УДК 681.3.05:004.056.5
Здобувач П.Ю. Грицюк, магістр – НЛТУ України;
проф. Ю.І. Грицюк, д-р техн. наук – НУ "Львівська політехніка"

ОСОБЛИВОСТІ РЕАЛІЗАЦІЇ МАТРИЧНОЇ АФІННОЇ КРИПТОСИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

Розглядаються особливості розроблення надійної криптосистеми захисту інформації, яка поєднує матричні Афінні перетворення, багатораундові дії з різними ключами, а також перестановні алгоритми, що загалом дає змогу значно підвищити її криптостійкість до брутальних атак. Встановлено, що, порівняно з іншими методами захисту, класична криптографія гарантує захист інформації тільки за умов, якщо використано ефективний криптографічний алгоритм, а також дотримані умови секретності та цілісності ключів шифрування. Математично описано алгоритм шифрування/дешифрування інформації за допомогою багатораундової матричної Афінної перестановної криптосистеми з різними ключами шифрування на кожному раунді. Внаслідок проведеного криптоаналізу її стійкості встановлено, що розроблений алгоритм забезпечують достатню стійкість до брутальних атак навіть за значний проміжок часу при достатній продуктивності обчислювальних систем.

Ключові слова: захист інформації, шифрування/дешифрування, Афінна система підставлянь Цезаря, криптографічна система Хілла, монограмний і поліграмний шифр, матричні Афінні перетворення, перестановні алгоритми, криптоаналіз.

Вступ. Криптографічні перетворення інформації з використанням ключів шифрування призначені для приховування (відновлення) змісту інформації, підтвердження її достовірності, цілісності, авторства, дати створення тощо **[**3, 9**]**. Порівняно з іншими методами захисту класична криптографія гарантує захист інформації тільки за умов, якщо використано ефективний криптографічний алгоритм, а також дотримані умови секретності та цілісності ключів шифрування **[**1, 11**]**.

До класичних методів захисту інформації належить Афінна система підставлянь Цезаря і, як продовження, криптографічна система Лестера Хілла, в яких чітко виявлена спільність числових методів Афінних перетворень **[**12**]**. Однак, Афінна система **[**6**]**, будучи монограмним шифром простої заміни, є надзвичайно уразливою до атак, оскільки криптоаналітик шляхом частотного аналізу **[**9**]** чи повного перебору **[**11**]** може з'ясувати відповідність між двома будь-якими буквами початкового тексту і шифротексту. Водночас криптосистема Хілла **[**2, 10, 12**]**, хоча і є поліграмним шифром, також вразлива до атак на основі відкритих текстів, позаяк у алгоритмі використовуються лінійні матричні операції. Для збільшення його криптостійкості в алгоритм шифрування потрібно додати будь-які нелінійні операції **[**1**]**.

Свого часу комбінування лінійних операцій шифру Хілла і нелінійних математичних перетворень привело до створення підстановно-перестановної мережі Фейстеля **[**9**]**, в якій використовується ще й багатораундове виконання однотипних дій. Однак спробуємо дещо удосконалити Афінну криптосистему, особливо її матричний алгоритм, позаяк вона має ще багато прихованих можливостей. Тому розроблення надійної криптосистеми (де)шифрування інформації, яка б поєднувала матричні Афінні перетворення, а також багатораундові дії з різними ключами, є актуальним науковим завданням, результати реалізації якого продемонстровано в цій роботі.

Об'єкт дослідження – криптостійкість матричної Афінної системи перетворення інформації.

Предмет дослідження – методи і засоби удосконалення роботи багатораундової матричної Афінної криптосистеми захисту інформації.

Мета роботи полягає в розробленні надійної криптосистеми захисту інформації, яка поєднує матричні Афінні перетворення, багатораундові дії з різними ключами, а також перестановні алгоритми, що загалом дасть змогу значно підвищити її криптостійкість.

Для реалізації зазначеної мети потрібно виконати такі основні завдання:

1) здійснити реалізацію багатораундової матричної Афінної криптосистеми, яка мала б значно підвищити криптостійкість алгоритму шифрування;
2) здійснити реалізацію матричного перестановного алгоритму шифрування інформації, яка мала б дещо підвищити криптостійкість алгоритму шифрування;
3) здійснити реалізацію багатораундової матричної Афінної перестановної криптосистеми, яка мала б набагато підвищити криптостійкість алгоритму шифрування;
4) провести криптоаналіз багатораундової матричної Афінної перестановної криптосистеми;
5) зробити відповідні висновки та надати рекомендації щодо використання.

1. Реалізація багатораундової матричної Афінної криптосистеми

Нагадаємо, що алгебричний метод, який узагальнює Афінну систему підставлянь Цезаря, було сформульовано Лестером С. Хіллом для визначення *n*-грам **[**11**]**. Множина цілих чисел $\overline{Z}_m$, для якої визначені операції додавання, віднімання та множення за модулем *m*, є прикладом кільця *R*, тобто алгебричної системи пар елементів. Математичні перетворення в цій системі мають вигляд, який наведено у матричних співвідношеннях (2)-(3) **[**12**]**.

У розглянутій нижче матричній Афінній криптосистемі **[**5**]** використовуються такі матричні вирази для шифрування та дешифрування інформації:

$$\overline{\overline{K}} = \overline{\overline{A}} \underset{m}{\otimes} \overline{\overline{T}} \underset{m}{\oplus} \overline{B} \Rightarrow \overline{\overline{K}} = \left[\overline{K}_i = \left[k_{ij} = \sum_{l=1}^{n} a_{il} \underset{m}{\otimes} t_{lj} \underset{m}{\oplus} b_i,\ j = \overline{1, p} \right], i = \overline{1, n} \right]; \quad (1)$$

$$\overline{\overline{T}} = \overline{\overline{A}}' \underset{m}{\otimes} \overline{\overline{K}} \underset{m}{\oplus} \overline{B}' \Rightarrow \overline{\overline{T}} = \left[\overline{T}_i = \left[t_{ij} = \sum_{l=1}^{n} a'_{il} \underset{m}{\otimes} k_{lj} \underset{m}{\oplus} b'_i,\ j = \overline{1, p} \right], i = \overline{1, n} \right], \quad (2)$$

де: *m* – кількість символів алфавіту; $\overline{\overline{A}} = [\overline{A}_i = [a_{ij}, j = \overline{1, n}], i = \overline{1, n}]$ – матриця (ключ) шифрування, елементами якої є спеціально підібрані цілі числами з діапазону $1 \le a_{ij} < m$, а також НСД(*a*, *m*) = 1; $a = \det(\overline{\overline{A}}) \bmod m$ – визначник матриці $\overline{\overline{A}}$ за модулем *m*; $\overline{B} = [b_i, i = \overline{1, n}]$ – стовпець (ключ) коригування, елементами якого є цілі числами з діапазону $1 \le b_i < m$; $\overline{\overline{T}} = [\overline{T}_j = [t_{ij} = KodSym(s_{(i-1)\cdot p + j}), i = \overline{1, n}], j = \overline{1, p} : p \ge n]$ – матриця, елементами якої є числові коди символів вхідного повідомлення $\overline{S} = \{s_j, j = \overline{1, n \cdot p}\}$; $\overline{\overline{K}} = [\overline{K}_j = [k_{ij}, i = \overline{1, n}], j = \overline{1, p}]$ – матриця, елементами якої є числові коди символів зашифрованого повідомлення.

