БІОЛОГІЧНІ ТА МЕДИЧНІ ПРИЛАДИ І СИСТЕМИ

УДК 681.5.017:616-71

О. М. Роїк, А. В. Поплавський, А. О. Азарова

СТРУКТУРНО-АГОРИТМІЧНІ МЕТОДИ ПІДВИЩЕННЯ ТОЧНОСТІ ВИМІРЮВАНЬ В СИСТЕМАХ ДІАГНОСТИКИ БІОЛОГІЧНИХ ТА ТЕХНІЧНИХ ОБ'ЄКТІВ

Вінницький національний технічний університет, Вінниця

Анотація: Розроблено узагальнену математичну модель штучного розчленування замкнених кіл у задачах медичної діагностики, система індексації у якій визначає алгоритми побудови комплексу базових структур первинних перетворювачів електропунктурної діагностики. Розроблено узагальнену математичну модель мультиплікативних похибок комплексу базових структур первинних перетворювачів електропунктурної діагностики.

Ключові слова: узальнена математична модель, електропунктурна діагностика (ЕД), штучне розчленування, первинні перетворювачі.

Аннотация:. Розроботана обобщенная математическая модель искусственного разделения замкнутых цепей в задачах медыцинской диагностики, система индексации в которой определяет алгоритмы построения комплекса базовых структур первичных преобразователей электропунктурной диагностики. Розроботана обобщенная математическая модель мультипликативных погрешностей комплекса базовых структур первичных преобразователей электропунктурной диагностики.

Ключевые слова: обобщенная математическая модель, электропунктурня диагностика (ЭД), искусственное расчленение, первичные преобразователи.

Abstract: Generalized mathematical model of artificial separation closed circuits in medical diagnostics objectives was developed, indexation system algorithms of creating complex primary converters basic structures electropunctural diagnostic was determined. Generalized mathematical model of multiplicative error of complex primary converters basic structures electropunctural diagnostic was determined.

Key words: generalized mathematical model, electropunctural diagnostic, artificial separation, primary converters.

Вступ

На сьогоднішній день відомо, що фізіологічна особливість біологічно активних точок (БАТ) полягає в тому, що вони однозначно зв'язані з частиною або функцією визначеного органа.

Всі методи акупунктурної діагностики засновані на тому, що БАТ мають значення ряду фізичних характеристик, що сильно відрізняються від навколишніх тканин. З усіх параметрів найбільш доступні для спостереження є зміни провідності імпедансів БАТ. ЕД взяла на озброєння енергетичні лінії, що називаються меридіанами, а також БАТ, що розташовані на цих меридіанах, зокрема, так звані, репрезентативні БАТ, які опосередковано відображають стан відповідних меридіанів.

Актуальність

ЕД полягає у дослідженні біоелектричних параметрів точок акупунктури і заснована на тому, що органічні або функціональні зміни в різних системах організму супроводжуються зміною фізичного стану точок акупунктури. Об'єктивність ЕД визначається не тільки інтерпретацією отриманих результатів з позицій відповідності точок органам і взаємозв'язків між меридіанами. Багато в чому її об'єктивність залежить від точності вимірювань та вірогідності інтерпретації результатів виміру біоелектричних параметрів точок акупунктури. На цей час, незважаючи на розмаїтість методів та засобів ЕД, не можна вважати вирішеним питання про точність вимірів.

Основним недоліком найбільш росповсюджених методів ЕД Фоля і Накатані [1-5] є те, що під час вимірювань імпедансів точок акупунктури (двополюсників) не враховуються об'єктивно існуючі взаємозв'язки між меридіанами, що може привести до похибок первинних перетворень, оскільки під час вимірювань досліджувану точку акупунктури (досліджуваний двополюсник) шунтують інші двополюсники, що значно ускладнює проведення об'єктивної діагностики. Тому актуальним є застосування методів інваріантних (незалежних) перетворень параметрів компонентів складних об'єктів для задач медичної діагностики. У технічній діагностиці широкий розвиток отримали системи поелементного діагностування, в яких вимірювання імпедансів елементів складних об'єктів засновано на штучному розчленуванні замкнених електричних схем [6-9]. Аналогічний підхід можна застосувати і для даної задач медичної діагностики. В роботах [10-14] розглянуті деякі структури з штучним розчленуванням замкнених кіл складних об'єктів. Однак, наведені структури недостатньо формалізовані і систематизовані.

Мета

Метою роботи є формалізація з точки зору системного підходу задачі інваріантних перетворень в задачах медичної та технічної діагностики.

Задачі

Відповідно до мети досліджень формулюються такі задачі:

1. Побудова узагальненої математичної моделі розв'язання задачі інваріантного перетворення параметрів елементів у складних біологічних об'єктах.
2. Побудова комплексу базових структурних схем первинних перетворювачів у задачах медичної діагностики.
3. Побудова узагальненої математичної моделі мультиплікативних похибок комплексу базових структурних схем первинних перетворювачів у задачах медичної та технічної діагностики.
4. Розробка структурно-агоритмічних методів підвищення точності вимірювань в системах діагностики біологічних та технічних об'єктів.

Розв'язання задач

У загальному випадку організм людини, як об'єкт діагностування (ОД), можна розглядати у вигляді множини взаємозв'язаних між собою імпедансів репрезентативних біологічно активних точок (БАТ), так званих, меридіанів, які розглядаються як двополюсники щодо самої БАТ (активний електрод) і деякою еквіпотенціальною областю (пасивний електрод). Як вказувалось вище для забезпечення інваріантності перетворень параметрів елементів у складних об'єктах слід застосовувати методи штучного розчленування. замкнених кіл, що дасть можливість розглядати досліджувані імпеданси як ізольовані двополюсники. У даному підрозділі пропонується узагальнена математична модель поставленої задачі з метою формалізації синтезу і аналізу відповідних перетворювачів.

У вимірювальній техніці, перетворення параметрів ізольованих двополюсників здійснюють за допомогою дільників напруги, що утворюються послідовно з'єднаними зразковим $\dot{Y}_{\text{o}}$ і досліджуваним $\dot{Y}_x$ двополюсниками. При цьому, за допомогою деякого комутатора та контакту з БАТ через голковколювання (електроакупунктура) здійснюється реконфігурація структури ОД у коло типу трикутник, в якому одна з його гілок є досліджуваним двополюсником $\dot{Y}_x$, що шунтується двополюсниками $\dot{Y}_{\text{s}}$ і $\dot{Y}_h$, які утворюються під час декомпозиції ОД. Таким чином досліджуванню підлягає чотириполюсник коло пасивних компонент GПК (рис.1), де полюс φ_h відповідає активному електроду, полюс φ_s – пасивному електроду, а полюс φ_g утворюється об'єднанням усіх БАТ крім досліджуваною.

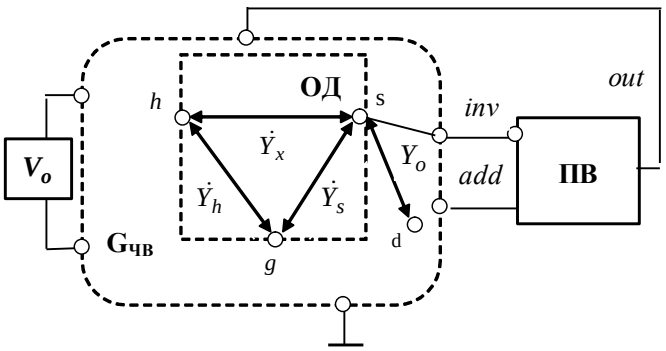


Рисунок 1 – Чотириполюсник кола пасивних компонент $G_{ПК}$

Як вказувалось вище, для того щоб реалізувати інваріантні перетворення параметрів елементів у замкнених колах, в першу чергу необхідно розв'язати задачу штучного розчленування замкненого кола. Розглянемо цю задачу із загальної точки зору.

Нехай на полюсах досліджуваного кола GПК діють напруги, що визначаються щодо потенціалу деякого базового полюса φ_o відповідними потенціалами $\varphi_h, \varphi_g, \varphi_d$ і φ_s. Припустимо, що потенціали φ_h, φ_g і φ_d формуються деякими джерелами сигналів, що мають низькі вихідні опори. З огляду на це запишемо вираз для визначення потенціалу φ_s:

$$\varphi_{\text{s}} = \left(\varphi_h \dot{Y}_x + \varphi_g \dot{Y}_s + \varphi_d Y_o\right) \Big/ \left(\dot{Y}_x + \dot{Y}_s + Y_o\right), \qquad (1)$$

Як видно з (1), у даний вираз не входить провідність $\dot{Y}_h$, що пояснюється тим, що даний двополюсник шунтується з обох сторін низькими вихідними опорами джерел потенціалів φ_h і φ_g. Звідси очевидно, що для того, щоб розв'язати задачу штучного розчленовування кола типу трикутник, необхідно ізолювати двополюсник $\dot{Y}_x$ від двополюсника $\dot{Y}_s$. Для цього достатньо створити рівність потенціалів φ_g та φ_s, при цьому, оскільки через двополюсник $\dot{Y}_s$ в даному випадку буде протікати нульовий струм, на ньому організується режим електричного розриву. Інакше задача розчленовування замкненого кола зводиться до задачі врівноваження чотириполюсника, що з математичної точки зору еквівалентно задачі розв'язання рівняння $\varphi_g - \varphi_s = 0$. З урахуванням (1), після нескладних перетворень отримаємо вираз

$$\varphi_g \frac{\dot{Y}_x + Y_o}{\dot{Y}_x + Y_o + \dot{Y}_s} - \varphi_h \frac{\dot{Y}_x}{\dot{Y}_x + Y_o + \dot{Y}_s} - \varphi_d \frac{Y_o}{\dot{Y}_x + Y_o + \dot{Y}_s} = 0, \qquad (2)$$

який назвемо невизначеним рівнянням врівноваження досліджуваного кола.

Розв'язання рівняння (2) полягає у тому, щоб знайти такі значення потенціалів φ_h, φ_g і φ_d, для яких його ліва частина обертається в нуль. У загальному випадку рівняння (2) є невизначеним, оскільки в ньому існує три невідомих (φ_h, φ_g, φ_d), що дає нескінченну множину розв'язків. Однак відомо, що для організації процесу врівноваження досліджуване коло GПК підключають в деяку структуру активних компонент, яка визначена щодо шини нульового рівня, і яка містить деяке джерело тестового сигналу V_o і джерело сигналу, що призводить досліджуване коло у стан рівноваги. При цьому, визначається орієнтація полюсів досліджуваного чотириполюсника щодо цих сигналів і шини нульового рівня, а оскільки значення тестового сигналу і потенціал шини нульового рівня є величинами незалежними, в рівнянні (2) визначиться тільки один залежний потенціал, значення якого формується джерелом сигналу врівноваження.

Таким чином, розглядаючи значення сигналу врівноваження як шукану змінну, за умови визначення орієнтації полюсів чотириполюсника, що лишилися, рівняння врівноваження (2) буде мати єдиний розв'язок, що і забезпечить розчленовування кола типу трикутник. При цьому, неоднозначність вибору полюсів для підключення тестового сигналу, шини нульового рівня і сигналу врівноваження зумовлюють широке різноманіття методів розв'язку задачі штучного розчленування замкнених кіл.

З виразу (2) очевидні три можливих варіанти вибору шуканої змінної: $\dot{u}_h = \varphi_h$; $\dot{u}_d = \varphi_d$; $\dot{u}_g = \varphi_g$. При цьому для кожного з них можна реалізувати по дві інверсні конфігурації підключення тестового сигналу і шини нульового рівня. Крім того, джерело тестового сигналу може підключатися як стосовно шини нульового рівня, так і полюсу шуканої змінної. Отже, існує дванадцять можливих способів розв'язання задачі розчленування замкнених кіл. Для кожного з цих способів з невизначеного рівняння врівноваження (2) можна отримати відповідні рівняння врівноваження, що будуть вже визначеними, і які будуть описувати різні методи ізоляції двополюсника $\dot{Y}_x$ від двополюсників $\dot{Y}_s$ і $\dot{Y}_h$.

Проаналізуємо рівняння (2) з метою отримання визначених рівнянь врівноваження. Нехай, наприклад, шуканою змінною є потенціал $\dot{u}_h = \varphi_h$. Винесемо за дужки співмножник при цій змінній і позначимо його як $\dot{\beta}_h = \dot{Y}_x \big/ \left(\dot{Y}_x + \dot{Y}_s + Y_o\right)$, внаслідок чого (2) перепишеться у вигляді:

$$\left\{\dot{u}_h - \left(\varphi_g\left(1 + Y_o/\dot{Y}_x\right) - \varphi_d\, Y_o/\dot{Y}_x\right)\right\}\dot{\beta}_h = 0. \qquad (3)$$

В отриманому рівнянні полюс h визначається як полюс шуканої змінної, однак при цьому ще не визначений полюс, що підключається до шини нульового рівня, а також не визначений спосіб підключення джерела тестового сигналу. Дорівнюючи по черзі до нуля потенціали незалежних полюсів досліджуваного кола GПК, що лишилися після визначення полюса підключення шуканої змінної, рівняння (3) розіб'ється на два рівняння:

$$\left(\dot{u}_{hg}^{d} + \varphi_d \, Y_o / \dot{Y}_x\right)\dot{\beta}_h = 0; \tag{4}$$

$$\left(\dot{u}_{hd}^{g} - \varphi_g\left(1 + Y_o / \dot{Y}_x\right)\right)\dot{\beta}_h = 0, \tag{5}$$

де верхній індекс визначає полюс надходить тестовий сигнал, а другий нижній індекс визначає полюс, що підключається до шини нульового рівня.

Тепер, якщо у кожному з рівнянь (4) і (5) визначити спосіб підключення джерела тестового сигналу, для кожного з них отримаємо по два рівняння, які відповідають випадкам заземленого і незаземленого джерела тестового сигналу. При цьому, в першому випадку значення напруги на полюсі, куди буде надходити тестовий сигнал визначається значенням V_o, а в другому – визначатися як додаток $V_o + \dot{u}_h$:

$$\left.\begin{aligned}&\left(\dot{u}_{hg}^{dg} + V_o \, Y_o / \dot{Y}_x\right)\dot{\beta}_h = 0;\\ &\left(\dot{u}_{hg}^{dh} + V_o \, Y_o / \left(Y_o + \dot{Y}_x\right)\right)\dot{\beta}_h = 0;\end{aligned}\right\} \tag{6}$$

$$\left.\begin{aligned}&\left(\dot{u}_{hd}^{gd} - V_o\left(1 + Y_o / \dot{Y}_x\right)\right)\dot{\beta}_h = 0;\\ &\left(\dot{u}_{hd}^{gh} + V_o\left(1 + \dot{Y}_x / Y_o\right)\right)\dot{\beta}_h = 0.\end{aligned}\right\} \tag{7}$$

В отриманих рівняннях два верхні індекси при шуканій змінній відповідають полюсам чотириполюсника врівноваження, різниця потенціалів між якими визначається значенням сигналу джерела тестового впливу.

Дотримуючись таких саме правил індексації, для шуканих змінних $\dot{u}_d = \varphi_d$ і $\dot{u}_g = \varphi_g$ можна записати вісім відповідних виразів для повністю визначених рівнянь рівноваження:

$$\left.\begin{aligned}&\left(\dot{u}_{dg}^{hg} + V_o \, \dot{Y}_x / Y_o\right)\dot{\beta}_d = 0;\\ &\left(\dot{u}_{dg}^{hd} + V_o \, \dot{Y}_x / \left(Y_o + \dot{Y}_x\right)\right)\dot{\beta}_d = 0;\end{aligned}\right\} \tag{8}$$

$$\left.\begin{aligned}&\left(\dot{u}_{dh}^{gh} - V_o\left(1 + \dot{Y}_x / Y_o\right)\right)\dot{\beta}_d = 0;\\ &\left(\dot{u}_{dh}^{gd} - V_o \, Y_o / \dot{Y}_x\right)\dot{\beta}_d = 0;\end{aligned}\right\} \tag{9}$$

$$\left.\begin{aligned}&\left(\dot{u}_{gh}^{dh} - V_o \, Y_o / \left(\dot{Y}_x + \dot{Y}_o\right)\right)\dot{\beta}_g = 0;\\ &\left(\dot{u}_{gh}^{dg} - V_o \, Y_o / \dot{Y}_x\right)\dot{\beta}_g = 0;\end{aligned}\right\} \tag{10}$$

$$\left.\begin{aligned}&\left(\dot{u}_{gd}^{hd} - V_o \, \dot{Y}_x / \left(\dot{Y}_x + Y_o\right)\right)\dot{\beta}_g = 0;\\ &\left(\dot{u}_{gd}^{hg} - V_o \, \dot{Y}_x / Y_o\right)\dot{\beta}_g = 0.\end{aligned}\right\}, \tag{11}$$

де $\dot{\beta}_d = Y_o / \left(\dot{Y}_x + \dot{Y}_s + Y_o\right)$; $\dot{\beta}_g = \left(Y_o + \dot{Y}_x\right) / \left(\dot{Y}_x + \dot{Y}_s + Y_o\right)$.

Таким чином, рівняння (6)-(11) описують дванадцять повністю визначених рівнянь врівноваження, кожне з яких відповідає конкретним методам врівноваження досліджуваного кола $G_{ПК}$. Сукупність цих рівнянь можна розглядати як узагальнену математичну модель задачі штучного розчленовування замкнених кіл. Для спрощення викладень таку модель зручно описувати матричним рівнянням, що дозволяє здійснювати подальші дослідження із загальної точки зору. Для того, щоб здійснити такий перехід від конкретних рівнянь до загального, введемо для складових членів цих рівнянь такі позначення.

$$\left(\dot{\boldsymbol{U}} - \boldsymbol{V_o}\dot{\boldsymbol{W}}\right)\dot{\boldsymbol{\beta}} = 0, \tag{12}$$

де $\dot{\boldsymbol{U}}$ – діагональна матриця шуканих змінних сукупності повністю визначених рівнянь врівноваження; $\dot{\boldsymbol{W}}$ – діагональна матриця співвідношень параметрів пасивних змінних, $\dot{\boldsymbol{\beta}}$ – вектор-стовпець нормалізуючих множників (коефіцієнтів зворотного зв'язку).

З аналізу (12) безпосередньо видно, що оскільки значення координат вектора $\dot{\boldsymbol{\beta}}$ не дорівнюють нулю, то для того щоб досліджуване коло знаходилося у стані рівноваги, нулю повинен дорівнювати, співмножник при цьому векторі. Тобто стан рівноваги описується виразом

$$\dot{\boldsymbol{U}} = V_o \dot{\boldsymbol{W}} . \tag{13}$$

Вираз (13) буде відповідати дійсності тільки у випадку ідеальних характеристик пристрою врівноваження, тобто коли крутизна перетворень пристрою врівноваження α та його вхідна провідність $y_{âõ}$ будуть прагнути до нескінченності, а вихідна провідність $y_{âèõ}$ буде прагнути до нуля. В реальних же умовах, застосовуючи методи теорії графів, зокрема, двонаправлених [9] передатна функція первинного перетворювача буде описуватись виразом:

$$\dot{\boldsymbol{W}} = \dot{\boldsymbol{W}}_o \frac{1 + \dot{Y}_{out} / y_{âèõ}\boldsymbol{\alpha}}{1 + \boldsymbol{\alpha}^{-1}\left[(\dot{\boldsymbol{\beta}}^{-1} + \frac{y_{âõ}}{\dot{Y}_{out}}) + \frac{\mathbf{1}}{y_{âèõ}}(\dot{Y}_{in} + \dot{Y}_s + y_{âõ})\right]}, \tag{14}$$

де $\dot{\boldsymbol{W}}_o$ - значення передатної функції перетворювача з ідеальними характеристиками пристрою врівноваження, а $\dot{Y}_{in}$ (Y_o або $\dot{Y}_x$) та $\dot{Y}_{out}$ ($\dot{Y}_x$ або $\dot{Y}_o$) – імпеданси двополюсників відповідно прямого та зворотнього зв'зків активного елемента (операційного підсилювача).

Таблиця 1 – Значення елементів матриці рівняння врівноваження (12)

