МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

МІЖНАРОДНИЙ УНІВЕРСИТЕТ

МІЖНАРОДНА КОНФЕРЕНЦІЯ

ПЕРЕДОВІ ТЕХНОЛОГІЇ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНІЙ ІНЖЕНЕРІЇ

(ПТІКІ'2026)

Одеса, Україна, 16 липня 2026 р.

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

МІЖНАРОДНИЙ УНІВЕРСИТЕТ

ПЕРЕДОВІ ТЕХНОЛОГІЇ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНІЙ ІНЖЕНЕРІЇ (ПТІКІ'2026)

Матеріали

IV Міжнародної конференції

16 липня 2026 р.

Одеса - 2026

УДК 004.9
П 27

Проведення заходу зареєстровано в Державній науковій установі «Український інститут науково-технічної експертизи та інформації» (Реєстраційний номер: 3326U000765 від 01-07-2026 р.).

Рецензенти:
Надія КАЗАКОВА – д.т.н., професор, завідувач кафедри інформаційних технологій Одеського національного університету ім. І.І. Мечнікова
Віктор СТРЕЛЬБИЦЬКИЙ – к.т.н., доцент, доцент кафедри підйомно-транспортні машини та інжиніринг портового технологічного обладнання Одеського національного морського університету

Передові технології в інформаційно-комунікаційній інженерії (ATICE'2026) : матеріали IV міжнар. конф. (м. Одеса, Україна, 16 липня 2026 р.) / від. за вип.: Н. Пунченко, Д. Розенвассер. Одеса : Міжнар. ун-т, 2026. 149 с. DOI: https://doi.org/10.32837/11300.33747

Advanced Technology in Information and Communication Engineering (ATICE'2026) : proceedings of the IV International conference (Odesa, Ukraine 16 July 2026) / Responsible for the issue: N. Punchenko, D. Rozenvasser. Odesa : International University, 2026. 149 p**.** DOI: https://doi.org/10.32837/11300.33747

У збірнику подано результати наукових досліджень, висвітлено обговорення актуальних проблем, викликів і тенденцій з інформаційних систем, технологій захисту інформації, використання сучасних інформаційних технологій в управлінні системами у різних галузях народного господарства. Матеріали охоплюють інноваційні підходи, досвід упровадження сучасних рішень і приклади успішних практик трансформації різних галузях народного господарства .

Видання призначене для науково-педагогічних працівників, здобувачів освіти, науковців і фахівців ІТ галузі.

Відповідальні за випуск:
к.т.н., доцент Пунченко Наталія,
к.т.н., доцент Розенвассер Денис.

ОРГАНІЗАЦІЙНИЙ КОМІТЕТ

Голова

КІВАЛОВ С.В. – д.ю.н., проф., Міжнародний університет, м.Одеса, Україна.

Співголови

ГРОМОВЕНКО К.В. – д.ю.н., проф., Міжнародний університет, м. Одеса, Україна.
ЛЕФТЕРОВ В.О. – д.п.н., проф., Міжнародний університет, Одеса, Україна
СТРЕЛКОВСЬКА І.В. – д.т.н., проф., Міжнародний університет, Одеса, Україна.
УРИВСЬКИЙ Л.О. – д.т.н., проф., НТУ України "КПІ імені Ігоря Сікорського", Київ, Україна.

Члени організаційного комітету

СОЛОВСЬКА І.М. – к.т.н., доц., Міжнародний університет, Одеса, Україна.
ЙОНА Л.Г. – к.т.н., доц., Міжнародний університет, Одеса, Україна.
ГРИГОР'ЄВА Т.І. – к.т.н., доц., Міжнародний університет, Одеса, Україна.
РУСУ О.П. – к.т.н., доц., Міжнародний університет, Одеса, Україна.
РОЗЕНВАССЕР Д.М. – к.т.н., доц., Міжнародний університет, Одеса, Україна.
ВАКАРЧУК А.О. – к.т.н., доц., Міжнародний університет, Одеса, Україна.
ПУНЧЕНКО Н.О. – к.т.н., доц., Міжнародний університет, Одеса, Україна.
ГРІБОВА В.В. – к.ф.-м.н., доц., Міжнародний університет, Одеса, Україна.

РЕДАКЦІЙНИЙ КОМІТЕТ

СОЛОВСЬКА І.М. – к.т.н., доц., Міжнародний університет, Одеса, Україна.
РОЗЕНВАССЕР Д.М. – к.т.н., доц., Міжнародний університет, Одеса, Україна.
ПУНЧЕНКО Н.О. – к.т.н., доц., Міжнародний університет, Одеса, Україна.

