ity to set a confidence interval for the assessment of false information will allow to obtain results that satisfy the task of detecting false information with appropriate accuracy. But this leads to solving the task of optimizing the evaluation criteria and the time to solve the set task. The scientific novelty consists in substantiating and evaluating the comparative importance of factors that limit the appointment of each individual expert to identify false information using the group expert evaluation method.
The direction of further research is the task of optimizing evaluation criteria.
Keywords: expert, false information, forecasting, algorithm, information technologies.

Лукова-Чуйко Наталія Вікторівна, доктор технічних наук, професор, завідувачка кафедри кібербезпеки та захисту інформації Факультету інформаційних технологій, Київський національний університет імені Тараса Шевченка, Київ, Україна.

Nataliya Lukova-Chuiko, Doctor of technical sciences, professor, Head of the Department of cyber security and information protection, Faculty of Information Technologies, Taras Shevchenko National University of Kyiv, Ukraine
E-mail: lukova@knu.ua.
Orcid ID: 0000-0003-3224-4061.

Лаптєва Тетяна Олександрівна, аспірантка кафедри кібербезпеки та захисту інформації, Факультет інформаційних технологій, Київський національний університет імені Тараса Шевченка, Київ, Україна

Tetiana Laptieva, PhD-student, Department of Cyber Security and Information Protection Faculty of information technology, Taras Shevchenko National University of Kyiv, Ukraine.
E-mail: tetiana1986@ukr.net.
Orcid ID: 0000-0002-5223-9078.

DOI: 10.18372/2410-7840.26.18825
УДК 004.056.55

АРИФМЕТИКА АСИМЕТРИЧНИХ КРИПТОСИСТЕМ В ПОЛІ КОМПЛЕКСНИХ ЧИСЕЛ

Андрій Алілуйко, Михайло Касянчук

На сучасному етапі розвитку інформаційних технологій виникає необхідність у вдосконаленні існуючих і розробці нових методів і засобів підвищення продуктивності асиметричних криптоалгоритмів. У статті наведено теоретичні основи модулярних обчислень та асиметричної криптографії в комплексній числовій області. Зокрема, розглянуто метод визначення комплексного та дійсного залишку за комплексним модулем. Розглянуто алгоритм Евкліда та його наслідок для пошуку оберненого елемента в комплексній числовій області. Здійснено порівняння складності алгоритму Евкліда для знаходження оберненого елементи при знаходженні найменших додатних та абсолютно найменших залишків. Проведено пошук аналогу функції Ейлера в комплексній числовій області та використано цю функцію для знаходження оберненого елемента до комплексного числа. Продемонстровано відновлення комплексного числа з допомогою китайської теореми про остачі. Розглянуті модулярні обчислення в області комплексних чисел можна використати при побудові нових підходів до асиметричного шифрування.
***Ключові слова**: асиметрична криптосистема, комплексне число, алгоритм Евкліда, функція Ейлера, система залишкових класів.*

ВСТУП

На сучасному етапі розвитку інформаційних технологій виникає ряд проблем та науково-технічних задач, пов'язаних з підвищенням стійкості комп'ютерних систем до різного виду атак [2, 4], швидкодії алгоритмів шифрування/ розшифрування/аутентифікації [1, 5], оптимізацією обчислень над багаторозрядними числами [8], зменшенням часових складностей виконання базових операцій в асиметричних криптоалгоритмах [9] та створенням засобів захисту інформаційних потоків. Такі задачі опрацювання інформаційних потоків в сучасних комп'ютерних системах розв'язуються на основі використання відомих алгоритмів шифрування, факторизації, дискретного логарифмування, модулярних та інших операцій.

Слід зазначити, що в сучасній асиметричній криптографії, яка функціонує в позиційних системах числення, постає завдання вирішення трудомістких обчислювальних науково-практичних задач з необхідністю виконання значних обсягів обчислень в реальному часі [3]. Переважна більшість таких криптоалгоритмів ґрунтуються на цілочисельній модулярній арифметиці. Зокрема, в основі асиметричної криптосистеми RSA лежить пошук найбільшого спільного дільника (НСД) двох чисел (як правило, за допомогою алгоритму Евкліда), пошук оберненого елемента за модулем (переважно, за допомогою наслідку з

алгоритму Евкліда [10]), пошук функції Ейлера та модулярне експоненціювання. В основі криптосистеми Рабіна лежить модулярне піднесення до квадрату, пошук квадратного кореня за модулем та використання китайської теореми про залишки [7], яка випливає з алгоритму Евкліда та його наслідку [6]. Стійкість обох цих криптосистем до криптоаналізу визначається часом факторизації добутку двох великих простих чисел. В основі криптосистеми Ель-Гамаля лежить модулярне експоненціювання та пошук оберненого елемента за модулем. Її стійкість визначається часом пошуку дискретного логарифму.

Кожна з цих асиметричних криптосистем передбачає розширюваність, тобто збільшення довжини ключа при збільшенні обчислювальних можливостей зловмисника. Наприклад, з 2007 року система шифрування RSA вважалась надійною при довжині ключа в 1024 біти, на даний час мінімальна довжина ключа повинна бути 2048 біт. Однак збільшення довжини ключа не може безмежно зростати, оскільки це призводить до збільшення блоку відкритого тексту, який потрібно зашифрувати. Тому виникає потреба у застосуванні нових підходів до асиметричного шифрування без зменшення їх стійкості до криптоаналізу. Одним із них є застосування більш складних полів із більшими циклічними групами, наприклад, цілих комплексних чисел або чисел Гауса.

Тому метою нашої роботи є розробка теоретичних основ модулярних обчислень та асиметричної криптографії, зокрема, алгоритму Евкліда, його наслідку, пошуку оберненого елемента, китайської теореми про остачі, пошуку функції Ейлера в комплексній числовій області.

ОСНОВНА ЧАСТИНА

Теоретичні основи виконання арифметичних модулярних операцій на множині комплексних чисел заклав Гаус. Аналогічно до традиційної асиметричної криптографії, доцільно розглядати тільки цілі комплексні числа (їх ще називають гаусовими), в яких дійсна та уявна частини є цілими: $\dot{a} = a + bi$; $a, b \in Z$.