У виразах (1) і (2) символами $\underset{m}{\otimes}$ і $\underset{m}{\oplus}$ позначено відповідно множення та додавання елементів матриць за модулем *m*. Сучасне шифрування будь-якої вхідної інформації дає змогу використовувати розширену таблицю кодів ASCII, тобто значення елементів матриць $\bar{\bar{T}}$, $\bar{\bar{A}}$ і $\bar{B}$ можна встановлювати в межах від 1 до 255, при цьому кількість символів алфавіту *m* становитиме 256.

Для отримання зворотної матриці дешифрування $\bar{\bar{A}}' = [\bar{A}'_i = [a'_{ij},\ j = \overline{1,n}],\ i = \overline{1,n}]$ та зворотного стовпця коригування $\bar{B}' = [b'_i, i = \overline{1,n}]$ потрібно виконати такі дії. Насамперед знаходимо обернену матрицю $\bar{\bar{A}}^{-1} = [\bar{A}_i^{-1} = [a_{ij}^{-1},\ j = \overline{1,n}],\ i = \overline{1,n}]$ до матриці $\bar{\bar{A}}$, елементами якої є дійсні числами. Розв'язавши лінійне рівняння $a \cdot x + m \cdot y = 1$ за допомогою алгоритму Евкліда, знаходимо його корені *x* та *y*, внаслідок чого отримаємо $\det^{-1}(\bar{\bar{A}}) = x$. Тоді зворотне значення до визначника матриці $\bar{\bar{A}}$ становитиме $a' = \det^{-1}(\bar{\bar{A}}) \bmod m$. Звідси зворотну матрицю дешифрування знаходимо за таким виразом

$$\bar{\bar{A}}' = \bar{\bar{A}}^{-1} \underset{m}{\otimes} \det(\bar{\bar{A}}) \underset{m}{\otimes} a' \Rightarrow \bar{\bar{A}}' = [\bar{A}'_i = [a'_{ij} = (a_{ij}^{-1} \cdot \det(\bar{\bar{A}}) \cdot a') \bmod m,\ j = \overline{1,n}],\ i = \overline{1,n}]. \quad (3)$$

Для перевірки правильності отримання значень зворотної матриці дешифрування використовуємо такий матричний вираз $\bar{\bar{A}} \underset{m}{\otimes} \bar{\bar{A}}' = \bar{\bar{E}}$, де $\bar{\bar{E}}$ – одинична матриця.

Щоб отримати зворотний стовпець коригування $\bar{B}'$, потрібно виконати такі матричні дії:

$$\bar{B}' = -\bar{\bar{A}}' \underset{m}{\otimes} \bar{B} \Rightarrow \bar{B}' = \left[b'_i = -\sum_{j=1}^{n} a'_{ij} \underset{m}{\otimes} b_j, i = \overline{1,n} \right]. \quad (4)$$

У перетворенні (1), тобто при шифруванні вхідного повідомлення $\bar{\bar{T}}$, символи *n*-грами, яким відповідають числа *j*-го стовпця $\bar{T}_j$, замінюють на символи *n*-грами, що відповідають числовим значенням $(\bar{A}_i \times \bar{T}_j + b_i) \bmod m$, внаслідок чого отримуємо зашифроване повідомлення. При зворотному перетворенні (2), тобто дешифруванні повідомлення $\bar{\bar{K}}$, символи *n*-грами, яким відповідають числа *j*-го стовпця $\bar{K}_j$, замінюють на символи *n*-грами, що відповідають числовим значенням $(\bar{A}'_i \times \bar{K}_j + b'_i) \bmod m$.

Якщо до матричного виразу (1), який дає змогу зашифрувати повідомлення $\bar{\bar{T}}$, застосувати *R*-раундову процедуру шифрування і кожного разу з новими ключами $\bar{\bar{A}}_r, \bar{B}_r$ $(r \in R)$, то отримаємо багатораундову матричну Афінну криптосистему (де)шифрування інформації, аналогічну **[**5, 7**]**. Водночас, процес дешифрування інформації за виразом (2) також повторюватиметься *R* разів. У цьому випадку узагальнені вирази для прямого та зворотного перетворення багатораундової матричної Афінної криптосистеми будуть мати такий вигляд:

$$\bar{\bar{K}} = \underbrace{\bar{\bar{A}}_R \underset{m}{\otimes} \ldots \left(\bar{\bar{A}}_2 \underset{m}{\otimes} \left(\bar{\bar{A}}_1 \underset{m}{\otimes} \bar{\bar{T}} \underset{m}{\oplus} \bar{B}_1 \right) \underset{m}{\oplus} \bar{B}_2 \right) \ldots \underset{m}{\oplus} \bar{B}_R}_{R \text{ раундів}}; \quad (5)$$

$$\bar{\bar{T}} = \underbrace{\bar{\bar{A}}'_1 \underset{m}{\otimes} \ldots \left(\bar{\bar{A}}'_{R-1} \underset{m}{\otimes} \left(\bar{\bar{A}}'_R \underset{m}{\otimes} \bar{\bar{K}} \underset{m}{\oplus} \bar{B}'_R \right) \underset{m}{\oplus} \bar{B}'_{R-1} \right) \ldots \underset{m}{\oplus} \bar{B}'_1}_{R \text{ раундів}}; \quad (6)$$

$$a_r = \det(\bar{\bar{A}}_r) \bmod m;\ a'_r = \det^{-1}(\bar{\bar{A}}_r) \bmod m;\ \det^{-1}(\bar{\bar{A}}_r) = x_r,\ r = \overline{1,R}; \quad (7)$$

$$\bar{\bar{A}}'_r = \bar{\bar{A}}_r^{-1} \underset{m}{\otimes} \det(\bar{\bar{A}}_r) \underset{m}{\oplus} a'_r;\ \bar{B}'_r = -\bar{\bar{A}}'_r \underset{m}{\otimes} \bar{B}_r,\ r = \overline{1,R}, \quad (8)$$

де: $\bar{\bar{A}}_r, \bar{\bar{A}}'_r, r \in R$ – матриці (ключі) (де)шифрування для *r*-го раунду; $a_r, a'_r, r \in R$ – визначники матриць $\bar{\bar{A}}_r$ та $\bar{\bar{A}}'_r$ за модулем *m* для *r*-го раунду дії алгоритму, при цьому НСД(a_r, *m*) = 1 та НСД(a'_r, *m*) = 1; $\bar{B}_r, \bar{B}'_r, r \in R$ – стовпці (ключі) коригування для *r*-го раунду дії алгоритму (див. рис. 1).

