УДК 681.327.11

Н. В. Сачанюк-Кавецька, О. П. Прозор, В. В. Хом'юк, І. О. Бондаренко

МАТЕМАТИЧНИЙ ОПИС ОПЕРАЦІЇ НЕРІВНОЗНАЧНОСТІ В ЛОГІКО-ЧАСОВОМУ СЕРЕДОВИЩІ

Вінницький національний технічний університет, Вінниця

Анотація. Нині є актуальною проблема інформаційної безпеки, яка пов'язана із збереженням конфіденційності інформації, що обробляється та зберігається в комп'ютерних системах. Цілісність і конфіденційність інформації має вагоме значення для конкурентоспроможності та репутації організації чи підприємства. Аналітична обробка цифрових сигналів в графічному чи в чисто цифровому представленні дещо обмежена і не враховує динаміку сигналів та повідомлень. Щоб полегшити попередню обробку динамічних цифрових змінних та сигналів можна використати логіко-часову функцію багатозначної логіки. В статті зазначено, що обчислювальне математичне моделювання стає основним інструментом дослідження складних динамічних процесів і систем. Класичний апарат логіки є недостатнім для опису динаміки поведінки системи в часі. Тому актуальною є розробка моделей так званого булевого диференціального числення, оскільки даний підхід спирається на загальне поняття зміни логічної змінної, що призведе до універсальної, з точки зору динаміки, системи понять та операцій. Для полегшення попередньої обробки динамічних цифрових змінних та сигналів можна використати логіко-часову функцію багатозначної логіки. В роботі розглянуто одну з важливих операцій – операцію нерівнозначності та деякі її властивості. Показано, що для логіко-часової функції двійкової логіки дана операція співпадає з сумую по модулю два. Нерівнозначність дозволить, в подальшому, ввести більш складні операції над багатозначними логіко-часовими функціями, такими як похідна і первісна та здійснювати кодування, шифрування інформації в логіко-часовому середовищі. Продемонстровано можливість використання нерівнозначності при побудові індикаторних операцій та диференціала змінної. Змодельовано схему реалізації операції нерівнозначності.

Ключові слова: логіко-часова функція багатозначної логіки, нерівнозначність, сума за модулем 2, жвавість, диференціал.

Abstract. Currently, there is an urgent problem of information security, which is related to the preservation of the confidentiality of information processed and stored in computer systems. The integrity and confidentiality of information is of great importance for the competitiveness and reputation of an organization or enterprise. Analytical processing of digital signals in a graphical or purely digital representation is somewhat limited and does not take into account the dynamics of signals and messages. To facilitate the preprocessing of dynamic digital variables and signals, the logic-time function of multivalued logic can be used. The article notes that computational mathematical modeling is becoming the main tool for studying complex dynamic processes and systems. The classical apparatus of logic is insufficient to describe the dynamics of system behavior over time. Therefore, it is important to develop models of so-called Boolean differential calculus, as this approach is based on the general concept of changing the logical variable, which will lead to a universal, in terms of dynamics, system of concepts and operations. It is shown that for the logic-time function of binary logic, this operation coincides with the sum modulo two. You can use the logic-time function of multivalued logic to facilitate the pre-processing of dynamic digital variables and signals. The paper considers one of the important operations - the operation of inequality and some of its properties. Inequality will allow, in the future, to introduce more complex operations on multivalued logical-temporal functions, such as derivative and initial, and to perform encoding, encryption of information in the logical-temporal environment. The possibility of using inequality when constructing indicator operations and variable differential is demonstrated. The implementation scheme of the inequality operation is modeled.

Keywords: logic-time function of multivalued logic, inequality, sum by module 2, liveliness, differential.
DOI: https://doi.org/10.31649/1999-9941-2022-54-2-124-130.