Число $\dot{b} = p + qi$ є дільником числа $\dot{a}$, якщо відношення $\frac{\dot{a}}{\dot{b}} = \frac{ap+bq}{p^2+q^2} + \frac{bp-aq}{p^2+q^2} i$ є цілим комплексним числом, тобто для нього має виконуватися умова:

$$\begin{cases} (ap+bq) \bmod N(\dot{b}) = 0, \\ (bp-aq) \bmod N(\dot{b}) = 0, \end{cases}$$

де $N(\dot{b}) = p^2 + q^2$ – норма числа $\dot{b}$. Норма володіє властивістю мультиплікативності: $N(\dot{a} \cdot \dot{b}) = N(\dot{a}) \cdot N(\dot{b})$.

Ненульове число $\dot{a}$ називається простим, якщо воно не має інших дільників, окрім тривіальних одиниць (1, -1, i, $-i$). У протилежному випадку таке число називається складеним. Якщо норма комплексного числа є простим числом, то і саме комплексне число є простим.

Якщо для двох комплексних чисел $\dot{a}$ та $\dot{b}$ виконується рівність $\dot{a} = i^k \cdot \dot{b}$, $i = \overline{0,3}$, то вони називаються асоціативними. До них, наприклад, належать числа $1+2i$, $-1-2i$, $-2+i$, $2-i$.

Число $\dot{r} = x + yi$ називається залишком числа $\dot{a}$ за модулем $\dot{b}$ ($\dot{a} \bmod \dot{b} = \dot{r}$), якщо різниця $\dot{a} - \dot{r}$ ділиться на $\dot{b}$.

Для знаходження залишку $\dot{r} = x + yi$ потрібно розв'язати систему рівнянь:

$$\begin{cases} (ap+bq) \bmod N(\dot{b}) = xp + yq = r, \\ (bp-aq) \bmod N(\dot{b}) = yp - xq = r'. \end{cases} \quad (1)$$

Розв'язок системи (1) має вигляд:

$$x = \frac{rp - r'q}{N(\dot{b})}; \quad y = \frac{r'p + rq}{N(\dot{b})}. \quad (2)$$

Здійснимо оцінку норми $N(\dot{r})$. Враховуючи (2), отримаємо $N(\dot{r}) = x^2 + y^2 = \frac{r^2 + r'^2}{N(\dot{b})}$.

Якщо вважати r і r' найменшими додатними залишками за дійсним модулем $N(\dot{b})$, тобто $0 \le r \le N(\dot{b}) - 1 < N(\dot{b})$, $0 \le r' \le N(\dot{b}) - 1 < N(\dot{b})$, то справедлива оцінка $N(\dot{r}) \le \frac{2(N(\dot{b})-1)^2}{N(\dot{b})} < 2N(\dot{b})$.

Отже, для комплексних чисел $\dot{a}$ та $\dot{b} \ne 0$ існують такі комплексні числа $\dot{q}$ та $\dot{r}$, для яких:

$$\dot{a} = \dot{b}\dot{q} + \dot{r} \text{ і } N(\dot{r}) \le \frac{2(N(\dot{b})-1)^2}{N(\dot{b})} < 2N(\dot{b}). \quad (3)$$

Якщо ж вважати r і r' абсолютно найменшими залишками за дійсним модулем $N(\dot{b})$, тобто $|r| \le \frac{1}{2} N(\dot{b})$, $|r'| \le \frac{1}{2} N(\dot{b})$, то в (3) маємо наступну оцінку норми: $N(\dot{r}) \le \frac{1}{2} N(\dot{b})$.

Приклад 1. Для комплексних чисел $\dot{a}=25-22i$ та $\dot{b}=8+3i$ знайти такі числа $\dot{q}$ та $\dot{r}$, для яких виконується рівність $\dot{a}=\dot{b}\dot{q}+\dot{r}$.

Спершу складемо систему рівнянь відповідно до співвідношень (1):

$$\begin{cases}(25\cdot 8-22\cdot 3)\bmod N(\dot{b})=134\bmod 73=61\bmod 73=-12=r,\\(-22\cdot 8-25\cdot 3)\bmod N(\dot{b})=-251\bmod 73=41\bmod 73=-32=r'.\end{cases}$$

Якщо взяти найменші додатні залишки $r=61$ та $r'=41$, то за формулами (2) отримаємо комплексний залишок $\dot{r}=5+7i$, норма якого $N(\dot{r})=74<\dfrac{2(N(\dot{b})-1)^2}{N(\dot{b})}=144<2N(\dot{b})=148$ і більша за $N(\dot{b})=73$. Далі шукаємо $\dot{q}=\dfrac{\dot{a}-\dot{r}}{\dot{b}}=\dfrac{(\dot{a}-\dot{r})\bar{\dot{b}}}{N(\dot{b})}=1-4i$. В результаті отримуємо розклад $25-22i=(8+3i)(1-4i)+(5+7i)$.

Якщо ж взяти абсолютно найменші залишки $r=-12$ та $r'=-32$, то за формулами (2) отримаємо комплексний залишок $\dot{r}=-4i$, норма якого $N(\dot{r})=16$ значно менша за $\dfrac{1}{2}N(\dot{b})=\dfrac{73}{2}$. Знаходимо $\dot{q}=\dfrac{\dot{a}-\dot{r}}{\dot{b}}=2-3i$ та отримуємо розклад $25-22i=(8+3i)(2-3i)+(-4\mathrm{i}).$

Якщо $5+7i$ поділити на $8+3i$ з абсолютно найменшими залишками $r=-12$ та $r'=-32$, то отримаємо $5+7i=(8+3i)(1+i)+(-4i)$.

Нижче наведено усі можливі залишки при різних r та r' (табл. 1).

Таблиця 1

Розклад комплексного числа $25-22i$ за модулем $8+3i$

$r=61,$ $r'=41$	$25-22i=$ $(8+3i)(1-4i)+(5+7i)$	$N(\dot{r})=$ $74>73$
$r=61,$ $r'=-32$	$25-22i=$ $(8+3i)(1-3i)+(8-i)$	$N(\dot{r})=$ $65<73$
$r=-12,$ $r'=41$	$25-22i=$ $(8+3i)(2-4i)+(-3+4i)$	$N(\dot{r})=$ $25<73$
$r=-12,$ $r'=-32$	$25-22i=$ $(8+3i)(2-3i)+(-4i)$	$N(\dot{r})=$ $16<73$

Найкраще при діленні комплексних чисел шукати залишки $\dot{r}$, для яких має місце обмеження $N(\dot{r})<N(\dot{b})$. Але для спрощення розрахунків доцільно використовувати абсолютно найменші залишки, які гарантують виконання обмеження $N(\dot{r})\le\dfrac{1}{2}N(\dot{b})$.

