Аналіз множини операцій, синтезованих на основі додавання за модулем два

Бабенко В.Г.[1], Лада Н.В.[2], Лада С.В.[3]

[1]Доц., к.т.н., доцент кафедри інформаційної безпеки та комп'ютерної інженерії, Черкаський державний технологічний університет
бул. Шевченка, 460, м. Черкаси, Україна, zolot_verba@rambler.ru
[2]Аспірант, Черкаський державний технологічний університет
бул. Шевченка, 460, м. Черкаси, Україна, LadaHatali256@gmail.com
[3]Аспірант, Черкаський національний університет ім. Б. Хмельницького
бул. Шевченка, 81, м. Черкаси, Україна, raphaello1986@gmail.com

***Анотація* — Проведено аналіз множини операцій синтезованих на основі додавання за модулем два з точністю до перестановки відносно властивості комутативності. Визначено комутативні пари та групи комутативних операцій. Проведено дослідження визначених груп операцій з метою встановлення взаємозв'язків між групами та операндами. Виявлені міжгрупові та міжоперандні взаємозв'язки дозволяють використовувати операції для прямого та оберненого перетворення інформації.**

Ключові слова: операція, група, перестановка, додрвання за модулем два, комутативність.

Analysis of set of operations synthesized on the basis of the addition modulo two

Babenko V.G.[1], Lada N.V.[2], Lada S.V.[3]

[1]Associate professor, Ph.D., associate professor of Department of Information Security and Computer Engineering, Cherkasy State Technological University
Shevchenko blv., 460, Cherkasy, Ukraine, zolot_verba@rambler.ru
[2]Postgraduate student, Cherkasy State Technological University
Shevchenko blvd., 460, Cherkasy, Ukraine, LadaHatali256@gmail.com
[3]Postgraduate student, The Bohdan Khmelnytsky National University of Cherkasy
Shevchenko blvd., 81, Cherkasy, Ukraine, raphaello1986@gmail.com

***Abstract* — The analysis of the set of operations synthesized on the basis of the addition modulo two up to a permutation concerning the properties of commutativity. Defined commutative pairs and groups of commutative operations. The study of specific groups operations, to determine the relationships between groups and operands. Detected between operand and intergroup relationships allow you to use operation for straight and reverse transformation information.**

Keywords: operation, group, permutation, the addition modulo two, commutativity.

ВСТУП

Однією з базових операцій функцій перетворення даних в криптографічних алгоритмах є додавання за модулем два та перестановка. Тому проведення синтезу та дослідження множини операцій криптографічного додавання за модулем два з точністю до перестановки з метою виявлення груп операцій, які можуть бути застосовані в якості операції криптографічного додавання за модулем два може бути одним із шляхів вдосконалення функцій криптоперетворення. Адже виявлені додаткові операції, що можуть застосовуватися для криптографічного перетворення даних, дозволять розширити кількість операцій, що застосовуються у блокових та потокових шифрах.

МНОЖИНА ОПЕРАЦІЙ ДОДАВАННЯ ЗА МОДУЛЕМ ДВА З ТОЧНІСТЮ ДО ПЕРЕСТАНОВКИ ОПЕРАНДІВ ТА ВИЗНАЧЕННЯ КОМУТАТИВНИХ ГРУП ОПЕРАЦІЙ

Повна множина операцій синтезованих на основі додавання за модулем два $O_1^{\oplus} - O_{24}^{\oplus}$ з точністю до перестановки операндів наведена в табл. 1. Так як представлені операції можуть розглядатися як одна операція з точністю до перестановки даних, то вони повинні зберігати всі властивості операції двохрозрядного додавання за модулем два [1].

Розглянемо можливість використання даних операцій в криптографічних перетвореннях. Однією з властивостей операції двохрозрядного криптографічного додавання за модулем два є комутативність.

Так як операція двохрозрядного криптографічного додавання за модулем два є

базовою для багатьох функцій перетворення криптографічних алгоритмів, то можемо допустити, що її можливо замінити на будь-яку іншу операцію із тих, що отримані в результаті синтезу повної множини операцій (табл. 1) [2]. Перевіримо, чи можливо використати ще якісь операції для криптоперетворення наведені в табл. 1.