№	$\dot{\boldsymbol{U}} = V_o \dot{\boldsymbol{W}}_o\left(\boldsymbol{1} + \dot{\boldsymbol{\gamma}}^{(\cdot)(\cdot)}_{(\cdot)(\cdot)}\right)$				$\dot{\boldsymbol{\gamma}}^{(\cdot)(\cdot)}_{(\cdot)(\cdot)} = -\left[\boldsymbol{1} + \boldsymbol{\alpha}\dot{\boldsymbol{\beta}}^{(\cdot)(\cdot)}_{(\cdot)(\cdot)}\right]^{-1}$
	$\boldsymbol{\varphi_h}$	$\boldsymbol{\varphi_d}$	$\boldsymbol{\varphi_g}$	$\dot{\boldsymbol{W}}_o$	$\dot{\boldsymbol{\beta}}$
1	$\dot{\boldsymbol{u}}^{\boldsymbol{dg}}_{\boldsymbol{hg}}$	$\boldsymbol{V_o}$	**0**	$\dot{\boldsymbol{w}}^{\boldsymbol{dg}}_{\boldsymbol{hg}} = -\boldsymbol{Y_o}/\dot{\boldsymbol{Y}}_{\boldsymbol{x}}$	$\dot{\boldsymbol{\beta}}^{\boldsymbol{dg}}_{\boldsymbol{hg}} = \dot{\boldsymbol{Y}}_{\boldsymbol{x}}/\left(\dot{\boldsymbol{Y}}_{\boldsymbol{x}} + \dot{\boldsymbol{Y}}_{\boldsymbol{s}} + \boldsymbol{Y_o}\right)$
2	$\dot{\boldsymbol{u}}^{\boldsymbol{dh}}_{\boldsymbol{hg}}$	$\dot{\boldsymbol{u}}^{\boldsymbol{dh}}_{\boldsymbol{hg}} + \boldsymbol{V_o}$	**0**	$\dot{\boldsymbol{w}}^{\boldsymbol{dh}}_{\boldsymbol{hg}} = -\boldsymbol{Y_o}/\left(\boldsymbol{Y_o} + \dot{\boldsymbol{Y}}_{\boldsymbol{x}}\right)$	$\dot{\boldsymbol{\beta}}^{\boldsymbol{dh}}_{\boldsymbol{hg}} = \left(\dot{\boldsymbol{Y}}_{\boldsymbol{x}} + \boldsymbol{Y_o}\right)/\left(\dot{\boldsymbol{Y}}_{\boldsymbol{x}} + \dot{\boldsymbol{Y}}_{\boldsymbol{s}} + \boldsymbol{Y_o}\right)$
3	$\dot{\boldsymbol{u}}^{\boldsymbol{gd}}_{\boldsymbol{hd}}$	**0**	$\boldsymbol{V_o}$	$\dot{\boldsymbol{w}}^{\boldsymbol{gd}}_{\boldsymbol{hd}} = \left(\dot{\boldsymbol{Y}}_{\boldsymbol{x}} + \boldsymbol{Y_o}\right)/\dot{\boldsymbol{Y}}_{\boldsymbol{x}}$	$\dot{\boldsymbol{\beta}}^{\boldsymbol{gd}}_{\boldsymbol{hd}} = \dot{\boldsymbol{Y}}_{\boldsymbol{x}}/\left(\dot{\boldsymbol{Y}}_{\boldsymbol{x}} + \dot{\boldsymbol{Y}}_{\boldsymbol{s}} + \boldsymbol{Y_o}\right)$
4	$\dot{\boldsymbol{u}}^{\boldsymbol{gh}}_{\boldsymbol{hd}}$	**0**	$\dot{\boldsymbol{u}}^{\boldsymbol{gh}}_{\boldsymbol{hd}} + \boldsymbol{V_o}$	$\dot{\boldsymbol{w}}^{\boldsymbol{gh}}_{\boldsymbol{hd}} = \left(\dot{\boldsymbol{Y}}_{\boldsymbol{x}} + \boldsymbol{Y_o}\right)/\boldsymbol{Y_o}$	$\dot{\boldsymbol{\beta}}^{\boldsymbol{gh}}_{\boldsymbol{hd}} = \boldsymbol{Y_o}/\left(\dot{\boldsymbol{Y}}_{\boldsymbol{x}} + \dot{\boldsymbol{Y}}_{\boldsymbol{s}} + \boldsymbol{Y_o}\right)$
5	$\boldsymbol{V_o}$	$\dot{\boldsymbol{u}}^{\boldsymbol{hg}}_{\boldsymbol{dg}}$	**0**	$\dot{\boldsymbol{w}}^{\boldsymbol{hg}}_{\boldsymbol{dg}} = -\dot{\boldsymbol{Y}}_{\boldsymbol{x}}/\boldsymbol{Y_o}$	$\dot{\boldsymbol{\beta}}^{\boldsymbol{hg}}_{\boldsymbol{dg}} = \boldsymbol{Y_o}/\left(\dot{\boldsymbol{Y}}_{\boldsymbol{x}} + \dot{\boldsymbol{Y}}_{\boldsymbol{s}} + \boldsymbol{Y_o}\right)$
6	$\dot{\boldsymbol{u}}^{\boldsymbol{hd}}_{\boldsymbol{dg}} + \boldsymbol{V_o}$	$\dot{\boldsymbol{u}}^{\boldsymbol{hd}}_{\boldsymbol{dg}}$	**0**	$\dot{\boldsymbol{w}}^{\boldsymbol{hd}}_{\boldsymbol{dg}} = -\dot{\boldsymbol{Y}}_{\boldsymbol{x}}/\left(\dot{\boldsymbol{Y}}_{\boldsymbol{x}} + \boldsymbol{Y_o}\right)$	$\dot{\boldsymbol{\beta}}^{\boldsymbol{hd}}_{\boldsymbol{dg}} = \left(\dot{\boldsymbol{Y}}_{\boldsymbol{x}} + \boldsymbol{Y_o}\right)/\left(\dot{\boldsymbol{Y}}_{\boldsymbol{x}} + \dot{\boldsymbol{Y}}_{\boldsymbol{s}} + \boldsymbol{Y_o}\right)$
7	**0**	$\dot{\boldsymbol{u}}^{\boldsymbol{gh}}_{\boldsymbol{dh}}$	$\boldsymbol{V_o}$	$\dot{\boldsymbol{w}}^{\boldsymbol{gh}}_{\boldsymbol{dh}} = \left(\dot{\boldsymbol{Y}}_{\boldsymbol{x}} + \boldsymbol{Y_o}\right)/\boldsymbol{Y_o}$	$\dot{\boldsymbol{\beta}}^{\boldsymbol{gh}}_{\boldsymbol{dh}} = \boldsymbol{Y_o}/\left(\dot{\boldsymbol{Y}}_{\boldsymbol{x}} + \dot{\boldsymbol{Y}}_{\boldsymbol{s}} + \boldsymbol{Y_o}\right)$
8	**0**	$\dot{\boldsymbol{u}}^{\boldsymbol{gd}}_{\boldsymbol{dh}}$	$\dot{\boldsymbol{u}}^{\boldsymbol{gd}}_{\boldsymbol{dh}} + \boldsymbol{V_o}$	$\dot{\boldsymbol{w}}^{\boldsymbol{gd}}_{\boldsymbol{dh}} = \left(\dot{\boldsymbol{Y}}_{\boldsymbol{x}} + \boldsymbol{Y_o}\right)/\dot{\boldsymbol{Y}}_{\boldsymbol{x}}$	$\dot{\boldsymbol{\beta}}^{\boldsymbol{gd}}_{\boldsymbol{dh}} = \dot{\boldsymbol{Y}}_{\boldsymbol{x}}/\left(\dot{\boldsymbol{Y}}_{\boldsymbol{x}} + \dot{\boldsymbol{Y}}_{\boldsymbol{s}} + \boldsymbol{Y_o}\right)$
9	**0**	$\boldsymbol{V_o}$	$\dot{\boldsymbol{u}}^{\boldsymbol{dh}}_{\boldsymbol{gh}}$	$\dot{\boldsymbol{w}}^{\boldsymbol{dh}}_{\boldsymbol{gh}} = \boldsymbol{Y_o}/\left(\dot{\boldsymbol{Y}}_{\boldsymbol{x}} + \boldsymbol{Y_o}\right)$	$\dot{\boldsymbol{\beta}}^{\boldsymbol{dh}}_{\boldsymbol{gh}} = \left(\dot{\boldsymbol{Y}}_{\boldsymbol{x}} + \boldsymbol{Y_o}\right)/\left(\dot{\boldsymbol{Y}}_{\boldsymbol{x}} + \dot{\boldsymbol{Y}}_{\boldsymbol{s}} + \boldsymbol{Y_o}\right)$
10	**0**	$\dot{\boldsymbol{u}}^{\boldsymbol{dg}}_{\boldsymbol{gh}} + \boldsymbol{V_o}$	$\dot{\boldsymbol{u}}^{\boldsymbol{dg}}_{\boldsymbol{gh}}$	$\dot{\boldsymbol{w}}^{\boldsymbol{dg}}_{\boldsymbol{gh}} = \boldsymbol{Y_o}/\dot{\boldsymbol{Y}}_{\boldsymbol{x}}$	$\dot{\boldsymbol{\beta}}^{\boldsymbol{dg}}_{\boldsymbol{gh}} = \dot{\boldsymbol{Y}}_{\boldsymbol{x}}/\left(\dot{\boldsymbol{Y}}_{\boldsymbol{x}} + \dot{\boldsymbol{Y}}_{\boldsymbol{s}} + \boldsymbol{Y_o}\right)$
11	$\boldsymbol{V_o}$	**0**	$\dot{\boldsymbol{u}}^{\boldsymbol{hd}}_{\boldsymbol{gd}}$	$\dot{\boldsymbol{w}}^{\boldsymbol{hd}}_{\boldsymbol{gd}} = \dot{\boldsymbol{Y}}_{\boldsymbol{x}}/\left(\dot{\boldsymbol{Y}}_{\boldsymbol{x}} + \boldsymbol{Y_o}\right)$	$\dot{\boldsymbol{\beta}}^{\boldsymbol{hd}}_{\boldsymbol{gd}} = \left(\dot{\boldsymbol{Y}}_{\boldsymbol{x}} + \boldsymbol{Y_o}\right)/\left(\dot{\boldsymbol{Y}}_{\boldsymbol{x}} + \dot{\boldsymbol{Y}}_{\boldsymbol{s}} + \boldsymbol{Y_o}\right)$
12	$\dot{\boldsymbol{u}}^{\boldsymbol{hg}}_{\boldsymbol{gd}} + \boldsymbol{V_o}$	**0**	$\dot{\boldsymbol{u}}^{\boldsymbol{hg}}_{\boldsymbol{gd}}$	$\dot{\boldsymbol{w}}^{\boldsymbol{hg}}_{\boldsymbol{gd}} = \dot{\boldsymbol{Y}}_{\boldsymbol{x}}/\boldsymbol{Y_o}$	$\dot{\boldsymbol{\beta}}^{\boldsymbol{hg}}_{\boldsymbol{gd}} = \boldsymbol{Y_o}/\left(\dot{\boldsymbol{Y}}_{\boldsymbol{x}} + \dot{\boldsymbol{Y}}_{\boldsymbol{s}} + \boldsymbol{Y_o}\right)$

Аналізуючи вираз (14) можна дійти висновку, що члени, які містять співмножники $\alpha^{-1}\, y_{вих}^{-1}$ і $y_{вх}\, \alpha^{-1}$ мають менші порядки малості і ними можна зневажити. Таким чином (14) можна переписати у вигляді:

$$\dot{W} = \dot{W}_o(1+\dot{\gamma}), \tag{15}$$

$$\dot{\gamma} = -\left[1+\alpha\dot{\beta}\right]^{-1},$$

де $\dot{\gamma}$ визначає мультиплікативну складову похибки перетворень, а вихідний сигнал перетворювачав буде визначатися виразом:

$$\dot{U} = V_o\, \dot{W}_o(1+\dot{\gamma}).$$

Виходячи з вище викладеного, можна дійти висновку, що коли притримуватися зазначеним вище правилам індексації під час конкретного розв'язання задачі врівноваження досліджуваних кіл, то правила визначення такої системи індексації формально можна розглядати як узагальнений алгоритм синтезу структурних схем перетворювачів параметрів елементів замкнених електричних кіл.

Таким чином формули, що описують конкретні розв'язання задачі врівноваження будуть визначати функції перетворення відповідних структур перетворювачів. Конкретні структурні схеми перетворювачів, що побудовані із застосуванням вищеописаного алгоритму, наведені у табл. 2.

Для усіх структурних схем електрична ізоляція досліджуваних двополюсників $\dot{Y}_x$ від двополюсника $\dot{Y}_s$ забезпечується за умови досягнення рівноваги потенціалів на полюсах двополюсника $\dot{Y}_s$. Стан рівноваги для груп структурних схем C_h і C_d досягається під час врівноваження струмів, а для групи структурних схем C_g – під час врівноваження напруг.

Для усіх структурних схем електрична ізоляція досліджуваних двополюсників $\dot{Y}_x$ від двополюсника $\dot{Y}_s$ забезпечується за умови досягнення рівноваги потенціалів на полюсах двополюсника $\dot{Y}_s$. Стан рівноваги для груп структурних схем C_h і C_d досягається під час врівноваження струмів, а для групи структурних схем C_g – під час врівноваження напруг.

Наведені вище структурні схеми розглядаються надалі як базові структури перетворювачів параметрів елементів у замкнених колах.

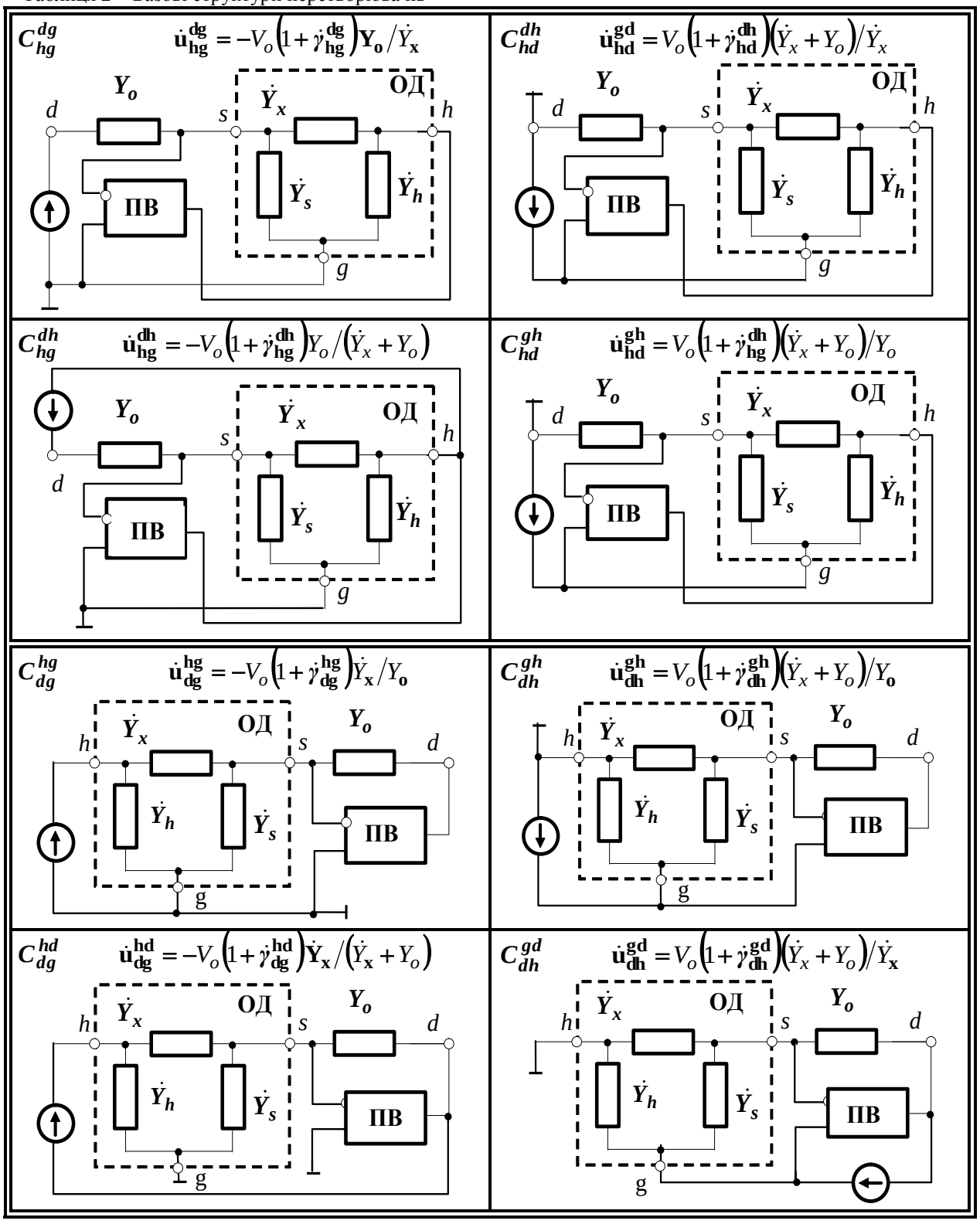
З аналізу виразів у табл. 1 можна зробити зробити висновки що застосовуючи лва перетворення у структурах що мають однакові значення нормалізуючих множників $\dot{\beta}$ і розділити їх результати перетворень можна виключити мультиплікативну складову похибки, при цьому отримати лінійну залежність перетворень. До таких пар структур слід віднести пари C_{hg}^{dh}/C_{dg}^{hd} і C_{gh}^{dh}/C_{dg}^{hd} . При цьому передатні функції для цих пар будуть визначатись як:

$$w(C_{hg}^{dh}/C_{dg}^{hd}) = Y_o/\dot{Y}_x,$$
$$w(C_{gh}^{dh}/C_{dg}^{hd}) = Y_o/\dot{Y}_x.$$

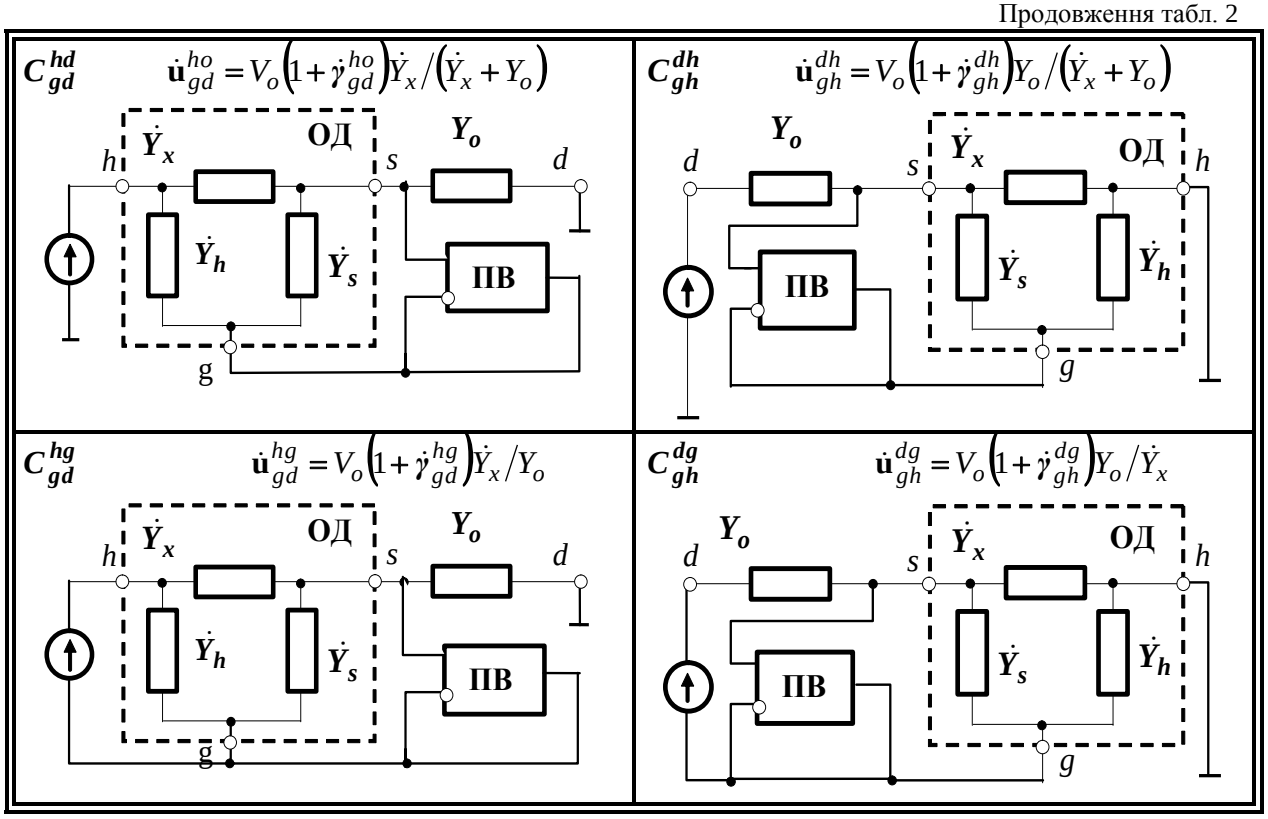
Або, якщо поміняти місцями чисельники зі знаменниками, отримаємо фннкцію:

$$w = \dot{Y}_x/Y_o.$$

Таблиця 2 – Базові структури перетворювачів



Продовження табл. 2



Висновки

1. Побудована узагальнена математична модель розв'язання задачі інваріантних перетворень параметрів елементів у складних біологічних об'єктах.

2. Визначено комплекс базових структурних схем інваріантних перетворювачів у задачах медичної та технічної діагностики.

3. Визначено мультиплікативні похибки перетворень базових структурних схем.

4. Розроблено структурно-агоритмічні методи підвищення точності вимірювань в системах діагностики біологічних та технічних об'єктів.

Список літератури

1. Портнов Ф.Г. Электропунктурная рефлексотерапия. – Рига: Зинатне, 1988. – 352 с.

2. Електропунктурна діагностика по Фоллю: http://biosan.te.ua/diagnostyka-po-follju.html

3. Метрологические основы электропунктурной диагностики**:** http://medem.kiev.ua/page.php?pid=1799

4. Основные принципы электропунктурной диагностики Бойцов И.В. // Рефлексотерапия. - М, 2003. - № 3(6).-С.51-55.

5. Основные принципы электропунктурной диагностики Бойцов И.В. // Рефлексология. - М, 2003. - № 1.- 61-62

6. Роїк О.М. Контроль і діагностика радіоелектронної апаратури на етапах її виробництва. Монографія. – Вінниця: УНІВЕСУМ - Вінниця, 2000. – 170 с.

7. Роїк О.М., Арсенюк І.Р., Месюра В.І. Перетворення параметрів елементів замкнених кіл. Монографія. – Вінниця: УНІВЕРСУМ-Вінниця, 2004. - 110 с.

8. Роїк О.М., Арсенюк І.Р. Діагностування аналогових пристроїв радіоелектронної апаратури. Монографія. – Вінниця: УНИВЕРСУМ – Вінниця, 2005. – 250 с.

9. Роїк О.М. Інваріантні перетворення параметрів елементів складних об'єктів. Монографія. – Вінниця: УНІВЕСУМ - Вінниця, 2001. – 152 с.

10. Роїк О.М., Власюк А.І. Інваріантні вимірювання параметрів біологічних об'єктів в системах медичної діагностики // Вісник ВПІ, 1999. – №2. – С. 8-11.

11. Роїк О.М., Власюк А.І. Методи вимірювання параметрів біологічних об'єктів в задачах медичної діагностики / Контроль і управління в складних системах (КУСС-99). – Т.3. – Вінниця: УНІВЕРСУМ - Вінниця. – 1999. – С. 166-177.

12. Роїк О.М., Перевозніков С.І., Снігур А.В., Яремко С.А. Інформаційно-вимірювальна система діагностування функціонального стану людини на основі первинного інваріантного перетворювача // Інформаційні технології та комп'ютерна інженерія. – 2010. – №1(17). – С.28-31.

13. Роїк О.М., Яремко С.А. Система діагностування функціонального стану людини на основі інваріантного перетворювача параметрів БАТ // Інформаційні технології та комп'ютерна інженерія. – 2010. - №2(18). – С.80-84.

14. Роїк О.М., Яремко С.А. Методи і засоби моделювання телемедичних систем функціонального стану людини. Монографія. – Вінниця: УНІВЕРСУМ –Вінниця : ВНТУ, 2012. – 144 с.

Відомості про авторів

Роїк Олександр Митрофанович – д. т. н., професор, завідувач кафедри менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет, Хмельницьке шосе, 95, м. Вінниця, 21021: тел. 598294.

Поплавський Анатолій Вацлавович – к. т. н., доцент кафедри менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет, Хмельницьке шосе, 95, м. Вінниця, 21021: тел. 598294.

Азарова Анжеліка Олексіївна – к. т. н., професор кафедри менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет, Хмельницьке шосе, 95, м. Вінниця, 21021: тел. 598294.

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

УДК 004.942:504.05

О. Н. Землянський, О. Н. Мирошник, А. Н. Черненко, С. В. Куценко

АСПЕКТЫ НЕОПРЕДЕЛЕННОСТИ ПРОЦЕССА МОНИТОРИНГА КОНЦЕНТРАЦИИ ОПАСНЫХ ВЕЩЕСТВ ПРИ АВАРИЙНОМ ВЫБРОСЕ

Черкасский институт пожарной безопасности им. Героев Чернобыля Национального университета гражданской защиты Украины

Анотація. Розглянуто аспекти невизначеності процесу моніторингу концентрації небезпечних речовин при аварійному викиді. Доведено, що прогнозування наслідків аварій відбувається в умовах невизначеності викликаної їх раптовістю і критичністю процесів прийняття рішень. Вказано на необхідність здійснення поспрогнозірованія або уточнення значень параметрів хімічних аварій в післяаварійний період. Запропоновано вихідні дані для прогнозування отримувати з експертних висновків із додатковим точковим вимірюванням концентрації небезпечної хімічної речовини в реперних точках, і на їх підставі здійснювати корекцію прийнятих рішень. Для визначення зони і характеру зараження використані моделі нечіткої логіки і нейромережеві технології.

Ключові слова: прогнозування; концентрація небезпечної хімічної речовини; зона зараження.

Аннотация. Рассмотрены аспекты неопределённости процесса мониторинга концентрации опасных веществ при аварийном выбросе. Доказано, что прогнозирования последствий аварий происходит в условиях неопределенности вызванной их внезапностью и критичностью процессов принятия решений. Указано на необходимость осуществления прогнозирования или уточнение значений параметров химических аварий в послеаварийный период. Предложено исходные данные для поспрогнозирования получать с экспертных заключений с дополнительным точечным замером концентрации опасного химического вещества в реперных точках, и на их основании осуществлять коррекцию принимаемых решений. Для определение зоны и характера заражения использованы модели нечеткой логики и нейросетевые технологии.

Ключевые слова: прогнозирование; концентрация опасного химического вещества; зона заражения.

Abstract. Examined the uncertainty aspects of the process of monitoring of concentration of dangerous substances in case of emergency ejection. It is proved that the prediction of consequences of accidents occur in conditions of uncertainty due to their suddenness and criticality of decision-making processes. Indicated the need for the implementation of postprocesarea ABO clarification of the values of the parameters of chemical accidents in the post-accident period. Proposed baseline data for pospro is forecasting to obtain expert opinions with additional spot measurements of the concentrations of hazardous chemicals at fixed points, and on their basis to carry out the cor-the calibre of decisions. For the definition of the zone and the nature of the infection model used fuzzy logic and neural network technology.

Keywords: prediction; the concentration of dangerous chemical substances; the area of infection.