При діленні комплексних чисел також можна скористатися першою фундаментальною теоремою Гауса, яка встановлює ізоморфізм між комплексними числами та їх дійсними залишками: для комплексних чисел $\dot{a}=a+bi$ та $\dot{b}=p+qi$ з взаємно простими p та q має місце рівність $\dot{a}\bmod\dot{b}=x$, де x – дійсне число, яке може приймати лише одне значення з ряду 0, 1, 2, …, $N(\dot{b})$. Причому x шукається із співвідношення $(a+b\rho)\bmod N(\dot{b})=x$, де $\rho=uq-vp$, $up+vq=1$.

Якщо в модулі $\dot{b}=p+qi$ параметри p та q не є взаємно простими, то ізоморфізму з дійсними числами не існує.

Приклад 2. Для комплексних чисел $\dot{a}=25-22i$ та $\dot{b}=8+3i$ з прикладу 1 знайти дійсне число x, для якого виконується рівність $\dot{a}\bmod\dot{b}=x$.

Тут $\rho=-1\cdot 3-3\cdot 8=-27$, оскільки при $u=-1$ та $v=3$ виконується рівняння $u\cdot 8+v\cdot 3=1$. Тоді $x=\left(25-22\cdot(-27)\right)\bmod N(\dot{b})=619\bmod 73=35.$ Отже, $(25-22i)\bmod(8+3i)=35$.

Для знаходження дійсного залишку $\dot{a}\bmod\dot{b}=x$ за комплексним модулем можна скористатися рівняннями (1). Якщо вважати, що $y=0$ в $x+yi$, то отримаємо систему рівнянь:

$$\begin{cases}(ap+bq)\bmod N(\dot{b})=xp,\\(bp-aq)\bmod N(\dot{b})=-xq.\end{cases}\qquad(4)$$

Для знаходження дійсного числа x достатньо розв'язати одне з рівнянь системи (4), які є конгруенціями першого степеню відносно змінної x.

Дослідимо всі можливі випадки розв'язування, наприклад, першої в (4) лінійної конгруенції, переписавши її для зручності в такому вигляді:

$$px\bmod N(\dot{b})=ap+bq.\qquad(5)$$

I. Якщо для дійсних чисел p і q з рівняння (5) $НСД(p,q)=1$, то $НСД(p,N(\dot{b}))=1$. Тоді з теорії конгруенцій для (5) існує єдиний дійсний розв'язок $x<N(\dot{b})$.

II. Якщо $НСД(p,q)=d$, $d>1$, то $НСД(p,N(\dot{b}))=d$. Оскільки $ap+bq$ завжди ділиться націло на d, то конгруенція (5) має d розв'язків –

різних класів залишків за модулем $N(\dot{b})$. Дійсно, якщо $p = p_1 d$, $q = q_1 d$, то поділивши обидві частини конгруенції (5) та модуль на *d*, отримаємо:

$$p_1 x \bmod N_1 = a p_1 + b q_1, \qquad (6)$$

де $N_1 = d(p_1^2 + q_1^2)$, $НСД(p_1, q_1) = 1$, що рівносильно випадку I.

Розв'язавши конгруенцію (6) отримаємо d розв'язків конгруенції (5), тобто d дійсних залишків числа $\dot{a} = a + bi$ за модулем $\dot{b} = p + qi$: x, $x+$, N_1, …, $x+(d-1)N_1$; $x < N_1$.

Приклад 3. Для числа $\dot{a} = 25 - 22i$ знайти дійсний залишок за модулем $\dot{b} = 8 + 3i$.

На відміну від прикладу 2, пошук залишку здійснимо за формулою (5). Оскільки $НСД(8,3) = 1$, то $НСД(8,73) = 1$, $ap+bq$=25·8-22·3=134 і конгруенція $8x \bmod 73 = 134$ має єдиний розв'язок, який знайдемо за допомогою теореми Ейлера $x = 8^{\varphi(73)-1} \cdot 134 \bmod 73 = 8^{71} \cdot 134 \bmod 73 = 35$. Отже, $(25-22i) \bmod (8+3i) = 35$, причому $35 < N(\dot{b})$.

Тепер для $\dot{a} = 25 - 22i$ візьмемо модуль $\dot{b} = 6 + 4i$, для якого $(6,4) = 2$. Тоді за (6) отримаємо конгруенцію $3x \bmod 26 = 31$, яка має розв'язок $x = 3^{\varphi(26)-1} \cdot 31 \bmod 26 = 3^{11} \cdot 31 \bmod 26 = 19$. Конгруенція $6x \bmod 52 = 62$ має два розв'язки $x = 19$ та $x = 19 + 31 = 45$. Отже, $(25-22i) \bmod (6+4i) = 19$, $19 < N(\dot{b})$ або $(25-22i) \bmod (6+4i) = 45$, $45 < N(\dot{b})$.

Алгоритм Евкліда для комплексних чисел

Число $\dot{d}$ називається спільним дільником комплексних чисел $\dot{a}$ та $\dot{b}$, відмінних від нуля, якщо кожне з цих чисел ділиться на $\dot{d}$. Число $\dot{D} = НСД(\dot{a}, \dot{b})$ називається найбільшим спільним дільником комплексних чисел $\dot{a}$ та $\dot{b}$, відмінних від нуля, якщо $\dot{D}$ є спільним дільником із найбільшою нормою.

Зауважимо, якщо $\dot{D} = НСД(\dot{a}, \dot{b})$, то найбільшими спільними дільниками також будуть числа $-\dot{D}$, $\dot{D}i$, $-\dot{D}i$.

Числа $\dot{a}$ та $\dot{b}$ називаються взаємно простими, якщо їх НСД дорівнює одній з тривіальних одиниць.

Для знаходження НСД для комплексних чисел $\dot{a}$ та $\dot{b}$, відмінних від нуля, можна скористатися алгоритмом Евкліда:

$$\begin{aligned}
&\dot{a} = \dot{b}\dot{q}_1 + \dot{r}_1, \quad N(\dot{r}_1) < N(\dot{b}),\\
&\dot{b} = \dot{r}_1\dot{q}_2 + \dot{r}_2, \quad N(\dot{r}_2) < N(\dot{r}_1),\\
&\dot{r}_1 = \dot{r}_2\dot{q}_3 + \dot{r}_3, \quad N(\dot{r}_3) < N(\dot{r}_2),\\
&\cdots\cdots\cdots\cdots\\
&\dot{r}_{n-2} = \dot{r}_{n-1}\dot{q}_n + \dot{r}_n, \quad N(\dot{r}_n) < N(\dot{r}_{n-1}),\\
&\dot{r}_{n-1} = \dot{r}_n\dot{q}_{n+1}.
\end{aligned}$$

Звідси $НСД(\dot{a}, \dot{b}) = \dot{r}_n$, тобто остання, відмінна від нуля, остача, є найбільшим спільним дільником.

