УДК 004.8:004.056:339.1
DOI https://doi.org/10.32689/maup.it.2025.3.9

В'ячеслав КОВАЛЕВСЬКИЙ
аспірант кафедри інженерії програмного забезпечення,
Державний університет «Житомирська політехніка»,
s.kovalevskyi@gmail.com
***ORCID:** 0000-0001-7144-1899*

Тетяна ВАКАЛЮК
доктор педагогічних наук, професор,
завідувач кафедри інженерії програмного забезпечення,
Державний університет «Житомирська політехніка»,
tetianavakaliuk@gmail.com
***ORCID:** 0000-0001-6825-4697*

ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ У СИСТЕМАХ ЗАХИСТУ СЕРВІСІВ ЕЛЕКТРОННОЇ КОМЕРЦІЇ

Анотація. *У статті розглянуто підходи на основі штучного інтелекту для вдосконалення існуючих систем безпеки сервісів електронної комерції. Разом з постійно зростаючою кількістю транзакцій, що проходять через платформи електронної комерції, розширюється і поле можливостей для атак зловмисників, які дедалі частіше використовують і вдосконалюють автоматизовані системи, що імітують поведінкові шаблони справжніх користувачів. Традиційні системи безпеки з використанням сигнатур та статичними механізмами обмежень погано адаптуються до динамічної зміни тактик зловмисників та потребують подальшого розвитку. Сучасні системи захисту, які використовують системи штучного інтелекту пропонують перехід до неперервного аналізу потоків подій у реальному часі. Це дозволяє детально відстежувати взаємодію користувачів з системою та вчасно реагувати на загрози. Лідери індустрії постійно працюють над розвитком цього напрямку та задають тенденції, що стають стандартами реалізації безпекової складової сервісів електронної комерції. В статті також окреслено переваги поведінкової біометрії, яка дає можливість моделювати індивідуальні особливості користувачів та вибудовувати стійкі профілі для точного відокремлення легітимних сесій від небажаних. Використання методів безперервного машинного навчання та аналізу підвищує швидкість виявлення аномалій серед потоків подій, що відбуваються в системі.*

Методологія. *У статті проведено аналіз сучасних методів використання систем штучного інтелекту, що можуть бути використані для побудови багаторівневої архітектури системи безпеки.*

Наукова новизна. *У роботі узагальнено сучасні методи використання систем штучного інтелекту для протидії актуальним безпековим викликам, що постають перед системами захисту сервісів електронної комерції.*

Висновки. *Інтеграція технологій штучного інтелекту з вже існуючими системами захисту сервісів електронної комерції значно розширює їх можливості адаптуватись до сучасних загроз. Застосування штучного інтелекту з підтримкою моделей неперервного аналізу даних створює збалансовану стратегію захисту сервісів електронної комерції, підвищує точність виявлення небажаної активності, знижує фінансові втрати постачальників послуг та зміцнює довіру кінцевих користувачів до сервісів електронної комерції.*

Ключові слова: *штучний інтелект, електронна комерція, інформаційна безпека, поведінкова біометрія, захист, моделювання.*

Viacheslav KOVALEVSKYI, Tetiana VAKALIUK. USE OF ARTIFICIAL INTELLIGENCE IN SECURITY SYSTEMS OF E-COMMERCE SERVICES

Abstract. *The article considers artificial intelligence based approaches for improving existing security systems of e-commerce services. Along with the constantly growing number of transactions passing through e-commerce platforms, the field of opportunities for malicious attacks also expands, as adversaries more and more often use and refine automated systems that imitate the behavioral patterns of real users. Traditional security solutions that rely on signatures and static threshold mechanisms adapt poorly to the dynamic change of attackers tactics and therefore require further development. Modern protection systems that employ artificial intelligence suggest a move from static checks to continuous, real-time analysis of event streams. This approach makes it possible to observe user interactions with system in detail and to respond to threats in a timely manner. Industry leaders continuously develop this direction and set tendencies that later become common standards for implementing the security component of e-commerce services. The article also outlines the advantages of behavioral biometrics, which allows modeling individual user characteristics and building stable profiles for accurately distinguishing legitimate sessions from unwanted ones. The use of continuous machine-learning and analytical methods increases the speed of anomaly detection within the event flows occurring in the system.*

Methodology. *The article presents an analysis of modern methods of using artificial intelligence systems that can be applied to the development of a multi-layered security system architecture.*

Scientific novelty. *The paper summarizes modern methods of applying artificial intelligence systems to counter current security challenges faced by the protection systems of e-commerce services.*