2. Матричні перестановні алгоритми шифрування інформації

Якщо вхідне повідомлення подати у вигляді матриці $\bar{\bar{T}}$, елементами якої є натуральні числа з будь-якого діапазону, то, використовуючи перестановні матриці **[**5**]**, можна переставляти місцями елементи матриці $\bar{\bar{T}}$. Наприклад, при множенні вхідної матриці $\bar{\bar{T}}$ зліва та справа на відповідні перестановні матриці отримаємо перестановний алгоритм шифрування такого вигляду:

$$\bar{\bar{T}}^{\text{п}}_{\text{рс}} = \bar{\bar{P}}^{\text{п}}_{\text{р}} \times \bar{\bar{T}} \times \bar{\bar{P}}^{\text{п}}_{\text{с}}, \quad (9)$$

а зворотний алгоритм дешифрування матиме такий вигляд:

$$\bar{\bar{T}} = \bar{\bar{P}}'^{\text{п}}_{\text{р}} \times \left(\bar{\bar{T}}^{\text{п}}_{\text{рс}} \times \bar{\bar{P}}'^{\text{п}}_{\text{с}} \right), \quad (10)$$

де: $\bar{\bar{T}}$ – вхідна матриця розмірами $n \times p$; $\bar{\bar{P}}^{\text{п}}_{\text{р}}$, $\bar{\bar{P}}'^{\text{п}}_{\text{р}}$ та $\bar{\bar{P}}^{\text{п}}_{\text{с}}$, $\bar{\bar{P}}'^{\text{п}}_{\text{с}}$ – квадратні перестановні матриці відповідно рядків і стовпців вхідної матриці $\bar{\bar{T}}$ для прямого і зворотного ходів. Основу матричних виразів (9) і (10) становлять перестановні матриці $\bar{\bar{P}}^{\text{п}}$, в яких у кожному стовпці та в кожному рядку є тільки один елемент, який дорівнює 1, а всі інші – 0. Наприклад, нехай задана така перестановка

$$\tilde{\Pi} = \left\{ \pi_j,\ j = \overline{1,n} \right\} \Rightarrow \left\{ \begin{matrix} 1 & 2 & 3 & 4 & 5 \\ \mathbf{4}, & \mathbf{3}, & \mathbf{5}, & \mathbf{1}, & \mathbf{2} \end{matrix} \right\}. \quad (11)$$

Тоді перестановна матриця шифрування матиме такий вигляд:

$$\bar{\bar{P}}^{\text{п}} = \left[\bar{P}_i^{\text{п}} = \left[p_{ij}^{\text{п}} = \begin{cases} \mathbf{1}, \text{ якщо } \pi_j = i; \\ 0, \text{ якщо } \pi_j \neq i, \end{cases} j = \overline{1,n} \right], i = \overline{1,n} \right] = \begin{array}{c|ccccc} & \mathbf{4} & \mathbf{3} & \mathbf{5} & \mathbf{1} & \mathbf{2} \\ \hline 1 & 0 & 0 & 0 & \mathbf{1} & 0 \\ 2 & 0 & 0 & 0 & 0 & \mathbf{1} \\ 3 & 0 & \mathbf{1} & 0 & 0 & 0 \\ 4 & \mathbf{1} & 0 & 0 & 0 & 0 \\ 5 & 0 & 0 & \mathbf{1} & 0 & 0 \end{array}. \quad (12)$$

Водночас зворотна перестановна матриця дешифрування матиме такий вигляд:

$$\bar{\bar{P}}'^{\text{п}} = \left[\bar{P}'^{\text{п}}_i = \left[p'^{\text{п}}_{ij} = \begin{cases} \mathbf{1}, \text{ якщо } \pi_i = j; \\ 0, \text{ якщо } \pi_i \neq j, \end{cases} j = \overline{1,n} \right], i = \overline{1,n} \right] = \begin{array}{c|ccccc} & 1 & 2 & 3 & 4 & 5 \\ \hline \mathbf{4} & 0 & 0 & 0 & \mathbf{1} & 0 \\ \mathbf{3} & 0 & 0 & \mathbf{1} & 0 & 0 \\ \mathbf{5} & 0 & 0 & 0 & 0 & \mathbf{1} \\ \mathbf{1} & \mathbf{1} & 0 & 0 & 0 & 0 \\ \mathbf{2} & 0 & \mathbf{1} & 0 & 0 & 0 \end{array}. \quad (13)$$