При проведенні досліджень синтезованої множини операцій було встановлено, що операції даної множини утворюють з 6 операціями комутативні пари, тому їх можна поділити на 6 груп. Так як результат застосування операцій в групі, буде однаковий, то приходимо до припущення, що достатньо для дослідження всіх операцій із синтезованої множини, що можуть бути використані для криптографічного перетворення на основі додавання за модулем два з точністю до перестановки дослідити лише 6 операцій.

В табл. 1 наведено 6 груп операцій, що утворюють комутативні пари операцій.

Таблиця 1 – Комутативні пари операцій

Відповідні пари операцій		
$O_1^{\oplus} = \begin{vmatrix} x_1 \oplus y_1 \\ x_2 \oplus y_2 \end{vmatrix} \cong O_{10}^{\oplus} = \begin{vmatrix} x_1 \oplus y \\ y_2 \oplus x \end{vmatrix}$	$O_1^{\oplus} = \begin{vmatrix} x_1 \oplus y_1 \\ x_2 \oplus y_2 \end{vmatrix} \cong O_{13}^{\oplus} = \begin{vmatrix} y_1 \oplus x_1 \\ x_2 \oplus y_2 \end{vmatrix}$	$O_1^{\oplus} = \begin{vmatrix} x_1 \oplus y_1 \\ x_2 \oplus y_2 \end{vmatrix} \cong O_{21}^{\oplus} = \begin{vmatrix} y_1 \oplus x_1 \\ y_2 \oplus x_2 \end{vmatrix}$
$O_2^{\oplus} = \begin{vmatrix} x_1 \oplus y_2 \\ x_2 \oplus y_1 \end{vmatrix} \cong O_6^{\oplus} = \begin{vmatrix} x_1 \oplus y_2 \\ y_1 \oplus x_2 \end{vmatrix}$	$O_2^{\oplus} = \begin{vmatrix} x_1 \oplus y_2 \\ x_2 \oplus y_1 \end{vmatrix} \cong O_{20}^{\oplus} = \begin{vmatrix} y_2 \oplus x_1 \\ x_2 \oplus y_1 \end{vmatrix}$	$O_2^{\oplus} = \begin{vmatrix} x_1 \oplus y_2 \\ x_2 \oplus y_1 \end{vmatrix} \cong O_{23}^{\oplus} = \begin{vmatrix} y_2 \oplus x_1 \\ y_1 \oplus x_2 \end{vmatrix}$
$O_3^{\oplus} = \begin{vmatrix} x_2 \oplus y_1 \\ x_1 \oplus y_2 \end{vmatrix} \cong O_7^{\oplus} = \begin{vmatrix} y_1 \oplus x_2 \\ x_1 \oplus y_2 \end{vmatrix}$	$O_3^{\oplus} = \begin{vmatrix} x_2 \oplus y_1 \\ x_1 \oplus y_2 \end{vmatrix} \cong O_{18}^{\oplus} = \begin{vmatrix} x_2 \oplus y_1 \\ y_2 \oplus x_1 \end{vmatrix}$	$O_3^{\oplus} = \begin{vmatrix} x_2 \oplus y_1 \\ x_1 \oplus y_2 \end{vmatrix} \cong O_{22}^{\oplus} = \begin{vmatrix} y_1 \oplus x_2 \\ y_2 \oplus x_1 \end{vmatrix}$
$O_4^{\oplus} = \begin{vmatrix} x_2 \oplus y_2 \\ x_1 \oplus y_1 \end{vmatrix} \cong O_{11}^{\oplus} = \begin{vmatrix} y_2 \oplus x \\ x_1 \oplus y \end{vmatrix}$	$O_4^{\oplus} = \begin{vmatrix} x_2 \oplus y_2 \\ x_1 \oplus y_1 \end{vmatrix} \cong O_{16}^{\oplus} = \begin{vmatrix} x_2 \oplus y_2 \\ y_1 \oplus x_1 \end{vmatrix}$	$O_4^{\oplus} = \begin{vmatrix} x_2 \oplus y_2 \\ x_1 \oplus y_1 \end{vmatrix} \cong O_{24}^{\oplus} = \begin{vmatrix} y_2 \oplus x_2 \\ y_1 \oplus x_1 \end{vmatrix}$
$O_5^{\oplus} = \begin{vmatrix} x_1 \oplus x_2 \\ y_1 \oplus y_2 \end{vmatrix} \cong O_9^{\oplus} = \begin{vmatrix} x_1 \oplus x \\ y_2 \oplus y \end{vmatrix}$	$O_5^{\oplus} = \begin{vmatrix} x_1 \oplus x_2 \\ y_1 \oplus y_2 \end{vmatrix} \cong O_{15}^{\oplus} = \begin{vmatrix} x_2 \oplus x_1 \\ y_1 \oplus y_2 \end{vmatrix}$	$O_5^{\oplus} = \begin{vmatrix} x_1 \oplus x_2 \\ y_1 \oplus y_2 \end{vmatrix} \cong O_{17}^{\oplus} = \begin{vmatrix} x_2 \oplus x_1 \\ y_2 \oplus y_1 \end{vmatrix}$
$O_8^{\oplus} = \begin{vmatrix} y_1 \oplus y_2 \\ x_1 \oplus x_2 \end{vmatrix} \cong O_{12}^{\oplus} = \begin{vmatrix} y_2 \oplus y \\ x_1 \oplus x \end{vmatrix}$	$O_8^{\oplus} = \begin{vmatrix} y_1 \oplus y_2 \\ x_1 \oplus x_2 \end{vmatrix} \cong O_{14}^{\oplus} = \begin{vmatrix} y_1 \oplus y_2 \\ x_2 \oplus x_1 \end{vmatrix}$	$O_8^{\oplus} = \begin{vmatrix} y_1 \oplus y_2 \\ x_1 \oplus x_2 \end{vmatrix} \cong O_{19}^{\oplus} = \begin{vmatrix} y_2 \oplus y_1 \\ x_2 \oplus x_1 \end{vmatrix}$