Приклад 4. Довести, що числа $38+9i$ та $3+12i$ є взаємно простими.

Використаємо алгоритм Евкліда. При діленні комплексних чисел із абсолютно найменшими залишками отримаємо:

$$\begin{aligned}
&38+9i = (3+12i)(1-3i) + (-1+6i),\\
&3+12i = (-1+6i)(2-i) + (-1-i),\\
&-1+6i = (-1-i)(-3-4i) + (-i),\\
&-1-i = -i(1-i) + 0.
\end{aligned}$$

Останній відмінний від нуля залишок дорівнює $-i$, тому числа $38+9i$ та $3+12i$ мають лише спільні тривіальні множники і є взаємно простими.

Приклад 5. Довести, що числа $\dot{a} = 38+9i$ та $\dot{b} = 4+12i$ є взаємно простими. Знову скористаємося алгоритмом Евкліда (залишки вибираємо абсолютно найменші):

$$\begin{aligned}
&38+9i = (4+12i)(1-2i) + (4+5i),\\
&4+12i = (4+5i)(2+i) + (1-2i),\\
&4+5i = (1-2i)(-1+3i) + (-1),\\
&1-2i = -1(-1+2i) + 0.
\end{aligned}$$

Останній відмінний від нуля залишок становить -1, тому числа $\dot{a}$ та $\dot{b}$ є взаємно простими.

Якщо $\dot{D}$ є найбільшим спільним дільником чисел $\dot{a}$ та $\dot{b}$, то $N(\dot{D})$ є дільником для $N(\dot{a})$, $N(\dot{b})$ і $НСД(N(\dot{a}), N(\dot{b}))$. Тоді $N(\dot{D}) \le НСД(N(\dot{a}), N(\dot{b}))$. В прикладі 5 $\dot{a}$ і $\dot{b}$ є взаємно простими, найбільший спільний дільник яких має норму рівну 1. Але $N(38+9i) = 1525 = 5^2 \cdot 61$, $N(4+12i) = 160 = 2^5 \cdot 5$ і $(N(\dot{a}), N(\dot{b})) = 5$.

Якщо $НСД(N(\dot{a}), N(\dot{b})) = 1$, то $N(\dot{D}) = 1$ і $\dot{D}$ є тривіальною одиницею. В прикладі 4 $N(38+$

$9i) = 1525 = 5^2 \cdot 61$, $N(3+12i) = 153 = 3^2 \cdot 17$ є взаємно простими, тобто $НСД(N(\dot{a}), N(\dot{b})) = 1$.

Отже, якщо комплексні числа мають взаємно прості норми, то вони взаємно прості. Цю умову можна використовувати для перевірки взаємної простоти комплексних чисел. Обернене твердження невірне.

Приклад 6. Знайти НСД чисел $\dot{a} = 32 + 6i$ та $\dot{b} = 2 + 11i$.

Використаємо алгоритм Евкліда (залишки вибираємо абсолютно найменші):

$$32 + 6i = (2 + 11i)(1 - 3i) + (-3 + i),$$
$$2 + 11i = (-3 + i)(-4i) + (-2 - i),$$
$$-3 + i = (-2 - i)(1 - 4i) + 0.$$

отже, $НСД(\dot{a}, \dot{b}) = -2 - i$. На другому кроці алгоритму Евкліда при діленні $2 + 11i$ та $-3 + i$ ми отримали співвідношення для знаходження залишку:

$$\begin{cases} 5 \bmod 10 = 5 = r, \\ -35 \bmod 10 = 5 = r'. \end{cases}$$

Якщо ж вибрати інші дійсні залишки, наприклад, $r = -5$, $r' = -5$, то отримаємо інший розклад:

$$32 + 6i = (2 + 11i)(1 - 3i) + (-3 + i),$$
$$2 + 11i = (-3 + i)(1 - 3i) + (2 + i),$$
$$-3 + i = (2 + i)(-1 + 4i) + 0.$$

Отже, $НСД(\dot{a}, \dot{b}) = 2 + i$. Числа $-1 + 2i$ та $1 - 2i$ також будуть НСД для $\dot{a}$ та $\dot{b}$, Кожен із наведених чотирьох НСД можна отримати з іншого множенням на одну з тривіальних одиниць. Для комплексних чисел $\dot{a}$ та $\dot{b}$ також має місце співвідношення Безу

$$\dot{D} = \dot{a}\dot{x} + \dot{b}\dot{y}, \qquad (7)$$

де $\dot{D} = НСД(\dot{a}, \dot{b})$, $\dot{x}$, $\dot{y}$ – деякі комплексні числа.

Приклад 7. В прикладі 6 показати, що *НСД* $(\dot{a} = 32 + 6i, \dot{b} = 2 + 11i) = -2 - i$. Використаємо обернені підстановки в алгоритмі Евкліда:

$$-2 - i = 2 + 11i - (-3 + i)(-4i) =$$
$$2 + 11i - \big(32 + 6i - (2 + 11i)(1 - 3i)\big)(-4i) =$$
$$= (2 + 11i)(1 + (1 - 3i)4i) + (32 + 6i)4i =$$
$$\dot{a}4i + \dot{b}(13 + 4i).$$

Отже, найбільший спільний дільник $-2 - i$ є лінійною комбінаціє (7) комплексних чисел $\dot{a}$ та $\dot{b}$. Якщо $\dot{a}$ та $\dot{b}$ взаємно прості, то (7) буде мати вигляд:

$$1 = \dot{a}\dot{x} + \dot{b}\dot{y}. \qquad (8)$$

Число $\dot{x}$ називається мультиплікативно оберненим до числа $\dot{a}$ за модулем $\dot{b}$, якщо для взаємно простих $\dot{a}$ та $\dot{b}$ виконується конгруенція $(\dot{a} \cdot \dot{x}) \bmod \dot{b} = 1$ і позначається $\dot{x} = \dot{a}^{-1} \bmod \dot{b}$.