Conclusions. *The integration of artificial intelligence technologies with existing security systems of e-commerce services significantly expands their ability to adapt to modern threats. Applying artificial intelligence with the support of continuous data-analysis models creates a balanced strategy for protecting e-commerce services, improves the accuracy of detecting unwanted activity, reduces financial losses for service providers, and strengthens the trust of end users in e-commerce services.*

Key words: *artificial intelligence, e-commerce, information security, behavioral biometrics, protection, modeling.*

Постановка проблеми. Постійне збільшення об'ємів використання сервісів електронної комерції супроводжується невід'ємною еволюцією методів шахрайства із залученням прийомів соціальної інженерії, мереж ботів та підробки шаблонів поведінки користувачів, що в свою чергу призводить до малоефективної роботи систем захисту які базуються на використані обмежень порогових значень тих чи інших подій. Для сучасних систем захисту сервісів електронної комерції є необхідним перехід від статичного аналізу подій до гнучкої, неперервної обробки потоків даних, що виникають під час роботи системи. Важливою складовою такого підходу має бути здатність системи захисту швидко виявляти аномалії та відокремлювати сесії користувачів та інший небажаний трафік з високою точністю. Системи штучного інтелекту відіграють суттєву роль у цьому процесі.

Аналіз останніх досліджень і публікацій. Проблема захисту інформаційних систем та безпосередньо сервісів електронної комерції, не втрачає своєї актуальності, та навпаки потребує постійного вивчення і розвитку. Олег Колодізєв, у своїй роботі пропонує використання алгоритмів машинного навчання для виявлення шахрайських дій [3]. Шіні Ренджит (Shini Renjith) описує використання історичних даних користувачів для побудови поведінкових патернів [5]. Дослідники Чанг Жанг (Chang Zhang), Ючен Жанг (Yuchen Zhang) та Фулін Лі (Fullin Li) пропонують метод побудови унікальних характеристик користувача на базі аналізу його шаблонів набору тексту [10]. Алок Джаккула (Alok Jakkula) у своїй статті проводить аналіз загроз які можуть супроводжувати впровадження систем штучного інтелекту у процеси роботи систем електронної комерції. Автор зазначає, що незважаючи на всі переваги та покращення отримані при використанні систем штучного інтелекту, їх інтеграція з системами електронної комерції створює додаткові ризики витоку чутливих даних та вимагає всебічної оцінки безпекових аспектів [6]. Кожен з дослідників аналізує цю проблему, спираючись на власний досвід та специфіку тієї галузі, у якій він працює. Проведений аналіз літератури та публікацій свідчить, що проблема використання систем штучного інтелекту для побудови систем захисту сервісів електронної комерції є багатогранною та потребує подальших досліджень направлених на поєднання різних методів використання систем штучного інтелекту і створення прикладних рішень, що враховуватимуть технологічні та організаційні особливості роботи сервісів електронної комерції.

Метою даної статті є огляд актуальних методів залучення систем штучного інтелекту у процеси моніторингу та моделювання безпекових загроз при побудові систем захисту сервісів електронної комерції та інформаційних систем загалом.

Виклад основного матеріалу. Сервіси електронної комерції стали невід'ємною частиною сучасного світу та глобальної економіки. Вони забезпечують швидкий обіг товарів і послуг, зручність для індивідуальних користувачів, а також гнучкість для розширення і ведення бізнесу загалом. Постійне зростання кількості онлайн транзакцій супроводжується збільшенням нелегітимної діяльності, де особливо гостро стоїть проблема шахрайства та несанкціонованого доступу до персональних та фінансових даних користувачів [2]. За даними компанії Mastercard втрати від шахрайської діяльності у сфері електронної комерції перевищують 40 мільярдів доларів [8]. У своєму щорічному звіті присвяченому використанню платіжних систем у сфері електронної комерції компанія Visa зазначає відчутне зростання кількості шахрайських дій, що спричиняють фінансові збитки, підривають довіру споживачів, а також спонукають компанії витрачати значні ресурси на боротьбу з діями шахраїв. Автори звіту оцінюють втрати компаній у 3% річного доходу [9].

Класичні методи захисту, що використовують статичні правила та ручний моніторинг, все частіше проявляють недостатню ефективність коли стикаються зі складними та швидко еволюціонуючими шахрайськими схемами. Подібні виклики збільшують потребу у використанні технологій штучного інтелекту, які, у режимі реального часу, здатні проводити аналіз великих обсягів даних, виявляти та реагувати на загрози [2].