Вступ

Використання методів математичного моделювання та автоматизованих рішень інженерно-наукових завдань дозволяє значно підвищити ефективність процесів проектування, реконструкції, обробки та управління. Обчислювальне математичне моделювання стає основним інструментом дослідження складних динамічних процесів і систем. Загально прийнятим математичним апаратом дослідження цифрових сигналів є алгебра логіки. З її допомогою було сформульовано та розв'язано безліч задач опису, перетворення та побудови логічних систем. Класичний апарат логіки, що достатньо точно описує структуру та функціональні зв'язки між входами та виходами таких систем, є недостатнім для опису динаміки поведінки системи в часі. Питання «динаміки у великому» досить легко розв'язуються за допомогою теорії автоматів, однак вона не відображає динаміку перехідних процесів, пов'язану із часовими характеристиками елементів системи, що вимірюються в реальному часі. Тому актуальною є розробка моделей так званого булевого диференціального числення, оскільки даний підхід спирається на загальне поняття зміни логічної змінної, що призведе до універсальної, з точки зору динаміки, системи понять та операцій за допомогою яких можна ставити та розв'язувати задачі типові як для теорії автоматів, так і для дискретної «динаміки в малому».

Огляд та постановка задачі

З появою та розвитком інформаційних технологій актуальною проблема інформаційної безпеки, яка пов'язана із збереженням конфіденційності інформації, що обробляється та зберігається в комп'ютерних системах. Саме цілісність і конфіденційність інформації має вагоме значення для конкурентоспроможності та репутації підприємства. Аналітична обробка цифрових сигналів в графічному чи в чисто цифровому представленні дещо обмежена і не враховує динаміку сигналів та повідомлень. Тому, щоб полегшити попередню обробку динамічних цифрових змінних та сигналів можна використати логіко-часову

функцію багатозначної логіки (БЛЧФ) [1]. Для комп'ютерної обробки в режимі реального часу аналоговий сигнал повинен бути оцифрований шляхом його вибірки за одиничними $\Delta-$ інтервалами та реалізовано квантування на k рівнів амплітуди. В роботі [2] було розглянуто індексну форму подання БЛЧФ, поняття продукуючого слова та базові операції над функціями, які дозволяють розробляти більш складні операції. Зокрема такі операції, які дозволять кодувати інформацію та будувати крипто-ключі, оскільки це є одним із ключових моментів розробки політики інформаційної безпеки [3].

Тому актуальною буде розробка математичного апарату, який в простій і доступній формі дозволить здійснювати аналітичну обробку динамічних цифрових сигналів та здійснювати прогнозування змін параметрів сигналів суто засобами математики. В роботі [1] було введено операцію нерівнозначного віднімання, що визначалась різницею по модулю значень та була досить громіздкою при використанні. Враховуючи подання БЛЧФ, яке було запропоновано [2] та узагальнюючи логіко-часові функції (ЛЧФ) двійкової та багатозначної логіки таку операцію більш доцільно вважати логічною операцією нерівнозначності, а модуль різниці амплітуд змінних є мірою цієї нерівнозначності.

Мета

Метою даної статті є представлення операції нерівнозначності логіко-часових функцій багатозначної логіки з використанням моделювання її схеми.

Основні положення

Для позначення нерівнозначності $\left|{}^{x}_{k}a_t - {}^{y}_{k}d_t\right|$ використаємо символ «$\ominus$» і запишемо нерівнозначність БЛЧФ у вигляді:

$$\left({}_k x^{T_x}_{t_x} \ominus_k y^{T_y}_{t_y}\right) = \underset{i=0}{\overset{T_{\max}-1}{W}} \left({}^{x}a_i \ominus {}^{y}c_i\right) \Big|_k \left(x \ominus y\right)^{T_{\max}}_{\min(t_x,\, t_y)},$$

де W – оператор впорядкування за часом та розбиття значень аргументів БЛЧФ на одиничні $\Delta-$інтервали.

Операція нерівнозначності має властивість комутативності: ${}_k x(t) \ominus_k y(t) = {}_k y(t) \ominus_k x(t)$. Для ілюстрації справедливості даної властивості проаналізуємо таблиці Келлі, наприклад для $k = 2, 3, ma\ 4$ (див. рис. 1). Оскільки всі таблиці симетричні відносно головної діагоналі, то це означає, що операція нерівнозначності комутативна.

