МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ ІМЕНІ ВАДИМА ГЕТЬМАНА
ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В ЕКОНОМІЦІ
НАУКОВИЙ ПАРК КНЕУ
PHILIPPS UNIVERSITÄT MARBURG (НІМЕЧЧИНА)
OLD DOMINION UNIVERSITY (США)
SUSTAINABILITY INNOCENTER (ШВЕЦІЯ)
ARENGUKOOSTÖÖ ÜMARLAUD (ЕСТОНІЯ)
AMERICAN UNIVERSITY OF ARMENIA (ВІРМЕНІЯ)
UNIWERSYTET W BIAŁYMSTOKU (ПОЛЬЩА)



ЦИФРОВА ЕКОНОМІКА

Збірник матеріалів III Міжнародної науково-практичної конференції

5-6 червня 2025 р.

КИЇВ 2025

УДК 330:004(06)
Ц75

Упорядник:
Осипова О.І., канд. екон. наук, доцент кафедри математичного моделювання та статистики, КНЕУ імені Вадима Гетьмана

Організаційний комітет конференції

Голова організаційного оргкомітету: **Лук'яненко Д. Г.**, д.е.н., професор.
Члени організаційного комітету:
Антонюк Лариса, д.е.н., професор, проректор з наукової роботи КНЕУ імені Вадима Гетьмана, Україна; **Сільченко Марина**, к.е.н., доцент, проректор з науково-педагогічної роботи та цифрової трансформації КНЕУ імені Вадима Гетьмана, Україна; **Аавік Іті,** менеджер міжнародних проєктів Arengukoostöö Ümarlaud, Естонія; **Ващаєв Сергій,** к.е.н., доцент, директор навчально-наукового інституту «Інститут інформаційних технологій в економіці КНЕУ імені Вадима Гетьмана», Україна; **Великоіваненко Галина**, к.ф.-м.н., професор, завідувач кафедри математичного моделювання та статистики КНЕУ імені Вадима Гетьмана, Україна; **Джалладова Ірада,** д.ф.-м.н., професор, завідувач кафедри системного аналізу та кібербезпеки КНЕУ імені Вадима Гетьмана, Україна; **Іванець Ірина,** к.е.н., доцент інституційної економіки Philipps Universität Marburg, Німеччина; **Іщук Ярослава,** к.е.н., доцент, доцент кафедри математичного моделювання та статистики КНЕУ імені Вадима Гетьмана, Україна; **Красюк Юлія,** к.п.н., доцент, в.о. директора Інституту дистанційної освіти, завідувач кафедри інформатики та системології КНЕУ імені Вадима Гетьмана, Україна; **Кмитюк Тетяна**, к.е.н., доцент, доцент кафедри математичного моделювання та статистики КНЕУ імені Вадима Гетьмана, Україна; **Мазур Маргарита,** к.е.н., доцент, доцент кафедри математичного моделювання та статистики КНЕУ імені Вадима Гетьмана, Україна; **Матвійчук Андрій**, д.е.н., професор, професор кафедри математичного моделювання та статистики КНЕУ імені Вадима Гетьмана, генеральний директор Наукового парку КНЕУ, Україна; **Осипова Ольга**, к.е.н., доцент, доцент кафедри математичного моделювання та статистики КНЕУ імені Вадима Гетьмана, Україна; **Пєтухова Олена**, старший викладач кафедри математичного моделювання та статистики КНЕУ імені Вадима Гетьмана, Україна; **Піскунова Олена**, д.е.н., професор, професор кафедри математичного моделювання та статистики КНЕУ імені Вадима Гетьмана, Україна; **Покойовий Майкл,** PhD., доцент кафедри науки про дані, науковий співробітник Школи статистики науки про дані, Old Dominion University, США; **Притоманова Ольга,** д.ф.-м.н., професор, професор кафедри математичного моделювання та статистики КНЕУ імені Вадима Гетьмана, Україна; **Ружечкова Мирослава,** професор, Uniwersytet w Białymstoku, Республіка Польща; **Скіцько Володимир,** к.е.н., доцент, доцент кафедри математичного моделювання та статистики КНЕУ імені Вадима Гетьмана, Україна; **Фомічов Олександр**, керівник проєктів Sustainability InnoCenter, Швеція.

