елементів бази знань / Р.Р. Даревич, Д.Г. Досин, В.В. Литвин, З.Т. Назарчук // Искусственный интеллект. – Донецк. – № 3. – 2006. – С. 500–509. 8. Sowa J. Conceptual graphs for a database interface / J.Sowa // IBM Journal of Research and Development. – Vol. 20. – 1976. – № 4. – P. 336–357. 9. Цветков А.М. Разработка алгоритмов индуктивного вывода с использованием деревьев решений / А.М. Цветков // Кибернетика и системный анализ. – 1993. – № 1. – С. 174–178. 10. Даревич Р.Р. Метод автоматичного визначення інформаційної ваги понять в онтології бази знань / Р.Р. Даревич, Д.Г. Досин, В.В. Литвин // Відбір та обробка інформації. – 2005. – Вип. 22(98). – С.105–111. 11. Фаулер М. UML в кратком изложени / М. Фаулер, К. Скотт. – М.: Мир, 1999. – 340 с.

УДК 681.142.2; 622.02.658.284; 621. 325

Ю.Ю Рашкевич, А.М. Ковальчук, Д. Д. Пелешко, М.Л. Навитка
Національний університет "Львівська політехніка",
кафедра автоматизованих систем управління

ПОТОКОВА МОДИФІКАЦІЯ АЛГОРИТМУ RSA З ВИКОРИСТАННЯМ ПРОЕКТИВНИХ ТА АФІННИХ ПЕРЕТВОРЕНЬ ДЛЯ ДЕЯКИХ КЛАСІВ ЗОБРАЖЕНЬ

На основі алгоритму RSA як найбільш вживаного промислового стандарту шифрування даних запропоновано модифікації з використанням проективних відображень та афінних перетворень для шифрування зображень, що дають змогу строго виділяти контури.

Ключові слова: алгоритм RSA, шифрування даних, проективні відображення, контур

Based on the algorithm of RSA, as the most common industry standard data encryption, proposed modifications using projective mappings and affine transformation for image encryption, allowing strictly allocate paths.

Keywords: algorithm RSA, data encryption, projective mapping, contour.

Вступ

У сучасному світі бурхливого розвитку інформаційних технологій все гострішим стає питання захисту інформації. Однією з найпоширеніших форм представлення інформації в цифровому вигляді є цифрові зображення.

Одним з найбільш вживаних і захищених алгоритмів шифрування даних є алгоритм RSA [1]. Він належить до групи асиметричних алгоритмів з відкритим ключем. Безпека алгоритму RSA ґрунтується на ресурсно витратній факторизації великих чисел. При цьому відкритий і закрити ключі є функціями двох простих чисел з розрядністю 100–200 десяткових знаків і більше.

Алгоритм RSA є універсальним алгоритмом, тобто може застосовуватись до будь-яких сигналів. Однак недоліком такої універсальності є те, що деякі класи зашифрованих сигналів можуть бути частково відтворені іншими засобами обробки. До таких класів сигналів належать цифрові зображення. В такому випадку виникає потреба в реалізації спеціальних алгоритмів або модифікації існуючих. Детально проблему використання алгоритму RSA стосовно зображень описано в [4].

Представлення зображення матрицею кольорів пікселів

Нехай задано зображення P розмірностей h – висота – кількість пікселів по вертикалі, та l – довжина – кількість пікселів по горизонталі. Це зображення можна розглядати як матрицю пікселів $P_{l,h}$, відповідно до якої ставиться матриця кольорів $C_{P_{l,h}}$.

$$P = P_{l,h} = \left\lfloor pxl_{ij} \right\rfloor_{1\le i\le n(l),\,1\le j\le m(h)} \to C_{P_{l,h}} = \left\lfloor c_{ij} \right\rfloor_{1\le i\le n(l),\,1\le j\le m(h)}, \tag{1}$$

де pxl_{ij} – піксел з кординатами (i, j) дискретизованого зображення P; n та m – кількості пікселів у напрямках l та h відповідно.