ВСТАНОВЛЕННЯ ВЗАЄМОЗВ'ЯЗКІВ МІЖ ГРУПАМИ ТА ОПЕРАНДАМИ СИНТЕЗОВАНИХ ОПЕРАЦІЙ

Розглянемо більш детально отримані групи операцій та проведемо їх класифікацію.

До першої групи належать операції:

$$O_1^{\oplus} = \begin{vmatrix} x_1 \oplus y_1 \\ x_2 \oplus y_2 \end{vmatrix}, \quad O_{10}^{\oplus} = \begin{vmatrix} x_1 \oplus y_1 \\ y_2 \oplus x_2 \end{vmatrix},$$

$$O_{13}^{\oplus} = \begin{vmatrix} y_1 \oplus x_1 \\ x_2 \oplus y_2 \end{vmatrix}, \quad O_{21}^{\oplus} = \begin{vmatrix} y_1 \oplus x_1 \\ y_2 \oplus x_2 \end{vmatrix}.$$

Особливістю даної групи операцій є те, що в них немає перестановок між x_1 і x_2 та між y_1 і y_2 відносно базової операції $O_1^{\oplus} = O_{mod\,2}$. Тобто дана група включає в себе операції без перестановок операндів і для групи операцій встановлені взаємозв'язки описуються виконанням умов: якщо $(A)O_1^{\oplus}(B) = C$, то $(A)O_1^{\oplus}(C) = B$, $(B)O_1^{\oplus}(C) = A$, де A, B – операнди, C – результат виконання операції.

Для операцій $O_{10}^{\oplus}$, $O_{13}^{\oplus}$, $O_{21}^{\oplus}$, що належать до тієї ж першої групи операцій, взаємозв'язки описуються аналогічно.

Можна стверджувати, що всі операції групи операцій без перестановок можуть бути використані в криптографічних перетвореннях. Проте з практичної точки зору використання всієї групи операцій недоцільно, тому що вони всі дають один і той же результат криптографічного перетворення.

До другої групи належать операції:

$$O_2^{\oplus} = \begin{vmatrix} x_1 \oplus y_2 \\ x_2 \oplus y_1 \end{vmatrix}, \quad O_6^{\oplus} = \begin{vmatrix} x_1 \oplus y_2 \\ y_1 \oplus x_2 \end{vmatrix},$$

$$O_{20}^{\oplus} = \begin{vmatrix} y_2 \oplus x_1 \\ x_2 \oplus y_1 \end{vmatrix}, \quad O_{23}^{\oplus} = \begin{vmatrix} y_2 \oplus x_1 \\ y_1 \oplus x_2 \end{vmatrix}.$$

Особливістю даної групи операцій є те, що в них немає перестановок розрядів першого операнда (перестановкок між x_1 і x_2), та присутня перестановка розрядів другого операнда (перестановка між y_1 і y_2) відносно базової операції $O_1^{\oplus} = O_{mod\,2}$.