Рекомендовано до електронного видання
Вченою радою Київського національного економічного університету імені Вадима Гетьмана
Протокол № 11 від 26 червня 2025 р.

Цифрова економіка [Електронний ресурс]: зб. матеріалів ІІІ Міжнародної науково-
Ц75 практичної. конференції, 5-6 червня 2025 р., м. Київ. — К.: КНЕУ, 2025. — 1101 с.
ISBN 978-966-926-559-3
DOI: https://doi.org/10.33111/978-966-926-559-3

Матеріали ІІІ Міжнародної науково-практичної конференції, проведеної на базі Інституту інформаційних технологій в економіці за участю Наукового парку КНЕУ, розкривають сутність трансформацій сучасної економіки, швидкого розвитку цифрових технологій та їх впровадження в секторах промисловості, бізнесі та державному управлінні для підвищення їх ефективності, конкурентоздатності, забезпечення сталого національного розвитку, зростання обсягів виробництва високотехнологічної продукції та благополуччя населення України.

УДК 330:004(06)

Автори опублікованих статей несуть повну відповідальність за достовірність викладеного матеріалу, за правильне цитування джерел та посилання на них та за всі інші відомості. Думки авторів можуть не збігатися з позицією організаційного комітету

Розповсюджувати та тиражувати без офіційного дозволу КНЕУ забороняється

ISBN 978-966-926-559-3 © КНЕУ, 2025

Валькова Н.В. ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ОБЛІКОВОЇ ІНФОРМАЦІЇ 974

Грабарєв А.В., Мозговий С.А. АНАЛІТИЧНІ ЗАСОБИ УПРАВЛІННЯ ПІДПРИЄМСТВОМ В КОНТЕКСТІ INDUSTRY 4.0 978

Губарь О.В. КІБЕРБЕЗПЕКА ПЕРСОНАЛЬНИХ ДАНИХ У HR-АНАЛІТИЦІ: БАЛАНС МІЖ ЕФЕКТИВНІСТЮ ТА ЕТИКОЮ 982

Джалладова І.А., Камінський О.Є., Гребельний А. Б. ШТУЧНИЙ ІНТЕЛЕКТ У ВИЯВЛЕННІ СОЦІОТЕХНІЧНИХ ЗАГРОЗ КІБЕРБЕЗПЕКИ БІЗНЕСУ 985

Калганова В.І., Барташ О.В. ІНФОРМАЦІЙНА ЕТИКА ЯК ІНСТРУМЕНТ ПРОТИДІЇ КОРУПЦІЇ В СОЦІАЛЬНИХ МЕРЕЖАХ 990

Калюх В.О., Потапенко С.Д. АНАЛІТИКА БЕЗПЕКИ В ЗАДАЧАХ БІЗНЕСУ ТА ЕКОНОМІКИ 995

Карєва А. А. АНАЛІТИКА ДАНИХ В РЕАЛЬНОМУ ЧАСІ (REAL TIME DATA ANALYTICS): ПІДХОДИ ТА ІНСТРУМЕНТИ 1000

Колєчкіна Л. М., Лукашевич В.В. СМАРТ-АНАЛІТИКА ДЛЯ ВИЯВЛЕННЯ ФЕЙКОВИХ НОВИН ЯК ІНСТРУМЕНТ КІБЕРБЕЗПЕКИ БІЗНЕСУ 1005

Колєчкіна Л. М., Мещерякова А.І, Середа С.В. ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ТА ЙОГО МОЖЛИВОСТЕЙ ДЛЯ СМАРТ-АНАЛІТИКИ 1009

