МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

«ПОЛТАВСЬКА ПОЛІТЕХНІКА ІМЕНІ ЮРІЯ КОНДРАТЮКА»

ЗБІРНИК НАУКОВИХ ПРАЦЬ

за матеріалами XI Всеукраїнської науково-практичної конференції

«ЕЛЕКТРОННІ ТА МЕХАТРОННІ СИСТЕМИ:

ТЕОРІЯ, ІННОВАЦІЇ, ПРАКТИКА»

18 грудня 2025 року

Полтава 2025

УДК 004.021:004.89:004.056.5

Є. Живило, *к.держ.упр., доцент*
Національний університет «Полтавська політехніка імені Юрія Кондратюка»

АДАПТИВНА СИСТЕМА ВИЯВЛЕННЯ АНОМАЛІЙ У КІБЕРФІЗИЧНИХ СИСТЕМАХ НА ОСНОВІ ГІБРИДНИХ HNN-МОДЕЛЕЙ

Сучасні кіберфізичні та інформаційно-комунікаційні системи характеризуються зростанням складності та варіабельності інформаційних потоків, що призводить до появи нових класів кіберзагроз і форм аномальної поведінки які істотно ускладнють їх своєчасне виявлення. Класичні статистичні та детерміновані методи аналізу виявляються малоефективними в умовах динамічної зміни профілю атак, обмеженості апріорних знань і високого рівня завад. У зв'язку з цим актуальною є розробка адаптивних інтелектуальних систем виявлення аномалій, здатних до самонавчання та роботи в режимі реального часу.

В дослідженні представлено математичну модель адаптивної системи виявлення аномалій, побудовану на основі гібридних нейромережних архітектур, які поєднують методи глибокого навчання, стохастичного аналізу та ймовірнісного моделювання. Модель формалізує процес самоналаштування системи за допомогою узагальненого функціонала втрат із динамічними ваговими коефіцієнтами, що коригуються відповідно до змін поведінкових характеристик вхідних даних.

У запропонованій роботі адаптаційний механізм формалізовано як систему диференціальних рівнянь, що забезпечує аналітичну оцінку збіжності процесу навчання та стійкості моделі в умовах флуктуацій інформаційного середовища. Так для підвищення точності виявлення аномалій застосовано градієнтно-ентропійні методи оптимізації, а також байєсівський підхід до оцінювання невизначеностей, що забезпечує формування імовірнісних оцінок ризику та підвищує робастність системи.

Проаналізовано ефективність гібридних архітектур на основі комбінацій LSTM-Autoencoder, CNN та Transformer-моделей для обробки потокових даних у реальному часі. Важливо наголосити, що застосований адаптивний механізм превентивного реагування дозволяє не лише виявляти аномалії, а й прогнозувати їх появу та ініціювати запобіжні дії, що є вирішальним для захисту критичної інформаційної інфраструктури.

Отримані результати моделювання свідчать про перевагу запропонованої системи над класичними автоенкодерними та рекурентними підходами за показниками точності, швидкодії та стійкості до зміни типів загроз. Розроблена математична модель може бути використана як науково обґрунтована основа для створення інтелектуальних систем кіберзахисту

нового покоління, здатних до автономного функціонування та адаптації у динамічному інформаційному середовищі.

ЛІТЕРАТУРА:

1. National Institute of Standards and Technology (NIST). (2024). Cybersecurity Framework (CSF) 2.0. NIST CSWP 29. Retrieved from: https://doi.org/10.6028/NIST.CSWP.29.

2. 2. European Union Agency for Cybersecurity (ENISA). (2024). ENISA Threat Landscape 2024. Retrieved from: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024.

3. 3. NIST. (2018). Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1).

4. URL: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

ADAPTIVE SYSTEM FOR ANOMALY DETECTION IN CYBER-PHYSICAL SYSTEMS BASED ON HYBRID HNN MODELS

Y. Zhyvylo, *Candidate of Sciences in Public Administration, Associate Professor National University "Yuri Kondratyuk Poltava Polytechnic"*