Взаємозв'язки операцій в даній групі характеризуються визначеними особливостями:

Якщо $(A)O_2^{\oplus}(B) = C$, то $(A)O_2^{\oplus}(C) \neq B$, $(B)O_2^{\oplus}(C) \neq A$.

Проте, якщо $(A)O_2^{\oplus}(B) = C$, то $(A)O_3^{\oplus}(C) = B$, $(B)O_3^{\oplus}(C) = A$, $(C)O_3^{\oplus}(A) \neq B$, $(C)O_3^{\oplus}(B) \neq A$.

Якщо $(A)O_6^{\oplus}(B) = C$, то $(A)O_6^{\oplus}(C) \neq B$, $(B)O_6^{\oplus}(C) \neq A$.

Проте, якщо $(A)O_6^{\oplus}(B) = C$, то $(A)O_3^{\oplus}(C) = B$, $(B)O_3^{\oplus}(C) = A$, $(C)O_3^{\oplus}(A) \neq B$, $(C)O_3^{\oplus}(B) \neq A$.

Якщо $(A)O_{20}^{\oplus}(B) = C$, то $(A)O_{20}^{\oplus}(C) \neq B$, $(B)O_{20}^{\oplus}(C) \neq A$.

Проте, якщо $(A)O_{20}^{\oplus}(B) = C$, то $(A)O_3^{\oplus}(C) = B$, $(B)O_3^{\oplus}(C) = A$, $(C)O_3^{\oplus}(A) \neq B$, $(C)O_3^{\oplus}(B) \neq A$.

Якщо $(A)O_{23}^{\oplus}(B) = C$, то $(A)O_{23}^{\oplus}(C) \neq B$, $(B)O_{23}^{\oplus}(C) \neq A$.

Проте, якщо $(A)O_{23}^{\oplus}(B) = C$, то $(A)O_3^{\oplus}(C) = B$, $(B)O_3^{\oplus}(C) = A$, $(C)O_3^{\oplus}(A) \neq B$, $(C)O_3^{\oplus}(B) \neq A$.

Можна стверджувати, що всі операції групи операцій з перестановкою розрядів другого операнда, можуть бути використані в криптографічних перетвореннях лише в поєднанні з іншими групами операцій, так як вони виявилися несиметричними. Можливість використання операцій даної групи потребує проведення додаткового дослідження.

До третьої групи належать операції:

$$O_3^{\oplus} = \begin{vmatrix} x_2 \oplus y_1 \\ x_1 \oplus y_2 \end{vmatrix}, \quad O_7^{\oplus} = \begin{vmatrix} y_1 \oplus x_2 \\ x_1 \oplus y_2 \end{vmatrix},$$

$$O_{18}^{\oplus} = \begin{vmatrix} x_2 \oplus y_1 \\ y_2 \oplus x_1 \end{vmatrix}, \quad O_{22}^{\oplus} = \begin{vmatrix} y_1 \oplus x_2 \\ y_2 \oplus x_1 \end{vmatrix}.$$

Особливістю даної групи операцій є те, що в них немає перестановок розрядів другого операнда (перестановкок між y_1 і y_2) та присутня перестановка розрядів першого операнда (перестановка між x_1 і x_2), відносно базової операції $O_1^{\oplus} = O_{mod\,2}$.

Взаємозв'язки операцій в даній групі, що включає в себе операції перестановки розрядів першого операнда, характеризуються визначеними особливостями:

Якщо $(A)O_3^{\oplus}(B) = C$, то $(A)O_3^{\oplus}(C) \neq B$, $(B)O_3^{\oplus}(C) \neq A$.

Проте, якщо $(A)O_3^{\oplus}(B) = C$, то $(A)O_2^{\oplus}(C) = B$, $(B)O_2^{\oplus}(C) = A$, $(C)O_2^{\oplus}(A) \neq B$, $(C)O_2^{\oplus}(B) \neq A$.

Якщо $(A)O_7^{\oplus}(B) = C$, то $(A)O_7^{\oplus}(C) \neq B$, $(B)O_7^{\oplus}(C) \neq A$.