Якщо $\dot{a}$ та $\dot{b}$ не є взаємно простими, то мультиплікативно оберненого числа до $\dot{a}$ не існує. Якщо $\dot{b}$ – просте число, то для $\dot{a}$ завжди можна знайти мультиплікативно обернене число при умові, що $\dot{a}$ не ділиться на $\dot{b}$. У прикладі 6 не існує оберненого числа до числа $2 + 11i$ за модулем $32 + 6i$, оскільки вони мають спільний дільник $-2 - i$.

Приклад 8. Знайти обернене число до $\dot{a} = 3 + 12i$ за модулем $\dot{b} = 38 + 9i$ за допомогою алгоритму Евкліда.

Порівняємо виконання операцій ділення з абсолютно найменшими та найменшими додатними залишками (табл. 2).

Таблиця 2

Знаходження найбільшого спільного дільника
за Алгоритмом Евкліда

з абсолютно найменшими залишками	з найменшими додатними залишками
$38 + 9i = (3 + 12i)(1 - 3i) +$ $(-1 + 6i), 3 + 12i =$ $(-1 + 6i)(2 - i) + (-1 - i),$ $-1 + 6i = (-1 - i)(-3 - 4i) +$ $(-i), -1 - i = -i(1 - i) + 0;$	$38 + 9i = (3 + 12i)(1 - 3i) + (-1 + 6i),$ $3 + 12i = (-1 + 6i)(1 - i) + (-2 + 5i),$ $-1 + 6i = (-2 + 5i)(1 - i) + (-4 - i),$ $-2 + 5i = (-4 - i)(-2i) + (-3i),$ $-4 - i = -3i(-2i) + 2 - i,$ $-3i = (2 - i)(-2i) + 2 - i,\ 2 - i = (2 + i)(-i) + 1 + i,$ $2 + i = (1 + i)(1 - i) + i,\ 1 + i = i(1 - i) + 0;$

$-i=-1+6i-(-1-i)(-3-4i)=$ $=-1+6i-\left(\dot{a}-(-1+6i)(2-i)\right)(-3-4i)=$ $=(-1+6i)\left(1+(2-i)(-3-4i)\right)-\dot{a}(-3-4i)=$ $=\left(\dot{b}-\dot{a}(1-3i)\right)(-9-5i)-\dot{a}(-3-4i)=$ $=\dot{a}(27-18i)+\dot{b}(-9-5i);$	$i=\dot{a}(20-11i)+\dot{b}(-6-4i);$
$1=\dot{a}(18+27i)+\dot{b}(5-9i),$ $N(18+27i)=1053<N(\dot{b})=1525;$	$1=\dot{a}(-11-20i)+\dot{b}(-4+6i),$ $N(-11-20i)=521<N(\dot{b})=1525;$
$\dot{x}=\dot{a}^{-1}\bmod\dot{b}=(18+27i)\bmod\dot{b}=-11-20i;$	$\dot{x}=\dot{a}^{-1}\bmod\dot{b}=-11-20i.$

Наведені розрахунки ще раз демонструють суттєве збільшення кількості арифметичних операцій при виборі найменших додатних залишків.

Функція Ейлера для комплексного числа

Будь-яке комплексне число $\dot{a}$ з $N(\dot{a})>1$ можна однозначно записати як добуток простих комплексних чисел з точністю до перестановки множників та множення на тривіальну одиницю, тобто

$$\dot{a}=i^k\prod_{i=1}^{n}\dot{p}_i^{n_i},\ k=\overline{0,3},$$

де n,n_i – невід'ємні цілі числа.

Для комплексних цілих чисел можна розглядати функцію $\varphi(\dot{p})$, яка є аналогом функції Ейлера для натуральних чисел. Її значення для комплексного цілого числа $\dot{p}$ дорівнює кількості взаємно обернених комплексних чисел за модулем $\dot{p}$.

Оскільки взаємно обернені числа можна знайти лише для взаємно простих чисел, то значення $\varphi(\dot{p})$ дорівнює кількості взаємно простих чисел за модулем $\dot{p}$.

Функція $\varphi(\dot{p})$ мультиплікативна, тобто для взаємно простих чисел $\dot{a}$ та $\dot{b}$ має місце рівність $\varphi(\dot{a}\dot{b})=\varphi(\dot{a})\varphi(\dot{b})$.

Якщо $\dot{p}$ – просте число, то:

$$\varphi(\dot{p})=N(\dot{p})-1,$$

$$\varphi(\dot{p}^n)=N(\dot{p})^n\left(1-\frac{1}{N(\dot{p})}\right)=N(\dot{p})^{n-1}\left(N(\dot{p})-1\right),$$

$$n\in N.$$

Для довільного комплексного числа $\dot{z}=\dot{p}_1^{n_1}\dot{p}_2^{n_2}\dots\dot{p}_k^{n_k}$, де $\dot{p}_i$ прості числа, $n_i\in N$, за властивістю мультиплікативності

$$\varphi(\dot{z})=\varphi(\dot{p}_1^{n_1})\varphi(\dot{p}_2^{n_2})\dots\varphi(\dot{p}_k^{n_k})=$$
$$=N(\dot{p}_1)^{n_1}\left(1-\frac{1}{N(\dot{p}_1)}\right)N(\dot{p}_2)^{n_2}$$
$$\left(1-\frac{1}{N(\dot{p}_2)}\right)\dots N(\dot{p}_k)^{n_k}\left(1-\frac{1}{N(\dot{p}_k)}\right)=$$
$$=N(\dot{p}_1)^{n_1}N(\dot{p}_2)^{n_2}\dots N(\dot{p}_k)^{n_k}\left(1-\frac{1}{N(\dot{p}_1)}\right)$$
$$\left(1-\frac{1}{N(\dot{p}_2)}\right)\dots\left(1-\frac{1}{N(\dot{p}_k)}\right)=N(\dot{z})\prod_{i=1}^{k}\left(1-\frac{1}{N(\dot{p}_i)}\right).$$

На практиці зручніше користуватися формулою:

$$\varphi(\dot{z})=N(\dot{p}_1)^{n_1-1}\left(N(\dot{p}_1)-1\right)\cdot$$
$$N(\dot{p}_2)^{n_2-1}\left(N(\dot{p}_2)-1\right)\cdot\dots\cdot N(\dot{p}_k)^{n_k-1}\left(N(\dot{p}_k)-1\right).$$

Приклад 9. Обчислити $\varphi(15+20i)$.

