УДК 004.7(045)

Г.М. Кременецький, Є.Б. Артамонов
Національний авіаційний університет

ЗАХИСТ ВІД ЗБОЇВ СПЕЦІАЛІЗОВАНИХ МЕРЕЖ, ЩО ДИНАМІЧНО КЛАСТЕРИЗУЮТЬСЯ

Розглянуто методи побудови захищених від збоїв спеціалізованих мереж, що динамічно кластеризуються. Запропоновано різні архітектури захисту від збоїв у Інтернет-середовищі.

Ключові слова: динамічна кластеризація, кластер, метод резервування "дзеркало", "перехресний" метод резервування, штучна нейронна мережа.

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

Key words: dynamic clustering, cluster, method backup "mirror", "cross" method of redundancy, an artificial neural network.

Вступ

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 у мережевому середовищі, зокрема в Інтернеті. Основною потребою у їх використанні є розподіл даних у просторі та ієрархічність прийняття рішень. Наприклад, якщо погодні дані збирають у різних куточках країни, то попередній аналіз логічно проводити на місці, та підготовлені результати, обсяг яких буде менш ніж необроблений, передавати до вищого рівня для подальшої обробки (рис. 1). На вищому рівні, де зібрано дані з радарів та інших джерел, буде створено загальний прогноз погоди.

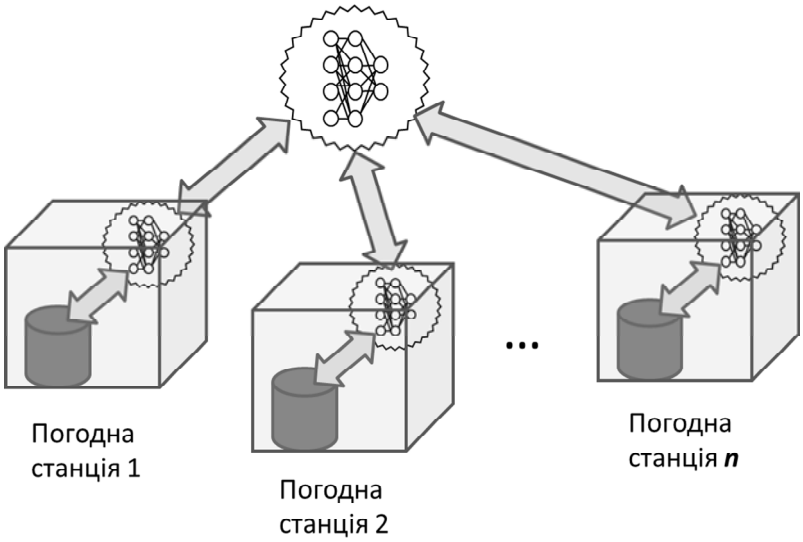

Рис. 1. Приклад системи прогнозування погоди

Огляд останніх досліджень

Динамічна кластеризація штучних нейронних мереж є перспективним напрямком розвитку штучних нейронних мереж в Інтернет-середовищі [1]. Розроблено різні методи розвитку мереж:

гравітаційний [2] та методи зростання з урахуванням обмежень. Також запропоновано використання інтерфейсів ВЕБ-сервісів для побудови розподіленої системи [3].

Завдання дослідження

Забезпечення захисту від різноманітних збоїв у кластеризованих штучних нейронних мережах є необхідним завданням для їх існування та практичного використання у Інтернет-середовищі. Тому потрібно вивчити різні існуючі методи захисту та пристосування їх до існуючої проблематики. Ґрунтуючись на попередніх дослідженнях [1, 2, 3], у роботі розглянуто методи: “дзеркало” та “перехресного” резервування.

Результати дослідження

Розглянемо два методи резервування кластерів штучних нейронних мереж. Перший метод – “дзеркало”. Основна ідея цього методу аналогічна до резервування жорстких дисків за технологію “дзеркало” відому, як RAID 1 (Redundant Array of Independent/inexpensive Disks). Для кожного кластера створюється повна копія на іншому обчислювальному вузлі (рис. 2). Кожен окремий обчислювальний вузол відповідає за роботу окремого кластера штучної нейронної мережі.