Впровадження та використання систем штучного інтелекту у якості складової системи захисту сервісів електронної комерції розширює можливості для автоматизації процесів захисту, підвищує точності виявлення аномалій, збільшує швидкість реагування та адаптації до нових видів атак. Використання машинного навчання, поведінкового аналізу дій користувачів та постійне вдосконалення методів використання систем штучного інтелекту у системах захисту сервісів електронної комерції забезпечують проактивний, гнучкий та ефективний захист.

Таким чином можна стверджувати, що застосування систем штучного інтелекту для забезпечення захисту сервісів електронної комерції є не лише сучасною тенденцією, а й необхідною умовою збереження довіри користувачів, підтримки фінансової стабільності бізнесу та готовності до новітніх безпекових викликів [1].

Поєднання системи захисту сервісів електронної комерції з системами машинного навчання надає можливості з побудови моделей, що використовуються для аналізу історичних даних про транзакції та визначенні потенційно небезпечних або небажаних операцій. Виявлення аномалій у поведінці користувачів та обробка великих обсягів даних про транзакції відбувається у режимі реального часу з подальшим використанням отриманих результатів для вдосконалення механізмів захисту, що підвищує загальний рівень захищеності сервісів електронної комерції.

Дослідник Олег Колодізєв, у своїй роботі, присвяченій алгоритмам автоматизованого машинного навчання для виявлення шахрайських дій у цифрових платіжних системах, демонструє, що впровадження подібних систем має значні перспективи для підвищення точності визначення недоброчесних операцій [3].

Пропонується використовувати алгоритми з використанням Баєсівської оптимізації та генетичних алгоритмів для автоматизації вибору архітектури моделі, гіперпараметрів для налаштування моделі та визначення найважливіших змінних з даних. Наступним кроком є створення ансамблів моделей для підвищення точності та надійності обробки даних.

У результаті проведених експериментів із використанням алгоритмів автоматизованого навчання, автор прийшов до висновку, що використані алгоритми автоматизації дозволяють за короткий час розглянути велику кількість варіантів моделей та складу вхідних даних. Побудований ансамбль моделей дозволив виявити до 85.7% шахрайських транзакцій. Водночас точність виявлення шахрайських транзакцій перебувала у діапазоні 79–85% [3].

Серед сучасних загроз сервісам електронної комерції окремо виділяють створення і використання підробних акаунтів користувачів. Дане явище стає значним безпековим ризиком, оскільки фейкові профілі користувачів часто використовуються для проведення небажаних чи відверто шахрайських операцій, маніпуляцій з бонусними програмами, а також для атак на інфраструктуру компаній. Підробні акаунти активно використовують для маніпуляцій з рейтингами та відгуками, спотворення результатів пошуку та рекомендаційних систем.

Під час пікових періодів бот-мережі створюють тисячі акаунтів для скуповування популярних товарів, що призводить до дефіциту для реальних покупців. У звіті компанії Radware, що є постачальником продуктів для кібербезпеки, вказується, що у сезон святкових розпродажів 2024 року понад 57% трафіку сервісів електронної комерції генерували саме боти [4].

Одним з дієвих підходів для виявлення шахрайських акаунтів користувачів сервісів електронної комерції є впровадження алгоритмів, що використовують метод опорних векторів. Використання цього підходу описує у своєму дослідженні Шіні Ренджит (Shini Renjith) [5]. Дослідник пропонує побудову моделі машинного навчання, що буде проводити класифікацію користувачів аналізуючи історичні дані сервісів електронної комерції, зокрема поведінкові патерни користувачів, транзакційні аномалії, характеристики користувацьких профілів, що були зареєстровані в системі (рис. 1).

Досліджуючи подібну проблему, Рауль Деко (Raoul Dekou) пропонує об'єднане використання декількох моделей машинного навчання для отримання кращої продуктивності та точності результатів [7]. Об'єднана модель продемонструвала F1-міру зі значенням 0.73, що виявилось найвищим показником серед протестованих моделей (табл. 1).

