Науковий вісник НЛТУ України
Scientific Bulletin of UNFU
ISSN 1994-7836 (print)
ISSN 2519-2477 (online)
https://doi.org/10.36930/40350320
Article received 29.04.2025
Article accepted 29.05.2025
UDC 004.8
Correspondence author: B. V. Shtohrinets bohdan.v.shtohrinets@lpnu.ua

І. Г. Цмоць, Б. В. Штогрінець, Т. Б. Мамчур
Національний університет "Львівська політехніка", м. Львів, Україна

ПРОБЛЕМНО-ОРІЄНТОВАНА КРИПТОГРАФІЧНА СИСТЕМА НЕЙРОМЕРЕЖЕВОГО ЗАХИСТУ ДАНИХ

Визначено, що значних техніко-експлуатаційних показників функціонування бортових систем криптографічного захисту даних досягають способом використання проблемно-орієнтованого підходу, сучасної елементної бази розроблення нових методів нейромережевого шифрування-дешифрування даних, алгоритмів і спеціалізованих структур для реалізації нейроподібних елементів. Розроблено метод нейромережевого криптографічного захисту даних, який за рахунок використання нейромереж прямого поширення автоасоціативного типу на підставі парадигми моделі послідовних геометричних перетворень, попереднього обчислення вагових коефіцієнтів та таблично-алгоритмічної реалізації нейроподібних елементів забезпечує високу криптографічну стійкість алгоритму шифрування-дешифрування даних у реальному часі та апаратно-програмну реалізацію з високими техніко-експлуатаційними показниками. Удосконалено таблично-алгоритмічний метод для обчислення скалярного добутку векторів, який за рахунок приведення до найбільшого спільного порядку вагових коефіцієнтів і формування для них таблиць макрочасткових добутків елементів векторів забезпечує швидке оброблення вхідних даних як з фіксованою, так і рухомою комою. Розроблено базову структуру пристрою для таблично-алгоритмічного обчислення скалярного добутку векторів, основними компонентами якого є блоки пам'яті для зберігання макрочасткових добутків елементів векторів, суматор, шинні формувачі та регістри. Використання цієї структури дає змогу скоротити тривалість розроблення пристроїв із заданими параметрами. Розроблено на підставі принципів змінності складу обладнання, модульності, спеціалізації та паралелізму структуру проблемно-орієнтованої системи нейромережевого криптографічного захисту даних, яка за рахунок взаємопоєднання універсального та спеціалізованого підходів, програмних і спеціалізованих апаратних засобів забезпечує ефективну реалізацію алгоритмів шифрування-дешифрування даних у реальному часі. Виконано моделювання спеціалізованих апаратних засобів нейромережевого шифрування даних мовою програмування апаратури VHDL у середовищі розроблення Quartus II вер. 13.1 з використанням FPGA EP3C16F484C6 сімейства Cyclone III та визначено, що тривалість шифрування одного вектора вхідних даних становить приблизно 160 нс, а для їх реалізації необхідно 3053 логічних елементів і 745 регістрів.

Ключові слова: шифрування; дешифрування; скалярний добуток; таблично-алгоритмічний метод; обчислювальні нейромережі; адаптивне програмно-апаратне середовище; реальний час.

Вступ / Introduction

За управління безпілотними літальними апаратами та наземними мобільними робототехнічними платформами (МРП) важливою проблемою є забезпечення криптографічного захисту передачі даних [4, 9]. Вирішення такої проблеми потребує розроблення методів нейромережевого криптографічного захисту даних, які орієнтовані на використання у бортових систем [15]. Під час розроблення бортових систем криптографічного захисту даних необхідно забезпечити режим реального часу, підвищити криптостійкість та зменшити масу, габарити, енергоспоживання та вартість. Одним із способів забезпечення таких вимог є використання автоасоціативної нейромережі прямого поширення, яка навчається на підставі методу головних компонент. Особливістю таких нейромереж є можливість наперед обчислити вагові коефіцієнти, використати таблично-алгоритмічний метод для реалізації нейроподібних елементів з використанням базису елементарних арифметичних операцій. Для нейромережевого шифрування та дешифрування даних пропонують використати симетричні ключі, які містять коди маскування, архітектуру нейромережі та матриці вагових коефіцієнтів.

Високих техніко-економічних показників бортових систем криптографічного захисту даних досягають способом використання проблемно-орієнтованого підходу, сучасної елементної бази (мікроконтролерів, програмованих логічних інтегральних схем (ПЛІС) типу FPGA), розроблення нових методів, алгоритмів і структур [8, 10]. Реалізація бортових систем криптографічного захисту на підставі проблемно-орієнтованого підходу пе-

Інформація про авторів:
Цмоць Іван Григорович, д-р техн. наук, професор, кафедра автоматизованих систем управління.
Email: ivan.h.tsmots@lpnu.ua; https://orcid.org/0000-0002-4033-8618
Штогрінець Богдан Володимирович, аспірант, кафедра автоматизованих систем управління.
Email: bohdan.v.shtohrinets@lpnu.ua; https://orcid.org/0009-0001-4956-3862
Мамчур Тарас Борисович, аспірант, кафедра автоматизованих систем управління.
Email: taras.b.mamchur@lpnu.ua; https://orcid.org/0009-0006-0593-7937
Цитування за ДСТУ: Цмоць І. Г., Штогрінець Б. В., Мамчур Т. Б. Проблемно-орієнтована криптографічна система нейромережевого захисту даних. Науковий вісник НЛТУ України. 2025, т. 35, № 3. С. 183–192.
Citation APA: Tsmots, I. H., Shtohrinets, B. V., & Mamchur, T. B. (2025). Problem-oriented cryptographic system for neural network-based data protection. *Scientific Bulletin of UNFU*, 35(3), 183–192. https://doi.org/10.36930/40350320

редбачає використання універсального процесорного ядра, доповненого спеціалізованими апаратними засобами, які реалізують нейроподібні елементи. Поєднання універсальних і спеціалізованих, програмних та апаратних засобів забезпечить створення малогабаритних систем нейромережевого криптографічного захисту даних у реальному часі зі швидкою зміною ключів шифрування та дешифрування даних.

Нейромережевого криптографічного шифрування та дешифрування даних у реальному часі досягають унаслідок використання розпаралелення процесів шифрування та дешифрування даних, апаратної реалізації нейроподібних елементів на базі багатооперандного підходу і макрочасткових таблиць.

Тому актуальною проблемою є розроблення методу та проблемно-орієнтованої системи нейромережевого криптографічного захисту даних з високими технікоексплуатаційними параметрами.

Об'єкт дослідження – розроблення проблемно-орієнтованої системи криптографічного захисту даних.

Предмет дослідження – методи та засоби розроблення проблемно-орієнтованої системи нейромережевого криптографічного захисту даних у реальному часі, що базуються на таблично-алгоритмічному обчисленні скалярного добутку векторів з урахуванням впливу вхідних параметрів і забезпечують підвищену швидкодію та криптографічну стійкість системи.

Мета роботи – розробити проблемно-орієнтовану систему нейромережевого криптографічного захисту даних у реальному часі, що забезпечує підвищену швидкодію та криптографічну стійкість.

Для досягнення зазначеної мети визначено такі основні *завдання дослідження*:

- розробити метод криптографічного захисту даних із використанням нейромереж прямого поширення автоасоціативного типу на підставі парадигми послідовних геометричних перетворень, застосування якого забезпечить ефективну таблично-алгоритмічну реалізацію нейроподібних елементів.
- удосконалити таблично-алгоритмічний метод обчислення скалярного добутку векторів способом використання вагових коефіцієнтів у форматі з плавучою комою, що дасть змогу підвищити точність обчислень, забезпечити гнучкість адаптації до різнорідних типів вхідних даних та зменшити кількість помилок заокруглення під час оброблення їхніх великих масивів з реальними значеннями.
- розробити базову структуру таблично-алгоритмічного пристрою обчислення скалярного добутку векторів, використання якого забезпечує зменшення тривалості його розроблення зі заданими параметрами.
- розробити структуру проблемно-орієнтованої системи нейромережевого криптографічного захисту даних, яка забезпечить можливість вибору архітектури нейромережі, зміни маски та таблиць макрочасткових добутків елементів векторів;
- реалізувати спеціалізовані апаратні засоби нейромережевого шифрування даних на базі напівпровідникового пристрою FPGA (англ. *Field-Programmable Gate Array*), що забезпечить високошвидкісне паралельне виконання операцій шифрування з мінімальними затримками, підвищену стійкість до криптоаналітичних атак завдяки використанню нелінійних функцій активації та адаптивної структури нейромережі, а також можливість гнучкого перепрограмування алгоритмів відповідно до вимог безпеки.