Колєчкіна Л. М., Оржинський О.О. АНАЛІЗ АДАПТИВНОЇ SEO-СИСТЕМИ З УРАХУВАННЯМ ДИНАМІКИ АЛГОРИТМІВ ПОШУКОВИХ СИСТЕМ ТА ЕЛЕМЕНТИ ЗАХИСТУ 1014

Колєчкіна Л. М., Проценко Я.С. АНАЛІЗ ПРОЦЕСУ СТВОРЕННЯ ПРОЄКТНОЇ ДОКУМЕНТАЦІЇ ПІДПРИЄМСТВА ТА МЕТОДИ ЇЇ ЗАХИСТУ 1017

Кордунов С.Ю. РОЛЬ БІЗНЕС-АНАЛІТИКИ В УПРАВЛІННІ ІТ-ПРОЄКТАМИ: ВІД ІДЕЇ ДО РЕАЛІЗАЦІЇ 1021

Корзаченко О.В., Процькова К-К. SMART GRID ТА АНАЛІТИКА ДАНИХ ЯК ДРАЙВЕРИ ТРАНСФОРМАЦІЇ ЕНЕРГЕТИКИ УКРАЇНИ 1025

Кучмійова Т. С., Орешко А. Ф. КІБЕРРИЗИКИ У ФІНАНСОВОМУ СЕКТОРІ: ЗАПОБІГАННЯ ТА КОНТРОЛЬ 1029

Лазарєва С.Ф., Марченко М.О. ВИКОРИСТАННЯ СМАРТ-ТЕХНОЛОГІЙ В ГАЛУЗІ МЕДІА ДЛЯ ПРИЙНЯТТЯ УПРАВЛІНСЬКИХ РІШЕНЬ В ЦИФРОВУ ДОБУ 1031

Малинка А. Д., Бєгун А.В. ОЦІНЮВАННЯ СТІЙКОСТІ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ В СОЦІАЛЬНИХ МЕРЕЖАХ 1036

Немченко Д.Д., Потапенко С.Д. КІБЕРБЕЗПЕКА ТА БІЗНЕС ПОТРЕБИ В ІНФРАСТРУКТУРНИХ РІШЕННЯХ: КОМПРОМІСИ ТА ВИКЛИКИ 1040

Осадчий М.Л. СМАРТ-АНАЛІТИКА В УПРАВЛІННІ КРИТИЧНО ВАЖЛИВИМИ ІНФРАСТРУКТУРАМИ: ДОСЛІДЖЕННЯ МОРСЬКИХ ПОРТІВ УКРАЇНИ В КОНТЕКСТІ КІБЕРБЕЗПЕКИ 1044

Остапенко Я.О., Даниленко С.В. РОЗРОБКА ОПТИМАЛЬНОЇ СТРАТЕГІЇ КІБЕРЗАХИСТУ З ВИКОРИСТАННЯМ МЕТОДІВ ТЕОРІЇ ІГОР ТА ОПТИМІЗАЦІЇ 1048

Павлов А.Г. МОДЕЛІ ПРОГНОЗУВАННЯ ПРОДАЖІВ НА ОСНОВІ МАШИННОГО НАВЧАННЯ 1051

Остапенко Я.О.,
канд. економічних наук, доцент,
Даниленко С.В.,
здобувачка першого (бакалаврського) рівня вищої освіти,
Державний податковий університет, м. Ірпінь, Україна

РОЗРОБКА ОПТИМАЛЬНОЇ СТРАТЕГІЇ КІБЕРЗАХИСТУ З ВИКОРИСТАННЯМ МЕТОДІВ ТЕОРІЇ ІГОР ТА ОПТИМІЗАЦІЇ

У сучасному цифровому середовищі кіберзагрози набувають дедалі складніших форм. Вони варіюються від простих фішингових атак до складних багаторівневих вторгнень, які використовують соціальну інженерію, шкідливе програмне забезпечення та вразливості нульового дня. У такому контексті традиційні підходи до безпеки вже не здатні повною мірою забезпечити захист інформаційних систем. Це обумовлює необхідність впровадження гнучких, адаптивних та інтелектуально обґрунтованих стратегій кіберзахисту, серед яких особливе місце займають методи теорії ігор та оптимізації.

