

випромінювання. Цей підхід дає можливість музеям представляти віртуальні реконструкції артефактів, пропонуючи відвідувачам інтерактивний досвід занурення.

Водночас ці досягнення у відновленні історичних та культурних артефактів, за допомогою технологій штучного інтелекту викликають ряд проблем. Забезпечення історичної автентичності сформованих реконструкцій ґрунтується на основі експертного оцінювання. Автоматизація процесів виявлення відсутніх частин залишається складним завданням. Майбутні вдосконалення допоможуть передбачати інтеграцію експертних знань у моделі на основі штучного інтелекту для керування реставрації з історично точними візерунками та кольорами. Розширення наборів даних для ефективнішого навчання моделей на основі штучного інтелекту допоможе покращити їх здатність формувати точніші реставрації, цифрові копії та двійники.

Поєднання процесів промальовування зображень на основі технологій штучного інтелекту та 3D-реконструкції є значним кроком для збереження культурної спадщини [4]. Завдяки цифровій реставрації артефактів і створенню інтерактивних 3D-моделей технології на основі штучного інтелекту допомагають зберегти культурні та історичні цінності, подолати розрив між збереженням історії та сучасними технологіями.

Технології на основі штучного інтелекту змінюють підходи до збереження об'єктів культурної спадщини, удосконалюючи процеси документування та реставрації артефактів завдяки технологіям комп'ютерного зору та полів нейронного випромінювання. Ці інновації розширюють доступність до цінних історичних артефактів. Проте важливо враховувати виклики, зокрема точність, культурну чутливість і збереження оригінальних творів. Відповідальне використання технологій та співпраця між фахівцями у сфері інформаційних технологій і культури є ключовими для збереження автентичності історичної спадщини.

#### Список посилань

1. Gaber, J. A., Youssef, S. M., and Fathalla, K. M.: "The role of artificial intelligence and machine learning in preserving cultural heritage and art works via virtual restoration", ISPRS Ann. Photogramm. Remote Sens. Spatial Inf. Sci., X-1/W1-2023, 185–190, <https://doi.org/10.5194/isprs-annals-X-1-W1-2023-185-2023>, 2023.
2. Ibrahim M. AI for Art & Heritage Conservation [Електронний ресурс]. – Режим доступу: <https://www.ultralytics.com/blog/ai-in-art-and-cultural-heritage-conservation>.
3. Stoean, R., Bacanin, N., Stoean, C., & Ionescu, L. Bridging the past and present: AI-driven 3D restoration of degraded artefacts for museum digital display. Journal of Cultural Heritage, 2024, 69, 18-26. <https://doi.org/10.1016/j.culher.2024.07.008>
4. Mazzacca, G., Karami, A., Rigon, S., Farella, E. M., Trybala, P., and Remondino, F.: NERF FOR HERITAGE 3D RECONSTRUCTION, Int. Arch. Photogramm. Remote Sens. Spatial Inf. Sci., XLVIII-M-2-2023, 1051–1058, <https://doi.org/10.5194/isprs-archives-XLVIII-M-2-2023-1051-2023>, 2023.

УДК 512.541.5:004.056.55

Покидько Д.Ю., аспірант  
ПВНЗ «Європейський університет», [denys.pokydko@e-u.edu.ua](mailto:denys.pokydko@e-u.edu.ua)

#### АЛГОРИТМИ ВИЯВЛЕННЯ ТА ЗАПОБІГАННЯ МАНІПУЛЯЦІЯМ У ГЕЙМІФІКОВАНИХ ОСВІТНІХ СЕРЕДОВИЩАХ

Гейміфікація, визначена як використання ігрових елементів у неігрових контекстах [1], підвищує мотивацію студентів у цифрових освітніх платформах. Проте вона вразлива до маніпуляцій, зокрема «фармінгу» — отримання балів чи нагород без засвоєння знань [2]. Фармінг, як форма поведінкових патернів (наприклад, швидке проходження занять через копіювання чи боти), підриває цілі навчання, створюючи потребу в захисних алгоритмах.