Аналіз останніх досліджень та публікацій. Проаналізувавши основні тенденції розвитку бортових систем криптографічного захисту даних у реальному часі, з'ясовано, що для виконання шифрування та дешифрування даних у таких системах дедалі більше використовують нейромережеві методи [4, 9, 15]. Проаналізувавши публікації [18, 28], встановлено, що реалізація нейромережевих методів криптографічного захисту даних переважно виконується програмним способом. Основним недоліком програмної реалізації нейромережевого криптографічного захисту даних є складність забезпечення режиму реального часу та обмежень, які висуваються до бортових систем щодо маси, габаритів, енергоспоживання та вартості.

У роботах [2, 29] розглянуто способи адаптації автоасоціативної нейронної мережі з неітераційним навчанням до задач криптографічного захисту даних. Особливістю функціонування такої нейромережі є можливість попереднього обчислення вагових коефіцієнтів унаслідок її навчання на підставі методу головних компонент. Цей метод використовує систему власних векторів, які відповідають власним значенням коваріаційної матриці вхідних даних [19]. Автоасоціативна нейромережа з наперед обчисленими ваговими коефіцієнтами використовується для шифрування та дешифрування даних. У роботі [12, 26] показано, що ключем за нейромережевого криптографічного шифрування та дешифрування даних є коди маскування, архітектура нейромережі та матриці вагових коефіцієнтів.

Проаналізувавши публікації [21, 25] з апаратної реалізації нейромереж, з'ясовано, що їх основою є нейроелементи. Особливістю таких нейроелементів є те, що кількість входів і їх розрядність визначається архітектурою нейромережі, яка є однією із характеристик ключа шифрування даних. Основною операцією реалізації нейроелемента є обчислення скалярного добутку з використанням попередньо обчислених вагових коефіцієнтів.

У роботах [11, 20, 23] розглянуто методи обчислення скалярного добутку з використанням базису елементарних арифметичних операцій – додавання та зсуву. Особливістю цих методів є формування макрочасткових добутків елементів векторів і їх додавання або зсуву до раніше накопиченої суми. Апаратна реалізація таких методів потребує значних затрат обладнання. Менших затрат обладнання та меншого часу обчислення потребує реалізація таблично-алгоритмічного методу обчислення скалярного добутку векторів, який зводиться до операцій читання макрочасткових добутків елементів векторів, додавання та зсуву [22, 24]. Недоліком цього методу є те, що він орієнтований на роботу із вхідними даними та ваговими коефіцієнтами у форматі з фіксованою комою.

З аналізу робіт [7, 17] видно, що нейромережеві засоби криптографічного симетричного шифрування та дешифрування даних реалізуються на базі мікропроцесорів, доповнених апаратними засобами, які реалізують часомісткі обчислювальні операції з використанням ПЛІС (програмована логічна інтегральна схема, англ. *Programmable Logic Device*, PLD). Високої швидкодії нейромережевих засобів криптографічного шифрування та дешифрування даних досягають за рахунок розпаралелювання, конвеєризації обчислювальних процесів і апаратної реалізації нейроелементів [5, 16]. Недоліком наявних нейромережевих засобів криптографічного захисту даних є складність швидкої зміни ключів шифрування та дешифрування.

Попри наявність великої кількості досліджень у сфері нейромережевого криптографічного захисту даних, у науковій літературі досі відсутні комплексні рішення, що передбачають апаратно-програмну реалізацію проблемно-орієнтованих систем шифрування та дешифрування з використанням автоасоціативних нейромереж прямого поширення та таблично-алгоритмічного методу обчислення скалярного добутку у форматах із фіксованою та плавучою комою. Це зумовлює актуальність розроблення нового методу криптографічного захисту, який поєднує переваги структурної оптимізації нейроподібних елементів, адаптивності до вхідних параметрів і можливості реалізації в режимі реального часу із забезпеченням високої швидкодії та техніко-експлуатаційної ефективності.

Результати дослідження та їх обговорення / Research results and their discussion

Метод нейромережевого криптографічного захисту даних. За управління рухом МРП у середовищі з динамічною зміною ситуації важливим завданням є забезпечення криптографічного захисту передачі даних. Системи криптографічного захисту даних у МРП повинні забезпечувати шифрування та дешифрування даних у реальному часі. Одним із способів забезпечення таких вимог є використання нейромереж прямого поширення автоасоціативного типу на підставі парадигми моделі послідовних геометричних перетворень. Особливістю таких нейромереж є можливість наперед обчислити вагові коефіцієнти, що дасть змогу використати таблично-алгоритмічний метод для реалізації нейроподібних елементів.

Під час використання методу нейромережевого криптографічного захисту шифрування даних відбувається над відкритим текстом з використанням ключа, який складається із заданої кількості нейронів N, матриці вагових коефіцієнтів W_{ji} і операцій маскування. Таке шифрування даних виконується за три кроки: вибір архітектури нейроподібної мережі, обчислення матриці вагових коефіцієнтів і шифрування.

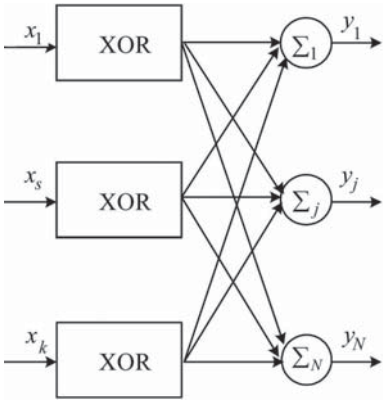

Рис. 1. Архітектура нейроподібної мережі для шифрування даних / Architecture of the neuromorphic network for data encryption

Крок вибору архітектури нейроподібної мережі зводиться до визначення кількості нейроелементів N, кількості входів k і розрядності входів m. Кількість нейронних елементів дорівнює кількості входів, що визначають за такою формулою:

$$N = n / m, \tag{1}$$

де: n – розрядність повідомлення; m – розрядність входів. Вхідні повідомлzення, які потрібно зашифрувати, можуть мати різну розрядність n та ділитися на різну кількість входів k. Від значення розрядності повідомлення n та кількості входів k залежить архітектура нейромережі. Архітектуру нейроподібної мережі, яку використовують для шифрування даних, наведено на рис. 1, де XOR – операція маскування з використанням елементів Виключне АБО, x_s – s-й елемент повідомлення.

На другому кроці обчислюється матриця вагових коефіцієнтів, яка є одним із елементів ключа шифрування:

$$\boldsymbol{W} = \begin{vmatrix} W_{11} & W_{12} & \cdots & W_{1k} \\ W_{21} & W_{22} & \cdots & W_{2k} \\ \vdots & \vdots & \cdots & \vdots \\ W_{N1} & W_{N2} & \cdots & W_{Nk} \end{vmatrix}. \tag{2}$$

Третій крок зводиться до виконання операції XOR маскування вектора вхідних даних $\bar{x}$ та множення матриці вагових коефіцієнтів W на замаскований вектор вхідних даних $\bar{x}_м$ згідно з таким матричним виразом:

$$\boldsymbol{W} \times X = Y \Rightarrow \begin{vmatrix} W_{11} & W_{12} & \cdots & W_{1k} \\ W_{21} & W_{22} & \cdots & W_{2k} \\ \vdots & \vdots & \cdots & \vdots \\ W_{N1} & W_{N2} & \cdots & W_{Nk} \end{vmatrix} \times \begin{vmatrix} x_1 \\ x_2 \\ \vdots \\ x_k \end{vmatrix} = \begin{vmatrix} y_1 \\ y_2 \\ \vdots \\ y_N \end{vmatrix}. \tag{3}$$

Множення матриці вагових коефіцієнтів W на вектор вхідних даних $\bar{x}_м$ зводиться до виконання N операцій обчислення скалярного добутку:

$$y_j = \sum_{s=1}^{k} W_{js} x_s, j = \overline{1,N}, \tag{4}$$

де: k – кількість добутків елементів векторів, s=1,2,…,k, j=1,2,…,N.