Саме теорія ігор забезпечує математичну основу для моделювання стратегічної взаємодії між різними суб’єктами, зокрема — між атакуючим та захисником. У сфері кібербезпеки ці взаємодії мають конфліктний характер, що дає змогу застосовувати моделі нульової суми, а також більш складні варіанти з асиметричною інформацією та стохастичними параметрами.

Однією з найбільш поширених моделей у цьому контексті є рівновага Неша, яка описує ситуацію, коли жоден з гравців не може покращити свій виграш, змінюючи стратегію одноосібно. У контексті кібербезпеки це означає досягнення стабільного стану, коли ані атакуючий, ані захисник не мають стимулу змінювати свої дії [6]. Наприклад, система виявлення вторгнень може бути налаштована так, що реагує на найвірогідніші вектори атаки, виходячи з передбачуваних стратегій зловмисника.

Інша важлива модель — Stackelberg Game, у якій один гравець (лідер) приймає рішення першим, а другий (послідовник) реагує, знаючи дії лідера. Цей підхід особливо корисний у ситуаціях, коли захисник розгортає захисні механізми, а зловмисник шукає оптимальні шляхи їх обходу [6]. Наприклад,

захисник може заздалегідь визначити політику автентифікації або поведінкові патерни, а атакуючий змушений адаптувати свою стратегію до цих умов.

Паралеллю до теорії ігор виступають методи оптимізації, які дають змогу формалізувати процес вибору найкращих дій з урахуванням обмежень — ресурсів, часу, бюджету, пропускної здатності систем тощо. Основні типи використовуваних оптимізаційних методів — лінійне програмування (ЛП), цілочислове програмування, нелінійна та стохастична оптимізація[4,5].

У практиці кіберзахисту оптимізація використовується, наприклад, для:

- розміщення засобів моніторингу у мережі,
- планування відповідей на інциденти,
- вибору політик доступу,
- балансування навантаження між різними захисними механізмами.

Особливий інтерес становить поєднання оптимізації з теорією ігор, що дозволяє вирішувати так звані ігрові задачі оптимізації, де оптимальне рішення враховує реакцію противника. Це важливо для розробки адаптивних систем, які не просто реагують на атаки, а й активно протидіють потенційним загрозам, знижуючи ризики ще до їх реалізації.

У 2024 році Kong та ін. запропонували підхід до оптимального розгортання обманних активів у системах кіберзахисту з використанням методу Nash Q-Learning. Це поєднання навчання з підкріпленням та ігрового моделювання у багатогравцевих стохастичних іграх. Згідно з дослідженням, захисники можуть ефективно розміщувати фальшиві активи (honeypots), які відволікають або виявляють зловмисників, ще до того, як ті досягнуть реальних цілей. Такий підхід дає змогу адаптивно коригувати стратегію у динамічному середовищі кіберзагроз [2].

Інше цікаве дослідження, представлене у 2023 році Dragotto та ін., описує модель Critical Node Game, яка дозволяє аналізувати ризики у хмарних інфраструктурах. У цій моделі оцінюється вплив атак на ключові вузли, і за допомогою теорії ігор визначаються найбільш ефективні способи їхнього

захисту. Це дає змогу приймати обґрунтовані рішення в умовах обмеженого бюджету на безпеку та високої невизначеності [1].

У 2025 році Kour та колеги запропонували інтеграцію теорії ігор з моделлю Cyber Kill Chain, яка охоплює весь життєвий цикл кібератаки — від розвідки до виконання цілей. Такий підхід дозволяє моделювати та аналізувати дії атакуючого на кожному етапі атаки, визначаючи, які саме контрзаходи можуть бути найбільш ефективними. Це значно розширює можливості аналітики загроз та підвищує рівень готовності до складних атак [3].

