НАПРЯМ 9. МІЖДИСЦИПЛІНАРНИЙ ПІДХІД В ІТ-ТЕХНОЛОГІЯХ ДЛЯ ВІДНОВЛЕННЯ ТА РОЗВИТКУ УКРАЇНИ ЧЕРЕЗ ІННОВАЦІЙНІ СТРАТЕГІЇ ТА ПРАКТИЧНІ РІШЕННЯ

DOI https://doi.org/10.36059/978-966-397-614-3-2-30

МОДЕЛЮВАННЯ БЕЗПЕКИ НЕЧІТКИХ СИСТЕМ УПРАВЛІННЯ БАЗАМИ ДАНИХ НА ОСНОВІ LSTM

Григор'єва Т. І.
кандидат технічних наук, доцент,
завідувачка кафедри інформаційних технологій
Міжнародний університет
м. Одеса, Україна

Мельник В. В.
здобувач вищої освіти ступеня доктора філософії
спеціальності F5 – Кібербезпека та захист інформації
факультету кібербезпеки, програмної інженерії
та комп'ютерних наук
Міжнародний університет
м. Одеса, Україна

Сучасні системи управління базами даних є важливою складовою інформаційних систем та потребують ефективного захисту від кіберзагроз, несанкціонованого доступу й витоку інформації. Традиційні методи забезпечення безпеки базуються на детермінованих алгоритмах і чітких правилах контролю доступу, однак вони не завжди ефективні в умовах невизначеності та змінної поведінки користувачів [1, с. 2].

Одним із перспективних напрямів підвищення рівня інформаційної безпеки є використання нечіткої логіки, яка дозволяє працювати з неповними та нечіткими даними, оцінювати рівень ризику та формувати адаптивні механізми захисту. Для аналізу часових послідовностей подій та прогнозування поведінки користувачів доцільним є застосування рекурентних нейронних мереж типу LSTM (Long Short-Term Memory), здатних виявляти приховані закономірності у процесах функціонування системи [2, с. 22819].

Поєднання нечіткої логіки та LSTM-моделей забезпечує можливість створення інтелектуальних систем безпеки, які адаптуються до змін інформаційного середовища та дозволяють ефективно визначати рівень довіри користувачів і виявляти аномальну активність.

Метою роботи є дослідження особливостей моделювання безпеки нечітких систем управління базами даних на основі LSTM та аналіз можливостей використання цього підходу для підвищення ефективності захисту інформації.

Сучасні системи управління базами даних функціонують у складних умовах, де значна частина параметрів безпеки має нечіткий характер. Поведінка користувачів, інтенсивність запитів, рівень ризику або ступінь підозрілої активності не можуть бути описані виключно за допомогою чітких числових значень. У таких умовах використання лише детермінованих алгоритмів контролю доступу є недостатнім, оскільки вони не враховують невизначеність та змінність поведінкових характеристик. Для розв'язання цієї проблеми доцільним є поєднання нечіткої логіки та рекурентних нейронних мереж типу LSTM. Нечітка логіка забезпечує можливість роботи з лінгвістичними змінними, такими як «низький рівень довіри», «середній ризик» або «висока підозрілість», а LSTM-модель дозволяє аналізувати послідовності подій та виявляти приховані закономірності у поведінці користувачів.

Архітектура LSTM належить до рекурентних нейронних мереж та спеціально призначена для аналізу часових рядів і послідовностей даних. Основною особливістю LSTM є наявність механізму пам'яті, що дозволяє зберігати інформацію про попередні стани системи протягом тривалого часу. Це особливо важливо у задачах інформаційної безпеки, де аналіз окремої події без урахування попередньої поведінки користувача не завжди дозволяє коректно визначити рівень загрози. У запропонованій моделі LSTM використовується для прогнозування рівня довіри на основі часових послідовностей подій безпеки. Вхідними параметрами можуть бути кількість SQL-запитів, частота звернень до критичних таблиць, кількість невдалих спроб автентифікації, часові характеристики активності користувача, рівень зміни привілеїв та інші показники. На основі отриманих даних система формує нечіткі оцінки ризику. Для цього використовується функція належності нечітких множин $\mu_A \epsilon [0;1]$, яка визначає ступінь належності параметра безпеки до певної нечіткої множини A. Наприклад, значення рівня активності користувача може одночасно частково належати до множин «нормальна активність» та «підозріла активність».

Адаптивний поріг довіри LSTM-моделі визначимо наступним чином:

$$T = \sum_{i=1}^{n} \omega_i P_i - k\sigma \quad (1)$$

де T – поріг довіри, P_i – прогнозоване значення довіри для окремої події, n – кількість проаналізованих подій, k – коефіцієнт нечіткості,

σ – середньоквадратичне відхилення прогнозованих значень довіри, яке дозволяє врахувати "шум" та нестабільність роботи мережі LSTM, ω_i – ваговий коефіцієнт релевантності події.

Коефіцієнт нечіткості – це параметр, який буде визначатися нечіткою системою. Наприклад, якщо загальний стан системи визначено як "тривожний", то k збільшується, роблячи поріг T жорсткішим.

Такий метод обчислення адаптивного порогу довіри базується на поєднанні методу EWMA (Exponentially Weighted Moving Average) та статистичного правила відхилень [2, с. 22820]. Формула (1) є узагальненою математичною моделлю, що використовується в задачах статистичного контролю процесів та динамічного оцінювання довіри.

Якщо отримане значення довіри стає нижчим за допустимий поріг, система автоматично активує механізми захисту: додаткову автентифікацію, блокування доступу або сповіщення адміністратора системи. Завдяки використанню LSTM-моделі система здатна враховувати довгострокові залежності між подіями та адаптуватися до змін поведінки користувачів.

Перевагою запропонованого підходу є поєднання здатності LSTM до аналізу часових послідовностей із можливостями нечіткої логіки працювати з невизначеними та неповними даними. Це дозволяє значно підвищити точність виявлення аномалій, зменшити кількість помилкових спрацювань та забезпечити адаптивність системи безпеки.

Таким чином, використання методу LSTM для визначення порогу довіри у нечітких системах управління базами даних забезпечує ефективне моделювання процесів безпеки в умовах невизначеності та динамічності інформаційного середовища. Перспективним напрямом подальших досліджень є інтеграція LSTM-моделей із методами глибинного навчання, нечіткими нейронними мережами та системами штучного інтелекту для побудови інтелектуальних адаптивних систем захисту інформації нового покоління.

Література:

1. Abdulla H. S., Aladdin A. M. Enhancing Design and Authentication Performance Model: A Multilevel Secure Database Management System. *Future Internet*. 2025. Vol. 17, no. 2. Art. 74. DOI: https://doi.org/10.3390/fi17020074.

2. An Improved LSTM-Based Prediction Approach for Resources and Workload in Large-Scale Data Centers / H. Yuan, J. Bi, S. Li et al. *IEEE Internet of Things Journal*. 2024. Vol. 11, no. 12. P. 22816–22829. DOI: 10.1109/JIOT.2024.3383512.