Можна показати, що дана операція не має властивості асоціативності:

$$\left(x \ominus y\right) \ominus z \neq x \ominus \left(y \ominus z\right),$$

і також немає властивості дистрибутивності кон'юнкції (диз'юнкції) відносно операції нерівнозначності. Зокрема, $\left(x_t \triangleq \left(y_t \ominus z_t\right)\right) \neq \left(x_t, \triangleq y_t\right) \ominus \left(x_t \triangleq z_t\right)$, де «$\triangleq$» – операція кон'юнкції БЛЧФ:

$$\left({}_k x^{T_x}_{t_x} \triangleq_k y^{T_y}_{t_y}\right) =$$

$$= \underset{i=0}{\overset{\substack{\min(t_x+T_x,\, t_y+T_y)- \\ -\max(t_x,\, t_y)-1}}{W}} \min\left({}^{x}a_i,\, {}^{y}c_i\right) \Big|_k \left(x \underline{\wedge} y\right)^{\min(t_x+T_x,\, t_y+T_y)-\max(t_x,\, t_y)}_{\max(t_x,\, t_y)}.$$

Індекси типу $\min, \max$ з параметрами, визначають інтервали існування функції, а значення власне самої функції, кон'юнкцію ${}^{x}a_t$ та ${}^{y}c_t$, потрібно вираховувати для кожного t з кроком рівним одиниці від $\max\left(t_x, t_y\right)$ до $\left(\min\left(t_x + T_x, t_y + T_y\right) - \max\left(t_x, t_y\right)\right)$.

$\ominus$	0	1
0	0	1
1	1	0

k=2

$\ominus$	0	1	2
0	0	1	2
1	1	0	1
2	2	1	0

k=3

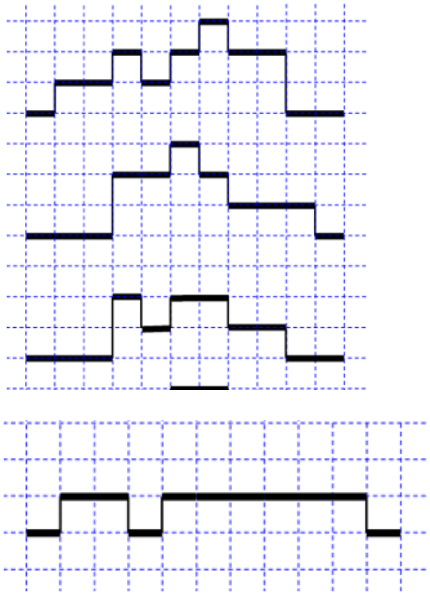
$\ominus$	0	1	2	3
0	0	1	2	3
1	1	0	1	2
2	2	1	0	1
3	3	2	1	0

k=4

а) б) в)

Рисунок 1 – Таблиці Келлі для: а) $k=2$; б) $k=3$; в) $k=4$

На рис. 2 подано графічну ілюстрацію операцій кон’юнкції та нерівнозначності БЛЧФ.



$${}_4x(t)=1^2 2^1 1^1 2^1 3^1 2^2\Big|_4 x_1^8$$

$${}_4y(t)=2^2 3^1 2^1 1^3\Big|_4 y_3^7$$

$${}_4x(t)\triangleq {}_4y(t)$$

$${}_4x(t)\ominus {}_4y(t)$$

Рисунок 2 – Графічна ілюстрація операцій «$\triangleq$» та «$\ominus$»

Для операції нерівнозначності за визначенням справедливі такі тотожності:

$$x\ominus x=0,$$
$$x\ominus 0=x,$$
$$x\ominus(k-1)=\tilde{x},$$

де $\tilde{x}$ – заперечення Лукасевича.