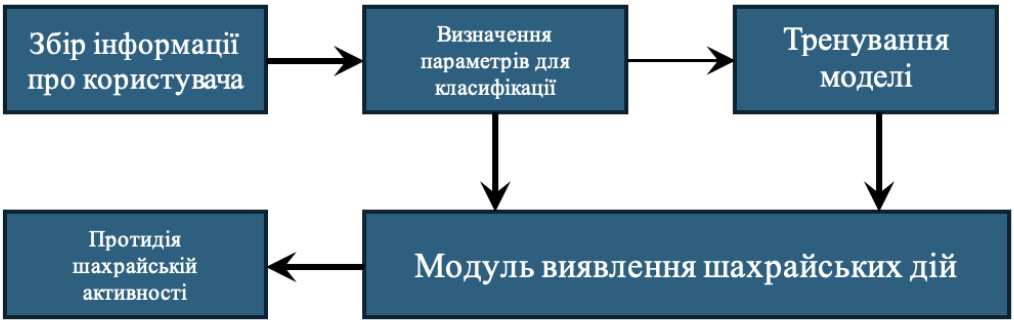

Рис. 1. Запропонований фреймворк для виявлення шахрайських акаунтів [5]

ISSN 2786-5460 (Print), ISSN 2786-5479 (Online)

Таблиця 1

Порівняльна таблиця продуктивності протестованих моделей машинного навчання [7]

Модель	F1	Точність	Повнота	AUC
AutoML	0.7293	0.7206	0.7833	0.9850
Xgb	0.7134	0.7104	0.7165	0.9794
Catboost	0.7127	0.7375	0.6895	0.9809
RF	0.6810	0.7274	0.6401	0.9786

Незважаючи на високу точність визначення шахрайських акаунтів, ця проблема залишається актуальною та вимагає постійного оновлення моделей машинного навчання. Окрім цього присутня загроза помилкового блокування легальних користувачів, особливо новостворених, де відсутня довга історія використання.

Окремо можна виділити перспективний напрямок з використання систем штучного інтелекту для впровадження поведінкової біометрії з безперервною аутентифікацією користувача. Це є суттєвим вдосконаленням систем захисту сервісів електронної комерції.

Концепція даного підходу полягає у неперервній оцінці унікальних шаблонів поведінки користувача та оцінки рівня довіри до нього. До унікальних поведінкових шаблонів користувача можна віднести характер рухів миші, динаміку набору тексту, швидкість переходів між сторінками тощо. Ці параметри можуть бути поєднані з біометричними даними, такими як розпізнавання обличчя, голосу, відбитків пальців. Таким чином створюється унікальний профіль користувача, що значно спрощує виявлення аномалій у його діяльності.

У контексті використання поведінкової біометрії для ідентифікації користувачів дослідники Чанг Жанг (Chang Zhang), Ючен Жанг (Yuchen Zhang) та Фулін Лі (Fullin Li) пропонують метод побудови унікальних характеристик користувача на базі аналізу його шаблонів набору тексту [10].

Автори використовують мультиваріативний процес Хоукса (Multivariate Hawkes Process) з експоненційним ядром для аналізу послідовностей натискання клавіш користувачем. Кожне натискання клавіші розглядається як подія у часовому просторі, де інтенсивність подій залежить від попередніх взаємодій.

У своєму дослідженні для визначення процесу Хоукса автори обрали метод визначення через умовну функцію інтенсивності.

$$\lambda_i(t) := \mu_i(t) + \sum_{j=1}^{D} \int_{-\infty}^{t} g_{ij}(t-\tau) dN_j(\tau) \quad (1)$$

Формула 1. Опис функції інтенсивності визначення процесу Хоукса [10].

Описана вище формула (формула 1) базується на припущенні, що багатовимірний лічильний процес є $N(t) = \{N_i(t)\}^{D}_{i=1}$, де $N(0)=0$, його розмірність дорівнює D, умовна функція інтенсивності має вигляд $\lambda(t) = \{\lambda_i(t)\}^{D}_{i=1}$, μ_i – константа, що визначає інтенсивність виникнення подій типу i. $G(t) = [gij(t)]^{D}i,j=1$ є DxD-вимірною матрицею ядра збудження, а функція збудження $g^{ij} \geq 0$ описує стимул подій, що відбулися в поточному *j*-му вимірі багатовимірного процесу Хоукса на інтенсивність події *i*-го виміру [10].

Дослідники роблять висновки, що процес Хоукса доцільно застосовувати для статистичного опису часових послідовностей натискання клавіш, оскільки його умовна інтенсивність $\lambda(t)$ відтворює самозбудження цієї активності – ймовірність настання події зростає одразу після попередньої та експоненціально згасає з плином часу. Працюючи неперервно, модель зберігає інформаційний зміст інтервалів між подіями без необхідності їх дискретизації, що критично важливо для виявлення відхилень на коротких часових проміжках [10]. Використання процесу Хоукса поєднує точність, інтерпретованість та обчислювальну ефективність, що робить його корисним інструментом для підвищення безпекових параметрів сервісів електронної комерції.