Обчислення скалярних добутків елементів векторів будемо виконувати з використанням таблично-алгоритмічного методу, за якого виконується зчитування макрочасткового добутку P_{Mi} з j-тої таблиці за адресою, який відповідає i-му розрядному зрізу N вхідних даних, і його додавання до раніше накопичених сум згідно з формулою:

$$y_{j0} = 0, y_{ji}^{м} = 2^{-1} y_{j(i-1)}^{м} + P_{ji}^{M}, i = \overline{1,k}; j = \overline{1,N}, \tag{5}$$

де m – розрядність вхідних даних. Кількість таблиць макрочасткових добутків елементів векторів відповідає кількості рядків матриці (2), тобто N.

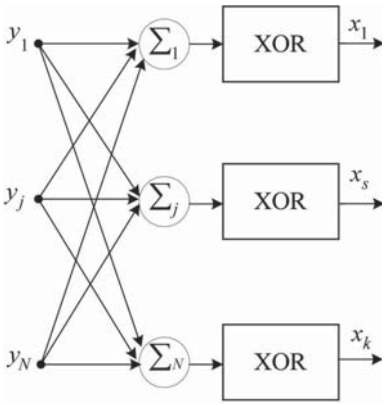

Рис. 2. Архітектура нейроподібної мережі для дешифрування зашифрованих даних / Architecture of the neuromorphic network for encrypted data decryption

За використання методу нейромережевого криптографічного захисту процес дешифрування зашифрованих даних відбувається за три кроки аналогічно до процесу шифрування. На першому кроці вибирається архі-

тектура нейроподібної мережі, яка за кількістю нейроподібних елементів відповідає мережі, яку використовують для шифрування даних. Архітектуру нейроподібної мережі, яку використовують для дешифрування зашифрованих даних, наведено на рис. 2.

На другому кроці обчислюється матриця вагових коефіцієнтів для дешифрування зашифрованих даних. Таке обчислення здійснюється способом транспонування матриці вагових коефіцієнтів для шифрування вхідних даних, а саме:

$$\boldsymbol{W}^T = \begin{vmatrix} W_{11} & W_{12} & \cdots & W_{1k} \\ W_{21} & W_{22} & \cdots & W_{2k} \\ \vdots & \vdots & \cdots & \vdots \\ W_{N1} & W_{N2} & \cdots & W_{Nk} \end{vmatrix}^T .$$

Дешифрування зашифрованих даних здійснюється способом множення матриці вагових коефіцієнтів $\boldsymbol{W}^T$ на вектор зашифрованих даних $\bar{y}$. Результатом такого множення є N скалярних добутків елементів векторів, обчислення яких здійснюється на підставі таблично-алгоритмічного методу. Для отримання результатів дешифрування обчислені скалярні добутки демаскуються способом виконання операції XOR.

Вдосконалення таблично-алгоритмічного методу обчислення скалярного добутку векторів. Базовими компонентами, на підставі яких синтезуються нейроподібні блоки шифрування та дешифрування даних, є пристрої обчислення скалярного добутку векторів:

$$Z = \sum_{j=1}^{N} W_j X_j \cdot \qquad (7)$$

У таких пристроях вагові коефіцієнтами W_j є попередньо обчисленими (константами), а вхідні дані X_j представляться в порозрядному вигляді згідно з такою формулою:

$$X_j = \sum_{i=1}^{n} 2^{-i} X_{ji} , \qquad (8)$$

де: X_{ji} – значення i-х розрядів множника X_j, n – розрядність множників.

Обчислення скалярного добутку векторів у такому разі запишемо так:

$$Z = \sum_{j=1}^{N} W_j X_j = \sum_{i=1}^{n} 2^{-i} \sum_{j=1}^{N} W_j X_{ji} = \sum_{i=1}^{n} 2^{-i} \sum_{j=1}^{N} P_{ji} = \sum_{i=1}^{n} 2^{-i} P_{Mi} , \qquad (9)$$

де: P_{ji} – j,i-ий частковий добуток; P_{Mi} – i-ий макрочастковий добуток, який формується додаванням N часткових добутків елементів вектора P_{ji}, тобто

$$P_{Mi} = \sum_{j=1}^{N} P_{ji} \cdot$$

Особливістю операції обчислення скалярного добутку є те, що вагові коефіцієнти W_j задають у форматі з плавучою комою, а вхідні дані X_j можуть бути як у форматі з фіксованою комою, так і з плавучою комою. Обчислення скалярного добутку будемо виконувати за таблично-алгоритмічним методом. Такий метод ґрунтується на багатооперандному підході, за якого процес обчислення скалярного добутку розглядають як виконання єдиної операції з використанням базису елементарних арифметичних операцій. Базовою операцією таблично-алгоритмічного методу обчислення скалярного добутку є табличне формування i-го макрочасткового добутку P_{Mi} і його додавання до раніше накопичених сум згідно з такою формулою:

$$Z_0 = 0; Z_i = 2^{-1} Z_{i-1} + P_{Mi}, i = \overline{1,n} . \qquad (10)$$

Табличне формування i-го макрочасткового добутку P_{Mi} передбачає приведення вагових коефіцієнтів $W_j = w_j 2^{km_{W_j}}$ (де w_j – мантиса W_j вагового коефіцієнта, k_{W_j} – порядок W_j вагового коефіцієнта) до найбільшого спільного порядку $k_{W\max c}$. Приведення вагових коефіцієнтів W_j до найбільшого спільного порядку $k_{W\max c}$ здійснюють виконанням таких операцій: визначення найбільшого спільного порядку вагових коефіцієнтів $k_{W\max c}$; обчислення різниці порядків для W_j вагового коефіцієнта $\Delta k_{W_j} = k_{W\max c} - k_{W_j}$; зсунення вправо мантиси w_j на різницю порядків Δk_{W_j} і отримання масштабованої мантиси w_j^h.

Таблицю макрочасткових добутків елементів вектора P_{Mi} обчислюють за такою формулою:

$$P_{Mi} = \begin{cases} 0, \quad якщо \quad x_{1i} = x_{2i} = x_{3i} = \ldots = x_{Ni} = 0 \\ w_1^h, \quad якщо \quad x_{1i} = 1, \quad x_{2i} = x_{3i} = \ldots = x_{Ni} = 0 \\ w_2^h, \quad якщо \quad x_{1i} = 0, x_{2i} = 1, x_{3i} = \ldots = x_{Ni} = 0 \\ w_1^h + w_2^h, \quad якщо \quad x_{1i} = 1, x_{2i} = 1, x_{3i} = \ldots = x_{Ni} = 0 \\ \vdots \\ w_2^h + \ldots + w_N^h, \cdots якщо \quad x_{1i} = 0, x_{2i} = x_{3i} = \ldots = x_{Ni} = 1 \\ w_1^h + w_2^h + \ldots + w_N^h, \quad якщо \quad x_{1i} = x_{2i} = x_{3i} = \ldots = x_{Ni} = 1 \end{cases} . \qquad (11)$$

Кількість можливих варіантів макрочасткових добутків елементів вектора P_{Mi} і відповідно обсяг таблиці визначають за формулою

$$Q = 2^N \cdot \qquad (12)$$

Процес обчислення скалярного добутку Z у таблично-алгоритмічних пристроях доцільно здійснювати з молодших розрядів, що забезпечить зменшення розрядності накопичувального суматора. Основними етапами реалізації вдосконаленого таблично-алгоритмічного методу обчислення оператора скалярного добутку є:

- обчислення таблиці всіх можливих макрочасткових результатів P_{Mi};
- запис у пам'ять обчислених значень макрочасткових результатів P_{Mi};
- зчитування макрочасткових результатів P_{Mi} з комірок пам'яті за адресою, яка відповідає значенню розрядних зрізів множників x_{ji};
- підсумовування макрочасткових результатів P_{Mi} із зсувом накопиченої суми вправо на один розряд.

Розроблення базової структури таблично-алгоритмічного пристрою обчислення скалярного добутку векторів. Нейроподібне шифрування та дешифрування даних у реальному часі забезпечується використанням спеціалізованих апаратних пристроїв таблично-алгоритмічного обчислення скалярного добутку векторів. Для розроблення широкого спектра таких пристроїв доцільно розробити базову структуру пристрою таблично-алгоритмічного обчислення скалярного добутку векторів. Базову структуру рекуреного пристрою таблично-алгоритмічного обчислення скалярного добутку з аналізом розрядного зрізу з використанням вагових коефіцієнтів у форматі з плавучою комою, а вхідних даних – у форматі з фіксованою комою, наведено на рис. 3, де Рг – регістр, Ліч A – лічильник адреси, БП – блок пам'яті, См – суматор, Км – комутатор, TI – тактові імпульси, $ШД$ – шина даних, ШФ – шинний формувач, $Зп_P$ – вхід запису макрочасткових добутків елементів

вектора, $Зп_k$ – вхід запису порядку, $У_1$, $У_2$ – входи управління відповідно режимом роботи пам'яті та режимом роботи регістрів вхідних даних, $X_1,\ldots,X_N$ – вхідні дані, $Зп_X$ – вхід запису даних, RS – вхід скиду.