Оскільки $15+20i=5(3+4i)=(1+2i)(1-2i)(2+i)^2$, то $\varphi(15+20i)=(5-1)\cdot(5-1)\cdot 5(5-1)=320$.

Якщо $\dot{a}$ та $\dot{p}$ взаємно прості, то має місце аналог теореми Ейлера з співвідношенням:

$$\dot{a}^{\varphi(\dot{p})}\bmod\dot{p}=1. \qquad (9)$$

Приклад 10. Обчислити $(1+2i)^{35}\bmod(3+5i)$.

Числа $1+2i$ та $3+5i$ є взаємно простими, оскільки норми $N(1+2i)=5$ та $N(3+5i)=34$ є взаємно прості. Розклад $34=2\cdot17$ на прості множники вказує на можливий розклад $3+5i=(1+i)(4+i)$. Тоді $\varphi(3+5i)=\varphi(1+i)\varphi(4+i)=(2-1)(17-1)=16$. Відповідно до (9) маємо конгруенцію $(1+2i)^{16}\bmod(3+5i)=1$. Підносячи до квадрату обидві частини конгруенції, отримуємо $(1+2i)^{32}\bmod(3+5i)=1$. Крім того, $(1+2i)^3\bmod(3+5i)=(-11-2i)\bmod(3+5i)=-3$. Отже, $(1+2i)^{32}\cdot(1+2i)^3\bmod(3+5i)=1\cdot(-3)=-3$.

Приклад 11. Довести, що числа $\dot{a}=5+3i$ та $\dot{b}=3+7i$ не є взаємно простими.

Оскільки $N(\dot{a})=34$ та $N(\dot{b})=58$ не взаємно прості, то зразу ж можна зробити висновок, що $\dot{a}$ та $\dot{b}$ не є взаємно простими. Підтвердимо це, використавши співвідношення (9), тобто покажемо, що $\dot{a}^{\varphi(\dot{b})} \bmod \dot{b} \neq 1$. $N(\dot{b})=58=2\cdot 29$, $\varphi(\dot{b})=(2-1)\cdot(29-1)=28$, тоді $\dot{x}=\dot{a}^{28} \bmod \dot{b}$.

Знайдемо наступні конгруенції:

$$\dot{a}^{1} \bmod \dot{b}=1+3i,$$
$$\dot{a}^{2} \bmod \dot{b}=(1+3i)^2 \bmod \dot{b}=-1+3i,$$
$$\dot{a}^{4} \bmod \dot{b}=(-1+3i)^2 \bmod \dot{b}=2-2i,$$
$$\dot{a}^{8} \bmod \dot{b}=(2-2i)^2 \bmod \dot{b}=3-i,$$
$$\dot{a}^{16} \bmod \dot{b}=(3-i)^2 \bmod \dot{b}=1-3i.$$

Оскільки $28=16+8+4=2^4+2^3+2^2$, то:

$$\dot{a}^{28} \bmod \dot{b}=\dot{a}^{16}\cdot\dot{a}^{8}\cdot\dot{a}^{4} \bmod \dot{b}=$$
$$(1-3i)(3-i)(2-2i) \bmod \dot{b}=$$
$$(-20-20i) \bmod \dot{b}=-4-2i\neq 1.$$

Отже, $\dot{a}$ та $\dot{b}$ не є взаємно простими.

В прикладі 11 здійснювалося дискретне піднесення до степеня. Обернена операція – дискретне логарифмування на множині комплексних чисел – виконується розв'язуванням рівняння $\dot{a}^{k} \bmod \dot{b}=\dot{c}$ відносно дійсного цілого k для простого числа $\dot{b}$. Найменший показник $k=\log_{\dot{a}} \dot{c} \bmod \dot{b}$ називається дискретним логарифмом з основою $\dot{a}$ за простим комплексним модулем $\dot{b}$, причому $0\le k<N(\dot{b})$.

Приклад 12. Знайти обернене число до $\dot{a}=3+12i$ за модулем $\dot{b}=34+9i$.

Використаємо рівність $\dot{x}=\dot{a}^{\varphi(\dot{b})-1} \bmod \dot{b}$, яка слідує з (9) та конгруенції $(\dot{a}\cdot\dot{x}) \bmod \dot{b}=1$, $(\dot{a},\dot{b})=1$. Тоді $\dot{x}=\dot{a}^{-1} \bmod \dot{b}$.

Оскільки число $N(\dot{b})=1237$ просте, то $\varphi(\dot{b})=1236$, тоді $\dot{x}=\dot{a}^{1236} \bmod \dot{b}$. Розглянемо розклад $1199=1024+128+32+8+4+1=2^{10}+2^7+2^5+2^3+2^2+2^0$ та обчислимо степені:

$$\dot{a}^{1} \bmod \dot{b}=3+12i,$$
$$\dot{a}^{2} \bmod \dot{b}=(3+12i)^2 \bmod \dot{b}=-6-3i,$$
$$\dot{a}^{4} \bmod \dot{b}=(-6-3i)^2 \bmod \dot{b}=2-7i,$$
$$\dot{a}^{8} \bmod \dot{b}=(2-7i)^2 \bmod \dot{b}=-11-19i,$$
$$\dot{a}^{16} \bmod \dot{b}=(-11-19i)^2 \bmod \dot{b}=13+12i,$$
$$\dot{a}^{32} \bmod \dot{b}=(13+12i)^2 \bmod \dot{b}=-5+13i,$$
$$\dot{a}^{64} \bmod \dot{b}=(-5+13i)^2 \bmod \dot{b}=-1+17i,$$
$$\dot{a}^{128} \bmod \dot{b}=(-1+17i)^2 \bmod \dot{b}=-7+4i,$$
$$\dot{a}^{256} \bmod \dot{b}=(-7+4i)^2 \bmod \dot{b}=15+12i,$$
$$\dot{a}^{512} \bmod \dot{b}=(15+12i)^2 \bmod \dot{b}=-8+9i.$$
$$\dot{a}^{1024} \bmod \dot{b}=(-8+9i)^2 \bmod \dot{b}=15+10i$$

Тоді обернений елемент шукається з конгруенції:

$$\dot{x}=\dot{a}^{1236} \bmod \dot{b}=(15+10i)(-7+4i)$$
$$(-1+17i)(13-4i)(13+12i)(2-7i) \bmod \dot{b}=$$
$$=(-129835-291155i) \bmod \dot{b}=12-12i.$$

