

## ЗАХИСТ ВІД ПЕРЕБОЇВ ДИНАМІЧНО КЛАСТЕРИЗОВАНИХ ШТУЧНИХ НЕЙРОННИХ МЕРЕЖ

У статті розглянуто методи побудови захищених від перебоїв динамічно кластеризованих штучних нейронних мереж. Запропоновано різні архітектури захисту від перебоїв в інтернет-середовищі.

**Постановка проблеми.** Виконання додатків в інтернет-середовищі має багато особливостей, які пов'язані з нестабільністю каналів зв'язку та динамічністю існуючих обчислювальних вузлів. Штучні нейронні мережі, що динамічно кластеризуються [1], пристосовані до існування в мережному середовищі, зокрема в Інтернеті. Основною необхідністю їх використання є розподіл даних у просторі та ієрархічність прийняття рішень. Наприклад, якщо радіолокаційні дані збирають у різних куточках країни, то попередній аналіз логічно проводити на місці, а підготовлені результати, обсяг яких буде меншим, ніж необроблених, передавати до більш вищого рівня для подальшої обробки (рис. 1). На найвищому рівні, де зібрано дані з радарів та інших джерел, буде прийнято рішення про можливі дії.

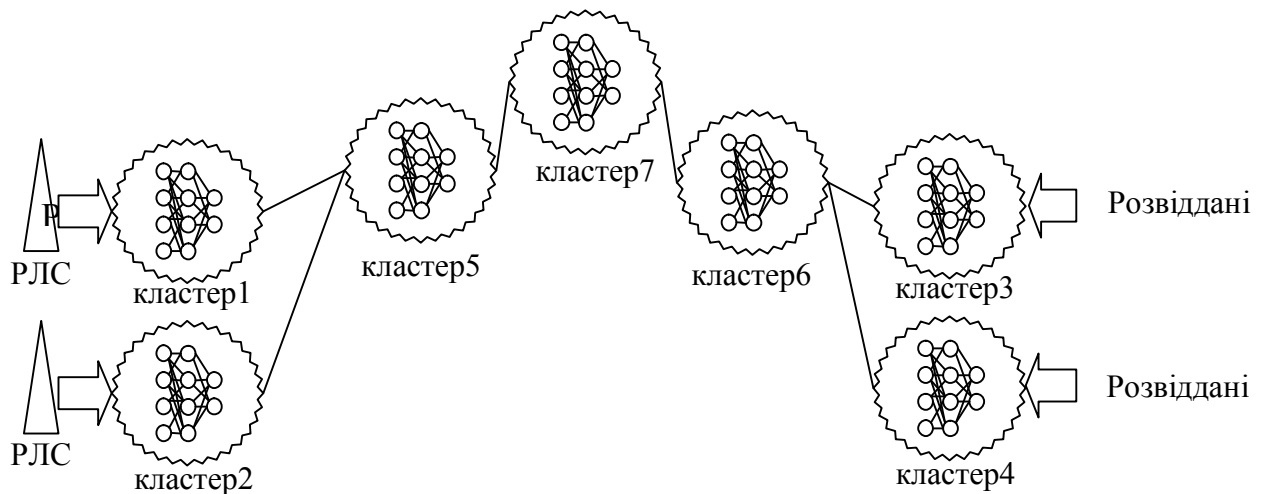


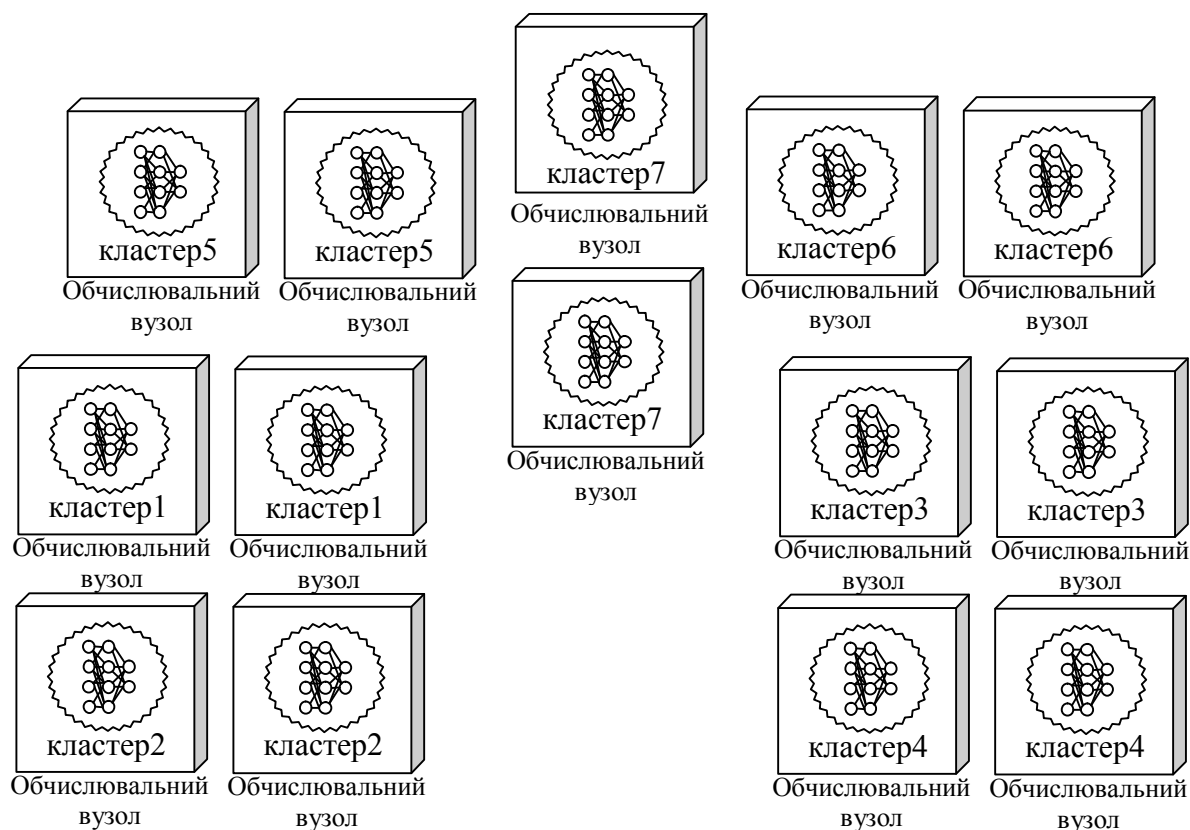
Рис. 1. Приклад системи сприяння прийняттю рішень про атаку противника на рівні країни

**Огляд останніх досліджень.** Динамічна кластеризація штучних нейронних мереж є перспективним напрямком їх розвитку в інтернет-середовищі [1]. Розроблено різні методи розвитку мереж: гравітаційний [2] та зростання з урахуванням обмежень. Також запропоновано використання інтерфейсів ВЕБ-сервісів для побудови розподіленої системи [3].