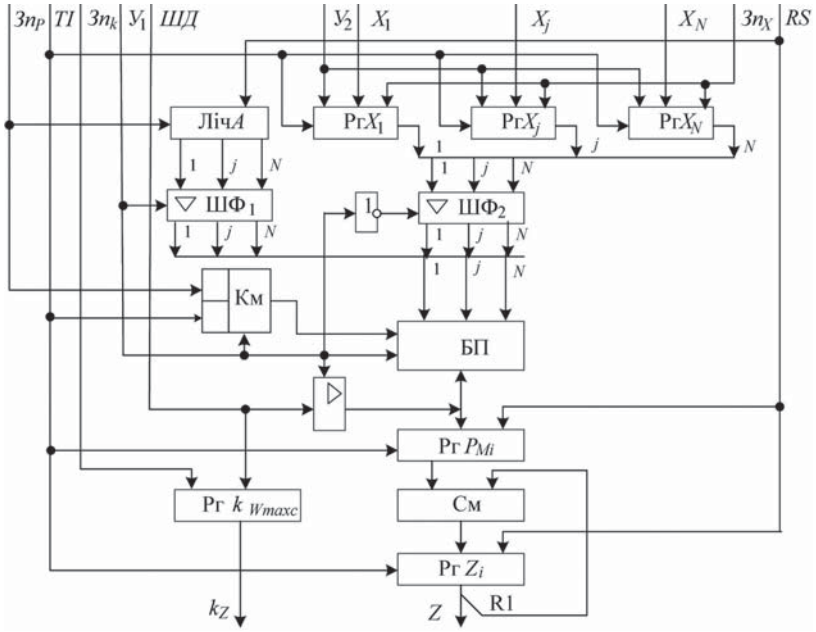

Рис. 3. Базова структура пристрою таблично-алгоритмічного обчислення скалярного добутку з ваговими коефіцієнтами у форматі з плавучою комою / Basic structure of the table-algorithmic scalar product computation unit with floating-point weighted coefficients

Перед початком роботи сигналом із входу RS лічильник ЛічA, регістри РгP_{Mi} та РгZ_i установлюються в нуль. Обчислення скалярного добутку виконується у два етапи.

На першому етапі виконується запис попередньо обчислених за формулою (11) макрочасткових добутків елементів вектора P_{Mi} у БП. Для цього на вхід $У_1$ надходить лог.0, який встановлює БП у режим запису, комутатор Км – на передачу від'ємних імпульсів із входу $Зп_P$, а шинні формувачі ШФ$_1$ і ШФ$_2$ відповідно – на передачу даних та у третій стан. Обчислені макрочасткові добутки P_{Mi} надходять на вхід ШД і від'ємним імпульсом із входу $Зп_P$ записуються в БП. Переднім фронтом (переходом з лог.0 у лог. 1) сигналу $Зп_P$ значення Ліч A збільшується на одиницю. За 2^N тактів виконується запис попередньо обчислених макрочасткових добутків елементів вектора P_{Mi} у БП. Попередньо обчислений найбільший спільний порядок вагових коефіцієнтів $_{kWmaxc}$ із ШД-імпульсом із входу $Зп_k$ записується в регістр Рг$_{kWmaxc}$.

На другому етапі виконують обчислення скалярного добутку векторів. Перед початком виконання другого етапу на вхід $У_2$ надходить лог.0, який встановлює регістри Рг$_{X1}$,…, Рг$_{XN}$ у режим паралельного запису. Вхідні дані із входів $X_1,\ldots,X_N$ переднім фронтом імпульсу із входу $Зп_X$ записуються в регістри Рг$_{X1}$,…,Рг$_{XN}$. Після цього на вході $У_2$ встановлюється лог.1, яка встановлює регістри Рг$_{X1}$,…,Рг$_{XN}$ у режим зсуву даних вправо, а на вході $У_1$ – лог.1, яка встановлює БП у режим читання, а шинні формувачі ШФ$_1$ і ШФ$_2$ відповідно – у третій стан і на передачу даних.

Обчислення скалярного добутку Z у пристрої, наведеному на рис. 3, виконують з використанням тактових імпульсів, які надходять із входу ТІ. У кожному i-му такті роботи на адресний вхід БП надходить i-й розрядний зріз, який є адресою макрочасткового добутку P_{Mi}. Зчитаний із БП i-й макрочастковий добуток P_{Mi} надходить на входити регістра Рг$P_{Mi.}$. На суматорі См виконують додавання (i-1)-го макрочасткового добутку $P_{M(i-1)}$ (виходи регістра Рг P_{Mi}) до зсунутої на один розряд вправо раніше накопиченої суми, яка надходить з виходів регістра РгZ_i. Переднім фронтом i-го ТІ-дані у регістрах Рг$_{X1}$,…,Рг$_{XN}$ зсуваються на один розряд вправо, а у регістри РгP_{Mi} та РгZ_i записується відповідно P_{Mi} та $Z_{i\text{-}1}$.

Кількість тактів, потрібних для отримання результату обчислення скалярного добутку Z за алгоритмом з аналізом розрядного зрізу вхідних даних $x_{1i},\ldots,x_{Ni}$, визначають їх розрядністю та одним тактом затримки. Період конвеєрного такту, з яким працює пристрій, визначають за формулою:

$$T_{TI} = t_{ШФ} + t_{БП} + t_{Рг}, \qquad (13)$$

де $t_{ШФ}$, $t_{Рг}$, $t_{ОЗП}$ – тривалість затримки відповідно на шинному формувачі ШФ, блоці пам'яті БП та регістрі Рг.

Перед початком процесу обчислення скалярного добутку Z обчислюють усі можливі варіанти макрочасткових добутків елементів вектора P_{Mi} згідно з формулою (11) і записують у блок пам'яті БП. Адресами для читання даних з БП є розрядний зріз x_{ij}. Використання вдосконаленого таблично-алгоритмічного методу обчислення скалярного добутку можливе для невеликих значень N. Обсяг пам'яті можна зменшити способом поділу вхідного розрядного зрізу на частини і формування для кожної частини окремої таблиці макрочасткових добутків елементів векторів P_{N1Mi} та P_{N2Mi}. Таблиці для P_{N1Mi} та P_{N2Mi} можуть зберігатися в окремих блоках пам'яті або зберігатися в одному блоці пам'яті. За використання двох блоків пам'яті частини макрочасткових добутків елементів векторів P_{N1Mi} та P_{N2Mi} зчитуються за один такт, а за одного блоку пам'яті – за два такти. Макрочастковий добуток P_{Mi} є сумою двох частин макрочасткових добутків елементів векторів P_{N1Mi} та P_{N2M}.

Розроблення структури проблемно-орієнтованої системи нейромережевого криптографічного захисту даних. Загалом завдання розроблення структури проблемно-орієнтованої системи нейромережевого криптографічного захисту даних можна сформулювати так:

- розробити алгоритм роботи проблемно-орієнтованої системи нейромережевого шифрування-дешифрування

даних та подати його у вигляді конкретизованого потокового графу;
- визначити алгоритми, що реалізуються апаратними засобами, та алгоритми, що реалізуються програмними засобами;
- розробити структуру проблемно-орієнтованої системи нейромережевого шифрування-дешифрування даних у реальному часі, яка враховує всі обмеження у частині габаритів та енергоспоживання;
- визначити основні характеристики нейроподібних елементів та здійснити їх синтез;
- вибрати способи обміну даними, визначити потрібні зв'язки та розробити алгоритми обміну між компонентами системи;
- визначити порядок реалізації у часі процесів нейромережевого шифрування-дешифрування даних та розробити алгоритми управління ними.

