

*Савінков Н.Д. аспірант
спеціальності 051 Економіка
Денісова О.О. доцент
кафедри інформаційних систем в економіці
Київський національний економічний
університет імені Вадима Гетьмана , Київ*

ГЕЙМІФІКАЦІЯ ОСВІТНЬОГО ПРОЦЕСУ ЗА ДОПОМОГОЮ ШТУЧНОГО ІНТЕЛЕКТУ

Сучасні освітні методики зазнають суттєвих трансформацій під впливом цифрових технологій, серед яких особливу роль відіграє гейміфікація. Впровадження ігрових механік у навчальний процес сприяє підвищенню мотивації студентів, їхньої залученості та результативності навчання. Використання штучного інтелекту (ШІ) у гейміфікованих системах відкриває перспективи для впровадження адаптивного навчання, персоналізованих завдань та інтерактивних засобів взаємодії. Дослідження підтверджують ефективність застосування ШІ у вдосконаленні навчальних стратегій, що сприяє покращенню рівня засвоєння знань і розвитку критичного мислення.

Гейміфікація освітнього процесу передбачає застосування ігрових механізмів, таких як рівневий прогрес, система винагород, рейтинги та інтерактивні сценарії, що стимулюють когнітивну активність студентів. Однак традиційні методи гейміфікації мають обмежену гнучкість, оскільки потребують значних ресурсів для адаптації завдань та оцінювання прогресу. Інтеграція ШІ дозволяє автоматизувати ці процеси, забезпечуючи динамічну персоналізацію навчального контенту відповідно до когнітивних характеристик кожного учня. Одним із ключових аспектів застосування ШІ є адаптивне навчання, що базується на алгоритмах машинного навчання, які аналізують індивідуальні освітні траєкторії студентів. Використання великих даних дозволяє автоматично формувати персоналізовані завдання, коригувати рівень складності навчального матеріалу та прогнозувати можливі труднощі у засвоєнні знань. Наприклад, системи на основі ШІ можуть змінювати сценарії навчальних ігор відповідно до рівня компетентності студента, що забезпечує більш ефективний навчальний процес. Інтеграція ШІ у гейміфікацію також сприяє розширенню можливостей використання віртуальних асистентів та чат-ботів, які виконують функції інтелектуальних наставників. Такі системи, що базуються на обробці природної мови, дозволяють забезпечити негайний зворотний зв'язок, оптимізувати навчальну діяльність та знизити когнітивне навантаження студентів. Дослідження доводять, що інтерактивна підтримка значно підвищує рівень залученості учнів та сприяє глибшому розумінню матеріалу. ШІ також відкриває нові можливості для аналізу освітніх досягнень шляхом збору та обробки великих масивів даних. Використання прогнозних аналітичних моделей дозволяє не лише оцінювати поточний рівень знань студентів, а й визначати потенційні труднощі, з якими вони можуть зіткнутися. Наприклад, алгоритми можуть ідентифікувати студентів, яким необхідна додаткова підтримка, та пропонувати їм персоналізовані навчальні стратегії для покращення результатів. Крім того, технології ШІ дозволяють створювати реалістичні симуляції та віртуальні навчальні середовища, що значно розширюють можливості практичного навчання. Доповнена та віртуальна реальність у поєднанні з адаптивними навчальними моделями дозволяють відтворювати складні професійні сценарії у безпечному середовищі. Наприклад, симуляційні навчальні програми з використанням ШІ активно застосовуються у підготовці медичних фахівців, інженерів та науковців, що забезпечує формування необхідних професійних компетентностей. Проте широке впровадження ШІ у гейміфікацію навчального процесу супроводжується низкою викликів. Зокрема, актуальними залишаються питання етичності використання персональних даних, потреба у значних фінансових ресурсах для розробки та впровадження ШІ-рішень, а також ризик надмірної автоматизації, що може знизити роль викладача

у навчальному процесі. Важливим завданням є пошук оптимального балансу між традиційними методами навчання та цифровими технологіями для забезпечення ефективного освітнього середовища.

Висновки

Гейміфікація освітнього процесу із залученням штучного інтелекту сприяє підвищенню ефективності навчання, покращенню мотивації студентів та персоналізації освітніх траєкторій. Використання адаптивних навчальних алгоритмів, аналітики великих даних, інтерактивних навчальних середовищ та віртуальних симуляцій дозволяє забезпечити більш інноваційні та результативні підходи до навчання. Водночас, для повноцінної інтеграції ШІ в освітній процес необхідний подальший розвиток нормативної бази, технологічної інфраструктури та етичних стандартів використання штучного інтелекту. Перспективні дослідження у цій галузі сприятимуть подальшому вдосконаленню освітніх технологій та їх адаптації до вимог сучасного суспільства.

Список використаних джерел

1. Deterding, S., Dixon, D., Khaled, R., & Nacke, L. (2011). From game design elements to gamefulness: Defining "gamification". Proceedings of the 15th International Academic MindTrek Conference, 9-15
2. https://znayshov.com/News/Details/heimifikatsiia_zaniat_krashchi_instrumenty_dlia_vchyteliv

Синицький Р. К., аспірант

*Київський національний економічний
університет імені Вадима Гетьмана
rost.sinitsky@kneu.edu.ua*

ZERO TRUST ДЛЯ ЗАКЛАДІВ ВИЩОЇ ОСВІТИ

Україна сьогодні перебуває в умовах гібридної війни, де кіберзагрози становлять одну з найголовніших складових. Гібридна війна – це поєднання військових операцій та кібератак [1].

Кожного року кількість кібератак на нашу країну зростає у все більших масштабах. Найактивніше атакують саме критичні сектори — уряд, оборону, енергетику та телекомунікації. У таких умовах університети залишилися нейтральними, адже деякі наукові установи та інститути є частиною національної інфраструктури і співпрацюють з державою. У 2024 році кількість кібератак на Україну зросла на 69,8%, досягнувши 4315 інцидентів, у порівнянні з 2023 роком, коли було зафіксовано 2541 кіберінцидентів [2]. З розширенням віддаленого навчання, хмарних сервісів і зросла і кількість підключень значно, а традиційний периметр, до якого звикли заклади вищої освіти майже зник. У цій ситуації модель Zero Trust стає дедалі актуальнішою, через можливості захисту важливих активів навіть у разі проникнення, не дозволяючи незваному гостю вільно пересуватися мережею.

Багато компаній або закладів вищої освіти досі захищають мережу периметровими засобами типу фаєрволу. Варто враховувати, що такий підхід має повну "довіру" до користувача, якщо він вже всередині мережі або доступів. Однак така постановка рівня довіри є поганим рішенням, адже будь-яка компрометація дозволяє зловмиснику вільно пересуватися всередині й отримувати доступ до будь-чого.

Концепція нульової довіри полягає в тому, що жодному користувачу чи пристрою не слід довіряти за замовчуванням, адже кожний запит на доступ вважається потенційною загрозою і вимагає обов'язкової перевірки. Основною відміною від традиційного підходу, що вважає