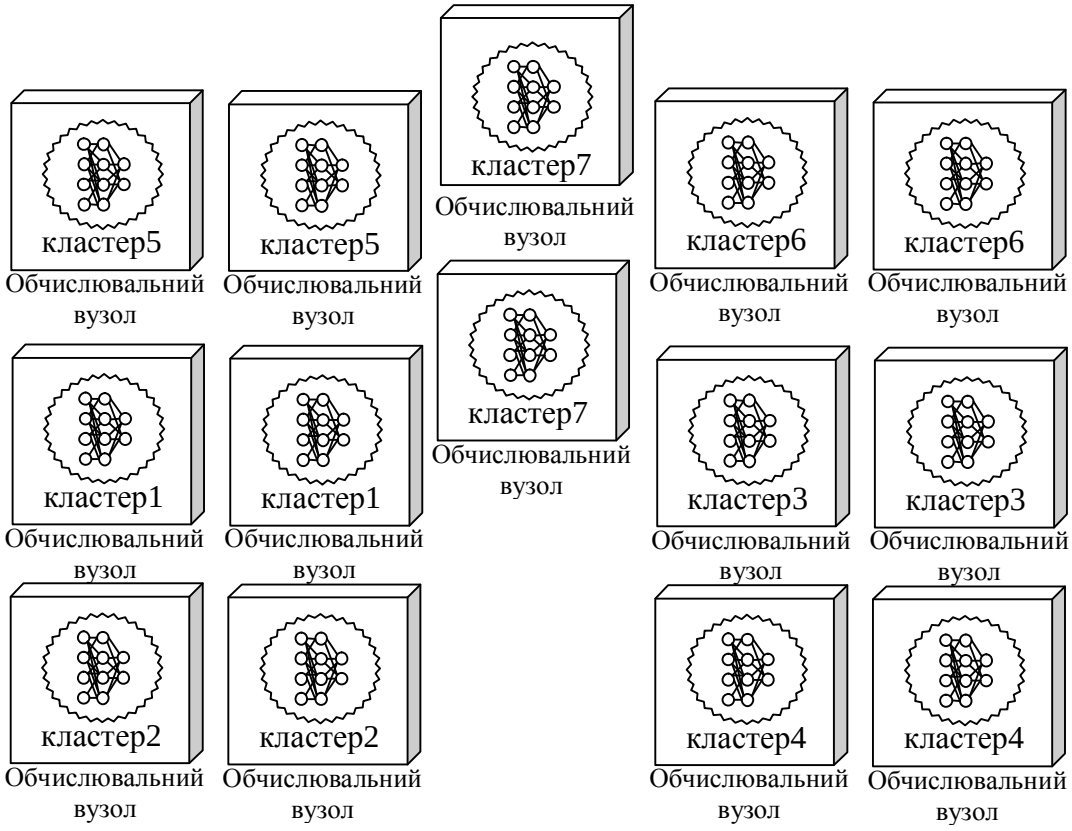

Рис. 2. Схема архітектури методу резервування “дзеркало”

Позитивними якостями цього методу є висока швидкість перемикання під час виникнення збою у обчислювальному вузлі. Цей метод потребує додаткових обчислювальних потужностей, що значно відобразиться на вартості усього комплексу. Якщо створювати лише дзеркало за функціоналом, а не копіювати штучну нейронну мережу з одного обчислювального вузла на інший, тобто дати змогу навчатися кількома кластерам на різних вузлах паралельно однієї функції, то є можливість підвищити точність отриманих результатів, використовуючи мажоритарні принципи у прийнятті рішень.

Другий метод – метод “перехресного” резервування (рис. 3) дає змогу забезпечувати захист кластерів на існуючому обладнанні. Упродовж навчання робиться копія кластера. Ця копія відсилається до іншого обчислювального вузла, де зберігається на жорсткому диску, і у разі потреби розгортається на поточному вузлі.