Введение

Масштабность химических аварий и их последствий определяют необходимость решения научно-технической проблемы прогнозирования концентрации опасного химического вещества (ОХВ) во всей зоне заражения. Поскольку аварии происходят, в основном, на предприятиях, производящих ОХВ, в местах их хранения или при транспортировке, то для каждого такого случая необходимо получить модели, позволяющие по начальным параметрам аварии определять поля концентрации во всей возможной зоне заражения или значение концентрации ОХВ в конкретных точках.

Прогнозирование последствий аварии происходит в условиях неопределенности, вызванной их внезапностью и критичностью процессов принятия решений. Очевидно, что нужно различать прогнозирование как оперативное, тактическое и стратегическое. В первом случае определяют масштабы аварии и предполагаемые последствия в ближайшее время (3-5 часов). Стратегическое прогнозирование призвано дать ответы на вопрос о зоне заражения, необходимость эвакуации людей, возможные убытки и действия спасательных служб. Определение времени ликвидации последствий аварии, ее влияния на окружающую среду, количественного и качественного состава технических средств составляет предмет стратегического прогнозирования. Необходимым является также постпрогнозирование или уточнение значений параметров химической аварии в послеаварийный период.

Результаты исследования

Поскольку исходные точные значения параметров аварии неизвестны, они определяются в результате экспертных заключений. На их основании принимаются следующие решения. Очевидно, что если точность таких выводов является низкой, то и эффективность принятых решений будет невысокой. Поэтому необходимо осуществлять точечные замеры концентрации опасного вещества в реперных точках и на их основании осуществлять коррекцию принимаемых решений.

В период времени, предшествующий аварии, необходимо идентифицировать зависимость

$$C = F(P), \tag{1}$$

где C – концентрация ОХВ. Вектор параметров и факторов P имеет следующую структуру:

$$P=(x_0,y_0,z_0,t_0,x,y,z,t,M,W,D,T,V,R,U), \quad (2)$$

где: (x_0,y_0,z_0,t_0) – координаты точки и времени возникновения аварии;

(x,y,z,t) – координаты точки, в которой определяется концентрация ОХВ, и соответствующее время; другие параметры аварии являются известными константами.

Идентификация (1) осуществляется с использованием нечетких продукционных правил. Далее будет предложено несколько методов идентификации параметров (2), в зависимости от того, известны ли параметры функций принадлежности [1, 2]. Составляющими технологиями является нечеткое логическое выведение в форме Мамдани, нейронечеткие сети и эволюционное моделирование. Показано, что решение задачи постпрогнозирования заключается в решении обратной задачи (определение начальных значений параметров аварии), то есть в идентификации отображения

$$G: C(x,y,z,t) \to (x_0,y_0,z_0,t_0). \quad (3)$$

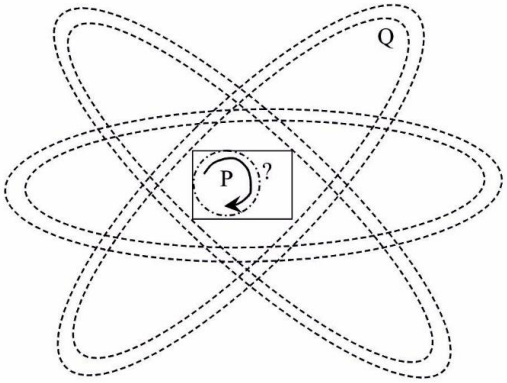


Рисунок 1 – Объект Ω и его окружение

Рассмотрим задачи прогнозирования техногенных и экологических катастроф. При этом будем считать, что объект, который представляет потенциальный источник опасности, является недвижимым. Обозначим его Ω, внутренние процессы объекта – P, внешние действия – Q. Таким образом, имеем некоторую информационную модель (рис. 1), на которой показано, что объект Ω находится в сфере влияния систем различной природы, которые, в большинстве случаев, имеют иерархическую структуру.

Определим аварию (A) как состояние некоторого объекта, при котором значения одной или нескольких характеристик превышает предельные значения, то есть

$$A=< S=(s_1,s_2,...,s_n)/\exists s_j : s_j > K_j >,$$

где $s_i, i=\overline{1,n}$ – характеристики объекта, K_j – критическое значение s_j-й характеристики; s_j – концентрация некоторого вещества, превышение которой значение K_j приводит к негативным последствиям без возможности возврата. Предположим, что значение характеристики является следствием влияния совокупности факторов $D=(d_1,d_2,...,d_m)$ з m источников, на нее оказывают влияние неуправляемые факторы внешней среды $E=(e_1,e_2,...,e_k)$ и осуществляет влияние человек через проведение совокупности мероприятий $Z=(z_1,z_2,...,z_l)$. Таким образом, значение s_j определяется функциональной зависимостью

$$s_j=F(D,E,Z)=F(g_1(d_1,d_2,...,d_m),g_2(e_1,e_2,...,e_k),g_3(z_1,z_2,...,z_l)),\ j=\overline{1,n}.$$

Каждая из функций $g_i, i=\overline{1,3}$, имеет характерные особенности. Так, значения факторов являются исходными характеристиками предприятий (источников потенциальной опасности) и являются функциями их внутреннего состояния и входных параметров. Предполагая устойчивую динамику функционирования предприятий, значение $d_i, i=\overline{1,m}$, можно прогнозировать. Если информация о его функциониро-

вании неизвестна, то статистика значений $d_i, i=\overline{1,m}$, позволяет ориентироваться на средние величины. Если необходим более точный прогноз, то рационально использовать экспертные выводы.

Предположим, что объект Ω может быть поврежден или разрушен в результате длительного действия внутренних, внешних факторов или их композиции. Если это не так, то имеет место случайная авария или катастрофа, вызванная быстрым действием другой системы, не имеющей непосредственного отношения к объекту Ω и релевантных систем. Конечно такое действие имеет механическую природу. Пусть внутренние факторы являются элементами множества $P=\{p_1, p_2, ..., p_n\}$, внешние действия – элементами множества $Q=\{q_1, q_2, ..., q_m\}$. Очевидно, что количество факторов, и внешних действий является значительно больше, но такой состав множеств P и Q определяется значимостью их составляющих. Упростим задачу и допустим, что авария или катастрофа возможна при критическом значении одного или нескольких элементов из множества Q.

В таком случае необходимо решить задачу идентификации зависимости

$$K_j = f_j(t, \xi_j), \tag{4}$$

где K_j – концентрация опасного вещества, ξ_j – обозначения группы факторов, оказывающих влияние на динамику K_j, $j=\{1,2,...,m\}$. Если внешнее воздействие, что вызывает катастрофические последствия, не является единичной, то имеют место задачи определения

$$\begin{aligned} K_{j_1} \vee K_{j_2} \vee ... \vee K_{j_k} &= K_{кр}^{\vee}, \\ K_{j_1} \wedge K_{j_2} \wedge ... \wedge K_{j_k} &= K_{кр}^{\wedge}, \end{aligned} \tag{5}$$

где

$$\begin{aligned} K_{кр}^{\vee} &= \max\{K_{j_1}, K_{j_2}, ..., K_{j_k}\} > K_{кат}, \\ K_{кр}^{\wedge} &= \min\{K_{j_1}, K_{j_2}, ..., K_{j_k}\} < K_{кат}, \end{aligned} \tag{6}$$

при таких ограничениях ($K_{кат}$ – значение, которое указывает на катастрофу):

$$\begin{aligned} &\max_l K_{j_l} < K_{\max}, \\ &\min_l K_{j_l} > K_{\min}, \; l=\overline{1,k}. \end{aligned} \tag{7}$$

В (7) $K_{\min}, K_{\max}$ – предельно возможные значения параметров внешней среды. Необходимым условием решения задач (4) – (7) есть поиск зависимости концентрации от времени и воздействующих факторов. Именно зависимость типа (3) позволяет осуществить анализ типа «Если $t=t^*$ и $\xi_j \in \Theta_j$, то $K_j = K^*$», где Θ_j – некоторая область изменения значений факторов. Однако, в подавляющем большинстве случаев получить зависимость (3) и решить задачи (4) – (7) оказывается невозможным. Причинами этого являются: отсутствие необходимых данных; наличие влияния факторов, которые априори не относятся до множеств, что учитываются; значительные колебания значений одного из факторов, которые не позволяют установить уровень его влияния на уровень концентрации опасного вещества и т. п.

В таких случаях было бы полезным учитывать опыт экспертов. Формальный аппарат для счисления выводов экспертов составляют модели и методы теории нечетких множеств [3, 4]. В нашем случае базовой моделью является система нечетких продукционных правил

$$\begin{aligned} &\textit{Если } q_1 \in A_1^1 \,\&\, q_2 \in A_2^1 \,\&\, ... \,\&\, q_m \in A_m^1, \textit{ то } K_j \in B_j^1, \\ &\textit{иначе, если } q_1 \in A_1^2 \,\&\, q_2 \in A_2^2 \,\&\, ... \,\&\, q_m \in A_m^2, \textit{ то } K_j \in B_j^2, \\ &\quad ..... \\ &\textit{иначе, если } q_1 \in A_1^{м} \,\&\, q_2 \in A_2^{м} \,\&\, ... \,\&\, q_m \in A_m^{м}, \textit{ то } K_j \in B_j^{м}, \end{aligned} \tag{8}$$

где A_i^l – нечеткие множества с соответствующими функциями принадлежности [5, 6, 7], $i=\overline{1,m}$, $l=\overline{1,v}$, v – количество возможных комбинаций нечетких значений параметров, которые опре-

деляются экспертами. Б. Коско было показано, что системой (8) можно как угодно точно приблизить любую непрерывную функцию, если консеквент является аддитивным выражением [8]. Так, если имеет место логический вывод в форме Сугено, то выражение $K_j \in B_j^d$ приобретает вид $K_j = z_1^j + z_2^j + ... + z_{w1}^j$, где z_i^j – концентрация опасного вещества, полученной с i-го источника. Очевидно, что решаемая задача с физическим содержанием не может быть приведенной к виду, где рациональным было бы применение нечеткого логического вывода в форме Сугено [9].

Лучше всего поставленной задаче соответствует нечеткое логическое выведение в форме Мамдани. Его рационально использовать в случае небольшого количества нечетких продукционных правил и возможности дефазифицировать полученные развязки. Приведем его основные шаги [2].

Для простоты предположим, что базу знаний организуют два нечетких правила вида:

P_1: если $x \in A_1$ і $y \in B_1$, то $Z \in C_1$,

P_2: если $x \in A_2$ і $y \in B_2$ то $Z \in C_2$.

Шаг 1. Находим степени истинности $A_1(x_0),\ A_2(x_0),\ B_1(y_0),\ B_2(y_0)$.

Шаг 2. Находим уровни "отсечения" для предпосылок каждого из правил

$$\alpha_1 = A_1(x_0) \wedge B_1(y_0),$$
$$\alpha_2 = A_2(x_0) \wedge B_2(y_0).$$

Шаг 3. Находим функции принадлежности

$$C_1^{'}(Z) = (\alpha_1 \wedge C_1(Z)),$$
$$C_2^{'}(Z) = (\alpha_2 \wedge C_2(Z)).$$

Шаг 4. Выполняем объединение найденных функций и находим результирующее нечеткое множество для переменной выхода с функцией принадлежности

$$\mu_\theta(Z) = C(Z) = C_1^{'}(z) \vee C_2^{'}(Z) = (\alpha_1 \wedge C_1(Z)) \vee (\alpha_2 \wedge C_2(Z)).$$

Шаг 5. Выполняем дефазификацию, например по методу центра тяжести и находим четкое значение $Z_0 = \frac{\int_{\underline{z}}^{\overline{z}} z\mu_\theta(z)dz}{\int_{\underline{z}}^{\overline{z}} \mu_\theta(z)dz}$, где интервал $[\underline{z}, \overline{z}]$ является носителем функции принадлежности.

Таким образом, система (8) позволяет осуществить прогнозирование и сценарный анализ, поскольку, подставляя значения параметров $(q_1^0, q_2^0, ..., q_m^0)$ в (8), определим искомое значение концентрации K_j^0 опасного вещества. Система (8) отражает опыт одного эксперта и результат, получаемый с ее использованием, часто является смещенным, таким, что представляет интерес только для предварительного заключения. Для объективизации результатов прогнозирования (8) может быть обобщен. В таком случае система выражений типа (8) представляет заключения коллектива экспертов.

Еще одним аспектом аварий и катастроф является то, что во многих случаях процессы, к ним приводящие, развиваются во времени. Существуют такие моменты времени, после которых катастрофа становится неизбежной. Как пример, достаточно представить концентрацию вредных веществ в воде. До определенного уровня она считается допустимой, но превышение этого уровня становится катастрофой и причиной человеческих жертв. В то же время такие процессы непросто остановить, поскольку даже при прекращении опасного производства рост концентрации вредных веществ какое-то время продолжается. В связи с этим рационально учитывать общие положения теории катастроф [10]. Динамика соответствующего процесса представлена на рис. 2.

Точками обозначены следующие события: A– концентрация ОХВ достигла опасного уровня и необходимо проводить мероприятия по ее уменьшению; B– точка, предшествующий катастрофе, поскольку в момент времени t_B катастрофу остановить, в большинстве случаев, невозможно вследствие инерционности процесса роста концентрации опасного вещества; C – точка катастрофы, после которой рост концентрации вещества имеет форму квадратичной или экспоненциальной зависимости.

Осуществляя формирование базы данных и идентификацию зависимости (8), необходимо учитывать то, что процессы на участках $(0, t_A)$, (t_A, t_B), (t_B, t_C), $(t_C, ...)$ имеют размытый характер. Учет соответствующих особенностей и опыта экспертов, сконцентрированного в функциях принадлежности си-

стемы (8), позволит осуществлять управляющие действия с целью предотвращения катастроф. Заметим, что технологии решения задач первого типа, то есть прогнозирование аварий и катастроф, в современной научной литературе почти отсутствуют.

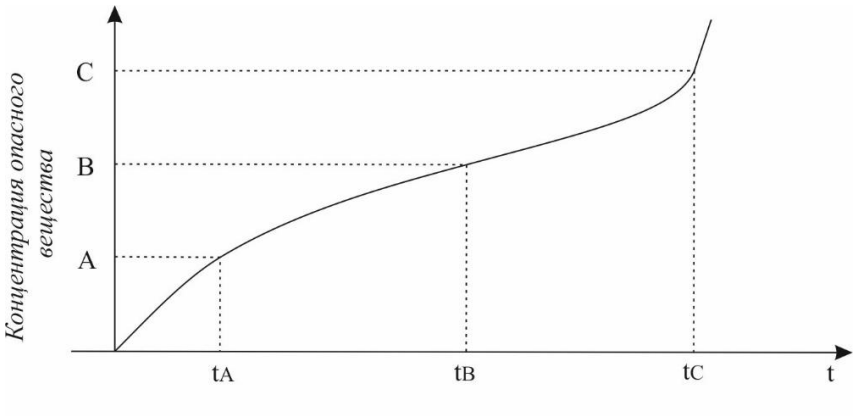


Рисунок 2 – Динамика концентрации опасного вещества

В отличие от них, задачи определения масштабов аварий или катастроф, расчета зоны возможного заражения широко представлены различного рода методиками. В то же время отметим, что они ориентированы на расчет размеров и площади зоны заражения, времени подхода облака зараженного воздуха к определенному объекту, времени поражающего действия и возможных потерь, исходя из таблиц, содержащих значения разного рода поправочных коэффициентов. Известно, что зона химического заражения рассчитывается, исходя из схемы (рис. 3).

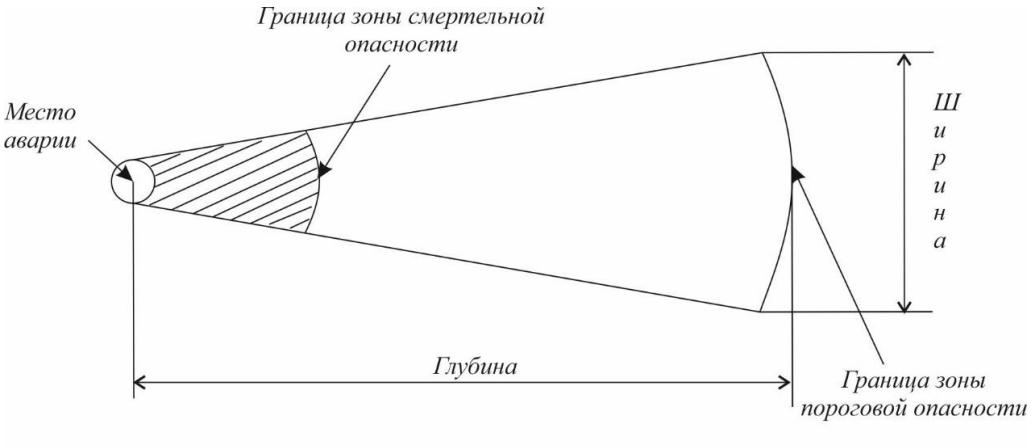


Рисунок 3 – Зона химического заражения

Все методики расчетов основаны на этой схеме. В большинстве практических ситуаций соответствующие результаты не будут отражать реальное послеаварийное состояние. Это связано с неполным учетом факторов, влияющих на концентрацию опасных веществ, в частности, рельеф местности и его характер могут быть причиной увеличения или уменьшения концентрации. Еще одной причиной является смена характера погодных условий и характера аварии. В таком случае получим схему (рис. 4), использование которой позволит уточнить результаты предыдущих расчетов (на схеме рис. 3).

Рис. 4 является всего лишь примерной схемой для определения последствий аварии. Можно предложить два способа определения концентрации опасного вещества в данной зоне. Первый из них базируется на идентификации зависимости

$$K_j = F_j(x, \varphi, P, Q), \tag{9}$$

где x и φ – полярные координаты точки, в которой определяем концентрацию, внутренние факторы интегрируют в себе показатели, связанные с объектом и местом аварии, Q – факторы внешнего воздействия (погодные условия, рельеф и т. п). Задавая значения указанных параметров, с помощью (9) можно рассчитать значение концентрации опасного вещества в любой точке. Второй способ заключается в ин-

теграции экспертных оценок с помощью системы (8). Нечеткие множества, которые присутствуют в (8), позволяют учесть размытость границ как зоны смертельной опасности, так и пороговой зоны опасности.

Построение моделей (8) и (9) необходимо осуществлять в пассивном режиме, то есть тогда, когда ни аварий, ни катастроф нет. Для этого необходима ретроспективная информация, которая содержит или параметры аварий, что уже произошли, или оценки экспертов. Очевидно, что такие данные не «покрывают» всю область заражения, поэтому получить и (8) и (9) можно с помощью обучения и, как следствие, интерполированием или экстраполированием. По результатам предварительного анализа моделей идентификации определено, что для модели (9) оптимальным представлением является прямосвязная нейронная сеть, а для моделей типа (8) – нейронечеткие сети типа TSK или ANFIS [11, 12, 13]. Выбор той или иной нейросетевой архитектуры определяется типом исходных данных, предполагаемых результатов и задачи.

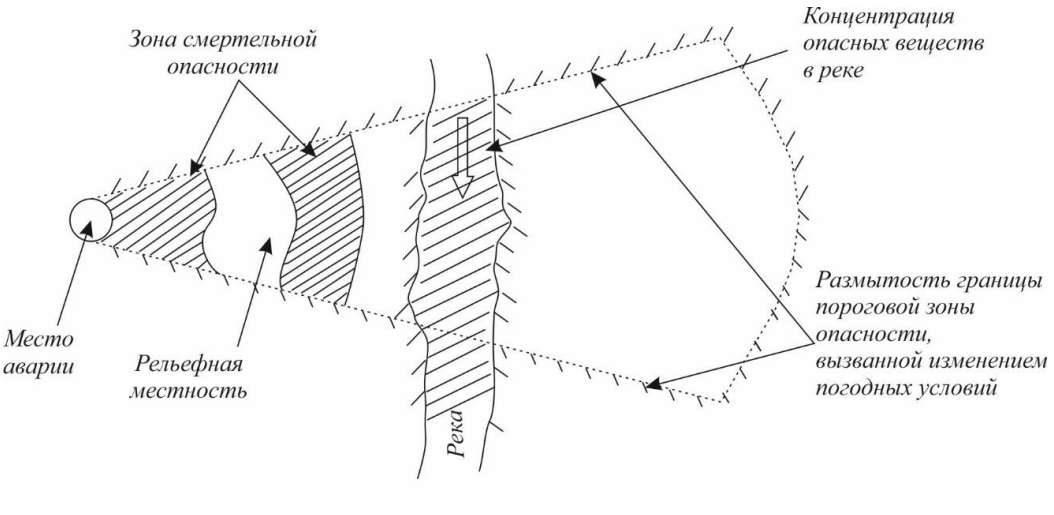


Рисунок 4 – Уточненная зона химического загрязнения

Выводы

Таким образом в статье рассмотрены аспекты неопределённости процесса мониторинга концентрации опасных веществ при аварийном выбросе. Доказано, что решить задачи третьего класса («послеаварийные задачи») можно с помощью полученных результатов предварительно решенных задач. При этом нужно использовать Марковский принцип – «Будущее зависит от настоящего времени и не зависит от прошлого». В частности, определение концентрации опасного вещества в воздухе, почве или в воде зависит от ее начального значения сразу же после аварии, или, в отдельных случаях, от того, какого максимального значения достиг уровень концентрации вещества после аварии.

Прогнозирование значений параметров зоны и характера заражения, может быть осуществлено с помощью моделей нечеткой логики и нейросетевых технологий. Исходные данные для прогнозирования можно получать с экспертных заключений с дополнительным точечным замером концентрации опасного химического вещества в реперных точках. На основании последних – осуществлять коррекцию принимаемых решений.

Список литературы

1. Байдык Т. Н. Нейронные сети и задачи искусственного интеллекта / Т. Н. Байдык. – К.: Наук. думка, 2001. - 260 с.
2. Снитюк В. Е. Прогнозирование. Модели, методы, алгоритмы / В. Е. Снитюк. – К.: Маклаут, 2008. – 364 с.
3. Барсегян А. А. Методы и модели анализа данных: OLAP и Data Mining / А.А. Барсегян, М. С. Куприянов, В. В. Степаненко, И. И. Холод. – СПб.: БХВ-Петербург, 2004. – 336 с.
4. Землянский О.Н. Элементы теории прогнозирования чрезвычайных ситуаций в условиях неопределенности / О.Н. Землянський // Материалы V межд. школы-семинара «Теория принятия решений». – Ужгород: УжНУ, 2010. – С. 102.
5. Fuzzy Models and Algorithms for Pattern Recognition and Image Processing / James C. Bezdek (et al). − Springer Science+Business Media, Inc. − 2005. − 776 p.
6. Землянский О. Н. Аспекты неопределенности процесса прогнозирования концентрации опасных химических веществ после аварии / О. Н. Землянский // Материалы 15-й межд. научн.-техн. конф.:

«Системный анализ и информационные технологиию» – К.: УНК «ИПСА» НТУУ «КПИ», 2013. – С.111.

7. Нечеткие множества в моделях управления и искусственного интеллекта / А.Н. Аверкин, И.З. Батыршин, А. Ф. Блишун [и др.]; Под ред. Д.А. Поспелова. - М.: Наука, 1986. - 311 с.
8. Kranenburg C. Fluid Mech. / C. Kranenburg. – 1984. – № 145. – P. 253-273.
9. Takagi T. Fuzzy identification of systems and its application to modeling and control / T. Takagi, M. Sugeno // IEEE Trans. Systems, Man, and Cybernetics. − 1985. − Vol. 15. − P. 116-132.
10. Арнольд В. И. Теория катастроф / В.И. Арнольд. – М.: Физматлит, 1990. – 128 с.
11. Зайченко Ю. П. Исследование эффективности нечеткой нейронной сети ANFIS в задачах макроэкономического прогнозирования / Ю. П. Зайченко, Ф. Севаее // Системні дослідження та інформаційні технології. − 2005. − № 1. − С. 100–112.
12. Землянский О.Н. Прогнозирование и мониторинг предаварийного развития процессов / О.Н. Землянский / Матеріали III міжн. наук.-практ. конф. «Системний аналіз. Інформатика. Управління» САІУ-2012. – Запоріжжя: КПУ, 2012. – С. 119-120.
13. Назаров А.В. Нейросетевые алгоритмы прогнозирования и оптимизации систем / А. В. Назаров, А. И. Лоскутов. – СПб.: Наука и Техника. – 2003. – 384 с.