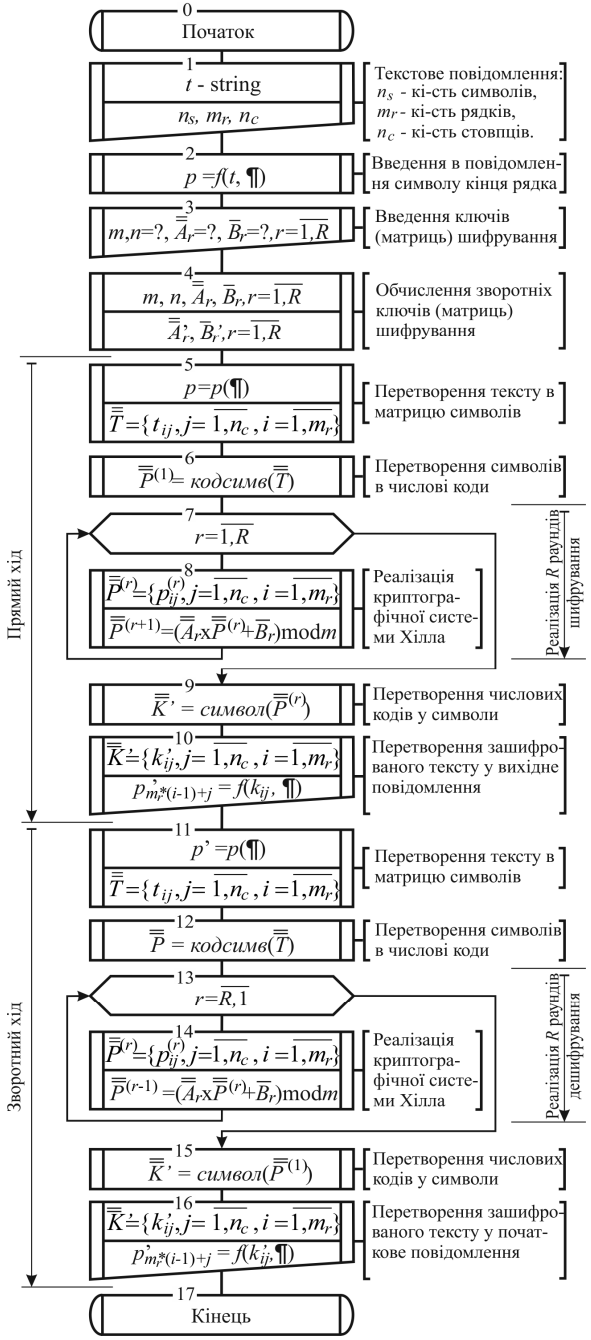

Рис. 1. Алгоритм реалізації багатораундової матричної Афінної криптосистеми

Нижче наведено приклад реалізації матричних виразів (9) і (10).

$\bar{\bar{P}}_{\text{р}}^{\text{п}}$

0	0	0	**1**	0
0	0	0	0	**1**
0	**1**	0	0	0
1	0	0	0	0
0	0	**1**	0	0

$\times$

$\bar{\bar{T}}$

247	223	26	104	249
32	143	98	187	86
191	152	188	135	16
236	50	235	146	217
178	12	28	134	242

$\times$

$\bar{\bar{P}}_{\text{с}}^{\text{п}}$

0	0	0	**1**	0
0	0	0	0	**1**
0	**1**	0	0	0
1	0	0	0	0
0	0	**1**	0	0

$=$

$\bar{\bar{T}}_{\text{рс}}^{\text{п}}$

146	235	217	236	50
134	28	242	178	12
187	98	86	32	143
104	26	249	247	223
135	188	16	191	152

$\bar{\bar{P}}_{\text{р}}^{\text{п}}$

0	0	0	**1**	0
0	0	**1**	0	0
0	0	0	0	**1**
1	0	0	0	0
0	**1**	0	0	0

$\times$

$\bar{\bar{T}}_{\text{рс}}^{\text{п}}$

146	235	217	236	50
134	28	242	178	12
187	98	86	32	143
104	26	249	247	223
135	188	16	191	152

$\times$

$\bar{\bar{P}}_{\text{с}}^{\text{п}}$

0	0	0	**1**	0
0	0	**1**	0	0
0	0	0	0	**1**
1	0	0	0	0
0	**1**	0	0	0

$=$

$\bar{\bar{T}}$

247	223	26	104	249
32	143	98	187	86
191	152	188	135	16
236	50	235	146	217
178	12	28	134	242

Однак, при такому поданні перестановних алгоритмів шифрування інформації використовується не вся множина можливих перестановок, оскільки елементи рядків чи стовпців матриці перемішуються за певними правилами **[**5**]**. Проблема полягає тут у такому.

Потужність множини всіх можливих матриць $\bar{\bar{P}}^{\text{п}}$ розміром $n \times n$ визначається за формулою $N = f(n) = n!$. Наприклад, кількість перестановних матриць розміром 5×5 становитиме 5!=1·2·3·4·5=120шт. Набори всіх можливих перестановок з 5 елементів показано нижче.

Набори всіх можливих перестановок з 5 елементів

	1	2	3	4	5
1	1	2	3	4	5
2	1	2	3	5	4
3	1	2	4	3	5
4	1	2	4	5	3
5	1	2	5	3	4
6	1	2	5	4	3
7	1	3	2	4	5
8	1	3	2	5	4
9	1	3	4	2	5
10	1	3	4	5	2
11	1	3	5	2	4
12	1	3	5	4	2
13	1	4	2	3	5
14	1	4	2	5	3
15	1	4	3	2	5
16	1	4	3	5	2
17	1	4	5	2	3
18	1	4	5	3	2
19	1	5	2	3	4
20	1	5	2	4	3
21	1	5	3	2	4
22	1	5	3	4	2
23	1	5	4	2	3
24	1	5	4	3	2

	1	2	3	4	5
25	2	1	3	4	5
26	2	1	3	5	4
27	2	1	4	3	5
28	2	1	4	5	3
29	2	1	5	3	4
30	2	1	5	4	3
31	2	3	1	4	5
32	2	3	1	5	4
33	2	3	4	1	5
34	2	3	4	5	1
35	2	3	5	1	4
36	2	3	5	4	1
37	2	4	1	3	5
38	2	4	1	5	3
39	2	4	3	1	5
40	2	4	3	5	1
41	2	4	5	1	3
42	2	4	5	3	1
43	2	5	1	3	4
44	2	5	1	4	3
45	2	5	3	1	4
46	2	5	3	4	1
47	2	5	4	1	3
48	2	5	4	3	1

	1	2	3	4	5
49	3	1	2	4	5
50	3	1	2	5	4
51	3	1	4	2	5
52	3	1	4	5	2
53	3	1	5	2	4
54	3	1	5	4	2
55	3	2	1	4	5
56	3	2	1	5	4
57	3	2	4	1	5
58	3	2	4	5	1
59	3	2	5	1	4
60	3	2	5	4	1
61	3	4	1	2	5
62	3	4	1	5	2
63	3	4	2	1	5
64	3	4	2	5	1
65	3	4	5	1	2
66	3	4	5	2	1
67	3	5	1	2	4
68	3	5	1	4	2
69	3	5	2	1	4
70	3	5	2	4	1
71	3	5	4	1	2
72	3	5	4	2	1

	1	2	3	4	5
73	4	1	2	3	5
74	4	1	2	5	3
75	4	1	3	2	5
76	4	1	3	5	2
77	4	1	5	2	3
78	4	1	5	3	2
79	4	2	1	3	5
80	4	2	1	5	3
81	4	2	3	1	5
82	4	2	3	5	1
83	4	2	5	1	3
84	4	2	5	3	1
85	4	3	1	2	5
86	4	3	1	5	2
87	4	3	2	1	5
88	4	3	2	5	1
89	4	3	5	1	2
90	4	3	5	2	1
91	4	5	1	2	3
92	4	5	1	3	2
93	4	5	2	1	3
94	4	5	2	3	1
95	4	5	3	1	2
96	4	5	3	2	1