Гейміфікована система моделюється як скінченний стохастичний автомат із множинами станів  $S$ , дій  $A$ , ймовірностями переходів  $P(s'|s, a)$  і функцією винагороди  $R(s)$  [3]. Нормальний шлях навчання — послідовність  $S_0 \rightarrow S_1 \rightarrow S_n$ , тоді як фармінг — це аномальний перехід  $S_0 \rightarrow S_n$  з низьким часом  $t_x \ll avg(t)$  виконання (наприклад, 5 секунд замість 300) і якістю, що прямує до нуля  $q_x \approx 0$ . Проблема: стандартна  $R(s)$  не враховує якість, що сприяє маніпуляціям.

В роботі запропоновано чотирьохетапний алгоритм для виявлення фармінгу:

- *збір даних*: послідовності дій  $seq(u)$ , час  $t(a)$ , довжина шляху  $|path|$ , частота  $f(a)$ ;
- *побудова графа*: орієнтований граф  $G = (S, E)$  з вагами  $w(a) = avg(t(a))$ , аналіз через PageRank [6];

- *виявлення аномалій*: DBSCAN групує поведінку, позначаючи шум як фармінг, а LOF обчислює локальні відхилення ( $LOF > 1.8$ ) [5];

- *адаптивна реакція*: ШІ додає завдання зі складністю  $d = d_{base} \cdot (1 + P_{anomaly})$ , де  $P_{anomaly} = \frac{LOF-1}{LOF_{max}-1}$ .

Для м'якої корекції використовується ШІ, що навчається. LOF тренується на історичних даних  $(t(a), |path|, f(a))$ , без міток, перенавчається щотижня через ковзне вікно [5]. Поріг  $LOF > 1.8$  зменшує хибнопозитивні спрацьовування. ШІ обирає  $n = [P_{anomaly} \cdot 3]$  завдань із бази  $T_{pool}$ , оптимізуючи вибір через Q-learning із винагородою

$$R_{correction} = 0.5 \cdot \Delta t_{new} + 0.3 \cdot completion - 0.2 \cdot abandonment [7].$$

Наприклад: користувач із  $t = 5$  сек отримує два завдання, що підвищують  $t_{new}$  до 60 сек.

Таким чином, запропонований в роботі алгоритмічний підхід ефективно вирішує проблему фармінгу в гейміфікованих освітніх середовищах шляхом поєднання аналізу графів переходів, кластеризації (DBSCAN), виявлення аномалій (LOF) і м'якої корекції через ШІ [5, 6, 7]. Навчання ШІ на історичних даних із щотижневим оновленням забезпечує адаптивність до нових патернів маніпуляцій, а оптимізація корекції через Q-learning зберігає мотивацію користувачів [7]. Новизна полягає в інтеграції цих методів для освіти та унікальній м'якій корекції, що відрізняє підхід від рішень у кібербезпеці [5]. Перспективи включають персоналізацію корекції та використання нейронних мереж для прогнозування фармінгу, що може підвищити ефективність навчальної платформ.

Запропонований алгоритмічний підхід ефективно вирішує проблему фармінгу в гейміфікованих освітніх середовищах шляхом поєднання аналізу графів переходів, кластеризації (DBSCAN), виявлення аномалій (LOF) і м'якої корекції через ШІ [5, 6, 7]. Навчання ШІ на історичних даних із щотижневим оновленням забезпечує адаптивність до нових патернів маніпуляцій, а оптимізація корекції через Q-learning зберігає мотивацію користувачів [7]. Новизна полягає в інтеграції цих методів для освіти та унікальній м'якій корекції, що відрізняє підхід від рішень у кібербезпеці [5]. Перспективи включають персоналізацію корекції та використання нейронних мереж для прогнозування фармінгу, що може підвищити ефективність навчальної платформ.

#### Список посилань

1. Russell, S., & Norvig, P. (2020). Artificial Intelligence: A Modern Approach (4th ed.). Pearson. (для формалізації автоматів)
2. Çeker, E., & Özdaml, F. (2017). What 'Gamification' is and What it's Not. European Journal of Contemporary Education, 6(2), 221–228.
3. Sutton, R. S., & Barto, A. G. (2018). Reinforcement Learning: An Introduction (2nd ed.). MIT Press. (для Q-learning)
4. Alam A., Mohanty A. Foundation for the Future of Higher Education or 'Misplaced Optimism' Being Human in the Age of Artificial Intelligence. Innovations in Intelligent Computing and Communication: First International Conference, ICICC 2022, Bhubaneswar, Odisha, India, December 16-17, 2022, Proceedings. – Cham : Springer International Publishing, 2023. С. 17–29.