Информация об авторах

Землянский Олег Николаевич — к. т. н., доцент кафедры автоматических систем безопасности и электроустановок, Черкасский институт пожарной безопасности имени Героев Чернобыля НУГЗ Украины, ул. Оноприенко, 8, м. Черкассы.

Мирошник Олег Николаевич — к. т. н., доцент, доцент кафедры пожарной тактики и аварийно-спасательных работ, Черкасский институт пожарной безопасности имени Героев Чернобыля НУГЗ Украины, ул. Оноприенко, 8, м. Черкассы.

Черненко Александр Николаевич — к. м. н., доцент, доцент кафедры организации мероприятий гражданской защиты, Черкасский институт пожарной безопасности имени Героев Чернобыля НУГЗ Украины, ул. Оноприенко, 8, м. Черкассы.

Куценко Станислав Васильевич — к. т. н., доцент, начальник кафедры автоматических систем безопасности и электроустановок, Черкасский институт пожарной безопасности имени Героев Чернобыля НУГЗ Украины, ул. Оноприенко, 8, м. Черкассы.

КОМП'ЮТЕРНІ СИСТЕМИ ТА КОМПОНЕНТИ

УДК 004.056 : 004.424.47

Ю. В. Баришев, В. М. Запасна

МЕТОД ТА ІНТЕРФЕЙСИ ДЛЯ ПЕРЕДАВАННЯ ДАНИХ В ЛІНІЯХ З ВИСОКИМ РІВНЕМ ЗАВАД

Вінницький національний технічний університет, м. Вінниця

Анотація. Розглянуто сучасні інтерфейси передавання даних. Наведено новий метод передавання даних в лініях з високим рівнем завад, який дозволяє забезпечити цілісність цих даних. Даний метод реалізовано у вигляді синхронного та асинхронного інтерфейсів. Для самосинхронізації передавання в асинхронному режимі передбачено використання групового кодування, яке реалізується відповідним структурним блоком мікропроцесорної системи. Контроль автентичності даних, отриманих протягом сеансу зв'язку, здійснюється за рахунок гешування, яке реалізується в інтерфейсах окремим блоком. Наведено результати компонентного тестування інтерфейсів, отриманих внаслідок комп'ютерного моделювання з використанням мови опису апаратури VHDL.

Ключові слова: мікропроцесор, завади, передавання даних, синхронний інтерфейс, асинхронний інтерфейс.

Аннотация. Рассмотрены современные интерфейсы передачи данных. Приведен новый метод передачи данных в линиях с высоким уровнем помех, который позволяет обеспечить целостность этих данных. Данный метод реализован в виде синхронного и асинхронного интерфейсов. Для самосинхронизации передачи в асинхронном режиме предусмотрено использование группового кодирования, которое реализуется соответствующим структурным блоком микропроцессорной системы. Контроль аутентичности данных, полученных во время сеанса связи, совершается за счет хеширования, реализованного в интерфейсах отдельным блоком. Приведены результаты компонентного тестирования интерфейсов, полученные вследствие компьютерного моделирования с использованием языка описания аппаратуры VHDL.

Ключевые слова: микропроцессор, помехи, передача данных, синхронный интерфейс, асинхронный интерфейс.

Abstract. The modern interfaces for data transfer are considered. New method for data transmission via lines with high interference level is proposed which allows to ensure the integrity of the data. This method is implemented as synchronous and asynchronous interfaces. Group encoding is implemented as appropriate structural microprocessor unit for self-synchronization providing for the asynchronous transfer mode. The control of data received at the transfer session authenticity is performed by hashing, which is implemented by the special interface block. Results of interfaces components testing are presented, which are gotten by computer modeling using hardware description language VHDL.

Keywords: microprocessor, interferences, data transfering, synchronous interface, asynchronous interface.

Вступ

Широке поширення електронних пристроїв разом з пришвидшенням роботи обробки даних привнесло низку нових задач. Однією з таких задач є забезпечення цілісності даних при передаванні даних. Це пов'язано з тим, що на багатьох підприємствах та організаціях лінії передавання даних проходять через приміщення з великою кількістю електричних кабелів, які створюють електромагнітні завади. Ці завади впливають на цілісність даних, що передаються такими лініями. Тому постає необхідність для розробки мікропроцесорної системи передавання даних, що допоможе зберегти цілісність даних, які передаються лініями з високим рівнем завад. Особливо проблема завад постає у силовій електроніці, адже вплив завад може порушити роботу всієї системи, а водночас силові пристрої, будучи джерелом завад, самі ж від них і страждають.

Актуальність

Передавання даних критичне для переважної більшості сучасних інформаційних систем, які передбачають розподілення обчислень між різними вузлами цих систем. При цьому такі обчислення можуть бути як безпосередньо задані користувачем, так і "допоміжними" (системними) – такими, що забезпечують виконання процесів, які вже розв'язують задачі задані користувачем. Така організація обробки даних дозволяє збільшити продуктивність системи за рахунок розпаралелення обчислень та/або використання обчислювальних вузлів, що мають спеціалізовані блоки, розроблені для розв'язання певних задач. Водночас це потребує забезпечення постійного обміну даними між різними вузлами.

Особливої значущості це набуває для інформаційних систем критичних інфраструктур, де висуваються підвищенні вимоги щодо забезпечення цілісності та автентичності інформації. Методи передавання даних, які використовуються в сучасних інтерфейсах мікроконтролерів, в більшості випадків можуть забезпечити відповідність цим вимогам, однак їх використання стає проблематичних за умов впливу завад на лінії зв'язку, що зокрема актуально для електроенергетичних систем, які відносяться до критичних інфраструктур. Використання додаткового кодування, що реалізується програмними засобами, які розв'язують ці задачі на мережевому, транспортному, сеансовому або, навіть, прикладному рівнях породжує необхідність у передаванні додаткових технічних даних для кожного з протоколів, що зменшує інформаційну швидкість обміну даними. З цього випливає актуальність розв'язку задачі забезпечення цілісності та автентичності даних при їх передаванні лініями зв'язку, в яких внаслідок завад підвищена

ймовірність виникнення помилок в кадрі порівняно зі стандартними вимогами QoS для інтерфейсів, саме на рівні апаратних засобів передавання.

Мета

Метою даного дослідження є покращення захищеності при передаванні інформації шляхом розробки мікропроцесорної системи передавання даних.

Задачі

Для досягнення мети необхідно розв'язати такі задачі:

1. Проаналізувати сучасні методи передавання даних, що використовуються в мікропроцесорних системах.
2. Розробити метод передавання даних, що підвищуватиме захист цілісності та автентичності даних, що передаються.
3. Розробити інтерфейси, що реалізують запропонований метод.

Аналіз відомих методів передавання даних, що використовуються в мікропроцесорних інтерфейсах

Одним з найпоширеніших методів асинхронного передавання в мікропроцесорних системах є метод, використаний в універсальному асинхронному приймачі-передавачі – інтерфейсі UART. Цей метод забезпечує напівдуплексний зв'язок і передбачає передавання даних по 8 біт в кадрах розміром в 10 або 11 бітів. Для забезпечення синхронізації даний метод передбачає обрамлення інформаційних даних стартовим та стоповим бітами, які сигналізують про ініціацію та коректне завершення передавання кадру відповідно [1]. Крім того більшість реалізацій UART передбачають автоматичний контроль цілісності даних методом контролю бітової парності. Коли ця функція ввімкнена, після останнього біту дописується біт, що містить інформацію про парність кількості одиничних біт в даному кадрі [1]. Цей метод забезпечує виявлення однократної помилки і може, за певних умов, дозволити виявити помилки більшої кратності, але даний метод не надає можливості виправити виявлену помилку. Це робить необхідним організацію запиту на повторне передавання даних, що відповідно до розміру кадру має бути 10 або 11 біт, яке за умови високого рівня завад може також спотворитись і потребуватиме, в свою чергу, формування на іншій сторони запиту на повторне передавання запиту на повторне передавання і так далі. Відповідно за умов високого рівня завад такий метод зіб'ється на постійне передавання запитів на повторне передавання даних замість надсилання власне даних, які потребують цього передавання (зручно уявити цю ситуацію при ймовірності некоректного прийому біта даних 0,1), що неприйнятно для передавання даних в межах критичних інфраструктур. Вищевикладена критика справедлива й для методів передавання, які будуються на даному, зокрема, метод, використаний в інтерфейсі Octal UART [2].

В методах передавання, які використовуються в інтерфейсах SPI та SSI забезпечується дуплексний зв'язок та синхронізація пристроїв, однак не передбачається підтвердження прийому даних з боку пристроїв, які працюють в режимі slave, тому дані можуть передаватись безадресно [3, 4]. Також дані методи не передбачають процедури виявлення помилок, а тому порівняно з інтерфейсом UART забезпечують менший рівень стійкості до завад.

Метод передавання даних, що використовується інтерфейсом I^2C, передбачає підтвердження приймання даних. Останнє, в свою чергу, надає можливість організації повторного передавання даних, які не були прийняті адресатом. Крім того, цей метод передбачає одночасну взаємодію декількох пристроїв в режимі master та протокол арбітражу, який попереджає виникнення колізій в шині при одночасному початку передавання даних декількома пристроями [5]. Проте такий метод передавання не дозволяє ні виявляти та виправляти помилки в кадрах, ні автентифікувати дані. Відповідно при виникненні помилки в кадрі, вона не буде виявленою, що не дозволяє адресату, приймаючи дані, визначити їх коректність.

Інтерфейс USB передбачає використання циклічних кодів для виявлення помилок і, у випадку виникнення такої події, повторного пересилання даних [6]. Причому залежно від виду трафіка може використовуватися CRC кодування різного типу. Крім того для поліпшення характеристик самосинхронізації цей інтерфейс використовує групове кодування 128b/132b. однак відсутність можливості виправлення помилки в кадрі при високому рівні завад може спричинити те, що для коректного передавання даних може знадобитися неоднократне повторення процедури передавання даних. Відповідно це негативно вплине на загальну інформаційну швидкість цього інтерфейсу.

Ще одним методом, який забезпечує передавання даних в мікропроцесорній техніці, є метод, що використовується в інтерфейсі CAN. Для досягнення безпеки CAN використовує поточний контроль (передатчики порівнюють рівні бітів, що були передані, з рівнями на шині), побітове заповнення та перевірку кадру повідомлення. Вузли CAN можуть відрізняти тимчасові помилки від постійних відмов [7]. Однак при виявленні помилок не передбачено жодного механізму її виправлення.

Таким чином, методи передавання даних, які використовуються в сучасних інтерфейсах не передбачають методів, які забезпечують виявлення та виправлення помилок, а як наслідок їх апаратну підтримку. Саме це робить необхідним "огортання" даних методів передавання іншими методами на вищих

рівнях моделі відкритих систем OSI, що породжує або збільшення технічної інформації, а також відсутність використання протоколами вищих рівнів всіх можливостей інтерфейсів щодо завадостійкості, або – необхідність у повторному передаванні даних, що, як показав аналіз, не може вважатись адекватним розв'язанням задачі передавання даних в лініях з високим рівнем завад.

Метод передавання даних

Для інтеграції інтерфейсів, що пропонуються в даному дослідженні, до існуючих систем передавання пропонується залишати існуючі способи адресації пристроїв. Для цього інтерфейси будуть імітувати для пристроїв роботу їх адресатів. Наприклад, якщо розглядати систему обміну інформацією між двома пристроями (Пристрій 1 та Пристрій 2), що здійснюють обмін за допомогою інтерфейсу SPI [3] (рис. 1).

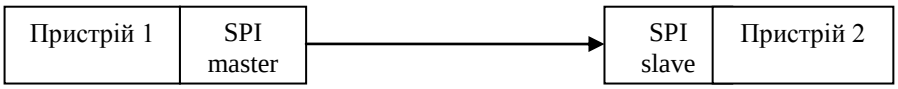


Рисунок 1 – Приклад системи обміну інформацією

Інтеграцію до даної системи пропонується здійснювати так, як це наведено на рис. 2.

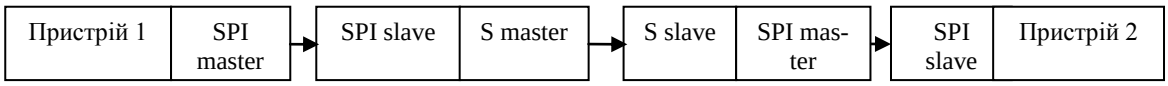


Рисунок 2 – Приклад використання інтерфейсу в лініях з високим рівнем завад

Як видно з рис. 1, при вбудовуванні пристроїв, що пропонуються, для програмного забезпечення Пристрою 1 та Пристрою 2 не доведуться вносити ніяких змін, оскільки як до інтеграції Пристрій 1 здійснював обмін з пристроєм, що має інтерфейс SPI slave, так і після неї він здійснює обмін з таким пристроєм. Аналогічним чином використання додаткових інтерфейсів не спричинятиме необхідність зміни програмного забезпечення Пристрою 2. На рис. 3 та 4 наведено алгоритми передавання та приймання даних відповідно, що формалізують запропонований метод передавання, у випадку асинхронного режиму передавання.

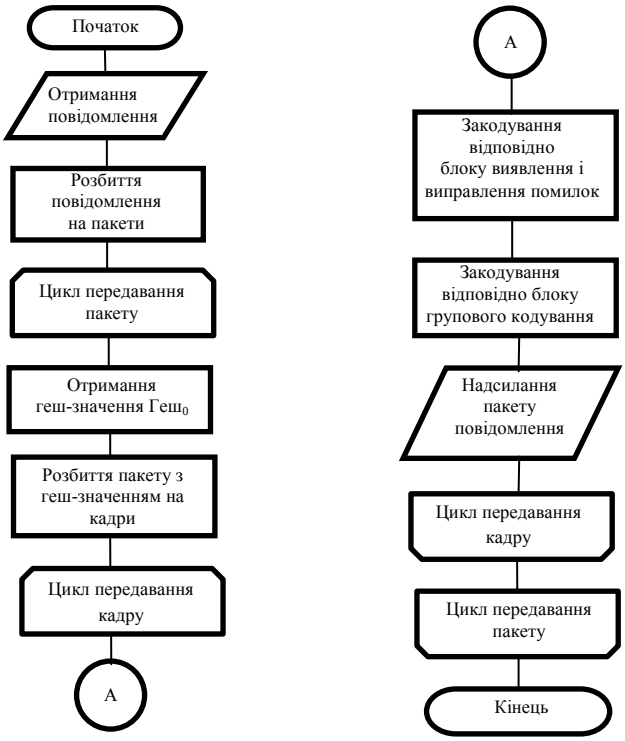


Рисунок 3 – Алгоритм передавання даних в асинхронному режимі в лініях з високим рівнем завад

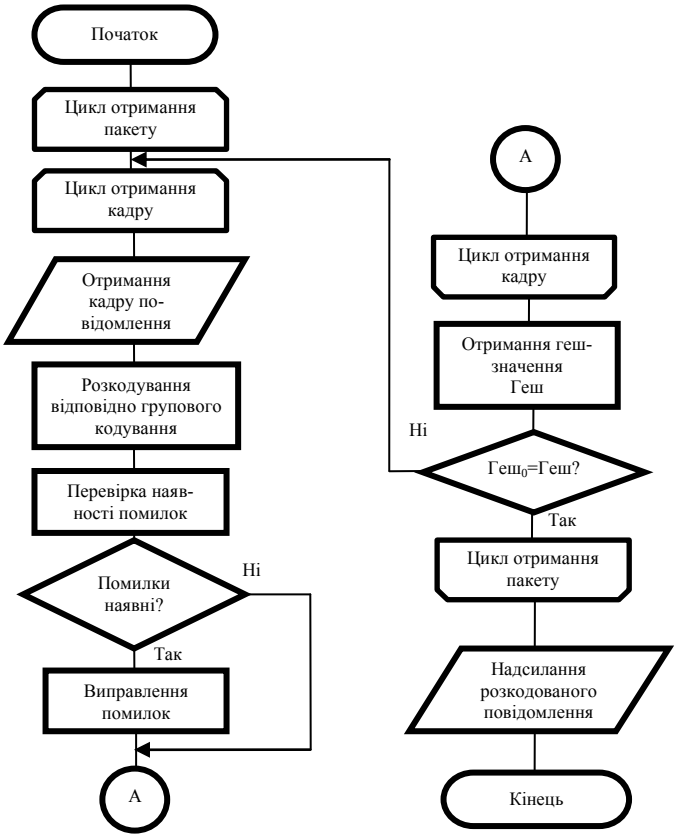


Рисунок 4 – Алгоритм отримування даних в асинхронному режимі в лініях з високим рівнем завад

У випадку синхронного режиму передавання алгоритми, що формалізують метод, мають аналогічний вигляд, однак у цьому випадку не виконується процедура закодування/розкодування відповідно до групового коду, який покликаний покращити показники самосинхронізації, а тому в синхронному режимі передавання його використання недоцільне.

Як видно з рис. 3 та 4 даний метод передбачає розбиття повідомлення на пакети для кожного з яких обчислюється геш-значення для забезпечення захисту автентичності та цілісності повідомлень. Апаратна реалізація гешування підвищеної швидкості для аналогічних задач розглядалася зокрема в роботах [8, 9]. Пакет із дописаним до нього геш-значенням відповідно до запропонованого методу, розбивається на кадри. В межах кадрів використовується кодування, що забезпечує виявлення та виправлення помилок, а також, у випадку асинхронного передавання, групове кодування [10, 11].

В табл. 1 наведено теоретичні оцінки ймовірності виявлення та виправлення помилок в кадрах при використанні запропонованого методу за умови різного рівня завад.

Таблиця 1 – Теоретичні оцінки ймовірності виявлення та виправлення помилок в кадрах при використанні запропонованого методу

Ймовірність помилки отримання 1 біта	Ймовірність наявності помилки в кадрі	Ймовірність однократної помилки в кадрі	Ймовірність багатократної помилки в кадрі	Частка коректно прийнятих кадрів
Синхронний режим передавання				
0,01	0,113615	0,1074	0,006215	0,945298
0,03	0,306158	0,2575	0,048658	0,841069
0,06	0,52408	0,3645	0,15958	0,695505
0,09	0,677525	0,3827	0,294825	0,56485
0,15	0,857758	0,3012	0,556558	0,351148
0,21	0,90758	0,2434	0,66418	0,268186

Продовження табл. 1

Ймовірність помилки отримання 1 біта	Ймовірність наявності помилки в кадрі	Ймовірність однократної помилки в кадрі	Ймовірність багатократної помилки в кадрі	Частка коректно прийнятих кадрів
Асинхронний режим передавання				
0,01	0,139942	0,129	0,010942	0,92181
0,03	0,366749	0,2575	0,109249	0,702115
0,06	0,604708	0,3645	0,240208	0,60277
0,09	0,756992	0,3827	0,374292	0,505554
0,15	0,912646	0,3012	0,611446	0,330029
0,21	0,970866	0,1885	0,782366	0,194157

Як видно з табл. 1, при ймовірності помилки в біті 0,01, ймовірність отримання кадру, що мітить помилку становитиме близько 0,1 і з цих 10% кадрів понад 92% будуть виправлені. При ймовірності помилки 0,1 запропонований метод, на відміну від розглянутих вище, дозволятиме коректно приймати половину зі спотворених завадами кадрів. При отриманні оцінок, наведених в табл. 1, враховувалась можливість коду виправляти лише однократні помилки в межах кадру. Очевидно, що при використанні параметрі кодів, які дозволяють виправляти помилки більшої кратності, оцінки даного методу покращаться.

Інтерфейси передавання даних лініями з високим рівнем завад

Для реалізації запропонованого методу було реалізовано інтерфейси для синхронного та асинхронного режимів передавання даних. На рис. 5 наведено структуру мікропроцесорного пристрою для передавання даних в лініях з високим рівнем завад.

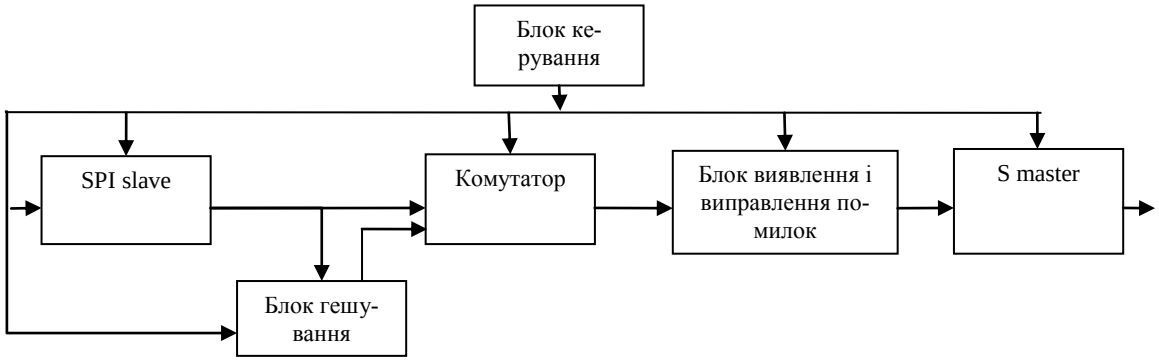


Рисунок 5 – Пристрій передавання з синхронним інтерфейсом S Master

Дані, що надсилаються з SPI slave, передаються на комутатор та паралельно проходять через блок гешування. Геш-значення передається останнім пакетом [9]. Після комутатора данні потрапляють на блок виявлення та виправлення помилок, де доповнюються даними, які дозволять у випадку виникнення помилок їх виправити після приймання на іншій стороні зашумленої лінії. Після чого дані потрапляють на синхронний інтерфейс S master, який призначений для синхронного передавання розширених в даному пристрої пакетів даних .

Аналогічним чином запропоновані ідеї можуть бути використані для асинхронного методу передавання. Однак в цьому випадку після блоку виявлення та виправлення помилок з метою забезпечення самосинхронізації даних пропонується використовувати блок групового кодування.

Для практичної реалізації запропонованого методу було розроблено синхронний та асинхронний інтерфейси, які використовували код Хемінга для виявлення та виправлення помилок, код ГК 4/5. На рис.6 наведено структуру асинхронного інтерфейсу.

З рис. видно, що інтерфейс має 17-розрядний регістр зсуву. Така кількість розрядів обумовлена тим, що відповідно до методу кодування за Хемінгом [10, 11] для 8 інформаційних біт необхідно обчислити 4 перевірочних біти. Отримана внаслідок такого кодування група з 12 бітів розбивається на 3 частини по 4 біти кожна. І, внаслідок кодування груповим кодом ГК 4/5, кожна група розширюється до кодового слова довжиною 5 біт. Таким чином, 12 бітів, які надходять на блок групового кодування перетворюються у 15 біт. Для організації асинхронного способу передавання попереду цих 15 біт додається біт "старт", а наприкінці біт "стоп". Таким чином, до іншого пристрою буде надсилатись 17 біт, що обумовлює розрядність регістру зсуву в інтерфейсі AS.