Незважаючи на всі переваги використання систем штучного інтелекту у системах захисту сервісів електронної комерції, слід зазначити, що їх інтеграція у робочі процеси сервісів електронної комерції потребує виваженого аналізу та додаткових перевірок на дотримання вимог безпечної обробки даних. Дослідник Алок Джаккула (Alok Jakkula) у своїй статті підкреслює критичну важливість застосування надійних заходів безпеки при залученні систем штучного інтелекту для опрацювання даних, що використовуються системами електронної комерції, які мають бути поєднані з чіткими та прозорими правилами контролю їх виконання [6].

Висновки. Сучасний захист систем електронної комерції потребує адаптивних рішень, що в режимі реального часу здатні проводити аналіз подій та особливостей поведінки користувачів. Використання систем штучного інтелекту робить це можливим та значно розширює можливості систем захисту сервісів електронної комерції. Застосування такого підходу збільшує точність виявлення аномалій, знижує частку хибних спрацювань і, завдяки прозорій побудові моделей, полегшує аудит рішень прийнятих системою захисту та дотримання нормативних вимог. В свою чергу інтеграція поведінкової біометрії з контекстною оцінкою транзакційних ризиків та мережевим моніторингом формує масштабовану й економічно доцільну багаторівневу систему захисту для сучасних систем електронної комерції. Інтеграція в системи захисту сервісів електронної комерції систем штучного інтелекту на всіх етапах повинна супроводжуватись попереднім аналізом безпекових ризиків та контролем їх роботи.

Список використаних джерел:

1. Музиченко Т. О., Скорба О. А., Шевчук А. А. Штучний інтелект як засіб оптимізації бізнес-процесів в електронній комерції. АКАДЕМІЧНІВІЗІЇ. 2023. № 23. URL: https://academy-vision.org/index.php/av/article/view/696/630.

2. Advancing E-Commerce Security: Strategic Innovations and Future Directions in AI and ML / L. A. A. Gracious et al. *IGI Global Scientific Publishing: International Academic Publisher*. URL: https://www.igi-global.com/chapter/advancing-e-commerce-security/356672.

3. Automatic machine learning algorithms for fraud detection in digital payment systems / O. Kolodiziev et al. *Eastern-European Journal of Enterprise Technologies*. 2020. Vol. 5, no. 9 (107). P. 14–26. URL: https://doi.org/10.15587/1729-4061.2020.212830.

4. Bots now dominate e-commerce traffic, warns Radware report – Intelligent CISO. *Intelligent CISO – Covering Security Across Borders*. URL: https://www.intelligentciso.com/2025/04/29/bots-now-dominate-e-commerce-traffic-warns-radware-report/.

5. Detection of Fraudulent Sellers in Online Marketplaces using Support Vector Machine Approach | Semantic Scholar. *Semantic Scholar*. URL: https://www.semanticscholar.org/reader/ac8972fe41c663b77b6dc99ea95d861ee56e06d2.

6. Jakkula A. R. Ensuring Data Privacy and Security in AI-Enabled E-commerce Platforms. *Journal of Artificial Intelligence & Cloud Computing*. 2024. Vol. 3, no. 1. P. 1–3. URL: https://doi.org/10.47363/jaicc/2024(3)288

7. Machine Learning Methods for Detecting Fraud in Online Marketplaces. / R. Dekou et al. *Conference: 2021 International Workshop on Privacy, Security, and Trust in Computational Intelligence*. URL: https://ceur-ws.org/Vol-3052/paper15.pdf.

8. Mastercard. Ecommerce fraud trends and statistics merchants need to know. *Payment and cybersecurity solutions*. URL: https://b2b.mastercard.com/news-and-insights/blog/ecommerce-fraud-trends-and-statistics-merchants-need-to-know-in-2024/.

9. The 2024 Global eCommerce Payments & Fraud Report. URL: https://www.cybersource.com/content/dam/documents/campaign/fraud-report/global-fraud-report-2024.pdf.

10. Zhang C., Zhang Y., Li F. Feature Extraction of Sequence of Keystrokes in Fixed Text Using the Multivariate Hawkes Process. *Mathematical Problems in Engineering*. 2021. Vol. 2021. P. 1–16. URL: https://doi.org/10.1155/2021/6648726.

Дата надходження статті: 23.09.2025
Дата прийняття статті: 20.10.2025
Опубліковано: 04.12.2025