Модифікація алгоритму шифрування даних RSA з використаннями проективних відображень першого порядку

Частковим проективним відображенням, описаним у [2], є відображення вигляду:

$$\begin{cases} u = \dfrac{(p_2 - p_3)(x - p_1)}{(p_2 - p_1)(x - p_3)}, \\ v = \dfrac{(p_2 - p_3)(y - p_1)}{(p_2 - p_1)(y - p_3)}; \end{cases} \tag{2}$$

якщо

$$d = \begin{vmatrix} p_2 - p_3 & -u(p_2 - p_1) \\ v(p_2 - p_1) & -(p_2 - p_3) \end{vmatrix} \neq 0, \tag{3}$$

то існує обернене до (2) перетворення і тоді

$$\begin{cases} x = \dfrac{d_x}{d}, \\ y = \dfrac{d_y}{d}; \end{cases} \tag{4}$$

де

$$d_x = \begin{vmatrix} p_1(p_2 - p_3) - p_3u(p_2 - p_1) & -u(p_2 - p_1) \\ p_3v(p_2 - p_1) - p_1(p_2 - p_3) & -(p_2 - p_3) \end{vmatrix}, \tag{5}$$

$$d_y = \begin{vmatrix} (p_2 - p_3) & p_1(p_2 - p_3) - p_3u(p_2 - p_1) \\ v(p_2 - p_3) & p_3v(p_2 - p_1) - p_1(p_2 - p_3) \end{vmatrix}. \tag{6}$$

Шифрування відбувається так:

- беруться два сусідні в рядку елементи матриці зображення (1)

$$x = c_{i,j},\ y = \frac{c_{i,j+1} + c_{i,j}}{2},\ i = \overline{1,n},\ j = \overline{1,m-1};$$

- шифруються за формулою (1) при

$$p_1 = z_2,\ p_2 = z_1 + 2(z_2 + d),\ p_3 = e - d;$$

- записуються на відповідні місця в матрицю зашифрованого зображення.

Процедура дешифрування відбувається в оберненому порядку:

- беруться два сусідні в рядку елементи матриці зашифрованого зображення

$$x' = c'_{i,j},\ y' = c'_{i,j+1},\ i = \overline{1,n},\ j = \overline{1,m-1};$$

- дешифруються за формулою (4) з урахуванням формул (3), (5) та (6);
- записуються на відповідні місця в матрицю дешифрованого зображення наступним чином:

$$c_{i,j} = x,\ c_{i,j+1} = 2y - c_{i,j},\ i = \overline{1,n},\ j = \overline{1,m-1}.$$

На рис. 1 наведено результати шифрування та дешифрування зображення модифікованим алгоритмом RSA з використанням проективних відображень першого порядку з різними значеннями ключів шифрування.

Модифікація алгоритму шифрування даних RSA з використаннями афінних перетворень

Бінарне афінне перетворення [3] площини в декартових координатах має вигляд:

$$\begin{aligned} x' &= a_1 x + b_1 y + d_1, \\ y' &= a_2 x + b_2 y + d_2; \end{aligned} \tag{7}$$

де

$$d = \begin{vmatrix} a_1 & b_1 \\ a_2 & b_2 \end{vmatrix} \neq 0 . \tag{8}$$

Обернене до (7) перетворення також існує і тоді

$$x = \frac{\Delta_x}{d}, \; y = \frac{\Delta_y}{d}, \tag{9}$$

де

$$\Delta_x = \begin{vmatrix} x' - d_1 & b_1 \\ y' - d_2 & b_2 \end{vmatrix}; \quad \Delta_y = \begin{vmatrix} a_1 & x' - d_1 \\ a_2 & y' - d_2 \end{vmatrix}. \tag{10}$$

