# *Використання нейроморфних обчислень для виявлення та запобігання кіберзагроз у комп'ютерних мережах*

https://doi.org/10.31713/MCIT.2024.058

Каштан Наталія
Національний університет водного господарства та природокористування
м. Рівне, Україна
nata.khel809@gmail.com

*Анотація* – **У роботі досліджуються способи захисту від кіберзагроз, які базуються на нейроморфних обчисленнях. Дослідження нейроморфних обчислень спрямоване на розробку обчислювальних систем, що імітують структуру та функції людського мозку. Нейроморфні системи володіють унікальними характеристиками, які можуть бути використані для створення більш ефективних і надійних методів протидії кіберзагрозам**

**Ключові слова** – ***ьнейроморфні обчислення, кібербезпека, комп'ютерні мережі, аномалія, методи захисту***

## I. Вступ

В епоху цифрової трансформації компанії та урядові організації стикаються з постійним зростанням кількості та складності кіберзагроз. Традиційні системи кіберзахисту, засновані на відомих шаблонах і сигнатурах, вже не здатні повною мірою захистити інфраструктуру від нових та швидко еволюціонуючих атак. Цей виклик вимагає впровадження нових підходів до кібербезпеки, які могли б забезпечити проактивний захист. Одним із перспективних рішень є нейроморфні обчислення – технологія, яка моделює роботу біологічних нейронів і має великий потенціал для виявлення та запобігання кіберзагрозам [1].

Застосування нейроморфних обчислень у сфері кібербезпеки охоплює інноваційні підходи для виявлення, запобігання та реагування на кіберзагрози з високою швидкістю та точністю. Однією з головних переваг нейроморфних обчислень є їх здатність до виявлення аномалій і розпізнавання образів.

## II. Нейроморфні обчислення

Нейроморфні обчислення – це міждисциплінарна галузь, яка поєднує принципи нейронауки, інформатики та комп'ютерної інженерії. Термін «нейроморфний» означає «подібний до мозку». Комп'ютери розробляються та проєктуються таким чином, щоб відображати структуру та функції людського мозку.

Основна мета нейроморфних обчислень полягає у створенні апаратного забезпечення, яке працює подібно до нейронних мереж у біологічних організмах, що дозволяє виконувати обчислення більш ефективно, з меншою енерговитратою та високою швидкістю, ніж звичайні комп'ютери, якими ми користуємося сьогодні [1].

Нейроморфні обчислення націлені на відтворення нейронної структури мозку за допомогою апаратних та програмних моделей, які називають нейроморфними чіпами або системами. Ці системи складаються зі штучних нейронів і синапсів, що дозволяють одночасно обробляти інформацію та адаптуватися до даних у реальному часі. На відміну від класичної архітектури фон Неймана, де пам'ять і процесор розділені, нейроморфні системи поєднують ці функції, що прискорює обчислення та знижує енергоспоживання, що особливо важливо для додатків з високими вимогами, як-от кібербезпека.

## III. Використання нейроморфних обчислень для виявлення та запобігання кіберзагроз

Нейроморфні обчислення відкривають нові можливості в сфері кібербезпеки завдяки інноваційним підходам для виявлення, запобігання та реагування на загрози з високою точністю і швидкістю. Особливо ефективними ці системи є у виявленні аномалій та розпізнаванні образів. Традиційні методи кіберзахисту здебільшого базуються на виявленні загроз через порівняння з відомими сигнатурами шкідливої активності. Проте такий підхід не завжди справляється з новими або змінюваними загрозами, для яких сигнатури ще не розроблені. Нейроморфні обчислення долають це обмеження завдяки здатності навчатися на нових даних та оперативно адаптуватися до невідомих шаблонів у реальному часі [4].

Нейроморфні моделі, навчені на великих масивах даних про нормальну та аномальну поведінку мережі, здатні самостійно ідентифікувати аномалії, що можуть свідчити про потенційні кіберзагрози. Нейронні мережі таких систем постійно оновлюють свої внутрішні моделі на основі нових даних, що дозволяє їм помічати навіть найменші відхилення від звичайної поведінки, які

можуть сигналізувати про атаку або спробу несанкціонованого доступу. Окрім цього, нейроморфні обчислення значно підсилюють кіберзахист завдяки своїм можливостям самонавчання і прогнозної аналітики. Аналізуючи історичні дані, нейронні мережі можуть виявляти повторювані шаблони атак і передбачати майбутні загрози ще до їхнього виникнення. Такий проактивний підхід дозволяє організаціям зміцнювати свій захист, реалізовувати ефективні стратегії зменшення ризиків і мінімізувати наслідки кіберінцидентів [2].