Має місце теорема: Логічний вираз бінарної логіки записаний в базисі І, АБО, НІ справедливий і для формул k-значної логіки при $k=2$.

Для ілюстрації доведення скористаємось формулою для нерівнозначності або додавання по модулю 2 для двох двійкових змінних: $x\oplus y=x\bar{y}\vee\bar{x}y$, що в k-значному форматі для $k=2$ виглядає так: $x\ominus y=x\tilde{y}\vee\tilde{x}y$. Можна показати, що функції І, АБО, НІ взаємно еквівалентні для алгебри Буля і

k -значної алгебри при $k=2$. Тоді взаємна еквівалентність справедлива і для логічних виразів. Побудуємо таблицю істинності для $x \oplus y$ та $x \ominus y$ (див. табл. 1).

Таблиця 1 − Таблиця істинності

x	y	$\overline{x}$	$\tilde{x}$	$\overline{y}$	$\tilde{y}$	$x \square \overline{y}$	$\overline{x} \square y$	$x \square \tilde{y}$	$\tilde{x} \square y$	$x \square \overline{y} \vee \overline{x} \square y$	$x \square \tilde{y} \bar{\vee} \tilde{x} \square y$
0	**0**	*1*	*1*	*1*	*1*	*0*	*0*	*0*	*0*	*0*	*0*
0	**1**	*1*	*1*	*0*	*0*	*0*	*1*	*0*	*1*	*1*	*1*
1	**0**	*0*	*0*	*1*	*1*	*1*	*0*	*1*	*0*	*1*	*1*
1	**1**	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*

З таблиці зрозуміло, що $x \square \overline{y} \vee \overline{x} \square y$ рівний $x \square \tilde{y} \bar{\vee} \tilde{x} \square y$.

Якщо вхідні змінні x та y є ЛЧФ, що мають по одному відрізку існування $x(t) = x_{t_x}^{T_x}$, $y(t) = y_{t_y}^{T_y}$, тоді $\tilde{x}(t) = x_0^{t_x} \dot{+} x_{t_x+T_x}^{\infty}$, $\tilde{y}(t) = y_0^{t_y} \dot{+} y_{t_y+T_y}^{\infty}$ відповідно. Використавши досконалу диз'юнктивну нормальну форму отримаємо:

$$
\begin{aligned}
& x(t) \ominus y(t) = (x_0^{t_x} \dot{+} x_{t_x+T_x}^{\infty}) \square y_{t_y}^{T_y} \bar{\vee} x_{t_x}^{T_x} \square (y_0^{t_y} \dot{+} y_{t_y+T_y}^{\infty}) = \\
& = \left(x_0^{t_x} \square y_{t_y}^{T_y} \dot{+} x_{t_x+T_x}^{\infty} \square y_{t_y}^{T_y} \right) \bar{\vee} \left(x_{t_x}^{T_x} \square y_0^{t_y} \dot{+} x_{t_x}^{T_x} \square y_{t_y+T_y}^{\infty} \right) = \\
& = \left((x \ominus y)_{t_y}^{\min(t_x,\, t_y+T_y)-t_y} \dot{+} (x \ominus y)_{\max(t_x+T_x,\, t_y)}^{(t_y+T_y)-\max(t_x+T_x,\, t_y)} \right) \bar{\vee} \\
& \bar{\vee} \left((x \ominus y)_{t_x}^{\min(t_x+T_x,\, t_y)-t_x} \dot{+} (x \ominus y)_{\max(t_x,\, t_y+T_y)}^{(t_x+T_x)-\max(t_x,\, t_y+T_y)} \right)
\end{aligned}
$$

Подальший аналітичний запис вимагає використання формули для диз'юнкції БЛЧФ:

$$
\left({}_k x_{t_x}^{T_x} \bar{\vee} {}_k y_{t_y}^{T_y} \right) = \dot{\bigvee_{i=0}^{T_{\max}-1}} \max\left({}^{x}a_i,\ {}^{y}c_i \right) \Big|_k \left(x \bar{\vee} y \right)_{\min(t_x,\, t_y)}^{T_{\max}},
$$

де « $\underline{\vee}$ » – операція диз'юнкції БЛЧФ , а $T_{\max} = \left(\max\left(t_x + T_x, t_y + T_y \right) - \min\left(t_x, t_y \right) \right)$.