	1	2	3	4	5
97	5	1	2	3	4
98	5	1	2	4	3
99	5	1	3	2	4
100	5	1	3	4	2
101	5	1	4	2	3
102	5	1	4	3	2
103	5	2	1	3	4
104	5	2	1	4	3
105	5	2	3	1	4
106	5	2	3	4	1
107	5	2	4	1	3
108	5	2	4	3	1
109	5	3	1	2	4
110	5	3	1	4	2
111	5	3	2	1	4
112	5	3	2	4	1
113	5	3	4	1	2
114	5	3	4	2	1
115	5	4	1	2	3
116	5	4	1	3	2
117	5	4	2	1	3
118	5	4	2	3	1
119	5	4	3	1	2
120	5	4	3	2	1

Дослідження властивостей перестановних матриць показує, що їхня множина із асоціативною операцією множення (×) (наприклад, $\bar{\bar{P}}_3^{\text{п}} \times \bar{\bar{P}}_7^{\text{п}} = \bar{\bar{P}}_{13}^{\text{п}}$ або $\bar{\bar{P}}_{10}^{\text{п}} \times \bar{\bar{P}}_{28}^{\text{п}} = \bar{\bar{P}}_{53}^{\text{п}}$, див. нижче) є групою, оскільки в ній є нейтральний елемент – одинична матриця $\bar{\bar{P}}_1^{\text{п}}$, а для кожного елемента $\bar{\bar{P}}_i^{\text{п}}$ існує зворотний $\bar{\bar{P}}_j'^{\text{п}}$ (наприклад, для матриці $\bar{\bar{P}}_{33}^{\text{п}}$ зворотною є матриця $\bar{\bar{P}}_{73}^{\text{п}}$, бо $\bar{\bar{P}}_{33}^{\text{п}} \times \bar{\bar{P}}_{73}^{\text{п}} = \bar{\bar{P}}_1^{\text{п}}$). Окрім цього, операція множення (×) є "некомутативною", оскільки $\bar{\bar{P}}_3^{\text{п}} \times \bar{\bar{P}}_7^{\text{п}}$ не дорівнює $\bar{\bar{P}}_7^{\text{п}} \times \bar{\bar{P}}_3^{\text{п}}$. Можна також зауважити, що в наборі перестановних матриць матриця $\bar{\bar{P}}_1^{\text{п}}$ не робить жодної перестановки, водночас як матриця $\bar{\bar{P}}_{120}^{\text{п}}$, яка є її дзеркальним відображенням (інверсією), робить зворотну перестановку елементів. Отже, не всі матриці з зазначеної множини можуть використовуватися для виконання перестановок рядків чи стовпців матриці **[**5**]**.

Приклади множення перестановних матриць з набору

P_3	1	2	4	3	5
1	**1**	0	0	0	0
2	0	**1**	0	0	0
3	0	0	0	**1**	0
4	0	0	**1**	0	0
5	0	0	0	0	**1**

×

P_7	1	3	2	4	5
1	**1**	0	0	0	0
2	0	0	**1**	0	0
3	0	**1**	0	0	0
4	0	0	0	**1**	0
5	0	0	0	0	**1**

=

P_{13}	1	4	2	3	5
1	**1**	0	0	0	0
2	0	0	**1**	0	0
3	0	0	0	**1**	0
4	0	**1**	0	0	0
5	0	0	0	0	**1**

P_{10}	1	3	4	5	2
1	**1**	0	0	0	0
2	0	0	0	0	**1**
3	0	**1**	0	0	0
4	0	0	**1**	0	0
5	0	0	0	**1**	0

×

P_{28}	2	1	4	5	3
1	0	**1**	0	0	0
2	**1**	0	0	0	0
3	0	0	0	0	**1**
4	0	0	**1**	0	0
5	0	0	0	**1**	0

=

P_{53}	3	1	5	2	4
1	0	**1**	0	0	0
2	0	0	0	**1**	0
3	**1**	0	0	0	0
4	0	0	0	0	**1**
5	0	0	**1**	0	0

P_{33}	2	3	4	1	5
1	0	0	0	**1**	0
2	**1**	0	0	0	0
3	0	**1**	0	0	0
4	0	0	**1**	0	0
5	0	0	0	0	**1**

-->

P_{33}^{-1}	1	2	3	4	5
2	0	**1**	0	0	0
3	0	0	**1**	0	0
4	0	0	0	**1**	0
1	**1**	0	0	0	0
5	0	0	0	0	**1**

-->

P_{73}	4	1	2	3	5
1	0	**1**	0	0	0
2	0	0	**1**	0	0
3	0	0	0	**1**	0
4	**1**	0	0	0	0
5	0	0	0	0	**1**

P_{33}	2	3	4	1	5
1	0	0	0	**1**	0
2	**1**	0	0	0	0
3	0	**1**	0	0	0
4	0	0	**1**	0	0
5	0	0	0	0	**1**

×

P_{73}	4	1	2	3	5
1	0	**1**	0	0	0
2	0	0	**1**	0	0
3	0	0	0	**1**	0
4	**1**	0	0	0	0
5	0	0	0	0	**1**

=

P_1	1	2	3	4	5
1	**1**	0	0	0	0
2	0	**1**	0	0	0
3	0	0	**1**	0	0
4	0	0	0	**1**	0
5	0	0	0	0	**1**

P_7	1	3	2	4	5
1	**1**	0	0	0	0
2	0	0	**1**	0	0
3	0	**1**	0	0	0
4	0	0	0	**1**	0
5	0	0	0	0	**1**

×

P_3	1	2	4	3	5
1	**1**	0	0	0	0
2	0	**1**	0	0	0
3	0	0	0	**1**	0
4	0	0	**1**	0	0
5	0	0	0	0	**1**

=

P_9	1	3	4	2	5
1	**1**	0	0	0	0
2	0	0	0	**1**	0
3	0	**1**	0	0	0
4	0	0	**1**	0	0
5	0	0	0	0	**1**

Для оцінювання потужності множини перестановних матриць як функції від n, потрібно провести відповідні розрахунки **[**8**]** кількості перестановних матриць при різних розмірах n, які подано в табл. 1. З цієї таблиці видно, що кількість перестановок при $n = 16$ сягає $2{,}0923 \cdot 10^{13}$, а при $n = 64$ сягає $1{,}2689 \cdot 10^{89}$.