Китайська теорема про залишки для комплексних чисел

Будь-яке комплексне число $\dot{A}$, представлене у позиційній системі числення, записується в системі залишкових класів (СЗК) єдиним способом у вигляді своїх найменших комплексних залишків $\dot{b}_i$ від ділення $\dot{A}$ на кожен із системи попарно взаємно простих комплексних модулів $\dot{m}_1$, $\dot{m}_2$, …, $\dot{m}_s$:

$$\dot{b}_i=\dot{A} \bmod \dot{m}_i,\ \ i=\overline{1,s}.$$

Відновлення числа $\dot{A}$ в позиційну систему числення можна здійснити на основі китайської теореми про залишки (КТЗ) в комплексній числовій області:

$$\dot{A}=\left(\sum_{i=1}^{s}\dot{b}_i\dot{M}_i\dot{f}_i\right) \bmod \dot{M}, \qquad (10)$$

де $\dot{M}=\prod_{i=1}^{s}\dot{m}_i$, $\dot{M}_i=\dfrac{\dot{M}}{\dot{m}_i}$, $\dot{f}_i$ шукається з виразу $\dot{f}_i=\dot{M}_i^{-1} \bmod \dot{m}_i$, s – кількість модулів. При цьому повинні виконуватися нерівності:

$$0\le ap_M+bq_M<N(\dot{M}),\ \ 0\le bp_M-aq_M<N(\dot{M}), \qquad (11)$$

де $\dot{M}=p_M+q_Mi$.

Застосуємо КТЗ до взаємно простих комплексних чисел $\dot{m}_1=2+i$, $\dot{m}_2=3+2i$, $\dot{m}_3=4+i$, які є основами системи $\dot{M}=\dot{m}_1\cdot\dot{m}_2\cdot\dot{m}_3=9+32i$. Спочатку число $\dot{A}=1+7i$ запишемо в СЗК у вигляді своїх найменших додатних комплексних залишків:

$$\dot{b}_1=\dot{A} \bmod \dot{m}_1=1+2i,\quad \dot{b}_2=\dot{A} \bmod \dot{m}_2=2i,$$
$$\dot{b}_3=\dot{A} \bmod \dot{m}_3=2+3i.$$

Для $\dot{M}_1 = \dot{m}_2 \cdot \dot{m}_3 = \frac{\dot{M}}{\dot{m}_1} = 10+11i$, $\dot{M}_2 = \dot{m}_1 \cdot \dot{m}_3 =$, $\frac{\dot{M}}{\dot{m}_2} = 7+6i$, $\dot{M}_3 = \dot{m}_1 \cdot \dot{m}_2 = \frac{\dot{M}}{\dot{m}_3} = 4+7i$ з конгруенцій $(\dot{M}_i \cdot \dot{f}_i) \bmod \dot{m}_i = 1$, $i = \overline{1,3}$ шукаються обернені елементи за відповідними модулями: $\dot{f}_1 = \dot{M}_1^{-1} \bmod \dot{m}_1 = 2$, $\dot{f}_2 = \dot{M}_2^{-1} \bmod \dot{m}_2 = 1+i$, $\dot{f}_3 = \dot{M}_3^{-1} \bmod \dot{m}_3 = -1+i$. Тут $N(\dot{M}) = 1105$ і виконуються обмеження (11): $ap_M + bq_M = 233 \in [0;1105)$, $bp_M - aq_M = 31 \in [0;1105)$.

Число $\dot{A}$ відновлюється у позиційну систему числення за формулою (10):

$$\dot{A} = \begin{pmatrix} (1+2i)(10+11i)2 + 2i(7+6i)(1+i) + \\ (2+3i)(4+7i)(-1+i) \end{pmatrix} \bmod 1105 =$$
$$= (-63+25i) \bmod 1105 = 1+7i.$$

Крім того, число $\dot{A} = 1+7i$ можна записати в СЗК у вигляді абсолютно найменших комплексних залишків:

$$\dot{b}_1 = \dot{A} \bmod \dot{m}_1 = -i, \quad \dot{b}_2 = \dot{A} \bmod \dot{m}_2 = 2i,$$
$$\dot{b}_3 = \dot{A} \bmod \dot{m}_3 = -1-2i.$$

В позиційну систему числення число $\dot{A}$ відновлюється за формулою (10) для тих самих обернених елементів f_1, f_2, f_3:

$$\dot{A} = \begin{pmatrix} -i(10+11i)2 + 2i(7+6i)(1+i) + \\ (-1-2i)(4+7i)(-1+i) \end{pmatrix} \bmod 1105 =$$
$$(1+7i) \bmod 1105 = 1+7i.$$

Можна помітити, що вибір абсолютно найменших залишків спрощує розрахунки при відновленні десяткового числа у порівнянні із вибором найменших додатних залишків. Для $\dot{A}$ також можна знайти дійсні залишки за модулями $\dot{m}_1$, $\dot{m}_2$, $\dot{m}_3$:

$$\dot{b}_1 = \dot{A} \bmod \dot{m}_1 = 2, \quad \dot{b}_2 = \dot{A} \bmod \dot{m}_2 = 10,$$
$$\dot{b}_3 = \dot{A} \bmod \dot{m}_3 = 7.$$

Знову ж за формулою (10) для тих самих обернених елементів f_1, f_2, f_3 в позиційну систему числення число $\dot{A}$ відновлюється таким чином:

$$\dot{A} = \begin{pmatrix} 2(10+11i)2 + 10(7+6i)(1+i) + \\ 7(4+7i)(-1+i) \end{pmatrix} \bmod 1105 =$$
$$(-27+153i) \bmod 1105 = 1+7i.$$

ВИСНОВКИ

В теорії та методології вирішення прикладних математичних задач захисту інформаційних потоків у сучасних комп'ютерних та кіберфізичних системах накопичено світовий досвід використання алгоритмів асиметричних криптосистем. Зокрема, можна розглянути нові підходи до асиметричного шифрування без зменшення їх стійкості до криптоаналізу. Одним із них є застосування більш складних полів із більшими циклічними групами, наприклад, цілих комплексних чисел або чисел Гауса.

У роботі розроблено теоретичні основи модулярних обчислень та асиметричної криптографії, зокрема, алгоритму Евкліда, його наслідку, пошуку оберненого елемента, китайської теореми про остачі, пошуку функції Ейлера в комплексній числовій області.