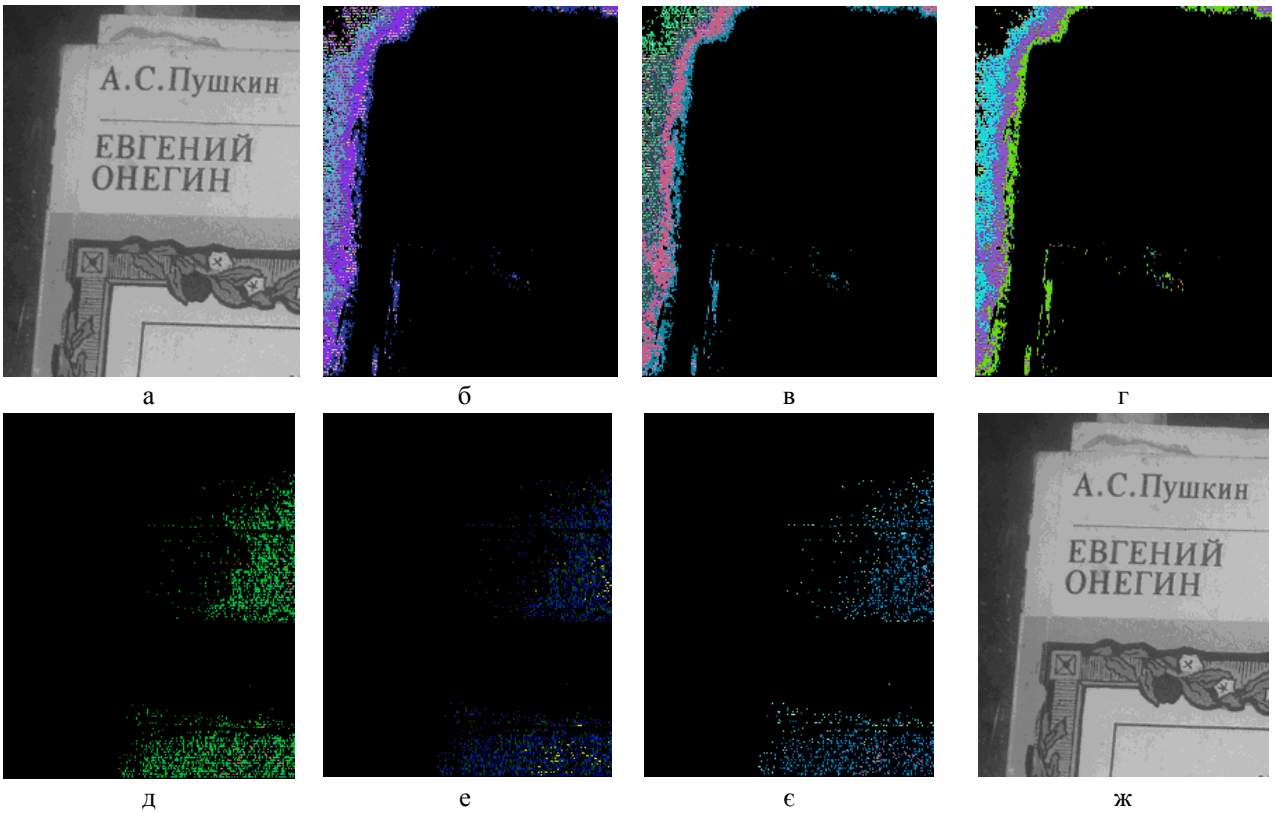

Рис. 1. Приклади зображень, зашифрованих різними ключами модифікованим алгоритмом з використанням проективних відображень: а – оригінальне зображення; б – зашифроване при $z_1 = 53,\ z_2 = 53,\ e = 2609,\ d = 1537$ *; в – зашифроване при* $z_1 = 59,\ z_2 = 53,\ e = 1181,\ d = 2541$*; г – зашифроване при* $z_1 = 97,\ z_2 = 59,\ e = 569,\ d = 137$ *; д – зашифроване при* $z_1 = 103,\ z_2 = 191,\ e = 1997,\ d = 18953$ *; е – зашифроване при* $z_1 = 109,\ z_2 = 191,\ e = 4231,\ d = 14671$*; є – зашифроване при* $z_1 = 139,\ z_2 = 191,\ e = 1979,\ d = 7499$ *; ж – дешифроване зображення*

Шифрування та дешифрування може відбуватись двома способами: за двома сусідніми елементами в рядку та стовпцем матриці зображення.

1) шифрування та дешифрування за двома сусідніми в рядку елементами матриці зображення

Шифрування відбувається так:

- беруться два сусідні в рядку елементи матриці зображення (1)

$$x = c_{i,j},\ y = \frac{c_{i,j+1} + c_{i,j}}{2},\ i = \overline{1,n},\ j = \overline{1,m-1};$$

- шифруються за формулою (7) при

$$a_1 = b_2 = (z_1 + z_2)^e \pmod z,\ b_1 = a_2 = (z_1 - z_2)^d \pmod z,\ d_1 = j \cdot j,\ d_2 = j \cdot j \cdot j,\ j = \overline{1,m};$$

- записуються на відповідні місця в матрицю зашифрованого зображення.

Процедура дешифрування відбувається в оберненому порядку:

- беруться два сусідні в рядку елементи матриці зашифрованого зображення

$$x' = c'_{i,j},\ y' = c'_{i,j+1},\ i = \overline{1,n},\ j = \overline{1,m-1};$$

- дешифруються за формулою (9) з урахуванням формул (8) та (10);
- записуються на відповідні місця в матрицю дешифрованого зображення так:

$$c_{i,j} = x,\ c_{i,j+1} = 2y - c_{i,j},\ i = \overline{1,n},\ j = \overline{1,m-1}.$$

На рис. 2 наведено результати шифрування та дешифрування зображення модифікованим алгоритмом RSA з використанням афінних перетворень за двома сусідніми в рядку елементами матриці зображення з різними значеннями ключів шифрування.