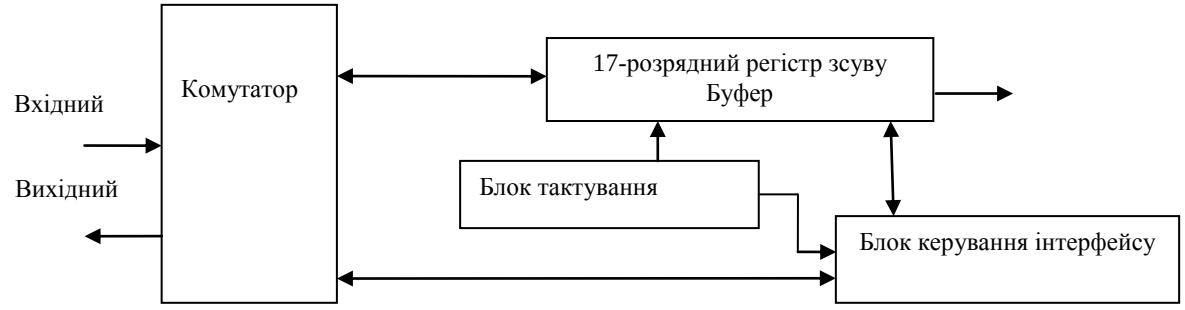


Рисунок 6 – Схема асинхронного інтерфейсу AS

Роботу даного інтерфейсу було досліджено за допомогою комп’ютерного моделювання у середовищі ModelSim Starter Edition. Для його реалізації були описані архітектури:

- GK_encoding_arc, яка передбачає наявність одного процесу, який виконуватиметься при зміні сигналу start (для реалізації сутності GK_encoding).
- GK_decoding_arc, яка передбачає наявність одного процесу, який виконуватиметься при зміні сигналу start (для реалізації сутності GK_decoding).
- Hamming_encoding_arc, яка передбачає наявність одного процесу, який виконуватиметься при зміні сигналу start (для реалізації сутності Hamming_encoding).
- Hamming_decoding_arc, яка передбачає наявність одного процесу, який виконуватиметься при зміні сигналу start (для реалізації сутності Hamming_decoding).

Результати тестування роботи блоку розкодування ГК 4/5 наведено в табл. 2. Внаслідок тестування роботи блоку закодування ГК 4/5 отримано вихідні дані, які відповідають результатам перекодування в код ГК-4/5 наведених в таблиці 2.

Таблиця 2 – Результати тестування розкодування ГК 4/5

№	Вхідні дані	Вихідні дані
1	inputData="10101"	outputData="0010" error='0'
2	inputData="01001"	outputData= "1011" error='0'
3	inputData="10111"	outputData= "0100" error='0'
4	inputData="00001"	outputData="1111" error='1'

Під час тестування роботи блоку розкодування ГК 4/5, коли надходять дозволені комбінації, то відбувається їх розкодування та надсилання на блок керування сигнала error='0', що сигналізує про успішне завершення роботи. Коли ж надходять заборонені комбінації, то надсилається сигнал error='1' та вихідні дані рівні "1111".

Під час роботи блоку закодування за Хемінгом вхідні дані inputData закодовуються відповідно до формул коду Хемінга, що підтверджують вихідні дані outputData, отримані при тестуванні даного блоку. Результати тестування роботи блоку розкодування за Хемінгом наведено в таблиці 3.

Таблиця 3 – Результати тестування блоку розкодування за Хемінгом

№	Вхідні дані	Вихідні дані
1	inputData="000000000000"	outputData="00000000" error='0' warning='0'
2	inputData="000000001000"	outputData= "10000000" error='0' warning='1'
3	inputData="001110010011"	outputData= "00111001" error='0' warning='1'
4	inputData="010101001111"	outputData= "00000000" error='1' warning='0'

Тестування роботи розкодування за Хемінгом дало підтвердження виправленню однієї помилки та виявленню багатьох помилок.

Під час першого випадку тестування подано дані без помилок, що підтвердили відправлені на блок керування сигнали error, warning. В наступних двох випадках присутня одна помилка, тому відбулось виправлення та відправлено про це сигнал warning='1' на блок керування. В останньому тестуванні відбулась трикратна помилка, тому inputData не були розкодованими, про що повідомляє сигнал error='1'.

Висновки

Аналіз відомих методів передавання даних в мікропроцесорних системах дозволив виявити необхідність у розробці методів та апаратних засобів передавання, які б забезпечували підвищення завадостійкості за умов наявності високого рівня завад у лінії зв'язку.

Для розв'язання поставленої задачі запропоновано використовувати метод передавання даних та нові інтерфейси на його основі. Цей метод за рахунок введення надлишковості в дані дозволив підвищити рівень захищеності цілісності та забезпечити захист автентичності цих даних. Високий рівень надлишковості даних (46,7 % у кодовому слові) робить його недоцільним при використанні в системах з високими вимогами до швидкості передавання, однак в системах з високим рівнем завад і меншими вимогами щодо швидкості передавання, зокрема системи керування електроенергетичними системами, використання запропонованого методу є доцільним, оскільки він забезпечує підвищену швидкість передавання порівняно з відомими методами за рахунок зменшення необхідності у повторному пересиланні кадрів. Відповідно до отриманих теоретичних оцінок останнє виконується за умов ймовірності спотворення одного біта даних понад 3%, що обумовлюється більшою ймовірністю у необхідності повторного передавання кадру та ймовірністю виникнення помилок у такому запиті щодо повторного надсилання кадру. Запропонований метод реалізовано у вигляді синхронного та асинхронного інтерфейсів, які реалізовано мовою VHDL та проведено комп'ютерне моделювання роботи їх та їхніх складових, що дозволило підтвердити отримані теоретичні оцінки.

Список літератури

1. KeyStone Architecture : Universal Asynchronous Receiver/Transmitter (UART). User Guide / Texas Instruments. Literature Number: SPRUGP1, November 2010 [Електронний ресурс]. – Режим доступу: http://www.ti.com/lit/ug/sprugp1/sprugp1.pdf – Назва з екрану.

2. Enhanced octal universal asynchronous receiver/transmitter (Octal UART). Data Sheet / Philips Semiconductors. SCC2698B, 07 Aug. 2006 (Supersedes data of 2000 Jan 31) [Електронний ресурс]. – Режим доступу: http://cache.nxp.com/documents/data_sheet/SCC2698B.pdf?pspll=1 – Назва з екрану.

3. Новицкий А. Синхронный последовательный интерфейс SPI в микроконтроллерах «от А до Я» и его реализация на примере ADuC70xx фирмы Analog Devices / А. Новицкий // Компоненты и технологии [Електронний ресурс]. – Режим доступу: http://www.kit-e.ru/articles/interface/2009_03_53.php – Назва з екрану.

4. Novak P. SSI - Interface and protocol for industrial sensors / Petr Novak // XXVI. ASR '2001 Seminar, Instruments and Control, Ostrava, April 26 - 27, 2001 [Електронний ресурс]. – Режим доступу: http://akce.fs.vsb.cz/2001/asr2001/Proceedings/papers/50.pdf – Назва з екрану.

5. UM10204. I^2C-bus specification and user manual / NXP Semiconductors. Rev. 6 — 4 April 2014. [Електронний ресурс]. – Режим доступу: http://www.nxp.com/documents/user_manual/UM10204.pdf – Назва з екрану.

6. USB 3.1 Specification. Revision. 1.0, July 26, 2013 / [Hewlett-Packard Company and others] [Електронний ресурс]. – Режим доступу: http://www.usb.org/developers/docs// – Назва з екрану.

7. CAN Specificatioin ver. 2.0 / Robert Bosch GmbH, 1991. – 72 p. [Електронний ресурс]. – Режим доступу: http://www.bosch-semiconductors.de/media/ubk_semiconductors/pdf_1/canliteratur/can2spec.pdf – Назва з екрану.

8. Баришев Ю. В. Методи та засоби швидкого багатоканального гешування даних в комп'ютерних системах : монографія / Ю. В. Баришев, В. А. Лужецький. — Вінниця : ВНТУ, 2016. — 142 с.

9. Лужецький В. А. Апаратні засоби для реалізації багатоканального керованого хешування. / В. А. Лужецький, Ю. В. Баришев. // Системи обробки інформації.– 2011. – №3. – С. 130–133.

10. Азаров О.Д. Аналого-цифрові інтерфейси ОЕМ: навч. Посіб. Для студ. вузів/ О.Д. Азаров, В.П. Марценюк., Н.О. Біліченко. – Вінниця: УНІВЕРСУМ – Вінниця, 2006 р. – 180с.

11. Кузьмин И.В. Основы теории информации и кодирования. 2-е узд./И.В. Кузьмин, В.А. Кедрус. – К.: "Вища школа", 1986 г. – 238 с.

Відомості про авторів

Баришев Юрій Володимирович – к. т. н., доцент кафедри захисту інформації, ВНТУ.
Запасна Валентина Миколаївна – магістрант кафедри захисту інформації, ВНТУ.

УДК 004.056.55

І. М. Журавська, М. П. Мусієнко, Д. І. Румянков

БЛОКОВИЙ МЕТОД ШИФРУВАННЯ ДЛЯ РУХОМИХ ОБ'ЄКТІВ З ОБМЕЖЕНИМИ ОБЧИСЛЮВАЛЬНИМИ РЕСУРСАМИ

Чорноморський національний університет імені Петра Могили, Миколаїв

Анотація. Проаналізовані особливості створення блокових методів шифрування, які працюють за рахунок комбінування простих операцій (логічних побітових операцій та бітових зсувів) під час обчислювального процесу, що виконується на мікроконтролерах малогабаритних рухомих об'єктів. В результаті роботи було створено новий блоковий метод шифрування, який надає захист інформації не тільки при використанні на великих ЕОМ та ПК, а й при шифруванні у пристроях на мікроконтролерах. Запропонований метод дозволяє підвищити ефективність шифрування інформації при застосуванні обмежених обчислювальних ресурсів та може використовуватися для захисту трафіка безпілотних літальних апаратів (БПЛА).

Ключові слова: симетричні блокові методи шифрування, захист трафіку БПЛА.

Аннотация. Проанализированы особенности создания блочных методов шифрования, работающих за счет комбинирования простых операций (логических побитовых операций и битовых сдвигов) при вычислительном процессе, выполняемом на микроконтроллерах малогабаритных подвижных объектов. В результате работы был создан новый блочный метод шифрования, который предоставляет защиту информации не только при использовании на больших ЭВМ и ПК, но и при шифровании в устройствах на микроконтроллерах. Предложенный метод позволяет повысить эффективность шифрования информации при применении ограниченных вычислительных ресурсов и может использоваться для защиты трафика беспилотных летательных аппаратов (БПЛА).

Ключевые слова: симметричные блочные методы шифрования, защита трафика БПЛА.

Abstract. The article provides the features of the block encryption methods' creation based on combining simple operations (bitwise logical operations and bit shifts) when computing process runs on microcontrollers of small moving objects. As a result, the new block encryption method was created that provides protection of information not only for use on mainframe computers and PCs, but also for encryption in devices based on microcontrollers. The proposed method can improve the efficiency of data encryption when using the limited computing resources. This method can be used to protect the traffic of unmanned aerial vehicles (UAVs).

Key words: symmetric block encryption methods, UAV traffic protection.

Вступ

Всі сучасні криптосистеми спираються на принцип Керкгоффса, відповідно якому секретність закодованих даних визначаються секретністю лише ключа кодування інформації користувача [1]. Тобто, усі алгоритми шифрування даних загальновідомі.

Найвідомішими блоковими методами шифрування є запроваджені у США стандарти шифрування DES та AES [2]. Але кожний з них має свої переваги та недоліки. Загальними недоліками для будь-якого методу є його зависока вибагливість до кількості та ємності обчислювальних ресурсів чи слабка криптостійкість до зламу.

Останнім часом стало популярним використання блокових методів шифрування для захисту трафіка рухомих об'єктів – безпілотних літальних апаратів (БПЛА) [3].

В такому разі використання методів шифрування не обмежується тільки їх застосуванням на комп'ютерах чи супер-комп'ютерах, але й потребує модифікації для роботи на мікроконтролерах. Але застосування методів шифрування в комп'ютерних системах на мікроконтролерах створює обмеження в використаних обчислювальних ресурсах, що змушує робити метод «легшим», – тобто таким, котрий буде використовувати якомога менше обчислювальних ресурсів.

Таким чином, постає проблемне питання щодо використання методу шифрування в сучасних об'єктах на мікроконтролерах, що мають ресурси оперативної пам'яті до 1 Мбайт [4].

Метою роботи є розробка блокового методу шифрування зі зниженими вимогами до обчислювальних ресурсів за рахунок використанням простих логічних операцій.

Результати дослідження

Хід Розглядаючи всі сучасні системи та програмне забезпечення (ПЗ), які використовують схожі методи шифрування даних, прототипом дослідження стала загальновідома програма Skype, яка використовує метод AES з довжиною ключа всередині метода 256 біт. Так як всі методи генерації ключів та реалізація раундів є неопублікованою інформацією, можна припустити, що для забезпечення захисту інформації користувачів виконана модифікація блокового методу, яка знаходиться на віддаленому сервері.

Розглядаючи усі доступні дані, за основу необхідно взяти простий алгоритм, який задовільнить вимогам стійкості криптосистеми та швидкого виконання кодування та декодування даних.

Під час дослідження роботи кожного з блокових методів шифрування DES та AES було виділено основні операції, які застосовуються: додавання, перемішування, здвиг бітів та бінарна операція XOR [5].

Справді, одним з легких та найпростіших відносно обчислювальних ресурсів є алгоритм з використанням операції XOR. Виходячи з цього, була прийнята спроба розробити блоковий метод, в основу якого буде покладена дана операція, але перед цим необхідно оцінити його криптостійкість щодо спроби злому та отримання інформації.

Розглядаючи концепцію використання операції XOR в існуючих методах потокового шифрування, наприклад, в комплексі ВРС-алгоритма для шифрування відеосигналів, які передаються поточно з літального пристрою, можна зауважити, що така задача є не цілком пріоритетною [6]. Таке суперечення обумовлено тим, що головною метою шифрування даних є підвищити прихованість наступних дій БПЛА в умовах зорового контакту з противником.

Так як кодування передаваної відеоінформації з рухомого пристрою вимагає немалих ресурсів, то, відповідно, вбудовувати в керуючий модуль алгоритм шифрування відеоданих не є цілком позитивним напрямом. Це обумовлене тим, що така складна архітектура модуля потребує великих обчислювальних ресурсів, й одна система повинна виконувати багато задач в одиницю часу – й саме шифрування даних, й передачу даних, й геопозиціонування рухомого об’єкту, й аналіз перешкод руху або відпрацювання команд кібер-оператора тощо. Описане рішення за сумою факторів обумовлює критичне застосування такої кіберфізичної системи, та може привести до втрати самого літального апарату [7].

Для забезпечення більш стабільної роботи комплексу системи керування необхідно розробляти окремо модуль кодування даних й налаштовувати з’єднання з керуючим модулем, що відповідно збільшує вагу БПЛА й вимагає конструктивних вдосконалень та в результаті веде до збільшення розміру апарату й підвищує вірогідність його виявлення тактичним противником [3].

Взагалі ідея шифрування відеопотоку не є гарною, так як командний пункт повинен якомога швидше отримати розвідувальні дані й надалі скерувати літальний апарат в потрібний квадрат ландшафту й гарантувати його бойову здатність до розвідувальних цілей.

Підвищити час виявлення маршруту БПЛА можливо за рахунок кодування його наступних координат геопозиціонування, які вказують наступну точку положення в просторі [3]. Тому дана мета є першопочатковою для забезпечення успіху в моніторингових операціях.

Навіть якщо прийняте рішення щодо кодування відеопотоку, наприклад, за допомогою ВРС-алгоритма, то для кодування геопозиційних координат такий або подібний метод не є доцільним за його “прожерливість” до обчислювальних ресурсів та архітектурну складність. А саме конкатенація даних з номером сеансу для розпізнавання «Свій-Чужий» є небезпечною, й таким чином, умовний противник, підібравши номер сеансу зв’язку, може заволодіти конфіденційними даними користувачів чи організації.

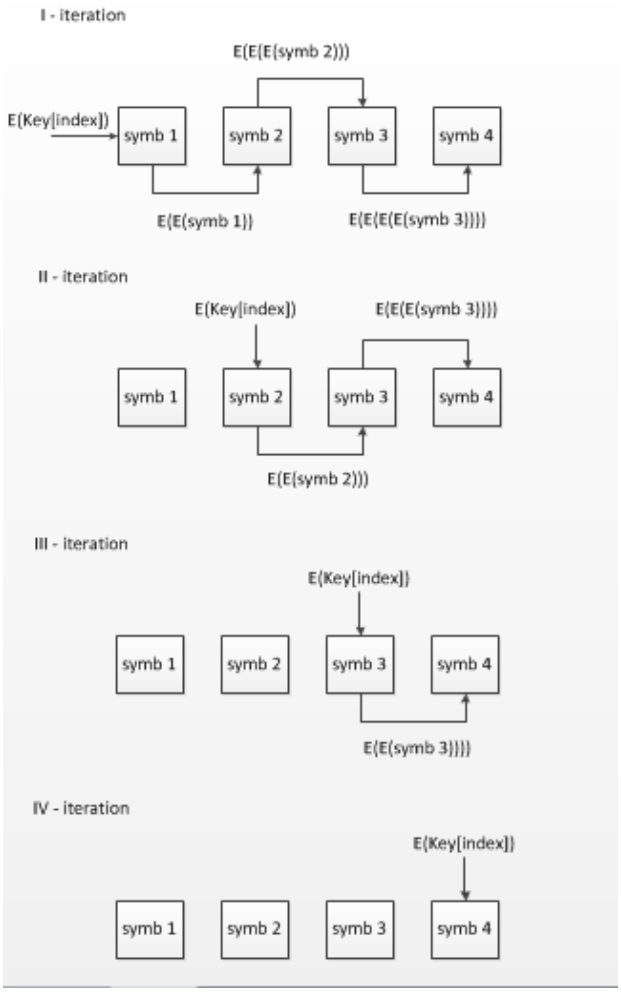


Рисунок 1 – Раунди блокового шифрування інформації

Маючи необхідний інструмент для виконання шифрування даних, доцільно розпочати роботу та дослідження кодування інформації простою операцією XOR [5]. Таким чином, маючи одну бінарну операцію в алгоритмі, можна сказати, що вже є реалізація симетричного алгоритму кодування, який кодує інформацію за принципом використання операції XOR між значенням ключа й відповідним бітом; натомість отримуємо нове значення в поточній позиції множини даних (послідовність бітів).

Але, виконуючи таку схему шифрування, бажаної безпеки не отримаємо. Такий алгоритм шифрування легко зламується навіть без комп’ютера.

Тому, окрім бінарної операції, необхідно використовувати комбінацію інших можливих операцій. Необхідно створити схему послідовності етапу шифрування (так званий «раунд» в криптографії), за якої б можна отримати унікальне значення кожного біту задля того, щоб вирішити проблему зламу XOR-шифрування, тобто визначити індекс збігу.

Але зробити в початковому наборі кожний біт унікальним неможливо, так як їх значення знаходиться у виборці, яка обмежена значенням 255. Тому для вирішення питання унікальності необхідно скористатися розбиттям інформації на блоки по 32/64/128/256 бітів. Таким чином можна досягнути унікальності набору в блоці.

Але цього недостатньо, так як сама інформація хоч й кодується, але можливість дістати її першопочатковий образ залишається можливим. Для забезпечення криптостійкості необхідно застосувати перемішування цих блоків між собою у певному порядку [8]. Причому, порядок перемішування генерується ґеш-функцією, яка може розбити блоки на 10/12/14 в залежності від довжини ключа [9]. Таким чином досягається унікальність набору, чим й підвищується криптостійкість системи.

Після етапу перемішування блоків необхідно використати повторне розбиття блоку на більш малі частини, які б займали по 32 біти, але перед цим необхідно виконати перевірку на умову повноти. Сутність повноти блоку полягає в тому, що вхідна інформація повинна ділитися націло на 32 біти; якщо ж цього не виконується, то вона доповнюється дописуванням спеціального символу.

Таким чином, розбивши вже закодовану інформацію на менші блоки, можна перейти до основного кодування інформації – це кодування наступного блоку попереднім блоком, щоб зав'язати відповідну послідовність розташування малих блоків (рис. 1).

Дослідження створеного методу показало, що його застосування не потребує великих ресурсних витрат на генерацію раундових ключів. Це надає змогу виконувати операції кодування та декодування інформації в короткі проміжки часу, що й забезпечує високу криптостійкість даної системи. Так, наприклад, використання такого «легкого» методу шифрування в мікроконтролерах малих БПЛА надає змогу розробити рухомий об'єкт невеликого розміру, що, в свою чергу. суттєво збільшує час виявлення БПЛА в умовах розвідувальних дій. Крім того, що малі розміри такого об'єкту роблять можливим здешевити виготовлення, вони ще й збільшують шанс, що літальний апарат вийде неушкодженим з території протипротивника [3].

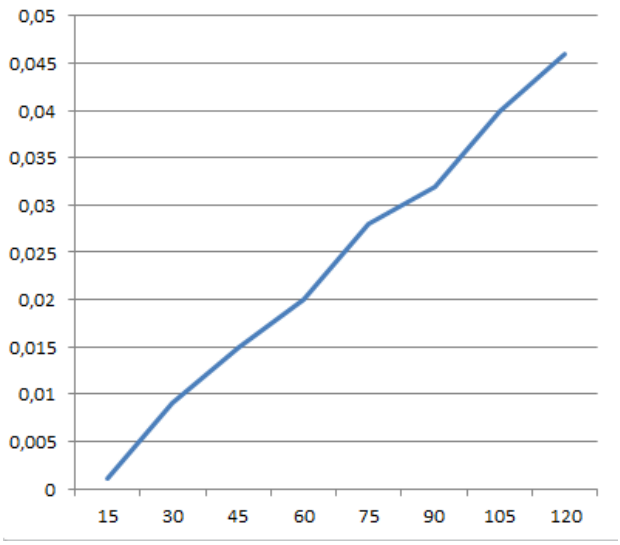


Рисунок 2 – Залежність часу шифрування (*c*) від обсягу інформації (байт)

Головна ідея методу полягає в тому, що інформація кодує сама себе, але за участю ключа користувача, який корегує схему кодування. Даний метод шифрування відповідає вимогам сучасності й надає повну свободу вибору ключа користувачем. Такий ключ може складатися з будь-яких символів з таблиці ASCII (окрім NULL).

На графіку рис. 2 зображено залежність кодування та декодування даних, що визначається за величинами часу та ємністю інформації (у байтах). Як видно з рис. 2, застосування даного методу кодування даних в літальних пристроях забезпечить швидку детермінацію напряму, який надсилає командний пункт (сервер).

Так як в запропонованому методі використовуються прості логічні операції, то кожна операція виконується в середньому 5 мкс. Тому нескладно обчислити теоретичний час P кодування даних:

$$P = P_{сер} \cdot m \cdot (k1 + k2 + k3), \qquad (1.1)$$

де P – загальний теоретичний час; $P_{сер}$ – опосередкований час виконання кожної операції; m – вага (обсяг) вхідної інформації; $k1$ – кількість операцій зсуву; $k2$ – кількість операцій логічного виключення; $k3$ – кількість пов'язаних блоків.

Треба зауважити, що в (1.1) величини k1, k2, k3 динамічно змінюються в залежності від довжини ключа та інформації, що шифрується.

З аналізу рис. 2 можна дійти висновку, що достатній обсяг поодиноких даних для передачі з БПЛА (показання датчиків окремих величин, координати знайдених об'єктів тощо) може бути зашифрованим

за дуже невеликий час, який не перевищує значення, співвідносні з часом в 1 с, необхідним сучасному обладнанню для зламу систем БПЛА з відомими характеристиками [10]. Це дозволить комп'ютерній системі рухомого об'єкта встигнути до зламу не тільки зашифрувати, а й передати та потім знищити з власних носіїв дані, отримані з датчиків та/або відеокамер.

Висновки

1. Під час виконання дослідження було проаналізовано блокові алгоритми кодування інформації й віднайдені основні риси, які характерні для кожного з них. Було сформовано фундаментальні правила для методу, який би забезпечив належний рівень захисту конфіденційної інформації, що передається в умовах неможливості забезпечення охорони периметру рухомої мережі (кібер-фізичної системи).

2. Були проаналізовані методи, які створюються шляхом комбінування операцій, простих для обчислювального процесу як ЕОМ, так і мікроконтролерних пристроїв. До таких операцій можна віднести операції зсуву, додавання, перемішування, логічного виключення.

Встановлено, що запропонований підхід дозволяє підвищити криптостійкість шифрованої інформації при зменшеному часі шифрування, у т. ч. на процесорах з низькою обчислювальною потужністю, які використовуються в БПЛА.