Проблемно-орієнтована система нейромережевого криптографічного захисту даних повинна забезпечувати: реалізацію вибраної нейромережі, можливість змінювати маски, обчислювати матриці вагових коефіцієнтів W_j і таблиці макрочасткових добутків елементів вектора P_{Mi} для різних варіантів нейромереж. Розроблення проблемно-орієнтованої системи нейромережевого криптографічного захисту даних будемо здійснювати з використанням таких принципів:

- змінності складу обладнання, що передбачає наявність процесорного ядра та змінних модулів, за допомогою яких ядро адаптується до вимог конкретного застосування;
- модульності, який передбачає розроблення компонентів системи у вигляді функціонально завершених пристроїв;
- конвеєризації та просторового паралелізму за шифрування та дешифрування даних;
- відкритості програмного забезпечення, що передбачає можливості нарощування та його вдосконалення, максимального використання стандартних драйверів і програмних засобів;
- спеціалізації та адаптації апаратно-програмних засобів до структури таблично-алгоритмічно шифрування і дешифрування даних.

Проблемно-орієнтована система нейромережевого криптографічного захисту даних складається із двох підсистем шифрування та дешифрування даних. Структуру проблемно-орієнтованої підсистеми нейромережевого шифрування даних наведено на рис. 4, де МК – мікроконтролер, ВМ – вузол маски, НМ – нейромережа, МД – макрочастковий добуток, Рг – регістр, См – суматор.

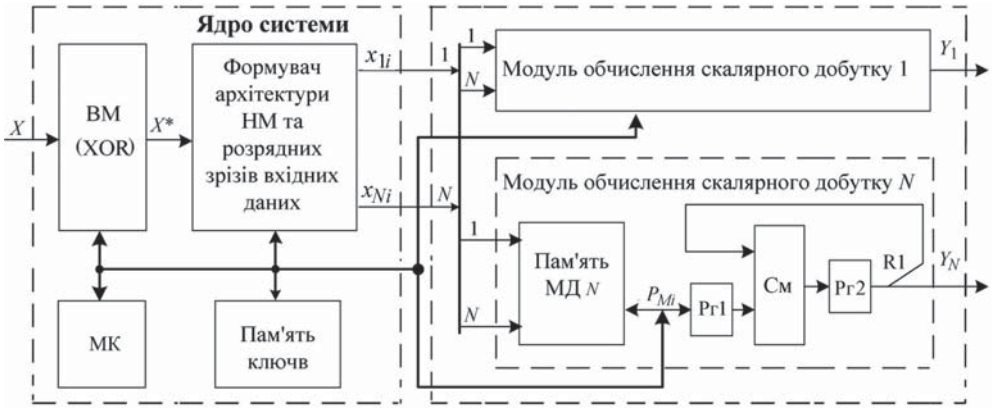

Рис. 4. Структура проблемно-орієнтованої підсистеми нейромережевого шифрування даних / Structure of the problem-oriented subsystem for neural network-based data encryption

Розроблена проблемно-орієнтована підсистема нейромережевого шифрування даних має змінний склад обладнання, основою якої є ядро системи та набір модулів обчислення скалярного добутку векторів. Ядро системи є постійним для всіх застосувань і складається з мікроконтролера МК, вузла маски ВМ, пам'яті ключів і формувача архітектури нейромережі та розрядних зрізів вхідних даних. Модулі обчислення скалярного добутку реалізують базовою операцією таблично-алгоритмічного методу обчислення скалярного добутку векторів. Кількість модулів обчислення скалярного добутку залежно від потрібної швидкодії визначають за такою формулою:

$$s = \frac{N}{2^v}, \qquad (13)$$

де: N – кількість нейроподібних елементів; $v = 0,\ldots d$, $d = \log_2 N$. Найбільшу швидкодію підсистема нейромережевого шифрування даних досягає у разі, якщо кількість модулів обчислення скалярного добутку відповідає кількості нейроподібних елементів N. Для забезпечення шифрування даних у реальному часі пропонуємо модулі обчислення скалярного добутку вузлів маски ВМ, формувач архітектури нейромережі та розрядних зрізів вхідних даних реалізувати у вигляді спеціалізованих апаратних засобів.

Проблемно-орієнтована підсистема нейромережевого шифрування даних працює так. Перед початком шифрування даних МК здійснюють налаштування архітектури нейромережі (визначають кількість N нейроподібних елементів, кількість входів k та їх розрядність m). Для вибраної архітектури нейромережі з допомогою МК обчислюють матрицю вагових коефіцієнтів W_j і таблиці макрочасткових добутків елементів вектора P_{Mi}, які записуються у пам'ять МД. Окрім цього, у вузол ВМ записують дані, вибрані із пам'яті ключів маски. Повідомлення X, яке потрібно зашифрувати, надходить на вхід ВМ у форматі з фіксованою комою, де воно маскується. Повідомлення з накладеною маскою X^* із виходу ВМ надходить на вхід формувача архітектури нейромережі та розрядних зрізів, де вони розбиваються на N груп розрядністю m і виконується формування розрядних зрізів $x_{1i},\ldots,x_{Ni}$. Потрібно зазначити, що формування розрядних зрізів $x_{1i},\ldots,x_{Ni}$ розпочинається з молодших розрядів. Сформовані розрядні зрізи $x_{1i},\ldots,x_{Ni}$ є адресою для читання із пам'яті МД макрочасткового добутку P_{Mi}. Зчитаний макрочастковий добуток P_{Mi}. записується у регістр Рг1. З допомогою суматора См виконується підсумовування макрочасткових добутків елементів вектора P_{Mi} за формулою (20). Кількість тактів, потрібних для обчислення скалярного добутку, визна-

чають розрядністю входів *m*. Управління процесом шифрування у бортові системі нейромережевого шифрування даних виконується МК.

Структура проблемно-орієнтованої підсистеми нейромережевого криптографічного дешифрування даних переважно відповідає структурі підсистеми нейромережевого шифрування даних, яку наведено на рис. 4.

Реалізація спеціалізованих апаратних засобів нейромережевого шифрування даних на FPGA. Проєктування спеціалізованих апаратних засобів підсистеми нейромережевого шифрування даних виконували мовою програмування апаратури VHDL у середовищі розроблення Quartus II вер. 13.1 з використанням бібліотек середовища розроблення. Середовище розроблення Quartus II підтримує весь процес проєктування спеціалізованих апаратних засобів, починаючи із введення проєкту користувачем і завершуючи програмуванням ПЛІС, налагодженням як самої мікросхеми, так і засобів загалом.

Принципову схему спеціалізованих апаратних засобів підсистеми нейромережевого шифрування даних наведено на рис. 5. Входи блоку XOR_Mask1_4_2: *X*[7..0] – вхідні дані; *Clk* – вхід синхронізації завантаження вхідних даних; *X_Mask*[7..0] – 8-бітна маска. На виході цього блоку формується *N* векторів розрядністю *m*. Синхронізацію реалізовано за переднім фронтом імпульсів *Clk*.

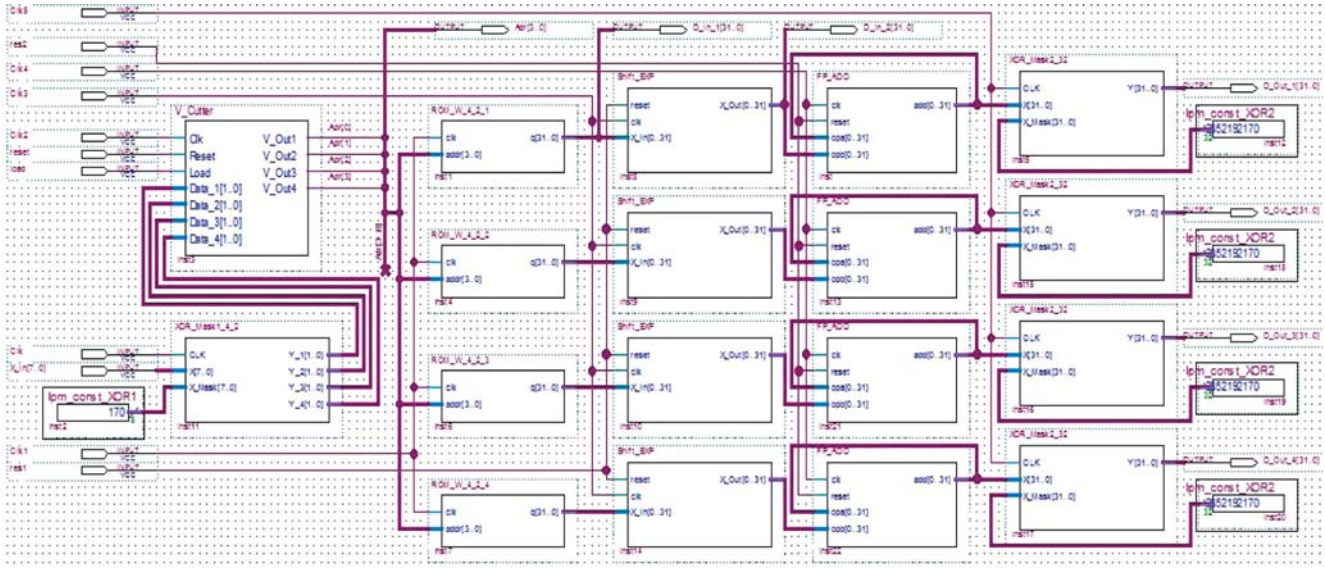

Рис. 5. Принципова схема спеціалізованих апаратних засобів підсистеми нейромережевого шифрування даних / Block diagram of specialized hardware components of the neural network-based data encryption subsystem