КОМІТЕТ МІЖНАРОДНИХ ЗВ'ЯЗКІВ

СТРЕЛКОВСЬКА І.В. – д.т.н., проф., Міжнародний університет, м.Одеса, Україна.
ГЛОБА Л. С. – д.т.н., проф., Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», м.Київ, Україна.

ВЧЕНИЙ СЕКРЕТАР

ПУНЧЕНКО Н.О. – к.т.н., доц., Міжнародний університет, Одеса, Україна.

ТЕХНІЧНО-ПРОГРАМНИЙ КОМІТЕТ

СТРЕЛКОВСЬКА І.В. – д.т.н., проф., Міжнародний університет, м.Одеса, Україна.
УРИВСЬКИЙ Л.О. – д.т.н., проф., Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», м.Київ, Україна.
ГЛОБА Л.С. – д.т.н., проф., Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», м.Київ, Україна.

ЗМІСТ

управління, навігації та зв'язку. 2024. № 2. С. 90-94. doi: 10.26906/SUNZ.2024.2.090
3. Квасніков В. П., Олійник О. В. Особливості застосування гетерогенних обчислювальних структур для задач машинного навчання. *Системи управління, навігації та зв'язку*, 2022. Вип. 3(69). С. 45–49.
4. Оптимізація процесу навчання штучних нейронних мереж / О. О. Безсонов, О. Г. Руденко, К. Олійник, О. Романюк // Інформаційні системи та технології : матеріали 9-ї Міжнар. наук.-техн. конф., 17–20 листопада 2020 р. – Харків : Друкарня Мадрид, 2020. С. 300–302.
5. Brain.js: Some cool AI tools. Now the community carries the torch. GitHub repository. URL: https://github.com/BrainJS/brain.js/blob/master/src/neural-network.ts (дата звернення: 29.06.2026).
6. Goodfellow I., Bengio Y., Courville A. Deep Learning. MIT Press, 2016

УДК 004.052.4:004.85:519.83

DOI: https://doi.org/10.32837/11300.33759

КОМПЛЕКСНИЙ ПІДХІД ДО ВЕРИФІКАЦІЇ КРИТИЧНИХ КОМП'ЮТЕРНИХ СИСТЕМ НА ОСНОВІ МАШИННОГО НАВЧАННЯ, НЕЧІТКОЇ ЛОГІКИ ТА ТЕОРІЇ ІГОР

Григор'єва Т.І., к.т.н., доцент
Салагор В.І., аспірант
Міжнародний університет, місто Одеса
tig15090808@gmail.com
V0634162060@gmail.com

Анотація. *Розглядаються сучасні підходи до верифікації комп'ютерних систем критичного призначення на основі виявлення аномалій та прогнозування збоїв. Запропоновано комплексний підхід, який поєднує прогностичні методи аналізу даних, нечіткі моделі прийняття рішень, технології машинного навчання на базі рекурентних нейронних мереж LSTM та алгоритму Isolation Forest, а також теоретико-ігрові моделі виявлення латентних дефектів. Показано, що інтеграція статистичних, інтелектуальних та теоретико-ігрових методів дозволяє підвищити ефективність верифікації критичного програмного забезпечення, забезпечити раннє виявлення аномалій та зменшити ризик виникнення відмов у процесі функціонування складних комп'ютерних систем.*

Особливого значення набувають задачі верифікації програмного забезпечення, виявлення аномалій та прогнозування можливих відмов ще на ранніх етапах їх виникнення. Традиційні методи контролю переважно орієнтовані на аналіз уже наявних відмов [1], тоді як сучасні умови

вимагають створення інтелектуальних систем прогнозування та діагностики, здатних працювати в умовах невизначеності та динамічної зміни параметрів функціонування системи.

Метою роботи є підвищення ефективності процесів верифікації комп'ютерних систем критичного призначення на основі розроблення комплексних моделей і методів, що поєднують нечіткі моделі прийняття рішень та теоретико-ігрові підходи для виявлення аномалій, латентних дефектів і прогнозування збоїв у процесі функціонування систем.

Пропонується використання прогностичного підходу виявлення аномалій та збоїв, основою якого є аналіз часових рядів параметрів функціонування комп'ютерної системи. Для кожного контрольованого параметра формується часовий ряд, який відображає динаміку зміни стану системи. На основі статистичних характеристик обчислюються математичне сподівання, дисперсія та коефіцієнти варіації. Відхилення фактичних значень від прогнозованих можуть свідчити про появу прихованих аномалій або початок процесу деградації програмного забезпечення.