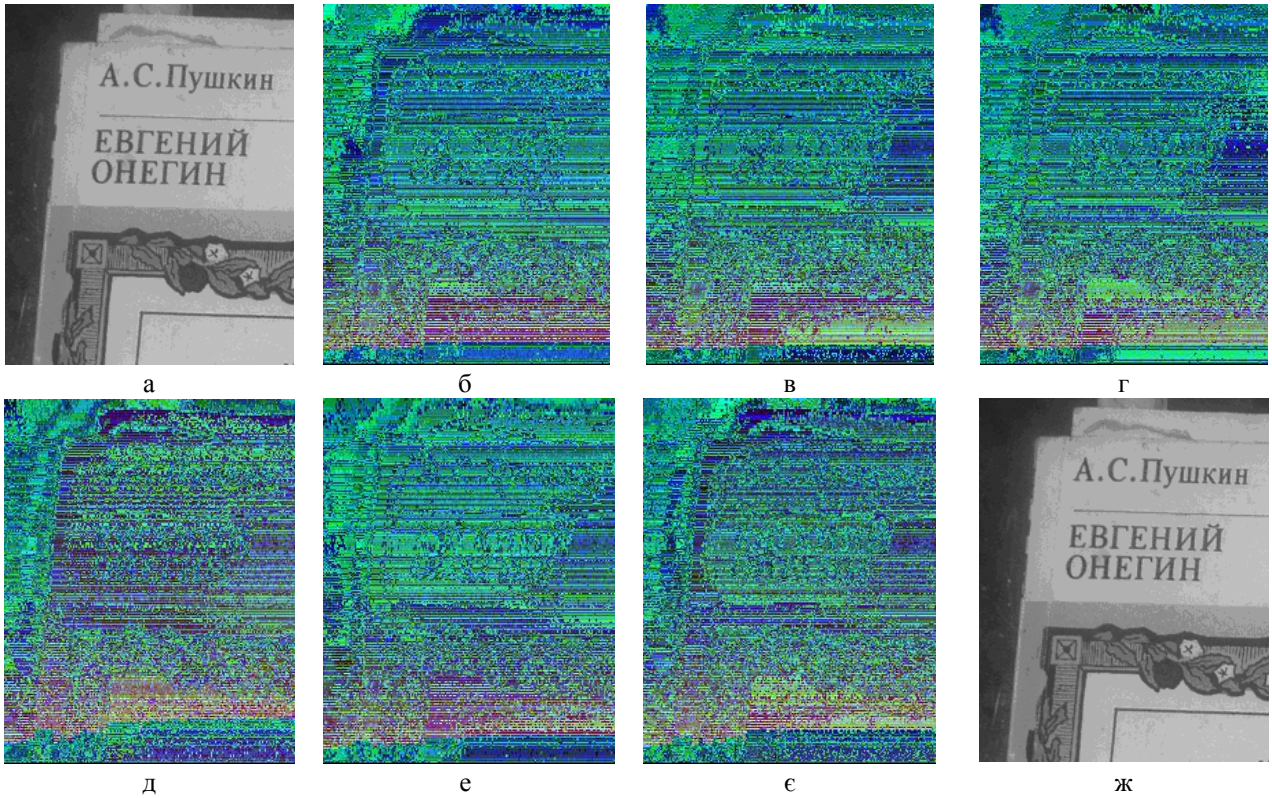

Рис. 2. Приклади зображень, зашифрованих різними ключами за двома сусідніми в рядку елементами модифікованим алгоритмом з використанням афінних перетворень: а – оригінальне зображення; б – зашифроване при $z_1 = 61,\ z_2 = 199,\ e = 4019,\ d = 10739$; *в – зашифроване при* $z_1 = 67,\ z_2 = 89,\ e = 4663,\ d = 3079$; *г – зашифроване при* $z_1 = 67,\ z_2 = 181,\ e = 2557,\ d = 11053$; *д – зашифроване при* $z_1 = 83,\ z_2 = 191,\ e = 8017,\ d = 14173$; *е – зашифроване при* $z_1 = 97,\ z_2 = 89,\ e = 5147,\ d = 4883$; *є – зашифроване при* $z_1 = 97,\ z_2 = 167,\ e = 6823,\ d = 6103$; *ж – дешифроване зображення*