Табл. 1. Кількість перестановних матриць при різних їх розмірах **n**

n	8	16	24	32	40	48	56	64
$N=n!$	40320	$2{,}0923 \cdot 10^{13}$	$6{,}2045 \cdot 10^{23}$	$2{,}6313 \cdot 10^{35}$	$8{,}1592 \cdot 10^{47}$	$1{,}2414 \cdot 10^{61}$	$7{,}1100 \cdot 10^{74}$	$1{,}2689 \cdot 10^{89}$
n^2	64	256	576	1024	1600	2304	3136	4096
n^2/Q	$6{,}400 \cdot 10^{-11}$	$2{,}560 \cdot 10^{-10}$	$5{,}760 \cdot 10^{-10}$	$1{,}024 \cdot 10^{-9}$	$1{,}600 \cdot 10^{-9}$	$2{,}304 \cdot 10^{-9}$	$3{,}136 \cdot 10^{-9}$	$4{,}096 \cdot 10^{-9}$
$n^2 \cdot N/Q$	$2{,}580 \cdot 10^{-6}$	$5{,}356 \cdot 10^{3}$	$3{,}574 \cdot 10^{14}$	$2{,}694 \cdot 10^{26}$	$1{,}305 \cdot 10^{39}$	$2{,}860 \cdot 10^{52}$	$2{,}230 \cdot 10^{66}$	$5{,}197 \cdot 10^{80}$
$t=\varphi(n)$	$8{,}183 \cdot 10^{-14}$	$1{,}698 \cdot 10^{-4}$	$1{,}133 \cdot 10^{7}$	$8{,}544 \cdot 10^{18}$	$4{,}140 \cdot 10^{31}$	$9{,}070 \cdot 10^{44}$	$7{,}070 \cdot 10^{58}$	$1{,}648 \cdot 10^{73}$

Сучасні технічні засоби, а особливо супер-ЕОМ, дають змогу працювати з великою продуктивністю оброблення даних ($Q = 10^{12} \div 10^{15}$ флопсів – кількість операцій з плаваючою комою за секунду). Оскільки у нашому випадку використовуються цілі числа, то кількість флопсів значно більша. У зв'язку з цим, не дивлячись на таку велику кількість перестановок, при відповідному нарощуванні мережевих ресурсів, тривалість перебору може бути не такою вже й значною, а тому бажано зробити хоча б грубе оцінювання тривалості реалізації атаки (перебору в перестановному алгоритмі шифрування).

Для визначення тривалості перебору $t = \varphi(n)$, тобто функція від кількості рядків чи стовпців n перестановної матриці, нами використано такі міркування. Вважатимемо, що одну перестановну матрицю розмірами $n \times n$ можна згенерувати за n^2/Q с. Оскільки в році є 365 діб, 24 год, 60 хв і 60 с, а також при $N = n!$, то тривалість брутальної атаки (в роках) визначимо за такою формулою:

$$t = \varphi(n) = \frac{n^2 \cdot N}{Q \cdot 60 \cdot 60 \cdot 24 \cdot 365}. \qquad (14)$$

З врахуванням продуктивності звичайної ЕОМ $Q = 10^{12}$ флопсів, а також при різних значеннях n отримано результати, які наведено в табл. 1. З цієї таблиці видно, що при розмірі матриці $n = 16$ тривалість перебору становить $1{,}698 \cdot 10^{-4}$ роки, отже вона досить мала, а при розмірі $n = 32$ становить $8{,}544 \cdot 10^{18}$ років, тобто, в даному випадку перебір займе досить значний час. Отже, з даних розрахунків випливає, що матриці розміром 24×24 чи 32×32 забезпечують достатню стійкість перестановних алгоритмів до брутальних атак навіть за значний проміжок часу при достатній продуктивності обчислювальних систем.

3. Багатораундова матрична Афінна перестановна криптосистема

Поєднання матричних Афінних криптосистем з матричними перестановними алгоритмами **[**5**]** дає змогу створити багатораундову матричну Афінну перестановну криптосистему для перетворення інформації, які в загальному випадку можуть подаватися у вигляді процедур багатораундового (де)шифрування на основі таких матричних виразів:

$$\bar{\bar{K}}_{\text{рс}}^{\text{п}} = \underbrace{\bar{\bar{A}}_R \underset{m}{\otimes} \ldots \left(\bar{\bar{A}}_2 \underset{m}{\otimes} \left(\bar{\bar{A}}_1 \underset{m}{\otimes} \left(\bar{\bar{P}}_{\text{р}}^{\text{п}} \times \bar{\bar{T}} \times \bar{\bar{P}}_{\text{с}}^{\text{п}} \right) \underset{m}{\oplus} \bar{B}_1 \right) \underset{m}{\oplus} \bar{B}_2 \right) \ldots \underset{m}{\oplus} \bar{B}_R}_{R\text{раундів}}; \qquad (15)$$

$$\bar{\bar{T}}_{\text{ср}}^{\text{п}} = \bar{\bar{P}}_{\text{р}}'^{\text{п}} \times \left(\underbrace{\bar{\bar{A}}_1' \underset{m}{\otimes} \ldots \left(\bar{\bar{A}}_{R-1}' \underset{m}{\otimes} \left(\bar{\bar{A}}_R' \underset{m}{\otimes} \bar{\bar{K}}_{\text{рс}}^{\text{п}} \underset{m}{\oplus} \bar{B}_R' \right) \underset{m}{\oplus} \bar{B}_{R-1}' \right) \ldots \underset{m}{\oplus} \bar{B}_1'}_{R\text{раундів}} \times \bar{\bar{P}}_{\text{с}}'^{\text{п}} \right). \qquad (16)$$

Можливі ще й такі матричні вирази для реалізації процедури багатораундового (де)шифрування інформації:

$$\overline{\overline{K}}_{\text{рс}}^{\text{п}} = \overline{\overline{P}}_{\text{р}}^{\text{п}} \times \underbrace{\overline{\overline{A}}_R \underset{m}{\otimes} \ldots \left(\overline{\overline{A}}_2 \underset{m}{\otimes} \left(\overline{\overline{A}}_1 \underset{m}{\otimes} \overline{\overline{T}} \underset{m}{\oplus} \overline{B}_1 \right) \underset{m}{\oplus} \overline{B}_2 \right) \ldots \underset{m}{\oplus} \overline{B}_R}_{R\text{ раундів}} \times \overline{\overline{P}}_{\text{с}}^{\text{п}}; \quad (17)$$

$$\overline{\overline{T}}_{\text{ср}}^{\text{п}} = \underbrace{\overline{\overline{A}}'_1 \underset{m}{\otimes} \ldots \left(\overline{\overline{A}}'_{R-1} \underset{m}{\otimes} \left(\overline{\overline{A}}'_R \underset{m}{\otimes} \left(\overline{\overline{P}}_{\text{р}}'^{\text{п}} \times \left(\overline{\overline{K}}_{\text{рс}}^{\text{п}} \times \overline{\overline{P}}_{\text{с}}'^{\text{п}} \right) \right) \underset{m}{\oplus} \overline{B}'_R \right) \underset{m}{\oplus} \overline{B}'_{R-1} \right) \ldots \underset{m}{\oplus} \overline{B}'_1}_{R\text{ раундів}}; \quad (18)$$

Перестановки можуть описуватися й іншими моделями **[**1**]**.