Аналітично це трохи громіздкий варіант, але для конкретних реальних змінних все набагато простіше. Звичайно аналітичні дослідження зручніше робити через продукуючі слова повної форми запису БЛЧФ.

На рис. 3 наведено графічні результати операції додавання по модулю 2 або нерівнозначності.

Тоді аналітичне обчислення відповідних функцій, зображених на рис. 3:

$$
\begin{aligned}
& x_1^2 \oplus y_2^4 = (x \oplus y)_2^{-1} \vee (x \oplus y)_3^3 \vee (x \oplus y)_1^1 \vee (x \oplus y)_6^{-3} = \\
& = (x \oplus y)_1^1 \vee (x \oplus y)_3^3;
\end{aligned}
$$

$$
\begin{aligned}
& x_1^2 \oplus z_5^3 = (x \oplus z)_5^{-4} \vee (x \oplus z)_5^3 \vee (x \oplus z)_1^2 \vee (x \oplus z)_8^{-5} = \\
& = (x \oplus z)_1^2 \vee (x \oplus z)_5^3.
\end{aligned}
$$

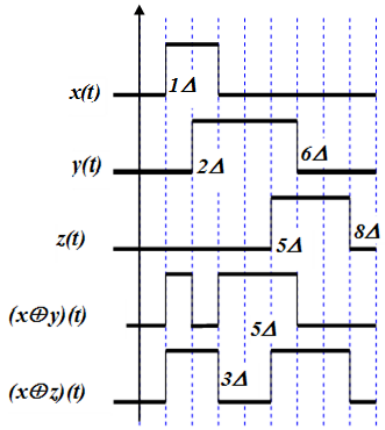


Рисунок 3 − Двійкова нерівнозначність

Операцію нерівнозначності можна застосувати при побудові так званих індикаторних операцій. Зокрема, для оцінки інтенсивності зміни БЛЧФ введемо поняття жвавості. Жвавість (V) це число, що показує сумарно як інтенсивно змінюється значення функції протягом всього відрізку її існування, який може включати нульові підінтервали і визначається за формулою:

$$V\left(a_0, a_1, \ldots, a_N \middle|_k x_{t_x}^{T_x}\right) = \sum_{i=0}^{N+1} \left(a_i \ominus a_{i+1}\right).$$

Для функції $_4x(t) = 1^2 2^1 1^1 2^1 3^1 2^2 \Big|_4 x_1^8$ жвавість $V = 8$. Максимальне значення жвавості на відрізку існування обчислюється за формулою: $V_{\max}\left(_k x_{t_x}^{T_x}\right) = \left[\left(k-1\right)\times\left(T_x+1\right)\right]$. Відповідно мінімальне значення жвавості $V_{\min} = 1$ і описує перехід БЛЧФ з однієї константи на сусідню вверх або вниз на логічну одиницю, а при $V = 0$ маємо справу з константою. Якщо для бінарної ЛЧФ з N відрізками існування, використати індексний запис БЛЧФ і добавити нульові підінтервали, отримаємо оцінку жвавості двійкової багатоінтервальної ЛЧФ. Такий підхід об’єднує всі $k \geq 2$ і дає можливість все розглядати як багатозначність. Бінарний варіант це окремий випадок загального $k-$значного варіанту.