Блок V_Cutter з *N*=4 вхідними векторами розрядністю *m*=2 складається з *N* регістрів паралельно-послідовного типу та формує вертикальні розрядні зрізи. Вхідні дані: *Data*_1[*n*-1..0], …, *Data_N*[*n*-1..0] – *N* вхідних векторів розрядністю *n*; *Clk* – імпульси синхронізації формування вертикальних розрядних зрізів; *Reset* – сигнал початкового скидання в "0" виходу регістрів R_Par_Ser; *Load* – сигнал дозволу завантаження даних у регістри R_Par_Ser. Виходи: *V_Out*1, …,*V_OutN* – вертикальний розрядний зріз. Формування вертикальних зрізів розпочинається з наймолодшого розряду.

Вагові коефіцієнти нейромережі з *N*=4 входами розрядністю *m*=2 зберігаються в ROM-пам'яті FPGA у вигляді чорирьох таблиць. Кожна з них складається із 16-ти слів розрядністю 32 біти. Вичитування даних з цих таблиць виконують з допомогою блоків ROM_W_4_2_1, …, ROM_W_4_2_4.

Входи цих блоків: *addr*[3..0] – адреса комірки таблиці, з якої вичитуватимуться дані; *clk* – імпульси синхронізації вичитування даних з таблиці. Синхронізацію реалізовано за переднім фронтом імпульсів *clk*. Вихід: *q*[31..0] – дані, вичитані з комірки із вхідною адресою.

Зчитані з таблиць дані надходять на вхід блоків Shift_EXP, які виконують їх множення на 2^j, де j =0, …, *n*-1. За надходження на цей блок даних, що відповідають нульовому розряду, онулюється лічильник розрядів. Синхронізація роботи цього блоку здійснюється з допомогою тактових імпульсів *Clk*. На виході *X_Out*[0..31] отримуємо перемножені на 2^j вхідні дані.

З виходу блоків Shift_EXP дані надходять на один із входів суматорів FP_ADD. Інший вхід суматорів з'єднаний з їх виходом. Вхідні сигнали суматора: *clk* – імпульси синхронізації; *reset* – сигнал онулення вхідних даних *opa* за реалізації суматора з акумулятором; *opa*[0..31], *opb*[0..31] – доданки. За переднім фронтом першого імпульсу *clk* у суматор завантажуються доданки, а за переднім фронтом другого імпульсу виводиться отримана сума. Вихід суматора: сума *add*[0..31].

З виходу суматорів FP_ADD дані надходять на вхід блоку XOR_Mask2_32, який виконує накладання 32-бітної маски. Входи блоку XOR_Mask2_32: *X*[31..0] – зашифровані вихідні дані; *Clk* – вхід синхронізації завантаження вхідних даних; *X_Mask*[31..0] – 32-бітна маска. Вихід блоку: вектор *Y*[31..0]. Синхронізацію реалізовано за переднім фронтом імпульсів *Clk*. Зашифровані дані отримуємо на виходах *D_Out*_1, *D_Out*_2, *D_Out*_3, *D_Out*_4.

Часову діаграму роботи спеціалізованих апаратних засобів підсистеми нейромережевого шифрування даних наведено на рис. 6. Для реалізації спеціалізованих апаратних засобів нейромережевого шифрування даних на базі FPGA EP3C16F484C6 сімейства Cyclone III п 3053 логічних елементів із 15408 логічних елементів і 745 регістрів. Час, потрібний для шифрування одного вектора вхідних даних, становить приблизно 160 наносекунд.

Отримані результати підтверджують ефективність запропонованого методу нейромережевого шифрування даних, реалізованого на базі FPGA. Використання тіль-

ки 3053 логічних елементів (менше 20 % від доступних ресурсів кристала) та 745 регістрів свідчить про раціональне використання апаратної бази, що є критично важливим для бортових систем з обмеженими ресурсами. Швидкодія на рівні 160 наносекунд для оброблення одного вектора вхідних даних демонструє доцільність застосування таблично-алгоритмічного підходу до реалізації нейроподібних елементів, що забезпечує виконання криптографічних операцій у режимі реального часу.

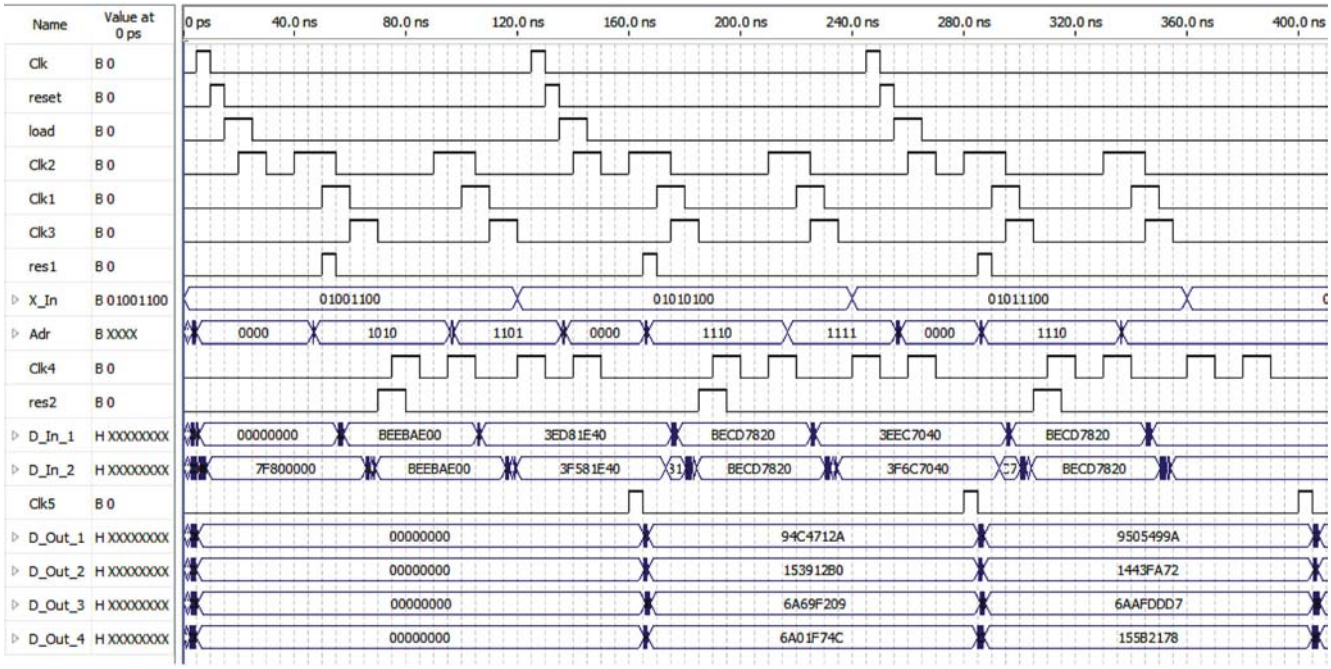

Рис. 6. Часова діаграма роботи спеціалізованих апаратних засобів підсистеми нейромережевого шифрування даних / Timing diagram of the operation of specialized hardware components in the neural network-based data encryption subsystem

Обговорення результатів дослідження. Наявні системи криптографічного захисту для вбудованих систем використовують класичні алгоритми AES (англ. – *Advanced Encryption Standard*), однак їх реалізація потребує значних обчислювальних ресурсів та збільшує енергоспоживання [3]. Метод криптографічного захисту даних з використанням нейромереж прямого поширення автоасоціативного типу на підставі парадигми моделі послідовних геометричних перетворень та таблично-алгоритмічної реалізації нейроподібних елементів, порівняно з наявними методами [8], орієнтований на апаратно-програму реалізацію, що враховує обмеження щодо обчислювальних ресурсів, маси, габаритів та енергоспоживання. Такий метод за рахунок можливої динамічної зміни ключа, який складається із заданої кількості нейронів, матриці вагових коефіцієнтів і операцій маскування, забезпечує високу криптографічну стійкість алгоритму, а за рахунок апаратної реалізації нейроподібних елементів забезпечує виконання шифрування та дешифрування даних у реальному часі.