Нейроморфні обчислення також відіграють ключову роль в адаптивних і динамічних механізмах захисту. Традиційні системи безпеки часто базуються на статичних правилах і порогових значеннях, які можуть бути легко обійдені досвідченими зловмисниками. Натомість нейроморфні системи постійно адаптують свої методи захисту відповідно до розвитку загроз і змін у середовищі. Вони здатні автоматично коригувати контроль доступу, змінювати протоколи шифрування або перенаправляти мережевий трафік у відповідь на підозрілі дії або аномалії. Це дозволяє знижувати ризики в режимі реального часу і забезпечувати стабільну роботу системи. Більше того, інтеграція нейроморфних обчислень із платформами для аналізу загроз та системами управління інформацією і подіями безпеки (SIEM) покращує масштабованість та ефективність операцій у сфері кібербезпеки [5].

Нейроморфні моделі здатні одночасно обробляти величезні обсяги різноманітних даних, таких як мережеві журнали, поведінкові патерни користувачів та інформацію про загрози. Це сприяє швидкому виявленню й кореляції можливих інцидентів безпеки. Завдяки здатності порівнювати різні джерела даних та знаходити приховані взаємозв'язки, нейроморфні системи допомагають аналітикам кібербезпеки ефективніше розставляти пріоритети та досліджувати попередження, скорочуючи час реакції і покращуючи здатність до реагування на інциденти.

## IV. Розробка методів кіберзахисту

Розробка методів кіберзахисту на основі нейроморфних обчислень включає кілька основних етапів, серед яких – створення моделей нейронних мереж для аналізу кіберзагроз, реалізація адаптивних систем виявлення загроз, автоматизована відповідь на атаки.

Спеціалізовані нейроморфні процесори можуть використовувати моделі штучних нейронних мереж для аналізу аномалій у мережевому трафіку. Це дозволяє виявляти небезпечну активність і блокувати її на ранніх стадіях, знижуючи ймовірність успішної атаки.

Нейроморфні системи здатні навчатися на нових патернах загроз у реальному часі, дозволяючи створювати адаптивні рішення для запобігання кіберзагрозам. Це особливо корисно для боротьби з сучасними атаками, які швидко змінюють свою форму [4].

Використовуючи здатність нейроморфних систем до швидкої обробки даних, вони можуть автоматично реагувати на виявлені загрози, нейтралізуючи їх ще до того, як вони зможуть завдати шкоди. Це значно зменшує ризики для інформаційної інфраструктури.

## V. Висновки та перспективи

Нейроморфні обчислення відкривають нові горизонти в розробці методів кіберзахисту, пропонуючи адаптивні, ефективні та енергоощадні рішення для боротьби з сучасними кіберзагрозами. Завдяки здатності до самоорганізації, адаптивності та швидкої обробки великих обсягів даних, ці системи можуть стати ключовим елементом нової ери в інформаційній безпеці.

Підсумовуючи, варто зазначити, що розробка методів захисту від кіберзагроз на основі нейроморфних обчислень є справжнім проривом у сфері кібербезпеки. Використовуючи принципи нейробіології для відтворення обчислювальної потужності мозку та його здатності до адаптивного навчання, нейроморфні системи надають організаціям можливість швидко, точно та ефективно виявляти, запобігати та реагувати на кіберзагрози, забезпечуючи високу стійкість до атак.

Впровадження нейроморфних обчислень у сферу кіберзахисту є перспективним напрямком, який дозволяє підвищити ефективність протидії сучасним кіберзагрозам, знизити ризики атак та забезпечити безпеку критично важливих інформаційних систем.

## Література


[1] Gigacloud, "Нейроморфні обчислення: що це та в чому суть," URL: https://gigacloud.ua/blog/navchannja/nejromorfni-obchislennja-scho-ce-ta-v-chomu-sut (date of access: 12.10.2024).

[2] Д.С. Мигуль, Н.Н. Шаповалова, "Нейроморфні процеси і системи," *Комп'ютерні інтелектуальні системи та мережі*: матеріали XIII Всеукраїнської науково-практичної web конференції аспірантів, студентів та молодих вчених (24-26 березня 2020 р.), Кривий Ріг, КРНУ, 2020, С. 176–178.

[3] L.R. Iyer, Y. Chua and H. Li, "Is Neuromorphic MNIST Neuromorphic? Analyzing the Discriminative Power of Neuromorphic Datasets in the Time Domain," *Frontiers in Neuroscience*, Vol. 15, 2021, 21p., DOI: https://doi.org/10.3389/fnins.2021.608567.

[4] H.-T. Peng, M.A. Nahmias, T. Ferreira de Lima, A.N. Tait and B.J. Shastri, "Neuromorphic Photonic Integrated Circuits," *IEEE Journal of Selected Topics in Quantum Electronics*, Vol. 24, №6, 2018, 15p., DOI: http://doi.org/10.1109/jstqe.2018.2840448.

[5] А.В. Лемешко, А.В. Антоненко, А.В. Петрик, "Нейроморфні системи як інструмент реалізації штучного інтелекту," *Вчені записки ТНУ імені В.І. Вернадського. Серія: Технічні науки*, Випуск 34 (73), Т.3, 2023, С. 175-183. DOI: https://doi.org/10.32782/2663-5941/2023.3.1/28