4. Криптоаналіз багатораундової матричної Афінної перестановної криптосистеми

Криптоаналіз зашифрованої інформації за допомогою такої криптосистеми є надзвичайно важким **[**3**]**.

По-перше, атака грубої сили при такому алгоритмі є надзвичайно складною, позаяк матриця-ключ шифрування має розмір $n \times n$, а вектор-стовпець коригування – розміром n. Оскільки кожен вхід може мати одне з 255 значень, то це означає, що кількість матриць шифрування становитиме $255^{n \times n}$, а векторів коригування – 255^n. Однак, як зазначалося в розд. 2, не всі матриці-ключі мають мультиплікативну інверсію, аналогічно як і стовпці коригування адитивну інверсію. Тому область існування ключів все ж таки дещо зменшується.

По-друге, запропонований криптографічний алгоритм не зберігає статистику звичайного тексту. Неможливо провести аналіз частоти окремих блоків з двох або трьох букв, позаяк відбувається перестановка як рядків, так і стовпців числових кодів символів вхідного повідомлення. Аналіз частоти появи слів розміром m (а в нашому випадку m=256) не може спрацювати, але такого не буває, щоби вхідний текст мав таку велику кількість символів.

По-третє, можна провести атаку на шифр, використовуючи метод знання вихідного тексту, якщо знати значення m і пари "вихідний текст/зашифрований текст", принаймні m блоків. Блоки можуть належати тому ж самому повідомленню або різними повідомленням, але мають бути різні. Тому можна створити дві матриці, P (звичайний текст) і C (зашифрований текст), в якому відповідні рядки представляють відомі пари звичайного/зашифрованого тексту. Оскільки $C = P \times K$, можна використовувати відносини $K = C \times P^{-1}$, щоб знайти ключ, якщо P є зворотним. Якщо P не є зворотним, то мають задіюватися різні набори m пар звичайного/зашифрованого тексту. Однак такий підхід в нашому випадку не увінчається успіхом через великі розміри m.

Отже, розроблена багатораундова матрична Афінна перестановна криптосистема забезпечують достатню стійкість до брутальних атак навіть за значний проміжок часу.

Висновки

1. З'ясовано, що порівняно з іншими методами захисту класична криптографія гарантує захист інформації тільки за умов, якщо використано ефективний криптографічний алгоритм, а також дотримані умови секретності та цілісності ключів шифрування.

2. Виявлено, що криптосистема Хілла, хоча і є поліграмним шифром, вразлива до атак на основі відкритих текстів, позаяк у алгоритмі використовуються лінійні матричні операції. Для збільшення його криптостійкості в алгоритм шифрування потрібно додати будь-які нелінійні операції.

3. Математично описано алгоритм (де)шифрування інформації за допомогою багатораундової матричної Афінної криптосистеми з різними ключами шифрування на кожному раунді, яка значно підвищує криптостійкість класичного алгоритму шифрування.

4. Математично описано алгоритм (де)шифрування інформації за допомогою матричного перестановного алгоритму, яка дещо підвищує криптостійкість класичного алгоритму шифрування.

5. Математично описано алгоритм (де)шифрування інформації за допомогою багатораундової матричної Афінної перестановної криптосистеми, яка набагато підвищує криптостійкість класичного алгоритму шифрування.

6. Проведено криптоаналіз багатораундової матричної Афінної перестановної криптосистеми. Встановлено, що розроблений алгоритм забезпечують достатню стійкість до брутальних атак навіть за значний проміжок часу при достатній продуктивності обчислювальних систем.

Література

1. Бєгун А.В. Інформаційна безпека / А.В. Бєгун. – К. : Вид-во КНЕУ, 2008. – 280 с.

2. Грицюк П.Ю. Афінні перетворення у криптографічній системі Лестера Хілла / П.Ю. Грицюк // 66-а науково-технічна студентська конференція НЛТУ України. – Серція: Інформаційні технології : результати 66-ої СНТК, м. Львів, 13 листопада 2014 р. – Львів : НЛТУ України. **[**Електронний ресурс**]**. – Доступний з http://it.nltu.edu.ua/index.php/kafedra/news/286-rezultaty-66-oi-snk-sektsiia-informatsiini-tekhnolohii

3. Ємець В. Сучасна криптографія: Основні поняття / В. Ємець, А. Мельник, Р. Попович. – Львів : Вид-во БаК, 2003. – 144 с.

4. Красиленко В.Г. Матричні афінні шифри для створення цифрових сліпих підписів на текстографічні документи / В.Г. Красиленко, С.К. Грабовляк // Системи обробки інформації : зб. наук. праць. – Х. : Вид-во ХУПС ім. Івана Кожедуба. – 2011. – Вип. 7 (97). – С. 60-63.

5. Красиленко В.Г. Матричні афінно-перестановочні алгоритми для шифрування та дешифрування зображень / В.Г. Красиленко, С.К. Грабовляк // Системи обробки інформації: зб. наук. праць. – Харків : Вид-во ХУПС ім. Івана Кожедуба. – 2012. – Вип. 3(101), т. 2. – С. 53-61.

6. Красиленко В.Г. Моделювання матричних алгоритмів криптографічного захисту / В.Г. Красиленко, Ю.А. Флавицька // Вісник Національного університету "Львівська політехніка". – Сер.: Комп'ютерні системи та мережі. – Львів : Вид-во НУ "Львівська політехніка". – 2009. – № 658. – С. 59-63.

7. Красиленко В.Г. Моделювання матричного афінно-перестановочного алгоритму для криптографічних перетворень зображень / В.Г. Красиленко, С.К. Грабовляк // Наука і навчальний процес : наук.-метод. збірник матер. наук.-практ. конф. ВСЕІ Університету "Україна". – Вінниця, 2012. – С. 171-172.