3. В результаті роботи було створено метод, який надає захист інформації шляхом шифрування не тільки на великих ЕОМ та ПК, а й може бути ефективно використаний в комп'ютерних системах на мікроконтролерах. Застосування методу шифрування в сфері використання БПЛА, які базуються на побудові архітектури керуючого пристрою на мікроконтролерах, надає відповідних результатів, головний з яких, – це перевага над тактичним ворогом у «неочікуваному маневруванні». Крім того, вірогідність, що БПЛА уціліє, збільшується на 30% за рахунок кодування команд щодо наступного місця знаходження літального пристрою.

4. Отримане співвідношення часу шифрування розробленим методом блоку даних для передачі іншому об'єкту мережі з часом, необхідним для зламу бортової системи БПЛА сучасним обладнанням, свідчить про достатньо високу криптостійкість та доцільність використання запропонованого методу, використання якого сприятиме подовженню життєвого циклу БПЛА.

Список літератури

1. Альбов, А. Квантовая криптография. – СПб. : ООО «Страта», 2015. – 248 с.

2. Шнайер, Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. – М. : Триумф, 2002. – 816 с. – ISBN 5-89392-055-4, 0-471-11709-9.

3. Малые беспилотные летательные аппараты: теория и практика / МакЛэйн Т. У., Биард Р. У. – М. Техносфера: Мир электроники, 2015. – 312 с. – ISBN 978-5-94836-393-6.

4. Сидоренко, Б. Микроконтроллеры Atmel SAM D – Cortex-M0+: оптимальное соотношение производительности и энергоэффективности // Электроника: наука | технология | бизнес. – 2014. – № 3 (00134). – С. 78–85.

5. Rosen, Kenneth. (2006). *Discrete Mathematics and Its Applications* (6th Ed.). McGraw-Hill Education. 1006 p. ISBN 978-0073229720.

6. Белецкий, А. Я. Программно-моделирующий комплекс ВРС алгоритма поточного шифрования и помехоустойчивого кодирования видеосигналов, передаваемых с борта БПЛА / А. Я. Белецкий, А. В. Максименко, Д. А. Навроцкий, А. Д. Свердлова, А. И. Семенюк // Захист інформації. – 2014. – Т. 16, № 3. – С. 184–191.

7. Musiyenko, M.P., Zhuravska, I.M., Burlachenko, I.S. and Denysov, O.O. (2016), "The Principles of the Cyber-Physical Components' Organization Based on the Methods of the Multi-Agent Interaction of the Moving Objects", Advances in Cyber-Physical Systems, Vol. 1 No. 1, pp. 48-57. Available from http://vlp.com.ua/files/special/10_289.pdf [Accessed 18 Sep. 2016].

8. Журавська, І. М. Підвищення ефективності шифрування керуючого трафіку БПЛА засобами модифікованого блокового методу [Текст] / І. М. Журавська, М. П. Мусієнко, Д. І. Румянков // Методи та засоби кодування, захисту й ущільнення інформації : тези доп. V-ї Міжнар. наук.-практ. конф., 19-21 квітня 2016 р., Вінниця. – Вінниця : Вид-во Вінниц. нац. техн. ун-ту», 2016. – С. 75–77.

9. Лужецький, В. А. Криптографічні примітиви для реалізації керованого хешування / В. А. Лужецький, Ю. В. Баришев // Вісник Вінницького політехнічного інституту : наук. журнал / ВНТУ. – 2011. – № 1. – С. 108–111.

10. Взлом беспилотника займет у комплекса РЭБ "Шиповник-АЭРО" секунду // Интерфакс. Новости ВПК. – 2016. – 14 сентября. – Режим доступа : URL : http://vpk.name/news/163641_vzlom_bespilotnika_zaimet_u_kompleksa_reb_shipovnikaero_sekundu.html (дата обращения 18.09.2016).

Відомості про авторів

Журавська Ірина Миколаївна – к. т. н., доцент кафедри комп'ютерної інженерії Чорноморського національного університету імені Петра Могили Миколаїв, 54003, Україна.

Мусієнко Максим Павлович – д-р техн. наук, професор, декан факультету комп'ютерних наук Чорноморського національного університету імені Петра Могили, Миколаїв, 54003, Україна.

Румянков Дмитро Ігорович – бакалаврант кафедри інтелектуальних інформаційних систем Чорноморського національного університету імені Петра Могили, Миколаїв, 54003, Україна.

УДК 004.582

Т .І. Трояновська, Л. А. Савицька, І. А. Жарий

МЕТОД ПОКРАЩЕННЯ ВІЗУАЛЬНИМ КЕРУВАННЯМ ГАЛЕРЕЯМИ ГРАФІЧНИХ ФАЙЛІВ

Вінницький національний технічний університет, м. Вінниця

Анотація. Дана робота присвячена дослідженню методів удосконалення інтерфейсу для відображення галереї зображень, яка реалізовує принцип багатопоточності, що застосовується до обраної множини графічних об'єктів. Зокрема, виконано аналіз систем керування галереями графічних файлів, запропоновано метод покращення візуальним керуванням галереями графічних файлів з можливістю організації кількох користувацьких галерей в ряд потоків з можливістю маніпулювання їх змістом та розроблено кросплатформений програмний засіб, що реалізовує запропонований метод. Розроблений програмний засіб є додатком інтерфейсу користувача (UI) з ієрархічним відображенням категорій графічних файлів різного рівня, надійно працює на портативних цифрових пристроях.

Ключові слова: галерея графічних файлів, метод відображення галереї зображень, багатопоточність, кросплатформеність.

Аннотация. Данная работа посвящена исследованию методов совершенствования интерфейса для отображения галереи изображений, реализующая принцип многопоточности, которая применяется к выбранной множества графических объектов. В частности, выполнен анализ систем управления галереями графических файлов, предложен метод улучшения визуальным управлением галереями графических файлов с возможностью организации нескольких пользовательских галерей в ряд потоков с возможностью манипулирования их содержанием и разработаны кроссплатформенных программное средство, реализующее предложенный метод. Разработанный программный средство является приложением интерфейса (UI) с иерархическим отображением категорий графических файлов различного уровня, надежно работает на портативных цифровых устройствах.

Ключевые слова: галерея графических файлов, метод отображения галереи изображений, многопоточность, кроссплатформенность.

Abstract. This work is devoted to methods for improving the interface to display the image gallery, which implements multithreading principle applied to the selected set of graphic objects. In particular, the analysis of galleries managing image files, the method of improving the visual galleries running graphic files with custom galleries of several streams in a row with the ability to manipulate their content and developed a cross-platform software tool that implements the proposed method. The developed software tool is the application user interface (UI) with hierarchical categories display image files at various levels, works reliably on portable digital devices.

Key words: gallery image files, a method of displaying image galleries, multi, cross-platform.

Вступ

Розвиток інформаційних технологій створює необхідність швидко і ефективно організовувати потрібні для роботи файли. Якщо із текстовими файлами проблем немає – для цього існують навіть спеціальні бібліотечні програми, які мають систему індексів та повнотекстового пошуку, то зовсім інша річ – мультимедійні файли, насамперед, графічні файли.

Як правило, графічні файли іменуються без сталої схеми, а самі імена не мають семантичного навантаження. Тому необхідно використовувати додаткові методи для їх організації. Зазвичай використовують файлову систему, організуючи графічні файли в окремі папки.

Однак це доволі надлишковий метод організації, оскільки одні й ті самі файли можуть належати одночасно до кількох категорій, а у поєднанні із кількістю на певному етапі це створить хаос, і ситуацію, коли пошук потрібного графічного файлу значно ускладняється [1].

Вирішенням може стати використання різноманітних програм попереднього перегляду, які дозволяють швидко пролистувати великі обсяги графічних файлів.

Актуальність

З настанням комп'ютерного століття користувачі комп'ютерів і програмного забезпечення звикли до дружніх програмних додатків відображення файлів графічного формату. Зазвичай графічні зображення актуалізуються програмами відображення як просто файли, що містять назву категорії і перелік посилань на зображення. Такий функціонал підтримують більшість програм швидкого перегляду, але лише як додаткову, а, у більшості випадків, й другорядну функцію.

Мета

Метою статті є розробка методу покращення візуальним керуванням галереями графічних файлів з можливістю організації кількох користувацьких галерей в ряд потоків з можливістю маніпулювання їх змістом.

Задачі

1. Аналіз систем керування галереями графічних файлів та виявлення способів подання графічних об'єктів.

2. Розробка методу покращення візуальним керуванням галереями графічних файлів з можливістю організації кількох користувацьких галерей в ряд потоків з можливістю маніпулювання їх змістом.

3. Розробка та тестування програмного засобу, що реалізовує метод покращення візуальним керуванням галереями графічних файлів.

1. Аналіз систем керування галереями графічних файлів

Галерея графічних файлів – прикладна програма або пакет прикладних програм (ППП), що дозволяє її користувачеві переглядати графічні файли на екрані монітора.

Нині все більше користувачів використовують операційні системи (ОС), з яких виділяються різні версії Linux. Особливістю кросплатформеного програмного забезпечення (ПЗ) є те, що воно може працювати на різних ОС без необхідності додаткової підготовки або переробки програми.

Системою керування графічними файлами (СКГФ) вважається спеціалізована БД організована у вигляді набору графічних файлів. Ця модель нагадує картотечну організацію файлів, при якій папки зберігаються в каталогах вищого порядку, а в кожній папці міститься деяке число графічних елементів [2].

СКГФ не можна класифікувати як СКБД, тому що звичайно вони є частиною спеціалізованих ППП для перегляду графічних даних і не оперують внутрішнім змістом файлів, що відображаються. Це враховано в ППП, що працюють із графічними файлами.

Така модель БД незручна, час виконання запитів збільшується, а програміст повинен мати більше високу кваліфікацію, тому що йому потрібно продумати не тільки логічну, але й фізичну структуру зберігання графічних даних. Це приводить до того, що між додатком і файлом утворюється тісний зв'язок.

Зі збільшенням обсягів графічної інформації (конкретно - файлів) зростає складність СКГФ. Зміни у структурі СКГФ приводять до необхідності зміни кожного програмного компонента, для якого це актуально. Формування нових запитів займає стільки часу, що найчастіше втрачає усякий зміст.

СКГФ не можуть перешкодити дублюванню інформації. До того ж, не існує механізмів, що запобігають непогодженості даних.

Безпека звичайних файлів контролюється ОС. Окремий файл може бути заблокований для перегляду або модифікації з боку того або іншого користувача, але це виконується тільки на рівні ОС. У конкретний момент часу лише один додаток може здійснювати відображення графічного файлу, що знижує загальну продуктивність.

2. Розробка методу покращення візуальним керуванням галереями графічних файлів

Використання різноманітних програм попереднього перегляду (таких, як IrfanView, або ACDSee) дозволяє швидко пролистувати великі обсяги зображень. Автори пропонують змістити акцент на організацію саме галерей графічних файлів, і створити програмний засіб, який би підтримував одночасно кілька таких галерей.

Основу розробленого методу покращення візуальним керуванням галереями графічних файлів реалізовують користувацькі класи, розроблені автором.

Зокрема, клас потоку графічних файлів для програми для організації відображення потоків графічних файлів формує колекції графічних об'єктів (КГО), розподіляє їх по потокам, дає можливість керувати їх змістом (рис. 1).

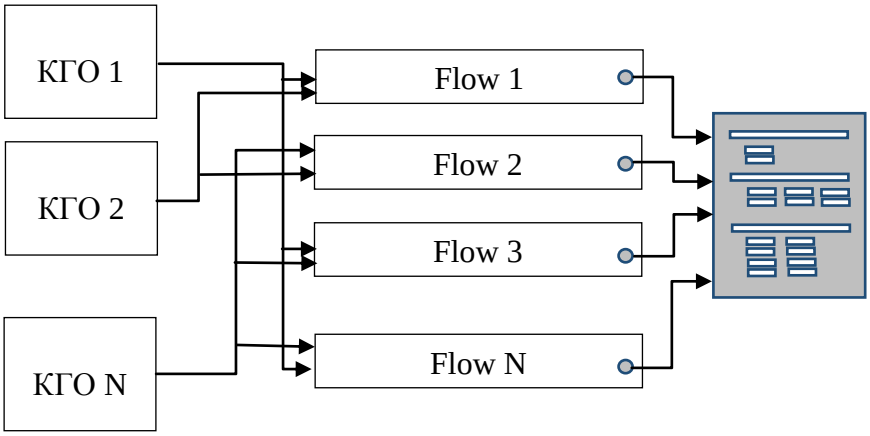


Рисунок 1 – Модель представлення графічних файлів

До складу програми, що реалізовує метод покращення візуальним керуванням галереями графічних файлів входять чотири класи – два основних і два допоміжних: ImageStreamer (головний клас програми, а також диспетчер всіх подій), GalleryStream (клас, який репрезентує потік графічних файлів), ImageStreamItem (клас, який репрезентує елемент потоку), ImageListCellRenderer (клас, який забезпечує відображення файлів картинок).

Діаграма відношень між складовими методу покращення візуальним керуванням галереями графічних файлів та використаними стандартними компонентами показана на рисунку 2. Алгоритм роботи програми наведено на рис. 3.

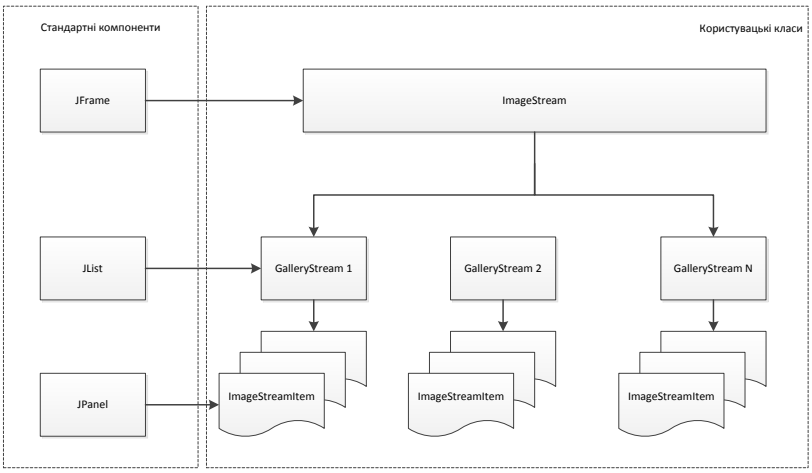


Рисунок 2а – Складові методу покращення візуальним керуванням галереями графічних файлів

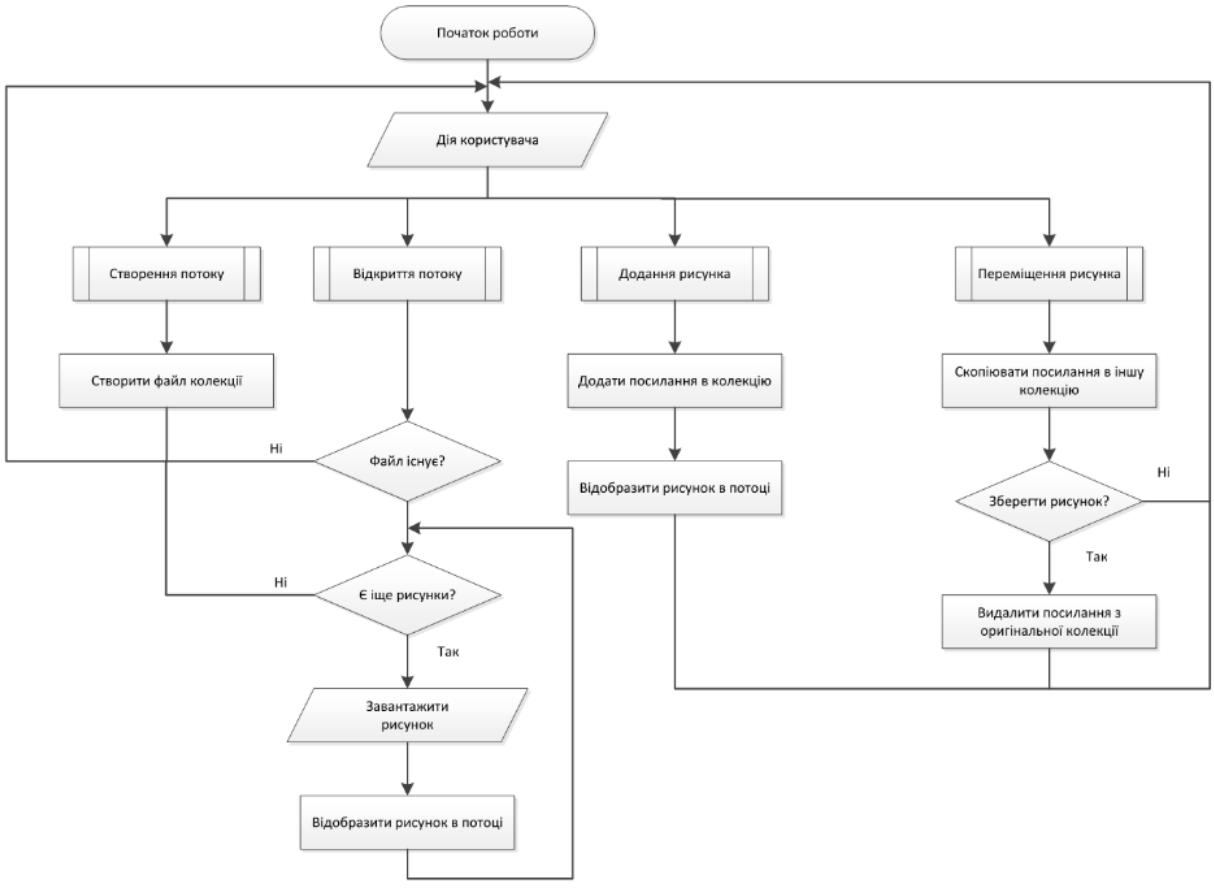


Рисунок 2б – Алгоритм роботи програми, що реалізовує метод покращення візуальним керуванням галереями графічних файлів

3. Розробка та тестування програмного засобу, що реалізовує метод покращення візуальним керуванням галереями графічних файлів

Програмний засіб, що реалізовує запропонований авторами метод дозволяє не лише переглядати, а й маніпулювати змістом галереями графічних файлів. Для цього ми пропонуємо використати поняття «потік графічних файлів». Цей термін запозичений із галузі сучасних соціальних мереж, де користуваць-

кі повідомлення організовуються в стрічку. Коли користувач має кілька облікових записів, вони організовуються в ряд потоків повідомлень. Ми пропонуємо аналогічний підхід застосувати і для графічних файлів, організовуючи їх колекції в потоки [3].

Ключові ресурси програми організації відображення потоків графічних файлів такі: public class ImageStreamItem; public String getImagePath; public void setImageData; public BufferedImage getImageData. Оголошення цих ресурсів та їх функції наведені на лістингу 1.

```
public class ImageStreamItem
 {  private String imagePath = "";
  public void setImagePath(String imagePath)
  {   this.imagePath = imagePath;  }
  public String getImagePath()
  {   return imagePath;  }
  public void setImageData(BufferedImage imageData)
  {   this.imageData = imageData;  }
  public BufferedImage getImageData()
  {   return imageData;  }
  private BufferedImage imageData = null;
```

Лістинг 1 – Ресурси програми для організації відображення потоків графічних файлів

Етапи побудови програми покращення візуальним керуванням галереями графічних файлів:

1. Розробка головного класу програми.
2. Розробка користувацького інтерфейсу.
3. Реалізація основних функцій, зокрема, методу покращення візуальним керуванням галереями графічних файлів з можливістю організації кількох користувацьких галерей в ряд потоків з можливістю маніпулювання їх змістом.

В процесі розробки скористаємось можливістю динамічно змінювати розмітку робочого вікна програми за подією (в даному випадку – додання нового потоку графічних файлів). Таким чином, ми економимо робочий простір програми, і досягаємо максимуму подачі інформації. Після того, як інтерфейс сконструйовано, можна розподілити функції за відповідними елементами (табл. 1).

Таблиця 1 – Співставлення функцій

Елемент керування	Функція
Меню Gallery	Операції роботи з потоками графічних файлів
Меню Process	Операції з активним потоком графічних файлів

Зовнішній вигляд розробленого програмного засобу можна побачити на рис. 3.

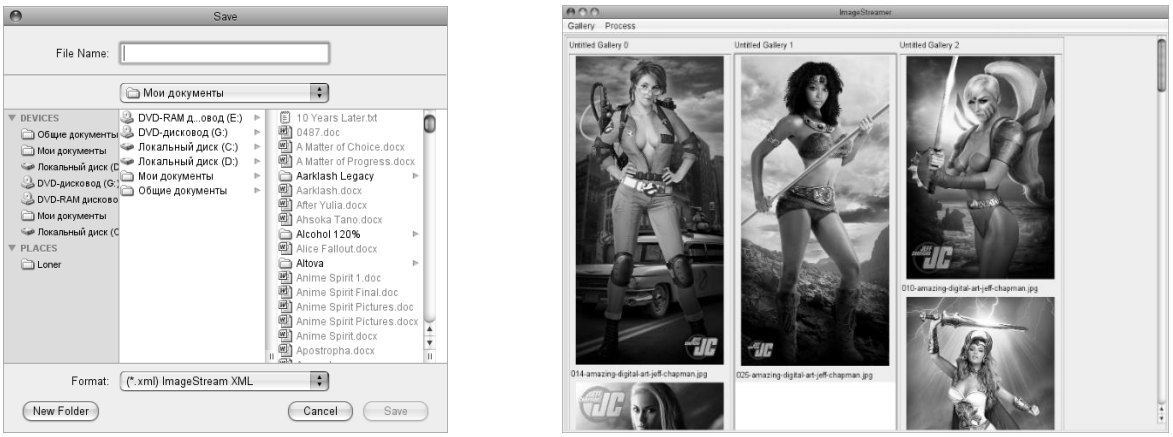


Рисунок 3 – Вигляд робочого простору із декількома потоками одночасно

Слід зауважити, в програмі керування галереями графічних файлів весь функціонал сконцентровано в меню і співставлений гарячим клавішам.

Базовим носієм інформації про потоки графічних файлів будуть файли в форматі XML. Це викликано тим, що файл, який міститиме каталожну інформацію, повинен задовольняти таким критеріям відкритості, читабельності та підтримки деревовидної структури [4].

DTD (Document Type Definition) визначає те, що можна назвати список елементів і їх утворень для використання у визначених документах. Таким чином, вміст документа, його структура, типи використовуваних у ньому елементів і його вигляд визначаються окремо. Незважаючи на веб-орієнтованість цього формату (хоча ця властивість в майбутньому може бути використана при вдосконаленні даного програмного засобу), він легко читається людиною, для роботи з ним існують бібліотеки більшості мов програмування.

Висновки

1. В результаті виконання даної роботи було проаналізовано існуючі програми каталогізації графічних зображень, і виявлено, що вони дозволяють працювати лише з галереєю (колекцією) зображень.

2. Виходячи з цього, була розроблена нова модель представлення графічних файлів та метод покращення візуальним керуванням галереями графічних файлів, побудований на потоковому представленні галерей, які таким чином можуть бути розміщені в межах одного вікна. Це інноваційний підхід для програм, що не використовуються інтернет-сервісах, тому для реалізації такого підходу була обрана мова Java, в якій є необхідний інструментарій.

3. Програма відображення потоків графічних файлів, що розроблена в рамках даної роботи, реалізує всі вимоги, і демонструє потенціал для подальшого розвитку. Потокове представлення колекцій може бути застосоване не лише для зображень, а й до інших типів даних – що закладає можливості для подальшої роботи в цьому напрямку.

Список літератури

1. Єжова. Л. Ф. "Алгоритмізація та програмування процедур обробки інформації". Київ: КНЕУ, 2000 р.
2. J. Roschelle, C. DiGiano, M. Koutlis, A. Repenning, J. Philips, N. Jackiw, D. Suthers Developing Educational Software Components – // Educational Computing Research, 2001.
3. B. McLaughlin, J. Edelson Java and XML – O'Reilly, 2003.
4. E. R. Harold, W. Scott Means XML in a Nutshell – O'Reilly, 2005.