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

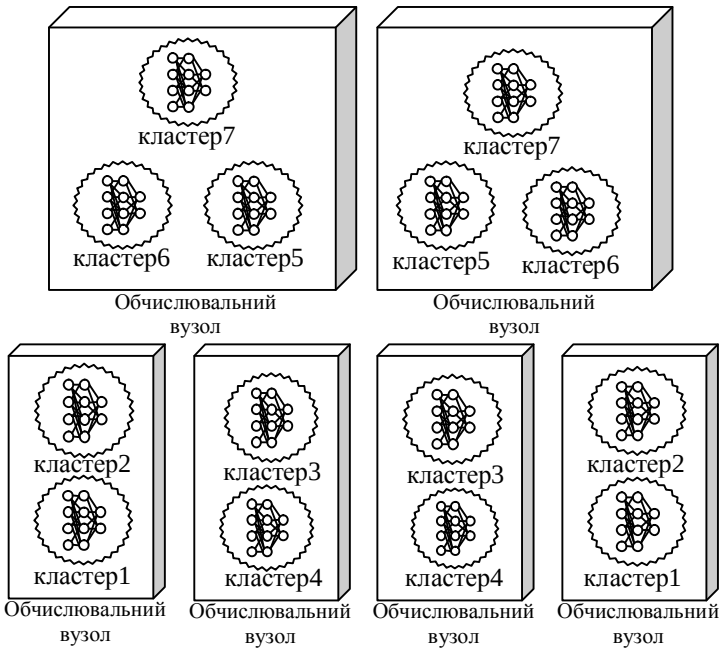

Рис. 3. Схема архітектури “перехресного” методу резервування

Метод “гібридного”, або часткового резервування інтегрує позитивні якості обох методів. У разі необхідності (важливості ділянки або слабих каналів зв’язку) можна використовувати метод “дзеркало”, а в інших випадках – метод “перехресного” резервування.

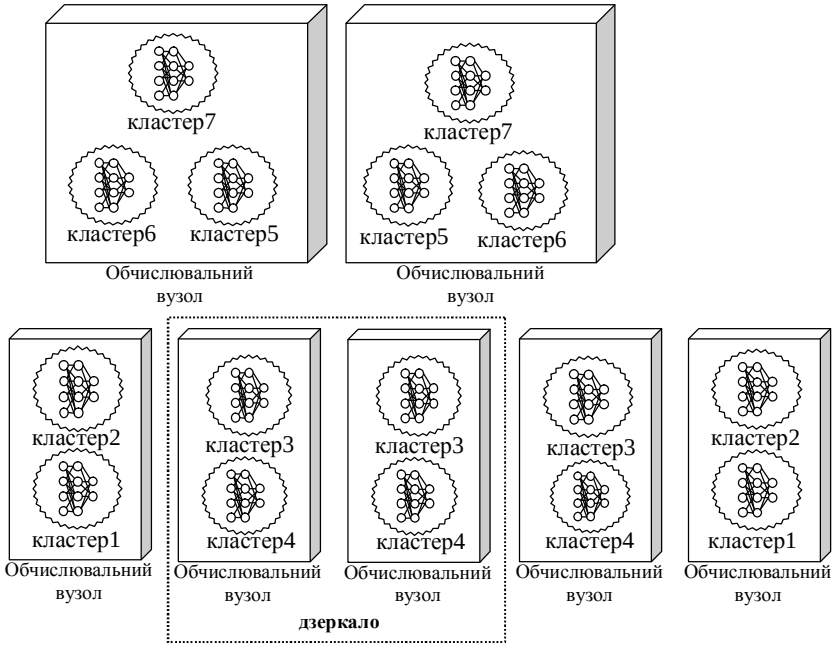

Рис. 4. Схема архітектури “гібридного” методу резервування

Для існування в Інтернет-середовищі зв'язок між кластерами організовано з використанням технології ВЕБ-сервісів [3]. Для підвищення рівня захисту інформації у технології ВЕБ-сервісів існує можливість кодованої передачі даних з використанням протоколу HTTPS (Hyper Text Transfer Protocol Secured) (рис. 5).

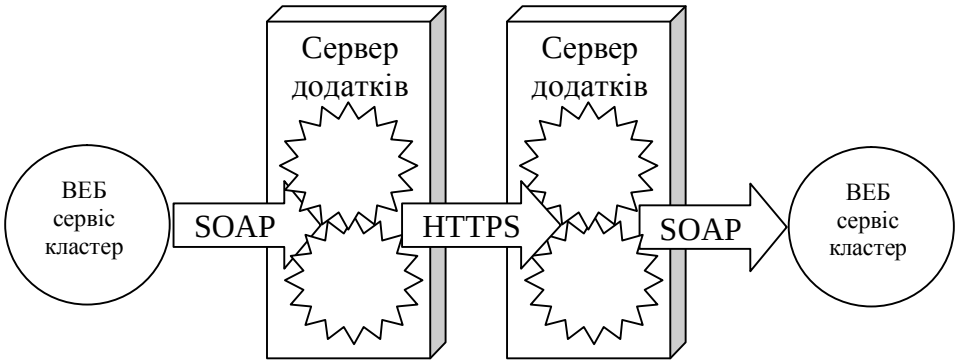

Рис. 5. Схема використання HTTPS для кодованого зв'язку між ВЕБ-сервісами

Варіант використання протоколу HTTPS є стандартним рішенням для ВЕБ-сервісів. Цей варіант дає змогу 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. 6).