Використання моделей прогнозування дозволяє не лише фіксувати наявність відхилень, але й оцінювати ймовірність виникнення майбутніх відмов, що суттєво підвищує ефективність процесу верифікації. У процесі верифікації часто виникає ситуація, коли неможливо однозначно визначити поточний стан програмної системи. Для розв'язання цієї проблеми застосовується апарат нечітких множин.

Стан системи описується функцією належності $\mu(x) \in [0;1]$, де значення функції характеризує ступінь відповідності поточного стану системи вимогам надійності. Для прийняття рішень використовується база нечітких правил типу: «Якщо кількість помилок висока та час відгуку перевищує норму, то рівень ризику відмови є високим». На основі механізму нечіткого висновку формується інтегральна оцінка технічного стану програмного забезпечення, що дозволяє враховувати невизначеність і неповноту діагностичної інформації.

Для підвищення точності діагностування запропоновано використання гібридної моделі, яка поєднує нейронні мережі довготривалої короткочасної пам'яті (LSTM), алгоритм Isolation Forest та нечітку логіку. Модель LSTM [2] використовується для прогнозування майбутніх значень параметрів системи та виявлення прихованих тенденцій у часових рядах. Isolation Forest [3] забезпечує автоматичне виявлення аномальних спостережень шляхом аналізу ізольованості об'єктів у просторі ознак. Результати роботи обох моделей надходять до нечіткої системи прийняття рішень, яка формує інтегральний показник ризику:

$$R = \omega_1 R_{LSTM} + \omega_2 R_{IF} + \omega_3 R_{Fuzzy},$$

де R_{LSTM} – оцінка ризику на основі нейронної мережі, R_{IF} – результат роботи Isolation Forest, R_{Fuzzy} – нечітка оцінка ризику, а ω_i – вагові коефіцієнти.

Запропонована гібридна модель дозволяє підвищити точність прогнозування та зменшити кількість хибних спрацювань системи моніторингу.

Для врахування конфліктної взаємодії між потенційним порушником та системою захисту в роботі запропоновано використовувати апарат теорії ігор. У межах побудованої моделі розглядаються два гравці: атакуюча сторона та система моніторингу комп'ютерної мережі. Стан кожного мережевого вузла описується нечіткою функцією належності $\mu_i \in [0;1]$, яка характеризує ступінь дефектності i-го вузла. Значення функції належності відображає рівень відхилення параметрів функціонування вузла від нормального стану та дозволяє враховувати невизначеність і неповноту діагностичної інформації. На основі сукупності отриманих оцінок визначається інтегральний рівень ризику компрометації системи та приймаються рішення щодо необхідності проведення додаткових перевірок.

Для вибору оптимальних стратегій у задачах виявлення латентних дефектів використовується концепція рівноваги Неша у змішаних стратегіях. На відміну від чистих стратегій, за яких кожен учасник обирає лише один варіант поведінки, змішані стратегії передбачають вибір дій відповідно до певного ймовірнісного розподілу. Такий підхід більш адекватно відображає реальні умови функціонування комп'ютерних систем критичного призначення, оскільки поведінка як атакуючої сторони, так і системи захисту характеризується значною невизначеністю та залежить від багатьох зовнішніх факторів.

У межах запропонованої теоретико-ігрової моделі атакуюча сторона формує множину можливих сценаріїв впливу на систему, серед яких розглядаються спроби компрометації окремих вузлів, перевантаження мережевих ресурсів, приховане поширення шкідливого програмного забезпечення та інші види деструктивних дій. Система моніторингу, у свою чергу, обирає стратегії контролю, що включають перевірку критичних компонентів, аналіз мережевого трафіку, посилення механізмів автентифікації, а також раціональний розподіл ресурсів спостереження між окремими сегментами мережі. Оскільки жодна зі сторін не володіє повною інформацією щодо намірів та майбутніх дій опонента, застосування змішаних стратегій є найбільш доцільним підходом до моделювання їхньої поведінки.

Рівновага Неша досягається за таких умов, коли жоден із гравців не може покращити значення власної функції виграшу шляхом односторонньої зміни стратегії за фіксованих стратегій інших учасників

гри. У цьому випадку формується стійкий баланс між можливими діями атакуючої сторони та механізмами протидії системи захисту. Для системи моніторингу це означає оптимальний розподіл обмежених ресурсів контролю між різними напрямами спостереження, тоді як для порушника зменшується можливість прогнозування поведінки системи захисту та вибору найбільш уразливих точок атаки.