Відомості про авторів

Трояновська Тетяна Іванівна, к. т. н., доцент кафедри обчислювальної техніки, ВНТУ, кафедра обчислювальної техніки, Вінниця, Хмельницьке шосе, 95

Савицька Людмила Анатоліївна, к. т. н., доцент кафедри обчислювальної техніки, ВНТУ, кафедра обчислювальної техніки, Вінниця, Хмельницьке шосе, 95

Жарий Ігор Анатолійович, магістр кафедри обчислювальної техніки, ВНТУ, кафедра обчислювальної техніки, Вінниця, Хмельницьке шосе, 95

МАТЕМАТИЧНЕ МОДЕЛЮВАННЯ ТА ОБЧИСЛЮВАЛЬНІ МЕТОДИ

УДК 004.056.55

Р. Н. Квєтний[1], Є. О. Титарчук [1], А. А. Гуржій[2]

МЕТОД ТА АЛГОРИТМ ОБМІНУ КЛЮЧАМИ СЕРЕД ГРУПИ КОРИСТУВАЧІВ НА ОСНОВІ АСИМЕТРИЧНИХ ШИФРІВ ECC ТА RSA

1 – Вінницький Національний Технічний Університет, м. Вінниця
2 – Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», м. Київ

Анотація. У статті представлено порівняння швидкодії реалізацій методу обміну ключами Діффі-Геллманна для багатьох учасників на основі асиметричних алгоритмів шифрування ECC та RSA. Даний метод дає змогу групі користувачів згенерувати спільний симетричний ключ шифрування у незахищених каналах зв'язку, без необхідності використання централізованого серверу. У роботі надається приклад реалізації алгоритму на кожній з вище названих асиметричних схем шифрування у вигляді математичної моделі та алгоритму на мові програмування C#, проведено порівняння швидкості генерації асиметричних ключів шифрування та спільного симетричного ключа для різної кількості сторін.

Ключові слова: Метод Діффі-Геллмана, Гібридне шифрування, ECC, RSA.

Аннотация. В статье представлено сравнение быстродействия двух реализаций метода обмена ключами Диффи-Хелмана для группы участников на основе ассиметричных шифров ECC и RSA. Данный метод дает возможность группе пользователей сгенерировать общий ключ шифрования в незащищенных каналах связи, без необходимости использования централизованного сервера. В статье приводиться пример реализации алгоритма для каждой из выше названых асимметричных схем шифрования в виде математической модели и на языке программирования C#. Также приводиться сравнение скорости генерации асимметрических ключей шифрования и общего симметрического ключа для разного количества участников.

Ключевые слова: Метод Диффи-Хелмана, Гибридное шифрование, ECC, RSA.

Abstract. The article presents a comparison of performance implementations of key exchange method Diffie-Hellmanna for many participants based on asymmetric codes ECC and RSA. This method allows a group of users to generate a common encryption key in unprotected communication channels, without the need of a centralized server. The article provided an example of the algorithm for each of these encryption schemes in the form of mathematical models and algorithms in the programming language C#. Also, a comparison of the rate of generation of asymmetric encryption keys and of common symmetric key for a different number of participants is given.

Key words: Diffie-Hellman method, Hybrid encrypting, ECC, RSA.

Вступ

Поява асиметричних алгоритмів шифрування зробила можливим обмін ключами у незахищених каналах зв'язку. Безліч сучасних систем авторизації та ідентифікації використовують різноманітні асиметричні шифри для захисту інформації користувачів. Проте важливим обмеженням їх застосування є відносно невисока швидкодія у порівнянні з симетричними алгоритмами. Тому не є дивною поява гібридного шифрування, що дозволяє поєднати найкращі сторони симетричних та асиметричних алгоритмів та нівелювати їх недоліки. Так, для генерації спільного ключа шифрування використовується асиметричний алгоритм, коли ж кожен з учасників встановив спільний ключ шифрування, повідомлення зашифровується одним з симетричних шифрів, наприклад AES.

Прикладом алгоритму встановлення спільного ключа є протокол Діффі-Геллмана, для багатьох учасників. Фактично, будь-яка кількість учасників може узяти участь в узгоджені ключів через ітеративне виконання протоколу узгодження, при цьому проміжні данні можуть бути відкритими. Такий протокол можна реалізувати декількома асиметричними алгоритмами шифрування, найпопулярніші серед яких – RSA та ECC. [2]

Але така генерація спільного ключа шифрування вимагає значних обчислювальних потужностей і залежить від довжини ключа, а також кількості учасників які генерують спільний ключ шифрування. Метою даної статті є визначення оптимального асиметричного шифру для генерації спільних ключів шифрування серед багатьох учасників.

У роботі представлено способи реалізації протоколу Діффі-Гелмана для обміну ключами для двох та більше учасників як на основі алгоритму RSA, так і з використанням алгоритму ECC. [1, 2, 3]

Важливою характеристикою створюваної системи є швидкість генерації ключів, тому у роботі було виконано порівняння двох реалізацій протоколу на мові програмування C# та платформі .NET Framework 4.5 з використанням математичної бібліотеки MPIR [6] для розрахунків з великими числами.

Актуальність

На сьогоднішній день створено багато протоколів обміну інформацією серед груп користувачів, а також програм, що їх використовують. Дані протоколи направлені не тільки (і не стільки) на ефективність обміну інформацією, а на її захист. Проте керування ключами зазвичай відбувається лише на стороні сервера, або ж підтримує лише двох учисників, що робить такі протоколи вразливими. Зарадити

цьому може алгорит обміну ключами серед багатьох учасників, що дозволяє згенерувати спільних ключ використовуючи незахищені канали зв'язку. Тому є актуальною задача визначення оптимального асиметричного алгоритму шифрування для генерації спільних ключів шифрування серед багатьох учасників.

Мета

Метою даної статті є визначення оптимального асиметричного шифру для генерації спільних ключів шифрування серед багатьох учасників.

Задачі

1. Реалізувати протокол обміну ключами Діффі-Гелмана на основі алгоритму ECC.
2. Реалізувати протокол обміну ключами Діффі-Гелмана на основі алгоритму RSA.
3. Порівняти реалізації протоколу.

1 Опис алгоритму

В даному розділі подано протокол обміну ключами в двох реалізаціях: з використанням алгоритму шифрування RSA, та алгоритму шифрування на еліптичних кривих – ECC.

Протокол спілкування клієнтів використовує метод Діффі-Геллмана для утворення симетричного ключа шифрування. Спільні для учасників параметри шифрування генерує та зберігає сервер. Такими параметрами для алгоритму шифрування на еліптичних кривих є власне еліптична крива E(a, b), точка-генератор G, що належить даній кривій та її порядок NG, а також просте число (P_E) – модуль поля кривої. Для алгоритма шифрування RSA – це просте число A, що буде використано для утворення симетричного ключа шифрування, та (P_R), що є модулем поля. [2, 3, 5]

2 Алгоритм ECC

2.1 Генерація асиметричних ключів

Генерація приватного ключа (K_{sec}) з випадкового числа (R) має вигляд:

$$K_{sec} = R \bmod P_E \tag{1}$$

Генерація публічного ключа шифрування (K_{pub}) кожної із сторін на основі їх приватних ключів може бути описана формулою: [6]

$$K_{pub} = K_{sec} \times G \tag{2}$$

Створений на основі формул алгоритм матиме вигляд:

GenerateKey:
```
Random rnd = new Random();
var privateKey = new mpz_t(rnd.Next(GeneratorPoint.PointDimention);
if (privateKey < 0) privateKey = privateKey * -1;
var key = new ECCKey();
key.PrivateKey = privateKey;
key.OpenKey = ECCPoint.Multiply(privateKey, GeneratorPoint);
```

2.2 Генерація спільного ключа

Для генерації спільного ключа шифрування користувачі, незалежно, на основі спільних параметрів обраної криптосистеми, формують асиметричну пару ключів, а потім обмінюючись ними формують спільний секретний ключ.

Спільний ключ шифрування (K_{sym}) для і-того учасника при кількості учасників – N, та виборі алгоритму шифрування ECC має вигляд:

$$K_{sym} = K_{sec_i} \times \prod_{\substack{j=1 \\ j \neq i}}^{N} K_{pub_j} \tag{3}$$

Так, як, в еліптичній криптографії операція множення точки на точку не визначена, при реалізації даної формули відбувається передача часткових ключів між учасниками. Тобто, кожен з учасників відповідаючи на запит іншого учасника, помножує до отриманого ключа свій секретний ключ та повертає ре-

зультат. Таких повторень повинно бути строго N-1, при більшому числі запитів має місце атака Men-in-Middle і зв'язок необхідно розірвати. Також, всі передачі ключів повинні проходити перевірку на автентичність з використанням постійних відкритих ключів шифрування. Після останнього запиту учасник домножує до ключа власний приватний ключ, утворюючи, таким чином, спільний симетричний ключ шифрування.

Реалізація на мові програмування:

GenerateSymetricWithECC:

```
var tempKey = ECCPoint.Multiply(allPersons.Count, keyPair.G);
//now each person have to add his key
foreach (var person in allPersons)
{
   if (person != this)
      person.AddOwnSecretKey(tempKey);
}
//add own private key
var secretKey = ECCPoint.Multiply(keyPair.PrivateKey, symmetricKey.OpenKey);
var leftBytes = secretKey.X.ToByteArray(0);
var rightBytes = secretKey.Y.ToByteArray(0);
var resultSymetricKey = new mpz_t(left.Concat(right).ToArray(0));
```

AddOwnSecretKey:

```
tempKey = ECCPoint.Multiply(keyPair.PrivateKey, tempKey);
```

Якщо підставити формулу 2 у формулу 3, то можна побачити, що після реалізації наведеного вище алгоритму, кожен з учасників отримає однаковий симетричний ключ шифрування:

$$K_{sym} = N \times G \times \sum_{j=1}^{N} K_{sec_j} \quad (4)$$

3 Алгоритм RSA

3.1 Генерація асиметричних ключів

При використанні алгоритму RSA, спочатку утворюємо відкритий ключ, для чого необхідно згенерувати прості числа p та q, та обчислити їх добуток, отримавши модуль поля:

$$n = pq \quad (5)$$

Використовуючи функцію Ейлера ($\varphi(x)$) вибирається такий публічний ключ K_{pub}, що $1 < K_{pub} < \varphi(n)$, та який взаємно простий з $\varphi(n)$ [7]:

$$\varphi(n) = (p-1)(q-1) \quad (6)$$

Закритий ключ знаходимо як число обернене по модулю $\varphi(n)$, до відкритого ключа [8]:

$$K_{pub} \cdot K_{sec} \equiv 1 \pmod{\varphi(n)} \quad (7)$$

Створений на основі формул алгоритм матиме вигляд:

GenerateKey:

```
mpz_t p, q, e, d, n;
p.SetNumber(Generator.Random(2^512 -1, 2^512 -1));
p.RabinMiller();
```

```
q.SetNumber(Generator.Random(2^512 -1, 2^512, bytes));
q.RabinMiller();
n = p.GetPrimeNumber() * q.GetPrimeNumber();
mpz_t eulersPhiFunction = (p.GetPrimeNumber() - 1) * (q.GetPrimeNumber() - 1);
d = MathExtended.ModularLinearEquationSolver(e, 1, eulersPhiFunction);
var key = new RSAKey();
key.PrivateKey = d;
key.OpenKey = e;
key.P = n;
```

3.2 Генерація спільного ключа

Для створення симетричного ключа шифрування, кожен з учасників повинен по запиту підносити переданий йому ключ в степінь свого приватного ключа шифрування. Так, як і в описаному в розділі 2.1 алгоритмі, після останнього запиту, користувач підносить утворений ключ в степінь свого приватного ключа, для утворення спільного симетричного ключа шифрування.

$$K_{sym} = A^{\sum_{j=1}^{N} K_{sec_j}} \bmod P_R \tag{8}$$

Реалізація на мові програмування:

GenerateSymetricWithRSA:

```
var tempKey = publicPrimeA;
foreach (var person in allPersons)
   if (person != this)
      person.AddOwnSecretKey(tempKey);
var Ksym = tempKey.PowerMod(keyPair.PrivateKey, Pr);
```

AddOwnSecretKey:

```
tempKey = tempKey.PowerMod(keyPair.PrivateKey, Pr);
```

4 Порівняння реалізацій протоколу

В процесі порівняння були використані наступні характеристики алгоритмів шифрування: довжина ключа алгоритму RSA – 1024 біти, та ECC з використанням еліптичних кривих P-192 та P-512, з довжинами ключів 192 та 512 бітів відповідно. Еліптичні криві були обрані з рекомендованих національним інститутом стандартів і технологій США (NIST) [10].

Тест було виконано на комп'ютері з наступними характеристиками:

- Процесор – Intel Core i5-3230M 2.60 GHz.
- Об'єм оперативної пам'яті – 8 Gb
- Операційна система – Microsoft Windows 8.1 Pro

Процес генерації симетричного ключа шифрування складається з двох етапів:

1. Генерація асиметричних ключів шифрування кожним з учасників протоколу.
2. Обмін ключами та генерація спільного симетричного ключа шифрування.

Так, як перший з цих етапів може бути виконаний кожним з учасників окремо, то він хоча і має вплив на швидкість встановлення захищеного зв'язку, проте не залежить від кількості учасників. Середній час генерації однієї пари асиметричних ключів шифрування наведено у таблиці 1.

Таблиця 1 – Час генерації асиметричного ключа шифрування

Алгоритм	Час генерації (с)
RSA 1024	0,758
ECC P-192	0,008
ECC P-512	0,034

Отже, загальний час встановлення зв'язку (t_{res}) складається з суми часу генерації пари асиметричних ключів кожним з учасників окремо (t_a) та часу генерації спільного симетричного ключа шифрування (t_s):

$$t_{res} = t_a + t_s \quad (9)$$

Загальній час встановлення зв'язку при кількості учасників (N) від 2 до 20 представлено на графіку на рис. 1.

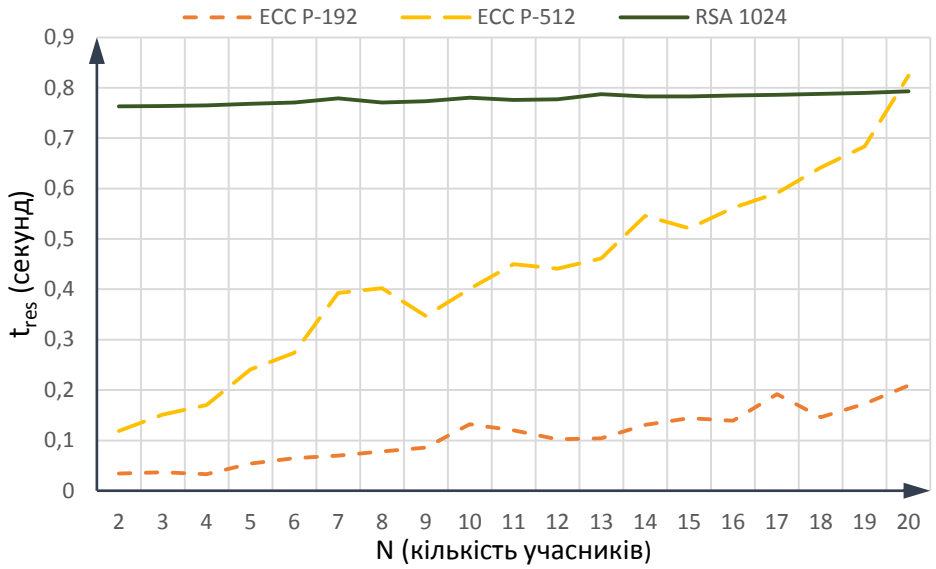


Рисунок 1 – Час встановлення спільного ключа в залежності від кількості учасників

Загальний графік залежності для кількості учасників від 2 до 300 наведено на графіку на рис. 2.

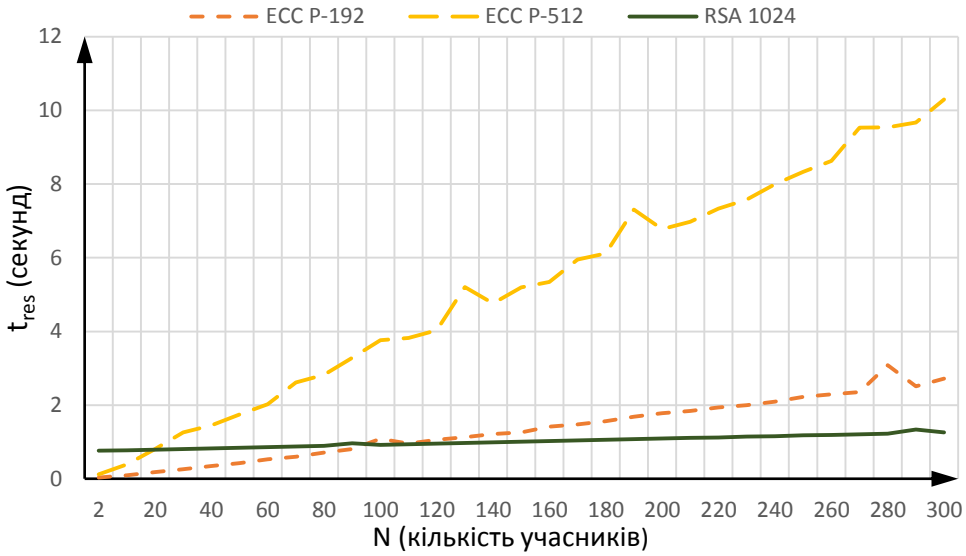


Рисунок 2 – Час встановлення спільного ключа в залежності від кількості учасників

В таблиці 2 наведено час генерації спільного ключа шифрування для 500, 700 та 900 учасників.

Таблиця 2 – Час генерації спільного ключа шифрування

Кількість учасників	Час генерації (с)		
	ECC P-192	ECC P-512	RSA 1024
500	4,353	17,022	1,595
700	7,077	23,097	1,866
900	8,420	30,980	2,387

З даних графіків можна побачити, що завдяки більшій швидкості створення асиметричних ключів алгоритми шифрування на еліптичних кривих більш продуктивні при малій кількості учасників. При цьому, якщо довжина ключа 512 біт, то загальній час встановлення зв'язку менший, ніж в алгоритмі RSA для $N < 20$, якщо ж використати алгоритм ECC з ключем 192 біти, то кількість учасників N для яких він має перевагу, збільшується до 100, що достатньо для більшості з існуючих сценаріїв.

Варто зазначити, що найбільш затратною операцією для алгоритму ECC є множення точки еліптичної кривої на число, для якої було створено декілька оптимізацій [6, 11, 12], а зважаючи на постійний ріст обчислювальних потужностей комп'ютерної техніки і швидший ріст довжини ключа алгоритму RSA, перевага алгоритму ECC буде лише збільшуватись. [1, 2, 10, 11, 12]

Висновки

1. Висновок перший. У алгоритма ECC значно менший час генерації асеметричного ключа шифрування. Найбільш затратною у данному алгоритмі є операція множення точки кривої на число, для якої існують оптимізації, що не були виконані у данній роботі.

2. Висновок другий. Результат порівняння показав, що алгоритм ECC є перспективнішим для застосування у протоколі обміну ключами серед багатьох учасників, проте його елементарна реалізація програє такій з алгоритмом RSA, якщо кількість сторін зростає до 100.

Список літератури

1. E. Titarchuk. Usage of the hybrid encryption in a cloud instant messages exchange system / R. Kvyetnyy, O. Romanyuk, E. Titarchuk, K. Gromaszek, N. Mussabekov // Photonics Applications in Astronomy, Communications, Industry, and High-Energy Physics Experiments 2016, 100314S, September 28, 2016

2. W. Diffie, and M. Hellman. New Directions in Cryptography / IEEE Transactions on Information Theory, Vol. IT-22, NO. 6, November 1976

3. Standards for efficient cryptography. SEC 1: Elliptic Curve Cryptography. Version 1.0 / Certicom Corp. 20, September 2000

4. Mpir.Net – Multiple Precision Integers and Rationals http://wezeku.github.io/Mpir.NET/

5. D. Hankerson, A. Menezes, and S. A. Vanstone. Guide to Elliptic Curve Cryptography / Springer-Verlag, New York 2004

6. Lawrence Washington. Elliptic Curves. Number Theory and Cryptography. 2th edition. / University of Maryland College Park, Maryland, U.S.A, 2008

7. R. Rivest, A. Shamir, L. Adleman. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems / Communications of the ACM, February 1978

8. D. Johnson, A. Menezes, S. Vanstone. The Elliptic Curve Digital Signature Algorithm (ECDSA) / Certicom Corporation, 2001

9. Recommended elliptic curves for federal government use / NIST, July1999

10. Bill Buchanan. Diffie-Hellman Example in ASP.NET / Bill's Security Tips, retrieved 2015-08-27 http://buchananweb.co.uk/security02.aspx.

11. Patrick Longa. Accelerating the Scalar Multiplication on Elliptic Curve Cryptosystems over Prime Fields / University of Ottawa, Canada, 2007.

12. R. P. Gallant, R. J. Lambert, S. Vanstone. Faster Point Multiplication on Elliptic Curves with Efficient Endomorphism / University of Waterloo, Canada, 2001.

Відомості про авторів

Квєтний Роман Наумович – д. т. н., професор, завідувач кафедри АІВТ.

Титарчук Євгеній Олександрович – аспірант кафедри АІВТ.

Гуржій Андрій Андрійович – к. т. н., науковий співробітник, Національний технічний університет України «Київський політехнічний інститут імені Ігора Сікорського».

УДК 004.932.2

Т. Б. Мартинюк, А. В. Кожем'яко, І. Ю. Видмиш, Д. О. Шаромов

НОРМАЛІЗОВАНА КОРЕЛЯЦІЙНА ОБРОБКА ДВОВИМІРНИХ ЗОБРАЖЕНЬ

Вінницький національний технічний університет, м. Вінниця

Анотація. В роботі розглянуто особливості нормалізованої кореляційної обробки двовимірних бінарних зображень. Цей підхід реалізован на матричному оптоелектронному кореляторі, в якому базовим вузлом є кореляційна матриця. В такій матриці існує можливість створення тороїдальних зв'язків між її крайніми елементами (комірками). Наведено два варіанти виконання нормалізованої кореляційної обробки бінарних зображень. Розглянуті варіанти реалізації кореляційної обробки зображень дозволяють значно скоротити апаратні витрати матричного корелятора.

Ключові слова: нормалізована кореляційна обробка, бінарне зображення, тороїдальна топологія зв'язків, взаємокореляційна функція.

Аннотация**.** В работе рассмотрены особенности нормализованной корреляционной обработки двумерных бинарных изображений. Этот подход реализовано на матричном оптоэлектронном корреляторе, в котором базовым узлом является корреляционная матрица. В такой матрице существует возможность создания тороидальных связей между её крайними элементами (ячейками). Приведены два варианта выполнения нормализованной корреляционной обработки бинарных изображений. Рассмотренные варианты реализации корреляционной обработки изображений позволяют значительно сократить аппаратные затраты матричного коррелятора.

Ключевые слова: нормализованная корреляционная обработка, бинарное изображение, тороидальная топология связей, взаимнокорреляционная функция.

Abstract. In the work normalized correlation processing of 2D binary images was considered. This approach in optoelectronic matrix correlator wherein the base block is a correlation matrix was implemented. In this matrix it is possible to build toroidal links between extreme elements (cells). There are two embodiments of the normalized correlation processing of binary images. Considered embodiments of correlation imaging processing allow significantly reduce hardware costs of matrix correlator.

Key words: normalized correlation processing, binary image, toroidal topology links, cross-correlation function.

Вступ

Процес кореляції займає значне місце в обробці та аналізі сигналів і зображень. Так цей математичний апарат знайшов застосування в обробці зображень у сфері комп'ютерного зору та дистанційного зондування із супутників, в яких порівнюються дані з різних зображень, в радарному та гідроакустичному обладнанні для дальнометрії і визначення місцезнаходження (пеленгації), в яких порівнюються передані і відбиті сигнали [1, 2]. Результати кореляції використовуються при детектуванні та ідентифікації сигналів в шумі, в організації технічного контролю для спостереження за впливом входу на вихід, в ідентифікації двійкових кодових слів в системі з імпульсно-кодовою модуляцією, в звичайних схемах оцінювання за методом найменших квадратів і в багатьох інших областях, зокрема, в кліматології [1 – 4].