2) шифрування та дешифрування за двома сусідніми в стовпці елементами матриці зображення

Шифрування відбувається так:

- беруться два сусідні в рядку елементи матриці зображення (1)

$$x = c_{i,j},\ y = \frac{c_{i+1,j} + c_{i,j}}{2},\ i = \overline{1, n-1},\ j = \overline{1, m};$$

- шифруються за формулою (7) при

$$a_1 = b_2 = (z_1 + z_2)^e \pmod z,\ b_1 = a_2 = (z_1 - z_2)^d \pmod z,\ d_1 = -j \cdot j,\ d_2 = -j \cdot j \cdot j,\ j = \overline{1, m};$$

- записуються на відповідні місця в матрицю зашифрованого зображення.

Процедура дешифрування відбувається в оберненому порядку:

- беруться два сусідні в рядку елементи матриці зашифрованого зображення

$$x' = c'_{i,j},\ y' = c'_{i+1,j},\ i = \overline{1, n-1},\ j = \overline{1, m};$$

- дешифруютсья за формулою (9) з урахуванням формул (8) та (10);
- записуються на відповідні місця в матрицю дешифрованого зображення наступним чином:

$$c_{i,j} = x,\ c_{i+1,j} = 2y - c_{i,j},\ i = \overline{1, n-1},\ j = \overline{1, m}.$$

На рис. 3 наведено результати шифрування та дешифрування зображення модифікованим алгоритмом RSA з використанням афінних перетворень за двома сусідніми в стовпці елементами матриці зображення з різними значеннями ключів шифрування.