5. Huang X. et al. Trends, research issues and applications of artificial intelligence in language education. *Educational Technology & Society*. 2023. Т. 26. № 1. С. 112–131.

6. García-Peñalvo F. J. The perception of Artificial Intelligence in educational contexts after the launch of ChatGPT: Disruption or Panic. 2023, <http://repositorio.grial.eu/handle/grial/28-38>

7. Huang X. et al. Trends, research issues and applications of artificial intelligence in language education. *Educational Technology & Society*. 2023. Т. 26. № 1. С. 112–131.

УДК 004.08: 621.37

**Ярова І.А., канд. техн. наук, доцент**

yarova@op.edu.ua

**Дідик Є.Ю., бакалаврант**

Національний університет «Одеська політехніка», 10252751@stud.op.edu.ua

## **ДОСЛІДЖЕННЯ ВРАЗЛИВОСТЕЙ RFID-СИСТЕМ В КІБЕРПРОСТОРИ**

В сучасних промислових і комерційних процесах контроль переміщення різноманітних об'єктів або осіб реалізується шляхом впровадження технологій радіочастотної ідентифікації, або RFID-технологій (Radio-Frequency Identification Technology). Використання RFID-технологій для ідентифікації, відстеження й управління матеріальними ресурсами має низку переваг, до яких належать висока швидкість та ефективність функціонування систем, відсутність вимог, пов'язаних із прямим візуальним контролем міток (що дозволяє зекономити на системах освітлення), підвищена стійкість до природних впливів (забруднення, висока вологість). Але водночас самі принципи функціонування інтелектуальних автоматизованих систем зумовлюють загрози, пов'язані з можливістю несанкціонованого доступу до даних, переданих між RFID-мітками і зчитувачами. Можливість використання RFID-систем у різних сферах – від логістики та торгівлі до контролю безпеки та доступу до об'єктів – підтверджує важливість захисту цих систем від загроз в кіберпросторі.

RFID-системи є програмно-апаратними комплексами, що складаються з трьох основних компонентів: RFID-міток для збереження і передавання даних по переміщуваних об'єктах, RFID-зчитувачів – пристроїв для зчитування і передавання інформації, та програмного забезпечення – централізованої системи управління даними. Ці елементи спільно забезпечують передачу інформації між об'єктами і системою управління, що дозволяє автоматизувати процеси відстеження та ідентифікації неживих і живих об'єктів. RFID-зчитувачі можуть встановлюватися у різних об'єктах: торгових центрах, підприємствах, транспортних засобах, забезпечуючи безконтактний обмін даними в режимі реального часу. Використання цих систем дозволяє контролювати доступ до приміщень, вести облік продукції на складі та організовувати різні автоматизовані процеси.

Процес функціонування RFID-системи зазвичай складається з кількох етапів. На першому етапі за допомогою RFID-терміналу завантажуються завдання по інвентаризації. Далі на терміналі обирається тип інвентаризації (повна або за певним фільтром) і за допомогою курка або кнопки запускається процес зчитування міток. Для цього не потрібно наводити термінал на мітку, а достатньо здійснювати рух в бік ОЗ з мітками на відстані від 10 см до 10 м, періодично змінюючи положення терміналу. Про всі виявлені мітки термінал сповіщає звуковим сигналом, а знайдені мітки позначаються відповідним символом на екрані. Натиснувши на терміналі на назву мітки, можна зайти в картку ОЗ, переглянути і при необхідності змінити інформацію про ОЗ (наприклад, місцезнаходження, стан тощо). Після закінчення інвентаризації результати вивантажуються на сервер.

Вразливості RFID-систем можна поділити на чотири основні групи [2]. Перш за все, це вразливості, пов'язані з клонуванням RFID-міток. Використання відкритих стандартів без захищених каналів зв'язку дозволяє зловмисникам клонувати мітки для отримання