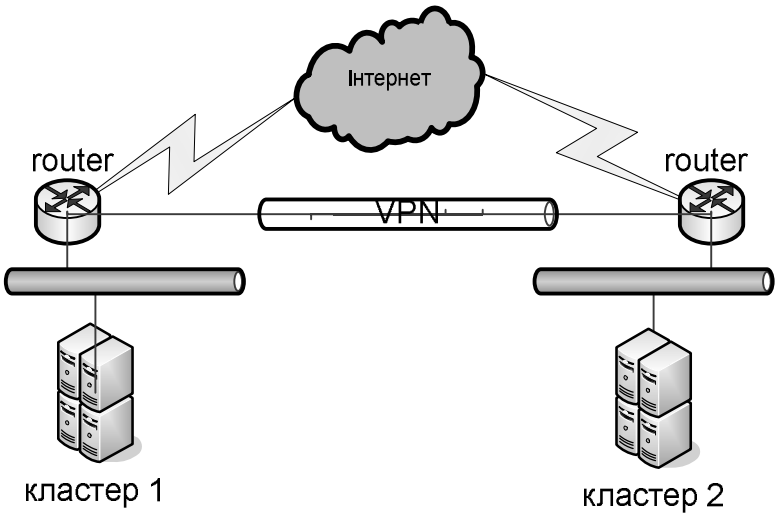

Рис. 6. Схема організації Інтранет-мережі на основі VPN

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

Висновки

Для побудови захищених від збоїв динамічно кластериних штучних нейронних мереж можна використовувати стандартні методи захисту "дзеркало" та "перехресний", які розглянуто у роботі. Крім того, можна розробити специфічні методи, що дають змогу ефективніше використовувати можливості штучних нейронних мереж, але ці методи потребують додаткових досліджень та перевірки.

До специфічних методів можна зарахувати метод “гібридного”, або часткового резервування. Цей метод передбачає захист як методом “дзеркало”, так і “перехресним” методом. У разі необхідності (важливості ділянки або слабких каналів зв’язку) використовується метод “дзеркало”, а в інших випадках – метод “перехресного” резервування.

Окремо можна відзначити можливість використання Web-сервісів для побудови динамічно кластерної нейронної мережі, що дають змогу легко, та не відходячи від об’єктної моделі, організовувати різноманітні конфігурації нейронної мережі. Також Web-сервіси дають можливість зберігати створений код за зміни структури мережі. Потрібно буде лише змінити відповідні файли налаштування.

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

УДК 004.056

С.М. Кущ, В.О. Шутовський
Національний технічний університет України “Київський політехнічний інститут”

ПОБУДОВА КСЗІ НА ОСНОВІ РЕЗУЛЬТАТІВ ОЦІНКИ РИЗИКІВ ІБ МЕТОДОМ АНАЛІЗУ ГРАФА АТАК

Запропоновано методику побудови КСЗІ ІС на основі результатів оцінки ризиків ІБ методом аналізу графа атак. Здійснено програмну реалізацію цієї методики. Наведено результати обчислювальних експериментів.

Ключові слова: інформаційна безпека, оцінка ризиків, комплексні системи захисту інформації, граф атак

The technique of complex information security systems construction is proposed. The technique is based on the results of information security risks assessment using an attack graph. A software solution for the technique was made and computational experiments were carried out.

Key words: information security, risks assessment, complex information security systems, attack graph

Вступ

Сучасна парадигма інформаційної безпеки (ІБ) приймає ризик-орієнтований підхід як стандартний підхід під час розроблення комплексних систем захисту інформації (КСЗІ) [1, 2], що уможливлює провести обґрунтоване конфігурування системи захисту інформаційної системи (ІС).

Мета роботи – побудувати КСЗІ ІС на основі результатів оцінки ризиків ІБ системи, отриманих методом аналізу графа атак.

Оцінка ризиків ІБ ІС методом аналізу графа атак з нечіткими ваговими коефіцієнтами

Для оцінки ризиків ІБ ІС сьогодні запропоновано велику кількість методик. Ці методики можна розділити на якісні, напівкількісні та кількісні. Особливий інтерес являють собою кількісні