**Формування завдання дослідження.** Забезпечення захисту від різноманітних перебоїв у кластеризованих штучних нейронних мережах є необхідним завданням для їх існування та практичного використання в інтернет-середовищі. Тому необхідним є вивчення різних існуючих методів захисту та пристосування їх до існуючої проблематики.

Базуючись на попередніх дослідженнях [1 – 3], у статті розглянуто методи: „дзеркало” та „перехресне” резервування.

**Виклад основного матеріалу.** Розглянемо два методи резервування кластерів штучних нейронних мереж. Основна ідея першого методу „дзеркало” аналогічна резервуванню жорстких дисків за технологію „дзеркало”, відомою як RAID 1 (Redundant Array of Independent/inexpensive Disks). Для кожного кластера створюється повна копія на іншому обчислювальному вузлі (рис. 2). Окремий обчислювальний вузол відповідає за роботу окремого кластера штучної нейронної мережі.



*Рис. 2. Схема архітектури методу резервування „дзеркало”*

Позитивними якостями цього методу є висока швидкість перемикавання при виникненні перебою в обчислювальному вузлі. Проте він потребує додаткових обчислювальних потужностей, що значно відобразиться на вартості всього комплексу. Якщо створювати лише дзеркало за функціоналом, а не копіювати штучну нейронну мережу з одного обчислювального вузла на інший, тобто дозволити навчатися декільком кластерам на різних вузлах паралельно однієї функції, то є можливість підвищити точність отриманих результатів, використовуючи мажоритарні принципи у прийнятті рішень.