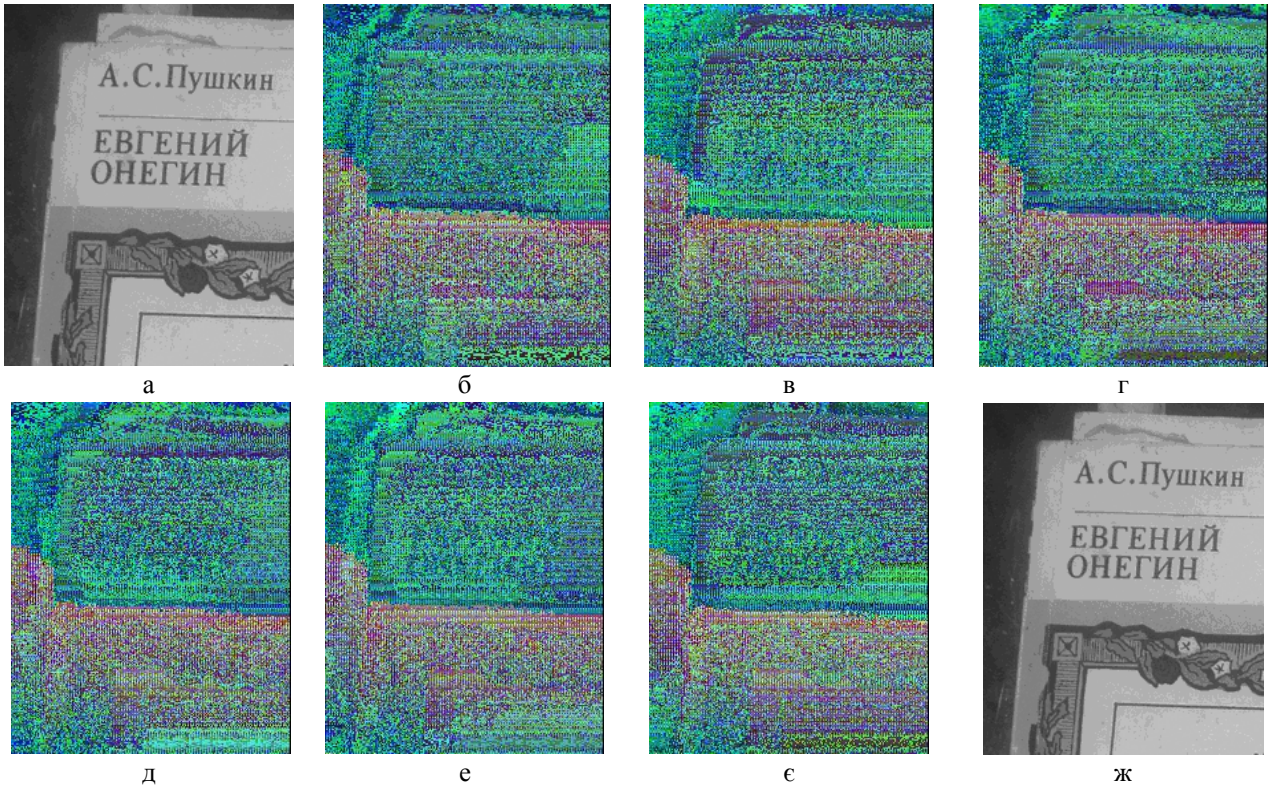

Рис. 3. Приклади зображень, зашифрованих різними ключами за двома сусідніми в стовпці елементами модифікованим алгоритмом з використанням афінних перетворень: а – оригінальне зображення; б – зашифроване при $z_1 = 73\ z_2 = 197, e = 5507, d = 8459$ *; в – зашифроване при* $z_1 = 79, z_2 = 191, e = 7951, d = 3931$ *; г – зашифроване при* $z_1 = 97, z_2 = 173, e = 12197, d = 3245$ *; д – зашифроване при* $z_1 = 97, z_2 = 181, e = 6869, d = 6269$ *; е – зашифроване при* $z_1 = 101, z_2 = 173, e = 2131, d = 5771$ *; є – зашифроване при* $z_1 = 103, z_2 = 193, e = 7331, d = 9227$ *; ж – дешифроване зображення*

Висновки

Запропоновані модифікації повністю відповідають стійкості до дешифрування алгоритму RSA і забезпечують при правильному підборі ключа практично повну зашумленість зашифрованого зображення, що унеможливлює отримання з нього будь-якої інформації без дешифрування.

1. Шнайдер Б. Прикладная криптография. – М.: Триумф, 2003. – 816 с. 2. Рашкевич Ю., Ковальчук А., Пелешко Д. Проективні відображення першого порядку в шифруванні і дешифруванні зображень з елементами алгоритму RSA // Технічні вісті. – 2009/№1(29), 2(30). – С. 41 – 44. 3. Рашкевич Ю.М., Ковальчук А.М., Пелешко Д.Д. Афінні перетворення в модифікаціях алгоритму RSA шифрування зображень. – Львів: ААЕКС, 2009/№2. 4. Рашкевич Ю.М., Пелешко Д.Д., Ковальчук А.М., Пелешко М.З. Модифікація алгоритму RSA для деяких класів зображень // Технічні вісті. – 2008/1(27), 2(28). – С. 59 – 62.

УДК 004.832.3:004.838.2

Р. Ткаченко, М. Машевська, Н. Кіцак
Національний університет "Львівська політехніка",
кафедра автоматизованих систем управління

ПРОГНОЗУВАННЯ ПАРАМЕТРІВ МІКРОКЛІМАТУ В ПРИМІЩЕННІ ЗА ДОПОМОГОЮ КОНТРОЛЕРА НЕЧІТКОЇ ЛОГІКИ

Розглянуто основні зовнішні фактори, що впливають на тепловий мікроклімат у приміщенні. Описано процес побудови нечіткої моделі для прогнозування параметрів мікроклімату. Показано результати використання контролера нечіткої логіки для вирішення задачі прогнозування. Побудовано математичну модель для поставленої задачі на основі регресійного аналізу.

Ключові слова: нечітка модель, рівняння регресії, кліматичні фактори, параметри мікроклімату

Basic external factors which influence on a thermal microclimate in an apartment are considered. The process of creation of the fuzzy-model for prognostication of parameters of the microclimate is described. The results of the use of fuzzy controller for the task of prognostication are shown. A mathematical model for the described problem by the regressive analysis is built.

Keywords: fuzzy-model, regression model, climatic factors, microclimate parameters

Вступ

Одним з напрямків реалізації програми доступного житла в Україні є забезпечення відповідного рівня комфорту проживання населення. Для покращання якості життя в „замкнутому просторі" необхідно вибирати такі параметри та конструктивні рішення будівлі, що забезпечують оптимальний рівень мікроклімату.

Сьогодні, враховуючи відсутність та значні проблеми, що виникають при побудові математичними методами точної та повної аналітичної моделі для розрахунку та прогнозування значень параметрів мікроклімату, доцільно як альтернативу використати засоби нечіткої логіки.