Розглянуті модулярні операції в полі комплексних чисел показують можливості їх застосування до більшості відомих криптоалгоритмів, які раніше були сформульовані для цілих чисел. При цьому перспективними є дослідження переваг застосування комплексних чисел для розробки високопродуктивних криптоалгоритмів, які дозволять забезпечити необхідний рівень захисту даних та більшу стійкість до криптоаналізу в порівнянні з класичними.

ЛІТЕРАТУРА

[1]. Дудикевич В., Микитин Г., Насилевський В., Фігурняк В. До питання безпечної багатофакторної аутентифікації у веб-застосунках. Захист інформації, 2023. Т. 25, № 2. С. 76-82.

[2]. Іванченко Є., Корченко О., Зарицький О., Зибін С., Вишневська Н. Аналіз поняття кіберстійкості критичної інфраструктури. Захист інформації, 2023. Т. 25, № 4. С. 221-233.

[3]. Adki V., Hatkar S. A Survey on Cryptography Techniques. International Journal of Advanced Research in Computer Science and Software Engineering, 2016. Vol. 6 (6). pp. 469-475.

[4]. Bajard J., Eynard J., Merkiche N. Multi-fault attack detection for RNS cryptographic architecture. Computer Arithmetic (ARITH 2016): Proceedings of the 23nd IEEE Symposium, Silicon Valley, CA, USA. 2016. pp. 16-23.

[5]. Havrylova A., Aksonova I., Khokhlachova Y., Milevska T., Dunaiev S. Rationale for improving authentication protocols in the conditions of post-quantum cryptography. Ukrainian Scientific Journal of Information Security, 2024. Vol. 30, issue 1. pp. 130-139.

[6]. Hayder R.H. H-Rabim Cryptosystem. Journal of Mathematics and Statistics, 2014. Vol. 10 (3). pp. 304-308.

[7]. Karpinski M., Rajba S., Zawislak S., Warwas K., Kasianchuk M., Ivasiev S., Yakymenko I. A Method for Decimal Number Recovery from its Residues Based on the Addition of the Product Modules. Proceedings of the 2019 IEEE 9th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS–2019). V.1. 2019. pp. 13-17.
[8]. Kasianchuk M., Yakymenko I., Ivasiev S. High-Productivity Methods of Finding Residues Multidigital Numbers By Modulo, in Inżynier XXI Wieku: VI Międzynarodowa Konferencja studentow oraz doktorantow, 02.12.2016: monografia, 1st ed., Bielsko, Biała (Poland): Akademia Techniczno-Humanistyczna w Bielsku-Białej, 2016, pp. 123-130. Chapter in monograph.
[9]. Nykolaychuk Ya.M., Kasianchuk M.M., Yakymenko I.Z. Theoretical Foundations for the Analytical Computation of Coefficients of Basic Numbers of Krestenson's Transformation. Cybernetics and Systems Analysis, 2014. Vol. 50, № 5. pp. 649-654.
[10]. Zhengbing Hu., Dychka I., Onai M., Bartkoviak A. The Analysis and Investigation of Multiplicative Inverse Searching Methods in the Ring of Integers Modulo M. International Journal of Intelligent Systems and Applications (IJISA), 2016. Vol. 8, №11. pp. 9-18.

ARITHMETIC OF ASYMMETRIC CRYPTOSYSTEMS IN THE FIELD OF COMPLEX NUMBERS

At the current stage of information technology development, there is a need to improve existing and develop new methods and means of increasing the productivity of asymmetric crypto-algorithms. The article develops the theoretical foundations of modular calculations and asymmetric cryptography in the complex numerical domain. The method of determining the complex and real residues based on the complex module is considered. Euclid's algorithm and its consequence for finding an inverse element in a complex numerical domain are considered. A comparison of the complexity of Euclid's algorithm for finding the inverse of the element when finding the smallest positive and absolutely smallest residues was made. An analogue of Euler's function in the complex numerical domain was searched and this function was used to find the inverse of a complex number. The restoration of a complex number using the Chinese remainder theorem is demonstrated. The considered modular calculations in the field of complex numbers can be used in the construction of new approaches to asymmetric encryption.

Keywords: asymmetric cryptosystem, complex number, Euclid's algorithm, Euler's function, residue number system.

Алілуйко Андрій Миколайович, к.фіз.-мат.н., доцент, доцент кафедри прикладної математики Західноукраїнського національного університету.
Andrii Aliluiko, Ph.D., associate professor, associate professor of the Department of Applied Mathematics, West Ukrainian National University.
E-mail: aliluyko82@gmail.com.
Orcid ID: 0000-0002-4650-9350.

Касянчук Михайло Миколайович, д.т.н., професор, професор кафедри кібербезпеки Західноукраїнського національного університету.
Mykhailo Kasianchuk, doctor of technical science, professor, professor of the Department of Cyber Security, West Ukrainian National University.
E-mail: kasyanchuk@ukr.net.
Orcid ID: 0000-0002-4469-8055.

DOI: 10.18372/2410-7840.26.18824
УДК 336.71:004.056

РОЗРОБКА МОДЕЛІ ЗАХИСТУ ОСОБИСТИХ ДАНИХ У СОЦІАЛЬНИХ МЕРЕЖАХ

Сергій Лаптєв

Десятки мільйонів людей по всьому світу щорічно стають жертвами крадіжок особистих даних. Користувачі мережі втрачають величезні гроші через шахраїв, які використовують їхні дані у незаконний спосіб, і жертвою цього може стати абсолютно будь-яка людина. Крадіжка особистих даних – це будь-який злочин, у якому зловмисник отримує дані іншої особи та використовує особистість жертви для шахрайства. Згідно з дослідженнями, в 2020 році викрадення даних завдало збитків у розмірі 16 мільярдів доларів 15,4 мільйонам споживачів у Сполучених Штатах. У тому ж році британська організація з запобігання шахрайства Cifas зафіксувала майже 173 тисячі випадків шахрайства, пов'язаних з особистими відомостями у Великобританії. Це найбільша кількість випадків шахрайства за останні 13 років. Тому проблема розробки та дослідження математичних моделей захисту особистих даних є дуже актуальною. Вирішенню завдання розробки моделі та дослідження стійкості системи захисту особистої інформації і присвячена робота. Важливим напрямком є слідкування за поведінкою динамічної системи захисту інформації. В роботі проаналізували, використовуючи методи якісної теорії диференціальних рівнянь, зокрема метод фазової площини, поведінку системи захисту інформації. За допомогою цього методу знаходять характеристики особливих точок, ізольованих замкнутих траєкторій і сепаратриси, що в свою чергу дозволяє оцінити динаміку дослі-