Використання змішаних стратегій дозволяє враховувати динамічний характер функціонування мережевого середовища, у якому структура зв'язків, інтенсивність інформаційних потоків та рівень кіберзагроз змінюються в часі. Крім того, такий підхід забезпечує адаптивність системи моніторингу до нових типів атак і невідомих сценаріїв розвитку аномальних процесів. У результаті підвищується ефективність виявлення латентних дефектів, знижується ризик пропуску критичних аномалій та забезпечується більш стійке функціонування комп'ютерних систем критичного призначення в умовах невизначеності та конфліктної взаємодії. Застосування теоретико-ігрового підходу також створює передумови для адаптивного управління ресурсами моніторингу та підвищення ефективності процесів верифікації складних програмно-технічних комплексів.

Висновки. Запропоновано комплексний підхід до верифікації комп'ютерних систем критичного призначення, який поєднує прогностичні методи аналізу даних, нечіткі моделі прийняття рішень, технології машинного навчання та теоретико-ігрові механізми підтримки прийняття рішень. Показано, що використання гібридних моделей на основі LSTM-мереж, алгоритму Isolation Forest та нечіткої логіки сприяє підвищенню точності прогнозування збоїв і ефективності виявлення аномалій. Включення теоретико-ігрових моделей дозволяє враховувати конфліктний характер взаємодії між атакуючою стороною та системою захисту, що є важливою умовою забезпечення функційної безпечності сучасних комп'ютерних систем критичного призначення. Отримані результати можуть бути використані під час розроблення інтелектуальних систем верифікації, моніторингу та підтримки прийняття рішень у складних програмно-технічних комплексах.

Література

1. Zamojski W., Mazurkiewicz J., Sugier J., Walkowiak T., Kacprzyk J. Engineering in Dependability of Computer Systems and Networks. Proc. of the Fourteenth International Conference on Dependability of Computer Systems DepCoS-RELCOMEX (Brunów, Poland July 1–5, 2019). Brunów, Poland, 2019. URL: https://www.springer.com/gp/book/9783030195007.
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.
https://researchwith.njit.edu/en/publications/an-improved-lstm-based-prediction-approach-for-resources-and-work/
3. Liu F. T., Ting K. M., Zhou Z. H. Isolation-based anomaly detection // ACM Transactions on Knowledge Discovery from Data (TKDD). – 2012. – Vol. 6, No. 1. – P. 1–39. https://www.lamda.nju.edu.cn/publication/tkdd11.pdf

УДК 007.52:629.3

DOI: https://doi.org/10.32837/11300.33760

СИСТЕМА АВТОМАТИЗОВАНОГО ПЕРЕВЕЗЕННЯ ВАНТАЖІВ «HEX ROBOT»

Бобуйок Максим Вадимович
здобувач 1 курсу першого (бакалаврського) рівня
факультету кібербезпеки, програмної інженерії та комп'ютерних наук
Міжнародний університет
klekklaks@gmail.com
Павленко Максим Константинович
здобувач 1 курсу першого (бакалаврського) рівня
факультету кібербезпеки, програмної інженерії та комп'ютерних наук
Міжнародний університет
pokkoplo222@gmail.com
Кузнєцова Валерія Євгенівна
Координатор науково-дослідницьких проектів
факультету кібербезпеки, програмної інженерії та комп'ютерних наук
Міжнародний університет
kuznietsova996@gmail.com

Анотація: *Під час виконання різноманітних вантажних робіт значна кількість травм працівників пов'язана з фізичним перевантаженням, підйомом важких матеріалів та їх транспортуванням територією робочого майданчика [1]. Вирішенням цієї проблеми команда здобувачів факультету кібербезпеки, програмної інженерії та комп'ютерних наук Міжнародного університету розпочала розробку стартапу «HEX Robot» – системи автоматизованого перевезення вантажів (рис. 1).*

Проект передбачає створення автономної роботизованої платформи для транспортування вантажів із точки А в точку Б за допомогою технології SLAM та алгоритмів штучного інтелекту. Система здатна самостійно будувати маршрут руху, аналізувати навколишнє середовище та здійснювати обхід перешкод у режимі реального часу.

Інформаційне видання

ЗБІРНИК МАТЕРІАЛІВ

Четвертої міжнародної конференції

«Передові технології в інформаційно-комунікаційній інженерії»

Fourth International Conference

“Advanced Technology in Information and Communication Engineering”

(ATICE'2026)

16 липня 2026 року

Відповідальні за випуск: *Д. М. Розенвассер*, *Н. О. Пунченко*
Комп’ютерний набір і верстка *Н. О. Пунченко*
Редактор *Н. О. Пунченко*
Технічні редактори: *І. В. Новітська, Т. М. Стефанчишена*

Підп. до друку 31.08.2026 р. Об’єм електрон. даних 7,18 Мбайт.

Міжнародний університет м. Одеса
Фонтанська дорога 33, Одеса,