Отже, в якості складових елементів багатьох систем обробки та аналізу радіотехнічних, електричних, біомедичних сигналів на практиці широко застосовуються корелятори, що працюють в реальному часі [1 – 4].

Актуальність

Серед великого розмаїття задач кореляційної обробки двовимірних зображень, в процесі виконання яких визначається відповідність зображень або найкраще розміщення еталона на зображені, або відповідність однієї частини зображення іншій [5 – 7], можна виділити задачу визначення місцезнаходження центра еталона на полі поточного зображення. В цьому випадку серед відомих критеріїв локальної подібності, що застосовуються на різних етапах кореляційної обробки при пошуку об'єктів [5], доцільно вибрати взаємнокореляційну функцію (ВКФ). ВКФ відноситься до достатніх статистик в задачах координатної прив'язки зображень та пошуку об'єктів при наявності гауссового шуму [8]. Необхідно відзначити, що розмір та форма еталонного зображення при пошуку об'єктів повинні відповідати об'єкту, що розшукується, щоб виключити вплив неінформативних точок на точність визначення координат [8].

Мета

Метою даної роботи є вдосконалення процесу кореляційної обробки у матричному кореляторі.

Постановка задачі

Базове кореляційне співвідношення для двовимірних зображень можна представити таким чином [2]:

$$C(u,v) = \sum_{y=1}^{M} \sum_{x=1}^{N} f(x+u, y+v) \cdot t(x,y), \quad (1)$$

де u, v – координати фрагмента кадру f, причому координати пікселів x, y змінюються в межах розміру $N \times M$ шаблона t.

Значення величини $C(u, v)$ з виразу (1) в значній мірі залежить від величини яскравості шаблона та кадру [2]. Вищу надійність при виявленні об'єкта забезпечує нормалізована кореляція C_n, яка приймає значення в діапазоні $C_n \in [0, +1]$. При цьому близьке до одиниці значення C_n свідчить про високу подібність шаблона та фрагмента кадру, а рівне нулю про їх взаємне неспівпадіння [2].

Такий підхід можна реалізувати на відомій структурі оптоелектронного корелятора, яка містить матрицю обчислювальних комірок для визначення кореляційних коефіцієнтів, а також блок керування [9 – 12].

Кореляційна матриця містить обчислювальні комірки 1.i.j (рис. 1) для визначення кореляційних коефіцієнтів (i – номер стовпця; j – номер рядка), кожна з них має адресний вхід 2, синхровхід 3, вхід 4 початкового встановлення, вхід 5 еталонного сигналу, оптичний вхід 6, оптичний вихід 7, інформаційні входи 8-11, інформаційні виходи 12-15, керуючі шини 16-18 матриці, вхід 19 еталонного сигналу матриці. Інформаційні виходи 14 і 12, 13 і 15 кожної обчислювальної комірки 1.i.j, крім крайніх, з'єднані з інформаційними входами 10 і 8, 9 і 11 відповідно сусідніх обчислювальних комірок, розташованих праворуч (1.i+1.j), ліворуч (1.i-1.j), зверху (1.i.j+1) і знизу (1.i.j-1) [12].

У даній кореляційній матриці оптичні сигнали на вході 6 перетворюються у цифровий бінарний код, який в подальшому обробляється в кожній обчислювальній комірці матриці, а результат формується у вигляді наявності чи відсутності оптичного сигналу на виході 7 кожної обчислювальної комірки [12]. Разом с тим аналого-цифрове та цифро-аналогове перетворення оптичних і цифрових сигналів може бути реалізовано за межами кореляційної матриці сучасними методами та засобами АЦП і ЦАП [13, 14].

Корелятор (рис. 1) визначає місцезнаходження центра двовимірного еталонного зображення $G = \{g_{ij}\}$ на полі двовимірного поточного зображення $F = \{f_{ij}\}$, де $N \times M$ – розмірність поточного зображення F, $n \times m$ – розмірність еталонного зображення G. Поточне F та еталонне G зображення є бінарними зображеннями, тобто кожний їх піксель подається одноразрядним двійковим кодом. На полі поточного зображення F і на полі еталонного зображення G обов'язково присутні центрований рядок і центрований стовпець, які мають нульові номери.

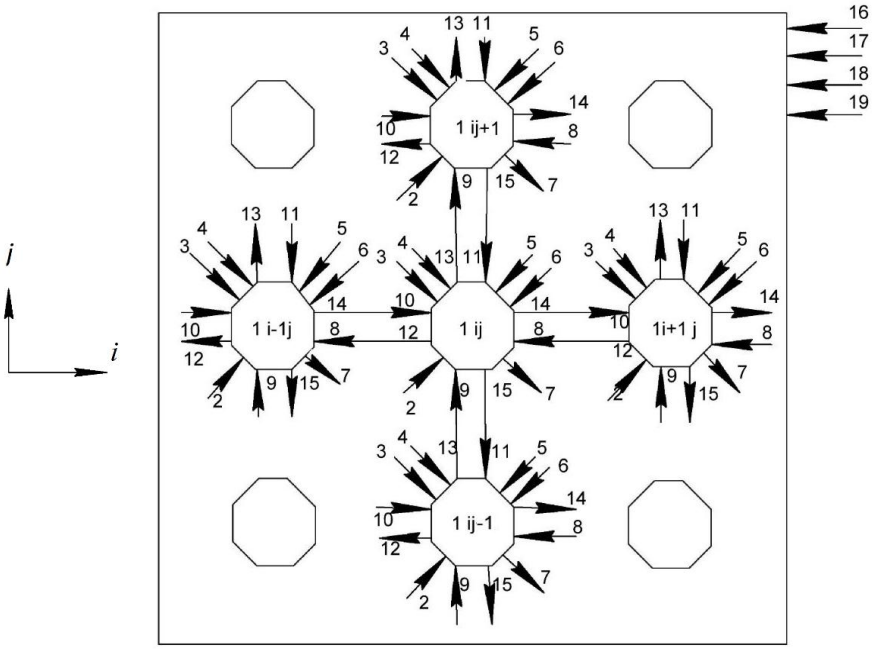


Рисунок 1 – Структура оптоелектронної матриці корелятора

Для наведеної структури корелятора для обчислення взаємнокореляційної функції (ВКФ) використовується таке співвідношення [10, 12]:

$$C_{kl} = \sum_{-\frac{n}{2}}^{\frac{n}{2}} \sum_{-\frac{m}{2}}^{\frac{m}{2}} g_{ij} \cdot f_{i-k,j-l}, \qquad (2)$$

де f_{ij} – елемент (піксель) великоформатного поточного зображення (ПЗ) F; g_{ij} – елемент (піксель) дрібноформатного еталонного зображення (ЕЗ) G; C_{kl} – кореляційний коефіцієнт матриці рельєфу C з координатами (k, l) по відповідних осях (i, j). Таким чином вектор зсуву пікселів f_{ij} поточного зображення F можна подати як $(\overline{-k, -l})$.

В результаті в операційно-транзитному режимі на l-му такті ($l = \overline{0,\ n \times m}$) в кожній обчислювальній комірці формується елемент τ_{ij}^{l} кореляційного рельєфу вигляду:

$$\tau_{ij}^{l} = g_l \cdot f_{ij}\,, \tag{3}$$

причому

$$g_l = \varphi(g_{ij})\,, \tag{4}$$

де функція $\varphi(g_{ij})$ визначає спосіб сканування еталонного зображення G. Наприклад, сканування по спіралі починається з центрального елемента еталонного зображення G з координатами (0; 0) [10, 11].

Приклад нормалізованої кореляційної обробки

Для прискорення процесу обчислення ВКФ пропонується такий підхід до визначення координат центра еталонних зображень G на полі поточного зображення F, який дозволяє відмовитись від «вирощування» кореляційного рельєфу вигляду (2) за рахунок поступового зменшення елементів матриці поточного кореляційного рельєфу на загальну величину у кожному такті обробки [11]. В результаті одиничне значення на робочому поля зберігають тільки глобальні максимуми, що не лише дозволяє перейти від багатоградаційного до бінарного результуючого кореляційного рельєфу, але й за рахунок візуалізації збільшити наочність результату і прискорити визначення необхідних координат. Для збереження інформації при зсуві поточного зображення F за формулою (2) розмірність робочого поля, що дорівнює матриці обчислювальних комірок, повинна бути не менше $(N + n - 1)\times(M + m - 1)$ [10, 12].

На рис. 2 показано графічне подання матриці обчислювальних комірок для визначення кореляційних коефіцієнтів [10].

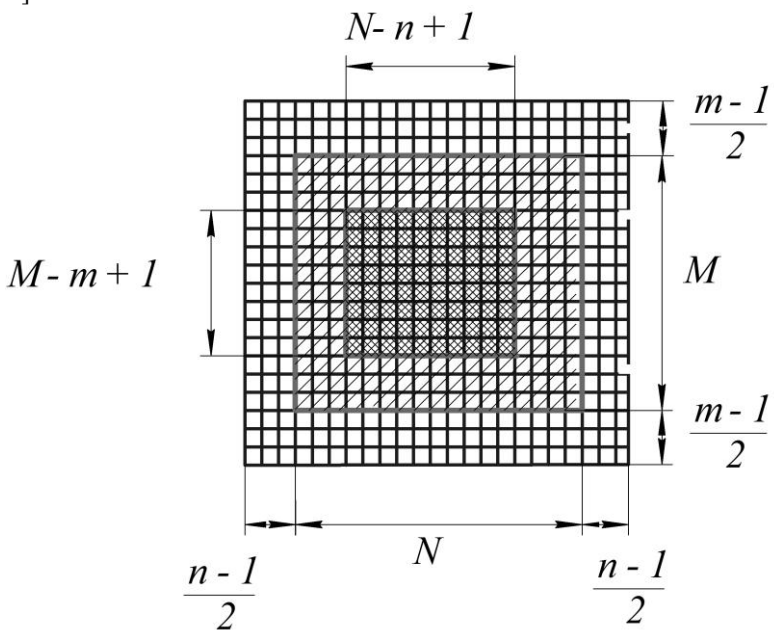


Рисунок 2 – Графічне подання матриці обчислювальних комірок корелятора

З урахуванням поля двовимірного поточного зображення F розмірністю $N\times M$ і поля двовимірного еталонного зображення G розмірністю $n\times m$ в процесі виконання кореляційної обробки можливий зсув у полі поточного зображення праворуч і ліворуч як максимум на величину $\left[\frac{n-1}{2}\right]$, а вгору і вниз на величину $\left[\frac{m-1}{2}\right]$. Тоді матриця обчислювальних комірок містить відповідно $\left(N + 2\left[\frac{n-1}{2}\right]\right)$ стовпців і $\left(M + 2\left[\frac{m-1}{2}\right]\right)$ рядків [10].

Для зчитування результату кореляційної обробки двовимірних зображень виділяється центральна частина матриці обчислювальних комірок розмірністю $(N - n + 1)\times(M - m + 1)$ у вигляді «вікна».

Розмір «вікна» і його розташування на полі матриці обчислювальних комірок визначається розмірами поля $N{\times}M$ поточного і поля $n{\times}m$ еталонного зображень і застосованим способом сканування еталонного зображення [10, 15, 16].

На рис. 3 – 5 наведено приклади виконання кореляційної обробки двовимірних бінарних поточного F та еталонного G зображень з використанням матриці обчислювальних комірок для випадку, коли $N{\times}M = 5{\times}5$ (рис. 3а) і $n{\times}m = 3{\times}3$ (рис. 3б). Інформаційні пікселі обох зображень показано чорними точками. Спосіб розгортки (сканування) еталонного зображення G показано на рис. 3в.

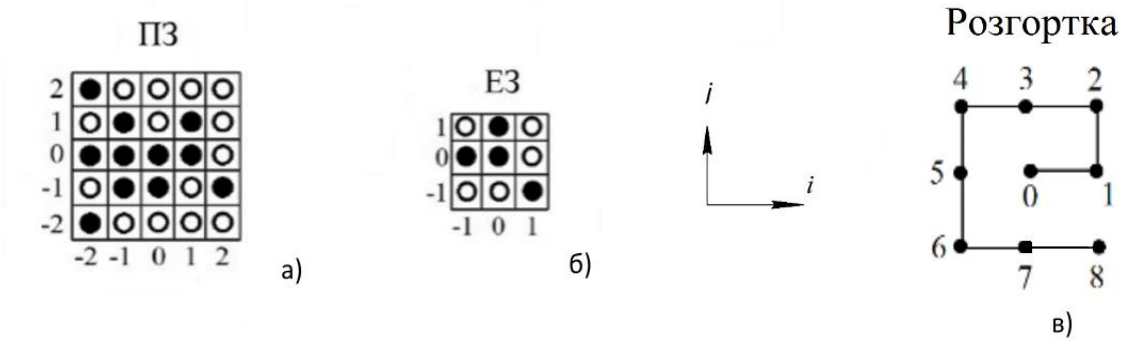


Рисунок 3 – а) – поточне зображення ПЗ; б) – еталонне зображення ЕЗ; в) – розгортка ЕЗ.

Для випадку не застосування з'єднань між крайніми рядками і стовпцями матриці обчислювальних комірок і вказаному способі сканування еталонного зображення G (рис. 3в) та початковому одиничному стані робочого поля (рис. 4а) показано поля поточного зображення F (рис. 4б) з визначеним зсувом поточного зображення F у відповідні такти роботи, вміст кожної обчислювальної комірки матриці показано праворуч на рис. 4в. Робоче поле для зсуву поточного зображення F реалізоване на матриці обчислювальних комірок розмірністю $(N + n - 1){\times}(M + m - 1)$ для збереження інформації при зсуві поточного зображення F за формулою (2).

Всього виконується дев'ять тактів від нульового до восьмого за кількістю пікселів еталонного зображення G (рис. 3б). На восьмому такті формується кінцевий результат кореляційної обробки, який свідчить про те, що обчислювальні комірки матриці, які знаходяться в одиничному стані, відповідають координатам центра еталонного зображення G на полі поточного зображення F. Результат кореляційної обробки свідчить, що центри еталонного зображення знаходяться у точках з координатами (-1; 0) та (1; 0) (рис. 4в).

На рис. 5а наведено вигляд початкового одиничного стану робочого поля розміром $N{\times}M$ з урахуванням інформаційних зв'язків між обчислювальними комірками першого і старшого стовпців та першого і старшого рядків матриці [15, 16]. На восьмому такті формується кінцевий результат кореляційної обробки з координатами центрів еталонного зображення (-1; 0) та (1; 0) (рис. 5в), який співпадає з отриманим на рис. 4в. Робочі такти, тобто такти, в яких виконувались зміни кореляційного рельєфу, показано на рис. 4в і 5в

Оскільки результат кореляційної обробки зчитується з «вікна» матриці обчислювальних комірок розмірністю $(N - n + 1){\times}(M - m + 1)$, то накладання інформації при зсуві поточного зображення F в полі матриці обчислювальних комірок розмірністю $N{\times}M$ не призводить до спотворення результату [10, 15, 17].

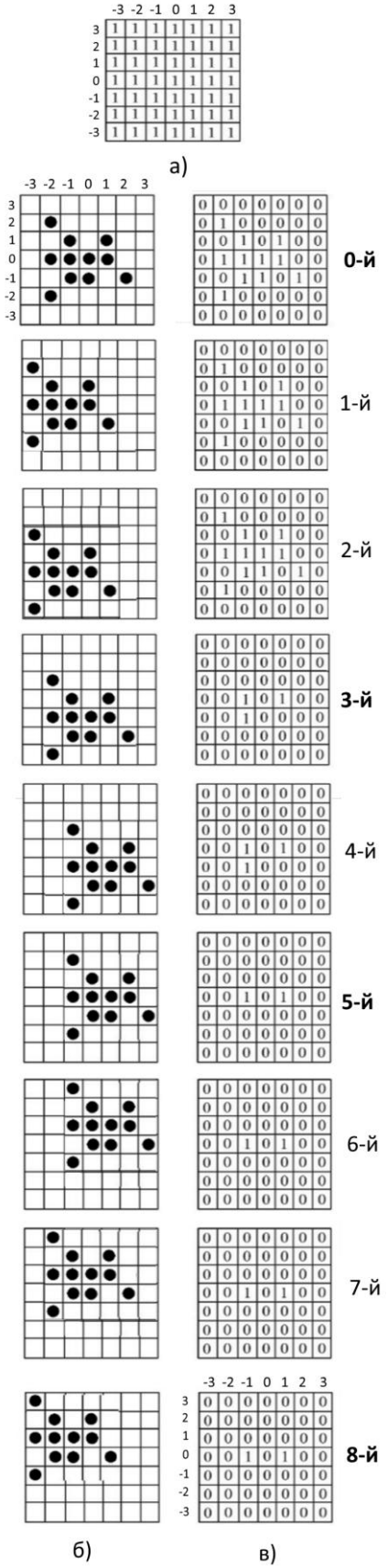


Рисунок 4 – а) – початковий стан робочого поля; б) – робоче поле поточного зображення; в) – результат кореляційної обробки

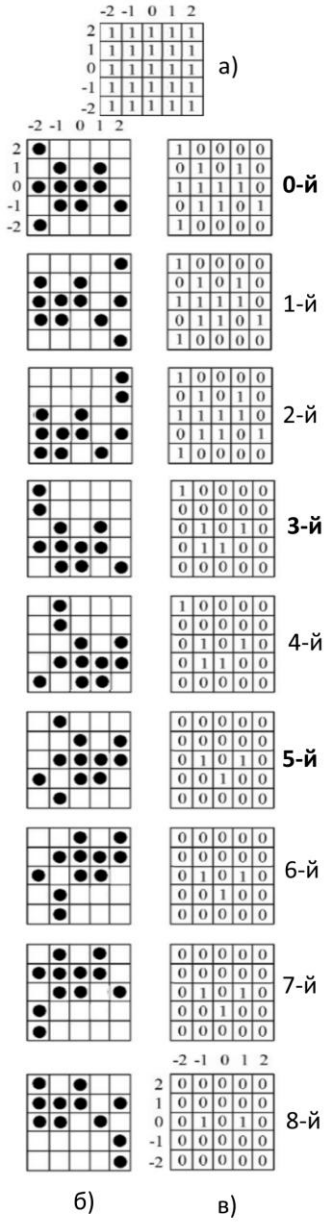


Рисунок 5 – а) – початковий стан робочого поля; б) – робоче поле поточного зображення; в) – результат кореляційної обробки

Висновки

1. Одним з перспективних способів реалізації кореляційної обробки двовимірних зображень є її природнє виконання на матричному кореляторі, базовим вузлом якого є матриця кореляційних коефіцієнтів. Це дозволяє зробити тривалість процесу кореляції незалежною від розмірності вхідного зображення.

2. Можливість використання тороїдальної топології зв'язків у кореляційній матриці дозволяє реалізувати на робочій матриці кореляційний процес за розмірністю вхідного зображення без додаткових рядків і стовпців матриці, що зменшить апаратні витрати.

3. Застосування методу нормалізації вмісту матриці кореляційних коефіцієнтів забезпечує перехід від багатоградаційного до бінарного результуючого кореляційного рельєфу, що дозволяє не тільки зменшити апаратні витрати, але й збільшити наочність результату, оскільки одиничне значення зберігають тільки максимуми на робочому кореляційному полі. Крім того, в процесі кореляції не «вирощуються» максимуми кореляційного рельєфу.

Список літератури

1. Беде Лиу. Цифровая обработка сигналов: практический подход / Беде Лиу, Петренко А.И. Абрахам Пелед, С. Эммануил, Айфичер, У. Барри: пер. с англ. – М.: Издательский дом «Вильямс», 2004. – 992 с.

2. Алпатов Б.А. Методы автоматического обнаружения и сопровождения объектов. Обработка изображений и управление / Б.А. Алпатов, П.В. Бабаян, О.Е. Балашов, А.И. Степашкин. – М.: Радиотехника, 2008. – 176 с.

3. Дуда Ф. Распознавание образов и анализ сцен / Ф. Дуда, П. Харт: пер. с англ. – М.: Мир, 1976. – 512 с.

4. Прэтт У. Цифровая обработка изображений / У. Прэтт: пер. с англ. – Кн. 2. – М.: Мир, 1982. – 480 с.

5. Кун С. Матричные процессоры на СБИС / С. Кун: пер. с англ. – М.: Мир, 1991. – 672 с.

6. СБИС для распознавания образов и обработки изображений / Под ред. К. Фу: пер. с англ. – М.: Мир, 1998. – 248 с.

7. Обидин Ю.В. Специализированный коррелятор /Ю.В. Обидин // Автометрия. – 1989. – №2. – С. 15-18.

8. Кендал М.Д. Статистические выводы и связи / М.Д. Кендал, А. Стюарт: пер. с англ. – М.: Наука, 1973. – 280 с.

9. Relief Determination of Correlation Function in Image Processing / T. Martyniuk, A. Kozhemjako, M. Homchuk // Обробка сигналів і зображень та розпізнавання образів: 3-я Всеукр. міжнар. наук.-техн. конф., 26-30 листопада 1996; праці. – Київ, 1996. – С. 90-91.

10.Мартинюк Т.Б. Кореляція, фільтрація та сегментація зображень. Лабораторний практикум / Т.Б. Мартинюк, Г.Л. Лисенко, Я.Г. Скорюкова. – Вінниця: ВНТУ, 2006. – 80 с.

11.Мартинюк Т.Б. Реалізація кореляційної обробки на матричних структурах / Т.Б. Мартинюк, А.В. Кожем'яко, М.А. Хомчук // Вісник ВПІ. – 1997. - №3. – С. 33-37.

12.Пат. 95168 Україна, МПК G06F17/00. Корелятор / Т.Б. Мартинюк, С.В. Сидорук, С.В. Костюк. – № u 2014 07561; заявл. 04.07.2014; опубл. 10.12.2014, Бюл. №23.

13.Азаров О. Д. Обчислювальні АЦП і ЦАП, що самокалібруються, для систем цифрового обробляння аналогових сигналів. : монографія / О. Д. Азаров, О. О. Коваленко. - УНІВЕРСУМ-Вінниця, 2006.- 146 с.

14.Azarov, O.D., Dudnyk, O.D., Duk, M., Porubov, D. (2013) Static and dynamic characteristics of the self-calibrating multibit ADC analog components //Proc. SPIE. 8698, Optical Fibers and Their Applications 2012, 86980N (January 11.2013); doi 10.1117/12.2019737.

15.Мартинюк Т. Б. Цифровий матричний корелятор з тороїдальною топологією зв'язків / Т.Б. Мартинюк, А.М. Гринчук, О.В. Калінін // Вісник ВПІ. – 2001. – №1. – С. 45-48.

16.Пат.105178 Україна, МПК G06F15/00. Корелятор / Т. Б. Мартинюк, А. В. Кожем'яко, І. Ю. Видмиш, Т. Ю. Позднякова. – № u 2015 07905; заявл. 10.08.2015; опубл. 10.03.2016, Бюл. №5.

17.Особенности реализации топологии связей в матричном корреляторе / Т. Б. Мартынюк, Г.Л. Лысенко, В. А. Ткаченко, С.Е. Тужанский, А.В. Кожемяко // Теорія і практика перебудови економіки: збірник наук. праць. – Черкаси: ЧІТІ, 2001. – С. 255-258.

Відомості про авторів

Мартинюк Тетяна Борисівна – д. т. н., професор, професор кафедри ОТ, службовий тел. 24-50.

Кожем'яко Андрій Вікторович – к. т. н., доцент, доцент кафедри ЛОТ, службовий тел. 21-25.

Видмиш Інна Юріївна – студентка 2-го курсу магістратури кафедри ЛОТ.

Шаромов Дмитро Олександрович – студент 5-го курсу факультету КСА.

ДО ВІДОМА АВТОРІВ

Найновіші правила оформлення і подання статей знаходяться на сайті журналу **http://itce.vntu.edu.ua/index.php/itce/about/submissions#onlineSubmissions**