Для повної форми представлення БЛЧФ:

$$V\left(x_{t_x}^{T_x}\right) = V\left(\overset{T_x-1}{\underset{i=0}{W}} a_i \middle| x_{t_x}^{T_x}\right) = \sum_{i=0}^{T_x-1} \overset{T_x-1}{\underset{i=0}{W}} \left(a_i \ominus a_{i+1}\right) = \left[\sum_{i=0}^{T_x-1} \left(a_i \ominus a_{i+1}\right)\right]$$

В роботі [4] було введено змінну dx , що названа диференціалом змінної x. Вона описує зміну x^* по заданому значенні x та значенню dx із співвідношення $x^* = x \oplus dx$. Якщо згадати, що функція додавання по модулю 2 фактично представляє собою нерівнозначність, то для k -значних змінних згадане співвідношення матиме вигляд:

$$_k x^* = {}_k x \ominus {}_k dx$$

Значення $_k dx \in \{1, 2, \cdots, k-1\}$ описує величину і факт зміни $_k x$, а $_k dx = 0$, подібно до булевих змінних, описує незмінність значення $_k x$. Для логіко-часових функцій можна записати $t^* = t + dt$ і відповідно, для загального випадку, маємо диференціал по часі ЛЧФ $_k z(t)$:

$$_k dz(t) = {}_k z(t) \ominus {}_k z(t+dt).$$

Для $dt = \Delta = 1$ отримаємо

$$\left[dz(t) = z(t) \ominus z(t+\Delta) = z(t) \ominus z(t+1)\right];$$

$$dz(t) = z(t) \ominus Dz(t).$$

Схему нерівнозначності синтезовано на двійкових логічних елементах з використання двійкового кодування: «0» – 00, «1» – 01 та «2» – 10 (див. рис. 4). Вхід «А» стробуючий.

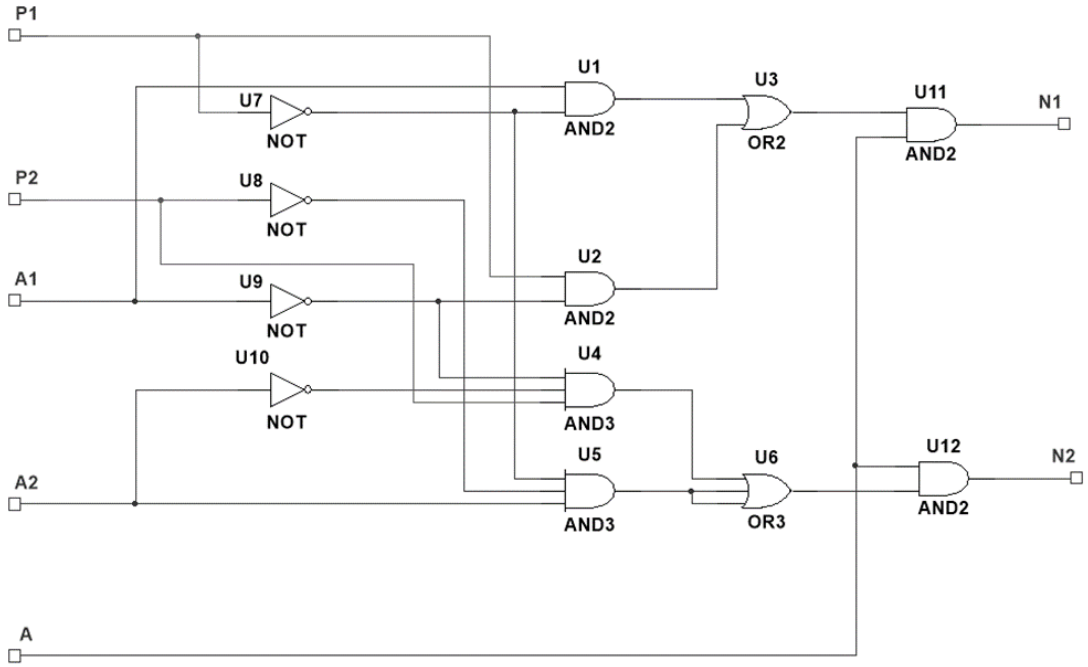


Рисунок 4 − Схема реалізації операції нерівнозначності

Висновки

1. Розглянуто одну з важливих операцій – операцію нерівнозначності, яка дозволить, в подальшому, ввести більш складні операції над БЛЧФ, такі як похідна та первісна.