Подальші дослідження зі створення системи нейромережевого криптографічного захисту даних у МРП пов'язано з розробленням нейроподібних мереж з нелінійними синаптичними зв'язками для шифрування-дешифрування даних із симетричними ключами. За реалізації симетричної криптосистеми ключ шифрування та ключ дешифрування є однаковими, або ключ дешифрування легко обчислюється із ключа шифрування. Нейроподібне шифрування даних з нелінійними синаптичними зв'язками відбувається над відкритим текстом з використанням ключа, який складається із сукупності даних, що визначаються архітектурою нейроподібної мережі (кількість $p \cdot N$ нейроподібних елементів, де p – максимальне значення показника поліному, N – кількість входів нейроподібної мережі) та p матриць вагових коефіцієнтів з плавучою комою. Значення N визначають розрядністю повідомлення n та розрядністю входів нейромережі m.

Проаналізовані актуальні публікації підтверджують доцільність використання нейромережевих структур у криптографічному захисті даних. Так, у роботі [13] розглянуто використання глибоких згорткових генеративно-змагальних мереж (DCGAN) у задачах шифрування медичних зображень. Запропонована схема забезпечує високий рівень захисту та стійкість до атак, хоча й орієнтована переважно на оброблення зображень, а не символьних потоків у реальному часі.

У дослідженні [14] представлено апаратну реалізацію криптографічного методу на підставі мережі Хопфілда з використанням мемристорних структур. Результати демонструють переваги у швидкодії та стійкості до атак, однак модель не враховує таблично-алгоритмічної оптимізації, яка є ключовою перевагою нашого підходу.

У публікації [1] запропоновано легкий криптографічний алгоритм на підставі гібридного квантового підходу з хаотичними картами, орієнтований на IoT-пристрої з обмеженими ресурсами. Основна відмінність у нашій роботі полягає в уніфікованій нейроподібній архітектурі, яка дає змогу масштабувати систему відповідно до обсягу даних.

У роботі [6] закцентовано на атаках, спрямованих на відновлення функціонально еквівалентної нейромережі-шифратора. Запропонована в нашій роботі архітектура з поєднанням таблично-алгоритмічної реалізації, нелінійних перетворень та плавучої коми значно ускладнює таке відновлення через внутрішню варіативність структури.

У статті [27] розглянуто підходи до побудови легких криптографічних алгоритмів, які забезпечують надійний захист за обмежених апаратних можливостей.

Наш підхід аналогічно орієнтований на обмежені ресурси, проте реалізується на принципово іншій парадигмі – нейроподібних мережах з апаратною підтримкою шифрування та дешифрування.

Узагальнення результатів дослідження та порівняльний аналіз сучасних підходів до реалізації нейромережевого криптографічного захисту даних дає підстави стверджувати, що в наявній науковій літературі відсутні комплексні рішення, які поєднували б автоасоціативні нейромережі прямого поширення, таблично-алгоритмічне обчислення скалярного добутку з плавучою комою та апаратну реалізацію з урахуванням обмежених ресурсів вбудованих систем. Запропонований підхід дає змогу усунути обмеження класичних методів, підвищити швидкодію шифрування-дешифрування та забезпечити внутрішню варіативність криптографічної структури, що ускладнює атаки на нейромережу. Це підтверджує наукову та практичну доцільність проведеного дослідження та свідчить про його інноваційність у контексті сучасного розвитку криптографії для вбудованих застосунків.

Отже, за результатами виконаної роботи можна сформулювати такі наукову новизну та практичну значущість результатів дослідження.

Наукова новизна отриманих результатів дослідження – вперше розроблено метод нейромережевого криптографічного захисту даних, який на підставі використання нейромереж прямого поширення автоасоціативного типу, реалізованих за парадигмою послідовних геометричних перетворень із попереднім обчисленням вагових коефіцієнтів та вдосконаленою табличноалгоритмічною структурою нейроподібних елементів, забезпечує його значну криптографічну стійкість, підтримку процесу шифрування й дешифрування даних у реальному часі, а також ефективну апаратно-програмну реалізацію з покращеними техніко-експлуатаційними характеристиками.

Практична значущість результатів дослідження – розроблений метод нейромережевого криптографічного захисту даних можна ефективно застосовувати для реалізації високошвидкісного апаратно-програмного шифрування та дешифрування даних у реальному часі з значною криптографічною стійкістю до атак, а також для зменшення тривалості розроблення спеціалізованих пристроїв з обчислення скалярного добутку векторів із заданими параметрами, що є критично важливим у системах безпеки та захищеного зв'язку.

Висновки / Conclusions

Розроблено проблемно-орієнтовану систему нейромережевого криптографічного захисту даних у реальному часі, що забезпечує підвищену її швидкодію та криптографічну стійкість. За результатами проведеного дослідження можна зробити такі основні висновки.

1. Розроблено метод нейромережевого криптографічного захисту даних, який за рахунок використання нейромереж прямого поширення автоасоціативного типу на підставі парадигми моделі послідовних геометричних перетворень, попереднього обчислення вагових коефіцієнтів та таблично-алгоритмічної реалізації нейроподібних елементів забезпечує високу її криптографічну стійкість, шифрування-дешифрування даних у реальному часі та апаратно-програмну реалізацію з високими техніко-експлуатаційними характеристиками.
2. Удосконалено таблично-алгоритмічний метод обчислення скалярного добутку векторів, який за рахунок приведення до найбільшого спільного порядку вагових коефіцієнтів і формування для них таблиць макрочасткових добутків елементів векторів забезпечує швидке обчислення скалярного добутку для вхідних даних як з фіксованою, так і плавучою комами.
3. Розроблено базову структуру пристрою таблично-алгоритмічного обчислення скалярного добутку, основними компонентами якої є блоки пам'яті для зберігання макрочасткових добутків елементів векторів, суматор, шинні формувачі та регістри, її використання забезпечує зменшення тривалості розроблення пристрою обчислення скалярного добутку зі заданими параметрами.
4. Розроблено, на підставі принципів змінності складу обладнання, модульності, спеціалізації та паралелізму, структуру проблемно-орієнтованої системи нейромережевого криптографічного захисту даних, яка за рахунок взаємопоєднання універсального та спеціалізованого підходів, програмних і спеціалізованих апаратних засобів забезпечує ефективну реалізацію алгоритмів шифрування-дешифрування даних у реальному часі.
5. Виконано моделювання спеціалізованих апаратних засобів нейромережевого шифрування даних мовою програмування апаратури VHDL у середовищі розроблення Quartus II вер. 13.1 з використанням FPGA EP3C16F484C6 сімейства Cyclone III та визначено, що тривалість шифрування одного вектора вхідних даних становить приблизно 160 нс, а для їх реалізації потрібно 3053 логічних елементів і 745 регістрів.

References

1. Aljaedi, S., Manogaran, G., & Hassan, M. M. (2025). A hybrid lightweight quantum encryption for secure IoT environments. *Scientific Reports*, *15*, article ID 2788. URL: https://www.nature.com/articles/s41598-025-97822-6
2. Atrey, P. K., & Pal, A. (2016). Neural Network Based Cryptography. ResearchGate. URL: https://www.researchgate.net/publication/309230198_Neural_Network_Based_Cryptography
3. Avoine, G., & Kara, O. (Eds.). (2013). Lightweight Cryptography for Security and Privacy: Second International Workshop, LightSec 2013, Gebze, Turkey, May 6–7, 2013, Revised Selected Papers. Lecture Notes in Computer Science. Springer. https://doi.org/10.1007/978-3-642-40392-7
4. Awad, A. I., Furnell, S., Paprzycki, M., & Sharma, S. K. (Eds.). (2021). Security in Cyber-Physical Systems: Foundations and Applications. Springer, 105–112. https://doi.org/10.1007/978-3-030-67361-1
5. Balsara, R. A., Sardar, S. S., & Jain, A. J. (2017). Design of an Autonomous Robot Security System Using Neural Networks. *International Journal of Computer Engineering & Technology* (IJCET), *8*(3), 68–75. URL: https://iaeme.com/Home/issue/IJCET?Volume=8&Issue=3
6. Chen, X., Wang, Y., & Zhang, T. (2024). Attack towards neural cryptographic models via equivalence discovery. *arXiv preprint*. URL: https://arxiv.org/abs/2409.11646
7. Chen, Y., Cheng, C., Zhang, Y., & Sun, L. (2022). A neural network-based navigation approach for autonomous mobile robot systems. *Applied Sciences*, *12*(15), 7796. https://doi.org/10.3390/app12157796
8. Delacour, K. J., & Wolf, C. (2020). A Survey of Neural Network Applications to Cryptography. *Neural Computing and Applications*, *32*(17), 13349–13374. https://doi.org/10.1007/s00521-020-04859-9
9. Dressler, F., & Tonguz, O. (2008). Self-Organization in Sensor and Actor Networks. Hoboken, NJ: Wiley, 55–59 URL: https://www.wiley.com/en-us/Self-Organization+in+Sensor+and+Actor+Networks-p-9780470724453
10. Goodfellow, I., Bengio, Y., & Courville, A. (2016). Deep Learning. Cambridge: MIT Press, 305–317. URL: https://www.deeplearningbook.org