Проте, якщо $(A)O_7^{\oplus}(B) = C$, то $(A)O_2^{\oplus}(C) = B$, $(B)O_2^{\oplus}(C) = A$, $(C)O_2^{\oplus}(A) \neq B$, $(C)O_2^{\oplus}(B) \neq A$.

Якщо $(A)O_{18}^{\oplus}(B) = C$, то $(A)O_{18}^{\oplus}(C) \neq B$, $(B)O_{18}^{\oplus}(C) \neq A$.

Проте, якщо $(A)O_{18}^{\oplus}(B) = C$, то $(A)O_2^{\oplus}(C) = B$, $(B)O_2^{\oplus}(C) = A$, $(C)O_2^{\oplus}(A) \neq B$, $(C)O_2^{\oplus}(B) \neq A$.

Якщо $(A)O_{22}^{\oplus}(B) = C$, то $(A)O_{22}^{\oplus}(C) \neq B$, $(B)O_{22}^{\oplus}(C) \neq A$.

Проте, якщо $(A)O_{22}^{\oplus}(B) = C$, то $(A)O_2^{\oplus}(C) = B$, $(B)O_2^{\oplus}(C) = A$, $(C)O_2^{\oplus}(A) \neq B$, $(C)O_2^{\oplus}(B) \neq A$.

Можна стверджувати, що всі операції третьої групи можуть бути використані в криптографічних перетвореннях лише в поєднанні з іншими групами операцій, так як вони виявилися несиметричними. Можливість використання операцій даної групи також потребує проведення додаткового дослідження.

До четвертої групи належать операції:

$$O_4^{\oplus} = \begin{vmatrix} x_2 \oplus y_2 \\ x_1 \oplus y_1 \end{vmatrix}, \quad O_{11}^{\oplus} = \begin{vmatrix} y_2 \oplus x_2 \\ x_1 \oplus y_1 \end{vmatrix},$$

$$O_{16}^{\oplus} = \begin{vmatrix} x_2 \oplus y_2 \\ y_1 \oplus x_1 \end{vmatrix}, \quad O_{24}^{\oplus} = \begin{vmatrix} y_2 \oplus x_2 \\ y_1 \oplus x_1 \end{vmatrix}.$$

Особливістю даної групи операцій є те, що в них присутня перестановка розрядів як першого операнда (перестановка між x_1 і x_2) так і перестановка розрядів другого операнда (перестановка між y_1 і y_2) відносно базової операції $O_1^{\oplus} = O_{mod\,2}$. Група, що включає в себе операції перестановки розрядів першого та другого операнда, описується взаємозв'язками операцій:

Якщо $(A)O_4^{\oplus}(B) = C$, то $(A)O_4^{\oplus}(C) \neq B$, $(B)O_4^{\oplus}(C) \neq A$.

Проте, якщо $(A)O_4^{\oplus}(B) = C$, то $(A)O_2^{\oplus}(C) = B$, $(C)O_3^{\oplus}(A) = B$, $(B)O_2^{\oplus}(C) = A$, $(C)O_3^{\oplus}(B) = A$.

Якщо $(A)O_{11}^{\oplus}(B) = C$, то $(A)O_{11}^{\oplus}(C) \neq B$, $(B)O_{11}^{\oplus}(C) \neq A$.

Проте, якщо $(A)O_{11}^{\oplus}(B) = C$, то $(A)O_2^{\oplus}(C) = B$, $(C)O_3^{\oplus}(A) = B$, $(B)O_2^{\oplus}(C) = A$, $(C)O_3^{\oplus}(B) = A$.

Якщо $(A)O_{16}^{\oplus}(B) = C$, то $(A)O_{16}^{\oplus}(C) \neq B$, $(B)O_{16}^{\oplus}(C) \neq A$.

Проте, якщо $(A)O_{16}^{\oplus}(B) = C$, то $(A)O_2^{\oplus}(C) = B$, $(C)O_3^{\oplus}(A) = B$, $(B)O_2^{\oplus}(C) = A$, $(C)O_3^{\oplus}(B) = A$.

Якщо $(A)O_{24}^{\oplus}(B) = C$, то $(A)O_{24}^{\oplus}(C) \neq B$, $(B)O_{24}^{\oplus}(C) \neq A$.

