Міністерство внутрішніх справ України
Харківський національний університет внутрішніх справ
Національна академія правових наук України
Організація з безпеки та співробітництва в Європі

ОБСЄ Організація з безпеки та співробітництва в Європі

БЕЗПЕКА У КІБЕРСФЕРІ

Збірник матеріалів
Міжнародної науково-практичної конференції
(м. Кам’янець-Подільський, 28 травня 2025 року)

Кам’янець-Подільський 2025

УДК [351.74:004](477)(08)
Б39

Друкується згідно з рішенням оргкомітету
за дорученням Харківського національного університету внутрішніх
справ від 26.02.2025 № 19

Б39 **Безпека** у кіберсфері : зб. матеріалів Міжнарод. наук.-практ. конф. (м. Кам'янець-Подільський, 28 трав. 2025 р.) / МВС України, Харків. нац. ун-т внутр. справ ; Нац. акад. правових наук України ; Організація з безпеки та співробітництва в Європі. – Кам'янець-Подільський : ХНУВС, 2025. – 246 с.

У матеріалах конференції окреслено найбільш актуальні проблеми безпеки у кіберсфері на сучасному етапі; проаналізовано окремі питання правового та організаційного забезпечення безпеки у кіберсфері; використання інформаційних технологій і технічних засобів у протидії правопорушенням; забезпечення кібербезпеки на об'єктах інформаційної діяльності; інформаційної безпеки суспільства та держави.

УДК [351.74:004](477)(08)

Матеріали викладено в авторській редакції з незначними коректорськими правками.
За достовірність наукового матеріалу, професійного формулювання,
фактичних даних, цитат, власних назв, географічних назв,
а також за розголошення фактів, що не належать відкритому друку, тощо
відповідають автори публікацій та їх наукові керівники.
Електронна копія збірника розміщується
у відкритому доступі на сайті Харківського національного
університету внутрішніх справ (http://www.univd.edu.ua) у розділі «Наука»,
сторінка «Конференції, семінари та круглі столи»,
а також у репозитарії ХНУВС (http://dspace.univd.edu.ua/xmlui/).

окремих систем моніторингу, а й загалом стабільність об'єктів критичної інфраструктури.

Список використаних джерел

1. F. Li *et al*. "Online Distributed IoT Security Monitoring With Multidimensional Streaming Big Data," in *IEEE Internet of Things Journal*, vol. 7, no. 5, pp. 4387-4394, May 2020, doi: 10.1109/JIOT.2019.2962788.

2. Demestichas, K.; Peppes, N.; Alexakis, T. Survey on Security Threats in Agricultural IoT and Smart Farming. *Sensors* 2020, *20*, 6458. https://doi.org/10.3390/s20226458.

Одержано 30.04.2024

УДК 004.056.5+534.8

СЕМЕНОВ Сергій Геннадійович,
доктор технічних наук, професор,
завідувач кафедри комп'ютерної інженерії та кібербезпеки
Університету комісії Національної освіти (Краків, Польща)
https://orcid.org/0000-0003-4472-9234;

ЄНГАЛИЧЕВ Сергій Олександрович,
аспірант Харківського національного
економічного університету ім. Семена Кузнеця
https://orcid.org/0000-0001-5298-2251;

ПЕРЕСІЧАНСЬКИЙ Валерій Миколайович,
старший викладач кафедри кібербезпеки та DATA-технологій
навчально-наукового інституту № 5
Харківського національного університету внутрішніх справ
https://orcid.org/0000-0002-0130-9339

ОБГОВОРЕННЯ РЕЗУЛЬТАТІВ ДОСЛІДЖЕННЯ ІНТЕЛЕКТУАЛЬНОГО МЕТОДУ ПЛАНУВАННЯ ЗАДАЧ У РОЗПОДІЛЕНИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ

У сучасних розподілених інформаційних системах (РІС) проблема ефективного планування задач є однією з ключових, особливо в умовах гетерогенності обчислювальних ресурсів і високої динамічності навантаження. Для вирішення цих викликів у дослідженні було розроблено інтелектуальний метод планування задач, що поєднує класичні графові моделі DAG (Directed Acyclic Graph) і GERT (Graphical Evaluation and Review Technique) із сучасними алгоритмами штучного інтелекту [1, 2].

Запропонований метод інтегрує кілька підходів: прогнозування критичного шляху задач із використанням Graph Attention Network (GAT) [1], динамічне прийняття рішень на основі Proximal Policy Optimization (PPO) [3] та оптимізацію розподілу ресурсів за допомогою Bayesian Optimization. Такий підхід дозволяє враховувати ймовірнісні залежності між задачами, динамічні зміни доступності ресурсів і стохастичний характер середовища виконання.

Результати експериментального моделювання продемонстрували суттєве покращення ключових показників ефективності системи. Середній час виконання

задач було знижено з 51.5 до 35.2 секунд, що свідчить про значне підвищення швидкості обробки запитів. Крім того, стандартне відхилення навантаження між обчислювальними вузлами зменшилося з 0.47 до 0.22, що вказує на якісніше балансування ресурсів у системі. Це стало можливим завдяки здатності моделі адаптивно реагувати на зміни в навколишньому середовищі та самонавчатися на основі накопичених даних.

Використання GERT-графів для моделювання залежностей між задачами дозволило забезпечити наявність альтернативних маршрутів виконання у випадках виникнення збоїв або затримок, а компоненти машинного навчання сприяли підвищенню стійкості планування. На відміну від традиційних методів, запропонована модель враховує стохастичність процесів та мінливість середовища, що особливо важливо для хмарних інфраструктур та IoT-систем.

Таким чином, результати дослідження підтверджують ефективність запропонованого інтелектуального методу планування задач у гетерогенних розподілених системах. Розроблений підхід демонструє високу гнучкість, масштабованість і стійкість, що відкриває широкі перспективи його застосування в критичних сферах обробки великих даних, керування автономними системами та оптимізації хмарних обчислень.

Список використаних джерел

1. Semenov, S., Zhang, L., Cao, W., Bulba, S., Babenko, V., & Davydov, V. (2021). Development of a fuzzy GERT-model for investigating common software vulnerabilities. Eastern-European Journal of Enterprise Technologies, 6(2 (114), 6–18. https://doi.org/10.15587/1729-4061.2021.243715

2. Moskalenko, V.; Kharchenko, V.; Semenov, S. Model and Method for Providing Resilience to Resource-Constrained AI-System. Sensors 2024, 24, 5951. https://doi.org/10.3390/s24185951

3. Meleshko, Y., Raskin, L., Semenov, S., & Sira, O. (2019). Methodology of probabilistic analysis of state dynamics of multidimensional semiMarkov dynamic systems. Eastern-European Journal of Enterprise Technologies, 6(4 (102), 6–13. https://doi.org/10.15587/1729-4061.2019.184637.

Одержано 30.04.2025