8. Красиленко В.Г. Оцінювання стійкості та часу зламування у матрично-перестановочних алгоритмах криптографічних перетворень / В.Г. Красиленко, С.К. Грабовляк // Наука і навчальний процес : наук.-метод. збірник матер. наук.-практ. конф. ВСЕІ Університету "Україна. – Вінниця, 2012. – С. 173-174.

9. Петраков А.В. Основы практической защиты информации : учеб. пособ. – М. : Изд-во "Радио и Связь", 2012. – 384 с.

10. Поберейко Б.П. Особливості реалізації Афінних перетворень у криптографічній системі Лестера Хілла / Б.П. Поберейко, П.Ю. Грицюк // Проблеми застосування інформаційних технологій, спеціальних технічних засобів у діяльності ОВС та навчальному процесі : зб. наук. стат. за матер. доп. учасн. наук.-практ. конф., м. Львів, 26 грудня 2014 р. – Львів : Львівський ДУВС. – 2014. – С. 71-75.

11. Хорошко В.О. Методи та засоби захисту інформації : навч. посібн. / В.О. Хорошко, А.О. Четков. – К. : Вид-во "Юніор", 2003. – 502 с.

12. Юзьків Ю.Т. Спільність числових методів афінних перетворень у класичних криптосистемах / Ю.Т. Юзьків, Ю.І. Грицюк // Захист інформації і безпека інформаційних систем : матер. І-ої Міжнар. наук.-техн. конф., м. Львів, 31 травня – 01 червня 2012 р. – Львів : Вид-во НУ "Львівська політехніка". – 2012. – С. 134-135.

Грыцюк П.Ю., Грыцюк Ю.И. **Особенности реализации матричной Аффинной криптосистемы**

Рассматриваются особенности разработки надежной криптосистемы защиты информации, которая сочетает матричные Аффинные преобразования, многораундовые действия с различными ключами, а также перестановочный алгоритм, что в целом позволяет значительно повысить ее криптостойкость к грубым атак. Выяснено, что, по сравнению с другими методами защиты, классическая криптография гарантирует защиту информации только при условии, если использовано эффективный криптографический алгоритм, а также соблюдены условия секретности и целостности ключей шифрования. Математически описан алгоритм шифрования/дешифрования информации с помощью многораундовой матричной Аффинной перестановочной криптосистемы с различными ключами шифрования на каждом раунде. Проведенный криптоанализ ее устойчивости показал, что разработанный алгоритм обеспечивают достаточную устойчивость к агрессивным атакам даже за значительный промежуток времени при достаточной производительности вычислительных систем.

Ключевые слова: защита информации, шифрование/дешифрование информации, Аффинная система подстановки Цезаря, криптографическая система Хилла, монограммный и полиграммный шифр, матричные аффинные преобразования, перестановочный алгоритм, криптографический анализ.

Grytsyuk P.Yu., Gryciuk Yu.I. **Features of the implementation matrix Affine cryptosystem**

The features of the development of robust cryptosystems of information security. The system combines the matrix Affine transformation, multi-round action with different keys, as well as commuting the algorithm. This can significantly increase its crude to the cryptographic attacks. It was found that classical cryptography guarantees the protection of information only on condition, that the cryptographic algorithm used effectively and complied with the conditions of the privacy and integrity of encryption keys. The algorithm encryption/decryption of data using multi-round permutation matrix Affine cryptosystem with a variety of encryption keys for each round is mathematically description. Held cryptanalysis its stability showed that the developed algorithm to provide sufficient resistance to aggressive attacks even for a significant time period at a sufficient performance computing systems.

Keywords: information security, to encryption/decryption of information, Affinity system substitution Caesar, cryptosystem Hill, monogram and poligramy code, cipher matrix Affine transformations, commuting algorithm, cryptographic analysis.

6. ОСВІТЯНСЬКІ ПРОБЛЕМИ ВИЩОЇ ШКОЛИ

УДК 004.42

Доц. М.С. Пасєка, канд. техн. наук –
Івано-Франківський НТУ нафти і газу

ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ДЛЯ ПРОФЕСІЙНОЇ ПІДГОТОВКИ ФАХІВЦІВ У ГАЛУЗІ ПЕДАГОГІКИ

Розглянуто необхідність використання сучасних інформаційних технологій для підвищення професійності підготовки педагогів у вищій школі. Визначено педагогічні етапи й умови формування готовності майбутнього педагога до впровадження сучасних інформаційних технологій у вищому навчальному закладі. Запропоновано структуру професійно-педагогічної інформаційної культури фахівців у галузі педагогіки. Визначено перспективи розвитку у царині застосування інформаційно-комунікаційних технологій у процесі творення віртуально-навчального педагогічного середовища, розробленні методик і технологій формування інформаційної компетенції у фахівців відповідно до галузей знань та дослідження подальшого розвитку ключових життєвих компетентностей особистостей у зв'язку з бурхливим розвитком інформаційного суспільства та глобалізаційними впливами.

Ключові слова: інформаційна компетентність, готовність, інформаційні технології, комп'ютерна грамотність, мислення студентів, готовність.

Актуальність. У сучасному світі підготовка професіональних фахівців – одне з найважливіших завдань вищої школи. Професіоналізм розуміють як високу майстерність, що дає змогу випускнику бути конкурентоспроможним на ринку праці. Підготовка висококваліфікованого фахівця потребує впровадження сучасних інформаційних технологій навчання.

Одним із пріоритетних завдань реформування освіти є підготовка нового покоління педагогів, здатних до професійної діяльності в умовах запровадження сучасних інформаційних технологій у навчальний процес. Інноваційні зміни у педагогіці розпочалися досить давно (40-50-ті роки XX ст.) і до наших днів набули широкого розмаху якісного розмаїття, наслідком якого спочатку було створення технічних, аудіовізуальних, електронних засобів навчання, а в останнє десятиріччя – і комп'ютерної підтримки навчального процесу. Появу педагогічних технологій названо четвертою революцією в освіті (після створення шкіл, використання у навчанні письмового слова і винайдення книгодрукування).

Використання комп'ютерної техніки і програмно-інформаційних засобів у навчально-виховний процес у вищій школі дає змогу в комплексі вирішити низку актуальних проблем:

- підвищити інформаційну культуру майбутнього фахівця, зробити доступним для нього світові інформаційні ресурси;
- посилити інформаційну насиченість всього навчально-виховного процесу в закладах освіти.

У процесі поширення інновацій у сфері освіти формується й розвивається сучасна освітня система – глобальна система відкритої, гнучкої, індивідуалізованої неперервної освіти людини протягом усього її життя.