11. Heineman, G. T., Pollice, G., & Selkow, S. (2011). Algorithms in a Nutshell. OReilly Media. URL: https://archive.org/details/algorithmsinnuts0000hein_i4t5_2
12. Khavalko, V., & Tsmots, I. (2019). Image classification and recognition on the base of autoassociative neural network usage. In 2019 IEEE 2nd *Ukraine Conference on Electrical and Computer Engineering* (UKRCON-2019), 1118–1121. Lviv, Ukraine. https://doi.org/10.1109/UKRCON.2019.8879897
13. Kumar, R., Singh, S., Pandey, H. M., et al. (2025). A secure medical image encryption scheme using DCGAN with virtual planetary domain. *Scientific Reports*, 15, article ID 1675. URL: https://www.nature.com/articles/s41598-024-84186-6
14. Liu, Y., & Hu, Y. (2024). Hopfield neural network and memristor-based image encryption hardware architecture. *SSRN*, 14. https://doi.org/10.2139/ssrn.4774124
15. Mahmoud, M. M., Gad, R. M., Younis, M., & Alghamdi, T. A. (2021). Secure Communication Protocols for Mobile Robotic Networks: Challenges and Solutions. *IEEE Communications Surveys & Tutorials*, *23*(2), 1287–1312. https://doi.org/10.1109/COMST.2020.3048767
16. Olaoye, G. (2025). Self-Learning Neural Networks in the Cloud: Towards Autonomous AI Systems. SSRN. https://doi.org/10.2139/ssrn.5129553
17. Smith, J., & Johnson, M. (2019). Hardware acceleration techniques in cryptographic applications. *Journal of Cryptographic Research*, *15*(3), 123–134. https://doi.org/10.48550/arXiv.2501.04394
18. Stallings, W. (2017). Cryptography and Network Security: Principles and Practice (7th ed.). Boston: Pearson, 108–116 URL: https://staff.ustc.edu.cn/~mfy/moderncrypto/crypto7ed.pdf
19. Tcimbal, Iu. V. (2018). Neiromerezhevii metod simetrichnogo shifruvannia danikh. *Bulletin of Lviv Polytechnic National University. Series: Journalistic sciences*, *901*, 118–122. URL: https://ena.lpnu.ua/handle/ntb/44537
20. Tsmots, I. H., & Skorokhoda, O. V. (2011). Device for scalar product calculation. Utility model patent of Ukraine, 66138. *Bulletin*, 24. URL: https://iprop-ua.com/inv/6295y8t3/
21. Tsmots, I. H., Opotyak, Y. V., Shtohrynets, B. V., Mamchur, T. B., & Holubets, V. M. (2024). Model, structure, and synthesis method of a matrix-type neural element. *Scientific Bulletin of UNFU*, *34*(4), 68–77. https://doi.org/10.36930/40340409
22. Tsmots, I. H., Skorokhoda, O. V., & Medykovskyi, M. O. (2019). Device for scalar product calculation. Invention patent of Ukraine, 118596. Bulletin, 3. URL: https://iprop-ua.com/inv/0rtysziq/
23. Tsmots, I. H., Skorokhoda, O. V., & Teslyuk, V. M. (2013). Device for scalar product calculation. *Invention patent of Ukraine*, 101922. Bulletin, 9. URL: https://iprop-ua.com/inv/k1jqmw30/
24. Tsmots, I. H., Teslyuk, V. M., Teslyuk, T. V., Medykovskyi, M. O., & Tsymbal, Y. V. (2019). Device for calculating the sum of even products. Patent of Ukraine, 120210. Bulletin, 20/2019. URL: https://iprop-ua.com/inv/6ueuxvh7/
25. Tsmots, I., Teslyuk, V., Łukaszewicz, A., Lukashchuk, Y., Kazymyra, I., Holovatyy, A., & Opotyak, Y. (2023). An approach to the implementation of a neural network for cryptographic protection of data transmission at UAV. *Drones*, *7*(8), article ID 507. https://doi.org/10.3390/drones7080507
26. Tsmots, I., Tsymbal, Y., Skorokhoda, O., & Tkachenko, R. (2019). Neural-like methods and hardware structures for real-time data encryption and decryption. In CSIT 2019: *Proceedings of the XIV International Scientific and Technical Conference*, 248–253. Lviv, Ukraine. https://doi.org/10.1109/STC-CSIT.2019.8929809
27. Ullah, H., Javed, A., & Farooq, U. (2024). Lightweight cryptographic algorithms for secure IoT communication: a comparative study. *International Journal of Information Security and Technologies*, *10*(2), 110–120. URL: https://journal.50sea.com/index.php/IJIST/article/view/1127
28. Zhang, Y., & Li, X. (2015). Neural cryptography: A new approach to secure communication. *Journal of Cryptographic Engineering, 7*(3), 197–209. https://doi.org/10.1007/s13389-015-0101-1
29. Zhou, L., Zhang, X., & Li, H. (2021). Deep-learning-based cryptanalysis through topic modeling. *Proceedings of the International Conference on Cryptography and Network Security* (ICCNS), 59–67. https://doi.org/10.1007/978-3-030-80129-8_59

I. H. Tsmots, B. V. Shtohrinets, T. B. Mamchur
Lviv Polytechnic National University, Lviv, Ukraine

PROBLEM-ORIENTED CRYPTOGRAPHIC SYSTEM FOR NEURAL NETWORK-BASED DATA PROTECTION

The paper deals with the study the problem-oriented cryptographic system for neural network-based data protection. In the course of research, it has been established that high technical and operational performance of onboard cryptographic data protection systems can be achieved through the use of a problem-oriented approach, a modern component base, the development of new methods of neural network-based encryption and decryption, as well as algorithms and specialized structures for implementing neuro-like elements. A method for neural network-based cryptographic data protection has been developed. By employing feedforward autoassociative neural networks based on the paradigm of sequential geometric transformations, pre-calculation of weight coefficients, and a table-algorithmic implementation of neuro-like elements, this method ensures high cryptographic resistance of the encryption-decryption algorithm in real-time, along with a hardware-software implementation that exhibits excellent technical and operational characteristics. Moreover, a table-algorithmic method for computing the scalar product of vectors has been improved. By reducing weight coefficients to their greatest common order and generating tables of macro-partial products, the method provides fast processing of input data with both fixed-point and floating-point formats. Furthermore, the basic structure of a device for table-algorithmic computation of the scalar product of vectors has been developed. Its main components include memory blocks for storing macro-partial products, an adder, bus shapers, and registers. Utilization of this structure enables a reduction in the design time for devices with predetermined parameters. Based on the principles of equipment configuration variability, modularity, specialization, and parallelism, a structure of a problem-oriented system for neural network-based cryptographic data protection has been developed. Through the integration of universal and specialized approaches, as well as software and specialized hardware tools, this system enables efficient real-time execution of encryption and decryption algorithms. Simulation of the specialized hardware for neural network-based data encryption was performed using the VHDL hardware description language in the Quartus II v13.1 development environment, targeting the Cyclone III family FPGA (EP3C16F484C6). It was determined that the encryption time of a single input data vector is approximately 160 ns, requiring 3053 logic elements and 745 registers for implementation.

Keywords: encryption; decryption; scalar product; table-algorithmic method; computational neural networks; adaptive hardware-software environment; real time.