Другий метод – „перехресне” резервування (рис. 3) дозволяє забезпечувати захист кластерів на існуючому обладнанні. Протягом навчання робиться копія кластера, яка відсилається до іншого обчислювального вузла, де зберігається на жорсткому диску й у разі потреби розгортається на поточному вузлі.

Метод „перехресного” резервування дозволяє зменшити вартість комплексу порівняно з „дзеркалом”, але у разі його використання потрібно пересилати більші обсяги інформації – дані + опис кластера.

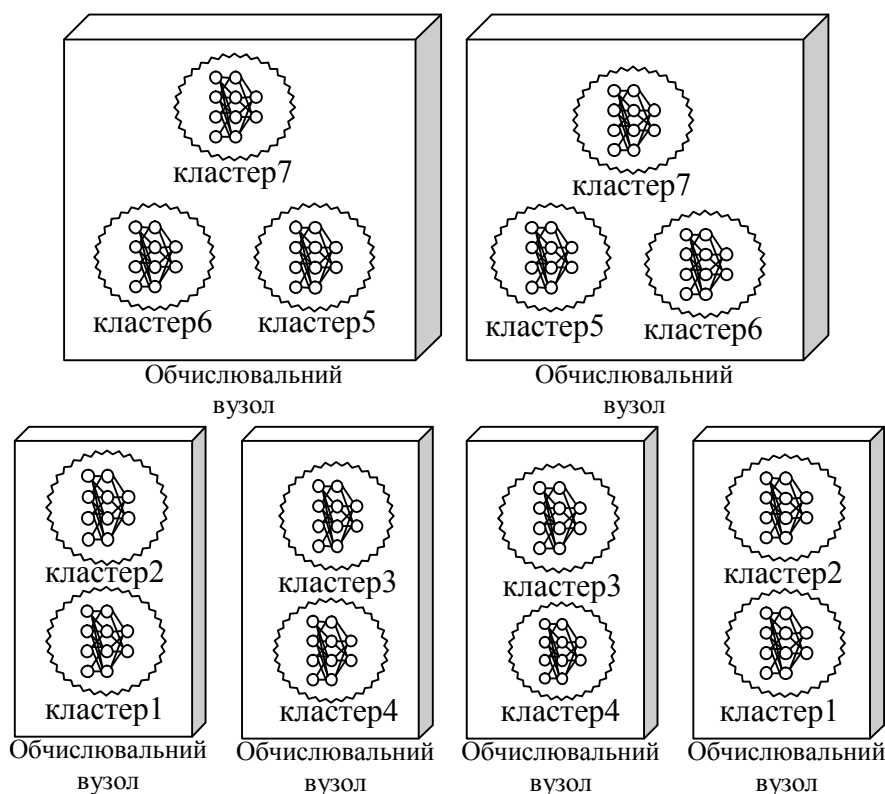


Рис. 3. Схема архітектури „перехресного” методу резервування

Для існування в інтернет-середовищі зв'язок між кластерами організовано з використанням технології ВЕБ-сервісів [3]. Для підвищення рівня захисту інформації ця технологія не передбачає можливість кодованої передачі даних з використанням протоколу HTTPS (Hyper Text Transfer Protocol Secured) (рис. 4).

