*2,$$
$$x_2=x_0-q_1*x_1=1-(1-\varepsilon*2)*0=1;$$

2) $\frac{5+\varepsilon*4}{1+\varepsilon*5}=5-\varepsilon*21$, $r_3=0$.

Поскольку $r_2=1+\varepsilon*5$, то $M_2'=x_2/(1+\varepsilon*5)=\frac{1}{1+\varepsilon*5}=1-\varepsilon*5$.

Рассмотрим третье уравнение:

$$M_3M_3'\equiv 1\bmod(3-\varepsilon*2),$$
$$(10+\varepsilon*13)M_3'\equiv 1\bmod(3-\varepsilon*2).$$

Начальные значения:

$$r_0=10+\varepsilon*13, \qquad x_0=1,$$
$$r_1=3-\varepsilon*2, \qquad x_1=0.$$

1) $\frac{10+\varepsilon*13}{3-\varepsilon*2}=\frac{30}{9}+\varepsilon*\frac{59}{9}$,

$30\bmod(9)\equiv 3$, $59\bmod(9)\equiv 5$, => $r_2=\frac{3*3}{9}+\varepsilon*\frac{5*3-3*2}{9}=1+\varepsilon$,

$$q_1=\frac{(10+\varepsilon*13-(1+\varepsilon))}{3-\varepsilon*2}=3+\varepsilon*6,$$
$$x_2=x_0-q_1*x_1=1-(3+\varepsilon*6)*0=1;$$

2) $\frac{3-\varepsilon*2}{1+\varepsilon}=3-\varepsilon*5$, $r_3=0$.

Поскольку $r_2=1+\varepsilon$, то $M_3'=x_3/(1+\varepsilon)=1-\varepsilon$.

Отсюда:

$$y=\sum_{i=1}^{3}\alpha_iM_iM_i',$$

$$y = (\varepsilon)(15 + \varepsilon * 2)(1 - \varepsilon) + (\varepsilon * 4)(6 - \varepsilon)(1 - \varepsilon * 5) +$$
$$+ (2 - \varepsilon)(10 + \varepsilon * 13)(1 - \varepsilon) = 20 + \varepsilon * 35,$$
$$x = y \bmod(M) = (20 + \varepsilon * 35) \bmod(30 + \varepsilon * 19),$$

$$\frac{20 + \varepsilon * 35}{30 + \varepsilon * 19} = \frac{600}{900} + \varepsilon * \frac{670}{900},$$

$$600 \bmod(900) \equiv 600, \quad 670 \bmod(900) \equiv 670.$$

Тогда $x = \dfrac{600 * 30}{900} + \varepsilon * \dfrac{670 * 30 + 600 * 19}{900} = 20 + \varepsilon * 35$.

Работа выполнялась под руководством научного руководителя д.т.н., профессора М.В. Синькова.

1. *Синьков М.В., Бояринова Ю.Е., Калиновский Я.А., Трубников П.В.* Развитие задачи разделения секрета // Реєстрація, зберігання і оброб. даних. — 2003. — Т. 5, № 4. — С. 90–96.

2. *Бояринова Ю.Е., Одарич Я.В., Трубников П.В.* Разработка алгоритмов восстановления информации в задаче разделения секрета // Реєстрація, зберігання і оброб. даних. — 2004. — Т. 6, № 4. — С. 107–112.

3. *Синьков М.В., Бояринова Ю.Е., Калиновский Я.А., Трубников П.В.* Расширение возможностей постановки задачи разделения секрета. Безопасность информации в информационно-телекоммуникационных системах. Материали VII международной научно-практической конференции. — С. 64–65.

4. *Бояринова Ю.Е., Одарич Я.В., Трубников П.В.* Реализация алгоритма Евклида для задачи разделения секрета // Реєстрація, зберігання і оброб. даних. — 2004. — Т. 6, № 3. — С. 58–65.

5. *Ноден П., Китте К.* Алгебраическая алгоритмика с упражнениями и решениями. — М.: Мир, 1999. — 720 с.

6. *Синьков М.В., Губарени Н.М.*. Непозиционные представления в многомерных числовых системах. — К.: Наук. думка, 1979. — 138 с.

Поступила в редакцию 09.03.2005