2. Розглянуто окремі властивості операції нерівнозначності та показано, що для ЛЧФ двійкової логіки дана операція співпадає з сумую по модулю два, що дозволить створювати схемотехнічні варіанти реалізації математичних операцій в логіко-часовому середовищі на двійкових елементах.

3. Продемонстровано можливість використання нерівнозначності при побудові індикаторних операцій та диференціала змінної.

4. Змодельовано схему реалізації операції нерівнозначності.

5. Для кращого приховування інформації та її захисту від модифікацій, підробки або викривлення, операція нерівнозначності дозволить здійснювати кодування та шифрування інформації в логіко-часовому середовищі, створювати графічні паролі, будувати крипто-ключі і т ін.

Список літератури

[1] Н. В. Сачанюк-Кавецька, В. П. Кожем'яко, *Елементи око-процесорної обробки зображень в логіко-часовому середовищі. Монографія*. Вінниця, Україна: УНІВЕРСУМ, 2004, 135 с.

[2] Н. В. Сачанюк-Кавецька, О. П. Прозор, "Елементи математичного опису логіко-часових функцій багатозначної логіки та окремих операцій над ними," *Інформаційні технології та комп`ютерна інженерія*, том 53 (№ 1), с. 111-118. 2022.

[3] Н. В Сачанюк-Кавецька, "Кодування як засіб захисту інформації у системах контролю доступу з використанням логіко-часових функцій у формі поліномів і біометричних даних суб'єктів," *Реєстрація, зберігання і обробка даних. – Інститут проблем реєстрації інформації НАН України*, том 20, № 2, с. 60-68. 2018.

[4] D. Bochmann, C. Posthoff, *Binare dinamische systeme*. Akademie-Verlag, Berlin, 1981, 400 p.

Стаття надійшла 04.04.2022.

References

[1] N. V. Sachaniuk-Kavetska, V. P. Kozhemiako, *Elementy oko-protsesornoi obrobky zobrazhen v lohiko-chasovomu seredovyshchi. Monohrafiia*. Vinnytsia, Ukraina: UNIVERSUM, 2004, 135 s. [in Ukrainian].

[2] N. V. Sachaniuk-Kavetska, O. P. Prozor, "Mathematical description of logic-time functions of multiple-valued logic and some operations over them," *Information technology and computer engineering*, tom 53 (№ 1), pp. 111-118. 2022 [in Ukrainian].

[3] N. V Sachaniuk-Kavetska, "Koduvannia yak zasib zakhystu informatsii u systemakh kontroliu dostupu z vykorystanniam lohiko-chasovykh funktsii u formi polinomiv i biometrychnykh danykh subiektiv," *Reyestratsiia, zberihannia i obrobka danykh. – Instytut problem reiestratsii informatsii NAN Ukrainy*, tom 20, № 2, pp. 60-68. 2018 [in Ukrainian].

[4] D. Bochmann, C. Posthoff, *Binare dinamische systeme*. Akademie-Verlag, Berlin, 1981, 400 p.

Відомості про авторів

Сачанюк-Кавецька Наталія Василівна − кандидат технічних наук, доцент, доцент кафедри вищої математики.

Прозор Олена Петрівна − кандидат педагогічних наук, доцент, доцент кафедри вищої математики.

Хом'юк Віктор Вікторович − кандидат технічних наук, доцент, доцент кафедри вищої математики.

Бондаренко Ірина Олексіївна − кафедра менеджменту безпеки інформаційних систем.

N. Sachaniuk-Kavets'ka, O. Prozor, V. Khomyuk, I. Bondarenko

MATHEMATICAL DESCRIPTION OF THE INEQUALITY OPERATION IN A LOGIC-TIME ENVIRONMENT

Vinnytsia National Technical University, Vinnytsia

ДО ВІДОМА АВТОРІВ

Найновіші правила оформлення і подання статей знаходяться на сайті журналу
http://itce.vntu.edu.ua/