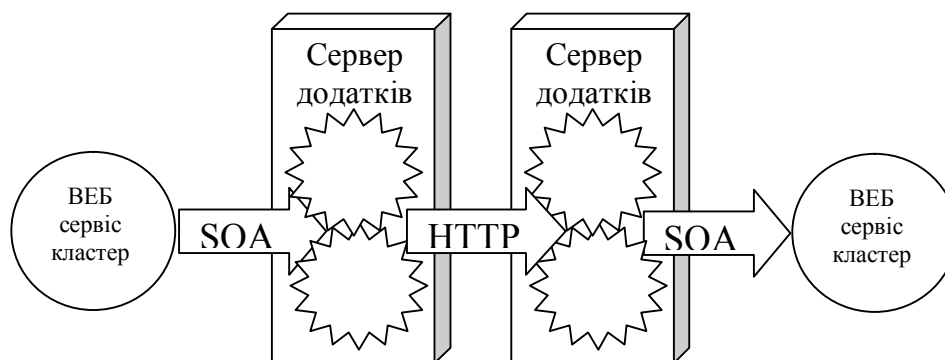


Рис. 4. Схема використання HTTPS для кодованого зв'язку між ВЕБ-сервісами

Варіант використання протоколу HTTPS є стандартним рішенням для ВЕБ-сервісів. Він дозволяє користуватися лише стандартними можливостями серверів додатків, тобто не потрібно додаткового обладнання або програмного забезпечення.

Інший варіант захисту інформації – побудова захищеної віртуальної інтранет-мережі з використанням технології VPN (Virtual Private Network) (рис. 5).

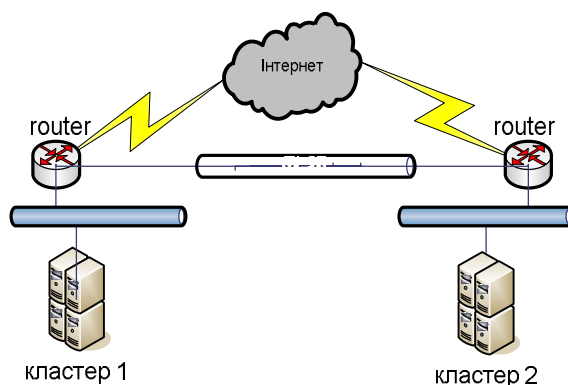


Рис. 5. Схема організації інтранет-мережі на базі VPN

Для створення віртуальної мережі існує можливість використання програмного забезпечення, але більш якісним варіантом є використання спеціалізованого апаратного забезпечення, наприклад, маршрутизаторів (router). Це обладнання включає до свого складу спеціальні апаратні VPN прискорювачі, що дозволяє швидше формувати кодовані пакети даних на передачу.

**Висновки.** Для побудови захищених від перебоїв динамічно кластеризованих штучних нейронних мереж можна використовувати стандартні методи захисту „дзеркало” та „перехресний”, які розглянуто у статті. Крім того, можлива розробка специфічних методів, що дозволять більш ефективно використовувати можливості штучних нейронних мереж, але вони потребують додаткових досліджень та перевірки.

#### СПИСОК ЛІТЕРАТУРИ

1. Жуков І. А. Динамічна просторово-логічна кластеризація нейронної мережі / І. А. Жуков, Г. М. Кременецький // Інформаційні технології та комп'ютерна інженерія. – Вінниця: ВНТУ. – 2009. – Вип. 1(14). – С. 39 – 43.
2. Кременецький Г. М. Гравітаційний метод динамічної кластеризації нейронної мережі / Г. М. Кременецький, С. В. Журавель // Проблеми інформатизації та управління : зб. наук. праць. – К. : НАУ. – 2009. – Вип. 1 (25). – С. 86 – 89.
3. Кременецький Г. М. Побудова динамічної кластерної нейронної мережі з використанням WEB-сервісів / Г. М. Кременецький // Проблеми інформатизації та управління: зб. наук. праць. – К. : НАУ. – 2009. – Вип. 2 (26). – С.76 – 81.

Подано 15.10.09

**И. А. Жуков, Г. Н. Кременецкий**

#### **ЗАЩИТА ОТ СБОЕВ ДИНАМИЧЕСКИ КЛАСТЕРИЗУЕМЫХ ИСКУССТВЕННЫХ НЕЙРОННЫХ СЕТЕЙ**

*В статье рассмотрены методы построения защищенных от сбоев динамически кластеризуемых искусственных нейронных сетей. Предложены разные архитектуры защиты от сбоев в среде Интернет.*

**I. A. Zhukov, G. M. Kremenetsky**

#### **PROTECTING FROM IRREGULARITY OF DYNAMICALLY KLASTERED ARTIFICIAL NEURON NETWORKS**

*This article describes fault tolerance methods for the dynamic clustering artificial neural networks. In this article proposed different fault tolerance architectures in Internet environment.*