Проте, якщо $(A)O_{24}^{\oplus}(B) = C$, то $(A)O_2^{\oplus}(C) = B$, $(C)O_3^{\oplus}(A) = B$, $(B)O_2^{\oplus}(C) = A$, $(C)O_3^{\oplus}(B) = A$.

Можна стверджувати, що всі операції групи операцій з перестановкою розрядів як першого (перестановка між x_1 і x_2) так і другого операндів (перестановок між y_1 і y_2) відносно базової операції $O_1^{\oplus} = O_{mod\,2}$ можуть бути використані в криптографічних перетвореннях. Проте з практичної точки зору використання всієї групи операцій недоцільно, тому що вини всі дають один і той же результат криптографічного перетворення.

Крім того необхідно окремо виділити наступні дві групи операцій. До п'ятої групи належать операції:

$$O_5^{\oplus} = \begin{vmatrix} x_1 \oplus x_2 \\ y_1 \oplus y_2 \end{vmatrix}, \quad O_9^{\oplus} = \begin{vmatrix} x_1 \oplus x_2 \\ y_2 \oplus y_1 \end{vmatrix},$$

$$O_{15}^{\oplus} = \begin{vmatrix} x_2 \oplus x_1 \\ y_1 \oplus y_2 \end{vmatrix}, \quad O_{17}^{\oplus} = \begin{vmatrix} x_2 \oplus x_1 \\ y_2 \oplus y_1 \end{vmatrix}.$$

Слід зазначити, що операції п'ятої групи не придатні для застосування в операціях криптографічного перетворення, тому що їх застосування призведе до втрати інформації, бо для них не існує операції оберненого перетворення.

До шостої групи належать операції:

$$O_8^{\oplus} = \begin{vmatrix} y_1 \oplus y_2 \\ x_1 \oplus x_2 \end{vmatrix}, \quad O_{12}^{\oplus} = \begin{vmatrix} y_2 \oplus y_1 \\ x_1 \oplus x_2 \end{vmatrix},$$

$$O_{14}^{\oplus} = \begin{vmatrix} y_1 \oplus y_2 \\ x_2 \oplus x_1 \end{vmatrix}, \quad O_{19}^{\oplus} = \begin{vmatrix} y_2 \oplus y_1 \\ x_2 \oplus x_1 \end{vmatrix}.$$

Операції шостої групи аналогічно операціям п'ятої групи не придатні для застосування в криптографічних перетвореннях, тому що їх застосування призведе до втрати інформації.

ВИСНОВКИ

Проведений аналіз множини операцій синтезованих на основі додавання за модулем два з точністю до перестановки відносно властивості комутативності дозволив визначити комутативні пари та групи комутативних операцій. Проведено дослідження визначених груп операцій з метою встановлення взаємозв'язків між групами та операндами. На основі визначених особливостей операцій групи виявлено взаємозв'язки між операціями, що дозволить використовувати синтезовані операції для прямого та оберненого перетворення інформації. В результаті аналізу взаємозв'язків операцій групи виявленоно групи, які характеризуються несиметричністю операцій та можуть бути використані в криптографічних перетвореннях лише в поєднанні з іншими групами операцій після проведення додаткового дослідження.

ЛІТЕРАТУРА REFERENCES

[1] V.I. Sushchanskiy, V.S. Sikora. Operations on groups of substitutions. Theory and Application [Text]. M. of Education and Science of Ukraine, Taras Shevchenko National University of Kyiv, Yuriy Fedkovych Chernivtsi. National University. – Chernivtsi: Ruta, 2003. – 255 pp. (in Ukr.).

[2] Babenko V.G., Lada N.V. (2014). Synthesis and analysis of cryptographic operations addition modulo two. Information processing systems, (2(118)), pp. 116-118. (in Ukr.).

[3] Сущанський, Віталій Іванович. Операції на групах підстановок. Теорія та застосування [Текст] / В.І. Сущанський, В.С. Сікора ; М-во освіти і науки України, Київ. нац. ун-т ім. Тараса Шевченка, Чернів. нац. ун-т ім. Ю.Федьковича. - Чернівці : Рута, 2003. - 255 с.

[4] Бабенко В.Г. Синтез і аналіз операцій криптографічного додавання за модулем два / В.Г. Бабенко, Н.В. Лада // Системи обробки інформації: зб. наук. пр. – Харків: ХУПС ім. І. Кожедуба. – 2014. – Вип. 2(118) – С. 116-118.