Отже, у сукупності, використання методів теорії ігор та оптимізації дає змогу не лише моделювати поведінку атакуючих і захисників, а й знаходити раціональні, зважені та адаптивні стратегії кіберзахисту. Такий підхід дозволяє організаціям ефективно розподіляти ресурси, зменшувати ризики та підвищувати стійкість інформаційної інфраструктури до загроз різної природи. З огляду на стрімку еволюцію кібератак та обмеженість ресурсів, інтеграція ігрових моделей та оптимізаційних методів стає не просто бажаною, а необхідною умовою забезпечення кіберстійкості у сучасному цифровому середовищі.

Список використаних джерел

1. Dragotto, G., Boukhtouta, A., Lodi, A., & Taobane, M. (2024). The critical node game. *Journal of Combinatorial Optimization*, *47*(5). https://doi.org/10.3390/app14010357

2. Kong, G., Chen, F., Yang, X., Cheng, G., Zhang, S., & He, W. (2023). Optimal deception asset deployment in cybersecurity: A nash q-learning approach in multi-agent stochastic games. *Applied Sciences*, *14*(1), 357. http://dx.doi.org/10.3390/app14010357

3. Kour, R., Karim, R., & Dersin, P. (2025). Modelling cybersecurity strategies with game theory and cyber kill chain. *International Journal of System Assurance Engineering and Management*. https://doi.org/10.1007/s13198-025-02733-4

4. Остапенко Я. О., Замота І. О. Моделювання оптимального виробництва продукції на виробничому підприємстві. Математичне моделювання в економіці. *Міжнародний науковий журнал.* 2018. № 1 (10). С. 139–151.

5. Остапенко Я. О. Економіко-математичне моделювання як інструментарій прогнозування: теоретичний аспект. *International Scientific – Practical Conference Modern Transformation of Economics and Management in the Era of Globalization* : Conference Proceedings. January 29, 2016. Klaipeda : Baltija Publishing, 2016. P. 321–323.

6. Як теорія ігор може допомогти нашому суспільству? 2024. Ucu.edu.: веб-сайт. URL: https://ucu.edu.ua/news/yak-teoriya-igor-mozhe-dopomogty-nashomu-suspilstvu/

Павлов А.Г.,
здобувач третього (наукового) рівня вищої освіти,
Київський національний економічний університет імені Вадима Гетьмана

МОДЕЛІ ПРОГНОЗУВАННЯ ПРОДАЖІВ НА ОСНОВІ МАШИННОГО НАВЧАННЯ

У сучасних умовах високої конкуренції в роздрібній торгівлі ефективне прогнозування продажів відіграє вирішальну роль у плануванні поставок, управлінні запасами, оптимізації персоналу та маркетингових активностей.

Одним із головних викликів у цьому контексті є складність попиту, який піддається впливу як внутрішніх (сезонність, цінова політика), так і зовнішніх чинників (погодні умови, економічні шоки, святкові періоди). Зростання обсягів даних стимулює застосування не лише класичних статистичних підходів, але й сучасних алгоритмів машинного навчання.

У цій роботі здійснено аналіз сучасних методів прогнозування продажів у ритейлі, включаючи класичні моделі часових рядів, регресійні підходи з урахуванням зовнішніх змінних, а також перспективні машинні та гібридні підходи. Окрему увагу приділено порівнянню точності моделей на основі

Наукове видання

ЦИФРОВА ЕКОНОМІКА

Збірник матеріалів III Міжнародної науково-практичної конференції

5-6 червня 2025 р.

Видано в авторській редакції

Підп. до друку 01.07.2025. Формат 60×84/8.
Друк. арк. 45,87. Зам. 25-5939

Київський національний економічний університет імені Вадима Гетьмана
03680, м. Київ, проспект Берестейський, 54/1

Свідоцтво про внесення до Державного реєстру
суб'єктів видавничої справи (серія ДК, № 235 від 07.11.2000)

E-mail: litera@kneu.edu.ua